Cisco IOS Dial Technologies Command Reference

July 2011

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Cisco IOS Dial Technologies Command Reference

CONTENTS

Introduction

This book contains the commands to configure and maintain Cisco IOS dial and access applications. These applications are documented in the following parts of the *Cisco IOS Dial Technologies Configuration Guide*:

- Dial Interfaces, Controllers, and Lines
- Modem Configuration and Management
- ISDN Configuration
- Signaling Configuration
- Dial-on-Demand Routing Configuration
- Dial-Backup Configuration
- Dial-Related Addressing Services
- Configuring Virtual Templates and Profiles
- PPP Configuration
- Callback and Bandwidth Allocation Configuration
- Dial Access Specialized Features
- Dial Access Scenarios

Dial Commands

aaa authorization configuration default

To download static route configuration information from the authorization, authentication, and accounting (AAA) server using TACACS+ or RADIUS, use the **aaa authorization configuration default** command in global configuration mode. To remove static route configuration information, use the **no** form of this command.

aaa authorization configuration default {**radius** | **tacacs+**}

no aaa authorization configuration default

Syntax Description

radius	RADIUS static route download.
tacacs+	TACACS+ static route download.

Command Default

No configuration authorization is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Examples

The following example downloads static route information using a TACACS+ server:

```
aaa authorization configuration default tacacs+
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
aaa route download	Enables the download static route feature and sets the amount of time between downloads.
clear ip route download	Clears static routes downloaded from a AAA server.
show ip route	Displays all static IP routes, or those installed using the AAA route download function.

aaa route download

To enable the static route download feature and set the amount of time between downloads, use the **aaa route download** command in global configuration mode. To disable this function, use the **no** form of this command.

aaa route download [*time*] [**authorization** *method-list*]

no aaa route download

Syntax Description

time	(Optional) Time between downloads, in minutes. The range is from 1 to 1440 minutes.
authorization *method-list*	(Optional) Specify a named method list to which RADIUS authorization requests for static route downloads are sent. If these attributes are not set, all RADIUS authorization requests will be sent to the servers that are specified by the default method list.

Command Default

The default period between downloads (updates) is 720 minutes.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.1	This command was integrated into Cisco IOS Release 12.1.
12.2(8)T	The **authorization** keyword was added; the *method-list* argument was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

This command is used to download static route details from the authorization, authentication, and accounting (AAA) server if the name of the router is *hostname*. The name passed to the AAA server for static routes is *hostname-1*, *hostname-2*... *hostname-n*—the router downloads static routes until it fails an index and no more routes can be downloaded.

Examples

The following example sets the AAA route update period to 100 minutes:

```
aaa route download 100
```

The following example sets the AAA route update period to 10 minutes and sends static route download requests to the servers specified by the method list name “list1”:

```
aaa route download 10 authorization list1
```

Related Commands

Command	Description
aaa authorization configuration default	Downloads static route configuration information from the AAA server using TACACS+ or RADIUS.
clear ip route download	Clears static routes downloaded from a AAA server.
show ip route	Displays all static IP routes, or those installed using the AAA route download function.

arap callback

To enable an AppleTalk Remote Access (ARA) client to request a callback, use the **arap callback** command in global configuration mode. To disable callback requests, use the **no** form of this command.

arap callback

no arap callback

Syntax Description

This command has no arguments or keywords.

Command Default

Callback requests are not accepted on lines configured for ARA.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

This command enables the router to accept callback requests from ARA clients. You first have to enable AppleTalk routing on the router and then enable automatic ARA startup on the line. You can use this command with either local username authentication or TACACS+ authentication.

Examples

The following example accepts a callback request from an ARA client:

```
arap callback
```

Related Commands

Command	Description
arap callback	Enables an ARA client to request a callback from an ARA client.
autoselect	Configures a line to start an ARA, PPP, or SLIP session.
ppp bap call	Sets PPP BACP call parameters.
ppp callback (DDR)	Enables a dialer interface that is not a DTR interface to function either as a callback client that requests callback or as a callback server that accepts callback requests.
server (RLM)	Enables the Cisco IOS software to call back clients that request a callback from the EXEC level.
virtual-profile aaa	Enables virtual profiles by AAA configuration.

async default routing

Note Beginning in Cisco IOS Release 12.3(11)T, the **async default routing** command is replaced by the **routing dynamic** command. See the **routing dynamic** command for more information.

To enable the router to pass routing updates to other routers over an asynchronous interface, use the **async default routing** command in interface configuration mode. To disable dynamic addressing, use the **no** form of this command.

async default routing

no async default routing

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(11)T	This command was replaced by the **routing dynamic** command.

Usage Guidelines

Use the **async default routing** command to define the default behavior for router-to-router communication over connections to the AUX port configured as an asynchronous interface. This command is commonly used to enable two routers to communicate over an async dial backup link.

To require a remote user to manually configure routing over connections to the AUX port configured as an asynchronous interface, use the **async dynamic routing** command.

Examples

The following example enables routing over asynchronous interface 0:

```
interface async 0
 async default routing
```

Related Commands

Command	Description
async dynamic routing	Enables manually configured routing on an asynchronous interface.

async dynamic address

To specify dynamic asynchronous addressing, use the **async dynamic address** command in interface configuration mode. To disable dynamic addressing, use the **no** form of this command.

async dynamic address

no async dynamic address

Syntax Description

This command has no arguments or keywords.

Command Default

Dynamic addressing is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You can control whether addressing is dynamic (the user specifies the address at the EXEC level when making the connection) or whether default addressing is used (the address is forced by the system). If you specify dynamic addressing, the router must be in interactive mode and the user will enter the address at the EXEC level.

It is common to configure an asynchronous interface to have a default address and to allow dynamic addressing. With this configuration, the choice between the default address or dynamic addressing is made by users when they enter the **slip** or **ppp** EXEC command. If the user enters an address, it is used, and if the user enters the **default** keyword, the default address is used.

Examples

The following example shows dynamic addressing assigned to asynchronous interface six.

```
interface ethernet 0
 ip address 10.0.0.1 255.0.0.0
interface async 6
 async dynamic address
```

Related Commands

Command	Description
peer default ip address	Specifies an IP address, an address from a specific IP address pool, or an address from the DHCP mechanism to be returned to a remote peer connecting to this interface.

async dynamic routing

To enable manually configured routing on an asynchronous interface, use the **async dynamic routing** command in interface configuration mode. To disable routing protocols, use the **no** form of this command; static routing is still used.

async dynamic routing

no async dynamic routing

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **async dynamic routing** command is commonly used to manually bring up PPP from an EXEC session.

Examples

The following example shows how to enable manually configured routing on asynchronous interface 1. The **ip tcp header-compression passive** command enables Van Jacobson TCP header compression and prevents transmission of compressed packets until a compressed packet arrives from the asynchronous link.

```
interface async 1
 async dynamic routing
 async dynamic address
 async default ip address 10.1.1.2
 ip tcp header-compression passive
```

A remote user who establishes a PPP or SLIP connection to this asynchronous interface can enable routing by using the **/routing** switch or the **ppp/routing** command. However, if you want to establish routing by default on connections to an asynchronous interface, use the **async default routing** command when you configure the interface.

Related Commands

Command	Description
async default routing	Enables the router to pass routing updates to other routers over the AUX port configured as an asynchronous interface.
async dynamic address	Specifies dynamic asynchronous addressing versus default addressing.
ip tcp header-compression	Enables TCP header compression.

async mode dedicated

To place a line into dedicated asynchronous mode using Serial Line Internet Protocol (SLIP) or PPP encapsulation, use the **async mode dedicated** command in interface configuration mode. To return the line to interactive mode, use the **no** form of this command.

async mode dedicated

no async mode dedicated

Syntax Description

This command has no arguments or keywords.

Command Default

Asynchronous mode is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

With dedicated asynchronous network mode, the interface will use either SLIP or PPP encapsulation, depending on which encapsulation method is configured for the interface. An EXEC prompt does not appear, and the router is not available for normal interactive use.

If you configure a line for dedicated mode, you will not be able to use the **async dynamic address** command because there is no user prompt.

Examples

The following example assigns an IP address to an asynchronous line and places the line into network mode. Setting the stop bits to 1 enhances performance.

```
interface async 4
 async default ip address 172.31.7.51
 async mode dedicated
 encapsulation slip

line 20
 location remote computer
 stopbits 1
 speed 115200
```

Related Commands

Command	Description
async dynamic address	Specifies dynamic asynchronous addressing.
async mode interactive	Returns a line that has been placed into dedicated asynchronous network mode to interactive mode, thereby enabling the **slip** and **ppp** EXEC commands.

async mode interactive

To return a line that has been placed into dedicated asynchronous network mode to interactive mode, thereby enabling the **slip** and **ppp** EXEC commands, use the **async mode interactive** command in interface configuration mode. To prevent users from implementing Serial Line Internet Protocol (SLIP) and PPP at the EXEC level, use the **no** form of this command.

async mode interactive

no async mode interactive

Syntax Description

This command has no arguments or keywords.

Command Default

Asynchronous mode is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Interactive mode enables the **slip** and **ppp** EXEC commands. In dedicated mode, there is no user EXEC level. The user does not enter any commands, and a connection is automatically established when the user logs in, according to the configuration.

Examples

The following example places asynchronous interface 6 into interactive asynchronous mode:

```
interface async 6
 async default ip address 172.31.7.51
 async mode interactive
 ip unnumbered ethernet 0
```

Related Commands

Command	Description
async mode dedicated	Places a line into dedicated asynchronous mode using SLIP or PPP encapsulation.
ppp	Starts an asynchronous connection using PPP.
slip	Starts a serial connection to a remote host by using SLIP.

autodetect encapsulation

To enable automatic detection of the encapsulation types operating over a point-to-point link to a specified serial or ISDN interface or dialer interface under Media Gateway Control Protocol (MGCP) network access server (NAS) packages, use the **autodetect encapsulation** command in interface configuration mode. To disable automatic dynamic detection of the encapsulation types on a link, use the **no** form of this command.

autodetect encapsulation {[**lapb-ta**] [**ppp**] [**v120**]}

no autodetect encapsulation {[**lapb-ta**] [**ppp**] [**v120**]}

Syntax Description

lapb-ta	Link Access Procedure, Balanced (LAPB) for an ISDN terminal adapter.
ppp	PPP encapsulation on the interface.
v120	V.120 encapsulation on B channels.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.0(4)T	The **lapb-ta** keyword was added.
12.3(7)YB	Support was added for MGCP NAS packages.
12.4(6)T	Support for MGCP NAS packages was integrated into Cisco IOS Release 12.4(6)T.

Usage Guidelines

At least one encapsulation type must be specified, but you can specify multiple encapsulation types. Encapsulation types can be specified in any order.

Use this command to enable the specified serial or ISDN interface or dialer interface under an MGCP NAS package to accept calls and dynamically change the encapsulation in effect on the interface when the remote device does not signal the call type. For example, if an ISDN call does not identify the call type in the Lower Layer Compatibility fields and is using an encapsulation that is different from the one configured on the interface, the interface can change its encapsulation type dynamically.

This command enables interoperation with ISDN terminal adapters that use V.120 encapsulation but do not signal V.120 in the call setup message. An ISDN interface that by default answers a call as synchronous serial with PPP encapsulation can change its encapsulation and answer such calls.

Autodetection of LAPB traffic on an ISDN terminal adapter is possible by issuing the **lapb-ta** keyword. This allows recognition of incoming LAPB-terminal adapter (TA) calls.

Automatic detection is attempted for 10 seconds after the link is established or the first five packets exchanged over the link, whichever is first.

Examples

The following example configures BRI 0 to call and receive calls from two sites, use PPP encapsulation on outgoing calls, and use Challenge Handshake Authentication Protocol (CHAP) authentication on incoming calls. This example also enables BRI 0 to configure itself dynamically to answer calls that use V.120 but that do not signal V.120.

```
interface bri 0
 encapsulation ppp
 autodetect encapsulation v120
 no keepalive
 dialer map ip 172.17.36.10 name EB1 234
 dialer map ip 172.17.36.9 name EB2 456
 dialer-group 1
 isdn spid1 0146334600
 isdn spid2 0146334610
 isdn T200 1000
 ppp authentication chap
```

The following example enables the LAPB-TA and V.120 protocols for autodetection on the serial interface after you have configured the virtual terminals to handle asynchronous traffic:

```
vty-async
interface serial0:23
 autodetect encapsulation lapb-ta v120
```

The following example enables PPP encapsulation and LAPB-TA and V.120 protocols for autodetection on the dialer interface under an MGCP NAS package:

```
interface Dialer1
 ip unnumbered Loopback1
 encapsulation ppp
 dialer in-band
 dialer idle-timeout 240
 dialer extsig
 dialer-group 1
 autodetect encapsulation ppp v120 lapb-ta
 ppp authentication chap
!
```

Related Commands

Command	Description
encapsulation	Sets the encapsulation method used by the interface.

autohangup

To configure automatic line disconnect, use the **autohangup** command in line configuration mode. To disable automatic line disconnect, use the **no** form of this command.

autohangup

no autohangup

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command causes the EXEC to issue the **exit** command when the last connection closes. The **autohangup** command is useful for the UNIX-to-UNIX Copy Program (UUCP) applications that automatically disconnect lines because UUCP scripts cannot issue the **exit** command to hang up the telephone.

Examples

The following example enables automatic line disconnect on lines 5 through 10:

```
line 5 10
 autohangup
```

Related Commands

Command	Description
exit (EXEC)	Closes an active terminal session by logging off the router.

autoselect

To configure a line to start an Appletalk Remote Access (ARA), PPP, or Serial Line Internet Protocol (SLIP) session, use the **autoselect** command in line configuration mode. To disable this function on a line, use the **no** form of this command.

autoselect {**arap** | **ppp** | **slip** | **during-login** | **timeout** *seconds*}

no autoselect [**timeout**]

Syntax Description

arap	ARA session.
ppp	PPP session.
slip	SLIP session.
during-login	Displays the username or password prompt without the user pressing the Return key. After the user logs in, the autoselect function begins.
timeout *seconds*	Timeout period from 1 to 120 seconds for the autoselect process. This argument applies only when the **arap**, **ppp,** or **slip** keyword functions are enabled and has no effect when the **during-login** keyword function is enabled.

Command Default

ARA session
No timeout default

Command Modes

Line configuration

Command History

Release	Modification
10.3	This command was introduced.
11.3	The following keywords were added: • **during-login** • **no autoselect** • **timeout** *seconds*

Usage Guidelines

This command eliminates the need for users to enter an EXEC command to start an ARA, PPP, or SLIP session.

Note SLIP does not support authentication. For PPP and ARAP, you must enable authentication.

The **autoselect** command configures the Cisco IOS software to identify the type of connection being requested. For example, when a user on a Macintosh running ARA selects the Connect button, the Cisco IOS software automatically starts an ARAP session. If, on the other hand, the user is running SLIP or PPP and uses the **autoselect ppp** or **autoselect slip** command, the Cisco IOS software automatically

starts a PPP or SLIP session, respectively. This command is used on lines making different types of connections. You should configure **autoselect ppp** when the gateway is configured for interactive PPP authentication. You do not need to configure **autoselect ppp** for dedicated PPP configurations.

Note If you configure **autoselect ppp**, you should not configure a **no exec** under the same line; these processes are mutally exclusive.

A line that does not have **autoselect** configured views an attempt to open a connection as noise. The router does not respond and the user client times out.

When a timeout period is configured and the initial sample byte is not received before that timeout period, a default EXEC process (if configured) is initiated.

Note After the modem connection is established, a Return is required to evoke a response, such as to get the username prompt. You might need to update your scripts to include this requirement. Additionally, the activation character should be set to the default and the exec-character-bits set to 7. If you change these defaults, the application cannot recognize the activation request.

Examples

The following example enables ARA on a line:

```
line 3
 arap enable
 autoselect arap
```

The following example enables a timeout of 30 seconds on a PPP-enabled line:

```
line 7
 autoselect ppp
 autoselect timeout 30
```

The following example enables ARA on a line and allows logins from users with a modified CCL script and an unmodified script to log in:

```
line 3
 arap enable
 autoselect arap
 autoselect during-login
 arap noguest if-needed
```

Related Commands

Command	Description
arap use-tacacs	Enables TACACS for ARA authentication.
arap warning time	Sets when a disconnect warning message is displayed.
exec	Allows an EXEC process on a line, use the exec command in line configuration mode.
ppp authentication chap	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
ppp authentication pap	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
ppp bap call	Sets PPP BACP call parameters.
ppp use-tacacs	Enables TACACS for PPP authentication.

backup delay

To define how much time should elapse before a secondary line status changes after a primary line status has changed, use the **backup delay** command in interface configuration mode. To return to the default so that as soon as the primary fails, the secondary is immediately brought up without delay, use the **no** form of this command.

backup delay {*enable-delay-period* | **never**} {*disable-delay-period* | **never**}

no backup delay {*enable-delay-period* | **never**} {*disable-delay-period* | **never**}

Syntax Description

enable-delay-period	Number of seconds that elapse after the primary line goes down before the Cisco IOS software activates the secondary line.
disable-delay-period	Number of seconds that elapse after the primary line comes up before the Cisco IOS software deactivates the secondary line.
never	Secondary line is never activated or deactivated.

Command Default

0 second delay

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.

Usage Guidelines

For environments in which spurious signal disruptions appear as intermittent lost carrier signals, we recommend that you enable some delay before activating and deactivating a secondary line.

For the Cisco 7600 Backup Interface for Flexible UNI feature to work correctly, the enable and disable backup delay must be 0.

Examples

The following example sets a 10-second delay on deactivating the secondary line (serial interface 0); however, the line is activated immediately.

```
interface serial 0
 backup delay 0 10
```

backup interface

To configure an interface as a secondary or dial backup, use the **backup interface** command in interface configuration mode. To disable the interface from serving as a backup, use the **no** form of this command.

Cisco 7200 Series and Cisco 7500 Series Routers Only

backup interface *slot/port-adapter/port*

no backup interface *slot/port-adapter/port*

Other Cisco Routers

backup interface *type number*

no backup interface *type number*

Syntax Description

slot/port-adapter/port	The chassis slot, port adapter, and port number of the interface to configure as a backup. Include a slash (/) between slot, port-adapter, and port (for example, 1/1/1). See your hardware installation manual for the specific slot, port adapter, and port numbers.
type number	Type and port number of the interface being configured as a backup.

Command Default

This command is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.

Usage Guidelines

The interface you define with this command can back up only one other interface.

Routers support only serial and ISDN backup interfaces. Access servers support both asynchronous and serial backup interfaces.

In Cisco IOS Release 12.2(33)SRB1 and later releases, you can configure a backup interface for Gigabit Ethernet on the Cisco 7600 router. The configurations on the primary and backup interfaces must match or the backup interface does not work. Note, however, that if the interface configuration includes the **xconnect** command, you must specify a different virtual circuit ID (VCID) on the primary and backup interfaces.

Examples

The following example sets serial 1 as the backup line to serial 0:

```
interface serial 0
 backup interface serial 1
```

The following example sets gigabitEthernet4/0/1 as the backup interface for gigabitEthernet3/0/1 on the Cisco 7600 router:

```
interface gigabitEthernet 3/0/1
  backup interface gigabitEthernet 4/0/1
```

Related Commands

Command	Description
xconnect	Configures a pseudowire for transporting data over the network.

backup interface dialer

To configure a dialer interface as a secondary or dial backup, use the **backup interface dialer** command in interface configuration mode. To disable this feature, use the **no** form of this command.

backup interface dialer *number*

no backup interface dialer *number*

Syntax Description

number	Dialer interface number to use as the backup interface.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Multiple dialer interfaces can use the same dialer pool, which might have a single ISDN interface as a member. Thus, that ISDN interface can back up different serial interfaces and can make calls to different sites.

Examples

The following example shows the configuration of a site that backs up two leased lines using one BRI. Two dialer interfaces are defined. Each serial (leased line) interface is configured to use one of the dialer interfaces as a backup. Both of the dialer interfaces use dialer pool 1, which has BRI 0 as a member. Thus, BRI 0 can back up two different serial interfaces and can make calls to two different sites.

```
interface dialer0
 ip unnumbered loopback0
 encapsulation ppp
 dialer remote-name Remote0
 dialer pool 1
 dialer string 5550112
 dialer-group 1

interface dialer1
 ip unnumbered loopback0
 encapsulation ppp
 dialer remote-name Remote1
 dialer pool 1
 dialer string 5550134
 dialer-group 1

interface bri 0
 encapsulation PPP
 dialer pool-member 1
 ppp authentication chap
```

```
interface serial 0
 ip unnumbered loopback0
 backup interface dialer 0
 backup delay 5 10

interface serial 1
 ip unnumbered loopback0
 backup interface dialer 1
 backup delay 5 10
```

backup load

To set a traffic load threshold for dial backup service, use the **backup load** command in interface configuration mode. To return to the default value, use the **no** form of this command.

backup load {*enable-threshold* | **never**} {*disable-load* | **never**}

no backup load {*enable-threshold* | **never**} {*disable-load* | **never**}

Syntax Description

enable-threshold	Percentage of the primary line's available bandwidth that the traffic load must exceed to enable dial backup.
disable-load	Percentage of the available bandwidth that the traffic load must be less than to disable dial backup. The transmitted or received load on the primary line plus the transmitted or received load on the secondary line is less than the value entered for the *disable-load* argument to disable dial backup.
never	The secondary line is never activated or deactivated because of the traffic load.

Command Default

No threshold is defined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.

Usage Guidelines

When the transmitted or received load on the primary line is greater than the value assigned to the *enable-threshold* argument, the secondary line is enabled.

The secondary line is disabled when one of the following conditions occurs:

- The transmitted load on the primary line plus the transmitted load on the secondary line is less than the value entered for the *disable-load* argument.
- The received load on the primary line plus the received load on the secondary line is less than the value entered for the *disable-load* argument.

If the **never** keyword is used instead of an *enable-threshold* argument, the secondary line is never activated because of traffic load. If the **never** keyword is used instead of a *disable-load* argument, the secondary line is never activated because of traffic load.

Examples

The following example sets the traffic load threshold to 60 percent of the primary line serial 0. When that load is exceeded, the secondary line is activated and will not be deactivated until the combined load is less than 5 percent of the primary bandwidth.

```
interface serial 0
 backup load 60 5
 backup interface serial 1
```

busyout (port)

To disable a port by waiting for the active services on the specified port to terminate, use the **busyout** command in port configuration mode. To reenable the ports, use the **no** form of this command.

busyout

no busyout

Syntax Description

This command has no arguments or keywords.

Command Default

Busyout is not enabled.

Command Modes

Port configuration

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5800.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

The **busyout** command disables a port by waiting for the active services on the specified port to terminate. Use the **no** form of this command to reenable the ports.

Examples

The following example will disable service processing element (SPE) ports 1 to 10 on slot 1 once active services have terminated:

```
Router(config)# port 1/1 1/10
Router(config-port)# busyout
```

Related Commands

Command	Description
clear port	Resets the NextPort port and clears any active call.
clear spe	Reboots all specified SPEs.
shutdown (port)	Disables a port.
show spe	Displays SPE status.

busyout (privileged EXEC)

To inform a central-office switch that a channel is out-of-service, and to busyout an entire card on a dial shelf and remove it from dial services, use the **busyout** (privileged EXEC) command in privileged EXEC mode. To cancel busyout, use the **no** form of this command.

busyout *shelf/slot/port*

no busyout *shelf/slot/port*

Syntax Description

shelf/slot/port	Shelf number, slot number, and port number. You must include the slash marks.

Command Default

Busyout is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced and supported T1 and T3 only.
12.0	This command was enhanced to support E1 and DMM HMM (Double Modem Module [12] Hex Modem Module [6]).

Usage Guidelines

This command does not terminate an existing call; instead, after you hang up or end a call, a new call cannot be established on a channel that has received a **busyout** command instruction.

Use the **busyout** command before you remove a card from a shelf. The maintenance LED on the card goes ON after all the channels (or calls) have been terminated. The ON LED indicates that it is safe to remove the card from the shelf.

Use this command to busyout digital signal level 0s (DS0s) on a trunk card or all modems on a modem card.

To busyout an individual DS0, use the **ds0 busyout** controller configuration command.

To display the busyout information, use the **show busyout** privileged EXEC command.

Restrictions

If the trunk card is using ISDN signaling, there is a limit on the amount of traffic that the exchange can accept on the signaling channel. The restrictions are as follows:

- A busyout can take 1 or 2 minutes to complete for a T1 or T2 trunk card.
- The **no busyout** command cannot be used within 3 minutes of the **busyout** command and vice versa; otherwise, the command will be rejected.

Examples

The following example enables busyout on the card in dial shelf 5, slot 4, port 1:

```
busyout 5/4/1
```

Related Commands

Command	Description
ds0 busyout (channel)	Forces a DS0 timeslot on a controller into the busyout state.
modem busyout	Disables a modem from dialing or answering calls whereby the disabling action is not executed until the active modem returns to an idle state.
modem busyout-threshold	Maintains a balance between the number of DS0s and modems.
modem shutdown	Abruptly shuts down an active or idle modem installed in an access server or router.
show dial-shelf	Displays information about the dial shelf, including clocking information.

busyout (spe)

To disable active calls on the specified service processing elements (SPEs), use the **busyout** command in SPE configuration mode. To reenable the SPEs, use the **no** form of this command.

busyout

no busyout

Syntax Description

This command has no arguments or keywords.

Command Default

Busyout is not enabled.

Command Modes

SPE configuration

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5800.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

You can perform autodiagnostic tests and firmware upgrades when you put the SPEs in the Busiedout state. Active ports on the specified SPE will change the state of the specified range of SPEs to the BusyoutPending state. The state changes from BusyoutPending to Busiedout when all calls end. Use the **show spe** command to display the state of the range of SPEs. Use the **shutdown** command to override the **busyout** command. Use the **no busyout** command to reenable the SPEs.

Examples

The following example shows all active ports on SPE 1 to 10 on slot 1 being busied out:

```
spe 1/1 1/10
 busyout
```

Related Commands

Command	Description
clear port	Resets the NextPort port and clears any active call.
clear spe	Reboots all specified SPEs.
shutdown (port)	Disables a port.
show spe	Displays SPE status.

call progress tone country

To specify the country code for retrieving the call progress tone parameters from the call progress tone database, use the **call progress tone country** command in global configuration mode. To cancel the previous setting and to generate the call progress tones according to modem settings, use the **no** version of this command.

call progress tone country *country-name*

no call progress tone country *country-name*

Syntax Description

country-name	Selects default call progress tones (ring and cadence settings) for the specified country. Valid entries are: **argentina**, **australia**, **austria**, **belgium**, **brazil**, **canada**, **china**, **colombia**, **cyprus**, **czech-republic**, **denmark**, **finland**, **france**, **germany**, **greece**, **hongkong**, **hungary**, **iceland**, **india**, **indonesia**, **ireland**, **israel**, **italy**, **japan**, **korea**, **luxembourg**, **malaysia**, **mexico**, **netherlands**, **peru**, **philippines**, **poland**, **portugal**, **russia**, **singapore**, **slovakia**, **slovenia**, **south-africa**, **spain**, **sweden**, **switzerland**, **taiwan**, **thailand**, **turkey**, **unitedkingdom**, **usa**, and **venezuela**.

Command Default

Default modem settings. (The *country-name* keyword **northamerica** was the default in Cisco IOS releases earlier than release 12.0(3)XG; **usa** is the default country keyword for Cisco IOS Release 12.0(3)XG and later releases.)

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced.
12.0(4)XI	This command was enhanced with additional country keywords.

Usage Guidelines

Use the **call progress tone country** configuration to specify the country for call progress tone generation. While in many cases the country is chosen automatically on the basis of the modem setting, automatic selection does not work for all users because many modems do not support all countries and many users choose the “us” or “default-t1” or “default-e1” setting on their modem.

This command affects the tones generated at the local interface and does not affect any information passed to the remote end of a connection or any tones generated at the remote end of a connection.

For dial platforms (AS5200, AS5300, and AS5800), call progress tones are used only for the resource pool management application. Resource pool management assumes that the call progress tone selection is global. Select only one call progress tone set, and it will globally override country settings on all ports.

Examples

The following example shows the call progress tone set for Japan tone parameters:

```
call progress tone country japan
```

Related Commands

Command	Description
show call progress tone	Displays the contents of the internal CP tone database for a specific country.

callback forced-wait

To force the Cisco IOS software to wait before initiating a callback to a requesting client, use the **callback forced-wait** command in global configuration mode. To disable the forced waiting period, use the **no** form of this command.

callback forced-wait

no callback forced-wait

Syntax Description

This command has no arguments or keywords.

Command Default

The forced waiting period is not set.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Use this command when the router is calling back a modem that initiated a call, then dropped the connection, but requires a rest period before subsequent input is accepted.

Examples

The following example sets a waiting period during which a callback chat script is delayed from being sent on an outgoing target line:

```
callback forced-wait
```

Related Commands

Command	Description
arap callback	Enables an ARA client to request a callback from an ARA client.
chat-script	Places calls over a modem and logs in to remote systems.
debug callback	Displays callback events when the router is using a modem and a chat script to call back on a terminal line.
ppp callback (DDR)	Enables a dialer interface that is not a DTR interface to function either as a callback client that requests callback or as a callback server that accepts callback requests.
server (RLM)	Defines the IP addresses of the server.
virtual-profile aaa	Enables virtual profiles by AAA configuration.

callback nodsr-wait

To set the time period for which an asynchronous callback waits to see the DSR signal go low after the router signals a hang-up request on the incoming call, use the **callback nodsr-wait** command in line configuration mode. To negate or change the line setting, use the **no** form of this command.

callback nodsr-wait *milliseconds*

no callback nodsr-wait

Syntax Description

milliseconds	The timeout value in a range from 5000 to 30,000 milliseconds (ms). Default is 5000 ms.

Defaults

5000 ms

Command Modes

Line configuration

Command History

Release	Modification
11.2(6.1)P	This command was introduced.

Usage Guidelines

Use the **callback nodsr-wait** command when the dial-out modem takes longer than 5000 ms to drop a carrier after the router signals a hang-up on the incoming call.

Increase the duration of the callback if the **debug callback** command displays the following failed callback attempt message:

```
callback process fail - timeout with DSR up
```

Examples

The following example sets the callback duration to 10 seconds for lines 1/0 to 1/107:

```
line 1/0 1/107
callback nodsr-wait 10000
```

Related Commands

Command	Description
callback forced-wait	Sets a waiting period when DSR signals decrease after a callback, before the router attempts another callback.
debug callback	Displays callback events when the router is using a modem and a chat script to call back on a terminal line.

called-number (modem pool)

To assign a called party number to a pool of modems, use the **called-number** command in modem pool configuration mode. To remove a number from a modem pool, use the **no** form of this command.

called-number *number* [**max-conn** *number*]

no called-number *number* [**max-conn** *number*]

Syntax Description

number	Called number for a modem pool.
max-conn *number*	(Optional) Maximum number of simultaneous connections allowed for the called party number.

Command Default

Disabled

Command Modes

Modem pool configuration

Command History

Release	Modification
11.2P	This command was introduced.

Usage Guidelines

A called party number is a telephone number that is used to reach a remote destination. For example, a mobile laptop dials a called party number to reach the POP of an ISP. Some ISPs set up several called party numbers to enable remote clients to dial in, but to the end user, it appears and functions as one unified service.

Cisco's implementation of a called party number is based on the dialed number identification service (DNIS). You can configure multiple DNIS numbers in a single modem pool. However, the same DNIS number cannot be used in multiple modem pools. Each modem pool must be assigned different DNIS numbers.

Use the **max-conn** option to provide overflow protection, which specifies a maximum number of simultaneous connections that a called party number can consume. For example, if you create one modem pool to serve two or more services or customers, this option guarantees how many modems each service or customer can have access to at any given time.

The Cisco IOS software also includes a feature that simplifies the called number configuration. By using an x variable as the last digit in a called telephone number (for example, issuing the **called-number 408555121x** command), clients dialing different called numbers such as 4085551214 or 4085551215 will automatically be sent to the same modem pool. The x variable is a floating place holder for digits 1 through 9.

Note Modem pools using MICA technologies or Microcom modems support incoming analog calls over ISDN PRI. However, only MICA modems support modem pooling for CT1 and CE1 configurations with channel associated signaling.

Examples

In the following example, the modem pool called v90service is virtually partitioned between two customers using different DNIS numbers. The **pool-range** command assigns modems 1 to 110 to the shared modem pool. The **called-number 5550112 max-conn 55** command assigns the DNIS number 5550112 to the v90service modem pool. The total number of simultaneous connections is limited to 55. The **called-number 5550132 max-conn 55** command assigns the DNIS number 5550132, which is for a different customer, to the same v90service modem pool. The total number of simultaneous connections is also set to 55.

```
modem-pool v90service
 pool-range 1-110
 called-number 5550112 max-conn 55
 called-number 4440132 max-conn 55
```

The following configuration rejects the **pool-range 30** command because modem TTY line 30 is already a member of the modem pool v90service, which was configured in the previous example. Each modem in the access server is automatically assigned to a unique TTY line. TTY line numbers are assigned according to your shelf, slot, or port hardware configuration.

```
modem-pool v34service
# pool-range 30
```

Related Commands

Command	Description
clear modempool-counters	Clears active or running counters associated with one or more modem pools.
modem-pool	Creates a new modem pool or specifies an existing modem pool, which allows you to physically or virtually partition your access server for dial-in and dial-out access.
pool-range	Assigns a range of modems to a modem pool.
show modem-pool	Displays the configuration and connection status for one or more modem pools.

calltracker call-record

To enable call record system logging (syslog) generation for the purpose of debugging, monitoring, or externally saving detailed call record information, use the **calltracker call-record** command in global configuration mode. To disable call record syslog generation, use the **no** form of this command.

calltracker call-record {**terse** | **verbose**} [**quiet**]

no calltracker call-record {**terse** | **verbose**} [**quiet**]

Syntax Description

terse	Generates a brief set of call records containing a subset of the data stored within Call Tracker used primarily to manage calls.
verbose	Generates a complete set of call records containing all of the data stored within Call Tracker used primarily to debug calls.
quiet	(Optional) Call record will be sent only to the configured syslog server and not to the console.

Command Default

Call Tracker call record logging is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

Syslog call records will be generated in the order of ten seconds of call termination. A small delay is needed to ensure that all subsystems finish reporting all appropriate information on call termination. Furthermore, the process of logging is considered a very low priority with respect to normal call processing and data routing. As such, logging all call records can be guaranteed if Call Tracker is properly configured. However, the delay from the time a call actually terminated can vary if the CPU is busy handling higher-priority processes.

Call Tracker records must be found within the History table for at least one minute after call termination for this capability to work. As such, one must ensure that Call Tracker history collection is not disabled with the **calltracker history** configuration options.

Because the call rates possible on a high-capacity access server can be rather large and the information provided by the call records is substantial, simply enabling normal syslog call records can make the use of the console difficult. As such, by using the **quiet** option and having a syslog server configured to capture the call records, the console can be freed from displaying any call records, yet still have the call records captured by a syslog server.

The following informational logs are available:

- CALL_RECORD provides generic data information shared for all call categories. This record is generated for both terse and verbose configuration options.
- MODEM_CALL_RECORD provides overall modem call information for modem calls only. This record is generated for both **terse** and **verbose** configuration options.
- MODEM_LINE_CALL_REC provides modem transport physical layer information used to debug modem connection problems for modem calls only. This record is generated for the **verbose** configuration option only.
- MODEM_INFO_CALL_REC provides modem status information used to debug modem problems for modem calls only. This record is generated for the **verbose** configuration option only.
- MODEM_NEG_CALL_REC provides client-host negotiation information used to debug modem negotiation problems for modem calls only. This record is generated for the **verbose** configuration option only.

Examples

The following example reports the Verbose Call Records for a normal modem call termination:

```
*Nov 16 18:30:26.097: %CALLTRKR-3-CALL_RECORD: ct_hndl=5, service=PPP, origin=Answer,
category=Modem, DS0 slot/cntr/chan=0/0/22, called=71071, calling=6669999, resource
slot/port=1/0, userid=maverick5200, ip=192.9.1.2, mask=255.255.255.0, account id=5,
setup=10/16/1999 18:29:20, conn=0.10, phys=17.12, srvc=23.16, auth=23.16, init-rx/tx
b-rate=31200/33600, rx/tx chars=246/161, time=53.50, disc subsys=ModemDrvr, disc
code=0xA220, disc text= Rx (line to host) data flushing - not OK/EC condition - locally
detected/received DISC frame -- normal LAPM termination

*Nov 16 18:30:26.097: %CALLTRKR-3-MODEM_CALL_REC: ct_hndl=5, prot: last=LAP-M,
attempt=LAP-M, comp: last=V.42bis-Both, supp= V.42bis-RX V.42bis-TX, std: last=V.34+,
attempt=V.34+, init=V.34+, snr=38, sq=3, rx/tx: chars=246/161, ec: rx/tx=22/12, rx bad=46,
rx/tx b-rate: last=33600/33600, low=31200/33600, high=33600/33600,
desired-client=33600/33600, desired-host=33600/33600, retr: local=0, remote=0, fail=0,
speedshift: local up/down=1/0, remote up/down=0/0, fail=0, v90: stat=No Attempt,
client=(n/a), fail=None, time(sec)=52, disc reason=0xA220

*Nov 16 18:30:26.101: %CALLTRKR-3-MODEM_LINE_CALL_REC: ct_hndl=5, rx/tx levl=-17/-16,
phase-jit: freq=0, levl=0, far-end echo-levl=-71, freq offst=0, phase-roll=-98,
round-trip=1, d-pad=None, d-pad comp=0, rbs=0, const=16, rx/tx: sym-rate=3429/3429,
carr-freq=1959/1959, trel-code=0/0, preemph-index=6/0, rx/tx: const-shape=Off/On,
nonlin-encode=Off/On, precode=Off/On, xmit levl-reduct=2/3,
shape=0x1920212120202120202020202020202020202020201F1D191100

*Nov 16 18:30:26.101: %CALLTRKR-3-MODEM_INFO_CALL_REC: ct_hndl=5, general info=0x0, rx/tx
link-layer=264/182, NAKs=0/0, rx/tx ppp-slip=5/7, bad ppp-slip=0, proj max rx b-rate:
client=19200, host=24000, rx/tx: max neg I frame=128/128, neg window=15/15, T401
timeouts=1, tx window closures=0, rx overruns=0, retrans frames=0, v110: rx good=0, rx
bad=0, tx=0, sync-lost=0, ss7/cot=0x00, v42bis size: dict=1024, test err=0, reset=0, v0
synch-loss=0, mail lost: host=0, sp=0, diag=0x00000000000000000000000000000000

*Nov 16 18:30:26.101: %CALLTRKR-3-MODEM_NEG_CALL_REC: ct_hndl=5, v8bis
cap=0x00000000000000000000000000000000000000000000, v8bis
mod-sl=0x00000000000000000000000000000000000000000000000000, v8
jnt-menu=0x01E0C14513942A0000000000000000000000000000000, v8
call-menu=0x01C14513942A000000000000000000000000000000, v90 train=0x00000000, v90
sgn-ptrn=0x00000000, state
trnsn=0x000102030410204042430451FF0000000000000000000000000000000000000000,
phase2=0x010000F4EF221FF37E0001E4EFA21FF2E30001A4EF980101B7CF98003C0000000034EF40000502160
AE0301FFFFE1C07A707A70D650D6500
```

Related Commands

Command	Description
calltracker history max-size	Sets the maximum calls saved in the history table.
calltracker history retain-mins	Sets the number of minutes to save calls in the history table.
show call calltracker history	Displays all information stored within the Call Tracker history database table for the most recent disconnected calls.
show call calltracker summary	Displays Call Tracker activity and configuration information such as the number of active calls and the history table attributes.

calltracker enable

To enable Call Tracker on the access server, use the **calltracker enable** command in global configuration mode. To restore the default condition, use the **no** form of this command.

calltracker enable

no calltracker enable

Syntax Description

This command has no arguments or keywords.

Command Default

Call Tracker is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

To enable real-time call statistics from the MICA technologies modem to Call Tracker, you must configure the **modem link-info poll time** command.

Examples

The following example shows how to enable the Call Tracker feature:

```
calltracker enable
calltracker history max-size number
calltracker history retain-mins minutes
calltracker call-record terse
snmp-server packetsize byte-count
snmp-server queue-length length
snmp-server enable traps calltracker
snmp-server host host community-string calltracker
```

Related Commands

Command	Description
calltracker history max-size	Sets the maximum calls saved in the history table.
calltracker history retain-mins	Sets the number of minutes to save calls in the history table.
debug calltracker	Displays debug messages tracing the Call Tracker processing flow.
dnis	Enables Call Tracker SYSLOG support for generating detailed Call Records.
modem link-info poll time	Sets the polling interval at which link statistics are retrieved from the MICA modem.
show call calltracker active	Displays all information stored within the Call Tracker active database for all active calls.

show call calltracker history	Displays all information stored within the Call Tracker history database table for the most recent disconnected calls.
show call calltracker summary	Displays Call Tracker activity and configuration information such as the number of active calls and the history table attributes.
snmp-server host	Specifies the host to receive Call Tracker traps.

calltracker history max-size

To set the maximum number of call entries stored in the Call Tracker history table, use the **calltracker history max-size** command in global configuration mode. To restore the default value, use the **no** form of this command.

calltracker history max-size *number*

no calltracker history max-size *number*

Syntax Description

number	Maximum call entries to store in the Call Tracker history table. The valid range is from 0 through 10 times the maximum DS0 supported on a platform. A value of 0 prevents any history from being saved.

Command Default

The default maximum is dynamically calculated to be 1 times the maximum DS0 supported on a platform.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

Be careful when extending the maximum number of call entries stored in the Call Tracker history table, as this activity causes Call Tracker to use more memory resources to store the additional call data. Network access server memory consumption must be considered when increasing this parameter. The active call table is not affected by this command.

Examples

The following example sets the history table size to 50 calls:

```
calltracker history max-size 50
```

Related Commands

Command	Description
calltracker history retain-mins	Sets the number of minutes to save calls in the history table.
show call calltracker history	Displays all information stored within the Call Tracker history database table for the most recent disconnected calls.
show call calltracker summary	Displays Call Tracker activity and configuration information such as the number of active calls and the history table attributes.

calltracker history retain-mins

To set the number of minutes for which call entries are stored in the Call Tracker history table, use the **calltracker history retain-mins** command in global configuration mode. To restore the default value, use the **no** form of this command.

calltracker history retain-mins *minutes*

no calltracker history retain-mins *minutes*

Syntax Description

minutes	The length of time to store calls in the Call Tracker history table. The valid range is from 0 through 26,000 minutes. A value of 0 prevents any history from being saved.

Defaults

The default number of minutes is 5000.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

Active calls are not affected by this command. Entries in the active table are retained as long as the calls are connected.

Examples

The following example sets the retention time for the history table to 5000 minutes:

```
calltracker history retain-mins 5000
```

Related Commands

Command	Description
calltracker history max-size	Sets the maximum calls saved in the history table.
show call calltracker history	Displays all information stored within the Call Tracker history database table for the most recent disconnected calls.
show call calltracker summary	Displays Call Tracker activity and configuration information such as the number of active calls and the history table attributes.

calltracker timestamp

To display the millisecond value of the call setup time in the Call Record (CDR) on the access server, use the **calltracker timestamp** command in global configuration mode. To restore the default value, use the no form of this command.

calltracker timestamp msec

no calltracker timestamp msec

Syntax Description

This command has no arguments or keywords.

Command Default

The default value of the call setup time does not contain milliseconds. It is in the hh:mm:ss form.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.3	This command was integrated into Cisco IOS Release 12.3.
12.3T	This command was integrated into Cisco IOS Release 12.3.T.
12.4T	This command was integrated into Cisco IOS Release 12.4T.
12.4	This command was integrated into Cisco IOS Release 12.4.

Usage Guidelines

This AS5400 command is used to add a milliseconds time stamp (hh:mm:ss.ms) to call detail records. These call records of originating and terminating calls are written to flat files on the subscriber server. These files may be passed periodically from the subscriber to the publisher server. Third-party applications such as billing and accounting use CDR data.

All calltracker commands (including **calltracker timestamp**) are only supported for dial services and not for voice.

Examples

The following configuration example shows calltracker options and a display of calltracker active including time stamp:

```
u5400# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
u5400(config)# calltracker ?
  call-record  Generate a SYSLOG Call Record at end of call
  enable       start calltracker
  history      Aspects of the CT History Table
  timestamp    CDR timestamp config
```

```
u5400(config)# calltracker timestamp ?
  msec  Shows millisecond value in timestamp

u5400(config)# calltracker timestamp msec ?
  <cr>

u5400# show call calltracker active
------------------------- call handle = 206 ------------------------------
status-Active, service=PPP, origin=Anser, category-Modem
DSO slot/port/dsl/chan=7/0/0/19, called=40852 68222,calling=(n/a)
userid=myusername, ip=10.1.1.2, mask=10.1.1.2
setup=08/05/2003 192.04.41.645, conn=0.01,phys=23.73,service=16.33,authen=26.33
init rx/tx b-rate=28800/28800,rx/tx chars=0/0
resource slot/port=4/97, mp bundle=0,charged units=0,accontid=198
ibd handle=0x0,tty handle=0x63B4F010,tcb handle=0x0
```

Related Commands

Command	Description
calltracker enable	Enables Call Tracker on the access server.
calltracker history retain-mins	Sets the number of minutes to save calls in the history table.
show call calltracker history	Displays all information stored within the Call Tracker history database table for the most recent disconnected calls.
show call calltracker summary	Displays Call Tracker activity and configuration information such as the number of active calls and the history table attributes.

call-type

To reject particular types of calls, use the **call-type** command in call discriminator profile configuration mode. To disable this feature, use the **no** form of this command.

call-type {**all** | **digital** | **speech** | **v110** | **v120**}

no call-type {**all** | **digital** | **speech** | **v110** | **v120**}

Syntax Description

all	All calls.
digital	Digital calls.
speech	Speech calls.
v110	V.110 calls.
v120	V.120 calls.

Command Default

All calls are accepted by the network access server.

Command Modes

Call discriminator profile configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **call-type** call discriminator command to reject particular types of calls. Call type **all** is mutually exclusive for all other call types. If call type **all** is set in the discriminator, no other call types are allowed. Also, once a DNIS is associated with a call type in a discriminator, it cannot be used in any other discriminator.

Examples

The following example shows the call discriminator being configured to reject speech calls for the call discriminator profile named “userd3”:

```
resource-pool profile discriminator userd3
 call-type speech
```

call-type cas

To statically set the call-type override for incoming channel-associated signaling (CAS) calls, use the **call-type cas** command in DNIS group configuration mode. To disable this service, use the **no** form of this command.

call-type cas {**digital** | **speech**}

no call-type cas {**digital** | **speech**}

Syntax Description

digital	Override call type to digital. The incoming call with the DNIS in the called group is treated as a digital call type.
speech	Override call-type to speech. The incoming call with the DNIS in the called group is treated as a speech call type.

Command Default

No default behavior or values.

Command Modes

DNIS group configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **call-type cas** DNIS group configuration command to set the call-type override. From the resource pooling call-type perspective, use CT1 (CAS) to support either analog calls (speech) or digital calls (switched 56K).

Switched 56K calls are digital calls that connect to High-Level Data Link Control (HDLC) framers. Unlike ISDN, it is impossible to communicate the call type in CT1. Therefore, switched 56K services in CT1 can be differentiated by the DNIS numbers. This command identifies that the call arriving with the DNIS in the DNIS group is assigned to the call type specified in the command.

Examples

The following example shows the DNIS group configuration mode being accessed to use the **call-type cas** command to set the call type override for CAS to **speech**:

```
dialer dnis group modem-group1
 call-type cas speech
```

cas-custom

To customize signaling parameters for a particular E1 or T1 channel group on a channelized line, use the **cas-custom** command in controller configuration mode. To disable the signaling customization, use the **no** form of this command.

cas-custom *channel*

no cas-custom *channel*

Syntax Description

channel	For E1, specifies a single channel group number, which can be from 0 to 30. This channel group number must match the channel number specified in the **cas-group** command. For T1, specifies a single channel group number, which can be between 0 and 23.

Command Default

No customized signaling parameters are set. If you do not specify a country name using the **country** *name* command, which is described in Table 1, ITU is the selected default signal.

Command Modes

Controller configuration

Command History

Release	Modification
11.2P	This command was introduced to support E1 channel groups.
11.3(2)T	This command was implemented on additional Cisco access server and router platforms.
12.0(1)T	This command was implemented on the Cisco 3600 series, and support for T1 channel groups was added.
12.1(5)T	This command was implemented on the Cisco 3600 series, and support for T1 channel groups was added.

Usage Guidelines

The customization parameters set by the **cas-custom** *channel* command are applied to the same channel group number used in the **cas-group** *channel* **timeslots** *range* **type** *signal* command. These channel group numbers must match. Otherwise, the customized features specified by the **cas-custom** command will not be applied to the **cas-group** command's configuration. The signaling customization will not take effect. See Example 1 (T1), page 52.

However, you will not need to configure or set more than one channel group number per E1 line in most cases. Though rarely used, it is possible to split a single E1 (time slots 1 to 31) into two groups (for example, 1 to 15 on group 1 and time slots 17 to 31 in group 2).

Cisco strongly recommends that you use the optional **use-defaults** keyword when specifying a particular country type; see the **country** *name* command in Table 1. This additional keyword ensures that all the local country settings are correctly enabled. For example, issue the **country greece use-defaults** command. If the **use-defaults** option is not specified, generic ITU will be the default setting for all countries. See Example 2 (E1 on AS5800), page 52.

You can configure the system to deviate from a country's default settings as defined by Cisco. To do this, choose from the following list of commands described in Table 1: **ani-digits min** *number* **max** *number*, **answer-signal** {**group-a** | **group-b**} *number*, **caller-digits** *number*, **category** *number*, **dnis-digits min** *number* **max** *number*, **invert-abcd**, **ka** *number*, **kd** *number*, **metering**, **nc-congestion**, and **unused-abcd** *value*. To return a country back to its country specific default settings, issue the **country** *name* **use-defaults** command. To return a country back to the ITU standard, issue the **default country** *name* **use-defaults** command. See Example 4 (Localized E1 R2), page 53 and Example 6 (E1 R2 Country Defaults), page 54.

Beginning in Cisco IOS Release 12.3(11)YK and Cisco IOS Release 12.4(2)T, you can block incoming collect calls for in-line signaling with the double-answer feature, which is activated by entering the **double-answer** keyword. The double-answer feature sends the incoming collect call through a series of answer functions that can last up to two seconds and which causes the switch to drop the collect call while the normal calls stay connected. See Example 7 (E1 Collect Call Blocking).

Note Incoming collect calls in Brazil send a II-8 response and to block such calls, a category B-7 response must be sent instead of the usual answer signal. This is known as category based blocking. Brazil is the only country that supports category based call blocking. If the double-answer feature is configured for Brazil, it will overwrite the category blocking and will not send the category B7 response.

Note Only integrated Cisco MICA technologies modems support E1 R2 signaling on Cisco 5000 series access servers and Cisco 3600 series routers.

Table 1 shows a list of command options in cas-custom mode, which is used to customize R2 signaling settings.

Table 1 Available Commands in cas-custom Mode

CAS Options	Purpose
ani-digits min *number* **max** *number*	Expected number of ANI digits. The minimum number of collected digits is set by **min** *number*. Replace *number* with a value between 0 and 64. The maximum number of collected digits is set by **max** *number*. Replace *number* with a value between 3 and 64. The default is 0 digits, which is the ITU default.
answer-signal {**group-a** | **group-b**} *number*	Answer signal to be used. You can specify the group A signal or the group B signal. The signal *number* can be 1 to 15. Default is group-b 6, which is the ITU default.
caller-digits *number*	Specifies the number of digits the access server needs to collect before it requests ANI or CallerID information. The digits can be from 1 to 10. Default is 1, which is the ITU default.
category *number*	Specifies the type of incoming call, which is mapped to a group signal *number*. Signal numbers from 1 to 15 are available. Default is 1, which is the ITU default.

Table 1 Available Commands in cas-custom Mode (continued)

CAS Options	Purpose
country *name*	Specifies local country settings to use with R2 signaling. Replace the *name* variable with one of the following supported country names. Cisco strongly recommends that you include the **use-defaults** option, which enables the default settings for a specific country. Default country setting is ITU. • **argentina** [**use-defaults**] • **australia** [**use-defaults**] • **brazil** [**use-defaults**] • **china** [**use-defaults**] • **columbia** [**use-defaults**] • **costarica** [**use-defaults**] • **easteurope** [**use-defaults**] The **easteurope** option supports Croatia, Russia, and the Slovak Republic.
	• **ecuador-itu** [**use-defaults**] • **ecuador-lme** [**use-defaults**] • **greece** [**use-defaults**] • **guatemala** [**use-defaults**] • **hongkong-china** [**use-defaults**] The Hong Kong options uses the China variant. • **indonesia** [**use-defaults**] • **israel** [**use-defaults**] • **itu** ITU is the signaling default. ITU provides support for the following list of countries: Denmark, Finland, Germany, Russia (ITU variant), Hong Kong (ITU variant), and South Africa (ITU variant). The expression "ITU variant" means that there are multiple R2 signaling types deployed in the specified country, but Cisco supports the ITU variant. • **korea** [**use-defaults**] • **malaysia** [**use-defaults**] • **newzealand** [**use-defaults**]

Table 1 Available Commands in cas-custom Mode (continued)

CAS Options	Purpose
	• **paraguay** [**use-defaults**] • **peru** [**use-defaults**] • **philippines** [**use-defaults**] • **saudiarabia** [**use-defaults**] • **singapore** [**use-defaults**] • **southafrica-panaftel** [**use-defaults**] The South Africa option uses the Panaftel variant. • **telmex** [**use-defaults**] • **telnor** [**use-defaults**] The telemex and telnor options are used in Mexico. • **thailand** [**use-defaults**] • **uruguay** [**use-defaults**] • **venezuela** [**use-defaults**] • **vietnam** [**use-defaults**]
default	Sets a command to its default setting.
dnis-digits min *number* **max** *number*	Expected number of DNIS digits. The minimum number of collected digits is set by **min** *number*. Replace *number* with a value between 3 and 64. The maximum number of collected digits is set by **max** *number*. Replace *number* with a value between 3 and 64. The default is 0 digits, which is the ITU default.
double-answer	Enables collect call blocking on E1 with R2 digital signaling. Default is that the double-answer feature is turned off.
exit	Takes you out of cas custom mode.
invert-abcd	Inverts the ABCD bits before tx and after rx. This feature is disabled by default, which is the ITU default.
ka *number*	Specifies the KA signal code. You can choose 1 to 15. Default is 0, which is the ITU default.
kd *number*	Specifies the KD signal code. You can choose 1 to 15. Default is 0, which is the ITU default.
metering	Specifies sending a metering pulse when the access server is making an outgoing call. Metering is turned off by default, which is the ITU default.
nc-congestion	Specifies the noncompelled congestion signal. This signal is sent to the central office when the access server is congested and cannot accept the call. The default is B4, which is the ITU default.
no	Negates a command or sets its defaults.
request-category	Specifies a range of 1 to 64, but using this command you either turn on the request-category or turn it off by eliminating the line in your configuration.
unused-abcd *value*	Specifies unused ABCD bit values, which can have a 0 or 1 bit value. This feature is disabled by default, which is the ITU default.

Examples

Example 1 (T1)

The following example enables this feature on channel 1:

```
Router(config)# controller T1 1/0/1
Router(config-controller)# cas-custom 1
```

Example 2 (E1 on AS5800)

The following example displays the available signaling parameters after you enter cas-custom mode. Notice that the same channel group 1 is specified in the **ds0-group** command and the **cas-custom** command.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
Router(config)# controller e1 1/0/1
Router(config-controller)# ds0-group 1 timeslots 1-31 type r2-digital r2-compelled
Router(config-controller)# cas-custom 1
Router(config-ctrl-cas)# ?
CAS custom commands:
  ani-digits     Expected number of ANI digits
  answer-signal  Answer signal to be used
  caller-digits  Digits to be collected before requesting CallerID
  category       Category signal
  country        Country Name
  default        Set a command to its defaults
  dnis-digits    Expected number of DNIS digits
  exit           Exit from cas custom mode
  invert-abcd    invert the ABCD bits before tx and after rx
  ka             KA Signal
  kd             KD Signal
  metering       R2 network is sending metering signal
  nc-congestion  Non Compelled Congestion signal
  no             Negate a command or set its defaults
  unused-abcd    Unused ABCD bit values
```

Example 3 (E1)

The following example displays the available signaling parameters after you enter cas-custom mode. Notice that the same channel group 1 is specified in the **cas-group** command and the **cas-custom** command.

```
Router(config)# controller e1 1
Router(config-controller)# cas-group 1 timeslots 1-31 type r2-digital r2-compelled
Router(config-controller)# cas-custom 1
Router(config-ctrl-cas)# ?

CAS custom commands:
  ani-digits     Expected number of ANI digits
  answer-signal  Answer signal to be used
  caller-digits  Digits to be collected before requesting CallerID
  category       Category signal
  country        Country Name
  default        Set a command to its defaults
  dnis-digits    Expected number of DNIS digits
  exit           Exit from cas custom mode
  invert-abcd    invert the ABCD bits before tx and after rx
  ka             KA Signal
  kd             KD Signal
  metering       R2 network is sending metering signal
  nc-congestion  Non Compelled Congestion signal
  no             Negate a command or set its defaults
  unused-abcd    Unused ABCD bit values
```

Example 4 (Localized E1 R2)

You can localize your R2 configuration for a specific country. Do not forget to include the **use-defaults** option as described in Table 1. For example, use the **country argentina use-defaults** command for a R2 scenario in Argentina.

```
Router(config-ctrl-cas)# country ?

  argentina             Argentina
  australia             Australia
  bolivia               Bolivia
  brazil                Brazil
  bulgaria              Bulgaria
  china                 China
  colombia              Colombia
  costarica             Costa Rica
  croatia               Croatia
  easteurope            East Europe
  ecuador-itu           Ecuador ITU
  ecuador-lme           Ecuador LME
  greece                Greece
  guatemala             Guatemala
  hongkong-china        Hong Kong (China variant)
  india                 India
  indonesia             Indonesia
  israel                Israel
  itu                   ITU
  korea                 Korea
  laos                  LAOS Network (Thailand Variant)
  malaysia              Malaysia
  malta                 Malta
  newzealand            New Zealand
  paraguay              Paraguay
  peru                  Peru
  philippines           Philippines
  saudiarabia           Saudi Arabia
  singapore             Singapore
  southafrica-panaftel  South Africa Panaftel
  telmex                Telmex
  telnor                Telnor
  thailand              Thailand
  uruguay               Uruguay
  venezuela             Venezuela
  vietnam               Vietnam

Router(config-ctrl-cas)# country argentina ?

  use-defaults   Use Country defaults
  <cr>

Router(config-ctrl-cas)# country argentina use-defaults
```

Example 5 (Collect ANI Digits)

The following example customizes the signaling for channel group 1. The configuration collects three digits before it requests ANI information for analog calls received on a Cisco AS5800 in Argentina.

```
Router(config)# cas-custom 1
Router(config-ctrl-cas)# country argentina use-defaults
Router(config-ctrl-cas)# caller-digits 3
Router(config-ctrl-cas)# ^z
```

Example 6 (E1 R2 Country Defaults)

Because cas-custom mode gives you the flexibility to customize R2 parameters, the margin for user error increases. Therefore, the Cisco IOS software enables you to return a country back to its default R2 settings using the **use-defaults** option. The following configuration brings up the Argentina default settings, changes a few customization parameters, then returns the Argentina R2 setting back to its original state.

```
Router(config-ctrl-cas)# country argentina use-defaults
Router(config-ctrl-cas)# caller-digits 3
Router(config-ctrl-cas)# unused-abcd 1
Router(config-ctrl-cas)# metering
Router(config-ctrl-cas)# country argentina use-defaults
```

Example 7 (E1 Collect Call Blocking)

The following example configures the double-answer feature for incoming collect call blocking on the Cisco 2801 with R2 digital signaling with DTMF. The call blocking feature is for all countries.

```
Router(config)# controller e1 4/0
Router(config-controller)# ds0-group 1 timeslot 1 type r2-digital compelled
Router(config-controller)# cas-custom 1
Router(config-controller)# double-answer
```

To disable call blocking, use the **no** form of this command:

```
Router(config-controller)# no double-answer
```

Related Commands

Command	Description
cas-group (E1 controller)	Configures CAS on an E1 controller.
profile incoming	Defines a template formed by directives guiding the CSM to process the digit sequence for a signaling class.
signaling-class cas	Defines a signaling class which specifies the template that processes the ANI/DNIS delimiter.

cas-group (E1 controller)

To configure channel-associated signaling (CAS) on an E1 controller, use the **cas-group** command in controller configuration mode. To disable CAS for one or more time slots, use the **no** form of this command.

cas-group *channel* **timeslots** *range* **type** *signal*

no cas-group *channel* **timeslots** *range* **type** *signal*

Syntax Description

channel	Single channel group number from 0 to 30.
timeslots *range*	Time slot or time slot range, which can be from 1 to 31. You can specify a time slot range (for example, 1-29), individual time slots separated by commas (for example 1, 3, 5), or a combination of the two (for example 1-14, 15, 17-31). The 16th time slot is reserved for out-of-band signaling.
type *signal*	Type of CAS. Configure the signal type that your central office uses. For Cisco 5800 series access servers, replace the *signal* keyword with one of the following signal types: • **e&m-fgb** [**dtmf** [**dnis**] | **mf** [**dnis**]]—Specifies ear and mouth channel signaling with feature group B support, which includes the wink-start protocol. The optional signal tones are DTMF and MF with the option of provisioning DNIS. • **e&m-fgd**—Specifies ear and mouth channel signaling with feature group D support, which includes the wink-start protocol. • **e&m-immediate-start**—Specifies ear and mouth channel signaling with immediate-start support. • **fxs-ground-start**—Specifies Foreign Exchange Station ground-start signaling support. • **fxs-loop-start**—Specifies Foreign Exchange Station loop-start signaling support. • **p7**—Specifies the P7 switch type. • **r2-analog** [**dtmf** | **r2-compelled** [**ani**] | **r2-non-compelled** [**ani**] | **r2-semi-compelled** [**ani**]] • **r2-digital** [**dtmf** | **r2-compelled** [**ani**] | **r2-non-compelled** [**ani**] | **r2-semi-compelled** [**ani**]] • **r2-pulse** [**dtmf** | **r2-compelled** [**ani**] | **r2-non-compelled** [**ani**] | **r2-semi-compelled** [**ani**]] • **sas-ground-start**—Specifies Special Access Station ground-start signaling support. • **sas-loop-start**—Specifies Special Access Station loop-start signaling support.

type *signal* (continued)

For the Cisco 3600 series access servers, replace the *signal* variable with one of the following signal types:

- **r2-analog** {**r2-compelled** [**ani**] | **r2-non-compelled** [**ani**] | **r2-semi-compelled** [**ani**]}
- **r2-digital** {**r2-compelled** [**ani**] | **r2-non-compelled** [**ani**] | **r2-semi-compelled** [**ani**]}
- **r2-pulse** {**r2-compelled** [**ani**] | **r2-non-compelled** [**ani**] | **r2-semi-compelled** [**ani**]}

The following descriptions are provided for the previous R2 syntax bullets:

- **r2-analog**—Specifies R2 ITU Q411 analog line signaling, which reflects the on/off switching of a tone in frequency-division multiplexing circuits (before TDM circuits were created). The tone is used for line signaling.
- **r2-digital**—Specifies R2 ITU Q421 digital line signaling, which is the most common signaling configuration. The A and B bits are used for line signaling.
- **r2-pulse**—Specifies R2 ITU supplement 7 pulse line signaling, which is a transmitted pulse that indicates a change in the line state.
- **dtmf**—Specifies the DTMF tone signaling (Cisco 5800 series access server only).
- **r2-compelled** [**ani**]—Specifies R2 compelled register signaling. You can also specify provisioning the ANI address option.
- **r2-non-compelled** [**ani**]—Specifies R2 noncompelled register signaling.
- **r2-semi-compelled** [**ani**]—Specifies R2 semicompelled register signaling.

Command Default

No CAS is configured on the controller. All R2 signaling types have DNIS turned on by default.

Command Modes

Controller configuration

Command History

Release	Modification
11.2P	This command was introduced.
12.0(1)T	This command was implemented on the Cisco 3600 series.

Usage Guidelines

Use this command to configure support for incoming and outgoing call signals (such as on-hook and off-hook) on each E1 controller.

If you specify the time slot range 1-31, the system software automatically uses the 16th time slot to transmit the channel associated signaling.

The signaling you configure on the access server must match the signaling used by the central office. For example if the central office switch is forwarding R2 analog signaling to a Cisco AS5800, then the access server's E1 controller must also be configured for R2 analog signaling (**r2-analog**).

All R2 signaling options have DNIS support turned on by default. If you enable the **ani** option, the collection of DNIS information is still performed. Specifying the **ani** option does not disable DNIS. DNIS is the number being called. ANI is the caller's number. For example, if you are configuring router A to call router B, then the DNIS number is router B, the ANI number is router A. ANI is very similar to Caller ID.

To customize the R2 signaling parameters, refer to the **cas-custom** controller configuration command. When you enable the **cas-group** command, the **cas-custom** command is automatically setup to be polled for configuration information. However, unless you enable or turn on specific features with the **cas-custom** command, the cas-custom feature has an empty set of signaling parameters.

Note Only integrated MICA modems support E1 R2 signaling on Cisco access servers.

DNIS is automatically collected for modem pools and R2 tone signaling. You do not need to specify the collection of DNIS information with the **cas-group** command. However, if you are using non-R2 tone signaling, the system must be manually configured to collect DNIS information. For non-R2 cas signaling, DNIS collection is done only for E&M-fgb.

Examples

In most cases, you will configure the same channel-associated signaling on each E1 controller. The following examples configure signaling and customized parameters on controller E1 2 using the **cas-group** and **cas-custom** controller configuration commands.

The following example configures the E1 controller on a Cisco 5800 series access server. To configure a Cisco 3600 series access server, replace the command:

controller e1 2/1/0

with the command:

controller e1 2

Note The actual channel associated signaling is configured on the 16th time slot, which is the reason why this time slot does not come up in the following output.

```
Router(config-controller)# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config-controller)# controller e1 2/1/0
Router(config-controller)# cas-group 1 timeslots 1-31 type r2-digital r2-compelled ani

%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 1 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 2 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 3 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 4 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 5 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 6 is up
```

```
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 7 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 8 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 9 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 10 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 11 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 12 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 13 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 14 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 15 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 17 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 18 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 19 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 20 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 21 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 22 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 23 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 24 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 25 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 26 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 27 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 28 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 29 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 30 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 31 is up
```

The following example shows all the supported E1 signaling types on a Cisco AS5800:

```
Router(config-controller)# cas-group 1 timeslots 1-31 type ?

  e&m-fgb              E & M Type II FGB
  e&m-fgd              E & M Type II FGD
  e&m-immediate-start  E & M Immediate Start
  fxs-ground-start     FXS Ground Start
  fxs-loop-start       FXS Loop Start
  p7                   P7 Switch
  r2-analog            R2 ITU Q411
  r2-digital           R2 ITU Q421
  r2-pulse             R2 ITU Supplement 7
  sas-ground-start     SAS Ground Start
  sas-loop-start       SAS Loop Start

Router(config-controller)# cas-group 1 timeslots 1-31 type r2-analog ?

  dtmf               DTMF tone signaling
  r2-compelled       R2 Compelled Register signaling
  r2-non-compelled   R2 Non Compelled Register signaling
  r2-semi-compelled  R2 Semi Compelled Register signaling
  <cr>
```

R2 signaling parameters can be customized with the **cas-custom** controller configuration command:

```
Router(config-controller)# cas-custom 1?

CAS custom commands:
  caller-digits  Digits to be collected before requesting CallerID
  category       Category signal
  country        Country Name
  default        Set a command to its defaults
  exit           Exit from cas custom mode
  invert-abcd    invert the ABCD bits before tx and after rx
  metering       R2 network is sending metering signal
  nc-congestion  Non Compelled Congestion signal
  no             Negate a command or set its defaults
```

cas-group (T1 controller)

To configure channelized T1 time slots with robbed-bit signaling, and R1 channel-associated signaling, use the **cas-group** command in controller configuration mode. To disable signaling for one or more time slots, use the **no** form of this command.

Cisco AS5200, Cisco AS5300, and Cisco AS5800 Series Access Servers

cas-group *channel* **timeslots** *range* **type** *signal*

no cas-group *channel* **timeslots** *range* **type** *signal*

R1 Channel-Associated Signaling

cas-group *channel* **timeslots** *range* **type r1-modified** {**ani-dnis | dnis**}

no cas-group *channel* **timeslots** *range* **type r1-modified** {**ani-dnis | dnis**}

Syntax Description

channel	Single channel group number from 0 to 30.
timeslots *range*	Time slot or time slot range, which can be from 1 to 24 for T1, and from 1 to 31 for E1. You can specify a time slot range (for example, 1-31), individual time slots separated by commas (for example 1, 3, 5), or a combination of the two (for example 1-7, 8, 17-31). The 16th time slot is reserved for out-of-band signaling.
type *signal*	Type of robbed-bit signaling. Replace the *signal* variable with one of the following signal types. The keywords **service**, **data**, and **voice** are used for switched 56K configuration. These keywords are described at the end of this syntax description table. • **e&m-fgb** [**dtmf** [**dnis**] | [**service** {**data | voice**}]] | [**service** {**data | voice**}] | [**mf** [**dnis**] | [**service** {**data | voice**}]]—Specifies ear and mouth channel signaling with feature group B support, which includes the wink-start protocol. Use the options **dtmf** [**dnis**] to configure dual tone multifrequency (DTMF) tone signaling with optional dialed number information server (DNIS) provisioning. Use the options **mf** [**dnis**] to configure MF tone signaling with optional DNIS provisioning. Use the options **service** {**data | voice**} for switched 56K configurations. (See the end of this syntax description table for more information about these switched 56K keywords.) • **e&m-fgd** [**service** {**data | voice**}]—Specifies ear and mouth channel signaling with feature group D support, which includes the wink-start protocol. Use the options **service** {**data | voice**} for switched 56K configurations. (See the end of this syntax description table for more information.) • **e&m-immediate-start** [**service** {**data | voice**}]—Specifies ear and mouth channel signaling with immediate-start support. Use the options **service** {**data | voice**} for switched 56K configurations. (See the end of this syntax description table for more information.)**fxs-ground-start** [**service** {**data | voice**}]—Specifies Foreign Exchange Station ground-start signaling support. Use the options [**service** {**data | voice**} for switched 56K configurations. (See the end of this syntax description table for more information.)

type *signal* (continued)	• **fxs-loop-start** [**service** {**data** | **voice**}]—Specifies Foreign Exchange Station loop-start signaling support. Use the options **service** {**data** | **voice**} for switched 56K configurations. (See the end of this syntax description table for more information.) • **r1-modified ani-dnis**—Indicates R1 signaling will collect ani and dnis information. • **r1-modified dnis**—Indicates R1 signaling will collect only dnis information. • **sas-ground-start** [**service** {**data** | **voice**}]—Specifies Special Access Station ground-start signaling support. Use the options **service** {**data** | **voice**} for switched 56K configurations. (See the end of this syntax description table for more information.) • **sas-loop-start** [**service** {**data** | **voice**}]—Specifies Special Access Station loop-start signaling support. Use the options **service** {**data** | **voice**} for switched 56K configurations. • **service**—(Optional) Specifies the type of services provided for scenarios involving switched 56K connections. Do not include this option in the **cas-group** command statement if you are not using the access server to provide switched 56K connections. • **data**—Enables switched 56K digital data services on the specified range of time slots. The data is directly read from the time slot or channel. Time slots configured with this option will not accept analog modem calls. • **voice**—Enables analog modem services on the specified range of time slots. The call is forwarded to the modems for demodulation. Time slots configured with this option will not accept switched 56K digital calls.

Command Default

For ISDN PRI, the **cas-group** command is disabled.

If the channelized T1 is not configured as a PRI, the default value for line signaling is **e&m-fgb** and the default value for tone signaling is **DTMF**.

The R1 signaling default value is **ani-dnis**.

Command Modes

Controller configuration

Command History

Release	Modification
11.2	This command was introduced.
11.3T	The following signaling keywords were added: • **service** • **data** • **voice** The **R1** keyword was added.

Usage Guidelines

Use the **cas-group** command to configure T1 controllers with different types of robbed-bit signaling, such as on-hook and off-hook for E&M feature group B (**e&m-fgb**).

If you want to collect DNIS information on a T1 controller, you must manually configure it on the access server. DNIS collection is performed only for E&M-fgb. To collect DTMF DNIS for E&M-fgb under a controller T1 configuration, enter the **cas-group 0 timeslots 1-24 type e&m-fgb dtmf dnis** command. To collect MF DNIS for E&M-fgb, enter the **cas-group 0 timeslots 1-24 type e&m-fgb mf dnis** command.

Examples

The following example configures all 24 channels with ear and mouth robbed-bit signaling with feature group B support:

```
Router(config-controller)# controller T1 0
Router(config-controller)# cas-group 1 timeslots 1-24 type e&m-fgb

%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 1 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 2 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 3 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 4 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 5 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 6 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 7 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 8 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 9 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 10 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 11 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 12 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 13 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 14 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 15 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 16 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 17 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 18 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 19 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 20 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 21 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 22 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 23 is up
%DSX0-5-RBSLINEUP: RBS of controller 1 timeslot 24 is up
```

The following example configures the required signaling to support modem pooling and the digital number identification service (DNIS) over channelized T1 lines on a Cisco AS5300. The only supported signaling and tone types for modem pooling over CT1 RBS are E&M feature group B, DTMF tones, and MF tones. By configuring DNIS as part of the **cas-group** command, the system can collect DNIS digits for incoming calls, which can be redirected to specific modem pools setup for different customers or services. Additionally, you must be running MICA modems in the system and have at least 10% of your total modems in the default modem pool. Free modems are needed in the default pool to detect the incoming called number or DNIS before handing the call off to the appropriate modem pool. Therefore, two modems are actually needed to handle each incoming call.

Note Make sure that your switch provides inband address information for incoming analog calls before you enable this feature.

```
controller t1 0
cas-group 0 timeslots 1-24 type e&m-fgb dtmf dnis
exit
```

```
modem-pool accounts1
pool-range 30-50
called-number 2000 max-conn 21
exit
```

The following example configures a Cisco AS5200 to accept switched 56K digital calls on both of its T1 controllers:

```
copy running-config startup-config
```

The following example configures switched 56K digital services and analog modem services on one controller. Each service is assigned its own range of timeslots. Switched 56K calls are assigned to timeslots 1 through 15. Analog modem calls are assigned to timeslots 16 through 24. However, you must use different channel group numbers in each **cas-group** command entry.

```
controller T1 0
cas-group 0 timeslots 1-15 type e&m-fgb service data
cas-group 1 timeslots 16-24 type e&m-fgb service voice
framing esf
clock source line secondary
linecode b8zs
exit
```

The following example configures R1 signaling on a Cisco AS5200 (T1 interface) and specifies the collection of both ANI and DNIS information:

```
cas-group 1 timeslots 1-24 type r1-modified ani-dnis
```

The following example configures R1 modified signaling on a Cisco AS5800 (T1 interface) and specifies the collection of both ANI and DNIS information:

```
Router(config-controller)# cas-group 1 timeslots 1-24 type r1-modified ani-dnis
Router(config-controller)# ^Z
Router(config-controller)# debug csm

Call Switching Module debugging is on

1d16h:%CONTROLLER-5-UPDOWN:Controller E1 1/1/0, changed state to up
*Dec 17 11:27:47.946:allocate slot 4 and port 2 is allocated

*Dec 17 11:27:47.946:CSM v(4/2) c(E1 1/1/0:0):CSM_PROC_IDLE: ev_DSX0_CALL.
*Dec 17 11:27:47.961:CSM v(4/2) c(E1 1/1/0:0):CSM_PROC_IC1_RING: ev_MODEM_OFFHOOK.
*Dec 17 11:27:49.413:CSM v(4/2) c(E1 1/1/0:0):CSM_PROC_IC2_COLLECT_ADDR_INFO:
ev_IC_DNIS_INFO_COLLECTED.
*Dec 17 11:27:50.265:CSM v(4/2) c(E1 1/1/0:0):CSM_PROC_IC2_COLLECT_ADDR_INFO:
ev_IC_ADDR_INFO_COLLECTED.
*Dec 17 11:27:50.265:CSM v(4/2) c(E1 1/1/0:0):CSM_PROC_IC4_WAIT_FOR_CARRIER:
ev_DSX0_CONNECTED.

Router# show modem csm 1/4/2

VDEV_INFO:slot 4, port 2
vdev_status(0x00000001):VDEV_STATUS_ACTIVE_CALL.
csm_state(0x00000205)=CSM_IC5_CONNECTED, csm_event_proc=0x60665CB0, current call thru
Channelize line
invalid_event_count=0, wdt_timeout_count=0
watchdog timer is not activated
wait_for_dialing:False, wait_for_bchan:
pri_chnl=(E1 1/1/0:0), vdev_chnl=(s4, c2)
start_chan_p=0, chan_p=61994BC4, time_slot=0
The calling party phone number =
The called party phone number  = 6789
ring_no_answer=0, ic_failure=0, ic_complete=1
dial_failure=0, oc_failure=0, oc_complete=0
```

```
oc_busy=0, oc_no_dial_tone=0, oc_dial_timeout=0
remote_link_disc=0, busyout=0, modem_reset=0
call_duration_started=1d16h, call_duration_ended=00:00:00, total_call_duration=00:00:00

Router# debug mica msm

MICA modems state machine debugging is on
DA-Slot4#
1d16h:Msm2:MSM_IN_SERVICE:n_ring_ind:cc0x200 si5 dc3 ms0 cr56000,75
1d16h:Msm2:MSM_PREPARE:m_state_trans:newst MODEM_STATE_SETUP
1d16h:Msm2:MSM_SETUP:m_dig_det:di=0x23(#)
1d16h:Msm2:MSM_COLLECTING_DNIS:m_dig_det:di=0x41(A)
1d16h:Msm2:MSM_COLLECTING_DNIS:m_dig_det:di=0x36(6)
1d16h:Msm2:MSM_COLLECTING_DNIS:m_dig_det:di=0x37(7)
1d16h:Msm2:MSM_COLLECTING_DNIS:m_dig_det:di=0x38(8)
1d16h:Msm2:MSM_COLLECTING_DNIS:m_dig_det:di=0x39(9)
1d16h:Msm2:MSM_COLLECTING_DNIS:m_dig_det:di=0x42(B)
1d16h:Msm2:MSM_COLLECTING_ANI_PREFIX:m_dig_det:di=0x23(#)
1d16h:Msm2:MSM_COLLECTING_ANI:m_dig_det:di=0x41(A)
1d16h:Msm2:MSM_COLLECTING_ANI:m_dig_det:di=0x42(B)
1d16h:Msm2:MSM_COLLECTING_ANI_SUFFIX:t_timeout:
1d16h:Msm2:MSM_CALL_VERIFICATION:n_call_acc:
1d16h:Msm2:MSM_TRAING_NEGNG:m_state_trans:newst MODEM_STATE_CONNECT
1d16h:Msm2:MSM_TRAING_NEGNG:m_state_trans:newst MODEM_STATE_LINK
1d16h:Msm2:MSM_TRAING_NEGNG:m_state_trans:newst MODEM_STATE_TRAINUP
1d16h:Msm2:MSM_TRAING_NEGNG:m_state_trans:newst MODEM_STATE_EC_NEGOTIATING
1d16h:Msm2:MSM_TRAING_NEGNG:m_state_trans:newst MODEM_STATE_STEADY_STATE
```

channel-group

To configure serial WAN on a T1 or E1 interface, use the **channel-group** command in controller configuration mode. To clear a channel group, use the **no** form of this command.

Cisco 2600 Series

channel-group *channel-group-number* **timeslots** *range* [**speed** {**56** | **64**}] [**aim** *aim-slot-number*]

no channel-group *channel-group-number*

Cisco 2611 (Cisco Signaling Link Terminal [SLT])

channel-group *channel-number*

no channel-group *channel-number*

Cisco 2600XM Series, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, and Cisco 3745

channel-group *channel-group-number* {**timeslots** *range* [**speed** {**56** | **64**}] | **unframed**} [**aim** *aim-slot-number*]

no channel-group [*channel-group-number* **timeslots** *range*]

Cisco AS5350 and Cisco AS5400 Series

channel-group *channel-group-number*

no channel-group *channel-group-number*

Cisco MC3810

channel-group *channel-number* **timeslots** *range* [**speed** {**56** | **64**}]

no channel-group [*channel-number* **timeslots** *range*]

Syntax Description

channel-group-number	Channel-group number on the Cisco 2600 series, Cisco 2600XM, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, and Cisco 3745 routers. When a T1 data line is configured, channel-group numbers can be values from 0 to 23. When an E1 data line is configured, channel-group numbers can be values from 0 to 30. Valid values can be 0 or 1 on the Cisco AS5350 and Cisco AS5400.

timeslots *range*	Specifies one or more time slots separated by commas, and spaces or ranges of time slots belonging to the channel group separated by a dash. The first time slot is numbered 1. • For a T1 controller, the time slots range from 1 to 24. • For an E1 controller, the time slots range from 1 to 31. You can specify a time slot range (for example, 1-29), individual time slots separated by commas (for example 1, 3, 5), or a combination of the two (for example 1-14, 15, 17-31). See the "Examples" section for samples of different timeslot ranges.
speed {**56** | **64**}	(Optional) Specifies the speed of the underlying DS0s in kilobits per second. Valid values are 56 and 64. The default line speed when configuring a T1 controller is 56 kbps on the Cisco 2600 series, Cisco 2600XM series, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, Cisco 3745, and Cisco MC3810. The default line speed when configuring an E1 controller is 64 kbps on the Cisco 2600 series, Cisco 2600XM series, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, Cisco 3745, and Cisco MC3810. The line speed controls real-time (VBR-RT) traffic shaping, and the maximum burst size (MBS) is 255 cells.
aim *aim-slot-number*	(Optional) Directs HDLC traffic from the T1/E1 interface to the AIM-ATM-VOICE-30 digital signaling processor (DSP) card on the Cisco 2600 series, Cisco 2600XM series, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, and Cisco 3745.
channel-number	Number of the channel. Valid values can be 0 or 1 on the Cisco SLT (Cisco 2611).
unframed	Specifies the use of all 32 time slots for data. None of the 32 time slots is used for framing signals on the Cisco 2600XM series, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, and Cisco 3745. This keyword is applicable to E1 only.

Command Default

The T1/E1 line is connected to the Motorola MPC-860x processor serial communication controller (SCC) or network module with two voice or WAN interface card (VIC or WIC) slots and 0/1/2 FastEthernet ports DSCC4 by default on Cisco 2600 series, Cisco 2600XM, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, and Cisco 3745 routers.

There is no default behavior or values on the Cisco SLT (Cisco 2611).

The serial interface object encapsulation is set to HDLC on a network access server (NAS) (Cisco AS5350 and Cisco AS5400 series routers).

The default line speed is 56 kbps when a T1 controller is configured on the Cisco 2600 series, Cisco 2600XM series, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, Cisco 3745, and the Cisco MC3810.

The default line speed is 64 kbps when an E1 controller is configured on the Cisco 2600 series, Cisco 2600XM series, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, Cisco 3745, and the Cisco MC3810.

Command Modes Controller configuration

Command History

Release	Modification
11.3MA	This command was introduced on the Cisco MC3810.
12.0	This command was integrated into Cisco IOS Release 12.0 on the Cisco MC3810.
12.0(7)XE	This command was implemented on the Catalyst 6000 family switches.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(1)T	This command was modified to accommodate two channel groups on a port on 1- and 2-port T1/E1 multiflex voice or WAN interface cards on the Cisco 2600 and Cisco 3600 series routers.
12.1(3a)E3	The number of valid values for the *kbps* argument was changed on the Cisco MC3810; see the "Usage Guidelines" section for valid values.
12.2(11)T	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(15)T	The **aim** keyword was added for use on the Cisco 2600 series (including the Cisco 2691), Cisco 2600XM, Cisco 3660, Cisco 3725, and Cisco 3745.
12.3(1)	The **unframed** keyword was added for use on the Cisco 2600XM series, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, and Cisco 3745.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines Use this command to direct HDLC traffic from the T1/E1 interface to the AIM-ATM-VOICE-30 DSP card. A channel group is created using Advanced Integration Module (AIM) HDLC resources when a **channel-group** command with the **aim** keyword is parsed during system initialization or when the command is entered during configuration. You must specify the **aim** keyword under a T1/E1 controller port to direct HDLC traffic from the T1/E1 interface to the AIM-ATM-VOICE-30 DSP card on the Cisco 2600 series, Cisco 2600XM series, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, and Cisco 3745.

Note Neither the Cisco AS5400 series NAS nor the Cisco MC3810 is supported with the integrated voice and data WAN on T1/E1 interfaces using the AIM-ATM-VOICE-30 module.

If previous **channel-group** commands are configured with the **aim** keyword, subsequent **channel-group** commands without the **aim** keyword are rejected. Similarly, if a regular **channel-group** command is followed by another **channel-group** command with the **aim** keyword implemented, the second command is rejected on the Cisco 2600 and Cisco 2600XM.

A channel group using AIM HDLC resources is deleted only when a **no channel-group** command is entered.

By default, the **channel-group** command on a NAS sets the serial interface object encapsulation to HDLC. You must override the default by entering the **encapsulation ss7** command for that serial interface object. Once you override the default, encapsulation cannot be changed again for that object. The SS7 encapsulation option is new to the Integrated Signaling Link Terminal feature and is available only for interface serial objects created by the **channel-group** command. The Integrated Signaling Link Terminal feature added SLT functionality on Cisco AS5350 and Cisco AS5400 platforms.

A digital SS7 link can be deleted by entering the **no channel-group** *channel-group-number* command on the associated T1/E1 controller. The link must first be stopped using the **no shutdown** command. It is not necessary to remove the channel ID association first.

Use the **channel-group** command in configurations where the router or access server must communicate with a T1 or E1 fractional data line. The channel group number may be arbitrarily assigned and must be unique for the controller. The time-slot range must match the time slots assigned to the channel group. The service provider defines the time slots that comprise a channel group.

Note Channel groups, channel-associated signaling (CAS) voice groups, DS0 groups, and time-division multiplexing (TDM) groups all use group numbers. All group numbers configured for channel groups, CAS voice groups, and TDM groups must be unique on the local Cisco MC3810 concentrator. For example, you cannot use the same group number for a channel group and for a TDM group. Furthermore, on the Cisco MC3810, only one channel group can be configured on a controller.

The channel group number can be 0 or 1 on the Cisco SLT (Cisco 2611).

The **channel-group** command also applies to Voice over Frame Relay, Voice over ATM, and Voice over HDLC on the Cisco MC3810.

Examples

The following example shows basic configuration directing HDLC traffic from the T1/E1 interface to the AIM-ATM-VOICE-30 DSP card, starting in global configuration mode:

```
Router(config)# controller e1 1/0
Router(config-controller)# clock source internal
Router(config-controller)# channel-group 0 timeslots 1-31 aim 0
```

The following example explicitly sets the encapsulation type to PPP to override the HDLC default:

```
Router# configure terminal
Router(config)# controller t1 6/0
Router(config-controller)# channel-group 2 timeslots 3 aim 0
Router(config-controller)# exit
Router(config)# interface serial 6/0:2
Router(config-if)# encapsulation ppp
Router(config-if)# ip address 10.0.0.1 255.0.0.0
Router(config-if)# no shutdown
Router(config-if)# end
```

The following example shows how to explicitly set the encapsulation type to SS7 to override the HDLC default using the Integrated Signaling Link Terminal feature. This example uses an 8PRI DFC card inserted into slot 7, and DS0-timeslot 3 on trunk 5 of that card is used as an SS7 link:

```
Router# configure terminal
Router(config)# controller t1 7/5
Router(config-controller)# channel-group 2 timeslots 3
Router(config-controller)# exit
Router(config)# interface serial 7/5:2
Router(config-if)# encapsulation ss7
Router(config-if)# channel-id 0
Router(config-if)# no shutdown
Router(config-if)# end
```

The following example defines three channel groups. Channel-group 0 consists of a single time slot, channel-group 8 consists of seven time slots and runs at a speed of 64 kbps per time slot, and channel-group 12 consists of two time slots.

```
Router(config-controller)# channel-group 0 timeslots 1
Router(config-controller)# channel-group 8 timeslots 5,7,12-15,20 speed 64
Router(config-controller)# channel-group 12 timeslots 2
```

The following example configures a channel group on controller T1 0 on a Cisco MC3810:

```
Router(config)# controller T1 0
Router(config-controller)# channel-group 10 timeslots 10-64
```

The following example configures a channel group on controller E1 1 and specifies that all time slots are used for data:

```
controller e1 1
channel-group 1 unframed
```

Note SS7 digital F-link support for the 8PRI line card requires use of a third onboard TDM stream to route trunk DS0 messages to the onboard MGCs.

Related Commands

Command	Description
framing	Specifies the frame type for the T1 or E1 data line.
invert data	Enables channel inversion.
linecode	Specifies the line code type for the T1 or E1 line.
voice-card	Configures a card with voice processing resources and enters voice card configuration mode.
encapsulation	Sets the encapsulation type.

chat-script

To create a script that will place a call over a modem, use the **chat-script** command in global configuration mode. To disable the specified chat script, use the **no** form of this command.

chat-script *script-name expect-send*

no chat-script *script-name expect-send*

Syntax Description

script-name	Name of the chat script.
expect-send	Pairs of information elements: an item to expect and an item to send in response.

Command Default

No chat scripts are defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Chat scripts are used in dial-on-demand routing (DDR) to give commands to dial a modem and commands to log on to remote systems. The defined script will be used to place a call over a modem.

Some characteristics of chat scripts are as follows:

- Chat scripts are case sensitive.
- You can have any number of ABORT sequences active at once.
- When a chat script starts, the default timeout is 5 seconds. Changes to the timeout persist until the next time you change them in the script.
- A string within quotation marks is treated as a single entity.

We recommend that one chat script (a "modem" chat script) be written for placing a call and another chat script (a "system" or "login" chat script) be written to log on to remote systems, where required.

Suggested Chat Script Naming Conventions

A suggested chat script naming convention is *vendor-type-modulation.* If you follow this convention, the syntax of the **chat-script** command becomes **chat-script** *vendor-type-modulation expect-send.*

For example, if you have a Telebit T3000 modem that uses V.32*bis* modulation, you would name your chat script telebit-t3000-v32bis.

The **chat-script** command could be written as follows:

```
chat-script telebit-t3000-v32bis ABORT ERROR ABORT BUSY ABORT "NO ANSWER" "" "AT H" OK "AT
DT \T" DIALING \c TIMEOUT 30 CONNECT \c
```

Adhering to this naming convention allows you to use partial chat script names with regular expressions to specify a range of chat scripts that can be used. This capability is particularly useful for dialer rotary groups and is explained further in the next section.

Chat scripts are in the form *expect-send*, where the send string following the hyphen (-) is executed if the preceding expect string fails. Each send string is followed by a return unless it ends with the escape sequence \c. The sequence ^*x* is translated into the appropriate control character, and the sequence *x* is translated into *x* if *x* is not one of the special sequences listed in Table 2.

See the book titled *Managing uucp and Usenet* by Tim O'Reilly and Grace Todino for more information about chat scripts.

Escape Sequences

The escape sequences used in chat scripts are listed in Table 2.

Table 2 Chat Script Send String Escape Sequences

Escape Sequence	Description
\	Sends the ASCII character with its octal value.
\\	Sends a backslash (\) character.
\"	Sends a double-quote (") character (does not work *within* double quotes).
\c	Suppresses a new line at the end of the send string.
\d	Delays for 2 seconds.
\K	Inserts a BREAK.
\n	Sends a newline or linefeed character.
\N	Sends a null character.
\p	Pauses for 0.25 second.
\q	Reserved, not yet used.
\r	Sends a return.
\s	Sends a space character.
\t	Sends a tab character.
\T	Replaced by phone number.
" "	Expects a null string.
BREAK	Causes a BREAK. This sequence is sometimes simulated with line speed changes and null characters. May not work on all systems.
EOT	Sends an end-of-transmission character.

Expect-Send Pairs

Sample supported *expect-send* pairs are described in Table 3.

Table 3 Sample Supported Expect-Send Pairs

Expect and Send Pair	Function
ABORT *string*	Designates a string whose presence in the input indicates that the chat script has failed.
TIMEOUT *time*	Sets the time to wait for input, in seconds. The default is 5 seconds and a timeout of 60 seconds is recommended for V.90 modems.

For example, if a modem reports BUSY when the number dialed is busy, you can indicate that you want the attempt stopped at this point by including ABORT BUSY in your chat script.

Alternate Handlers

If you use the *expect-send* pair ABORT SINK instead of ABORT ERROR, the system terminates abnormally when it encounters SINK instead of ERROR.

Missed Characters

After the connection is established and you press the Return key, you must often press Return a second time before the prompt appears.

For example, you might include the following as part of your chat script:

```
ssword:-/r-ssword
```

This part of the script specifies that, after the connection is established, you want **ssword** to be displayed. If it is not displayed, you must press Return again after the timeout passes.

Examples

The following example shows the **chat-script** command being used to create a chat script named *t3000*:

```
chat-script t3000 ABORT ERROR ABORT BUSY ABORT "NO ANSWER" "" "AT H" OK "AT DT \T" DIALING
\c TIMEOUT 60 CONNECT \c
```

Related Commands

Command	Description
dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites.
script dialer	Specifies a default modem chat script.

class (controller)

To create a signaling class structure that can be referred to by its name, use the **class** command in controller configuration mode. To remove the structure, use the **no** form of this command.

class *name*

no class *name*

Syntax Description

name	The signaling class name which specifies the template that processes the automatic number identification/dialed number identification service (ANI/DNIS) delimiter.

Command Default

No signaling class structures are defined.

Command Modes

Controller configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

A signaling class allows the Cisco AS5300 and Cisco AS5800 universal access servers to provide the ANI/DNIS delimiter on incoming T1/CAS trunk lines. The digit collection logic in the call switching module (CSM) for incoming T1 CAS calls in dual tone multifrequency (DTMF) is modified to process the delimiters, the ANI digits, and the DNIS digits.

For this feature to work, a CAS signaling class with the template to process ANI/DNIS delimiters has to be defined. This creates a signaling class structure which can be referred to by its name. The *name* argument must match the name configured in the **signaling-class cas** command.

Examples

The following example defines a CAS signaling class with the template to process ANI/DNIS delimiters on channel 1:

```
Router(config)# signaling-class cas test
Router(config-sig-class)# profile incoming S<*a<*d<*n

Router(config)# controller T1 1/0/1
Router(config-controller)# class test
```

Related Commands

Commands	Descriptions
profile incoming	Defines a template formed by directives guiding the CSM to process the digit sequence for a signaling class.
signaling-class cas	Defines a signaling class which specifies the template that processes the ANI/DNIS delimiter.

clear cot summary

To reset the counters, use the **clear cot summary** command in privileged EXEC mode.

clear cot summary

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(7)	This command was introduced.

Examples

There is no display generated, but the counters in the **show cot summary** command would be all zeros.

Related Commands

Command	Description
show cot dsp	Displays information about the COT DSP configuration or current status.
show cot request	Displays COT request information.
show cot summary	Displays information about the COT activity.

clear counters (async)

To clear the counters of a specified asynchronous interface or specified asynchronous interface group, as displayed by the **show interface async** command, use the **clear counters** command in EXEC mode.

clear counters {**async** *async-interface-number* | **group-async** *group-async-interface-number*}

Syntax Description

async	Counters in a specified asynchronous interface.
async-interface-number	Required async interface number of the asynchronous interface that has been previously created with this number specification. The range is from 1 through 49.
group-async	Counters in a specified asynchronous interface group.
group-async-interface-number	Required group-async interface number that has been previously created with this number specification. The range is from 0 through 49.

Command Modes

EXEC

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Before using this command, use the **show interface async** command to display the asynchronous related counters on the specified asynchronous interface.

Examples

The following example uses the **show interface async** command to display the asynchronous related counters on the asynchronous interface named 1. The example then uses the **clear counters group-async** command to clear the counters. After the counters are cleared, the configuration file for the interface is displayed.

```
Router# show interface async 1

Async1 is down, line protocol is down
  modem(slot/port)=1/0, state=IDLE
  dsx1(slot/unit/channel)=NONE, status=VDEV_STATUS_UNLOCKED
  Hardware is Async Serial
  Interface is unnumbered.  Using address of Ethernet0 (1.18.31.9)
  MTU 1500 bytes, BW 115 Kbit, DLY 100000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive not set
  DTR is pulsed for 5 seconds on reset
  LCP Closed
  Closed: IPCP, CDPCP
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 00:03:46
  Input queue: 0/10/0 (size/max/drops); Total output drops: 0/////
  Queueing strategy: weighted fair
```

```
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions

Router#
Router# clear counters group-async 1

Clear "show interface" counters on this interface [confirm]
Router#

*Oct 17 00:42:27.083: %CLEAR-5-COUNTERS: Clear counter on interface Group-Asynce
```

Related Commands

Command	Description
clear modem counters	Clears the statistical counters on one or more manageable modems on access servers or routers.
show interface async	Displays the asynchronous related counters on the specified asynchronous interface.

clear counters line

To clear line counters, use the **clear counters line** command in EXEC mode.

clear counters line {*type* | *number*}

Syntax Description

type	Line type: **aux**, **console**, **tty**, or **vty**.
number	First line number to clear, which can be between 0 and 54.

Command Modes

EXEC

Command History

Release	Modification
11.2P	This command was introduced.

Usage Guidelines

This command clears the line counters shown by the **show line** command.

Examples

The following example shows the available options under the **clear counters line** command. When you issue this command, the counters (for example, Uses and Noise) displayed by the **show line** command are cleared.

```
Router# clear counters line ?

   <0-54>   First Line number
   aux      Auxiliary line
   console  Primary terminal line
   tty      Terminal controller
   vty      Virtual terminal

Router# exit

Router> show line

 Tty Typ     Tx/Rx     A Modem  Roty AccO AccI  Uses    Noise   Overruns
*  0 CTY               -    -      -    -    -     0        4        0/0
A  1 TTY 115200/115200 - inout     -    -    -     1        0        0/0
A  2 TTY 115200/115200 - inout     -    -    -     1        0        0/0
A  3 TTY 115200/115200 - inout     -    -    -     1        0        0/0
*  4 TTY 115200/115200 - inout     -    -    -     0        0        0/0
*  5 TTY 115200/115200 - inout     -    -    -     0        0        0/0
*  6 TTY 115200/115200 - inout     -    -    -     0        0        0/0
*  7 TTY 115200/115200 - inout     -    -    -     0        0        0/0
*  8 TTY 115200/115200 - inout     -    -    -     0        0        0/0
*  9 TTY 115200/115200 - inout     -    -    -     0        0        0/0
* 10 TTY 115200/115200 - inout     -    -    -     0        0        0/0
* 11 TTY 115200/115200 - inout     -    -    -     0        0        0/0
* 12 TTY 115200/115200 - inout     -    -    -     0        0        0/0
* 13 TTY 115200/115200 - inout     -    -    -     0        0        0/0
* 14 TTY 115200/115200 - inout     -    -    -     0        0        0/0
* 15 TTY 115200/115200 - inout     -    -    -     0        0        0/0
A 16 TTY 115200/115200 - inout     -    -    -     1        0        0/0
```

```
A 17 TTY 115200/115200 - inout     -    -    -     1        0        0/0
A 18 TTY 115200/115200 - inout     -    -    -     1        0        0/0
A 19 TTY 115200/115200 - inout     -    -    -     1        0        0/0
A 20 TTY 115200/115200 - inout     -    -    -     1        0        0/0
A 21 TTY 115200/115200 - inout     -    -    -     1        0        0/0
```

Related Commands

Command	Description
show line	Displays the parameters of a terminal line.

clear dialer

To clear the values of dialer statistics for one or more serial interfaces or BRIs configured for dial-on-demand routing (DDR), use the **clear dialer** privileged EXEC mode command

clear dialer [**interface** *type number*]

Cisco 7500 Series Routers Only

clear dialer [**interface serial** *slot*/*port*]

Syntax Description

interface	(Optional) Indicates that one interface will be specified.
type	(Optional) Interface type: **async**, **serial**, or **bri**.
number	(Optional) Interface number.
slot/*port*	(Optional) Backplane slot number and port number on the interface. See your hardware installation manual for the specific slot and port numbers.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

If the **interface** keyword and the arguments are not used, dialer statistics are cleared on all interfaces.

Examples

The following example clears the dialer statistics on serial interface 1:

```
Router# clear dialer interface serial 1
```

clear dialer dnis

To reset the counter statistics associated with a specific dialed number identification service (DNIS) group or number, use the **clear dialer dnis** command in privileged EXEC mode.

clear dialer dnis {**group** *name* | **number** *number*}

Syntax Description

group *name*	Dialer DNIS group statistics.
number *number*	Dialer DNIS number statistics.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **clear dialer dnis** EXEC command to reset the counter statistics associated with a specific DNIS group or number. This command clears the counters for a DNIS group to reset the counter statistics associated with a specific DNIS group or number. If an ISP is charging a customer for the number of calls to a DNIS, it can clear the number after a week or month by using this command.

Examples

The following example shows the result of using the **clear dialer dnis** command for the DNIS group named “dg1”. Note that the counters have been cleared after the **clear dialer dnis** command has been entered.

```
Router# show dialer dnis group dg1

DNIS Number:71028
  4 total connections
  3 peak connections
  1 calltype mismatches
DNIS Number:4156266541
  8 total connections
  5 peak connections
  0 calltype mismatches
DNIS Number:4085541628
  3 total connections
  2 peak connections
  0 calltype mismatches
DNIS Number:71017
  2 total connections
  1 peak connections
  0 calltype mismatches

Router# clear dialer dnis group dg1

Router# show dialer dnis group dg1

DNIS Number:71028
  0 total connections
```

```
  0 peak connections
  0 calltype mismatches
DNIS Number:4156266541
  0 total connections
  0 peak connections
  0 calltype mismatches
DNIS Number:4085541628
  0 total connections
  0 peak connections
  0 calltype mismatches
DNIS Number:71017
  0 total connections
  0 peak connections
  0 calltype mismatches
```

Related Commands

Command	Description
show dialer dnis	Displays the number of calls DNIS groups have had.

clear dialer sessions

To remove all dialer sessions and disconnect links when connected, use the **clear dialer sessions** command in EXEC mode.

clear dialer sessions

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced.

Examples

The following example shows how to use the **clear dialer sessions** command:

```
Router# clear dialer sessions
```

Related Commands

Command	Description
show dialer sessions	Displays all dialer sessions.

clear dsip tracing

To clear Distributed System Interconnect Protocol (DSIP) tracing statistics (trace logging), use the **clear dsip tracing** command in privileged EXEC mode.

clear dsip tracing {**counters** | **tracing**} [**control** | **data** | **ipc**]

Syntax Description

counters	DSIP counters.
tracing	DSIP tracing buffers.
control	(Optional) Control counters or tracing buffers.
data	(Optional) Data counters or tracing buffers.
ipc	(Optional) Inter-process communication counters or tracing buffers.

Command Default

If no option is specified, all control, data, and inter-process communication counters or tracing buffers are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to clear the counters displayed with the **show dsip tracing** EXEC command.

Examples

In the following example, the DSIP counters are cleared (including data, control, and ipc counters):

```
Router# clear dsip tracing
```

Related Commands

Command	Description
show dsip tracing	Displays DSIP tracing buffer information.
show dsip version	Displays DSIP version information.

clear interface virtual-access

To tear down the virtual access interface and free the memory for other dial-in uses, use the **clear interface virtual-access** command in privileged EXEC mode.

clear interface virtual-access *number*

Syntax Description

number	Virtual access interface number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2F	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

This command does not free the memory for uses unrelated to dial-in access.

Examples

The following example clears a specified virtual access interface. You can use the **show interfaces virtual-access** command to display the interface numbers before you clear any specific one.

```
Router# clear interface virtual-access 2.1
```

Related Commands

Command	Description
interface virtual-template	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.
show interfaces	Displays statistics for the interfaces configured on a router or access server.

clear ip route download

To clear static routes downloaded from an authentication, authorization, and accounting (AAA) server, use the **clear ip route download** command in EXEC mode.

clear ip route download {* | *network-number network-mask* | **reload**}

Syntax Description

*	All routes.
network-number network-mask	Destination network route and mask in standard IP address notation. For example, 10.1.1.1 255.255.255.255.
reload	Delete all routes, then reload static routes from the AAA server and reset the timer configured by the **aaa route download** command.

Command Modes

EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

This command forces the router to reload static routes from the AAA server before the update timer expires.

Examples

The following example shows how to clear all routes:

```
Router# clear ip route download *
```

Related Commands

Command	Description
aaa authorization configuration default	Downloads static route configuration information from the AAA server using TACACS+ or RADIUS.
aaa route download	Enables the download static route feature and sets the amount of time between downloads.
show ip route	Displays all static IP routes, or those installed using the AAA route download function.

clear line

To return a terminal line to idle state, use the **clear line** command in EXEC mode.

clear line *line-number*

Syntax Description

line-number	Absolute line number.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command to log out of a specific session running on another line. If the line uses a modem, the modem will be disconnected.

Examples

The following example resets line 3 to idle state:

```
Router# clear line 3
```

clear line async-queue

To reset the connections currently waiting to use a rotary line in the queue, use the **clear line async-queue** command in EXEC mode.

clear line async-queue [*rotary-group*]

Syntax Description

rotary-group	(Optional) Rotary group.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

Use this command without any argument to remove all rotary line queues and terminate the asynchronous queue manager. Use the **clear line async-queue** command with the *rotary-group* argument to reset only the specified rotary group.

Examples

The following example clears all the rotary queues and shows the resulting output:

```
Router# clear line async-queue

Clearing queued connections for ALL rotary groups ! [confirm]
Clearing rotary group 1
  Clearing line 69
  Clearing line 70
Clearing rotary group 2
  Clearing line 66
  Clearing line 67
  Clearing line 68
```

clear modem

To reset the hardware for one or more manageable modems on an access server or router, use the **clear modem** command in EXEC mode.

clear modem {*slot*/*port* | **all** | **group** *group-number* | **at-mode** *slot*/*port* | **test**}

Syntax Description

slot/*port*	Slot and modem port number. (Include the slash mark when entering this variable, for example: 1/1.)
all	All modems. This command disconnects any active calls.
group *group-number*	Group of modems. The modem group number is the number of the group you have previously created.
at-mode *slot*/*port*	AT directly connected session. The variable, *slot*/*port*, is required. This EXEC command clears an attention (AT) directly connected session to a manageable Microcom modem from a second Telnet session.
test	Log or test report that is displayed by the **show modem test** command. If you do not clear the test regularly, eventually the oldest test report will replace the current test report.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The modem hardware is reset for modems that are idle or busied out for long periods of time.

An AT directly connected session is usually initiated and closed from the same Telnet session when you enter the **modem at-mode** command and press **Ctrl-C**. However, you can clear an AT directly connected session that was mistakenly left open by enabling the **clear modem at-mode** command from a second Telnet session in to the access server.

Examples

The following example of the **clear modem** *slot*/*port* command resets the hardware for manageable modem 1/1:

```
Router# clear modem 1/1
```

The following is an example of using the **clear modem all** command:

```
Router# clear modem all

This command will disconnect any active calls.
Clear (reset) all modems? [confirm]
Clearing modems.............................................
Done
Router#
```

The following examples of the **clear modem group** command clear the manageable modems in group 1:

```
Router# clear modem group 1
Router# clear modem group1
```

The following example executes the **clear modem at-mode** command from a Telnet session:

```
modem at-mode 1/1
```

The following example executes the **clear modem at-mode** command from a second Telnet session while the first Telnet session is connected to the modem:

```
Router# clear modem at-mode 1/1

clear "modem at-mode" for modem 1/1 [confirm]
Router#
```

The following output is displayed in the first Telnet session after the modem is cleared by the second Telnet session:

```
Direct connect session cleared by vty0 (172.19.1.164)
```

Related Commands

Command	Description
clear modem counters	Clears the statistical counters on one or more manageable modems on access servers or routers.
interface group-async	Creates a group interface that will serve as master, to which asynchronous interfaces can be associated as members.
show modem at-mode	Opens a directly connected session and enters AT command mode, which is used for sending AT commands to Microcom manageable modems.
show modem test	Displays the modem test log.

clear modem counters

To clear the statistical counters on one or more manageable modems installed in an access server, use the **clear modem counters** command in EXEC mode.

clear modem counters [*slot*/*port-number* | **group** [*group-number*]]

Syntax Description

slot/*port-number*	(Optional) Slot and modem port number. (Include the slash mark when entering this variable, for example: 1/1.)
group [*group-number*]	(Optional) One or all groups of modems. The optional modem group number is the number of a group-async interface. The group number range is from 1 to 1002.

Command Default

Disabled

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Entering the **clear modem counters** command without specifying an optional keyword or argument resets the modem statistics on each modem and the summary statistics displayed in the **show modem summary** command.

The subcommand **clear modem counters group** without the group number clears counters in all modem groups. The optional modem group number is the number of a group you have previously created.

Examples

The following example of the **clear modem counters** *slot*/*port* command clears the statistical counters on manageable modem 1/1:

```
Router# clear modem counters 1/1
```

The following example of the **clear modem counters group** command clears the statistical counters on all manageable modem groups:

```
Router# clear modem counters group

Clear "show modem" counters for all modem groups [confirm]
Router#
*Oct 17 20:20:24.974: %CLEAR-5-COUNTERS: Clear counter on modems in all groups e
Router#
```

Related Commands

Command	Description
clear cot summary	Clears the counters of a specified asynchronous interface or specified asynchronous interface group.
show modem summary	Displays a high-level report for all manageable modems dialing into and out of the network.

clear modem log

To reset the log for one or more manageable modems installed in a Cisco AS5800 series access server, use the **clear modem log** command in EXEC mode.

clear modem log [*shelf*/*slot*/*port* [*shelf*/*slot*/*port* ...] | **group** [*group-number*]]

Syntax Description

shelf/*slot*/*port* [*shelf*/*slot*/*port* ...]	(Optional) One or several modem shelves listed in the order shelf, slot, and port. (Include the slash mark when entering the values.) The shelf value is the shelf ID of the dial shelf. The slot values range from 2 to 11 and the port values range from 0 to 323 on the UP324 modem card, and from 0 to 143 on the Double Density Modem Module (DMM) card.
group [*group-number*]	(Optional) One or all groups of modems. The optional modem group number is the number of a group-async interface. The group number range is from 1 to 1002.

Command Default

Reset logs for all modems.

Command Modes

EXEC

Command History

Release	Modification
12.1T	This command was introduced.

Usage Guidelines

Entering the **clear modem log** command without specifying an optional keyword or argument resets the log for all modems. Entering the **clear modem log** command and the **grou**p keyword without an argument clears the log for all modem groups. Use the optional *shelf*/*slot*/*port* or *group-number* argument to clear the log of a specific modem or modem group.

The *group-number* argument is the number of a group you have previously created using the **interface group-async** global configuration and **group range** interface configuration commands. These commands create a group of asynchronous interfaces that are associated with a group asynchronous interface on the same device.

Examples

The following example clears the modem log for shelf 1, slot 4, port 0:

```
Router# clear modem log 1/4/0

Clear Modem log for modem 1/4/00 [confirm]y
```

Use the **show modem log** command to verify that the modem log for shelf 1, slot 4, port 0 is cleared:

```
Router# show modem log 1/4/0

Modem 1/4/00 Events Log:
```

The following example clears the modem logs for shelf 1, slot 4, port 0 and shelf 1, slot 4, port 2:

```
Router# clear modem log 1/4/1 1/4/2

Clear modem log for modems 1/4/01 to 1/4/02 [confirm]y
```

Use the **show modem log** command to verify the modem logs for shelf 1, slot 4, port 0 and shelf 1, slot 4, port 2 are cleared:

```
Router# show modem log 1/4/1 1/4/2

Modem 1/4/01 Events Log:
Modem 1/4/02 Events Log:
```

The following example clears the log for all modems:

```
Router# clear modem log

Clear modem log for all modems [confirm]y
```

The following example clears the log for all modem groups:

```
Router# clear modem log group

Clear modem log for modems in all groups [confirm]y
```

The following example clears the log for modem group 0:

```
Router# clear modem log group 0

Clear modem log for modems in group 0 [confirm]y
```

Related Commands

Command	Description
group range	Creates a list of member asynchronous interfaces (associated with a group interface).
interface group-async	Creates a group interface that will serve as master, to which asynchronous interfaces can be associated as members.
show modem log	Displays the modem history event status performed on a manageable modem or group of modems.

clear modempool-counters

To clear the active or running counters associated with one or more modem pools, use the **clear modempool-counters** command in EXEC mode.

clear modempool-counters [*name*]

Syntax Description

name	(Optional) Modem pool name. If you do not include this option, all counters for all modem pools will be cleared.

Command Modes

EXEC

Command History

Release	Modification
11.2P	This command was introduced.

Usage Guidelines

The **clear modempool-counters** command clears the counters that are displayed in the **show modem-pool** command. This command is used only with MICA technologies digital modems.

Examples

The following examples show three modem pools set up on the access server: System-def-Mpool, v90service, and v34service:

```
Router# show modem-pool

modem-pool: System-def-Mpool
modems in pool: 20   active conn: 15
0 no free modems in pool

modem-pool: v90service
modems in pool: 50  active conn: 43
  3 no free modems in pool
 called_party_number: 4441000
   max conn allowed: 50, active conn: 43
   3 max-conn exceeded, 3 no free modems in pool

modem-pool: v34service
modems in pool: 50  active conn: 30
 1 no free modems in pool
 called_party_number: 4443000
   max conn allowed: 50, active conn: 30
   0 max-conn exceeded, 0 no free modems in pool
```

In the following example, the **clear modempool-counters v90service** command clears the running counters for the v90services modem pool:

```
Router# clear modempool-counters v90service
Router# show modem-pool

modem-pool: System-def-Mpool
modems in pool: 20   active conn: 15
0 no free modems in pool
```

```
modem-pool: v90service
modems in pool: 50  active conn: 0
 0 no free modems in pool
 called_party_number: 4441000
   max conn allowed: 50, active conn: 0
   0 max-conn exceeded, 0 no free modems in pool

modem-pool: v34service
modems in pool: 50  active conn: 30
 1 no free modems in pool
 called_party_number: 4443000
   max conn allowed: 50, active conn: 30
   0 max-conn exceeded, 0 no free modems in pool
```

Related Commands

Command	Description
called-number (modem pool)	Assigns a called party number to a pool of modems.
modem-pool	Creates a new modem pool or specifies an existing modem pool, which allows you to physically or virtually partition your access server for dial-in and dial-out access.
pool-member	Assigns a range of modems to a modem pool.
show modem-pool	Displays the configuration and connection status for one or more modem pools.

clear port

To reset the NextPort port and clear any active call to the port, use the **clear port** command in EXEC mode.

Cisco AS5400 with the NextPort Dial Feature Card (DFC)

clear port [*slot* | *slot*/*port*]

Cisco AS5800 with the Universal Port Card (UPC)

clear port [*shelf*/*slot* | *shelf*/*slot*/*port*]

Syntax Description

slot	(Optional) The slot number to be cleared. All ports on the specified slot will be cleared. For the Cisco AS5400, slot values range from 1 to 7.
slot/*port*	(Optional) The slot and port number to be cleared. For the Cisco AS5400, slot values range from 1 to 7 and port values range from 0 to one less than the number of ports supported by the card. You must type in the slash mark.
shelf/*slot*	(Optional) The shelf and slot number to be cleared. All ports on the specified shelf and slot will be cleared. For the Cisco AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11. You must type in the slash mark.
shelf/*slot*/*port*	(Optional) The shelf, slot, and port number to be cleared. For the Cisco AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and port values range from 0 to 323. You must type in the slash mark.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5800.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

If you specify the shelf, slot, and port, you clear that port on that SPE. If you specify only the shelf and slot, you clear all active ports on that particular shelf and slot. If you do not specify a shelf, slot, or port, you clear all the ports on the access server.

This command also clears the Bad state on a port and resets it. However, the port is not cleared if the SPE was previously in a Bad state due to an SPE firmware download.

Examples

The following example shows output from the **clear port** command on the Cisco AS5400 with the NextPort DFC. This example clears slot 1, port 1:

```
Router# clear port 1/1

This will clear port 1/01[confirm]y
```

The following example shows output from the **clear port** command on the Cisco AS5800 with the UPC. This example clears shelf 1, slot 3, port 0:

```
Router# clear port 1/3/0

This will clear port 1/03/00[confirm]y
```

Related Commands

Command	Description
busyout	Informs the central-office switch that a channel is out of service.
clear line	Returns a terminal line to idle state.
clear spe	Reboots all specified SPEs.
show port digital log	Displays the data event log for digital modems.
show port modem log	Displays the events generated by the modem sessions
show spe	Displays SPE status.
shutdown (port)	Disables a port.

clear port log

To clear all event entries in the port level history event log, use the **clear port log** command in EXEC mode.

Cisco AS5400 with NextPort DFC

clear port log [*slot* | *slot*/*port*]

Cisco AS5800 with Universal Port Card

clear port log [*shelf*/*slot* | *shelf*/*slot*/*port*]

Syntax Description

slot	(Optional) All ports on the specified slot. For the AS5400, slot values range from 0 to 7.
slot/*port*	(Optional) All ports on the specified slot and SPE. For the AS5400, slot values range from 0 to 7 and port values range from 0 to 107. Be sure to include the slash mark.
shelf/*slot*	(Optional) All ports on the specified shelf and slot. For the AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11. Be sure to include the slash mark.
shelf/*slot*/*port*	(Optional) All ports on the specified SPE. For the AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and port values range from 0 to 323. Be sure to include the slash mark.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5800.

Usage Guidelines

The **clear port log** command clears the entire port log. You cannot remove individual service events from the port log. On the Cisco AS5400 only, you can use **show port modem log** or the **show port digital log** to display specific service events, but you must use **clear port log** to clear the entire port event log.

Examples

The following example shows output from the **clear port log** command on the Cisco AS5400 with NextPort DFC. This example clears slot 1, port 1:

```
Router# clear port log 1/1

This will clear log event history for port(s)1/01 - 1/01[confirm]y
```

The following example shows output from the **clear port log** command on the Cisco AS5800 with universal port card. This example clears shelf 1, slot 3, port 0:

```
Router# clear port log 01/03/00

This will clear port 1/03/00[confirm]y
```

Related Commands

Command	Description
show port digital log	Displays the data event log for digital modems.
show port modem log	Displays the events generated by the modem sessions.

clear resource-pool

To reset the counter statistics associated with a specific customer profile, call discriminator, or physical resource, use the **clear resource-pool** command in privileged EXEC mode.

clear resource-pool {**customer** | **discriminator** | **resource**} {*name* | **all**}

Syntax Description

customer	Customer profile.
discriminator	Call discriminator.
resource	Physical resource. Checks the counters maintained for resource groups.
name	Specific customer profile, discriminator, or physical resource in the access server.
all	All customer profiles, discriminators, or physical resources in the access server.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **clear resource-pool** privileged EXEC command to reset the counter statistics associated with a specific customer profile, call discriminator, or physical resource.

Examples

The following example shows the use of the **clear resource-pool** command for the specific customer named "customer-isp":

```
Router# clear resource-pool customer ?

  WORD  Customer profile name
  all   Clear all customer profiles

Router# clear resource-pool customer customer-isp
```

Related Commands

Command	Description
show resource-pool call	Displays all active call information for all customer profiles and resource groups.
show resource-pool customer	Displays the contents of one or more customer profiles.
show resource-pool resource	Displays the resource groups configured in the NAS.

clear snapshot quiet-time

To end the quiet period on a client router within two minutes, use the **clear snapshot quiet-time** command in EXEC mode.

clear snapshot quiet-time *interface-type interface-number*

Syntax Description

interface-type interface-number	Interface type and number.

Command Modes

EXEC

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The **clear snapshot quiet-time** command places the client router in a state to reenter the active period within two minutes. The two-minute hold period ensures a quiet period of at least two minutes between active periods.

Examples

The following example ends the quiet period on dialer interface 1:

```
Router# clear snapshot quiet-time dialer 1
```

Related Commands

Command	Description
show snapshot	Displays snapshot routing parameters associated with an interface.
snapshot client	Configures a client router for snapshot routing.

clear spe

To reboot all specified service processing elements (SPEs), use the **clear spe** command in EXEC mode.

Cisco AS5400 with the NextPort Dial Feature Card (DFC)

clear spe [*slot* | *slot*/*spe*]

Cisco AS5800 with the Universal Port Card (UPC)

clear spe [*shelf*/*slot* | *shelf*/*slot*/*spe*]

Syntax Description

slot	(Optional) The slot number to be cleared. All ports on the specified slot will be cleared. For the Cisco AS5400, slot values range from 1 to 7.
slot/*spe*	(Optional) The slot and service processing element (SPE) number to be cleared. All ports on the specified slot and SPE will be cleared. For the Cisco AS5400, slot values range from 1to 7 and SPE values range from 1 to 17. You must type in the slash mark.
shelf/*slot*	(Optional) The shelf and slot number to be cleared. All ports on the specified shelf and slot will be cleared. For the Cisco AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11. You must type in the slash mark.
shelf/*slot*/*spe*	(Optional) The shelf, slot and SPE number to be cleared. All ports on the specified SPE will be cleared. For the Cisco AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 0 to 53. You must type in the slash marks.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5800.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

Execution of the **clear spe** command causes the configured firmware to be downloaded to the specified SPE or the range of SPEs and causes the power-on self-test (POST) to be executed. This command can be executed regardless of the state of the SPEs.

Note All active ports running on the SPE are prematurely terminated and messages are logged into the appropriate log.

This command downloads configured SPEs with firmware as configured. Unconfigured SPEs download with the default firmware, which is the bundled version. To configure and manage the downloading of firmware without abruptly terminating SPEs, use the firmware location or firmware upgrade commands as appropriate.

Examples

The following example clears SPEs when the **clear spe** command is entered on the Cisco AS5400 with the NextPort DFC. This example performs a coldstart on slot 1, SPE 1.

```
Router# clear spe 1/1

Router# This will tear all active calls on the SPE(s), if any.[confirm]y
```

The following example clears SPEs when the **clear spe** command is entered on the Cisco AS5800 with the UPC. This example performs a coldstart on shelf 1, slot 8, SPE 0.

```
Router# clear spe 1/8/0

Router# This will tear all active calls on the SPE(s), if any.[confirm]y
```

Related Commands

Command	Description
busyout	Disables a port by waiting for the active services on the specified port to terminate.
clear line	Returns a line to its idle state.
clear port	Resets the NextPort port and clears any active call.
show spe	Displays SPE status.
shutdown (port)	Disables a port.

clear spe counters

To clear all statistics, use the **clear spe counters** command in EXEC mode.

Cisco AS5350 and Cisco AS5400 with the NextPort Dial Feature Card (DFC)

clear spe counters [*slot* | *slot*/*spe*] [*slot* | *slot*/*spe*]

Cisco AS5800 with the Universal Port Card (UPC)

clear spe counters [*slot*/*spe* | *shelf*/*slot* | *shelf*/*slot*/*spe*] [*slot*/*spe* | *shelf*/*slot* | *shelf*/*slot*/*spe*]

Syntax Description

slot	(Optional) The slot number to be cleared. All ports on the specified slot will be cleared. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7. A range of slots can be cleared by entering a second value for the *slot* argument.
slot/*spe*	(Optional) The slot and service processing element (SPE) number to be cleared. All ports on the specified slot and SPE will be cleared. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7. The SPE values range from 0 to 17.You must type in the slash mark. A range of SPEs can be cleared by entering by entering a second value for the *slot*/*spe* argument.
shelf/*slot*	(Optional) The shelf and slot number to be cleared. All ports on the specified shelf and slot will be cleared. For the Cisco AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11. You must type in the slash mark. A range of slots can be cleared by entering by entering a second value for the *shelf*/*slot* argument.
shelf/*slot*/*spe*	(Optional) The shelf, slot and SPE number to be cleared. All ports on the specified SPE will be cleared. For the Cisco AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 0 to 53. You must type in the slash marks. A range of SPEs can be cleared by entering by entering a second value for the *shelf*/*slot*/*spe* argument.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5800.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

The **clear spe counters** command clears statistical counters of all service types for the specified SPE, range of SPEs, or all the SPEs. If you do not set a parameter, you clear all SPE statistical counters.

Examples

The following example shows how to clear all statistics by entering the **clear spe counters** command on the Cisco AS5350 with the NextPort DFC:

```
Router# clear spe counters 1/3 1/7

This will clear statistic counters for SPEs 1/03 - 1/07 [confirm]y
```

The following example shows how to clear all statistics by entering the **clear spe counters** command on the Cisco AS5800 with the UPC. This example clears shelf 1, slot 3, ports 0 to 11.

```
Router# clear spe counters 1/3/0 1/3/11

This will clear statistic counters for SPEs 1/03/00 - 1/03/11[confirm]y
```

clear spe log

To clear event entries in the slot history event log, use the **clear spe log** command in EXEC mode.

Cisco AS5400 with the NextPort Dial Feature Card (DFC)

clear spe log [*slot*] [*slot*]

Cisco AS5800 with the Universal Port Card (UPC)

clear spe log [*shelf*/*slot*] [*shelf*/*slot*]

Syntax Description

slot	(Optional) The slot number to be cleared. All ports on the specified slot will be cleared. For the Cisco AS5400, slot values range from 1 to 7. A range of slots can be cleared by entering a second value for the *slot* argument.
shelf/*slot*	(Optional) The shelf and slot number to be cleared. All ports on the specified shelf and slot will be cleared. For the Cisco AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11. You must type in the slash mark. A range of slots can be cleared by entering a second value for the *shelf*/*slot* argument.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5800.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

The **clear spe log** command clears event entries in the slot history event log. If you do not specify the shelf/slot range, all service processing element (SPE) event entries clear.

If you specify the shelf/slot, only the event entries for that slot clear.

Examples

The following example shows output from the **clear spe log** command on the Cisco AS5400 with the NextPort DFC. This example clears the SPE log from shelf 1, 2 and 3:

```
Router# clear spe log 1 3

This will clear slot event history for slot(s) 1 - 3[confirm]y
```

The following example shows output from the **clear spe log** command on the Cisco AS5800 with the UPC. This example clears shelf 1, slot 8:

```
Router# clear spe log 1/8
This will clear slot event history for slot(s) 8 - 8[confirm]y
```

Related Commands

Command	Description
show spe log	Displays the SPE system log.

clid group

To add a calling line identifier (CLID) group to a discriminator, use the **clid group** command in CLID configuration mode. To remove a CLID group from a discriminator, use the **no** form of this command.

clid group {*clid-group-name* | **default**}

no clid group {*clid-group-name* | **default**}

Syntax Description

clid-group-name	Name of the CLID group added to the discriminator. You can add an existing CLID group or one that is to be defined. Discrimination does not happen until the CLID group is defined.
default	Default discrimination profile. Any CLID number coming in on a call is in its respective default group unless it is specifically assigned a CLID group name.

Command Default

CLID screening is not used.

Command Modes

CLID configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.

Usage Guidelines

Use the **clid group** command to add a CLID group (which specifies the calls to reject) to the discriminator. If you use the default option, CLID call screening is not used.

Examples

The following example shows a call discriminator named “clidElim” created and configured to block digital calls from the CLID group named “group1”:

```
resource-pool profile discriminator clidElim
 call-type digital
 clid group group1
```

Related Commands

Command	Description
call-type	Specifies the type of calls you want to block.
resource-pool profile discriminator	Creates a call discrimination profile and assigns it a name.

clock source line

To set the E1 line clock source for the Cisco AS5200 access server, use the **clock source line** command in controller configuration mode. To change or remove the clocking source, use the **no** form of this command.

clock source line {**primary** | **secondary**}

no clock source line {**primary** | **secondary**}

Syntax Description

primary	Primary TDM clock source.
secondary	Secondary TDM clock source.

Command Default

Primary TDM clock source is taken from the E1 controller 0 on the Cisco AS5200.

Secondary TDM clock source is taken from the E1 controller 1 on the Cisco AS5200.

Command Modes

Controller configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Configure the **clock source line primary** command on the controller that takes the most reliable clocking from an E1 line. Configure the **clock source line secondary** command on the controller that has the next best known clocking. With this configuration, the primary line clocking is backed up to the secondary line if the primary clocking shuts down.

Examples

The following example configures the Cisco AS5200 to use E1 controller 0 as the primary clocking source and the E1 controller 1 as the secondary clocking source:

```
controller e1 0
 framing esf
 linecode hdb3
 pri-group timeslots 1-23
 clock source line primary
!
controller e1 1
 framing esf
 linecode hdb3
 pri-group timeslots 1-23
 clock source line secondary
```

Related Commands

Command	Description
clear controller	Resets the T1 or E1 controller.
controller	Configures a T1 or E1 controller and enters controller configuration mode.
linecode	Selects the linecode type for T1 or E1 line.
show controllers e1	Displays information about the E1 links supported by the NPM (Cisco 4000) or MIP (Cisco 7500 series).

copy modem

To copy modem firmware to integrated modems in an access server, use the **copy modem** command in EXEC mode.

copy {**flash** | **tftp** | **rcp**} **modem**

Syntax Description

flash	Flash memory.
tftp	Local TFTP server.
rcp	Local rcp server.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Note The **copy modem** command is no longer available for MICA portware and 56K Microcom modems on Cisco AS5200 and AS5300 access servers. Use the **spe** command instead.

The Microcom V.34 modems and Cisco AS5200 V.110 terminal adapter will continue to use the **copy modem** command. On bootup, because these modems do not require download, the command displays the location of the firmware as "feature_card_flash."

After you enable this command, you are asked to provide the download destination (a *slot/port* or **all**), the remote host name, and the path leading to the source modem firmware.

If a modem that you want to upgrade is busy with a call when the **copy modem** command is enabled, the upgrade for that modem yields until the active call is dropped. All other idle modems in the upgrade range proceed with the downloading operation.

Examples

The following example copies the modem firmware file called modem_upgrade from the TFTP server called Modem_Server to modem 2/0, which is installed in a Cisco AS5200 access server:

```
Router# copy tftp modem

Modem Numbers (<slot>/<port>[-<slot>/<port>] | group <number> | all)? 2/0
Address or name of remote host [UNKNOWN]? Modem_Server
Source file name? file1/elem/modem_upgrade
Accessing file 'file1/elem/modem_upgrade on Modem_Server...
Loading file1/elem/modem_upgrade .from 192.168.254.254 (via Ethernet0): ! [OK]

Loading file1/elem/modem_upgrade from 192.168.254.254 (via Ethernet0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 237503/278528 bytes]
```

```
Router#
%MODEM-5-DL_START: Modem (2/0) started firmware download
%MODEM-5-DL_GOOD: Modem (2/0) completed firmware download:
MNPClass10V.34/V.FCModemRev1.0.23/85.23/85
```

As shown in this example, you might want to upgrade and test one modem's firmware before upgrading the firmware of all the modems on the access server, as shown in the next example.

The following example downloads the same modem firmware file from the TFTP server to all the modems in the Cisco AS5200 access server:

```
Router# copy tftp modem

Modem Numbers (<slot>/<port>[-<slot>/<port>] | group <number> | all)? all
Address or name of remote host [UNKNOWN]? Modem_Server
Source file name? file1/elem/modem_upgrade
Accessing file 'file1/elem/modem_upgrade on Modem_Server...
Loading file1/elem/modem_upgrade .from 192.168.254.254 (via Ethernet0): ! [OK]

Loading file1/elem/modem_upgrade from 192.168.254.254 (via Ethernet0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 237503/278528 bytes]

Router#
%MODEM-5-DL_START: Modem (2/0) started firmware download
%MODEM-5-DL_START: Modem (2/1) started firmware download
%MODEM-5-DL_START: Modem (2/2) started firmware download
%MODEM-5-DL_START: Modem (2/3) started firmware download
%MODEM-5-DL_START: Modem (2/4) started firmware download
%MODEM-5-DL_START: Modem (2/5) started firmware download
%MODEM-5-DL_START: Modem (2/6) started firmware download
%MODEM-5-DL_START: Modem (2/7) started firmware download
%MODEM-5-DL_START: Modem (2/8) started firmware download
%MODEM-5-DL_START: Modem (2/9) started firmware download
%MODEM-5-DL_START: Modem (2/10) started firmware download
%MODEM-5-DL_START: Modem (2/11) started firmware download
%MODEM-5-DL_START: Modem (2/12) started firmware download
%MODEM-5-DL_START: Modem (2/13) started firmware download
%MODEM-5-DL_START: Modem (2/14) started firmware download
%MODEM-5-DL_START: Modem (2/15) started firmware download
%MODEM-5-DL_START: Modem (2/16) started firmware download
%MODEM-5-DL_START: Modem (2/17) started firmware download
%MODEM-5-DL_START: Modem (2/18) started firmware download
%MODEM-5-DL_START: Modem (2/19) started firmware download
%MODEM-5-DL_START: Modem (2/20) started firmware download
%MODEM-5-DL_START: Modem (2/21) started firmware download
%MODEM-5-DL_START: Modem (2/22) started firmware download
%MODEM-5-DL_START: Modem (2/23) started firmware download
%MODEM-5-DL_GOOD: Modem (2/2) completed firmware download:
MNPClass10V.34/V.FCModemRev1.0.23/85.23/85
%MODEM-5-DL_GOOD: Modem (2/10) completed firmware download:
MNPClass10V.34/V.FCModemRev1.0.23/85.23/85
%MODEM-5-DL_GOOD: Modem (2/4) completed firmware download:
MNPClass10V.34/V.FCModemRev1.0.23/85.23/85
%MODEM-5-DL_GOOD: Modem (2/6) completed firmware download:
MNPClass10V.34/V.FCModemRev1.0.23/85.23/85
%MODEM-5-DL_GOOD: Modem (2/7) completed firmware download:
MNPClass10V.34/V.FCModemRev1.0.23/85.23/85
%MODEM-5-DL_GOOD: Modem (2/12) completed firmware download:
MNPClass10V.34/V.FCModemRev1.0.23/85.23/85
%MODEM-5-DL_GOOD: Modem (2/11) completed firmware download:
MNPClass10V.34/V.FCModemRev1.0.23/85.23/85
```

```
%MODEM-5-DL_GOOD: Modem (2/13) completed firmware download:
MNPClass10V.34/V.FCModemRev1.0.23/85.23/85
%MODEM-5-DL_GOOD: Modem (2/1) completed firmware download:
MNPClass10V.34/V.FCModemRev1.0.23/85.23/85
%MODEM-5-DL_GOOD: Modem (2/14) completed firmware download:
MNPClass10V.34/V.FCModemRev1.0.23/85.23/85
%MODEM-5-DL_GOOD: Modem (2/19) completed firmware download:
MNPClass10V.34/V.FCModemRev1.0.23/85.23/85
%MODEM-5-DL_GOOD: Modem (2/22) completed firmware download:
MNPClass10V.34/V.FCModemRev1.0.23/85.23/85
%MODEM-5-DL_GOOD: Modem (2/5) completed firmware download:
MNPClass10V.34/V.FCModemRev1.0.23/85.23/85
%MODEM-5-DL_GOOD: Modem (2/8) completed firmware download:
MNPClass10V.34/V.FCModemRev1.0.23/85.23/85
%MODEM-5-DL_GOOD: Modem (2/9) completed firmware download:
MNPClass10V.34/V.FCModemRev1.0.23/85.23/85
%MODEM-5-DL_GOOD: Modem (2/17) completed firmware download:
MNPClass10V.34/V.FCModemRev1.0.23/85.23/85
%MODEM-5-DL_GOOD: Modem (2/0) completed firmware download:
MNPClass10V.34/V.FCModemRev1.0.23/85.23/85
%MODEM-5-DL_GOOD: Modem (2/3) completed firmware download:
MNPClass10V.34/V.FCModemRev1.0.23/85.23/85
%MODEM-5-DL_GOOD: Modem (2/21) completed firmware download:
MNPClass10V.34/V.FCModemRev1.0.23/85.23/85
%MODEM-5-DL_GOOD: Modem (2/16) completed firmware download:
MNPClass10V.34/V.FCModemRev1.0.23/85.23/85
%MODEM-5-DL_GOOD: Modem (2/15) completed firmware download:
MNPClass10V.34/V.FCModemRev1.0.23/85.23/85
%MODEM-5-DL_GOOD: Modem (2/18) completed firmware download:
MNPClass10V.34/V.FCModemRev1.0.23/85.23/85
%MODEM-5-DL_GOOD: Modem (2/20) completed firmware download:
MNPClass10V.34/V.FCModemRev1.0.23/85.23/85
%MODEM-5-DL_GOOD: Modem (2/23) completed firmware download:
MNPClass10V.34/V.FCModemRev1.0.23/85.23/85
```

The following example copies the modem firmware file called STAR.M from Flash memory to the integrated modem 1/2:

```
Router# copy flash modem

Modem Numbers (<slot>/<port> | group <number> | all)? 1/2

System flash directory:
File  Length   Name/status
  1   3539820  as5200-i-m.allcookies
  2   239203   STAR.M
  3   23072    BOOT.105 [3802288 bytes used, 4586320 available, 8388608 total]
Source file name? STAR.M
Router#
%MODEM-5-DL_START: Modem (1/2) started firmware download
%MODEM-5-DL_GOOD: Modem (1/2) completed firmware download:
MNPClass10V.34/V.FCModemRev1.0.23/85.23/85
Router
```

Related Commands

Command	Description
copy	Copies any file from a source to a destination.
spe	Enters SPE configuration mode and sets the range of SPEs.

corlist incoming

To specify the class of restrictions (COR) list to be used when a specified dial peer acts as the incoming dial peer, use the **corlist incoming** command in dial peer configuration mode. To clear the previously defined incoming COR list in preparation for redefining the incoming COR list, use the **no** form of this command.

corlist incoming *cor-list-name*

no corlist incoming *cor-list-name*

Syntax Description

cor-list-name	Name of the dial peer COR list that defines the capabilities that the specified dial peer has when it is used as an incoming dial peer.

Command Default

No default behavior or values.

Command Modes

Dial peer configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

The **dial-peer cor list** and **member** commands define a set of capabilities (a COR list). These lists are used in dial peers to indicate the capability set that a dial peer has when it is used as an incoming dial peer (the **corlist incoming** command) or to indicate the capability set that is required for an incoming dial peer to make an outgoing call through the dial peer (the **corlist outgoing** command). For example, if dial peer 100 is the incoming dial peer and its incoming COR list name is list100, dial peer 200 has list200 as the outgoing COR list name. If list100 does not include all the members of list200 (that is, if list100 is not a superset of list200), it is not possible to have a call from dial peer 100 that uses dial peer 200 as the outgoing dial peer.

Examples

In the following example, incoming calls from 526.... are blocked from being switched to outgoing calls to 1900.... because the COR list for the incoming dial peer (list2) is not a superset of the COR list for the outgoing dial peer (list1):

```
dial-peer list list1
 member 900call

dial-peer list list2
 member 800call
 member othercall

dial-peer voice 526 pots
 answer-address 408555....
 corlist incoming list2
 direct-inward-dial
```

```
dial-peer voice 900 pots
 destination pattern 1900.......
 direct-inward-dial
 trunkgroup 101
 prefix 333
 corlist outgoing list1
```

Related Commands

Command	Description
corlist outgoing	Specifies the COR list to be used by outgoing dial peers.
dial-peer cor list	Defines a COR list name.
member	Adds a member to a dial peer COR list.

corlist outgoing

To specify the class of restrictions (COR) list to be used by outgoing dial peers, use the **corlist outgoing** command in dial peer configuration mode. To clear the previously defined outgoing COR list in preparation for redefining the outgoing COR list, use the **no** form of this command.

corlist outgoing *cor-list-name*

no corlist outgoing *cor-list-name*

Syntax Description

cor-list-name	Required name of the dial peer COR list for outgoing calls to the configured number using this dial peer.

Command Default

No default behavior or values.

Command Modes

Dial peer configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

If the COR list for the incoming dial peer is not a superset of the COR list for the outgoing dial peer, calls from the incoming dial peer cannot use that outgoing dial peer.

Examples

In the following example, incoming calls from 526.... are blocked from being switched to outgoing calls to 1900.... because the COR list for the incoming dial peer (list2) is not a superset of the COR list for the outgoing dial peer (list1):

```
dial-peer list list1
member 900call

dial-peer list list2
 member 800call
 member othercall

dial-peer voice 526 pots
 answer-address 408555....
 corlist incoming list2
 direct-inward-dial

dial-peer voice 900 pots
 destination pattern 1900.......
 direct-inward-dial
 trunk group 101
 prefix 333
 corlist outgoing list1
```

cpp authentication

Note Effective with Cisco IOS Release 12.3(4)T, the **cpp authentication** command is no longer available in Cisco IOS software.

To enable negotiation of authentication with a router or bridge that supports the Combinet Proprietary Protocol (CPP) and that is calling in to this router, use the **cpp authentication** command in interface configuration mode. To disable negotiation of CPP authentication, use the **no** form of this command.

cpp authentication

no cpp authentication

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.3(4)T	This command was removed and is no longer available in Cisco IOS software.

Usage Guidelines

Use this command for authenticating the device that is calling in to this router.

Use this command to communicate over an ISDN interface with Cisco 700 and 800 series (formerly Combinet) routers that do not support PPP but do support the CPP.

Since most Cisco routers support PPP, Cisco routers can communicate over ISDN with CPP devices by using PPP encapsulation, which supports both routing and fast switching.

This command is supported on ISDN and dialer interfaces.

This command uses names and passwords from the **username password** command. It does not support TACACS.

Examples

The following example configures a PRI to communicate with a bridge that does not support PPP:

```
controller t1 1/1
 framing esf
 linecode b8zs
 pri-group timeslots 1-23
 isdn switchtype primary-4ess
```

```
interface Serial1/1:23
 encapsulation cpp
 cpp callback accept
 cpp authentication
```

The following example configures a BRI to communicate with a bridge that does not support PPP:

```
interface bri 0
 encapsulation cpp
 cpp callback accept
 cpp authentication
```

Related Commands

Command	Description
cpp callback accept	Enables the router to accept callback from a router or bridge that supports the CPP.
encapsulation cpp	Enables encapsulation for communication with routers or bridges using the CPP.
virtual-profile aaa	Enables virtual profiles by AAA configuration.

cpp callback accept

Note Effective with Cisco IOS Release 12.3(4)T, the **cpp callback accept** command is no longer available in Cisco IOS software.

To enable the router to accept callback from a router or bridge that supports the Combinet Proprietary Protocol (CPP), use the **cpp callback accept** command in interface configuration mode. To disable callback acceptance, use the **no** form of this command.

cpp callback accept

no cpp callback accept

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.3(4)T	This command was removed and is no longer available in Cisco IOS software.

Usage Guidelines

Use this command to communicate over an ISDN interface with Cisco 700 and 800 series (formerly Combinet) routers that do not support PPP but do support CPP.

Currently, most Cisco routers *do* support PPP. Cisco routers can communicate over ISDN with these devices by using PPP encapsulation, which supports both routing and fast switching.

This command is supported on ISDN and dialer interfaces.

Examples

The following example configures the PRI serial interface 1/1:23 to communicate with a router or bridge that does not support PPP:

```
controller t1 1/1
 framing esf
 linecode b8zs
 pri-group timeslots 1-23
 isdn switchtype primary-4ess
!
interface Serial1/1:23
 encapsulation cpp
 cpp callback accept
 cpp authentication
```

The following example configures BRI 0 to communicate with a router or bridge that does not support PPP:

```
interface bri 0
 encapsulation cpp
 cpp callback accept
 cpp authentication
```

Related Commands

Command	Description
cpp authentication	Enables negotiation of authentication with a router or bridge that supports the CPP and that is calling in to this router.
encapsulation cpp	Enables encapsulation for communication with routers or bridges using the CPP.

debounce-time rai

To configure a timer that prevents E1 or STM-1 trunk lines from being torn down in response to brief line outages, use the **debounce-time rai** command in controller configuration mode. To restore the default timer value, use the **no** form of this command.

debounce-time rai *milliseconds*

no debounce-time rai *milliseconds*

Syntax Description

milliseconds	Time, in milliseconds (ms), to wait before tearing down an E1 or STM-1 line after receiving a Receive Alarm Indication (RAI) signal. **AS5800** • E1 lines—Valid values range from 500 to 7000 ms. The value entered must be a multiple of 50. The default value is 500 ms. **AS5850** • E1 lines—Valid values range from 1000 to 7000 ms. The value entered must be a multiple of 50. The default value is 1000 ms. • STM-1 lines—Valid values range from 2000 to 7000 ms. The value entered must be a multiple of 50. The default value is 2000 ms.

Command Default

The default value for the timer is used:

- E1 lines on the AS5800—500 ms
- E1 lines on the AS5850—1000 ms
- STM-1 lines on the AS5850—2000 ms

Command Modes

Controller configuration

Command History

Release	Modification
12.2(2)XB5	This command was introduced on the Cisco AS5800 and the route switch controller (RSC) Cisco AS5850.
12.2(11)T	Support for this command on the Cisco AS5800 and the RSC Cisco AS5850 was integrated into Cisco IOS Release 12.2(11)T.
12.3(7)XI	Support for this command was added for the enhanced RSC (ERSC) Cisco AS5850.
12.3(4)T	Support for the ERSC Cisco AS5850 was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

Use the **debounce-time rai** command to configure a timer that allows Awaiting Info (I) calls to ignore brief trunk outages. When a Receive Alarm Indication (RAI) signal is received, the access server will wait the configured interval before tearing down the line.

Examples

The following example configures an E1 controller to wait for 5250 ms before tearing down an E1 trunk line:

```
Router(config)# controller e1 1/0/0
Router(config-controller)# debounce-time rai 5250
```

Related Commands

Command	Description
controller	Configures a T1, E1, or J1 controller and enters controller configuration mode.

description (interface)

To add a description to an interface configuration, use the **description** command in interface configuration mode. To remove the description, use the **no** form of this command.

description *string*

no description

Syntax Description

string	Comment or a description to help you remember what is attached to this interface. This string is limited to 238 characters.

Command Default

No description is added.

Command Modes

Interface configuration

Command History

Release	Modification
9.21	This command was introduced.

Usage Guidelines

The **description** command is meant solely as a comment to be put in the configuration to help you remember what certain interfaces are used for. The description appears in the output of the following EXEC commands: **more nvram:startup-config**, **show interfaces**, and **more system:running-config**.

Examples

The following example shows how to add a description for a T1 interface:

```
interface serial 0
 description Fractional T1 line to remote office -- 128 kbps
```

Related Commands

Command	Description
more nvram:startup-config	Displays the startup configuration file contained in NVRAM or specified by the CONFIG_FILE environment variable.
more system:running-config	Displays the running configuration.
show interfaces	Displays statistics for all interfaces configured on the router or access server.

dialer

To specify the dialer interface that an accept-dialout virtual private dialup network (VPDN) subgroup will use to dial out calls, use the **dialer** command in accept-dialout configuration mode. To remove the dialer interface from the accept-dialout VPDN subgroup, use the **no** form of this command.

dialer *dialer-interface*

no dialer

Syntax Description

dialer-interface	Number of the dialer interface.

Command Default

Disabled

Command Modes

Accept-dialout configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

You must first enable Layer 2 Tunneling Protocol (L2TP) on the accept-dialout VPDN subgroup by using the **protocol l2tp** command before you can enable the **dialer** command. Removing the **protocol** command will remove the **dialer** command from the accept-dialout subgroup.

You can only specify one dialer per accept dialout group. Configuring a second **dialer** command will replace the first **dialer** command.

Examples

The following example creates an accept-dialout VPDN subgroup that uses dialer interface 2:

```
VPDN-group 1
 accept dialout
  protocol l2tp
  dialer 2
 terminate-from hostname yourhost
```

Related Commands

Command	Description
accept-dialout	Accepts requests to tunnel L2TP dial-out calls and creates an accept-dialout VPDN subgroup.
protocol (VPDN)	Specifies the L2TP that the VPDN subgroup will use.
terminate-from	Specifies the host name of the remote LAC or LNS that will be required when accepting a VPDN tunnel.

dialer callback-secure

To enable callback security, use the **dialer callback-secure** command in interface configuration mode. To disable callback security, use the **no** form of this command.

dialer callback-secure

no dialer callback-secure

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

This command affects those users that are not authorized to be called back through configuration of the **dialer callback-server** command. If the username (the *host-name* argument in the **dialer map** command) is not authorized for callback, the call will be disconnected if the **dialer callback-secure** command is configured.

Examples

The following partial example configures BRI0 with the commands required to make it function as the callback server on the shared network. Callback security is enabled on BRI0, such that any user other than user1 will be disconnected and not called back.

```
interface BRI0
 ip address 172.19.1.9 255.255.255.0
 encapsulation ppp
 dialer callback-secure
 dialer enable-timeout 2
 dialer map ip 172.19.1.8 name user1 class dial1 81012345678901
 dialer-group 1
 ppp callback accept
 ppp authentication chap
!
map-class dialer dial1
 dialer callback-server username
```

Related Commands

Command	Description
dialer callback-server	Enables an interface to make return calls when callback is successfully negotiated.
dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites.
map-class dialer	Defines a class of shared configuration parameters associated with the **dialer map** command for outgoing calls from an ISDN interface and for PPP callback.
ppp callback (DDR)	Enables a dialer interface that is not a DTR interface to function either as a callback client that requests callback or as a callback server that accepts callback requests.

dialer callback-server

To enable an interface to make return calls when callback is successfully negotiated, use the **dialer callback-server** command in interface configuration mode. To disable return calls, use the **no** form of this command.

dialer callback-server [**username** | **dialstring**]

no dialer callback-server

Syntax Description

username	(Optional) Looks up the authenticated host name in a **dialer map** command. This is the default.
dialstring	(Optional) Identifies the return call during callback negotiation.

Command Default

Disabled. The default keyword is **username**.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.

Examples

The following partial example configures BRI 0 to function as the callback server on the shared network:

```
interface BRI0
 ip address 172.19.1.9 255.255.255.0
 encapsulation ppp
 dialer callback-secure
 dialer enable-timeout 2
 dialer map ip 172.19.1.8 name mymap class dial1 81012345678901
 dialer-group 1
 ppp callback accept
 ppp authentication chap
!
map-class dialer dial1
 dialer callback-server username
```

Related Commands

Command	Description
dialer callback-secure	Enables callback security.
dialer enable-timeout	Sets the length of time an interface stays down after a call has completed or failed and before the interface is available to dial again.
dialer hold-queue	Allows interesting outgoing packets to be queued until a modem connection is established.
dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites.

Command	Description
map-class dialer	Defines a class of shared configuration parameters associated with the dialer map command for outgoing calls from an ISDN interface and for PPP callback.
ppp callback (DDR)	Enables a dialer interface that is not a DTR interface to function either as a callback client that requests callback or as a callback server that accepts callback requests.

dialer called

To configure dial-on-demand routing (DDR) to perform DNIS-plus-ISDN-subaddress binding for dialer profile interfaces, use the **dialer called** command in dial-on-demand routing configuration mode. To disable DNIS-plus-ISDN-subaddress binding, use the **no** form of this command.

dialer called *DNIS*:*subaddress*

no dialer called *DNIS*:*subaddress*

Syntax Description

DNIS:*subaddress*	Dialed Number Identification Service or the called party number, a colon, and the ISDN subaddress.

Command Default

No default behavior or values.

Command Modes

Dial-on-demand routing configuration

Command History

Release	Modification
12.0(4)T	This command was introduced.

Usage Guidelines

If you have more than one DNIS-plus-ISDN-subaddress number to configure under the same dialer profile interface, you can configure multiple **dialer called** commands.

The parser accepts a **dialer called** command with a DNIS and without the subaddress; however, the call will fail. For a successful call, enter the DNIS, a colon, and the ISDN subaddress after the **dialer called** command.

Examples

The following example configures a dialer profile for a receiver with DNIS 12345 and ISDN subaddress 6789:

```
dialer called 12345:6789
```

Related Commands

Command	Description
dialer caller	Configures caller ID screening and, optionally, enables ISDN caller ID callback for legacy DDR or the dialer profiles DDR feature.

dialer caller

To configure caller ID screening for a dialer rotary group interface or to bind an incoming call to a particular dialer profile, and, optionally, to enable ISDN caller ID callback, use the **dialer caller** command in interface configuration mode. To disable this feature, use the **no** form of this command.

dialer caller *number* [**callback**]

no dialer caller *number* [**callback**]

Syntax Description

number	Remote telephone number for which to screen. Use a lower case letter x to represent a single "don't care" digit. The maximum length of each number is 25 characters.
callback	(Optional) Enables callback.

Command Default

Caller ID screening, call binding, and ISDN caller ID callback are disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

On a dialer rotary group interface, this command configures the Cisco IOS software to accept calls from the specified number or, used with the **callback** keyword, to reject incoming calls from the specified number but to initiate callback to the number.

When the optional **callback** keyword is used, the initial call is rejected (hence, not subject to tolls) and callback is initiated to the calling number.

When x's are used in the callback number, dialer caller screening is based on a best match system that uses the number of x's as a criterion. To make callback calls only to specified numbers or ranges of numbers but to accept any other incoming calls, make sure that the number of x's in any configuration line that uses the **callback** keyword is less than the number of x's in any configuration line that does not use the keyword.

For example, if you use at most four x's in the configuration lines with the **callback** keyword, then to accept calls from other numbers use at least five x's in a configuration line that does not use the **callback** keyword.

Note Caller ID screening requires a local switch that is capable of delivering the caller ID to the router or access server. If you enable caller ID screening but do not have such a switch, no calls will be allowed in.

For dialer profiles, this command helps bind a dialer profile to—and thus configure—the interface used for a call. The dialer command acts as a binding command by associating an incoming call with a specified dialer profile if the caller ID presented by the call matches the dialer caller value.

Note Incoming calls also can be bound to a dialer profile based on PPP name authentication, so in this instance the incoming call can be bound to the dialer profile even if the presented caller ID does not match the dialer caller value. To configure caller ID screening with dialer profiles, use the legacy **isdn caller** command.

Examples

In the following example, callback calls will be made only to numbers in the 555 and 556 exchanges, but any other number can call in:

```
dialer caller 408555xxxx callback
dialer caller 408556xxxx callback
dialer caller xxxxx
```

Related Commands

Command	Description
isdn caller	Configures ISDN caller ID screening and, optionally, enables ISDN caller ID callback for legacy DDR.
show dialer	Displays general diagnostic information for interfaces configured for DDR.

dialer clid group

To create a Calling Line Identification (CLID) group in the resource pool and assign it a name, use the **dialer clid group** command in global configuration mode. To remove a CLID group from the resource pool, use the **no** form of this command.

dialer clid group *clid-group-name*

no dialer clid group *clid-group-name*

Syntax Description

clid-group-name	Name of the CLID group created in the resource pool.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.

Usage Guidelines

Use the **dialer clid group** command to create a CLID group and assign it a name. The CLID group name must be the same as the name used when configuring the customer profile.

Customer profiles are configured with a DNIS and/or CLID group and call type. The DNIS and/or CLID and call type of the incoming call is used to find the appropriate customer profile.

Examples

The following example shows the command to configure a CLID group named "group1." After you enter this command, the router prompt changes to the CLID configuration mode, Router(config-clid-group)#.

```
Router(config)# dialer clid group group1
```

Related Commands

Command	Description
number	Adds a DNIS number to a dialer DNIS group.
resource-pool call treatment discriminator	Configures a CLID group in a discriminator.

dialer congestion-threshold

To specify congestion threshold in connected links, use the **dialer congestion-threshold** command in interface configuration mode. To disable this function, use the **no** form of this command.

dialer congestion-threshold *links*

no dialer congestion-threshold

Syntax Description

links	Number of connected links for congestion threshold in the range from 0 to 64,000.

Command Default

The default number of connected links is 64,000.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

This command is used to force the dialer to search for another uncongested system (the alternate network access server) in a stack group to dial out using Stack Group Bidding Protocol (SGBP).

Examples

The following example sets the congestion threshold to five connected links on the Dialer interface 0:

```
interface Dialer0
 dialer aaa
 dialer congestion-threshold 5
```

Related Commands

Command	Description
dialer reserved-links	Reserves links for dial-in and dial-out.
sgbp dial-bids	Allows the stack group to bid for dial-out connection.

dialer dnis group

To create a DNIS group, use the **dialer dnis group** command in global configuration mode. To remove a specific Dialed Number Identification Service (DNIS) group from the running configuration, use the **no** form of this command.

dialer dnis group *name*

no dialer dnis group *name*

Syntax Description

name	Name to assign to the DNIS group number.

Command Default

A dialer DNIS group named *default*.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **dialer dnis group** global configuration command to create a DNIS group. This command enables you to create and populate a DNIS group, which is then added to a profile (customer or discriminator) by using the **dnis group** command within that profile's configuration mode.

Examples

The following example shows a specific DNIS group named modem-group1 being created with the options available for further configuration:

```
dialer dnis group modem-group1

Dialer Called Configuration Commands:
  call-type  set call-type override
  default    Set a command to its defaults
  exit       Exit from dialer configuration mode
  help       Description of the interactive help system
  no         Negate a command or set its defaults
  number     Enter number in dnis group
```

In the following example, a customer profile called isp-1 is created, a DNIS group called dnis-isp-1 is associated with the customer profile, and DNIS numbers 1234 and 5678 are assigned to the DNIS group. Only DNIS numbers 1234 and 5678 are allocated physical resources by the isp-1 customer profile, which counts and manages the resources for these two DNIS numbers and ignores all other DNIS numbers:

```
resource-pool profile customer isp-1
dnis group dnis-isp-1
exit
dialer dnis group dnis-isp-1
number 1234
number 5678
```

Related Commands

Command	Description
dnis group	Includes a group of DNIS numbers in a customer profile.
resource-pool profile	Creates a resource group for RPM.

dialer dns

To obtain a user profile name on a remote network using reverse Domain Name System (DNS), use the **dialer dns** command in interface configuration mode. To disable this function, use the **no** form of this command.

dialer dns

no dialer dns

Syntax Description

This command has no arguments or keywords.

Command Default

The reverse DNS function is disabled by default.

Command Modes

Interface configuration of a dialer rotary group leader

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

This command allows the dialer to use reverse DNS to get a profile name for accessing the authentication, authorization, and accounting (AAA) server. This command is not required when using named static routes.

Examples

The following example shows how to allow the dialer to use reverse DNS for name lookup:

```
interface dialer 0
 dialer aaa
 dialer dns
```

Related Commands

Command	Description
dialer aaa	Allows a dialer to access the AAA server for dialing information.

dialer dtr

To enable dial-on-demand routing (DDR) on an interface and specify that the serial line is connected by non-V.25*bis* modems using Electronic Industries Association (EIA) signaling only—specifically, the data terminal ready (DTR) signal—use the **dialer dtr** command in interface configuration mode. To disable DDR for the interface, use the **no** form of this command.

dialer dtr

no dialer dtr

Syntax Description

This command has no arguments or keywords.

Command Default

DTR dialing is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

A serial interface configured for DTR dialing can place calls only; it cannot accept them.

When a local interface is configured for DTR dialing, the remote interface (that will be receiving the calls) can be configured for in-band dialing or not configured for anything but encapsulation, depending on the desired behavior. If the remote interface is expected to terminate a call when no traffic is transmitted for some time, it must be configured for in-band dialing (along with access lists and a dummy dialer string). If the remote interface is purely passive, no configuration is necessary.

Rotary groups cannot be configured for DTR dialing.

The **dialer map** and **dialer string** commands have no effect on DTR dialers.

Examples

The following example enables DDR and specifies DTR dialing on an interface:

```
Router(config-if)# dialer dtr
```

Related Commands

Command	Description
dialer in-band	Specifies that DDR is to be supported.
dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites.
dialer string (legacy DDR)	Specifies the destination string (telephone number) to be called for interfaces calling a single site.

dialer enable-timeout

To set the length of time an interface stays down after a call has completed or failed and before it is available to dial again, use the **dialer enable-timeout** command in interface configuration mode. To return to the default value, use the **no** form of this command.

dialer enable-timeout *seconds*

no dialer enable-timeout

Syntax Description

seconds	Time in seconds that the Cisco IOS software waits before the next call can occur on the specific interface. Acceptable values are positive, nonzero integers in the range from 1 through 2147483. This value must be greater than the serial pulse interval for this interface, set via the **pulse-time** command.

Command Default

15 seconds

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **dialer enable-timeout** command can be configured as a line down timer, to keep asynchronous interface lines down for a certain period of time, and as a callback timer for both synchronous and asynchronous interfaces.

If your phone lines are often busy or down, you may need to enforce a certain period of time before the system repeats an attempt to make a connection with a remote site. Configuring this timeout can prevent outgoing lines and switching equipment from being needlessly overloaded. In this application, the **dialer enable-timeout** command applies to both inbound and outbound calls on asynchronous interfaces only.

When the **dialer enable-timeout** command is configured on an ISDN interface, its only effect is to set a callback timer, because it is not possible (nor advisable) to keep an ISDN interface disconnected.

Examples

The following example shows how to specify a timeout period of 30 seconds on asynchronous interface 1 before attempting another connection:

```
interface async 1
 dialer enable-timeout 30
```

The following example shows how to configure a BRI interface for legacy dial-on-demand routing (DDR) and ISDN caller ID callback:

```
interface bri 0
 description Connected to NTT 81012345678901
 ip address 10.1.1.7 255.255.255.0
```

```
 no ip mroute-cache
 encapsulation ppp
 isdn caller 81012345678902 callback
 dialer enable-timeout 2
 dialer map ip 10.1.1.8 name spanky 81012345678902
 dialer-group 1
 ppp authentication chap
```

The following examples show how to configure a PPP callback server and client.

PPP Callback Server

The PPP callback server is configured on an ISDN BRI interface and requires an enable timeout period and a map class to be defined.

```
interface bri 0
 ip address 10.1.1.7 255.255.255.0
 encapsulation ppp
 dialer callback-secure
 dialer enable-timeout 2
 dialer map ip 10.1.1.8 name mymap class dial1 81012345678901
 dialer-group 1
 ppp callback accept
 ppp authentication chap
```

PPP Callback Client

The PPP callback client is also configured on an ISDN BRI interface, but does not require an enable timeout period or a map class to be defined.

```
map-class dialer dial1
dialer callback-server username
 interface bri 0
 ip address 10.1.1.8 255.255.255.0
 encapsulation ppp
 dialer map ip 10.1.1.7 name yourmap 81012345678902
 dialer-group 1
 ppp callback request
 ppp authentication chap
```

dialer fast-idle (interface)

To specify the amount of time that a line for which there is contention will stay idle before it is disconnected and the competing call is placed, use the **dialer fast-idle** command in interface configuration mode. To return to the default value, use the **no** form of this command.

dialer fast-idle *seconds*

no dialer fast-idle

Syntax Description

seconds	Idle time, in seconds, that must occur on an interface before the line is disconnected. Acceptable values are positive, nonzero integers.

Command Default

20 seconds

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The dialer fast idle timer is activated if there is contention for a line. The dialer fast idle timer is activated if a line is busy, a packet for a different next hop address is received, and the busy line is required to send the competing packet.

If the line becomes idle for configured length of time, the current call is disconnected immediately and the new call is placed.

If the line has not yet been idle as long as the fast idle timeout period, the packet is dropped because there is no way to get through to the destination. After the packet is dropped, the fast idle timer remains active and the current call is disconnected as soon as it has been idle for as long as the fast idle timeout.

The fast idle timer will be restarted if, in the meanwhile, another packet is transmitted to the currently connected destination and it is classified as *interesting*.

This command applies to inbound and outbound calls.

Combining this command with the **dialer idle-timeout** command allows you to configure lines to stay up for a longer period of time when there is no contention, but to be reused more quickly when there are not enough lines for the current demand.

Examples

The following example specifies a fast idle timeout of 35 seconds on asynchronous interface 1:

```
interface async 1
 dialer fast-idle 35
```

Related Commands

Command	Description
dialer idle-timeout (interface)	Specifies the idle time before the line is disconnected.
dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites.

dialer fast-idle (map-class)

To specify the fast idle timer value to use when placing a call to any telephone number associated with a specified class, use the **dialer fast-idle** command in map-class dialer configuration mode. To reset the dialer fast-idle timer to the default, use the **no** form of this command.

dialer fast-idle *seconds*

no dialer fast-idle

Syntax Description

seconds	Number of seconds to wait before placing a different call.

Command Default

Defaults to the fast idle timer value that is set for the interface.

Command Modes

Map-class dialer configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This fast idle timer is associated only with the map class, not the entire interface.

Examples

The following example specifies a dialer fast idle time of 10 seconds:

```
dialer string 4156884540 class Eng

! This map-class ensures that these calls use an ISDN speed of 56 kbps and a
! fast-idle time of 10 seconds.
map-class dialer Eng
 isdn speed 56
 dialer fast-idle 10
 dialer wait-for-carrier-time 30
```

Related Commands

Command	Description
dialer idle-timeout (interface)	Specifies the amount of time that a line for which there is contention will stay idle before it is disconnected and the competing call is placed.
dialer wait-for-carrier-time (map-class)	Specifies the length of time to wait for a carrier when dialing out to the dial string associated with a specified map class.
map-class dialer	Defines a class of shared configuration parameters associated with the dialer map command for outgoing calls from an ISDN interface and for PPP callback.

dialer hold-queue

To allow *interesting* outgoing packets to be queued until a modem connection is established, use the **dialer hold-queue** command in interface configuration mode. To disable the hold queue, use the **no** form of this command.

dialer hold-queue *packets* **timeout** *seconds*

no dialer hold-queue [*packets*]

Syntax Description

packets	Number of packets, in the range from 1 to 100 packets, to hold in the queue. This argument is optional with the **no** form of this command.
timeout *seconds*	Amount of time, in seconds, to queue the packets.

Command Default

The outgoing packet queue is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

A dialer hold queue can be configured on any type of dialer, including in-band synchronous, asynchronous, data terminal ready (DTR), and ISDN dialers. Rotary groups can be configured with a dialer hold queue. If a rotary group is configured with a hold queue, all members of the group will be configured with a dialer hold queue and no individual member's hold queue can be altered.

If no hold queue is configured, packets are dropped during the time required to establish a connection. Setting *packets* to 0 using the **dialer hold-queue** command is equivalent to using the **no dialer hold-queue** command.

Examples

The following command configures a dialer hold queue to hold 10 packets:

```
Router(config-if)# dialer hold-queue 10 timeout 60
```

Related Commands

Command	Description
dialer-group	Controls access by configuring an interface to belong to a specific dialing group.

dialer idle-timeout (interface)

To specify the duration of idle time before a line is disconnected, use the **dialer idle-timeout** command in interface configuration mode. To reset the idle timeout to the default, use the **no** form of this command.

dialer idle-timeout *seconds* [**inbound** | **either**]

no dialer idle-timeout

Syntax Description

seconds	Idle time, in seconds, that must occur on the interface before the line is disconnected. Acceptable values are positive, nonzero integers.
inbound	(Optional) Only inbound traffic will reset the idle timeout.
either	(Optional) Both inbound and outbound traffic will reset the idle timeout.

Command Default

Direction: outbound
Idle time: 120 seconds

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.1(1)T	The following keywords were added: • **inbound** • **either**

Usage Guidelines

This command is used on lines for which there is no contention. When contention occurs, the **dialer fast-idle** command is activated. For example, when a busy line is requested to send another packet to a different destination than it is currently connected to, line contention occurs and the **dialer fast-idle** command is activated.

By default, this command applies to inbound and outbound calls. For example, if a receiving system needs to make outgoing calls, you might configure it with a short idle timeout.

Only packets that match the dialer group reset the idle timer.

Use the **dialer idle-timeout** command to set a very high idle timer when Multilink PPP is configured and you want a multilink bundle to be connected indefinitely. (The **dialer-load threshold 1** command no longer keeps a multilink bundle of n links connected indefinitely and the **dialer-load threshold** command no longer keeps a multilink bundle of two links connected indefinitely.)

Examples

The following example specifies an idle timeout of 3 minutes (180 seconds) on asynchronous interface 1. Because the **inbound** keyword is included, only inbound traffic that matches the dialer group will reset the idle timer.

```
interface async 1
 dialer idle-timeout 180 inbound
```

Related Commands

Command	Description
dialer fast-idle (interface)	Specifies the amount of time that a line for which there is contention will stay idle before it is disconnected and the competing call is placed.
dialer-group	Controls access by configuring an interface to belong to a specific dialing group.

dialer idle-timeout (template)

To set the dialer idle timeout period in a virtual template interface, use the **dialer idle-timeout** command in template configuration mode. To change the dialer idle timeout, use the **no** form of this command.

dialer idle-timeout *seconds* [**inbound | either**]

no dialer idle-timeout *seconds* [**inbound | either**]

Syntax Description

seconds	Resets the idle timer after the period specified, in seconds.
inbound	(Optional) Resets the idle timer after the period specified based only on inbound traffic.
either	(Optional) Resets the idle timer after the period specified based on either inbound or outbound traffic.

Command Default

No default behavior or values.

Command Modes

Template configuration

Command History

Release	Modification
12.2(4)T	This command was introduced for Resource Pool Manager (RPM) template configuration.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300, Cisco AS5400, and Cisco AS5800.

Usage Guidelines

The **dialer idle-timeout** command allows the dialer idle timeout period to be specified in an RPM customer profile and applied on a per-dialed number identification service (DNIS) basis. The dialer idle timer configuration set in this command will override dialer idle timer configurations for dialer, group asynchronous, and virtual template interfaces, unless a per-user configuration is received from an authentication, authorization, and accounting (AAA) per-user interface configuration. In this case, the settings from the AAA per-user interface configuration take precedence over the local interface configuration.

The **dialer idle-timeout** command works well with Multilink PPP (MLP) and Multichassis Multilink PPP (MMP) when the master bundle interface is not a virtual access (projected) interface. For virtual access interfaces where the dialer idle timer cannot be used, you can classify traffic that resets the PPP idle timer using the **ip idle-group** commands.

Examples

The following example sets the idle timeout period in an RPM customer profile template to 45 seconds:

```
template template 1
 dialer idle-timeout 45
```

The following example sets the idle timeout period in an RPM customer profile template to 60 seconds and resets the idle timer based on either inbound or outbound traffic:

```
template template 1
 dialer idle-timeout 60 either
```

The following example sets the idle timeout period in an RPM customer profile template to 100 seconds and resets the idle timer based only on inbound traffic:

```
template template 1
 dialer idle-timeout 100 inbound
```

Related Commands

Command	Description
dialer-group (template)	Controls access by configuring a virtual template interface to belong to a specific dialing group.
ip idle-group	Configures interesting traffic on an interface for the PPP idle timer.
template	Accesses the template configuration mode for configuring a particular customer profile template.

dialer in-band

To specify that dial-on-demand routing (DDR) is to be supported, use the **dialer in-band** command in interface configuration mode. To disable DDR for the interface, use the **no** form of this command.

dialer in-band [**no-parity** | **odd-parity**]

no dialer in-band

Syntax Description

no-parity	(Optional) No parity is to be applied to the dialer string that is sent out to the modem on synchronous interfaces.
odd-parity	(Optional) Dialed number has odd parity (7-bit ASCII characters with the eighth bit as the parity bit) on synchronous interfaces.

Command Default

Disabled. By default, no parity is applied to the dialer string.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **dialer in-band** command specifies that chat scripts will be used on asynchronous interfaces and V.25*bis* will be used on synchronous interfaces. The parity keywords do not apply to asynchronous interfaces. The parity setting applies to the dialer string that is sent out to the modem. If you do not specify a parity, or if you specify no parity, no parity is applied to the output number. If odd parity is configured, the dialed number will have odd parity (7-bit ASCII characters with the eighth bit as the parity bit.) If an interface only accepts calls and does not place calls, the **dialer in-band** interface configuration command is the only command needed to configure it. If an interface is configured in this manner, with no dialer rotary groups, the idle timer never disconnects the line. It is up to the remote end (the end that placed the call) to disconnect the line based on idle time.

Examples

The following example specifies DDR for asynchronous interface 1:

```
interface async 1
 dialer in-band
```

Related Commands

Command	Description
dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites.
dialer string (legacy DDR)	Specifies the string (telephone number) to be called for interfaces calling a single site.

dialer isdn

To specify the bit rate used on the B channel associated with a specified map class and to specify whether to set up semipermanent connections for this map class, use the **dialer isdn** command in map-class dialer configuration mode. To remove the speed and connection settings, use the **no** form of this command.

dialer isdn [**speed** *speed*] [**spc**]

no dialer isdn [**speed** *speed*] [**spc**]

Syntax Description

speed *speed*	(Optional) Bit rate, in kilobytes per second (Kbps), used on the ISDN B channel. Values are **56** and **64**. Default is 64.
spc	(Optional) ISDN semipermanent connection is used for calls associated with this map class.

Command Default

Bit rate is 64 Kbps. Semipermanent connections are not set up.

Command Modes

Map-class dialer configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

This command is valid for ISDN interfaces only.

Examples

The following example configures a speed of 56 Kbps and no semipermanent connections for the Eng map class:

```
dialer string 4155550140 class Eng

! This map-class ensures that these calls use an ISDN speed of 56 kbps and that
! no semipermanent connection is set up.
map-class dialer Eng
dialer isdn speed 56
```

Related Commands

Command	Description
dialer wait-for-carrier-time (map-class)	Specifies the length of time to wait for a carrier when dialing out to the dial string associated with a specified map class.

dialer isdn short-hold

To configure the router to disconnect a call at the end of the current charging period if the line has been idle for at least the specified minimum period, use the **dialer isdn short-hold** command in map-class dialer configuration mode. To reset the ISDN short-hold timer to the default period, use the **no** form of this command.

dialer isdn short-hold *seconds*

no dialer isdn short-hold

Syntax Description

seconds	Minimum number of seconds of idle time on the line. Default is 120 seconds.

Command Default

Disabled; the router uses a static idle timeout. When this command is enabled, the default short-hold timeout is 120 seconds.

Command Modes

Map-class dialer configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

This command is used for configuring ISDN Advice of Charge (AOC) on Cisco routers.

Use the **dialer isdn short-hold** command if you subscribe to an ISDN AOC during-call service provided by the local ISDN network and want to use this option. The router uses the frequency at which the network sends the AOC-D message to determine the charging period. If the line has been idle for the short-hold timeout, the call disconnects at the end of the charging period. If the line has not been idle for at least that long, the call is maintained into the next charging period.

Examples

The following partial example configures the dialer map class Deutschland with a static idle timeout for outgoing calls. The static idle timer is to be used if for any reason the network does not provide charging information. It also configures a short-hold timeout to allow the router to determine dynamically whether to disconnect or continue the call at the end of the charging period.

```
dialer map-class myclass
 dialer idle-timeout 150
 dialer isdn short-hold 120
```

Related Commands

Command	Description
dialer map	Configures a serial interface or ISDN interface to call one or multiple sites, or to receive calls from multiple sites.
dialer string (dialer profiles)	Specifies the string (telephone number) to be used when placing a call from an interface.
dialer wait-for-carrier-time (map-class)	Specifies the length of time to wait for a carrier when dialing out to the dial string associated with a specified map class.
map-class dialer	Defines a class of shared configuration parameters associated with the dialer map command for outgoing calls from an ISDN interface and for PPP callback.

dialer load-threshold

To configure bandwidth on demand by setting the maximum load before the dialer places another call to a destination, use the **dialer load-threshold** command in interface configuration mode. To disable the setting, use the **no** form of this command.

dialer load-threshold *load* [**outbound | inbound | either**]

no dialer load-threshold

Syntax Description

load	Interface load used to determine whether to initiate another call or to drop a link to the destination. This argument represents a utilization percentage; it is a number between 1 and 255, where 255 is 100 percent.
outbound	(Optional) Calculates the actual load using outbound data only.
inbound	(Optional) Calculates the actual load using inbound data only.
either	(Optional) Sets the maximum calculated load as the larger of the outbound and inbound loads.

Command Default

No maximum load is predefined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When the cumulative load of all UP links (a number *n*) exceeds the load threshold the dialer adds an extra link and when the cumulative load of all UP links minus one (*n* - 1) is at or below load threshold then the dialer can bring down that one link. The dialer will make additional calls or drop links as necessary but will never interrupt an existing call to another destination.

The *load* argument is the calculated weighted average load value for the interface; 1 is unloaded and 255 is fully loaded. The load is calculated by the system dynamically, based on bandwidth. You can set the bandwidth for an interface in kilobits per second, using the **bandwidth** command.

The load calculation determines how much of the total bandwidth you are using. A *load* value of 255 means that you are using one hundred percent of the bandwidth. The load number is required.

See the description of the **bandwidth** command earlier in this guide for more information.

When multilink PPP is configured, the **dialer load-threshold 1** command no longer keeps a multilink bundle of *n* links connected indefinitely and the **dialer-load threshold 2** command no longer keeps a multilink bundle of 2 links connected indefinitely. If you want a multilink bundle to be connected indefinitely, you must set a high idle timer or make all traffic interesting.

When two connected routers are configured to dial out, only one router should have the **dialer max-call** or **dialer pool-member max-links** command configured. Otherwise, if both routers dial simultaneously, each will reject the incoming call when it exceeds the setting for the **max-links** argument. If the

maximum number of calls configured is one and dialing out is synchronized, no connection will come up or it will take many retries before the connection stays up. To prevent this problem, one of the following configurations is recommended:

- Use the **dialer max-call** command to restrict the number of connections, rather than the **dialer pool-member max-links** command. The result is the same and the **dialer max-call** command is easier to understand and configure.
- When two systems will dial each other and a maximum of one link is desired, configure the **dialer max-calls** command on only one side of the connection, not on both sides.
- Configure the **dialer load-threshold** command on only one side of the connection, either the local or remote router, and configure the **dialer max-call** command on the interface where the **dialer load-threshold** command is configured.

Note Dial-on-demand (DDR) load balancing does not forward packets correctly when the system dials out via the **dialer load-threshold** command and more than one remote device is connected by either dial-out or dial-in. This problem typically occurs on a PRI with **dialer load-threshold** configured, but it may also occur on BRI or multiple DDR interfaces in a dialer rotary group when more than one remote device is connected. As a workaround, remove the **dialer load-threshold** command.

Examples

In the following example, if the load to a particular destination on an interface in dialer rotary group 5 exceeds interface load 200, the dialer will initiate another call to the destination:

```
interface dialer 5
 dialer load-threshold 200
```

Related Commands

Command	Description
bandwidth	Specifies the maximum aggregate bandwidth for H.323 traffic.
busyout	Creates a “host-failed” message that displays when a connection fails.
dialer max-call	Specifies the maximum number of calls to a remote destination that can be up at any one time for a dialer profile.
dialer pool-member max-links	Configures a physical interface to be a member of a dialer profile dialing pool.
dialer reserved-links	Includes a specified interface in a dialer rotary group.
interface dialer	Defines a dialer rotary group.

dialer map

To configure a serial or ISDN interface to call multiple sites or to receive calls from multiple sites, use the **dialer map** command in interface configuration mode. Several options for using this command are possible; see the following description and the "Examples" section. To delete a particular dialer map entry, use the **no** form of this command.

Complete Syntax

dialer map *protocol-keyword protocol-next-hop-address* [**broadcast** | **class** *dialer-map-class-name* | **modem-script** *modem-regular-expression* | **vrf** *vrf-name* | **name** *host-name* | **spc** | **speed 56** | **speed 64** | **system-script** *system-regular-expression* | *dial-string*[**:***isdn-subaddress*]]

no dialer map *protocol-keyword protocol-next-hop-address* [**broadcast** | **class** *dialer-map-class-name* | **modem-script** *modem-regular-expression* | **vrf** *vrf-name* | **name** *host-name* | **spc** | **speed 56** | **speed 64** | **system-script** *system-regular-expression* | *dial-string*[**:***isdn-subaddress*]]

Dialer Map for an Asynchronous Interface

To configure an asynchronous interface to place a call to a single site that requires a system script or that has no assigned modem script, or to multiple sites on a single line, on multiple lines, or on a dialer rotary group, use the following form of the **dialer map** interface configuration command:

dialer map *protocol-keyword protocol-next-hop-address* [**name** *host-name*] [**broadcast**] [**modem-script** *modem-regular-expression*] [**system-script** *system-regular-expression*] [*dial-string*]

no dialer map *protocol-keyword protocol-next-hop-address* [**name** *host-name*] [**broadcast**] [**modem-script** *modem-regular-expression*] [**system-script** *system-regular-expression*] [*dial-string*]

Dialer Map for ISDN Interface and ISDN AOC Short-Hold Idle Timeout

To configure an ISDN interface to place a call to multiple sites, to authenticate calls from multiple sites, and to identify the class name that configures the ISDN Advice of Charge (AOC) short-hold idle timeout, use the following form of the **dialer map** interface configuration command:

dialer map *protocol-keyword protocol-next-hop-address* [**name** *host-name*] [**speed 56** | **speed 64**] [**broadcast**] **class** *dialer-map-class-name* [*dial-string*[**:***isdn-subaddress*]]

no dialer map *protocol-keyword protocol-next-hop-address* [**name** *host-name*] [**speed 56** | **speed 64**] [**broadcast**] **class** *dialer-map-class-name* [*dial-string*[**:***isdn-subaddress*]]

Dialer Map for German and Australian SPC

The following command syntax is used only in Germany for circuits between an ISDN BRI and a 1TR6 ISDN switch, and in Australia for circuits between an ISDN PRI and a TS-014 switch. To set up network addressing on an ISDN BRI interface to support semipermanent connection between customer equipment and the exchange, use the following form of the **dialer map** interface configuration command:

dialer map *protocol-keyword protocol-next-hop-address* [**name** *host-name*] [**spc**] [**speed 56** | **speed 64**] [**broadcast**] *dial-string*[**:***isdn-subaddress*]

no dialer map *protocol-keyword protocol-next-hop-address* [**name** *host-name*] [**spc**] [**speed 56** | **speed 64**] [**broadcast**] *dial-string*[**:***isdn-subaddress*]]

Dialer Map for MPLS VPN

To configure a serial or ISDN interface to support an IP-based VPN routing and forwarding instance (VFR)-aware dialer map for a Multiprotocol Label Switching (MPLS) VPN, use the following form of the **dialer map** interface configuration command:

dialer map ip *protocol-next-hop-address* **vrf** *vrf-name* **name** *host-name dial-string*

no dialer map ip *protocol-next-hop-address* **vrf** *vrf-name* **name** *host-name dial-string*

Dialer Map for Bridging

To configure a serial or ISDN interface to support bridging, use the following form of the **dialer map** interface configuration command:

dialer map bridge [**name** *host-name*] [**broadcast**] [*dial-string*[**:***isdn-subaddress*]]

no dialer map bridge [**name** *host-name*] [**broadcast**] [*dial-string*[**:***isdn-subaddress*]]

Syntax Description

protocol-keyword protocol-next-hop-address	Enter one of the protocol keywords listed followed by an appropriate address (for example, the **clns** keyword is followed by a network service access point, or NSAP, address): • **appletalk**—AppleTalk • **bridge**—Bridging (no address is required) • **clns**—Cisco IOS Connectionless Network Service (CLNS) • **decnet**—DECnet • **hpr**—High Performance Routing • **ip**—IP • **ipx**—Internetwork Packet Exchange • **llc2**—Logical Link Control, type 2 • **netbios**—NetBIOS • **pppoe**—PPP over Ethernet • **snapshot**—Snapshot routing protocol; refer to the **dialer map snapshot** command description for use of this keyword
broadcast	(Optional) Forwards broadcasts to the address specified with the *protocol-next-hop-address* argument.
class *dialer-map-class-name*	(Optional) Dialer map class name.
modem-script *modem-regular-expression*	(Optional) Modem script name to be used for the connection (asynchronous interfaces only).
vrf *vrf-name*	(Optional) VPN routing/forwarding instance (VRF) for use with a VRF-aware dialer map in an MPLS VPN. Provide a dial string after the VRF name.

name *host-name*	(Optional) The remote system with which the local router or access server communicates. Used for authenticating the remote system on incoming calls. The *host-name* argument is a case-sensitive name or ID of the remote device. For routers with ISDN interfaces, if calling line identification—sometimes called CLI, but also known as caller ID and automatic number identification (ANI)—is provided, the *host-name* argument can contain the number that the calling line ID provides.
spc	(Optional) Semipermanent connection between customer equipment and the exchange; used only in Germany for circuits between an ISDN BRI and a 1TR6 ISDN switch and in Australia for circuits between an ISDN PRI and a TS-014 switch.
speed 56 | **speed 64**	(Optional) Keyword and value indicating the line speed in kbps to use. Used for ISDN only. The default speed is **speed 64 (**64 kbps).
system-script *system-regular-expression*	(Optional) System script name to be used for the connection (asynchronous interfaces only).
dial-string[**:***isdn-subaddress*]	(Optional) Dial string (telephone number) sent to the dialing device when it recognizes packets with the specified address that matches the configured access lists, and the optional subaddress number used for ISDN multipoint connections (colon required for separating numbers). The dial string and ISDN subaddress, when used, must be the last item in the command line.

Command Default

For all forms of the command, no dialer map is configured. The default speed is 64 kbps. No scripts are defined for placing calls.

Command Modes

Interface configuration

Command History

Release	Modification
9.1	This command was introduced for synchronous serial interfaces using V.25*bis* dialing.
10.0	This command was enhanced to support asynchronous and ISDN interfaces.
11.3	This command was enhanced to support ISDN AOC.
12.2(8)T	The **vrf** *vrf-name* keyword and argument were added.
12.2(13)T	The **vines** and **xns** arguments were removed because Banyan Systems' Virtual Integrated Network Service (VINES) and the Xerox Network System (XNS) are no longer available in Cisco IOS software.

Usage Guidelines

Usage Guidelines for Asynchronous Interfaces

Configure a **dialer map** command for each remote destination for an asynchronous interface. Specify chat scripts for a physical interface that is not part of a dialer rotary group when no chat script is specified for the line, or when a system chat script is required to log in to the remote system. However, you need *not* specify a system script under the following conditions:

- The modem script can be used to dial in and log in to the remote system.
- You are calling a system that does not require a login script—that is, a system that answers and immediately goes into protocol mode.

If you adhere to the chat script naming convention suggested in the description of the **chat-script** command, use the form **modem-script** **modulation-type* in the **dialer map** command; for example, *-v32*bis*. This form allows you to specify the modulation type that is best for the system you are calling, and allows the modem type for the line to be specified by the **script dialer** command.

The period (.) is a wildcard that matches any character, and the asterisk (*) indicates that the preceding character can be duplicated multiple times. For more information about regular expressions, refer to the "Regular Expressions" appendix in the *Cisco IOS Dial Technologies Configuration Guide*.

If a modem script is specified in the **dialer map** interface configuration command and a modem script is specified in the **script dialer** line configuration command, the first chat script that matches both is used. If no script matches both, an error message is logged and the connection is not established. If there is no modem chat script specified for the line, the first chat script (that is, the one specified in the **chat-script** global configuration command) that matches the regular expression of the modem script is used. If there is a system script specified in the **dialer map** interface configuration command, the first chat script to match the regular expression is used.

The **modem-script** and **system-script** keywords and corresponding arguments are optional. They are ignored on synchronous interfaces.

If you have named your chat script according to the type of modem and modulation (for example, codex-v32 or telebit v32), your regular expression could be **codex-.*** in the **script dialer** line configuration command, and ***-v32bis** in the modem script specified in the **dialer map** command for a system to which you want to connect using V.32*bis* modulation.

The modem lines (specified by the *regular-expression* argument in the **script dialer** line configuration command) would be set to one of the following regular expressions to match patterns, depending on the kind of modem you have:

- **codex-.***
- **telebit-.***
- **usr-.***

Usage Guidelines for Synchronous Interfaces

Use the **dialer map** command with the **name** keyword but without the dial string in configurations in which remote sites are calling a central site, but the central site is not calling the remote site. With this command, the local device will authenticate the remote site using Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP), which will send the remote site's host name to the central site. The central site will then use this name to authenticate the caller, and will use the next hop address to send packets to the remote site. Because no dialer string is specified, the central site cannot call the remote router.

Usage Guidelines for ISDN Interfaces and ISDN AOC

Use the **dialer map** command with the **name** keyword in configurations in which remote sites are calling a central site, but the central site is not calling the remote site. With this command, the local device will authenticate the remote site using CHAP or PAP, which will send the remote site host name to the central site. The central site will then use this name to authenticate the caller, and will use the next hop address to send packets to the remote site. Because no dialer string is specified, the central site cannot call the remote router.

For ISDN interfaces only, you can specify an optional speed parameter for **dialer map** commands if you also specify a dial string. This option informs the ISDN software whether it should place a call at 56 or 64 kbps. If you omit the ISDN speed parameter, the default is 64 kbps.

For routers with ISDN interfaces, if CLI is provided, the *host-name* field may contain the number that calling line ID provides.

When the network provides ISDN AOC information, use the **dialer map** command with the **class** keyword for outgoing calls. Use the **map-class dialer** global command to identify the class name, the **dialer idle-timeout** command to define a static idle timeout period for outgoing calls to the class, and the **dialer isdn short-hold** command to define the minimum idle time to wait before disconnecting calls at the end of the charging period.

Usage Guidelines for MPLS VPN

Beginning with Cisco IOS Release 12.2(8)T, dialer software became capable of being "VRF-aware for MPLS VPN," meaning that it can distinguish between two destinations with the same IP address using information stored in a VRF. When the **dialer map** command is configured with the **vrf** keyword in an MPLS VPN, the dialer software looks up a map for the next hop address using the next hop address and the VRF name configured. Once dial-out takes place and authentication is complete, a virtual profile interface is created. The VRF is installed on the virtual profile interface using the following per-user authentication, authorization, and accounting (AAA) interface command:

cisco-avpair "lcp:interface-config=ip vrf forwarding vrf-name"

Data transfer occurs as defined by the virtual profile dialer. When an IP route for a particular VRF points to the dialer (configured using the **ip route** global configuration command), the dialer uses the VFR-aware dialer map to get the dial string and IP address, and to bring up the connection. Once the user is authenticated, a virtual access interface is created and the user details are downloaded from the AAA server, and finally, the appropriate IP VRF command is applied on the virtual access interface.

Examples

Asynchronous Interface Examples

The following example sets the dialer speed at 56 kbps to call a remote site at 172.19.2.5:

```
interface async 1
encapsulation ppp
ppp authentication chap
dialer map ip 172.19.2.5 speed 56
```

The following example shows a dialing chat script and a login chat script. The **dialer in-band** command enables dial-on-demand routing (DDR) on asynchronous interface 10, and the **dialer map** command looks for the specified dialing and the login scripts, then uses those scripts to dial the string 95550190.

```
chat-script dial ABORT ERROR "" "AT Z" OK "ATDT \T" TIMEOUT 30 CONNECT \c
chat-script login ABORT invalid TIMEOUT 15 name: billw word: wewpass ">" "slip default"
interface async 10
dialer in-band
dialer map ip 10.55.0.1 modem-script dial system-script login 95550190
```

In the following example, the remote site is calling the central site, and the central site is calling the remote site. The central router uses the name ZZZ to authenticate the remote router when connection is made, and uses the dialer string 14155550134 to call the remote router if it is not currently connected.

```
interface async 1
dialer map ip 172.19.2.5 name ZZZ 14155550134
```

In the following example, a remote site is calling a central site, but the central site is not calling the remote site. The local device will authenticate the site that is calling in using CHAP. CHAP causes the remote site name, YYY, to be sent to the site it is calling. The central site will then use this name to authenticate the remote site.

```
interface async 1
  encapsulation ppp
  ppp authentication chap
  dialer map ip 172.19.2.5 name YYY
```

ISDN AOC Short-Hold Idle Timeout Example

In the following legacy DDR example, a BRI interface is configured with dialer map classes to use for outgoing calls, and a dialer idle timeout period to use for all incoming calls. All of the map classes are configured with dialer idle timeout periods that override the interface static dialer idle timeout for outgoing calls. Two map classes are also configured for an ISDN AOC short-hold idle timeout.

```
hostname A
!
username IA password 7 1533121F0725
username IB password 7 110A1016262D29
username IC password 7 1533121F072508
isdn switch-type basic-net3
!
interface bri 0
 ip address 10.0.0.35 255.0.0.0
 encapsulation ppp
 dialer idle-timeout 150
 dialer map ip 10.0.0.33 name IA class One 06966600050
 dialer map ip 10.0.0.40 name IB class Two 778578
 dialer map ip 10.0.0.45 name IC class Three 778579
 ppp authentication chap
!
map-class dialer Three
 dialer idle-timeout 300
 dialer isdn short-hold 10
!
map-class dialer One
 dialer idle-timeout 300
!
map-class dialer Two
 dialer idle-timeout 300
 dialer isdn short-hold 10
```

SPC Example

The following example configures the interface for semipermanent connections in Germany; the IP address and the phone number are provided:

```
dialer map ip 192.168.48.2 spc 49305550155:3789
```

MPLS VPN Example

In the following partial example, the number to be dialed is based on the VRF name and destination IP address configured. The VRF is identified based on the incoming interface of the packet, and is used with the destination IP address to determine the number to be dialed, as defined in the **dialer map** command.

```
virtual-profile virtual-template 1
virtual-profile aaa
!
interface virtual-template 1
 ip unnumbered loopback0
 ppp authentication chap
 ppp multilink
.
.
.
interface dialer 1
 dialer map ip 10.9.9.9 vrf new_vrf name new_name 5550145
 dialer map ip 10.9.9.9 vrf branch_vrf name branch_name 5550156
 ppp authentication chap
 ppp multilink
.
.
.
ip route vrf vrfgreen_vrf 10.9.9.9 255.255.255.255 dialer1
ip route vrf vrfyellow_vrf 10.9.9.9 255.255.255.255 dialer1
```

Related Commands

Command	Description
chat-script	Places calls over a modem and logs in to remote systems.
dialer idle-timeout (map-class)	Specifies the fast idle timer value to use when placing a call to any telephone number associated with a specified class.
dialer isdn short-hold	Configures the router to disconnect a call at the end of the current charging period if the line has been idle for at least the specified minimum period.
dialer map snapshot	Defines a dialer map for the snapshot routing protocol on a client router connected to a DDR interface.
ip route	Establishes static IP routes, and pairs an IP address with a VRF-aware dialer map.
map-class dialer	Defines a class of shared configuration parameters associated with the **dialer map** command for outgoing calls from an ISDN interface and for PPP callback.
ppp bap call	Sets PPP BACP call parameters.
virtual-profile aaa	Enables virtual profiles by AAA configuration.

dialer map snapshot

To define a dialer map for Cisco's snapshot routing protocol on a client router connected to a dial-on-demand routing (DDR) interface, use the **dialer map snapshot** command in interface configuration mode. To delete one or more previously defined snapshot routing dialer maps, use the **no** form of this command.

dialer map snapshot *sequence-number dial-string*

no dialer map snapshot [*sequence-number*]

Syntax Description

sequence-number	A number in the range from 1 to 254, inclusive, that uniquely identifies a dialer map. (Optional for the **no** form.)
dial-string	Telephone number of a remote snapshot server to be called during an active period.

Command Default

No snapshot routing dialer map is defined.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

Enter a command for each remote snapshot server router the client router should call during an active period.

Use the **no dialer map snapshot** form of this command to remove all previously defined snapshot dialer maps on the client router; use the **no dialer map snapshot** *sequence-number* form of this command to delete a specified dialer map.

Examples

The following examples define snapshot dialer maps on a client router:

```
dialer map snapshot 12 4155550134
dialer map snapshot 13 4155550145
```

The following example removes one of the previously defined snapshot routing dialer maps on the client router:

```
no dialer map snapshot 13
```

Related Commands

Command	Description
dialer reserved-links	Includes a specified interface in a dialer rotary group.
interface dialer	Defines a dialer rotary group.
snapshot client	Configures a client router for snapshot routing.

dialer max-call

To specify the maximum number of calls to a remote destination that can be up at any one time for a dialer profile, use the **dialer max-call** command in interface configuration mode.

dialer max-call *number*

Syntax Description

number	Maximum number of calls, ranging from 1 to 4096.

Command Default

No maximum number of calls is specified.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The **dialer max-call** command is used to specify the maximum number of calls for the dialer interface. This command applies to dialer interfaces only.

This command can be configured only if a dialer profile is enabled using the **dialer pool** command. The **dialer max-call** command cannot be used with legacy dial-on-demand routing (DDR).

When two connected routers are configured to dial out, only one router should have the **dialer max-call** or **dialer pool-member max-links** command configured. Otherwise, if both routers dial simultaneously, each will reject the incoming call when it exceeds the setting for the **max-links** argument. If the maximum number of calls configured is one and dialing out is synchronized, no connection will come up or it will take many retries before the connection stays up. To prevent this problem, one of the following configurations is recommended:

- Use the **dialer max-call** command to restrict the number of connections, rather than the **dialer pool-member max-links** command. The result is the same and the **dialer max-call** command is easier to understand and configure.
- When two systems will dial each other and a maximum of one link is desired, configure the **dialer max-calls** command on only one side of the connection, not on both sides.
- Configure the **dialer load-threshold** command on only one side of the connection, either the local or remote router, and configure the **dialer max-call** command on the interface where the **dialer load-threshold** command is configured.

Examples

The following example sets a maximum of six calls:

```
dialer max-call 6
```

Related Commands

Command	Description
dialer isdn	Specifies the bit rate used on the B channel associated with a specified map class and specifies whether to set up semipermanent connections for this map class.
dialer load-threshold	Configures bandwidth on demand by setting the maximum load before the dialer places another call to a destination.
dialer pool	Specifies, for a dialer interface, which dialing pool to use to connect to a specific destination subnetwork.
dialer pool-member max-links	Configures a physical interface to be a member of a dialer profile dialing pool.
dialer wait-for-carrier-time (map-class)	Specifies the length of time to wait for a carrier when dialing out to the dial string associated with a specified map class.

dialer order

To specify the dialing order when multiple dial strings are configured, use the **dialer order** command in interface configuration mode. To change or remove the dialing order, use the **no** form of this command.

dialer order [**sequential** | **round-robin** | **last-successful**]

no dialer order [**sequential** | **round-robin** | **last-successful**]

Syntax Description

sequential	(Optional) Always starts dialing the first dial string configured in a list of multiple strings, and continues to the next dial string when a call fails. This keyword allows dial string order to be prioritized, and is the default.
round-robin	(Optional) Always starts dialing using the dial string that follows the most recently used dial string. If no calls have previously been made, the dialer uses the first dial string. When a call fails, the dialer tries the next dial string until all dial strings have been tried. This keyword allows calls to be shared equally among the configured dial strings. However, if the dial strings are associated with multiple ISDN B channels on the same remote device, a call may be placed to bring up a second B channel without trying to call the number associated with the first B channel.
last-successful	(Optional) Always starts dialing using the most recently successful dial string, and continues to the next dial string in a list when a call fails. This keyword reduces the time needed to find a dial string that successfully completes a call when the dial strings are not likely to be equally successful.

Command Default

Dial order is sequential.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

The **dialer order** command keywords can be configured on a per-interface basis. The configuration rules are as follows:

- The keyword you configure applies to dial strings configured on an interface by the **dialer map** and **dialer string** configuration commands.
- The keyword you configure for a dialer interface is effective for all destinations defined by that interface.

You can use the **dialer order** command in configurations that apply to both legacy dialers and dialer profiles. The command is also compatible with the following dialer features and protocols:

- Dialer redial
- Dialer Watch feature

- Dialer Persistent feature
- Bandwidth Allocation Control Protocol (BACP)
- Bandwidth on demand
- Multilink PPP

Examples

The following legacy dialer configuration shows how to set the dialing software to try the telephone number of the last successful call when starting a new call, rather than the first telephone number in the list (555-0104):

```
interface Serial0/0
 ip address 10.2.1.130 255.255.255.0
 encapsulation ppp
 dialer in-band
 dialer map ip 10.2.1.131 name mymap1 modem-script scr-3 5550104
 dialer map ip 10.2.1.131 name mymap1 modem-script scr-3 5550105
 dialer map ip 10.2.1.131 name mymap1 modem-script scr-3 5550106
 dialer-group 1
 dialer order last-successful
```

If in a previous attempt to dial network 10.2.1.131 the telephone number 555-0106 was successful, because the dial order is set to **last-successful**, the next attempt to dial network 10.2.1.131 will start again with the 555-0106 telephone number.

The following dialer profile configuration shows how to set the dialing software to try the telephone number that occurs after the most recently used dial string when starting a new call, rather than the first telephone number in the list (0104):

```
interface Dialer0
 ip address 10.1.1.130 255.255.255.0
 encapsulation ppp
 dialer pool 1
 dialer string 0104
 dialer string 0105
 dialer string 0106
 dialer string 0107
 dialer-group 1
 dialer order round-robin
```

If in a previous attempt to dial network 10.1.1.130 the telephone number 0106 was successful, because the dial order is set to **round-robin**, the next attempt to dial network 10.1.1.130 will start with the 0107 telephone number.

Related Commands

Command	Description
dialer map	Configures a serial interface or ISDN interface to call one or multiple sites, or to receive calls from multiple sites.
dialer string	Specifies the string (telephone number) to be used when placing a call from an interface.

dialer outgoing

To configure the dialer map class for a Network Specific Facilities (NSF) dialing plan to support outgoing calls, use the **dialer outgoing** command in map-class dialer configuration mode.

dialer outgoing *class-name*

Syntax Description

class-name	Keyword for a specified AT&T Primary-4ESS NSF dialing plan. The following keywords are supported: **sdn**, **megacomm**, and **accunet**.

Command Default

This command is disabled; no class name is provided.

Command Modes

Map-class dialer configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Use this command only to define a dialer map class for an NSF call-by-call service offered by AT&T on Primary-4ESS ISDN switches. This command is not used for other vendors and switch types.

Examples

The following partial example shows a class called sdn to support the Software Defined Network (SDN) dialing plan. For a more complete example using all the related commands, see the **map-class dialer** command.

```
dialer outgoing sdn
```

Related Commands

Command	Description
dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites.
dialer voice-call	Configures the dialer map class for an NSF dialing plan to support outgoing voice calls.
isdn nsf-service	Configures NSF on an ISDN PRI for outgoing calls configured as voice calls.
map-class dialer	Defines a class of shared configuration parameters associated with the dialer map command for outgoing calls from an ISDN interface and for PPP callback.

dialer persistent

To force a dialer interface to be connected at all times, even in the absence of interesting traffic, use the **dialer persistent** command in interface configuration mode. To disable this option, use the **no** form of this command.

dialer persistent [**delay** [**initial**] *seconds* | **max-attempts** *number*]

no dialer persistent

Syntax Description

delay	(Optional) Sets the delay before an attempt to reestablish a persistent connection after a network error has disrupted it.
initial	(Optional) Sets the delay before a persistent connection is established, after configuration or boot-up, in the absence of interesting traffic.
seconds	(Optional) Sets the time, in seconds, for the delay or initial delay set by the **delay** and **initial** keywords. Default is 1 second.
max-attempts *number*	(Optional) Maximum number of attempts for reconnecting after a network error has disrupted the persistent connection. There is no default or limit to the number of attempts.

Command Default

No persistent connections are established. The default delay and initial delay interval is 1 second. There is no default or limit to the number of reconnection attempts.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)T	This feature was implemented on Cisco access server platforms.

Usage Guidelines

Do not use the **dialer redial** command when a dialer profile has been configured with the **dialer persistent** command. Both these configuration commands prompt the router to dial out, so it is desirable to configure only one of them.

Do not use the **dialer idle-timeout** interface configuration command when a dialer profile has been configured with the **dialer persistent** command. Doing so has no effect on the idle timer, which is overridden by the **dialer idle-timeout** command as **dialer idle-timeout 0**.

You can use the **clear interface** EXEC command on the dialer interface to clear unsuccessful dial attempts on a line without interesting traffic; the dialer software continues attempting to bring up the connection as persistent. To disconnect a persistent connection and prevent the software from attempting more dialing, use the **shutdown** interface configuration command.

Once a connection has been brought up as persistent, it cannot be torn down due to a fast-idle timeout.

Examples

The following example shows how to configure a dialer interface for dialer persistent:

```
!
interface dialer 0
 ip address 10.1.1.2 255.255.255.0
 encapsulation ppp
 dialer string 5550189
 dialer pool 1
 dialer-group 1
 dialer persistent delay initial 20
  !
 access-list 101 permit icmp any any
 access-list 101 deny   ip any any
 dialer-list 1 protocol ip list 101
```

Related Commands

Command	Description
dialer-group	Controls access by configuring an interface to belong to a specific dialing group.
dialer-list protocol	Defines a DDR dialer list to control dialing by protocol or by a combination of a protocol and a previously defined access list.
dialer pool	Specifies for a dialer interface which dialing pool to use to connect to a specific destination subnetwork.
dialer redial	Configures redial after failed outbound dial attempts.
dialer string (dialer profiles)	Specifies the string (telephone number) to be used when placing a call from an interface.

dialer pool

To specify, for a dialer interface, which dialing pool to use to connect to a specific destination subnetwork, use the **dialer pool** command in interface configuration mode. To remove the dialing pool assignment, use the **no** form of this command.

dialer pool *number*

no dialer pool *number*

Syntax Description

number	Dialing pool number, in the range 1 through 255.

Command Default

Disabled; no default number is specified.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

This command applies to dialer interfaces only.

Examples

The following example shows a dialer interface configuration that is linked to the physical interface configuration shown for BRI 1 in the **dialer pool-member** command section. Dialer interface 1 uses dialer pool 3, of which BRI 1 is a member.

```
! This is a dialer profile for reaching remote subnetwork 10.1.1.1.
interface Dialer1
 ip address 10.1.1.1 255.255.255.0
 encapsulation ppp
 dialer remote-name Smalluser
 dialer string 4540
 dialer pool 3
 dialer-group 1
```

The following example might accompany the previous dialer profile configuration example. Physical interface BRI 1 has a reserved channel in dialer pool 3. That channel is inactive until BRI 1 uses it to place calls.

```
interface BRI1
 encapsulation ppp
 dialer pool-member 1 priority 50
 dialer pool-member 2 priority 50
! BRI 1 has a reserved channel in dialer pool 3; the channel remains inactive
! until BRI 1 uses it to place calls.
 dialer pool-member 3 min-link 1
 ppp authentication chap
```

Related Commands

Command	Description
dialer pool-member	Configures a physical interface to be a member of a dialer profiles dialing pool.
dialer wait-for-carrier-time (map-class)	Specifies the length of time to wait for a carrier when dialing out to the dial string associated with a specified map class.

dialer pool-member

To configure a physical interface to be a member of a dialer profile dialing pool, use the **dialer pool-member** command in interface configuration mode. To remove the configuration, use the **no** form of this command.

dialer pool-member *number* [**priority** *priority*] [**min-link** *minimum*] [**max-link** *maximum*]

no dialer pool-member *number*

Syntax Description

number	Dialing pool number. Range is from 1 to 255.
priority *priority*	(Optional) Specifies the priority of this interface within the dialing pool. • Range is from 1 (lowest) to 255 (highest). The default is 1. • Interfaces with the highest priority are selected first for dialing out.
min-link *minimum*	(Optional) Specifies the minimum number of B channels on the interface that are reserved for the dialing pool. • Range is from 1 to 255. The default minimum is 1. • A reserved channel is inactive until the specified interface uses it to place calls. This option applies to ISDN outgoing interfaces only.
max-link *maximum*	(Optional) Specifies the maximum number of B channels on the interface that can be used by the dialing pool. • Range is from 1 to 255. The default maximum is 255. • This option applies to ISDN interfaces only, and can be configured on both incoming and outgoing calls.

Command Default

The interface is not a member of a dialer profile dialing pool.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12(33)SRE	This command was modified. Support for SR releases was removed.

Usage Guidelines

This command applies to asynchronous serial, synchronous serial, BRI, and PRI physical interfaces only. It does not apply to the dialer interfaces.

The common number used in the **dialer pool** command and in the **dialer pool-member** command links the physical interface and dialer interface configurations.

The **min-link** keyword and value are used primarily for dial backup.

The Cisco IOS software provides the **dialer max-links** command in interface configuration mode and the **max-link** keyword with the **dialer pool-member** command to specify a maximum number of links. When two linked systems are configured to dial out, only one system needs to have the maximum number of links configured. Otherwise, if both systems dial simultaneously, each will reject the incoming call when it exceeds the specified maximum links. If the maximum number of links is configured to 1 and the dialing out is synchronized, no connection will come up or many retries will be required before a connection stays up. Some suggestions for correcting this behavior are as follows:

- Use only the **dialer max-links** command to restrict the number of connections. The result is the same as configuring the **dialer pool-member** command with the **max-link** keyword.
- If two systems will dial each other and only one link is desired, configure the **dialer max-links** command on just one system.
- Configure the **dialer load-threshold** command on only one side, either local or remote, and configure the **dialer max-links** command on the interface where the **dialer load-threshold** command was configured.

Note Cisco IOS Release 12.2(33)SRE and later releases do not support the **dialer pool-member** command.

Examples

The following example shows that only one channel is available for incoming calls and 22 channels are reserved for outgoing calls for a 23-channel ISDN PRI T1 interface:

```
dialer pool-member 1 min-link 22 max-link 23
```

The following sample output from the **debug dialer** EXEC command indicates that once one incoming call has been received, the next incoming call is denied:

```
Incoming call id 0x3 rejected, exceeded max calls
.
.
.
Incoming call id 0x3 rejected, exceeded
```

The following example reserves 19 channels for an incoming call on a 23-channel ISDN PRI T1 interface:

```
dialer pool-member 1 min-link 5 max-link 24
```

The following example shows the configuration of one ISDN BRI interface to be a member of dialer pool 2 with priority 100:

```
interface BRI2
 encapsulation ppp
 dialer pool-member 2 priority 100
 ppp authentication chap
```

In the following example, BRI physical interface configuration BRI 1 has one reserved channel in dialer pool 3. That channel is inactive until BRI 1 uses it to place calls.

```
interface BRI1
 encapsulation ppp
 dialer pool-member 1 priority 50
 dialer pool-member 2 priority 50
 !BRI 1 has a reserved channel in dialer pool 3; the channel remains inactive
 !until BRI 1 uses it to place calls.
 dialer pool-member 3 min-link 1
 ppp authentication chap
```

Related Commands

Command	Description
dialer load-threshold	Configures bandwidth on demand by setting the maximum load before the dialer places another call to a destination.
dialer pool	Specifies for a dialer interface which dialing pool to use to connect to a specific destination subnetwork.

dialer pre-classify

To force IP Security (IPSec) to check an interesting packet against a dialer-list before enabling a dialer interface, use the **dialer pre-classify** command in crypto-map configuration mode.

dialer pre-classify

Syntax Description

This command has no arguments or keywords.

Command Modes

Crypto-map configuration mode (config-crypto-map)

Command History

Release	Modification
12.3(15)T	This command was introduced.

Usage Guidelines

Use the **crypto map isakmp-profile** command to enter crypto-map configuration mode and create an Internet Security Association and Key Management Protocol (ISAKMP) profile on a crypto map, prior to using the **dialer pre-classify** command.

Examples

The following example shows how to check a dialer-list prior to enabling a dialer interface, by using the **dialer pre-classify** command:

```
Router> enable
Router# configure terminal
Router(config)# crypto map map-name ipsec-isakmp profile isakmp-profile-name
Router(config-crypto-map)# dialer pre-classify
```

Related Commands

Command	Description
crypto map isakmp-profile	Configures an ISAKMP profile on a crypto map.

dialer priority

To set the priority of an interface in a dialer rotary group, use the **dialer priority** command in interface configuration mode. To revert to the default setting, use the **no** form of this command.

dialer priority *number*

no dialer priority

Syntax Description

number	Priority of an interface in a dialer rotary group; the highest number indicates the highest priority. This is a number from 0 through 255. The default value is 0, the lowest priority.

Command Default

No priority is predefined. When priority is defined, the default value is 0.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command is meaningful only for interfaces that are part of dialer rotary groups.

The value 0 indicates the lowest priority, and 255 indicates the highest priority. The **dialer priority** command controls which interfaces within a dialer rotary group will be used first. Higher priority interfaces (configured with higher *n* value) are used first.

The **dialer priority** command gives you the ability to tell the dialer rotary group which free interface (and, by extension for asynchronous interfaces, which modem) to use first. This command applies to outgoing calls only.

For example, a router or access server might have a selection of many modems, some of which are better performers than others. You might have a 19.2-kbps, two 4800-bps, three 1200-bps, and one 300-bps modem on interfaces in one dialer rotary group. You do not want the router or access server to make the call on the 300-baud modem if any of the faster modems are free. You want to use the highest-performance modems first, and the slowest modems last.

Examples

In the following example, asynchronous interface 3 will be used after interfaces with higher priority and before interfaces with lower priority:

```
interface async 3
 dialer priority 5
```

Related Commands

Command	Description
dialer reserved-links	Includes a specified interface in a dialer rotary group.
interface dialer	Defines a dialer rotary group.

dialer redial

To configure redial after failed outbound dial attempts, use the **dialer redial** command in interface configuration mode. To disable redial, use the **no** form of this command.

dialer redial interval *interval-time* **attempts** *redials* [**re-enable** *disable-time*]

no dialer redial

Syntax Description

interval *interval-time*	Time, in seconds, between redial attempts. The time can range from 5 to 2147483 seconds.
attempts *redials*	The maximum number of redial attempts to be performed. The number can range from 0 to 2147483.
re-enable *disable-time*	(Optional) Time, in seconds, for which the interface will be disabled if all redial attempts fail. The time can range from 5 to 2147483 seconds.

Command Default

Redial timer disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(2)	This command was introduced.
12.2(4)T	This command was modified to allow the following: • A disable time can be applied to a dialer profile interface and to a serial dialer. • The dialer can be configured to apply a disable timer without performing any redial attempts. • The dialer may select a different physical dialer on each redial attempt. • The dialer will cycle through all dialer strings or matching dialer maps on each redial attempt before applying the redial interval.

Usage Guidelines

Use this command to customize the number of redial attempts to be made, the interval between redial attempts, and the amount of time the interface will be disabled if all redial attempts fail. Setting **attempts 0** prevents redial attempts without inactivating the **re-enable** option. The **re-enable** option can be applied to both serial dialers and dialer profile interfaces.

When a logical dialer interface such as a dialer profile or a dialer rotary group is used, redial attempts may occur on a different physical dialer on each attempt. The physical dialer selection algorithm may be customized using the **dialer rotor** interface configuration command.

Do not use the **dialer redial** command when a dialer profile has been configured with the **dialer persistent** command. Both these configuration commands prompt the router to dial out, so it is desirable to configure only one of them.

Examples

The following example configures the dialer to make five redial attempts with an interval of 10 seconds between attempts. If all redial attempts fail, the interface will be disabled for 50 minutes.

```
dialer redial interval 10 attempts 5 re-enable 3000
```

Related Commands

Command	Description
debug dialer events	Displays debugging information about the packets received on a dialer interface.
dialer persistent	Forces a dialer interface to be connected at all times, even in the absence of interesting traffic.
dialer rotor	Specifies the method for identifying the outbound line to be used for ISDN or asynchronous DDR calls.

dialer remote-name

To specify the authentication name of the remote router on the destination subnetwork for a dialer interface, use the **dialer remote-name** command in interface configuration mode. To remove the specified name, use the **no** form of this command.

dialer remote-name *user-name*

no dialer remote-name

Syntax Description

user-name	Case-sensitive character string identifying the remote device; maximum length is 255 characters.

Command Default

No remote name is specified.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

This command applies only to dialer interfaces.

Only one remote name can be associated with a dialer interface at a time. You may change the name associated with the dialer interface by reissuing the **dialer remote-name** command. Issuing the **no dialer remote-name** command removes the remote name configuration.

When using Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) authentication, *user-name* is the name of the remote device that is authenticating.

Examples

The following partial example sets the name of the remote host to yourhost:

```
interface dialer 1
 dialer remote-name yourhost
```

Related Commands

Command	Description
ppp bap call	Sets PPP BACP call parameters.

dialer reserved-links

To reserve links for dial-in and dial-out, use the **dialer reserved-links** command in interface configuration mode. To clear the link, use the **no** form of this command.

dialer reserved-links {*dialin-link* | *dialout-link*}

no dialer reserved-links

Syntax Description

dialin-link	Link reserved for dial-in.
dialout-link	Link reserved for dial-out.

Command Default

By default, no links are reserved.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Examples

The following example sets dial in reserved links to 1 and dialout reserved links to 0 on the Dialer0 interface:

```
interface Dialer0
 dialer aaa
 dialer reserved-links 1 0
```

Related Commands

Command	Description
dialer congestion-threshold	Specifies congestion threshold in connected links.
sgbp dial-bids	Allows the stack group to bid for dialout connection.

dialer rotary-group

To include a specified interface in a dialer rotary group, use the **dialer rotary-group** command in interface configuration mode. To remove the specified interface, use the **no** form of this command.

dialer rotary-group *interface-number*

no dialer rotary-group *interface-number*

Syntax Description

interface-number	Number of the previously defined dialer interface in whose rotary group this interface is to be included. This is a number from 0 to 255. The dialer interface is defined by the **interface dialer** command.

Command Default

No interfaces are included in a dialer rotary group.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following example places asynchronous interfaces 1 and 2 into dialer rotary group 1, defined by the **interface dialer 1** command:

```
hostname central-site
! PPP encapsulation is enabled for interface dialer 1.
interface dialer 1
 encapsulation ppp
 dialer in-band
 ip address 172.18.2.1 255.255.255.0
 ip address 172.16.4.1 255.255.255.0 secondary
!
! The first dialer map command allows the central site and remote site YYY
! to call each other and allows the central site to authenticate site YYY
! when it calls in. The second dialer map command, with no dialer string,
! allows the central site to authenticate remote site ZZZ when it calls in, but
! the central site cannot call remote site ZZZ (no phone number).
 dialer map ip 172.18.2.5 name YYY 14155550134
 dialer map ip 172.16.4.5 name ZZZ
!
! The DTR pulse signals for three seconds on the interfaces in dialer
! group 1. This holds the DTR low so the modem can recognize that DTR has been
! dropped.
pulse-time 3
!
! Interfaces async 1 and async 2 are placed in dialer rotary group 1.
! All of the interface configuration commands (the encapsulation and dialer
! map commands shown earlier in this example) applied to interface
! dialer 1 apply to the physical interfaces assigned to the dialer group.
!
```

```
interface async 1
 dialer rotary-group 1
interface async 2
 dialer rotary-group 1
```

Related Commands

Command	Description
interface dialer	Defines a dialer rotary group.

dialer rotor

To specify the method for identifying the outbound line to be used for ISDN or asynchronous dial-on-demand routing (DDR) calls, use the **dialer rotor** command in interface configuration mode. To remove the specified method, use the **no** form of this command.

dialer rotor {**priority** | **best**}

no dialer rotor {**priority** | **best**}

Syntax Description

priority	Selects the first outbound line with the highest priority; this is the selection criterion that was previously used.
best	Selects the outbound line with the most recent success. If that line also has the most recent failure, then it will try the line with the least recent failure. If that line also has the most recent failure, it will then try an as-of-yet untried outbound line.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command allows the router to skip outbound ISDN BRI and asynchronous lines that have problems. This command would not be useful for ISDN PRI, unless your local telephone service provider has problems keeping your lines properly configured.

Examples

The following example configures a dialer interface to select the outbound line that most recently placed a successful call:

```
dialer rotor best
```

Related Commands

Command	Description
dialer priority	Sets the priority of an interface in a dialer rotary group.

dialer string

To specify the string (telephone number) to be called for interfaces calling a single site, use the **dialer string** command in interface configuration mode. To delete the dialer string specified for the interface, use the **no** form of this command.

dialer string *dial-string*[**:***isdn-subaddress*]

no dialer string

Syntax Description

dial-string	String of characters to be sent to a DCE device.
:*isdn-subaddress*	(Optional) ISDN subaddress.

Command Default

No strings are predefined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

To use this command on an asynchronous interface, you must define a modem chat script for the associated line by using the **script dialer** command. A script must be used to implement dialing.

Dialers configured as **in-band** pass the string to the external dialing device. Specify one **dialer string** command per interface.

To specify multiple strings, use the **dialer map** command. In general, you include a **dialer string** or **dialer map** command if you intend to use a specific interface to initiate a dial-on-demand routing (DDR) call.

Note If a **dialer string** command is specified without a **dialer-group** command with access lists defined, dialing is never initiated. If the **debug dialer** command is enabled, an error message is displayed indicating that dialing never will occur.

The string of characters specified for the *dial-string* argument is the default number used under the following conditions:

- A **dialer map** command is not included in the interface configuration.
- The next hop address specified in a packet is not included in any of the **dialer map** interface configuration commands recorded—assuming that the destination address passes any access lists specified for DDR with the **dialer-list** command.

ITU-T V.25*bis* Options

On synchronous interfaces, depending on the type of modem you are using, International Telecommunication Union Telecommunication (ITU-T) Standardization Sector V.25*bis* options might be supported as *dial-string* parameters of the **dialer string** command. Supported options are listed in Table 4. The functions of the parameters are nation specific, and they may have different implementations in your country. These options apply only if you have enabled DDR with the **dialer in-band** command. Refer to the operation manual for your modem for a list of supported options.

Note The ITU-T carries out the functions of the former Consultative Committee for International Telegraph and Telephone (CCITT).

Table 4 ITU-T V.25bis Options

Option	Description
:	Wait tone.
<	Pause. Usage and duration of this parameter vary by country.
=	Separator 3. For national use.
>	Separator 4. For national use.
P	Dialing to be continued in pulse mode. Optionally accepted parameter.
T	Tone. Dialing to be continued in Dual Tone Multifrequency (DTMF) mode. Optionally accepted parameter.
&	Flash. (The flash duration varies by country.) Optionally accepted parameter.

Examples

The following example specifies a dial-on-demand routing (DDR) telephone number to be tone-dialed on interface async 1 using the **dialer string** command:

```
interface async 1
 dialer string T14085550134
```

Related Commands

Command	Description
dialer-group	Controls access by configuring an interface to belong to a specific dialing group.
dialer in-band	Specifies that DDR is to be supported.
dialer-list protocol (Dial)	Defines a DDR dialer list to control dialing by protocol or by a combination of a protocol and a previously defined access list.
dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites.
script dialer	Specifies a default modem chat script.

dialer string (dialer profiles)

To specify the string (telephone number) to be used when placing a call from an interface, use the **dialer string** command in interface configuration mode. To delete the telephone number specified for the interface, use the **no** form of this command.

dialer string *dial-string* [**class** *class-name*]

no dialer string

Syntax Description

dial-string	Telephone number to be sent to a DCE device.
class *class-name*	(Optional) Dialer map class associated with this telephone number.

Command Default

No telephone numbers and class names are predefined.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

When you use dialer profiles for DDR, use the **dialer string class** form of this command to define a map class for a specific dialer profile.

Dialer profiles make it unnecessary to use dialer maps to configure DDR.

Note If a **dialer string** command is specified without a **dialer-group** command with access lists defined, dialing is never initiated. If the **debug dialer** command is enabled, an error message is displayed indicating that dialing never will occur.

Examples

The following example specifies that the dial string 4155550134 be used in calls to destinations defined by the map class myclass:

```
dialer string 4155550134 class myclass
```

Related Commands

Command	Description
dialer-group	Controls access by configuring an interface to belong to a specific dialing group.
dialer wait-for-carrier-time (map-class)	Specifies the length of time to wait for a carrier when dialing out to the dial string associated with a specified map class.
interface dialer	Defines a dialer rotary group.

dialer string (legacy DDR)

To specify the destination string (telephone number) to be called for interfaces calling a single site, use the **dialer string** command in interface configuration mode. To delete the dialer string specified for the interface, use the **no** form of this command.

dialer string *dial-string*[**:***isdn-subaddress*]

no dialer string

Syntax Description

dial-string	String of characters to be sent to a DCE device.
:*isdn-subaddress*	(Optional) ISDN subaddress preceded by a colon.

Command Default

No strings are predefined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

To use this command on an asynchronous interface, you must define a modem chat script for the associated line by using the **script dialer** command. A script must be used to implement dialing.

Dialers configured as **in-band** pass the string to the external dialing device. Specify one **dialer string** command per interface.

In general, you include a **dialer string** command if you intend to use a specific interface to initiate a dial-on-demand routing (DDR) call.

Note If a **dialer string** command is specified without a **dialer-group** command with access lists defined, dialing is never initiated. If the **debug dialer** command is enabled, an error message is displayed indicating that dialing never will occur.

The string of characters specified for the *dial-string* argument is the default number used under the following conditions:

- A **dialer map** command is not included in the interface configuration.
- The next hop address specified in a packet is not included in any of the **dialer map** command in interface configuration modes recorded—assuming that the destination address passes any access lists specified for DDR with the **dialer-list** command.

ITU-T V.25*bis* Options

On synchronous interfaces, depending on the type of modem you are using, International Telecommunication Union Telecommunication (ITU-T) Standardization Sector V.25*bis* options might be supported as *dial-string* parameters of the **dialer string** command. Supported options are listed in Table 4. The functions of the parameters are nation specific, and they may have different implementations in your country. These options apply only if you have enabled DDR with the **dialer in-band** command. Refer to the operation manual for your modem for a list of supported options.

Note The ITU-T carries out the functions of the former Consultative Committee for International Telegraph and Telephone (CCITT).

Examples

The following example specifies a DDR telephone number to be tone-dialed on asynchronous interface 1 using the **dialer string** command:

```
interface async 1
dialer string T14085550134
```

Related Commands

Command	Description
dialer-group	Controls access by configuring an interface to belong to a specific dialing group.
dialer in-band	Specifies that DDR is to be supported.
dialer-list protocol (Dial)	Defines a DDR dialer list to control dialing by protocol or by a combination of a protocol and a previously defined access list.
dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites.
script dialer	Specifies a default modem chat script.

dialer string trunkgroup

To specify a dial-out telephone number and dial-out trunk group name for a static configuration on a network access server (NAS), use the **dialer string trunkgoup** command in interface configuration mode. To delete the static, dial-out trunk group configuration, use the **no** form of this command.

dialer string *dial-string* **trunkgroup** *trunkgroup-label*

no dialer string *dial-string* **trunkgroup** *trunkgroup-label*

Syntax Description

dial-string	String of characters to be dialed.
trunkgroup-label	A predefined dial-out trunk group name.

Command Default

No trunk groups are defined.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

A **dialer string** command, in general, enables a specific interface for initiating a dial-on-demand routing (DDR) call.

The **dialer string trunkgroup** command enables use of a dial-out trunk group, which directs an outbound synchronous or asynchronous call to be initiated by DDR on a specific channel of an ISDN circuit. The channel (also called a digital service 0 or DS0 link), is a member of a defined dial-out trunk group. Individual DS0s from various signaling circuits can be aggregated into a dial-out trunk group.

The dial-out trunk group configured by the **dialer string trunkgroup** command must be part of a static configuration on an NAS. See the "Related Commands" section for commands that allow other nonstatic configurations of dial-out trunk groups.

Examples

The following example enables use of dial-out trunk group TG1 on dialer interface 0 as part of a static NAS configuration:

```
interface dialer 0
dialer string 5550112 trunkgroup TG1
```

Related Commands

Command	Description
cas-custom	Customizes signaling parameters for a particular E1 or T1 channel group on a channelized line.
ds0-group	Defines E1 channels for the CAS method by which the router connects to the PSTN.

Command	Description
pri-group timeslots	Specifies an ISDN PRI group on a channelized T1 or E1 controller.
show trunk group	Displays one or more trunk groups.
trunk-group timeslots	Directs an outbound synchronous or asynchronous call initiated by DDR to use specific DS0 channels of an ISDN circuit.

dialer voice-call

To configure the dialer map class for a Network Specific Facilities (NSF) dialing plan to support outgoing voice calls, use the **dialer voice-call** command in map-class dialer configuration mode.

dialer voice-call

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Map-class dialer configuration

Command History

Release	Modification
11.0	This command was introduced.

Examples

The following partial example defines a dialer map class to support the SDN dialing plan and to support outgoing voice calls. For a more complete example using all the related commands, see the **map-class dialer** command.

```
map-class dialer sdnplan
  dialer voice-call
  dialer outgoing sdn
```

Related Commands

Command	Description
dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites.
dialer outgoing	Configures the dialer map class for a NSF dialing plan to support outgoing calls.
map-class dialer	Defines a class of shared configuration parameters associated with the dialer map command for outgoing calls from an ISDN interface and for PPP callback.

dialer vpdn

To enable a dialer profile or dial-on-demand routing (DDR) dialer to use Layer 2 Tunnel Protocol (L2TP) dialout, use the **dialer vpdn** command in interface configuration mode. To disable L2TP dialout on a dialer profile or DDR dialer, use the **no** form of this command.

dialer vpdn

no dialer vpdn

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

The **dialer vpdn** command must be configured on the LNSs dialer interface to enable L2TP dialout. This command enables the dialer to place a VPDN call.

Examples

The following example shows how to configure the dialer interface and VPDN group on an LNS for L2TP dialout:

```
interface Dialer2
 ip address 172.16.2.3 255.255.255.128
 encapsulation ppp
 dialer remote-name myname
 dialer string 5550134
 dialer vpdn
 dialer pool 1
 dialer-group 1
 ppp authentication chap

vpdn-group 1
 request-dialout
  protocol l2tp
  pool-member 1
 initiate-to ip 172.21.9.4
```

Related Commands

Command	Description
dialer aaa	Allows a dialer to access the AAA server for dialing information.
request-dialout	Enables an LNS to request VPDN dial-out calls by using L2TP.

dialer wait-for-carrier-time (interface)

To specify the length of time the interface waits for a carrier, use the **dialer wait-for-carrier-time** command in interface configuration mode. To reset the carrier wait time value to the default, use the **no** form of this command.

dialer wait-for-carrier-time *seconds*

no dialer wait-for-carrier-time

Syntax Description

seconds	Number of seconds that the interface waits for the carrier to come up when a call is placed. Acceptable values are positive, nonzero integers.

Command Default

30 seconds

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

On asynchronous interfaces, the **dialer wait-for-carrier-time** command sets the total time allowed for the chat script to run.

If a carrier signal is not detected in this amount of time, the interface is disabled until the enable timeout occurs (configured with the **dialer enable-timeout** command).

Do not use this command for BRI and leased-line interfaces.

Examples

The following example specifies a carrier wait time of 45 seconds on asynchronous interface 1:

```
interface async 1
 dialer wait-for-carrier-time 45
```

Related Commands

Command	Description
dialer enable-timeout	Sets the length of time an interface stays down after a call has completed or failed and before the interface is available to dial again.

dialer wait-for-carrier-time (map-class)

To specify the length of time to wait for a carrier when dialing out to the dial string associated with a specified map class, use the **dialer wait-for-carrier-time** command in map-class dialer configuration mode. To reset the carrier wait time value to the default, use the **no** form of this command.

dialer wait-for-carrier-time *seconds*

no dialer wait-for-carrier-time

Syntax Description

seconds	Number of seconds that the interface waits for the carrier to come up when a call is placed. Acceptable values are positive, nonzero integers. The default is 30 seconds.

Command Default

30 seconds

Command Modes

Map-class dialer configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You can define different dialer map classes with different wait-for-carrier times to suit the different types of lines and interfaces. For example, you must define a longer wait time for a map class used by serial interfaces than for one used by ISDN interfaces.

Do not use this command for BRI and leased-line interfaces.

Examples

The following example specifies a carrier wait time of 20 seconds for the class “Eng” on interface Dialer2:

```
interface Dialer2
 ip address 10.2.2.2 255.255.255.0
 encapsulation ppp
 dialer remote-name Mediumuser
 dialer string 5264540 class Eng
 dialer wait-for-carrier-time 20
 dialer load-threshold 50 either
 dialer pool 1
 dialer-group 2
```

dialer wait-for-line-protocol

To set a maximum time the dialer will wait for a line protocol after establishing a physical connection before considering the call unsuccessful, use the **dialer wait-for-line-protocol** command in interface configuration mode. To disable this function, use the **no** form of this command.

dialer wait-for-line-protocol *wait-time*

no dialer wait-for-line-protocol

Syntax Description

wait-time	Time, in seconds, that the dialer will wait for the line protocol to come up after the physical layer connection has been established. The time can range from 1 to 2147483 seconds.

Command Default

Timer is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

This command is supported only with encapsulation PPP.

By default the Cisco IOS software considers a dial-out attempt successful if a connection is established to the physical layer (Layer 1 of the Open System Interconnection reference model). The **dialer wait-for-line-protocol** command can be used to configure a router to wait a specific amount of time for a line protocol to come up once a physical layer connection has been established. If the call is dropped before the timer has elapsed, the call will be considered a failure. Redial will be triggered if the redial options have been configured with the **dialer redial** interface configuration command. The dialer failure statistics for the physical interface will be updated, which may influence the selection of a physical dialer for the next dial attempt. The physical dialer selection algorithm may be customized using the **dialer rotor** interface configuration command.

Note This command is not useful in conjunction with Cisco High-Level Data Link Control (HDLC) encapsulation. Cisco HDLC encapsulation is the default line protocol and will always come up regardless of line conditions.

Examples

The following example configures the dialer to wait 10 seconds for a line protocol after making a physical connection:

```
dialer wait-for-line-protocol 10
```

Related Commands

Command	Description
debug dialer events	Displays debugging information about the packets received on a dialer interface.
dialer redial	Configures the number of redial attempts to be made, the interval between redial attempts, and the amount of time the interface will be disabled if all redial attempts fail.
dialer rotor	Specifies the method for identifying the outbound line to be used for ISDN or asynchronous DDR calls.

dialer watch-disable

Note Effective with Cisco IOS Release 12.3(11)T, this command is replaced by the **dialer watch-list delay** command. See the **dialer watch-list delay** command page for more information.

To set a delay time to the backup interface, use the **dialer watch-disable** command in interface configuration mode. To disable this feature, use the **no** form of this command.

dialer watch-disable *timeout*

no dialer watch-disable

Syntax Description

timeout	The timeout value in seconds.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.3(11)T	This command was replaced by the **dialer watch-list delay** command.

Usage Guidelines

This command is used to add a delay time to the backup interface. The delay time delays the time it takes for the backup interface to disconnect after the primary interface recovers.

Examples

The following example forces a 6-second delay to the backup interface once the primary interface recovers:

```
interface bri0
 ip address 10.1.1.2 255.255.255.0
 encapsulation ppp
 dialer map ip 10.3.1.1 255.255.255.0 name mymap 5550134
 dialer-group 1
 dialer watch-group 1
 dialer watch-disable 6
```

Related Commands

Command	Description
show dialer dnis	Displays general diagnostic information for ISDN BRI interfaces configured for DDR.

dialer watch-group

To enable dial-on-demand routing (DDR) backup on an interface using Dialer Watch, configure the interface using the **dialer watch-group** command in interface configuration mode. To disable this feature, use the **no** form of this command.

dialer watch-group *group-number*

no dialer watch-group *group-number*

Syntax Description

group-number	Group number assigned that will point to a globally defined list of IP addresses to watch. The valid range is 1 to 255.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.3T	This command was introduced.

Usage Guidelines

Use the **dialer watch-group** command on the secondary interface you want to enable DDR backup.

The dialer watch group number points to a globally defined list (the **dialer watch-list** command) that contains the IP addresses to be watched. If you use the **dialer watch-group** command you must also use the **dialer watch-list** command.

You must configure the standard commands required to enable the router to perform DDR in addition to the Dialer Watch commands. Refer to the *Cisco IOS Dial Technologies Configuration Guide* and the *Cisco IOS Dial Technologies Command Reference* for additional information.

The **dialer watch-group** and **dialer watch-list** commands can be added in any order.

Examples

The following example configures BRI interface 0 as the backup interface:

```
interface bri0
 ip address 10.1.1.2 255.255.255.0
 encapsulation ppp
 dialer watch-group 1
```

Related Commands

Command	Description
dialer watch-list	Adds the list of IP addresses to be monitored for Dialer Watch.

dialer watch-list

To specify a list of watched routes of IP addresses or optionally, IP address and VPN routing and forwarding (VRF) instance pairs to be monitored by Dialer Watch, or to configure the router to dial the backup link if the primary link fails during initial startup, use the **dialer watch-list** command in global configuration mode. To disable these features, use the **no** form of this command.

dialer watch-list *group-number* {**ip** *ip-address address-mask* [**vrf** *vrf-name*] | **delay route-check initial** *seconds*}

no dialer watch-list *group-number* {**ip** *ip-address address-mask* [**vrf** *vrf-name*] | **delay route-check initial** *seconds*}

Syntax Description

group-number	Group number assigned to the list. Valid group numbers are from 1 to 255. The value of this argument must match the group number set with the **dialer watch-group** command.
ip *ip-address address-mask*	Specifies the IP address or address range and address mask to be applied to the list. IP is the only routed protocol supported for Dialer Watch.
vrf *vrf-name*	(Optional) Specifies a watched route using the VRF instance table named in the *vrf-name* argument.
delay route-check initial *seconds*	Number of seconds after which the router ensures that the primary route is up once initial startup is complete.

Command Default

The **dialer watch-list** command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.1(3)T	The **delay route-check initial** *seconds* keywords and argument were introduced.
12.3(7)T	The **vrf** *vrf-name* keyword and argument were introduced.

Usage Guidelines

Use this command to add all IP addresses or networks that you want monitored. There is no software limit to the number of IP addresses that can be added to a group.

Use this command with the **dialer watch-group** interface configuration command. The *group-number* value must match the group number set in the **dialer watch-group** interface configuration command. For example, if you use **dialer watch-group 1**, you must also use **dialer watch-list 1**.

The **dialer watch-list** and **dialer watch-group** commands can be added in any order.

Address matching is exact; therefore, you must apply the specific IP address and mask range for the networks that you want monitored. Use the **show ip route** command to verify that the route you are watching exists in the routing table. The route configured for the **dialer watch-list** command must match the one in the routing table exactly. This matching includes verifying that both the network and the masks

are identical. You must configure the standard commands required to enable the router to perform dial-on-demand routing (DDR) in addition to configuring the Dialer Watch commands. Refer to the *Cisco IOS Dial Technologies Configuration Guide* and the *Cisco IOS Dial Technologies Command Reference* for additional information.

Enabling the **delay route-check initial** keywords enables the router to check whether the primary route is up after the initial startup of the router is complete and the timer (in seconds) expires. Without this command, the Dialer Watch feature is triggered only when the primary route is removed from the routing table. If the primary link fails to come up during initial startup of the router, the route is never added to the routing table and hence cannot be watched. Therefore, using the **delay route-check initial** keywords enables the Dialer Watch feature to dial the backup link in the event of a primary link failure during the initial startup of the router.

Enabling the **vrf** *vrf-name* keyword and argument configures the corresponding VRF table to be used to detect when the watched route for the VRF has gone down. A VRF is a per-VPN routing information repository that defines the virtual private network (VPN) membership of a customer site attached to a network access server. A VRF consists of an IP routing table, a derived Cisco Express Forwarding (CEF) table, a set of interfaces that use the forwarding table, and a set of rules and routing protocol parameters that control the information that is included in the routing table. A separate set of routing and CEF tables is maintained for each VPN customer.

It is important to note that the VRF might have overlapping address space, as follows: At the provider edge (PE) router, each customer edge (CE) router will have a corresponding VRF associated with it. Further, two CE routers might be using the same address space, so that the corresponding VRFs at the PE router will have overlapping address space. For this reason, when using the **vrf** *vrf-name* keyword and argument, configure the watched route as an IP address-VRF name pair, where the IP address is the watched IP address and the VRF name is the routing and forwarding instance to which the IP address belongs. Configuring the Dialer Watch feature with only the IP address does not ensure that the correct CE route will be dialed when a watched route goes down. Configuring Dialer Watch with an IP address and VRF name pair ensures that the VRF table corresponding to the routing and forwarding instance to which the IP address belongs is found and the correct CE is dialed.

You can define one watch route that watches the same IP address, but belongs to a different VRF, in a single watch list.

Examples

The following example specifies a pair of watched routes in a legacy dialer configuration. In this configuration, watch lists 1 and 2 are both watching the same IP address, but belong to different VRFs.

```
interface BRI3/0
 ip address 10.0.2.2 255.255.255.0
 encapsulation ppp
 dialer map 10.1.2.0 vrf v1 3xxxxxx
 dialer map 10.1.2.0 vrf v2 4xxxxxx
 dialer-group 1
 dialer watch-group 1
 dialer watch-group 2
 isdn switch-type ntt
 ppp authentication chap
!
dialer watch-list 1 ip 10.2.1.0 255.255.255.0 vrf v1
dialer watch-list 2 ip 10.2.1.0 255.255.255.0 vrf v2
```

The following example specifies a pair of watched routes in a dialer rotary group configuration. In this configuration, watch lists 1 and 2 are both watching the same IP address, but belong to different VRFs.

```
interface BRI3/0
 no ip address
 encapsulation ppp
 dialer rotary-group 1
 isdn switch-type ntt
 ppp authentication chap
!
interface Dialer1
 ip address 10.0.2.2 255.255.255.0
 encapsulation ppp
 dialer remote-name c3640-B
 dialer map 10.1.2.0 vrf v1 3xxxxxx
 dialer map 10.1.2.0 vrf v2 4xxxxxx
 dialer watch-group 1
 dialer watch-group 2
 dialer-group 1
 ppp authentication chap
!
dialer watch-list 1 ip 10.2.1.0 255.255.255.0 vrf v1
dialer watch-list 2 ip 10.2.1.0 255.255.255.0 vrf v2
dialer watch-list 1 delay disconnect 30
```

The following example specifies a pair of watched routes in a dialer profile configuration. In this configuration, watch lists 1 and 2 are both watching the same IP address, but belong to different VRFs.

```
interface BRI3/0
 no ip address
 encapsulation ppp
 dialer pool-member 1
 isdn switch-type ntt
 ppp authentication chap
!
interface Dialer1
 ip vrf forwarding v1
 ip address 10.0.2.2 255.255.255.0
 encapsulation ppp
 dialer pool 1
 dialer remote-name c3640-B
 dialer watch-disable 30
 dialer string 03xxxxxxx1
 dialer caller 03xxxxxxx1 callback
 dialer watch-group 1
 dialer-group 1
 ppp authentication chap
!
interface Dialer2
 ip vrf forwarding v2
 ip address 10.0.2.2 255.255.255.0
 encapsulation ppp
 dialer pool 1
 dialer remote-name c3640-B
 dialer string 04xxxxxxx1
 dialer caller 04xxxxxxx1 callback
 dialer watch-group 2
 dialer-group 1
 ppp authentication chap
!
dialer watch-list 1 ip 10.2.1.0 255.255.255.0 vrf v1
dialer watch-list 2 ip 10.2.1.0 255.255.255.0 vrf v2
dialer watch-list 1 delay disconnect 30
dialer watch-list 2 delay disconnect 30
```

The following example lists IP addresses to be watched and forms a group of networks to monitor:

```
dialer watch-list 1 ip 10.1.1.0 255.255.255.0
dialer watch-list 1 ip 10.31.1.0 255.255.255.0
dialer watch-list 1 ip 10.12.1.0 255.255.255.0
```

The following partial example shows how to ensure that the router will check that the primary route is up after initial startup of the router is complete:

```
! Create backup link and enable process switching
interface BRI0/0
 ip address 10.13.1.1 255.255.255.0
 encapsulation ppp
 no ip route-cache
.
.
.
! Enable dialer watch on this backup interface.
! Watch the route specified with the dialer watch-list 1 command.
! Apply interesting traffic defined in dialer list 1.
! Apply crypto map on backup interface.
dialer watch-group 1
 dialer-group 1
isdn switch-type basic-ts013
 no peer neighbor-route
 no cdp enable
 ppp authentication chap
 crypto map cisco
.
.
.
! Access control list (ACL) 101 is the IPSec traffic used in match address.
! ACL 110 is for the dialer list to mark all IP traffic uninteresting.
! The dialer watch will trigger the ISDN backup when the route is lost.
access-list 101 permit ip host 10.11.11.11 host 10.11.22.22
access-list 110 deny ip any any
dialer watch-list 1 ip 192.168.0.222 255.255.255.255
! These commands define the routes to be watched
! and check whether the primary route is up after the initial startup of the
! router is complete.
! The exact route (including subnet mask) must exist in the routing table.
! The dialer watch-group 1 command applies this list to the backup interface.
dialer watch-list 1 delay route-check initial 10
dialer-list 1 protocol ip list 110
! Interesting traffic is defined by ACL 110.
! The ACL is applied to BRI0/0 using dialer group 1.
```

Related Commands

Command	Description
dialer watch-group	Enables DDR backup on an interface using Dialer Watch.
show ip route	Displays all static IP routes, or those installed using the AAA route download function.

dialer watch-list delay

To configure the router to delay before connecting or disconnecting a secondary link for a route monitored by Dialer Watch, use the **dialer watch-list delay** command in global configuration mode. To disable these delays, use the **no** form of this command.

dialer watch-list *group-number* **delay** {**connect** *connect-time* | **disconnect** *disconnect-time*}

no dialer watch-list *group-number* **delay** {**connect** *connect-time* | **disconnect** *disconnect-time*}

Syntax Description

group-number	Group number assigned to the list. Valid group numbers are from 1 to 255.
connect	Specifies that the router will delay dialing the secondary link when the primary link becomes unavailable.
connect-time	Time, in seconds, after which the router rechecks for availability of the primary link. If the primary link is still unavailable, the secondary link is then dialed. Valid times range from 1 to 2147483.
disconnect	Specifies that the disconnect timer is started when the secondary link is up and after the idle timeout period has expired, and only when software has determined that the primary route has come up.
disconnect-time	Time, in seconds. Valid times range from 1 to 2147483.

Command Default

No delay is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Use this command to configure a delay before connecting or disconnecting a secondary link for a route monitored by Dialer Watch. This command will not work unless dial-on-demand routing (DDR) is configured and Dialer Watch has been enabled.

Examples

The following example configures the router to wait 10 seconds before verifying that the primary link is still down and dialing a secondary link:

```
dialer watch-list 1 ip 10.1.1.0 255.255.255.0
dialer watch-list 1 delay connect 10
```

The following example configures the router to wait 10 seconds to disconnect a secondary link once the primary link has been reestablished:

```
dialer watch-list 1 ip 10.1.1.0 255.255.255.0
dialer watch-list 1 delay disconnect 10
```

Related Commands

Command	Description
dialer watch-group	Enables DDR backup on an interface using Dialer Watch.
dialer watch-list	Adds the list of IP addresses to be monitored for Dialer Watch.

dialer-group

To control access by configuring an interface to belong to a specific dialing group, use the **dialer-group** command in interface configuration mode. To remove an interface from the specified dialer access group, use the **no** form of this command.

dialer-group *group-number*

no dialer-group

Syntax Description

group-number	Number of the dialer access group to which the specific interface belongs. This access group is defined with the **dialer-list** command. Acceptable values are nonzero, positive integers between 1 and 10.

Command Default

No access is predefined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

An interface can be associated with a single dialer access group only; multiple **dialer-group** assignment is not allowed. A second dialer access group assignment will override the first. A dialer access group is defined with the **dialer-group** command. The **dialer-list** command associates an access list with a dialer access group.

Packets that match the dialer group specified trigger a connection request.

Examples

The following example specifies dialer access group number 1.

The destination address of the packet is evaluated against the access list specified in the associated **dialer-list** command. If it passes, either a call is initiated (if no connection has already been established) or the idle timer is reset (if a call is currently connected).

```
interface async 1
 dialer-group 1
access-list 101 deny igrp 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
dialer-list 1 protocol ip list 101
```

Related Commands

Command	Description
dialer-list protocol (Dial)	Defines a DDR dialer list to control dialing by protocol or by a combination of protocol and an access list.

dialer-group (template)

To control access by configuring a virtual access interface to belong to a specific dialing group, use the **dialer-group** command in template configuration mode. To remove an interface from the specified dialer access group, use the **no** form of this command.

dialer-group *dialer-list-number*

no dialer-group

Syntax Description

dialer-list-number	Number of the dialer access group to which the specific interface belongs. This access group is defined with the **dialer-list** command. Acceptable values are positive numbers from 1 to 128.

Command Default

No access is predefined.

Command Modes

Template configuration

Command History

Release	Modification
12.2(4)T	This command was introduced for Resource Pool Manager (RPM) template configuration.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300, Cisco AS5400, and Cisco AS5800.

Usage Guidelines

An interface can be associated with only a single dialer access group; multiple **dialer-group** assignment is not allowed. A second dialer access group assignment will override the first. A dialer access group is defined with the **dialer-group** template configuration command. The **dialer-list** command associates an access list with a dialer access group. For Cisco IOS Release 12.2(4)T, the number of dialer groups that can be configured was increased from 10 to 128.

Packets that match the dialer group specified trigger a connection request.

Examples

The following example specifies dialer access group number 1. The destination address of the packet is evaluated against the access list specified in the associated **dialer-list** command. If it passes, either a call is initiated (if no connection has already been established) or the idle timer is reset (if a call is currently connected).

```
template template1
 dialer-group 1
```

Related Commands

Command	Description
dialer-list protocol	Defines a dialer list to control dialing by protocol or by a combination of protocol and an access list.

dialer-list protocol (Dial)

To define a dial-on-demand routing (DDR) dialer list for dialing by protocol or by a combination of a protocol and a previously defined access list, use the **dialer-list protocol** command in global configuration mode. To delete a dialer list, use the **no** form of this command.

dialer-list *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | *access-group*}

no dialer-list *dialer-group* [**protocol** *protocol-name* [**list** *access-list-number* | *access-group*]]

Syntax Description

dialer-group	Number of a dialer access group identified in any **dialer-group** interface or template configuration command. Up to 128 dialer groups can be configured.
protocol-name	One of the following protocol keywords: **appletalk**, **bridge**, **clns**, **clns_es**, **clns_is**, **decnet**, **decnet_router-L1**, **decnet_router-L2**, **decnet_node**, **ip**, **ipx**, or **ipv6**.
permit	Permits access to an entire protocol.
deny	Denies access to an entire protocol.
list	Specifies that an access list will be used for defining a granularity finer than an entire protocol.
access-list-number	Access list numbers specified in any DECnet, IP, or Novell IPX standard or extended access lists, including Novell IPX extended service access point (SAP) access lists and bridging types. See Table 5 for the supported access list types and numbers.
access-group	Filter list name used in the **clns filter-set** and **clns access-group** commands.

Command Default

No dialer lists are defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
10.3	The **list** keyword and the *access-list-number* and *access-group* arguments were added.
12.2(2)T	The **ipv6** protocol keyword was added.
12.2(4)T	The number of dialer groups that can be configured was increased to 128.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300, Cisco AS5400, and Cisco AS5800.
12.2(13)T	The **igrp**, **vines**, and **xns** arguments were removed because the Interior Gateway Routing Protocol (IGRP), Banyan Systems Virtual Integrated Network Service (VINES), and the Xerox Network System (XNS) are no longer available in Cisco IOS software.

Usage Guidelines

The various **no** forms of this command have the following effects:

- The **no dialer-list** *dialer-group* command deletes all lists configured for the specified dialer access group, regardless of the keyword previously used (**permit**, **deny**, **protocol**, or **list**).
- The **no dialer-list** *dialer-group* **protocol** *protocol-name* command deletes all lists configured for the specified dialer access group and **protocol** *protocol-name*.
- The **no dialer-list** *dialer-group* **protocol** *protocol-name* **list** *access-list-number* command deletes the specified list.

The **dialer-list protocol** command permits or denies access to an entire protocol.

The **dialer-list protocol** command with the optional **list** keyword provides finer permission granularity and also supports protocols that were not previously supported. This command also applies protocol access lists to dialer access groups to control dialing using DDR. The dialer access groups are defined with the **dialer-group** command.

Table 5 lists the access list types and numbers that the **dialer-list protocol** command supports. The table does not include International Organization for Standardization Connectionless Network Service (ISO CLNS) because that protocol uses filter names instead of predefined access list numbers.

Table 5 dialer-list protocol Command Supported Access List Types and Numbers

Access List Type	Access List Number Range (Decimal)
AppleTalk	600–699
DECnet	300–399
IP (standard)	1–99
IP (extended)	100–199
Novell IPX (standard)	800–899
Novell IPX (extended)	900–999
Transparent Bridging	200–299

Examples

Dialing occurs when an interesting packet (one that matches access list specifications) needs to be output on an interface. Using the standard access list method, packets can be classified as interesting or uninteresting. The following example classifies all other IP packets as interesting and permits them to initiate calls:

```
access-list 101 permit ip 10.0.0.0 255.255.255.255 10.0.0.0 255.255.255.255
```

Then the following command places list 101 into dialer access group 1:

```
dialer-list 1 protocol ip list 101
```

In the following example, DECnet access lists allow any DECnet packets with source area 10 and destination area 20 to trigger calls:

```
access-list 301 permit 10.0 0.1023 10.0 0.1023
access-list 301 permit 10.0 0.1023 20.0 0.1023
```

Then the following command places access list 301 into dialer access group 1:

```
dialer-list 1 protocol decnet list 301
```

In the following example, a CLNS filter is defined and then the filter is placed in dialer access group 1:

```
clns filter-set ddrline permit 47.0004.0001....
!
dialer-list 1 protocol clns list ddrline
```

The following example configures an IPv6 access list named list2 and places the access list in dialer access group 1:

```
ipv6 access-list list2 deny fec0:0:0:2::/64 any
ipv6 access-list list2 permit any any
!
dialer-list 1 protocol ipv6 list list2
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.
clns filter-set	Builds a list of CLNS address templates with associated permit and deny conditions for use in CLNS filter expressions.
dialer-group (template)	Controls access by configuring a virtual template interface to belong to a specific dialing group.
ipv6 access-list	Defines an IPv6 access list and sets deny or permit conditions for the defined access list.

dial-peer cor custom

To specify that named class of restrictions (COR) apply to dial peers, use the **dial-peer cor custom** command in global configuration mode.

dial-peer cor custom

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or keywords.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

You must use the **dial-peer cor custom** command and the **name** command to define the names of capabilities before you can specify COR rules and apply them to specific dial peers.

Examples of possible names might include the following: call1900, call527, call9, and call911.

Note You can define a maximum of 64 COR names.

Examples

The following example defines two COR names:

```
dial-peer cor custom
 name group32
 name CatchAll
```

Related Commands

Command	Description
name (dial peer cor custom)	Provides a name for a custom COR.

dial-peer cor list

To define a class of restrictions (COR) list name, use the **dial-peer cor list** command in global configuration mode. To remove a previously defined COR list name, use the **no** form of this command.

dial-peer cor list *list-name*

no dial-peer cor list *list-name*

Syntax Description

list-name	List name that is applied to incoming or outgoing calls to specific numbers or exchanges.

Command Default

No default behavior or keywords.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

A COR list defines a capability set that is used in the COR checking between incoming and outgoing dial peers.

Examples

The following example adds two members to the COR list named list1:

```
dial-peer cor list list1
 member 900block
 member 800_call
```

Related Commands

Command	Description
dial-peer cor custom	Specifies that named COR apply to dial peers.
member (dial peer cor list)	Adds a member to a dial peer COR list.
name (dial peer cor custom)	Provides a name for a custom COR.

dial-shelf split backplane-ds0

To connect two router shelves to a dial shelf, use the **dial-shelf split backplane-ds0** command in global configuration mode. To remove the connection, use the **no** form of this command.

dial-shelf split backplane-ds0 {*predefined-option* | **userdefined** *option*}

no dial-shelf split backplane-ds0

Syntax Description

predefined-option	Predefined backplane DS0 pairs. See Table 6 for a list of these options.
userdefined *option*	Number of backplane DS0 interfaces used by the router shelf that you define, in the range 128 to 2048.

Command Default

Option pair 6

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.

Usage Guidelines

The options for this command come in pairs and vary according to the desired configuration. You will need to log in to each router shelf and separately configure the routers for the intended load. In most circumstances, it is recommended that the predefined options remain selected. These options are designed to be matched pairs, as seen in Table 6. You can select the **userdefined** keyword and define your own split, if needed. Table 6 lists the predefined options.

Table 6 dial-shelf split backplane ds-0 Predefined Options

	Router Shelf 1			Router Shelf 2			Total Calls
Option Pair	Option	Maximum Calls	Unused T1	Option	Maximum Calls	Unused T1	
1	`2ct3cas`	1344	—	`1ct3cas`	672	—	2016
2	`part2ct1ct3cas`	1152	4	`part1ct1ct3cas`	888	3	2040
3	`2ct3isdn`	1288	—	`part1ct1ct3isdn_b`	644	7	1932
4	`part2ct1ct3isdn`	1150	2	`part1ct1ct3isdn`	897	1	2047
5[1]	`3ce1`	960	—	`3ce1`	960	—	1920
6	Default (no option entered)	1/2 of current input	—	Default (no option entered)	1/2 of current input	—	—
7	`no dial-shelf backplane-ds0`	1024	—	`no dial-shelf backplane-ds0`	1024	—	2048

1. This option is used to revert to the default for an environment that uses six E1 lines.

The **dial-shelf split slot** command must be defined for the **dial-shelf split backplane-ds0** command to be active.

Even if your system is already using a split dial shelf configuration, configuring one router shelf to handle two T3 trunks and the other router to handle the third trunk requires you to take the entire access server out of service. Busyout all connections before attempting to reconfigure. The configuration must be changed to set up one pool of TDM resources that can be used by either DMM cards or UPC and a second pool of two streams that contains TDM resources that can be used only by UPCs.

You may have more trunk capacity than 2048 calls. It is your decision how to provision the trunks so the backplane capacity is not exceeded. If more calls come in than backplane DS0 capacity for that half of the split, the call will be rejected and an error message printed for each call. This cannot be detected while a new configuration is being built because the router cannot tell which T1 trunks are provisioned and which are not. The user may want some trunks in hot standby.

The DMM, HMM, and VoIP cards can use only 1792 DS0 of the available 2048 backplane DS0. The UPC and trunk cards can use the full 2048 backplane DS0.

The **show tdm splitbackplane** command shows the resources in two groups, the first 1792 accessible to all cards, and the remaining 256 accessible only to UPC and trunk cards.

Examples

The following example shows how to configure two router shelves. Refer to Table 6 to interpret the options specified.

Configure router shelf 1 to run two CT3 interfaces with channel-associated signaling (CAS) and the ability to answer 1344 calls:

```
dial-shelf split backplane-ds0 2ct3cas
```

Configure router shelf 2 to run one CT3 interface with CAS on the second router shelf and the ability to answer 672 calls:

```
dial-shelf split backplane-ds0 1ct3cas
```

The total calls configured for the system are 2036 (1344 plus 672).

Related Commands

Command	Description
dial-shelf split slots	Configures split dial shelves.
show tdm splitbackplane	Displays modem and PRI channel assignments with streams and channels on the modem side as assigned to the unit and channels on the PRI side of the TDM assignment.

dial-shelf split slots

To configure split dial shelves, use the **dial-shelf split slots** command in global configuration mode. To change the router shelf to normal mode, if a router is in split mode and the other router shelf has already relinquished control of all dial shelf slots or is switched off, use the **no** form of this command.

dial-shelf split slots *slot-numbers*

no dial-shelf split slots

Syntax Description

slot-numbers	List of the dial shelf slot numbers that the router owns in the range 0 to 11, separated by spaces. Slot ownership for each of the two router shelves is configured individually using the **dial-shelf split slots** command.

Command Default

No default behavior or keywords.

Command Modes

Global configuration

Command History

Release	Modification
11.3(8)AA	This command was introduced.

Usage Guidelines

You allocate the slots in the dial shelf between the two router shelves to achieve the desired configuration. The two router shelves are both configured to run in split mode by means of the **dial-shelf split slots** command. While a router is in split mode, additional slots can be added to the set that the router owns by re-entering the **dial-shelf split slots** command listing the new slots. The effect of entering two or more **dial-shelf split slots** commands with different slot numbers is cumulative.

Slots must be explicitly removed from the list of router-owned slots with the **dial-shelf split slots remove** command.

A single router can also be configured in split mode, but with no slots owned, by using the **dial-shelf split slots none** command.

When you configure a Cisco AS5800 system to operate in split mode, it is the same as having two Cisco AS5800 systems with each having a separate set of feature boards assigned to its router; they just happen to be sharing a single dial shelf. Modem pooling, for example, is the same as if you had two separate Cisco AS5800 systems. Router shelf 1 has a modem pool that consists of all the modem cards that reside in slots owned by router shelf 1. The same situation applies to router shelf 2.

Examples

The following example would configure the router shelf to own slots 0 through 2 and 6 through 8.

```
dial-shelf split slots 0 1 2 6 7 8
```

In this example, the other router shelf could be configured to own the other slots: 3, 4, 5, 9, 10, and 11.

Related Commands

Command	Description
dial-shelf split backplane-ds0	Connects two router shelves to a dial shelf.
dial-shelf split slots none	Configures the router in dial shelf split mode but with no slots owned.
dial-shelf split slots remove	Removes slots configured in split mode.

dial-shelf split slots none

To configure the router in dial shelf split mode but with no slots owned, use the **dial-shelf split slots none** command in global configuration mode.

dial-shelf split slots none

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or keywords.

Command Modes

Global configuration

Command History

Release	Modification
11.3(8)AA	This command was introduced.

Usage Guidelines

The **dial-shelf split slots none** command is useful for configuring a single router in split mode, but with no slots owned.

Examples

The following example changes dial shelf slot ownership. The router will no longer have ownership of any dial shelf slots.

```
dial-shelf split slots none
```

Related Commands

Command	Description
dial-shelf split slots remove	Removes slots configured in split mode.

dial-shelf split slots remove

To remove slots configured in split mode, use the **dial-shelf split slots remove** command in global configuration mode.

dial-shelf split slots remove *slot-numbers*

Syntax Description

slot-numbers	List of the dial shelf slot numbers to be removed ,separated by spaces, in the range 0 to 11.

Command Default

No default behavior or keywords.

Command Modes

Global configuration

Command History

Release	Modification
11.3(8)AA	This command was introduced.

Usage Guidelines

To move a slot from the control of one router shelf to the others, the router releasing the slot should be modified first by entering the **dial-shelf split slots remove** command, specifying the slot numbers to be released. The released slots can then be added to the slot set of the other router by re-entering the **dial-shelf split slots** command including the new slot numbers.

The router shelf that is losing the slot frees any resources and clears any state associated with the card in the slot it is relinquishing. The dial shelf controller (DSC) reconfigures its hub to ignore traffic from that slot, and if there is a card in the slot it will be reset. This ensures that the card frees up any TDM resource it might be using and allows it to restart under control of the router shelf that is subsequently configured to own the slot.

Examples

The following example removes dial shelf slot 8 from the list of owned dial shelf slots:

```
dial-shelf split slots remove 8
```

The effect of multiple commands is cumulative.

Related Commands

Command	Description
dial-shelf split slots none	Configures the router in dial shelf split mode but with no slots owned.

dial-tdm-clock

To configure the clock source and priority of the clock source used by the time-division multiplexing (TDM) bus on the dial shelf of the Cisco AS5800, use the **dial-tdm-clock** command in global configuration mode. To return the clock source and priority to the default values, use the **no** form of this command.

dial-tdm-clock priority *number* {**external** {**e1** | **t1**} [**120ohm**] | **freerun** | **trunk-slot** *slot* **port** *port*} [**line** {**0** | **1**}]

no dial-tdm-clock priority *number* {**external** {**e1** | **t1**} [**120ohm**] | **freerun** | **trunk-slot** *slot* **port** *port*} [**line** {**0** | **1**}]

Syntax Description

priority *number*	Specifies the priority of the clock source. The range is from 1 to 50. Priority 1 is the highest priority, and 50 is the lowest.
external	Specifies the priority of an external clock source. The external clock source is connected to the front panel of the Dial Shelf Controller (DSC) card.
{**e1** | **t1**} [**120ohm**]	Specifies priority of the E1 (2.048 MHz) or T1 (1.54 MHz) external clock source. The default value of the external coaxial cable impedance is 75 ohm. Specify the **120ohm** option if a 120 ohm coaxial cable is connected.
freerun	Specifies the priority of the local oscillator clock source.
trunk-slot *slot*	Specifies the priority of the trunk card to provide the clock source. The slot number is from 0 to 5 (these are the only slots capable of providing clock sources).
port *port*	Specifies the controller number on the trunk used to provide the clock source. The port number is from 0 to 28. The T1 and E1 trunk cards each have 12 ports. The T3 trunk card has 28 ports.
line {**0** | **1**}	(Optional) Specifies the optical port. If the physical optical port is 0, the **line** value is also 0.

Command Default

If no clock sources are specified, the software selects the first available good clock source on a trunk port.

Command Modes

Global configuration

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.2(15)T	The **line** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The TDM bus in the backplane on the dial shelf must be synchronized to the T1/E1 clocks on the trunk cards. The DSC card on the dial shelf provides hardware logic to accept multiple clock sources as input and use one of them as the primary source to generate a stable, PPL synchronized output clock. The input clock can be any of the following sources:

- Trunk port in slots 0 through 5 (up to 12 can be selected (two per slot)
- An external T1 or E1 clock source fed directly through a connector on the DSC card
- A free running clock from an oscillator in the clocking hardware on the DSC card

The clock commands are listed in the configuration file with the highest priority listed first.

If the current primary clock source is good, specifying another clock source of higher priority does not cause the clock source to switch to the higher priority clock source. The new higher priority clock source is used as a backup clock source. This prevents switching of the clock source as you enter multiple **dial-tdm-clock priority** configuration commands in random order. Also, it is important not to disturb the existing clock source as long as it is good. To force the new higher priority clock source to take over from a currently good primary clock source, configure the new clock source and use the **no dial-tdm-clock priority** command to remove the current primary clock source.

To display the current primary and backup clocks along with their priorities, use the **show dial-shelf clocks** EXEC command.

Examples

In the following example, an external clock source is set at priority 1 and the trunk card in slot 4, port 1 is set at priority 5:

```
Router(config)# dial-tdm-clock priority 1 external t1
Router(config)# dial-tdm-clock priority 5 trunk-slot 4 port 1
Router(config)# exit
```

Related Commands

Command	Description
show dial-shelf	Displays information about the dial shelf, including clocking information.

disconnect

To disconnect a line, use the **disconnect** command in EXEC mode.

disconnect [*connection*]

Syntax Description

connection	(Optional) Number of the line or name of the active network connection to be disconnected.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Do not disconnect a line to end a session. Instead, log off the host, so that the Cisco IOS software can clear the connection. Then end the session. If you cannot log out of an active session, disconnect the line.

Examples

In the following example, the user disconnects from the device Remote to return to the router:

```
Remote% disconnect
 Connection closed by remote host
```

Related Commands

Command	Description
login (EXEC)	Enables or changes a login user name.

dnis group

To include a group of Dialed Number Identification Service (DNIS) numbers in a customer profile, use the **dnis group** command in customer profile configuration mode. To remove a DNIS group from a customer profile, use the **no** form of this command.

dnis group {**default** | **name** *dnis-group-name*}

no dnis group {**default** | **name** *dnis-group-name*}

Syntax Description

default	Allows a specified customer profile to accept all DNIS numbers coming into the access server. For example, a stray DNIS number not listed in any customer profile passes through this default DNIS group. Most customer profiles do not have this option configured.
name	Assigns a name to a DNIS group.
dnis-group-name	DNIS group name. It can have up to 23 characters.

Command Default

No DNIS groups are associated with a customer profile.

Command Modes

Customer profile configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **dnis group** customer profile configuration command to include a group of DNIS numbers in a customer profile or discriminator.

Examples

The following example includes the DNIS group called customer1dnis in the customer1 customer profile:

```
resource-pool profile customer customer1
 dnis group name customer1dnis
```

Related Commands

Command	Description
dialer dnis group	Creates a DNIS group.
resource-pool profile customer	Creates a customer profile.

ds0 busyout (channel)

To busyout one or more digital signal level 0s (DS0s), use the **ds0 busyout** command in controller configuration mode. To cancel busyout on a DS0, use the **no** form of this command.

ds0 busyout *ds0*

no ds0 busyout *ds0*

Syntax Description

ds0	DS0 number listed as a single channel, or listed as a channel range with the starting channel number and the ending channel number seperated by a hyphen. The range of numbers can be from 1 to 24 for T1. For example, from 1 to 10, or from 10 to 24.

Command Default

Disabled

Command Modes

Controller configuration

Command History

Release	Modification
11.3(2)AA	This command was introduced, and supported T1 and T3 only.
12.0	This command was integrated into Cisco IOS Release 12.0, and supported the E1and DMM HMM (Double Modem Module [12] Hex Modem Module [6]).

Usage Guidelines

Use the **ds0 busyout** command when you to busyout a one or more DS0s (channels). If there is an active call, the software waits until the call terminates by a disconnection; then the DS0 is busied out. First you must specify the T1 line (port) containing the 24 DS0s, using the **controller T1** command.

To busyout all DS0s on a trunk card or all modems on a modem card, use the **busyout** privileged EXEC command.

To display the busyout information, use the **show busyout** privileged EXEC command.

Note The **ds0 busyout** command only applies to **cas-group** command configurations for channel-associated signaling. This command has no effect on **pri-group** command configurations.

Examples

In this example, the controller T1 is configured with cas-group (channel-associated signaling). The following example removes DS0s 1 through 10 from dialup services. These DS0s are assigned to the T1 port (line) in shelf 6, slot 0, port 0:

```
controller t1 6/0/0
 ds0 busyout 1-10
 exit
```

Related Commands

Command	Description
busyout	Informs the central-office switch that a channel is out of service.
modem busyout	Disables a modem from dialing or answering calls whereby the disabling action is not executed until the active modem returns to an idle state.
modem busyout-threshold	Maintains a balance between the number of DS0s and modems.
modem shutdown	Abruptly shuts down an active or idle modem installed in an access server or router.
show busyout	Displays the busyout status for a card on the dial shelf.
show dial-shelf	Displays information about the dial shelf, including clocking information.

ds0 busyout-threshold

To define a threshold to maintain a balance between the number of DS0s and modems, use the **ds0 busyout-threshold** command in global configuration mode. To remove the threshold, use the **no** form of this command.

Cisco AS5300 and AS5800 Access Servers Only

ds0 busyout-threshold *threshold-number*

no ds0 busyout-threshold *threshold-number*

Note This command is the same as the **modem busyout-threshold** command for the Cisco AS5350 and AS5400 access servers.

Syntax Description

threshold-number	Number of modems that are free when the router should enforce the stipulation that the number of free DS0 lines is less than or equal to the number of modems.

Command Default

No threshold is defined.

Command Modes

Global configuration

Command History

Release	Modification
11.3(2)AA	This command was introduced as **modem busyout-threshold**.
12.2	This command was changed to **ds0 busyout-threshold** for the Cisco AS5300 and AS5800 access servers.

Usage Guidelines

The **ds0 busyout-threshold** command functionality is also often termed **autobusyout**. This command applies to all DS0 lines coming into the router and counts all free modems in all pools.

The **ds0 busyout-threshold** command periodically checks to see if the number of free modems is less that the user specified threshold and if it is it ensures the number of free DS0 channels is less than or equal to the number of modems.

This command should only be used where excess calls to one router are forwarded by the exchange to an additional router on the same exchange group number.

Since the **ds0 busyout-threshold** command checks only periodically, the threshold should be greater than the number of calls the user expects to receive in 1 minute plus a safety margin. For example, if the user receives an average of 10 calls per minute, then a threshold of 20 would be advised. Very small thresholds should be avoided since they do not allow sufficient time for the exchange to respond to out-of-service notifications from the router, and callers may receive busy signals when free modems are all used.

Caution The number of DS0 lines in normal operating conditions should be approximately equal to the number of modems (for example, within 30). If it is not, this will cause a lot of messaging traffic to the exchange and may cause active calls to be dropped. This is not a concern for short periods, that is, when modem cards are replaced.

On T3 controllers, any contained T1 controllers that are not in use should be undeclared to remove them from the **autobusyout** list.

Examples

The following example shows how you might configure the **ds0 busyout-threshold** command:

```
ds0 busyout-threshold 30
```

Related Commands

Command	Description
busyout	Informs the central-office switch that a channel is out-of-service.
ds0 busyout (channel)	Forces a DS0 time slot on a controller into the busyout state.
modem busyout	Disables a modem from dialing or answering calls whereby the disabling action is not executed until the active modem returns to an idle state.
modem shutdown	Abruptly shuts down an active or idle modem installed in an access server or router.

ds0-group (controller e1)

To define E1 channels for compressed voice calls and the channel-associated signaling (CAS) method by which the router connects to the PBX or PSTN, enter the **ds0-group** command in controller configuration mode. To remove the group and signaling setting, use the **no** form of this command.

ds0-group *channel* **timeslots** *range* **type** *signal*

no ds0-group *channel* **timeslots** *range* **type** *signal*

Syntax Description

channel	Specifies a single channel group number. Replace the *channel* variable with a number from 0 through 30.
timeslots *range*	Specifies a time-slot range, which can be from 1 through 31. You can specify a time-slot range (for example, 1-31), individual time-slots separated by commas (for example 1, 3, 5), or a combination of the two (for example 1-14, 15, 17-31). The sixteenth time slot is reserved for out-of-band signaling.
type *signal*	Specifies the type of channel-associated signaling. Configure the signal type that your central office uses. Replace the *signal* argument with one of the following signal types: • **r2-analog** [**r2-compelled** [**ani**] | **r2-non-compelled** [**ani**] | **r2-semi-compelled** [**ani**]] • **r2-digital** [**r2-compelled** [**ani**] | **r2-non-compelled** [**ani**] | **r2-semi-compelled** [**ani**]] • **r2-pulse** [**r2-compelled** [**ani**] | **r2-non-compelled** [**ani**] | **r2-semi-compelled** [**ani**]] The following descriptions are provided for the previous three R2 syntax bullets: • **r2-analog**—Specifies R2 ITU Q411 analog line signaling, which reflects the on/off switching of a tone in frequency-division multiplexing circuits (before TDM circuits were created). The tone is used for line signaling. • **r2-digital**—Specifies R2 ITU Q421 digital line signaling, which is the most common signaling configuration. The A and B bits are used for line signaling. • **r2-pulse**—Specifies R2 ITU supplement 7 pulse line signaling, which is a transmitted pulse that indicates a change in the line state. • **r2-compelled** [**ani**]—Specifies R2 compelled register signaling. You can also specify provisioning the ANI address option. • **r2-non-compelled** [**ani**]—Specifies R2 noncompelled register signaling. • **r2-semi-compelled** [**ani**]—Specifies R2 semicompelled register signaling.

Command Default

No channel-associated signaling is configured on the controller. All R2 signaling types have DNIS turned on by default.

Command Modes

Controller configuration

Command History

Release	Modification
11.3MA	The command was introduced as the **voice-group** command on the Cisco MC3810 concentrator.
12.0(5)XK	The command was implemented on the Cisco 2600 and Cisco 3600 series with a different name and some keyword modifications.
12.0(7)T	The command was implemented on the Cisco 2600 and Cisco 3600 series with a different name and some keyword modifications.
12.1(2)XH	The command was modified for E1 R2 signaling.
12.1(3)T	The command was modified for E1 R2 signaling.
12.2	The command was modified to exclude **sas** keywords**.** The Single Attachment Station (SAS) CAS options of **sas-loop-start** and **sas-ground-start** are not supported as a type of signaling for the DS0 group.

Usage Guidelines

Use this command to configure support for incoming and outgoing call signals (such as on-hook and off-hook) on each E1 controller.

If you specify the time-slot range 1-31, the system software automatically uses the sixteenth time slot to transmit the channel-associated signaling.

The signaling you configure on the access server must match the signaling used by the central office. For example, if the central office switch is forwarding R2 analog signaling to a Cisco 2600 or 3600 series router, the E1 controller on the router must also be configured for R2 analog signaling (**r2-analog**).

All R2 signaling options have DNIS support turned on by default. If you enable the **ani** option, the collection of DNIS information is still performed. Specifying the **ani** option does not disable DNIS. DNIS is the number being called. ANI is the caller's number. For example, if you are configuring router A to call router B, the DNIS number is router B and the ANI number is router A. ANI is very similar to Caller ID.

To customize the R2 signaling parameters, refer to the **cas-custom** controller configuration command. When you enable the **ds0-group** command, the **cas-custom** command is automatically set up to be polled for configuration information. However, unless you enable or turn on specific features with the **ds0-custom** command, the cas-custom feature has an empty set of signaling parameters.

DNIS is automatically collected for modem pools and R2 tone signaling. You do not need to specify the collection of DNIS information with the **ds0-group** command. However, if you are using non-R2 tone signaling, the system must be manually configured to collect DNIS information. For non-R2 CAS signaling, DNIS collection is done only for E&M-fgb.

Examples

In most cases, you will configure the same channel-associated signaling on each E1 controller. The following examples configure signaling and customized parameters on controller E1 2 using the **ds0-group** and **cas-custom** controller configuration commands.

The actual channel-associated signaling is configured on the sixteenth time slot, which is the reason why this time slot does not come up in the following output.

```
Router(config)# controller e1 2
Router(config-controller)# ds0-group 1 timeslots 1-31 type r2-digital r2-compelled ani
```

```
Router(config-controller)#

%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 1 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 2 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 3 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 4 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 5 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 6 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 7 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 8 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 9 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 10 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 11 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 12 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 13 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 14 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 15 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 17 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 18 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 19 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 20 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 21 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 22 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 23 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 24 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 25 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 26 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 27 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 28 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 29 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 30 is up
%DSX0-5-RBSLINEUP: RBS of controller 0 timeslot 31 is up
```

The following example shows all the supported E1 signaling types on a Cisco 2600 or 3600 series router.

```
Router(config-controller)# ds0-group 1 timeslots 1-31 type ?

 e&m-fgb              E & M Type II FGB
 e&m-fgd              E & M Type II FGD
 e&m-immediate-start  E & M Immediate Start
 fxs-ground-start     FXS Ground Start
 fxs-loop-start       FXS Loop Start
 p7                   P7 Switch
 r2-analog            R2 ITU Q411
 r2-digital           R2 ITU Q421
 r2-pulse             R2 ITU Supplement 7
 sas-ground-start     SAS Ground Start
 sas-loop-start       SAS Loop Start
```

Note Cisco IOS Releases later than 12.2 do not support the Single Attachment Station (SAS) CAS options of **sas-loop-start** and **sas-ground-start**.

```
Router(config-controller)# cas-group 1 timeslots 1-31 type r2-analog ?

 r2-compelled       R2 Compelled Register Signalling
 r2-non-compelled   R2 Non Compelled Register Signalling
 r2-semi-compelled  R2 Semi Compelled Register Signalling
 <cr>
```

R2 signaling parameters can be customized with the **cas-custom** controller configuration command:

```
Router(config-controller)# cas-custom 1
Router(config-ctrl-cas)# ?
```

```
CAS custom commands:
 caller-digits  Digits to be collected before requesting CallerID
 category       Category signal
 country        Country Name
 default        Set a command to its defaults
 exit           Exit from cas custom mode
 invert-abcd    invert the ABCD bits before tx and after rx
 metering       R2 network is sending metering signal
 nc-congestion  Non Compelled Congestion signal
 no             Negate a command or set its defaults
```

encap-sequence

To assign an encapsulation sequence number to a priority class in a multiclass multilink PPP bundle, use the **encap-sequence** command in policy-map class configuration mode. To reset the default value, use the **no** form of this command.

encap-sequence [*sequence-id* | **none**]

no encap-sequence *sequence-id*

Syntax Description

sequence-id	Assigns a unique encapsulation sequence number to priority class in a multiclass multilink PPP bundle. Valid range is from 0 to 3.
none	Specifies that a certain priority class is classified as or is assigned the highest priority, and packets are not encapsulated with a sequence number for multiclass multilink PPP.

Command Default

Sequence numbers are not assigned to priority classes.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.2(31)SB2	This command was introduced and implemented on the Cisco 10000 series router for the PRE2.

Usage Guidelines

The **encap-sequence** command allows you to assign sequence numbers to priority classes in a policy map for multiclass multilink PPP encapsulation. This command is only supported on the PRE2.

A class with a multiclass multilink PPP sequence number must have an associated queue action such as bandwidth and shape. The sequence number assigned to each priority class must be unique.

The default sequence number for class-default is 0 and it is not configurable.

If you do not assign a sequence number to a priority class, the priority queue packets use PPP encapsulation. Interleaving is allowed for priority traffic regardless of the encapsulated sequence number configuration.

Examples

The following example shows that class voice has the highest priority and that packets are not encapsulated with a sequence number for multiclass multilink PPP.

```
Router(config)# policy-map prec1
Router(config-pmap)# class voice
Router(config-pmap-c)# priority
Router(config-pmap-c)# police 128
Router(config-pmap-c)# encap-sequence none
Router(config-pmap-c)# exit
Router(config-pmap)# class video
```

```
Router(config-pmap-c)# bandwidth 1000
Router(config-pmap-c)# police 1000
Router(config-pmap-c)# encap-sequence 1
Router(config-pmap-c)# exit
Router(config-pmap)# class game
Router(config-pmap-c)# bandwidth 1000
Router(config-pmap-c)# encap-sequence 2
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
```

Related Commands

Command	Description
show ppp multilink	Displays information for multilink PPP bundles.

encapsulation cpp

Note Effective with Cisco IOS Release 12.3(4)T, the **encapsulation cpp** command is no longer available in Cisco IOS software.

To enable encapsulation for communication with routers or bridges using the Combinet Proprietary Protocol (CPP), use the **encapsulation cpp** command in interface configuration mode. To disable CPP encapsulation, use the **no** form of this command.

encapsulation cpp

no encapsulation cpp

Syntax Description

This command has no arguments or keywords.

Command Default

CPP encapsulation disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.3(4)T	This command was removed and is no longer available in Cisco IOS software.

Usage Guidelines

Use this command to communicate over an ISDN interface with Cisco 700 and 800 series (formerly Combinet) routers that do not support PPP but do support CPP.

Most Cisco routers support PPP. Cisco routers can communicate over ISDN with these devices by using PPP encapsulation, which supports both routing and fast switching.

The Cisco 700 and 800 series routers support only IP, IPX, and bridging. For AppleTalk, these Cisco routers automatically perform half-bridging.

This command is supported on ISDN BRIs and PRIs only.

Examples

The following example configures BRI interface 0 to communicate with a router or bridge that does not support PPP:

```
interface bri 0
 encapsulation cpp
 cpp callback accept
 cpp authentication
```

The following example configures PRI serial interface 1/1:23 to communicate with a router or bridge that does not support PPP:

```
controller t1 1/1
 framing esf
 linecode b8zs
 pri-group timeslots 1-23
 isdn switchtype primary-4ess
!
interface Serial1/1:23
 encapsulation cpp
 cpp callback accept
 cpp authentication
```

Related Commands

Command	Description
cpp authentication	Enables negotiation of authentication with a router or bridge that supports the CPP and that is calling in to this router.
cpp callback accept	Enables the router to accept callback from a router or bridge that supports the CPP.

failover group-number

To configure shelf redundancy for Cisco AS5800 universal access servers, use the **failover group-number** command in redundancy configuration mode. To disable redundancy, use the **no** form of this command.

failover group-number *group-code*

no failover group-number *group-code*

Syntax Description

group-code	The failover group code. An integer that identifies a redundant pair of router shelves. Each member of the pair must be configured with the same group code. When failover mode is enabled, this group code is sent in place of the router MAC address.

Command Default

Redundancy is not enabled.

Command Modes

Redundancy configuration

Command History

Release	Modification
12.1(5)XV1	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

This command must be configured on both router shelves. The *group-code* argument is used by the system controller and must be the same for both router shelves forming the redundant pair.

For successful failover to occur, both router-shelf configurations must be synchronized. Configure each router shelf separately, as active and backup respectively, with the same configuration except for the IP address on egress interfaces.

Note Test the backup router shelf configuration before deployment in a production environment.

Examples

The following example assigns the configured router shelf to the redundancy pair designated as 25. These commands must be issued on both router shelves in the redundant router-shelf pair:

```
Router(config)# redundancy
Router(config-red)# failover group-number 25
```

Related Commands

Command	Purpose
redundancy	Enters redundancy mode for further configuration.
show redundancy	Displays current or historical status and related information and displays shelf-redundancy status.

firmware filename

To use a different DSL firmware other than the embedded one, use the **firmware filename** command in controller configuration mode. To revert back to the embedded firmware, use the **no** form of this command.

firmware filename flash:*firmware-filename*

no firmware filename

Syntax Description

firmware-filename	Filename for the binary firmware file to be upgraded.
flash:	Compact flash.

Defaults

The default uses the embedded firmware.

Command Modes

Configuration controller mode.

Command History

Release	Modification
15.0(1)M1	This command was introduced.

Usage Guidelines

The specified firmware will be used after **shutdown** and **no shutdown** of the controller.

Examples

The following example shows how to upgrade the firmware file.

```
Router(config)#controller vdsl 0/2/0
Router(config-controller)#firmware filename flash:myvdsl.bin
```

Related Commands

Command	Description
debug vdsl daemon	Debugs the VDSL firmware download state, DSL line training progress, and VDSL interface status

firmware location

To download firmware into the modems, use the **firmware location** command in Service Processing Element (SPE) configuration mode. To revert the router to the system embedded image default, use the **no** form of this command.

firmware location [*IFS*]*filename*

no firmware location

Syntax Description

IFS:	(Optional) IOS file specification (IFS), which can be any valid IFS on any local file system. Examples of legal specifications include: • **bootflash:**—Loads the firmware from a separate Flash memory device. • **flash:**—Loads the firmware from the Flash NVRAM located within the router. • **system:/**—Loads the firmware from a built-in file within the Cisco IOS image. The optional forward slash (**/**) and system path must be entered with this specification. Use the **dir all-filesystems** EXEC command to display legal IFSs.
filename	The firmware filename. When *filename* is entered without an IFS specification, this name defaults to the file in Flash memory.

Command Default

Downloads SPE firmware in Flash memory.

Command Modes

SPE configuration

Command History

Release	Modification
12.0(4)XI1	This command was introduced on the Cisco AS5200, Cisco AS5300, and Cisco AS5800.
12.0(6)T	This command was integrated into Cisco IOS Release 12.0(6)T.
12.0(7)T	This command was implemented on the Cisco AS5300 and Cisco AS5800 for MICA technologies modems.
12.1(1)XD	This command was implemented on the Cisco AS5400 for the NextPort dial feature card (DFC).
12.1(3)T	This command was implemented on the Cisco AS5400 for the NextPort DFC and on the Cisco AS5800 for the universal port card (UPC).
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

Use the **firmware location** SPE configuration command to download firmware into your modems. This command specifies the location of the firmware file *and* downloads the firmware in the range of SPEs specified, depending on the states configured by the **firmware upgrade** command. Use the **firmware location** command with the **firmware upgrade** command. The entire SPE is affected by the **firmware location** command.

The latest SPE firmware image can usually be retrieved from Cisco.com. You must first copy the SPE image from a TFTP server to Flash memory using the **copy tftp flash** command.

The **firmware location** command is a configuration command and must be saved into the system configuration using the **write memory** command; otherwise, at the next reboot downloading of the specified firmware will not occur.

The **firmware location** command was first supported in Cisco IOS Release 12.0(4)XI1. For earlier images, use the **copy** command. For the Cisco IOS Release 12.0(4)XI1 images, the **copy flash modem** command is disabled for MICA technologies modems and newer versions of the 56-kbps Microcom modems. The older V.34 Microcom modems still use the **copy** command for downloading in Cisco IOS Release 12.0(4)XI1 images.

Note This command should be used when traffic is low because the **firmware location** download will not begin until the modems have no active calls. Otherwise, use the **firmware upgrade** command to customize the scheduling of modem downloads for your needs.

You cannot use the **firmware location** command on SPEs that are in the Bad state.

Examples

The following example shows how to display all legal IFSs:

```
Router# dir all-filesystems

Directory of nvram:/

  121  -rw-        1543              <no date>  startup-config
  122  ----           5              <no date>  private-config

126968 bytes total (125368 bytes free)

Directory of system:/

    6  dr-x           0              <no date>  memory
    1  -rw-        2929              <no date>  running-config
    2  dr-x           0              <no date>  ucode
   17  dr-x           0              <no date>  vfiles

No space information available

Directory of flash:/

    1  -rw-    12575032              <no date>  c5300-js-mz.122-11.T

16777216 bytes total (4202120 bytes free)

Directory of bootflash:/

    1  -rw-     1155864              <no date>  c5300-boot-mz.113-10.T.bin
    2  -rw-      381540              <no date>  mica-modem-pw.2.6.2.0.bin
    3  -rw-      384056              <no date>  pw2621.ios
8388608 bytes total (5682340 bytes free)
```

```
Directory of lex:/

No files in directory

No space information available
```

The following example shows how to enter the SPE configuration mode, set the range of SPEs, specify the firmware file location in Flash memory, download the file to the SPEs, and display a status report using the **show spe** EXEC command:

```
Router# configure terminal
Router(config)# spe 7/0 7/17
Router(config-spe)# firmware location flash:np-6-75
Router(config-spe)# firmware upgrade busyout
Started downloading firmware flash:np-6-75.spe
Router(config-spe)# exit
Router# show spe 7
.
.
.
                     SPE          SPE     SPE  SPE   Port         Call
SPE#    Port #       State        Busyout Shut Crash State        Type
7/00    0000-0005    ACTIVE             1    0     0 BBBBBB       _______
7/01    0006-0011    DOWNLOAD           1    0     0 bbbbbb       _______
7/02    0012-0017    DOWNLOAD           1    0     0 bbbbbb       _______
7/03    0018-0023    DOWNLOAD           1    0     0 bbbbbb       _______
.
.
.
```

The following configuration example specifies a firmware file located in Flash memory:

```
spe 1/0 1/8
 firmware location np-spe-upw-1.0.1.2.bin
```

The following configuration example shows how to download firmware that is not bundled with the Cisco IOS image:

```
spe 1/2 1/4
 firmware location flash:portware.2620.ios
```

The following configuration example shows how to download firmware that is bundled with the Cisco IOS image:

```
spe 2/9 2/9
 firmware location system:/ucode/microcom_firmware
```

Related Commands

Command	Description
clear port	Resets the NextPort port and clears any active call.
clear spe	Reboots all specified SPEs.
copy	Copies any file from a source to a destination.
copy tftp flash	Copies the SPE image from a TFTP server to the Flash memory.
firmware upgrade	Specifies the method in which the SPE will be downloaded.
show spe version	Displays the firmware version on an SPE.
spe download maintenance	Performs download maintenance on SPEs that are marked for recovery.
spe recovery	Sets an SPE port for recovery.

firmware upgrade

To modify the way in which the service processing element (SPE) will be downloaded, use the **firmware upgrade** command in SPE configuration mode. To revert to the default SPE firmware upgrade option, busyout, use the **no** form of this command.

firmware upgrade {**busyout** | **recovery** | **reboot**}

no firmware upgrade

Cisco AS5350, Cisco AS5400, and Cisco AS5800

firmware upgrade [**busyout** | **download-maintenance** | **reboot**]

Syntax Description

busyout	Upgrades when all calls are terminated on the SPE.
recovery	Upgrades during download maintenance time.
reboot	Upgrades at the next reboot.
download-maintenance	Upgrades during download maintenance time.

Command Default

An upgrade occurs when all calls are terminated on the SPE (**busyout**).
For the Cisco AS5350, Cisco AS5400, and Cisco AS5800 there is no default.

Command Modes

SPE configuration

Command History

Release	Modification
12.0(4)XI1	This command was introduced on the Cisco AS5200, Cisco AS5300, and Cisco AS5800.
12.0(6)T	This command was integrated into Cisco IOS Release 12.0(6)T.
12.0(7)T	This command was implemented on the Cisco AS5300 and Cisco AS5800 for MICA technologies modems.
12.1(1)XD	This command was implemented on the Cisco AS5400 for the NextPort dial feature card (DFC).
12.1(3)T	This command was implemented on the Cisco AS5400 for the NextPort DFC and Cisco AS5800 for the universal port card (UPC).
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

Three methods of upgrade are available: busyout, reboot, and download-maintenance or recovery.

The **reboot** keyword requests the Cisco access servers to upgrade SPE firmware at the next reboot.

The **busyout** keyword upgrades SPE firmware after waiting for all calls to be terminated on an SPE.

The **download-maintenance** or **recovery** keyword requests SPE firmware download during maintenance time.

Use this command in conjunction with the **firmware location** command and the **spe download maintenance** command.

The SPE **firmware location** command is designed to integrate all continuous ranges of SPEs containing the same firmware location. However, the **firmware upgrade** command does not affect the ranges of SPEs. As such, all SPEs within the ranges of SPEs must have the same firmware upgrade mode or the router uses the default upgrade mode to busyout state. If you want to upgrade a single SPE within an existing range of SPEs with a different upgrade mode than is currently configured, you must first change the upgrade mode for the entire range of SPEs and then change the firmware location for the specific SPE being upgraded. Furthermore, each time you merge ranges of SPEs due to configuration changes, verify that the configuration of the SPE firmware upgrade remains effective to what is desired.

Examples

The following example sets the SPEs and specifies the firmware upgrade to take place once all calls are terminated on the SPE:

```
Router(config)# spe 1/03
Router(config-spe)# firmware location np-spe-upw-1.0.1.2.bin
Router(config-spe)# firmware upgrade busyout
```

If the **busyout upgrade** command is specified, or if no upgrade mode is specified, the SPE modems are set into a "pending download" state when you use the **firmware location** command on the specified SPE. The pending download state prevents any modem in that state to be allocated for new calls until the state is cleared. Modems with active calls remain active for their call durations, but enter the pending download state when they terminate. This pending download state can be cleared only when the SPE is finally downloaded. When all modems within the SPE are in the pending download state and no active calls remain on the SPE, the SPE is reloaded. The **busyout** option is the fastest way to upgrade modems on an active router but can severely impact the capacity of the router during the upgrade. The following example sets the default option for the firmware upgrade process:

```
Router(config-spe)# firmware upgrade busyout
```

If reboot upgrade is specified, the SPE modems are not reloaded to the new firmware location until the router is rebooted. The reboot upgrade option is useful for routers that need to have their SPE upgraded and that also will be rebooted for maintenance. When the new firmware is configured, the configuration takes effect after the reboot takes place. The following example sets the firmware upgrade reboot:

```
Router(config-spe)# firmware upgrade reboot
```

If recovery upgrade is specified, the SPE modems are reloaded based on the modem recovery algorithm. Only when no active calls exist on the SPE does the firmware download take place. Furthermore, at the time configured with the **modem recovery maintenance** command, the modem recovery maintenance process attempts, in a controller fashion, to reload the modems by busying out the modems for a window duration of time to make the download take place. Refer to the modem recovery documentation for more information. The recovery upgrade option upgrades modems on an active router with the least impact. Capacity is kept at a maximum. However, this option may take a few days for all modems to be reloaded to the new firmware location. The following example sets the system for a firmware upgrade recovery:

```
Router(config-spe)# firmware upgrade recovery
```

For the Cisco AS5350, Cisco AS5400, or Cisco AS5800, use the following syntax to set the system for a firmware upgrade recovery:

```
Router(config-spe)# firmware upgrade download-maintenance
```

Related Commands

Command	Description
firmware location	Downloads firmware into the modems from this file location.
modem recovery maintenance	Specifies the scheduled modem maintenance recovery behavior.
show spe version	Displays the firmware version on an SPE.
spe download maintenance	Performs download maintenance on SPEs that are marked for recovery.
spe recovery	Sets an SPE port for recovery.

flowcontrol

To set the method of data flow control between the terminal or other serial device and the router, use the **flowcontrol** command in line configuration mode. To disable flow control, use the **no** form of this command.

flowcontrol {**none** | **software** [**lock**] [**in** | **out**] | **hardware** [**in** | **out**]}

no flowcontrol {**none** | **software** [**lock**] [**in** | **out**] | **hardware** [**in** | **out**]}

Syntax Description

none	Turns off flow control.
software	Sets software flow control.
lock	(Optional) Makes it impossible to turn off flow control from the remote host when the connected device *needs* software flow control. This option applies to connections using the Telnet or rlogin protocols.
[**in** | **out**]	(Optional) Specifies the direction of software or hardware flow control: the keyword **in** causes the Cisco IOS software to listen to flow control from the attached device, and the **out** keyword causes the software to send flow control information to the attached device. If you do not specify a direction, both directions are assumed.
hardware	Sets hardware flow control. For more information about hardware flow control, see the hardware manual that was shipped with your router.

Command Default

Flow control is disabled.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

When software flow control is set, the default stop and start characters are Ctrl-S and Ctrl-Q (XOFF and XON). You can change them using the **stop-character** and **start-character** commands.

If a remote Telnet device requires software flow control, the remote system should not be able to turn it off. Using the **lock** option makes it possible to refuse “dangerous” Telnet negotiations if they are inappropriate.

Examples

The following example sets hardware flow control on line 7:

```
line 7
 flowcontrol hardware
```

Related Commands

Command	Description
start-character	Sets the flow control start character.
stop-character	Sets the flow control stop character.

group-range

To create a list of member asynchronous interfaces (associated with a group interface), use the **group-range** command in interface configuration mode. To remove an interface from the member list, use the **no** form of this command.

group-range *low-end-of-interfacerange high-end-of-interfacerange*

no group-range *interface*

Syntax Description

low-end-of-interfacerange	Beginning interface number to be made a member of the group interface.
high-end-of-interfacerange	Ending interface number to be made a member of the group interface.
interface	Interface number to be removed from the group interface.

Command Default

No interfaces are designated as members of a group.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Using the **group-range** command, you create a group of asynchronous interfaces that are associated with a group asynchronous interface on the same device. This group interface is configured by using the **interface group-async** command. This one-to-many structure allows you to configure all associated member interfaces by entering one command on the group interface, rather than entering this command on each interface. You can customize the configuration on a specific interface by using the **member** command. Interface numbers can be removed from the interface group using the **no group-range** command.

Examples

The following example defines interfaces 2, 3, 4, 5, 6, and 7 as members of asynchronous group interface 0:

```
interface group-async 0
 group-range 2 7
```

Related Commands

Command	Description
interface group-async	Creates a group interface that will serve as master, to which asynchronous interfaces can be associated as members.
member	Alters the configuration of an asynchronous interface that is a member of a group.

interface bri

To configure a BRI interface and enter interface configuration mode, use the **interface bri** command in global configuration mode.

Cisco 7200 Series and 7500 Series Routers

interface bri *number*

interface bri *slot*/*port*

Cisco 7200 Series and 7500 Series Routers with BRI Subinterfaces Only

interface bri *number*.*subinterface-number* [**multipoint** | **point-to-point**]

interface bri *slot*/*port*.*subinterface-number* [**multipoint** | **point-to-point**]

X.25 on an ISDN BRI Interface

interface bri *number*:**0**

interface bri *slot*/*port*:**0**

Syntax Description

number	Port, connector, or interface card number. The numbers are assigned at the factory at the time of installation or when added to a system, and can be displayed with the **show interfaces** command.
slot/*port*	On the Cisco 7200 series, slot location and port number of the interface. The slash mark is required.
.*subinterface-number*	Subinterface number in the range from 1 to 4,294,967,293. The *number* that precedes the period (.) must match the *number* this subinterface belongs to. The period is required.
multipoint | **point-to-point**	(Optional) Specifies a multipoint or point-to-point subinterface. The default is **multipoint**.
:0	Subinterface created by applying the **isdn x25 static-tei** and the **isdn x25 dchannel** commands to the specified BRI interface. This interface must be configured for X.25.

Command Default

The default mode for subinterfaces is multipoint.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
11.2F	This command was enhanced with the capability to carry X.25 traffic on the D channel.
11.2P	This command was modified to include slot/port syntax for the PA-8B-ST and PA-4B-U port adapters on the Cisco 7200 series.

Usage Guidelines

Subinterfaces can be configured to support partially meshed Frame Relay networks. (Refer to the Frame Relay chapters in the *Cisco IOS Wide-Area Networking Configuration Guide.*)

To specify the BRI interface that is created by enabling X.25 on a specified ISDN BRI interface, use the **interface bri** global configuration command with a subinterface 0 specification.

Examples

The following example configures BRI 0 to call and receive calls from two sites, use PPP encapsulation on outgoing calls, and use Challenge Handshake Authentication Protocol (CHAP) authentication on incoming calls:

```
interface bri 0
 encapsulation ppp
 no keepalive
 dialer map ip 172.16.36.10 name EB1 234
 dialer map ip 172.16.36.9 name EB2 456
 dialer-group 1
 isdn spid1 41346334600101 4633460
 isdn spid2 41346334610101 4633461
 isdn T200 1000
 ppp authentication chap
```

The following example creates a BRI 0:0 interface for X.25 traffic over the D channel and then configures the new interface to carry X.25 traffic:

```
interface bri 0
 isdn x25 dchannel
 isdn x25 static-tei 8
!
interface bri 0:0
 ip address 10.1.1.2 255.255.255.0
 x25 address 31107000000100
 x25 htc 1
 x25 suppress-calling-address
 x25 facility windowsize 2 2
 x25 facility packetsize 256 256
 x25 facility throughput 9600 9600
 x25 map ip 10.1.1.3 31107000000200
```

Related Commands

Command	Description
dialer-group	Controls access by configuring an interface to belong to a specific dialing group.
dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites.
encapsulation	Sets the encapsulation method used by the interface.

Command	Description
isdn spid1, isdn spid2	Defines the SPID number that has been assigned by the ISDN service provider for the B1 channel.
ppp bap call	Sets PPP BACP call parameters.
show interfaces bri	Displays information about the BRI D channel or about one or more B channels.

interface dialer

To define a dialer rotary group, use the **interface dialer** command in global configuration mode.

interface dialer *dialer-rotary-group-number*

no interface dialer *dialer-rotary-group-number*

Syntax Description

dialer-rotary-group-number	Number of the dialer rotary group in the range from 0 to 255.

Command Default

No dialer rotary groups are predefined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Dialer rotary groups allow you to apply a single interface configuration to a set of physical interfaces. This capability allows a group of interfaces to be used as a pool of interfaces for calling many destinations.

Once the interface configuration is propagated to a set of interfaces, those interfaces can be used to place calls using the standard dial-on-demand routing (DDR) criteria. When multiple destinations are configured, any of these interfaces can be used for outgoing calls.

Dialer rotary groups are useful in environments that require multiple calling destinations. Only the rotary group needs to be configured with the **dialer map** commands. The only configuration required for the interfaces is the **dialer rotary-group** command indicating that each interface is part of a dialer rotary group.

Although a dialer rotary group is configured as an interface, it is not a physical interface. Instead, it represents a group of interfaces. Interface configuration commands entered after the **interface dialer** command will be applied to all physical interfaces assigned to specified rotary groups. Individual interfaces in a dialer rotary group do not have individual addresses. The dialer interface has a protocol address, and that address is used by all interfaces in the dialer rotary group.

Examples

The following example identifies interface dialer 1 as the dialer rotary group leader. Interface dialer 1 is not a physical interface, but represents a group of interfaces. The interface configuration commands that follow apply to all interfaces included in this group.

```
interface dialer 1
 encapsulation ppp
 authentication chap
 dialer in-band
 ip address 10.2.3.4
 dialer map ip 10.2.2.5 name YYY 14155553434
 dialer map ip 10.3.2.6 name ZZZ
```

interface multilink

To create a multilink bundle and enter multilink interface configuration mode to configure the bundle, use the **interface multilink** command in global configuration mode. To remove a multilink bundle, use the **no** form of this command.

interface multilink *multilink-bundle-number*

no interface multilink

Syntax Description

multilink-bundle-number	Number of the multilink bundle (a nonzero number).

Command Default

No multilink bundles are created.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.0	This command was introduced on the PRE1 for the Cisco 10000 series router.
12.2(16)BX	This command was implemented on the PRE2.
12.2(28)SB	This command was integrated in Cisco IOS Release 12.2(28)SB for the PRE2.
12.2(31)SB2	This command was introduced on the PRE3 and the range of valid values for multilink interfaces was expanded on the PRE3.

Usage Guidelines

Cisco 10000 Series Router

The following describes the valid multilink interface values for the Cisco 10000 series router:

- 1 to 9999—(PRE2) Cisco IOS Release 12.2(28)SB and later releases
- 1 to 9999 and 65,536 to
  - 1 to 9999 and 65,536 to 2,147,483,647 (Cisco IOS Release 12.2(31)SB2 and later releases)
  - 1 to 9999 and 65,536 to 2,147,483,647 (Cisco IOS Release 12.2(31)SB2 and later releases)

valid multilink-bundle-number values are from 1 to 2,147,483,647.

Examples

The following example creates multilink bundle 1:

```
interface multilink 1
 ip address 192.168.11.4 255.255.255.192
 encapsulation ppp
 ppp multilink
 keepalive
```

Related Commands

Command	Description
ppp multilink fragment disable	Disables packet fragmentation.
ppp multilink group	Restricts a physical link to joining only a designated multilink-group interface.

interface serial

To specify a serial interface created on a channelized E1 or channelized T1 controller (for ISDN PRI, channel-associated signaling, or robbed-bit signaling), use the **interface serial** command in global configuration mode.

Cisco 7200 Series and Cisco 7500 Series Routers

interface serial *slot*/*port*:*timeslot*

no interface serial *slot*/*port*:*timeslot*

Cisco AS5200 Series and Cisco 4000 Series Access Servers

interface serial *controller-number*:*timeslot*

no interface serial *controller-number*:*timeslot*

Syntax Description

slot/*port*	Slot number and port number where the channelized E1 or T1 controller is located. The slash mark is required.
:*timeslot*	For ISDN, the D channel time slot, which is the **:23** channel for channelized T1 and the **:15 channel** for channelized E1. PRI time slots are in the range from 0 to 23 for channelized T1 and in the range from 0 to 30 for channelized E1. For channel-associated signaling or robbed-bit signaling, the channel group number. The colon is required. On a dual port card, it is possible to run channelized on one port and primary rate on the other port.
controller-number	Channelized E1 or T1 controller number.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You must explicitly specify a serial interface. The D channel is always the **:23** channel for T1 and the **:15** channel for E1.

Examples

The following example configures channel groups on time slots 1 to 11 and ISDN PRI on time slots 12 to 24 of T1 controller 0. Then the examples configures the first two channel groups as serial interfaces 0:0 and 0:1.

```
controller t1 0
channel-group 0 timeslot 1-6
channel-group 1 timeslot 7
channel-group 2 timeslot 8
channel-group 3 timeslot 9-11
pri-group timeslots 12-24
!
interface serial 0:0
ip address 172.18.13.2 255.255.255.0
encapsulation ppp
!
interface serial 0:1
ip address 172.18.13.3 255.255.255.0
encapsulation ppp
```

The following example configures ISDN PRI on T1 controller 4/1 and then configures the D channel on the resulting serial interface 4/1:23:

```
controller t1 4/1
framing crc4
linecode hdb3
pri-group timeslots 1-24

interface serial 4/1:23
ip address 172.18.13.1 255.255.255.0
encapsulation ppp
```

Related Commands

Command	Description
controller	Configures a T1 or E1 controller and enters controller configuration mode.
show controllers t1 call-counters	Displays the total number of calls and call durations on a T1 controller.
show interfaces	Displays statistics for all interfaces configured on the router or access server.

interface virtual-ppp

To enter interface configuration mode and assign a virtual-PPP interface number, use the **interface virtual-ppp** command in global configuration mode. To disable a virtual-PPP interface, use the **no** form of this command.

interface virtual-ppp *number*

no interface virtual-ppp *number*

Syntax Description

number	Virtual-PPP interface number. Valid values range from one to 2147483647.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.

Usage Guidelines

Use the **interface virtual-ppp** command to create a virtual interface with PPP encapsulation.

Issuing the **interface virtual-ppp** command enters interface configuration mode.

Examples

The following example configures a virtual-PPP interface with the number 503 and enters interface configuration mode:

```
interface virtual-ppp 503
```

Related Commands

Command	Description
l2tp-class	Creates a template of L2TP control plane configuration settings that can be inherited by different pseudowire classes and enters L2TP class configuration mode.
pseudowire-class	Specifies the name of an L2TP pseudowire class and enters pseudowire class configuration mode.
pseudowire	Binds an attachment circuit to an L2TPv3 pseudowire for xconnect service.

interface virtual-template

To create a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces, use the **interface virtual-template** command in global configuration mode. To remove a virtual template interface, use the **no** form of this command.

interface virtual-template *number*

no **interface virtual-template** *number*

Syntax Description

number	Number used to identify the virtual template interface. Up to 200 virtual template interfaces can be configured. On the Cisco 10000 series router, up to 4095 virtual template interfaces can be configured.

Command Default

No virtual template interface is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2F	This command was introduced.
12.2(4)T	This command was enhanced to increase the maximum number of virtual template interfaces from 25 to 200.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

A virtual template interface is used to provide the configuration for dynamically created virtual access interfaces. It is created by users and can be saved in NVRAM.

After the virtual template interface is created, it can be configured in the same way as a serial interface.

Virtual template interfaces can be created and applied by various applications such as virtual profiles, virtual private dialup networks (VPDNs), PPP over ATM, protocol translation, and Multichassis Multilink PPP (MMP).

Cisco 10000 Series Router

You can configure up to 4095 total virtual template interfaces on the Cisco 10000 series router.

To ensure proper scaling and to minimize CPU utilization, we recommend the following virtual template interface settings:

- A keepalive timer of 30 seconds or greater using the **keepalive** command. The default is 10 seconds.
- Do not enable the Cisco Discovery Protocol (CDP). CDP is disabled by default. Use the **no cdp enable** command to disable CDP, if necessary.

- Disable link-status event messaging using the **no logging event link-status** command.
- To prevent the virtual-access subinterfaces from being registered with the SNMP functionality of the router and using memory, do not use the router's SNMP management tools to monitor PPP sessions. Use the **no virtual-template snmp** command to disable the SNMP management tools.

When a virtual template interface is applied dynamically to an incoming user session, a virtual access interface (VAI) is created.

If you configure a virtual template interface with interface-specific commands, the Cisco 10000 series router does not achieve the highest possible scaling. To verify that the router does not have interface-specific commands within the virtual template interface configuration, use the **test virtual-template** *number* **subinterface** command.

Examples

Cisco 10000 Series Router

The following example creates a virtual template interface called Virtual-Template1:

```
Router(config)# interface Virtual-Template1
Router(config-if)# ip unnumbered Loopback1
Router(config-if)# keepalive 60
Router(config-if)# no peer default ip address
Router(config-if)# ppp authentication pap
Router(config-if)# ppp authorization vpn1
Router(config-if)# ppp accounting vpn1
Router(config-if)# no logging event link-status
Router(config-if)# no virtual-template snmp
```

Virtual Template with PPP Authentication Example

The following example creates and configures virtual template interface 1:

```
interface virtual-template 1 type ethernet
 ip unnumbered ethernet 0
 ppp multilink
 ppp authentication chap
```

IPsec Virtual Template Example

The following example shows how to configure a virtual template for an IPsec virtual tunnel interface.

```
interface virtual-template1 type tunnel
 ip unnumbered Loopback1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile virtualtunnelinterface
```

Related Commands

Command	Description
cdp enable	Enables Cisco Discovery Protocol (CDP) on an interface.
clear interface virtual-access	Tears down the live sessions and frees the memory for other client uses.
keepalive	Enables keepalive packets and to specify the number of times that the Cisco IOS software tries to send keepalive packets without a response before bringing down the interface.
show interface virtual-access	Displays the configuration of the active VAI that was created using a virtual template interface.
tunnel protection	Associates a tunnel interface with an IPsec profile.
virtual interface	Sets the zone name for the connected AppleTalk network.

Command	Description
virtual-profile	Enables virtual profiles.
virtual template	Specifies the destination for a tunnel interface.

ip address negotiated

To specify that the IP address for a particular interface is obtained via PPP/IPCP (IP Control Protocol) address negotiation, use the **ip address negotiated** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ip address negotiated [*previous*]

no ip address negotiated [*previous*]

Syntax Description

previous	(Optional) IPCP attempts to negotiate the previously assigned address.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

Use the **ip address negotiated** interface command to enable a Cisco router to automatically negotiate its own registered WAN interface IP address from a central server (via PPP/IPCP) and to enable all remote hosts to access the global Internet using this single registered IP address.

Examples

The following example configures an asynchronous interface (interface async1) to obtain its IP address via PPP/IPCP address negotiation:

```
interface async1
 ip address negotiated
 encapsulation ppp
```

Related Commands

Command	Description
encapsulation	Sets the encapsulation method used by the interface.
ip address	Sets a primary or secondary IP address for an interface.
ip unnumbered	Enables IP processing on an interface without assigning an explicit IP address to the interface.

ip address-pool

To enable a global default address pooling mechanism used to supply IP addresses to dial-in asynchronous, synchronous, or ISDN point-to-point interfaces, use the **ip address-pool** command in global configuration mode. To disable IP address pooling globally on all interfaces with the default configuration, use the **no** form of this command.

ip address-pool {**dhcp-pool** | **dhcp-proxy-client** | **local**}

no ip address-pool

Syntax Description

dhcp-pool	Uses on-demand address pooling as the global default address mechanism. This option supports only remote access PPP sessions using a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN). IP addresses are obtained from locally configured virtual routing and forwarding (VRF)-associated Dynamic Host Configuration Protocol (DHCP) pools.
dhcp-proxy-client	Uses the router as the proxy client between a third-party DHCP server and peers connecting to the router as the global default address mechanism.
local	Uses the local address pool named *default* as the global default address mechanism.

Command Default

IP address pooling is disabled globally.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(8)T	The **dhcp-pool** keyword was added.

Usage Guidelines

The global default IP address pooling mechanism applies to all interfaces that have been left in the default setting of the **peer default ip address** command.

If any **peer default ip address** command other than **peer default ip address pool** (the default) is configured, the interface uses that mechanism and not the global default mechanism. Thus all interfaces can be independently configured, or left unconfigured so that the global default configuration applies. This flexibility minimizes the configuration effort on the part of the administrator.

The **ip address-pool dhcp-pool** command supports only remote access PPP sessions using an MPLS VPN. IP addresses are obtained from locally configured VRF-associated DHCP pools. A VRF VPN instance is a per-VPN routing information repository that defines the VPN membership of a customer site.

Examples

The following example specifies the DHCP on-demand address pooling mechanism as the global default mechanism for assigning peer IP addresses:

```
ip address-pool dhcp-pool
```

The following example specifies the DHCP proxy client mechanism as the global default mechanism for assigning peer IP addresses:

```
ip address-pool dhcp-proxy-client
```

The following example specifies a local IP address pool named “default” as the global default mechanism for all interfaces that have been left in their default setting:

```
ip address-pool local
```

Related Commands

Command	Description
peer default ip address	Specifies an IP address, an address from a specific IP address pool, or an address from the DHCP mechanism to be returned to a remote peer connecting to this interface.

ip dhcp-client network-discovery

To control the sending of Dynamic Host Configuration Protocol (DHCP) Inform and Discover messages, use the **ip dhcp-client network-discovery** command in global configuration mode. To change or disable DHCP message control, use the **no** form of this command.

ip dhcp-client network-discovery informs *number-of-messages* **discovers** *number-of-messages* **period** *seconds*

no ip dhcp-client network-discovery informs *number-of-messages* **discovers** *number-of-messages* **period** *seconds*

Syntax Description

informs *number-of-messages*	Number of DHCP Inform messages. Valid choices are 0, 1, or 2 messages. Default is 0 messages.
discovers *number-of-messages*	Number of DHCP Discover messages. Valid choices are 0, 1, or 2 messages. Default is 0 messages.
period *seconds*	Timeout period for retransmission of DHCP Inform and Discover messages. Valid periods are from 3 to 15 seconds. Default is 15 seconds.

Command Default

0 DHCP Inform and Discover messages (network discovery is disabled when both the **informs** and **discovers** keywords are set to 0); 15-second timeout period.

Command Modes

Global configuration

Command History

Release	Modification
12.2	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **ip dhcp-client network-discovery** command allows peer routers to dynamically discover Domain Name System (DNS) and NetBIOS name server information configured on a DHCP server using PPP IP Control Protocol (IPCP) extensions. Setting the number of DHCP Inform or Discover messages to 1 or 2 determines how many times the system sends a DHCP Inform or Discover message before stopping network discovery, as follows:

- When the number of DHCP Inform messages is set to 1, once the first Inform messages is sent the system waits for a response from the DHCP server for the specified timeout period. If there is no response from the DHCP server by the end of the timeout period, the system sends a DHCP Discover message when the number of Discover messages is not set to 0. If the number of Discover messages is set to 1, network discovery stops. If the number of Discover messages is set to 2, the system waits

again for a response from the DHCP server for the specified timeout period. If there is no response from the DHCP server by the end of this second timeout period, the system sends a second DHCP Discover message and stops network discovery.

- When the number of DHCP Inform messages is set to 2, once the first Inform messages is sent, the system waits for a response from the DHCP server for the specified timeout period. If there is no response from the DHCP server by the end of the timeout period, the system sends another DHCP Inform message. If the number of Discover messages is set to 1, network discovery stops. If the number of Discover messages is set to 2, the system waits again for a response from the DHCP server for the specified timeout period. If there is no response from the DHCP server by the end of this second timeout period, the system sends a second DHCP Discover message and stops network discovery.

Network discovery also stops when the DHCP server responds to DHCP Inform and Discover messages before the configured number of messages and timeout period are exceeded.

Setting the number of messages to 0 disables sending of DHCP Inform and Discover messages, and is the same as entering the **no ip dhcp-client network-discovery** command. When the **ip dhcp-client network-discovery** command is disabled, the system falls back to the static configurations made using the **async-bootp dns-server** and **async-bootp nb-server** global configuration commands or, as a last resort, to a DNS server address assigned with the **ip name-server** command.

Examples

The following example sets two DHCP Inform and Discovery messages and a timeout period of 12 seconds:

```
ip dhcp-client network-discovery informs 2 discovers 2 period 12
```

Related Commands

Command	Description
async-bootp	Configures extended BOOTP requests for asynchronous interfaces as defined in RFC 1084.
ip dhcp-server	Specifies which DHCP servers to use on a network, and specifies the IP address of one or more DHCP servers available on the network.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.

ip dhcp client route

To configure the Dynamic Host Configuration Protocol (DHCP) client to associate any added routes with a specified tracked object number, use the **ip dhcp client** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

ip dhcp client route track *number*

no ip dhcp client route track

Syntax Description

route track *number*	Associates a tracked object number with the DHCP-installed static route. Valid values for the *number* argument range from 1 to 500.

Command Default

No routes are associated with a track number.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)XE	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

The **ip dhcp client** command must be configured before the **ip address dhcp** command is configured on an interface. The **ip dhcp client** command is checked only when an IP address is acquired from DHCP. If the **ip dhcp client** command is specified after an IP address has been acquired from DHCP, the **ip dhcp client** command will not take effect until the next time the router acquires an IP address from DHCP.

Examples

The following example configures DHCP on an Ethernet interface and associates tracked object 123 with routes generated from this interface:

```
interface ethernet 0/0
 ip dhcp client route track 123
 ip address dhcp
```

Related Commands

Command	Description
ip address dhcp	Acquires an IP address on an Ethernet interface from the DHCP.

ip dhcp-server

To specify which Dynamic Host Configuration Protocol (DHCP) servers to use on your network, or to specify the IP address of one or more DHCP servers available on the network, use the **ip dhcp-server** command in global configuration mode. To remove a DHCP server IP address, use the **no** form of this command.

ip dhcp-server [*ip-address* | *name*]

no ip dhcp-server [*ip-address* | *name*]

Syntax Description

ip-address	(Optional) IP address of a DHCP server.
name	(Optional) Name of a DHCP server.

Command Default

The IP limited broadcast address of 255.255.255.255 is used for transactions if no DHCP server is specified. This default allows automatic detection of DHCP servers.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

A DHCP server temporarily allocates network addresses to clients through the access server on an as-needed basis. While the client is active, the address is automatically renewed in a minimum of 20-minute increments. When the user terminates the session, the interface connection is terminated so that network resources can be quickly reused. You can specify up to ten servers on the network.

In normal situations, if a SLIP or PPP session fails (for example, if a modem line disconnects), the allocated address will be reserved temporarily to preserve the same IP address for the client when dialed back into the server. This way, the session that was accidentally terminated can often be resumed.

To use the DHCP proxy-client feature, enable your access server to be a proxy-client on asynchronous interfaces by using the **ip address-pool dhcp-proxy-client** command. If you want to specify which DHCP servers are used on your network, use the **ip dhcp-server** command to define up to ten specific DHCP servers.

Note To facilitate transmission, configure intermediary routers (or access servers with router functionality) to use an IP helper address whenever the DHCP server is not on the local LAN and the access server is using broadcasts to interact with the DHCP server. Refer to the chapters about configuring IP addressing in the *Cisco IOS IP Addressing Services Configuration Guide*.

The **ip address-pool dhcp-proxy-client** command initializes proxy-client status to all interfaces defined as asynchronous on the access server. To selectively disable proxy-client status on a single asynchronous interface, use the **no peer default ip address** interface command.

Examples

The following command specifies a DHCP server with the IP address of 172.24.13.81:

```
ip dhcp-server 172.24.13.81
```

Related Commands

Command	Description
ip address-pool	Enables an address pooling mechanism used to supply IP addresses to dial-in asynchronous, synchronous, or ISDN point-to-point interfaces.
ip helper-address	Forwards UDP broadcasts, including BOOTP, received on an interface.
peer default ip address	Specifies an IP address, an address from a specific IP address pool, or an address from the DHCP mechanism to be returned to a remote peer connecting to this interface.
show cot dsp	Displays information about the COT DSP configuration or current status.

ip idle-group

To configure interesting traffic on a virtual template interface for the PPP idle timer, use the **ip idle-group** command in interface configuration mode. To remove the configuration, use the **no** form of this command.

ip idle-group {*access-list-number* | *access-list-name*} {**in** | **out**}

no ip idle-group {*access-list-number* | *access-list-name*} {**in** | **out**}

Syntax Description

access-list-number	IP access list number.
access-list-name	IP access list name.
in	Classifies IP inbound traffic for the PPP idle timer.
out	Classifies IP outbound traffic for the PPP idle timer.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300, Cisco AS5400 and Cisco AS5800.

Usage Guidelines

The **ip idle-group** command is applied to a virtual template interface and configures interesting traffic on either inbound or outbound traffic.

Examples

The following example specifies access list 101 as interesting for inbound IP traffic and access list 102 as interesting for outbound IP traffic:

```
interface virtual-template 1
 ppp timeout idle 60
 ip idle-group 101 in
 ip idle-group 102 out
```

Related Commands

Command	Description
corlist incoming	Sets the PPP idle timeout parameters on a virtual template interface.

ip local pool

To configure a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface, use the **ip local pool** command in global configuration mode. To remove a range of addresses from a pool (the longer of the **no** forms of this command), or to delete an address pool (the shorter of the **no** forms of this command), use one of the **no** forms of this command.

ip local pool {**default** | *poolname*} [*low-ip-address* [*high-ip-address*]] [**group** *group-name*] [**cache-size** *size*] [**recycle delay** *seconds*]

no ip local pool *poolname low-ip-address* [*high-ip-address*]

no ip local pool {**default** | *poolname*}

Syntax Description

default	Creates a default local IP address pool that is used if no other pool is named.
poolname	Name of the local IP address pool.
low-IP-address [*high-IP-address*]	(Optional) First and, optionally, last address in an IP address range.
group *group-name*	(Optional) Creates a pool group.
cache-size *size*	(Optional) Sets the number of IP address entries on the free list that the system checks before assigning a new IP address. Returned IP addresses are placed at the end of the free list. Before assigning a new IP address to a user, the system checks the number of entries from the end of the list (as defined by the **cache-size** *size* option) to verify that there are no returned IP addresses for that user. The range for the cache size is 0 to 100. The default cache size is 20.
recycle delay *seconds*	(Optional) Indicates the time (in seconds) to hold an IP address in the local pool before making it available for reuse.

Command Default

No address pools are configured. Any pool created without the optional **group** keyword is a member of the base system group.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
11.3AA	This command was enhanced to allow address ranges to be added and removed.
12.1(5)DC	This command was enhanced to allow pool groups to be created.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and support was added for the Cisco 6400 node route processor 25v (NRP-25v) and Cisco 7400 platforms.
12.4(15)T	The **recycle delay** keyword and *seconds* argument were added.

Usage Guidelines

Use the **ip local pool** command to create one or more local address pools from which IP addresses are assigned when a peer connects. You may also add another range of IP addresses to an existing pool. To use a named IP address pool on an interface, use the **peer default ip address pool** interface configuration command. A pool name can also be assigned to a specific user using authentication, authorization, and accounting (AAA) RADIUS and TACACS functions.

If no named local IP address pool is created, a default address pool is used on all point-to-point interfaces after the **ip address-pool local** global configuration command is issued. If no explicit IP address pool is assigned, but pool use is requested by use of the **ip address-pool local** command, the special pool named "default" is used.

The optional **group** keyword and associated group name allows the association of an IP address pool with a named group. Any IP address pool created *without* the **group** keyword automatically becomes a member of a *base* system group.

The optional **recycle delay** keyword and its associated time indicates the time in seconds to hold the IP address from the pool before making it available for reuse.

An IP address pool name can be associated with only one group. Subsequent use of the same pool name, within a pool group, is treated as an extension of that pool, and any attempt to associate an existing local IP address pool name with a different pool group is rejected. Therefore, each use of a pool name is an implicit selection of the associated pool group.

Note To reduce the chances of inadvertent generation of duplicate addresses, the system allows creation of the special pool named "default" only in the base system group, that is, no group name can be specified with the pool name "default."

All IP address pools within a pool group are checked to prevent overlapping addresses; however, no checks are made between any group pool member and a pool not in a group. The specification of a named pool within a pool group allows the existence of overlapping IP addresses with pools in other groups, and with pools in the base system group, but not among pools within a group. Otherwise, processing of the IP address pools is not altered by their membership in a group. In particular, these pool names can be specified in **peer** commands and returned in RADIUS and AAA functions with no special processing.

IP address pools can be associated with Virtual Private Networks (VPNs). This association permits flexible IP address pool specifications that are compatible with a VPN and a VPN routing and forwarding (VRF) instance.

The IP address pools can also be used with the **translate** commands for one-step vty-async connections and in certain AAA or TACACS+ authorization functions. Refer to the chapter "Configuring Protocol Translation and Virtual Asynchronous Devices" in the *Cisco IOS Terminal Services Configuration Guide* and the "System Management" part of the *Cisco IOS Configuration Fundamentals Configuration Guide* for more information.

IP address pools are displayed with the **show ip local pool** EXEC command.

Examples

The following example creates a local IP address pool named "pool2," which contains all IP addresses in the range 172.16.23.0 to 172.16.23.255:

```
ip local pool pool2 172.16.23.0 172.16.23.255
```

The following example configures a pool of 1024 IP addresses:

```
no ip local pool default
ip local pool default 10.1.1.0 10.1.4.255
```

Note Although not required, it is good practice to precede local pool definitions with a **no** form of the command to remove any existing pool, because the specification of an existing pool name is taken as a request to extend that pool with the new IP addresses. If the intention is to extend the pool, the **no** form of the command is not applicable.

The following example configures multiple ranges of IP addresses into one pool:

```
ip local pool default 10.1.1.0 10.1.9.255
ip local pool default 10.2.1.0 10.2.9.255
```

The following examples show how to configure two pool groups and IP address pools in the base system group:

```
ip local pool p1-g1 10.1.1.1 10.1.1.50 group grp1
ip local pool p2-g1 10.1.1.100 10.1.1.110 group grp1
ip local pool p1-g2 10.1.1.1 10.1.1.40 group grp2
ip local pool lp1 10.1.1.1 10.1.1.10
ip local pool p3-g1 10.1.2.1 10.1.2.30 group grp1
ip local pool p2-g2 10.1.1.50 10.1.1.70 group grp2
ip local pool lp2 10.1.2.1 10.1.2.10
```

In the example:

- Group grp1 consists of pools p1-g1, p2-g1, and p3-g1.
- Group grp2 consists of pools p1-g2 and p2-g2.
- Pools lp1 and lp2 are not associated with a group and are therefore members of the base system group.

Note that IP address 10.1.1.1 overlaps groups grp1, grp2, and the base system group. Also note that there is no overlap within any group including the base system group, which is unnamed.

The following examples show configurations of IP address pools and groups for use by a VPN and VRF:

```
ip local pool p1-vpn1 10.1.1.1 10.1.1.50 group vpn1
ip local pool p2-vpn1 10.1.1.100 10.1.1.110 group vpn1
ip local pool p1-vpn2 10.1.1.1 10.1.1.40 group vpn2
ip local pool lp1 10.1.1.1 10.1.1.10
ip local pool p3-vpn1 10.1.2.1 10.1.2.30 group vpn1
ip local pool p2-vpn2 10.1.1.50 10.1.1.70 group vpn2
ip local pool lp2 10.1.2.1 10.1.2.10
```

The examples show configuration of two pool groups, including pools in the base system group, as follows:

- Group vpn1 consists of pools p1-vpn1, p2-vpn1, and p3-vpn1.
- Group vpn2 consists of pools p1-vpn2 and p2-vpn2.
- Pools lp1 and lp2 are not associated with a group and are therefore members of the base system group.

Note that IP address 10.1.1.1 overlaps groups vpn1, vpn2, and the base system group. Also note that there is no overlap within any group including the base system group, which is unnamed.

The VPN needs a configuration that selects the proper group by selecting the proper pool based on remote user data. Thus, each user in a given VPN can select an address space using the pool and associated group appropriate for that VPN. Duplicate addresses in other VPNs (other group names) are not a concern, because the address space of a VPN is specific to that VPN.

In the example, a user in group vpn1 is associated with some combination of the pools p1-vpn1, p2-vpn1, and p3-vpn1, and is allocated addresses from that address space. Addresses are returned to the same pool from which they were allocated.

The following example configures a recycle delay of 30 seconds to hold IP addresses in the pool before making them available for reuse:

```
ip local pool default 10.1.1.0 10.1.9.255 recycle delay 30
```

Related Commands

Command	Description
debug ip peer	Displays additional output when IP address pool groups are defined.
ip address-pool	Enables an address pooling mechanism used to supply IP addresses to dial in asynchronous, synchronous, or ISDN point-to-point interfaces.
peer default ip address	Specifies an IP address, an address from a specific IP address pool, or an address from the DHCP mechanism to be returned to a remote peer connecting to this interface.
show ip local pool	Displays statistics for any defined IP address pools.
translate lat	Translates a LAT connection request automatically to another outgoing protocol connection type.
translate tcp	Translates a TCP connection request automatically to another outgoing protocol connection type.

ip route

To establish static routes, use the **ip route** command in global configuration mode. To remove static routes, use the **no** form of this command.

ip route [vrf *vrf-name***]** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [**dhcp**] [*distance*] [**name** *next-hop-name*] [**permanent** | **track** *number*] [**tag** *tag*]

no ip route [vrf *vrf-name***]** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [**dhcp**] [*distance*] [**name** *next-hop-name*] [**permanent** | **track** *number*] [**tag** *tag*]

Syntax Description

vrf *vrf-name*	(Optional) Configures the name of the VRF by which static routes should be specified.
prefix	IP route prefix for the destination.
mask	Prefix mask for the destination.
ip-address	IP address of the next hop that can be used to reach that network.
interface-type interface-number	Network interface type and interface number.
dhcp	(Optional) Enables a Dynamic Host Configuration Protocol (DHCP) server to assign a static route to a default gateway (option 3). **Note** Specify the **dhcp** keyword for each routing protocol.
distance	(Optional) Administrative distance. The default administrative distance for a static route is 1.
name *next-hop-name*	(Optional) Applies a name to the next hop route.
permanent	(Optional) Specifies that the route will not be removed, even if the interface shuts down.
track *number*	(Optional) Associates a track object with this route. Valid values for the *number* argument range from 1 to 500.
tag *tag*	(Optional) Tag value that can be used as a "match" value for controlling redistribution via route maps.

Command Default

No static routes are established.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.3(2)XE	The **track** keyword and *number* argument were added.
12.3(8)T	The **track** keyword and *number* argument were integrated into Cisco IOS Release 12.3(8)T. The **dhcp** keyword was added.

Release	Modification
12.3(9)	The changes made in Cisco IOS Release 12.3(8)T were added to Cisco IOS Release 12.3(9).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The establishment of a static route is appropriate when the Cisco IOS software cannot dynamically build a route to the destination.

When you specify a DHCP server to assign a static route, the interface type and number and administrative distance may be configured also.

If you specify an administrative distance, you are flagging a static route that can be overridden by dynamic information. For example, routes derived with Enhanced Interior Gateway Routing Protocol (EIGRP) have a default administrative distance of 100. To have a static route that would be overridden by an EIGRP dynamic route, specify an administrative distance greater than 100. Static routes have a default administrative distance of 1.

Static routes that point to an interface on a connected router will be advertised by way of Routing Information Protocol (RIP) and EIGRP regardless of whether **redistribute static** commands are specified for those routing protocols. This situation occurs because static routes that point to an interface are considered in the routing table to be connected and hence lose their static nature. Also, the target of the static route should be included in the **network** (DHCP) command. If this condition is not met, no dynamic routing protocol will advertise the route unless a **redistribute static** command is specified for these protocols. With the following configuration:

```
rtr1 (serial 172.16.188.1/30)--------------> rtr2(Fast Ethernet 172.31.1.1/30) ------>

router [rip | eigrp]
 network 172.16.188.0
 network 172.31.0.0
```

- RIP and EIGRP redistribute the route if the route is pointing to the Fast Ethernet interface:

  ```
  ip route 172.16.188.252 255.255.255.252 FastEthernet 0/0
  ```

  RIP and EIGRP do not redistribute the route with the following **ip route** command because of the split horizon algorithm:

  ```
  ip route 172.16.188.252 255.255.255.252 serial 2/1
  ```

- EIGRP redistributes the route with both of the following commands:

  ```
  ip route 172.16.188.252 255.255.255.252 FastEthernet 0/0
  ip route 172.16.188.252 255.255.255.252 serial 2/1
  ```

With the Open Shortest Path First (OSPF) protocol, static routes that point to an interface are not advertised unless a **redistribute static** command is specified.

Adding a static route to an Ethernet or other broadcast interface (for example, ip route 0.0.0.0 0.0.0.0 Ethernet 1/2) will cause the route to be inserted into the routing table only when the interface is up. This configuration is not generally recommended. When the next hop of a static route points to an interface, the router considers each of the hosts within the range of the route to be directly connected through that interface, and therefore it will send Address Resolution Protocol (ARP) requests to any destination addresses that route through the static route.

A logical outgoing interface, for example, a tunnel, needs to be configured for a static route. If this outgoing interface is deleted from the configuration, the static route is removed from the configuration and hence does not show up in the routing table. To have the static route inserted into the routing table again, configure the outgoing interface once again and add the static route to this interface.

The practical implication of configuring the **ip route 0.0.0.0 0.0.0.0 ethernet 1/2** command is that the router will consider all of the destinations that the router does not know how to reach through some other route as directly connected to Ethernet interface 1/2. So the router will send an ARP request for each host for which it receives packets on this network segment. This configuration can cause high processor utilization and a large ARP cache (along with memory allocation failures). Configuring a default route or other static route that directs the router to forward packets for a large range of destinations to a connected broadcast network segment can cause your router to reload.

Specifying a numerical next hop that is on a directly connected interface will prevent the router from using proxy ARP. However, if the interface with the next hop goes down and the numerical next hop can be reached through a recursive route, you may specify both the next hop and interface (for example, **ip route 0.0.0.0 0.0.0.0 ethernet 1/2 10.1.2.3**) with a static route to prevent routes from passing through an unintended interface.

Note Configuring a default route that points to an interface, such as **ip route 0.0.0.0 0.0.0.0 ethernet 1/2**, displays a warning message. This command causes the router to consider all the destinations that the router cannot reach through an alternate route, as directly connected to Ethernet interface 1/2. Hence, the router sends an ARP request for each host for which it receives packets on this network segment. This configuration can cause high processor utilization and a large ARP cache (along with memory allocation failures). Configuring a default route or other static route that directs the router to forward packets for a large range of destinations to a connected broadcast network segment can cause the router to reload.

The **name** *next-hop-name* keyword and argument combination allows you to associate static routes with names in your running configuration. If you have several static routes, you can specify names that describe the purpose of each static route in order to more easily identify each one.

The **track** *number* keyword and argument combination specifies that the static route will be installed only if the state of the configured track object is up.

Recursive Static Routing

In a recursive static route, only the next hop is specified. The output interface is derived from the next hop.

For the following recursive static route example, all destinations with the IP address prefix address prefix 192.168.1.1/32 are reachable via the host with address 10.0.0.2:

```
ip route 192.168.1.1 255.255.255.255 10.0.0.2
```

A recursive static route is valid (that is, it is a candidate for insertion in the IPv4 routing table) only when the specified next hop resolves, either directly or indirectly, to a valid IPv4 output interface, provided the route does not self-recurse, and the recursion depth does not exceed the maximum IPv4 forwarding recursion depth.

The following example defines a valid recursive IPv4 static route:

```
interface serial 2/0
 ip address 10.0.0.1 255.255.255.252
 exit
ip route 192.168.1.1 255.255.255.255 10.0.0.2
```

The following example defines an invalid recursive IPv4 static route. This static route will not be inserted into the IPv4 routing table because it is self-recursive. The next hop of the static route, 192.168.1.0/30, resolves via the first static route 192.168.1.0/24, which is itself a recursive route (that is, it only specifies a next hop). The next hop of the first route, 192.168.1.0/24, resolves via the directly connected route via the serial interface 2/0. Therefore, the first static route would be used to resolve its own next hop.

```
interface serial 2/0
 ip address 10.0.0.1 255.255.255.252
 exit
ip route 192.168.1.0 255.255.255.0 10.0.0.2
ip route 192.168.1.0 255.255.255.252 192.168.1.100
```

It is not normally useful to manually configure a self-recursive static route, although it is not prohibited. However, a recursive static route that has been inserted in the IPv4 routing table may become self-recursive as a result of some transient change in the network learned through a dynamic routing protocol. If this situation occurs, the fact that the static route has become self-recursive will be detected and the static route will be removed from the IPv4 routing table, although not from the configuration. A subsequent network change may cause the static route to no longer be self-recursive, in which case it will be re-inserted in the IPv4 routing table.

Note IPv4 recursive static routes are checked at one-minute intervals. Therefore, a recursive static route may take up to a minute to be inserted into the routing table once its next hop becomes valid. Likewise, it may take a minute or so for the route to disappear from the table if its next hop becomes invalid.

Examples

The following example shows how to choose an administrative distance of 110. In this case, packets for network 10.0.0.0 will be routed to a router at 172.31.3.4 if dynamic information with an administrative distance less than 110 is not available.

```
ip route 10.0.0.0 255.0.0.0 172.31.3.4 110
```

Note Specifying the next hop without specifying an interface when configuring a static route can cause traffic to pass through an unintended interface if the default interface goes down.

The following example shows how to route packets for network 172.31.0.0 to a router at 172.31.6.6:

```
ip route 172.31.0.0 255.255.0.0 172.31.6.6
```

The following example shows how to route packets for network 192.168.1.0 directly to the next hop at 10.1.2.3. If the interface goes down, this route is removed from the routing table and will not be restored unless the interface comes back up.

```
ip route 192.168.1.0 255.255.255.0 Ethernet 0 10.1.2.3
```

The following example shows how to install the static route only if the state of track object 123 is up:

```
ip route 0.0.0.0 0.0.0.0 Ethernet 0/1 10.1.1.242 track 123
```

The following example shows that using the **dhcp** keyword in a configuration of Ethernet interfaces 1 and 2 enables the interfaces to obtain the next-hop router IP addresses dynamically from a DHCP server:

```
ip route 10.165.200.225 255.255.255.255 ethernet1 dhcp
ip route 10.165.200.226 255.255.255.255 ethernet2 dhcp 20
```

The following example shows that using the **name** *next-hop-name* keyword and argument combination for each static route in the configuration helps you remember the purpose for each static route.

```
ip route 172.0.0.0 255.0.0.0 10.0.0.1 name Seattle2Detroit
```

The name for the static route will be displayed when the **show running-configuration** command is entered:

```
Router# show running-config | include ip route

ip route 172.0.0.0 255.0.0.0 10.0.0.1 name Seattle2Detroit
```

Related Commands

Command	Description
network (DHCP)	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

ip route (large-scale dial-out)

To establish static routes and define the next hop for large-scale dial-out, use the **ip route** command in global configuration mode. To remove static routes, use the **no** form of this command.

ip route *network-number network-mask* {*ip-address* | *interface*} [*distance*] [**name** *name*]

no ip route

Syntax Description

network-number	IP address of the target network or subnet.
network-mask	Network mask that lets you mask network and subnetwork bits.
ip-address	Internet address of the next hop that can be used to reach that network in standard IP address notation. Example: 10.1.1.1.
interface	Network interface name and number to use.
distance	(Optional) Administrative distance, which is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers.
name *name*	(Optional) Name of the user profile.

Command Default

No static route is established.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

A static route is appropriate when the communication server cannot dynamically build a route to the destination.

If you specify an administrative distance, you are flagging a static route that can be overridden by dynamic information. For example, Interior Gateway Routing Protocol (IGRP)-derived routes have a default administrative distance of 100. To have a static route that would be overridden by an IGRP dynamic route, specify an administrative distance greater than 100. Static routes have a default administrative distance of 1.

Static routes that point to an interface will be advertised using RIP, IGRP, and other dynamic routing protocols, regardless of whether redistribute static commands were specified for those routing protocols. These static routes will be advertised because static routes that point to an interface are considered to be connected in the routing table and hence lose their static nature. However, if you define a static route to an interface that is not in one of the networks defined in a network command, no dynamic routing protocols will advertise the route unless a redistribute static command is specified for these protocols.

The user profile name is passed to an authentication, authorization, and accounting (AAA) server as the next hop for large-scale dial-out, and is the *name* argument with the -out suffix appended. The suffix is automatically supplied and is required because dial-in and user profile names must be unique.

Examples

In the following example, an administrative distance of 110 was chosen. In this case, packets for network 10.0.0.0 will be routed via to the communication server at 172.19.3.4 if dynamic information with an administrative distance less than 110 is not available.

```
ip route 10.0.0.0 255.0.0.0 172.19.3.4 110
```

In the following example, packets for network 172.19.0.0 will be routed to the communication server at 172.19.6.6:

```
ip route 172.19.0.0 255.255.0.0 172.19.6.6
```

In the following example, the user profile named “profile1-out” will be retrieved from the AAA server:

```
ip route 10.0.0.0 255.255.255.255 Dialer0 name profile1
```

Related Commands

Command	Description
show ip route	Displays all static IP routes, or those installed using the AAA route download function.

ip rtp reserve

To reserve a special queue for a set of Real-Time Transport Protocol (RTP) packet flows belonging to a range of User Datagram Protocol (UDP) destination ports, use the **ip rtp reserve** command in interface configuration mode. To disable the special queue for real-time traffic, use the **no** form of this command.

ip rtp reserve *lowest-udp-port range-of-ports* [*maximum-bandwidth*]

no ip rtp reserve

Syntax Description

lowest-udp-port	Lowest UDP port number to which the packets are sent.
range-of-ports	Number, which when added to the lowest UDP port value, yields the highest UDP port value.
maximum-bandwidth	(Optional) Bandwidth, in kilobits per second, reserved for the RTP packets to be sent to the specified UDP ports.

Command Default

This function is disabled by default. No default values are provided for the arguments.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

If the bandwidth needed for RTP packet flows exceeds the maximum bandwidth specified, the reserved queue will degrade to a best-effort queue.

This command helps in improving the delay bounds of voice streams by giving them a higher priority.

Examples

The following example reserves a unique queue for traffic to destination UDP ports in the range 32768 to 32788 and reserves 1000 kbps bandwidth for that traffic:

```
ip rtp reserve 32768 20 1000
```

Related Commands

Command	Description
ppp multilink	Enables MLP on an interface and, optionally, enables dynamic bandwidth allocation.
ppp multilink fragment delay	Specifies a maximum size, in units of time, for packet fragments on an MLP bundle.
ppp multilink interleave	Enables interleaving of packets among the fragments of larger packets on an MLP bundle.

ip tcp async-mobility server

To enable asynchronous listening, which in turn allows TCP connections to TCP port 57, use the **ip tcp async-mobility server** command in global configuration mode. To turn listening off, use the **no** form of this command.

ip tcp async-mobility server

no ip tcp async-mobility server

Syntax Description

This command has no arguments or keywords.

Command Default

Asynchronous listening is disabled (turned off).

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

After asynchronous listening is turned on by the **ip tcp async-mobility server** command, use the **tunnel** command to establish a network layer connection to a remote host. Both commands must be used to enable asynchronous mobility.

Examples

The following example shows how to configure asynchronous mobility. The **tunnel** command is used to establish a network layer connection with an IBM host named "mktg."

```
Router# configure terminal
Router(config)# ip tcp async-mobility server
Router(config)# exit

Router# tunnel mktg
```

Related Commands

Command	Description
tunnel	Sets up a network layer connection to a router.

ip telnet comport

To enable the Cisco IOS Telnet server to use the RFC 2217 Com Port extensions, use the **ip telnet comport** command in global configuration mode. To disable RFC 2217 Com Port extensions, use the **no** form of this command.

ip telnet comport {**disconnect delay** *seconds* | **enable** | **flow level** *number-of-characters* | **receive window** *window-size*}

no ip telnet comport enable

Syntax Description

disconnect delay	(Optional) Delay before TCP closes after the DTR drop. **Note** At lease one of these alternative keywords must be entered.
enable	(Optional) Enables the Cisco IOS Telnet server to use the RFC 2217 Com Port extensions.
flow level	(Optional) Sets the flow control level.
receive window	(Optional) Sets the maximum TCP receive window size.
seconds	Number of seconds to delay the TCP closure. Possible values: 0 to 360.
number-of-charcters	Number of characters to be saved in the device buffer before sending an RFC 2217 SUSPEND message.
window-size	Maximum window size. Possible values: 1 to 4128.

Command Default

Telnet Com Port extensions are enabled

Command Modes

Global configuration

Command History

Release	Modification
11.3(1)	This command was introduced.
12.1	This was integrated into Cisco IOS Release 12.1.
12.2	This was integrated into Cisco IOS Release 12.2.
12.3	This was integrated into Cisco IOS Release 12.3.
12.4	This was integrated into Cisco IOS Release 12.4.

Usage Guidelines

RFC 2217 Telnet Com Port extensions are used to communicate modem hardware signal status from a modem on a network access server (NAS) to a TCP/IP client. An example would be a client PC using a package such as DialOut/EZ (Tacticalsoftware.com) to provide an emulated COM port via a TCP connection to a Cisco AS5000 NAS with integrated modems.

When Com Port extensions are enabled on the NAS, the binary Telnet option (RFC 856) should be used. The Telnet client must connect to TCP ports 6000+ for individual lines, or 7000+ for rotaries on the Cisco NAS.

Setting the Command to Avoid Interruptions

Although the default settings for the **ip telnet comport** command are suitable for most applications, in a few cases some settings should be changed for efficient communications. Two possible situations are described below.

- Preventing Data Buffer Overflows

  Before the application can send data it must determine the modem's readiness for transmission. This checking process generates some initial data. If many of these checks occur in a short period of time, the data will be buffered.

  Command **ip telnet comport can be set** to prevent a buffer overflow from of these trivial data events. In this case, the ip telnet comport flow level (range: 1 through 1023) is adjusted. This enables the PC-hosted comm-serv to send a signal to the remote to prevent (SUSPEND) transmission of any data or commands. When the application is actually ready to receive data, the remote can start transmissions.

- Handling DTR Drops

  When a Data Terminal Ready (DTR, a signal pin on a serial interface) is dropped during a communcation, the PC application may incorrectly interpret the event as an error. This situation can be prevented by changing the disconnect delay (range is 1 to 360 seconds) of command **ip telnet comport** . Adding this delay gives the application time to receive and properly act on the DTR drop message before the tcp connection is closed down.

Examples

The following example disables Telnet Com Port extensions:

```
no ip telnet comport enable
```

Related Commands

Command	Description
debug telnet	Displays information about Telnet option negotiation messages for incoming Telnet connections to a Cisco IOS Telnet server.

ip telnet hidden

To hide IP address or host name information when a Telnet session is established, use the **ip telnet hidden** command in global configuration mode. To make IP address or hostname information visible, use the **no** form of this command.

ip telnet hidden {**addresses** | **hostnames**}

no ip telnet hidden {**addresses** | **hostnames**}

Syntax Description

addresses	Specifies that IP addresses will not be displayed when a Telnet session is established.
hostnames	Specifies that host names will not be displayed when a Telnet session is established.

Command Default

IP addresses and host names are visible

Command Modes

Global configuration

Command History

Release	Modification
12.2(1)	This command was introduced.

Usage Guidelines

By default, when a Telnet client connects to the server, the client will display a message with the server IP address and host name, as shown in the following example:

```
Router# telnet is-dialer

Trying is-dialer.cisco.com (10.20.0.167)... Open
```

The **ip telnet hidden** command can be configured to hide the IP address of the client or the host name of the client in the message. Configuring the **ip telnet hidden addresses** command results in the client displaying a message with the IP address of the server hidden, as shown in the following example:

```
Router# telnet is-dialer

Trying is-dialer.cisco.com address #1 ... Open
```

Configuring the **ip telnet hidden hostnames** command results in the client displaying a message with the host name of the server hidden, as shown in the following example:

```
Router# telnet is-dialer

Trying (10.20.0.167) ... Open
```

Configuring both the **ip telnet hidden addresses** and **ip telnet hidden hostnames** commands results in the client displaying a message with both the IP address and the host name of the server hidden, as shown in the following example:

```
Router# telnet is-dialer

Trying address #1 ... Open
```

Examples

The following example configures the Telnet client to hide both IP addresses and host name information when connecting to the server:

```
ip telnet hidden addresses
ip telnet hidden hostnames
```

Related Commands

Command	Description
busy-message	Creates a “host failed” message that displays when a connection fails.
ip telnet quiet	Suppresses the display of Telnet connection messages.
telnet	Logs in to a host that supports Telnet.

ip telnet quiet

To suppress the display of Telnet connection messages, use the **ip telnet quiet** command in global configuration mode. To cancel this option, use the **no** form of this command.

ip telnet quiet

no ip telnet quiet

Syntax Description

This command has no arguments or keywords.

Command Default

Telnet connection message suppression is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

The **ip telnet quiet** command does not suppress TCP or error messages. It is most useful to Internet service providers, to allow them to hide the onscreen messages displayed during connection, including Internet addresses, from subscription users.

Examples

The following example globally disables onscreen connect messages:

```
ip telnet quiet
```

The following example shows the login and logout messages displayed during login and logout when the **ip telnet quiet** command has *not* been configured to suppress Cisco IOS software messages:

```
Router# telnet Server3

Translating "Server3"...domain server (171.68.89.42) [OK]
Trying Server3--Server3.cisco.com (171.68.89.42)... Open
Kerberos:       No default realm defined for Kerberos!


login:User2
Password:
        Welcome to OpenVMS VAX version V6.1 on node CRAW
    Last interactive login on Tuesday, 15-DEC-1998 11:01
    Last non-interactive login on Sunday,  3-JAN-1999 22:32

Server3)logout
   User2        logged out at  16-FEB-2000 09:38:27.85
[Connection to Server3 closed by foreign host]
```

The following example shows the limited messages displayed during login and logout when the **ip telnet quiet** command has been configured to suppress Cisco IOS software messages:

```
Router# telnet Server3

login:User2
Password:
         Welcome to OpenVMS VAX version V6.1 on node CRAW
     Last interactive login on Tuesday, 15-DEC-1998 11:01
     Last non-interactive login on Sunday,  3-JAN-1999 22:32

Server3)logout
    User2        logged out at  16-FEB-2000 09:38:27.85
```

Related Commands

Command	Description
busy-message	Creates a "host-failed" message that displays when a connection fails.
rlogin	Logs in to a UNIX host using rlogin.
service hide-telnet-address	Hides addresses while trying to establish a Telnet session.
telnet	Logs in to a host that supports Telnet.

ip telnet timeout retransmit

To specify a maximum period that TCP will attempt to retransmit a segment for a Telnet connection, use the **ip telnet timeout** command in global configuration mode. To remove the maximum TCP retransmission period, use the **no** form of this command.

ip telnet timeout retransmit *seconds*

no ip telnet timeout retransmit

Syntax Description

seconds	Number of seconds for the timeout value. Values can range from 1 to 2147483.

Command Default

no ip telnet timeout retransmit

Command Modes

Global configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Configure the **ip telnet timeout** command to specify an explicit maximum period that TCP will attempt to retransmit a segment for a Telnet connection. For the default setting (**no ip telnet timeout retransmit**), TCP's retransmit timeout will be based on the estimated round trip time for the connection (typically, seven or eight minutes).

Note If Telnet has no data to transmit, the TCP connection remains indefinitely (regardless of whether the other end is reachable), unless you configure TCP keepalives. This setting has an effect on connections using the Telnet protocol (whether inbound or outbound), not on connections using other protocols such as rlogin and ssh (secure shell).

Examples

The following example sets the TCP retransmit time to a value of 12 hours:

```
Router(config)#ip telnet timeout retransmit 432000
```

Related Commands

Command	Description
service tcp-keepalives-in	Enables TCP keepalives on an inbound connection.
service tcp-keepalives-out	Enables TCP keepalives on an outbound connection.
telnet	Logs in to a host that supports Telnet.

ip telnet tos

To set the type of service (ToS) precedence bits in the IP header for Telnet packets sent by the router, use the **ip telnet tos** command in global configuration mode. To restore the default value, use the **no** form of this command.

ip telnet tos *hex-value*

no ip telnet tos

Syntax Description

hex-value	Hexadecimal value of the ToS precedence bits in the IP header. Valid values range from 0 to FF. The default value is 0xC0.

Command Default

The default ToS value for Telnet packets is 0xC0.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2(10)P	This command was introduced.
11.3(1)	This command was integrated into Cisco IOS Release 11.3(1).
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

Compatibility with older Telnet clients may require the configuration of the **ip telnet tos 0** command.

Examples

The following example configures a ToS precedence bit value of 0xF0 in the IP header:

```
Router(config)# ip telnet tos F0
```

The following example displays the output for an invalid ToS precedence value:

```
Router(config)# ip telnet tos F2
%Invalid TOS F2
```

Related Commands

Command	Description
telnet	Logs in to a host that supports Telnet.

ip udptn source-interface

To configure the source IP address for a User Datagram Protocol Telnet (UDPTN) interface connection, use the **ip udptn source-interface** command in global configuration mode. To disable the previously configured UDPTN interface, use the **no** form of this command.

ip udptn source-interface *type number*

no ip udptn source-interface

Syntax Description

type number	The interface type and number whose address is to be used as the source for UDPTN connections.

Command Default

The address of the interface closest to the destination is selected as the source address.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example shows how to configure Virtual Multipoint Interface (VMI) for a UDPTN connection:

```
Router# configure terminal
Router(config)# ip udptn source-interface vmi 23
```

Related Commands

Command	Description
ip tftp source-interface	Specifies the IP address of an interface as the source address for TFTP connections.

ipx compression cipx

To enable compression of Internetwork Packet Exchange (IPX) packet headers in a PPP session, use the **ipx compression cipx** command in interface configuration mode. To disable compression of IPX packet headers in a PPP session, use the **no** form of this command.

ipx compression cipx *number-of-slots*

no ipx compression cipx

Syntax Description

number-of-slots	Number of stored IPX headers allowed. The range is from 10 to 256. A slot is similar to a table entry for a complete IPX header. When a packet is received, the receiver stores the complete IPX header in a slot and tells the destination which slot it used. As subsequent CIPX packets are sent, the receiver uses the slot number field to determine which complete IPX header to associate with the CIPX packet before passing the packet up to IPX.

Command Default

No compression of IPX packets during a PPP session. Default number of slots is 16.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

This interface configuration command enables IPX header compression on PPP links.

Examples

The following example enables IPX header compression for PPP:

```
encapsulation ppp
ipx compression cipx 128
```

Related Commands

Command	Description
show ipx compression	Displays the current status and statistics of IPX header compression during PPP sessions.

ipx ppp-client

To enable a nonrouting Internetwork Packet Exchange (IPX) client to connect to an asynchronous interface, the interface must be associated with a loopback interface configured to run IPX. To permit such connections, use the **ipx ppp-client** command in interface configuration mode. To disable a nonrouting IPX client, use the **no** form of this command.

ipx ppp-client loopback *loopback-interface-number*

no ipx ppp-client loopback *loopback-interface-number*

Syntax Description

loopback	Loopback interface configured with a unique IPX network number.
loopback-interface-number	Number of the loopback interface.

Command Default

IPX client connections are not permitted over PPP.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

This command enables IPX clients to log in to the router from a device running a virtual terminal protocol, then issue the PPP command at the EXEC prompt to connect to a remote device.

You must first configure a loopback interface with a unique IPX network number. The loopback interface is then assigned to an asynchronous interface, which permits IPX clients to connect to the asynchronous interface.

Examples

The following example configures IPX to run over PPP on asynchronous interface 3:

```
ipx routing 0000.0c07.b509
interface loopback0
 no ip address
 ipx network 544
 ipx sap-interval 2000
interface ethernet0
 ip address 172.21.14.64
 ipx network AC150E00
 ipx encapsulation SAP
interface async 3
 ip unnumbered ethernet0
 encapsulation ppp
 async mode interactive
 async default ip address 172.18.1.128
 ipx ppp-client loopback0
 ipx sap-interval 0
```

Related Commands

Command	Description
interface loopback	Creates a loopback interface.
ipx network	Enables IPX routing on a particular interface and optionally selects the type of encapsulation (framing).

isdn all-incoming-calls-v120

To configure an ISDN BRI or PRI interface to answer all incoming calls as V.120 when the terminal adapter uses V.120 signaling but does not send the Lower-Layer Compatibility field in Setup messages, use the **isdn all-incoming-calls-v120** command in interface configuration mode. To remove this configuration, use the **no** form of the command.

isdn all-incoming-calls-v120

no isdn all-incoming-calls-v120

Syntax Description

This command has no arguments or keywords.

Command Default

By default, ISDN interfaces answer calls as synchronous serial with PPP encapsulation.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use this command only when you want *all* incoming calls to be answered as V.120. If you want the interface to automatically detect whether the incoming call uses V.120 or PPP encapsulation, use the **autodetect encapsulation** command.

This command applies only when the incoming call originates on an asynchronous device and needs to terminate in an available vty on the router.

Examples

The following partial example shows that BRI 0 is configured to answer all calls as V.120:

```
interface bri 0
 isdn all-incoming-calls-v120
```

Related Commands

Command	Description
autodetect encapsulation	Enables automatic detection of the encapsulation types in operation over a point-to-point link to a specified serial or ISDN interface.

isdn answer1, isdn answer2

To have the router verify a called-party number or subaddress number in the incoming setup message for ISDN BRI calls, if the number is delivered by the switch, use the **isdn answer1** command in interface configuration mode. To remove the verification request, use the **no** form of this command.

isdn answer1 [*called-party-number*][**:***subaddress*]

no isdn answer1 [*called-party-number*][**:***subaddress*]

To have the router verify an *additional* called-party number or subaddress number in the incoming setup message for ISDN BRI calls, if the number is delivered by the switch, use the **isdn answer2** command in interface configuration mode. To remove this second verification request, use the **no** form of this command.

isdn answer2 [*called-party-number*][**:***subaddress*]

no isdn answer2 [*called-party-number*][**:***subaddress*]

Syntax Description

called-party-number	(Optional) Telephone number of the called party. At least one value—*called-party-number* or *subaddress*—must be specified. The maximum number of digits for *called-party-number* is 50.
:	(Optional) Identifies the number that follows as a subaddress. Use the colon (:) when you configure both the called party number and the subaddress, or when you configure only the subaddress.
subaddress	(Optional) Subaddress number used for ISDN multipoint connections. At least one value—*called-party-number* or *subaddress*—must be specified. The maximum number of digits for *subaddress* is 50.

Command Default

The router does not verify the called party or subaddress number.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

If you do not specify the **isdn answer1** or **isdn answer2** command, all calls are processed or accepted. If you specify the **isdn answer1** or **isdn answer2** command, the router must verify the incoming called-party number and the subaddress before processing or accepting the call. The verification proceeds from right to left for the called-party number; it also proceeds from right to left for the subaddress number.

You can configure just the called-party number or just the subaddress. In such a case, only that part is verified. To configure a subaddress only, include the colon (:) before the subaddress number.

You can declare a digit a “don’t care” digit by configuring it as an *x* or *X*. In such a case, any incoming digit is allowed.

Examples

In the following example, 5550122 is the called-party number and 1234 is the subaddress:

```
interface bri 0
 isdn answer1 5550122:1234
```

In the following example, only the subaddress is configured:

```
interface bri 0
 isdn answer1 :1234
```

isdn autodetect

To enable the automatic detection of ISDN SPIDs and switch type, use the **isdn autodetect** command in interface configuration mode. To disable the automatic detection of ISDN SPIDs and switch type, use the **no** form of this command.

isdn autodetect

no isdn autodetect

Syntax Description

This command has no arguments or keywords.

Command Default

The automatic detection of ISDN SPIDs and switch type is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

This command applies to North America only. If you are outside of North America, you must use the **isdn switch-type** (BRI) or **isdn switch-type** (PRI) interface configuration command to specify the ISDN switch type.

Examples

The following example enables the automatic detection of ISDN SPIDs and switch type:

```
isdn autodetect
```

Related Commands

Command	Description
isdn spid1, isdn spid2	Defines the SPID number that has been assigned by the ISDN service provider for the B1 channel.
isdn switch-type (BRI)	Specifies the central office switch type on the ISDN BRI interface.
isdn switch-type (PRI)	Specifies the central office switch type on the ISDN PRI interface.

isdn bcac service audit

To enable service audits on an interface configured for B-Channel Availability Control (BCAC), use the **isdn bcac service audit** command in interface configuration mode. To disable service audits, use the **no** form of this command.

isdn bcac service audit

no isdn bcac service audit

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

This commands starts service audits for all triggers. Use the **isdn bcac service audit trigger** command to selectively enable and disable audit triggers.

Examples

The following example shows how to configure service audits on serial interface 2:23:

```
interface serial 2:23
 isdn bcac service audit
```

Related Commands

Command	Description
isdn bcac service audit interface	Specifies that the BCAC service audit needs to be triggered on the entire interface.
isdn bcac service audit trigger	Enables individual BCAC service triggers.
isdn bcac service retry in-serv-on-fail	Specifies that the BCAC service state of the channel needs to be changed to In Service because no acknowledgment was received.
isdn bcac service retry max	Specifies the maximum number of times a BCAC service message can be retransmitted when unacknowledged.
isdn bcac service timer	Changes the value of the BCAC T3M1 or T323 service message timer.
isdn bcac service update linkup	Triggers updates of the BCAC service states between peer nodes through exchange of SERV and SERV ACK messages.

Command	Description
isdn bcac service update provision	Enables the functionality of service status for provisioning ISDN PRI B channels.
isdn service	Takes an individual B channel or an entire PRI interface out of service or sets it to a different channel service state that is passed in to the switch.

isdn bcac service audit interface

To specify that B-Channel Availability Control (BCAC) service audit needs to be triggered on the entire interface, use the **isdn bcac service audit interface** command in interface configuration mode. To change or remove the specification, use the **no** form of this command.

isdn bcac service audit interface

no isdn bcac service audit interface

Syntax Description

This command has no arguments or keywords.

Command Default

The default can be to trigger audits on a single channel, a group of channels, or the entire interface, depending upon the type of trigger set. See the "Usage Guidelines" section for the **isdn bcac service audit trigger** command for the list of triggers.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Use this command when the service audit needs to be triggered on the entire interface when a condition to trigger the service audit is triggered for any channel.

Examples

The following example shows how to configure service audits on serial interface 2:23:

```
interface serial 2:23
 isdn bcac service audit interface
```

Related Commands

Command	Description
isdn bcac service audit	Enables service audits on an interface configured for BCAC.
isdn bcac service audit trigger	Enables individual BCAC service triggers.
isdn bcac service retry in-serv-on-fail	Specifies that the BCAC service state of the channel needs to be changed to In Service because no acknowledgment was received.
isdn bcac service retry max	Specifies the maximum number of times a BCAC service message can be retransmitted when unacknowledged.
isdn bcac service timer	Changes the value of the BCAC T3M1 or T323 service message timer.
isdn bcac service update linkup	Triggers updates of the BCAC service states between peer nodes through exchange of SERV and SERV ACK messages.

Command	Description
isdn bcac service update provision	Enables the functionality of service status for provisioning ISDN PRI B channels.
isdn service	Takes an individual B channel or an entire PRI interface out of service or sets it to a different channel service state that is passed in to the switch.

isdn bcac service audit trigger

To reenable individual B-Channel Availability Control (BCAC) service triggers, use the **isdn bcac service audit trigger** command in interface configuration mode. To disable individual service triggers, use the **no** form of this command.

isdn bcac service audit trigger *number*

no isdn bcac service audit trigger *number*

Syntax Description

number	A number from 1 to 6 that disables specific service triggers; see a list of these triggers in the "Usage Guidelines" section.

Command Default

All triggers are configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

The service audit procedure can be used by the either the user or network side to bring both ends of the interface into agreement about the service status through an exchange of SERV and SERV ACK messages.

Following is the list of triggers with the conditions that cause them. Triggers 1 through 4 are triggered by single-channel audits. Trigger 5 occurs on the entire interface. Trigger 6 applies to a group of channels, which in some cases may apply to the entire interface.

- Trigger 1: Upon receiving an incoming call indicating a channel that is in the out-of-service (OOS) or Maint (maintenance) state.
- Trigger 2: Upon receiving an unsolicited SERV ACK message when the received service status differs from the current status.
- Trigger 3: Upon receiving an unallowed response to a SERV message. An unallowed response means a SERV ACK message, which indicates a higher availability than was sent in the SERV message.
- Trigger 4: Upon receiving an ISDN call clearing message with cause code 44 (requested channel not available) when this message is not caused by "glare," which is a SETUP message collision requesting the same channel.
- Trigger 5: Once every 24 hours on all channels.
- Trigger 6: Once every hour on all channels that are in the OOS or Far-end state.

Examples

The following example shows how to disable service trigger 4 on serial interface 2:23:

```
interface serial 2:23
 no isdn bcac service audit trigger 4
```

Related Commands

Command	Description
isdn bcac service audit	Enables service audits on an interface configured for BCAC.
isdn bcac service audit interface	Specifies that the BCAC service audit needs to be triggered on the entire interface.
isdn bcac service retry in-serv-on-fail	Specifies that the BCAC service state of the channel needs to be changed to In Service because no acknowledgment was received.
isdn bcac service retry max	Specifies the maximum number of times a BCAC service message can be retransmitted when unacknowledged.
isdn bcac service timer	Changes the value of the BCAC T3M1 or T323 service message timer.
isdn bcac service update linkup	Triggers updates of the BCAC service states between peer nodes through exchange of SERV and SERV ACK messages.
isdn bcac service update provision	Enables the functionality of service status for provisioning ISDN PRI B channels.
isdn service	Takes an individual B channel or an entire PRI interface out of service or sets it to a different channel service state that is passed in to the switch.

isdn bcac service retry in-serv-on-fail

To specify that the B-Channel Availability Control (BCAC) service state of the channel needs to be changed to In Service because no acknowledgment was received, use the **isdn bcac service retry in-serv-on-fail** command in interface configuration mode. To change or remove this specification, use the **no** form of this command.

isdn bcac service retry in-serv-on-fail

no isdn bcac service retry in-serv-on-fail

Syntax Description

This command has no arguments or keywords.

Command Default

Original service state is maintained.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Use this command when there is a need to change the service state of a channel to In Service when no acknowledgment is received, even after retransmitting the service message the maximum number of allowed times. If this command is not configured, the original service state is maintained.

Examples

The following example shows how to configure an option whereby, on service message exchange failure, the service state of the concerned channel or channels will be set to In Service:

```
interface serial 2:23
 isdn bcac service retry in-serv-on-fail
```

Related Commands

Command	Description
isdn bcac service audit	Enables service audits on an interface configured for BCAC.
isdn bcac service audit interface	Specifies that the BCAC service audit needs to be triggered on the entire interface.
isdn bcac service audit trigger	Enables individual BCAC service triggers.
isdn bcac service retry max	Specifies the maximum number of times a BCAC service message can be retransmitted when unacknowledged.
isdn bcac service timer	Changes the value of the BCAC T3M1 or T323 service message timer.
isdn bcac service update linkup	Triggers updates of the BCAC service states between peer nodes through exchange of SERV and SERV ACK messages.

Command	Description
isdn bcac service update provision	Enables the functionality of service status for provisioning ISDN PRI B channels.
isdn service	Takes an individual B channel or an entire PRI interface out of service or sets it to a different channel service state that is passed in to the switch.

isdn bcac service retry max

To specify the maximum number of times a B-Channel Availability Control (BCAC) service message can be retransmitted when unacknowledged, use the **isdn bcac service retry max** command in interface configuration mode. To remove or change the specification, use the **no** form of this command.

isdn bcac service retry max *retries*

no isdn bcac service retry max *retries*

Syntax Description

retries	A number from 0 to 127 that determines the maximum number of times that a service message can be retransmitted when unacknowledged. Default is 2.

Command Default

Maximum retransmissions is 2.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

When a SERV message is sent to the far side, SERV message timer T3M1 or T323 is started. If no SERV ACK message is received before these timers expire, the SERV message is retransmitted. This command determines how many times retransmission occurs.

Examples

The following example shows how to set the maximum service message retransmissions on serial interface 2:23 to 50:

```
interface serial 2:23
 isdn bcac service retry max 50
```

Related Commands

Command	Description
isdn bcac service audit	Enables service audits on an interface configured for BCAC.
isdn bcac service audit interface	Specifies that the BCAC service audit needs to be triggered on the entire interface.
isdn bcac service audit trigger	Enables individual BCAC service triggers.
isdn bcac service retry in-serv-on-fail	Specifies that the BCAC service state of the channel needs to be changed to In Service because no acknowledgment was received.
isdn bcac service timer	Changes the value of the BCAC T3M1 or T323 service message timer.
isdn bcac service update linkup	Triggers updates of the BCAC service states between peer nodes through exchange of SERV and SERV ACK messages.

Command	Description
isdn bcac service update provision	Enables the functionality of service status for provisioning ISDN PRI B channels.
isdn service	Takes an individual B channel or an entire PRI interface out of service or sets it to a different channel service state that is passed in to the switch.

isdn bcac service timer

To change the value of the B-Channel Availability Control (BCAC) T3M1 or T323 service message timer, use the **isdn bcac service timer** command in interface configuration mode. To change the timer value, use the **no** form of this command.

isdn bcac service timer *milliseconds*

no isdn bcac service timer *milliseconds*

Syntax Description

milliseconds	Length, in milliseconds (ms), of the T3M1 or T323 service message timer. Valid range is from 500 to 120000 ms; default is 120000 ms.

Command Default

The T3M1 or T323 service message timer defaults to 120000 ms.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

The T3M1 or T323 service message timer is started when a SERV message is sent to the far side.

Examples

The following example shows how to change the service timers to 600 ms on serial interface 2:23:

```
interface serial 2:23
 isdn bcac service timer 600
```

Related Commands

Command	Description
isdn bcac service audit	Enables service audits on an interface configured for BCAC.
isdn bcac service audit interface	Specifies that the BCAC service audit needs to be triggered on the entire interface.
isdn bcac service audit trigger	Enables individual BCAC service triggers.
isdn bcac service retry in-serv-on-fail	Specifies that the BCAC service state of the channel needs to be changed to In Service because no acknowledgment was received.
isdn bcac service retry max	Specifies the maximum number of times a BCAC service message can be retransmitted when unacknowledged.
isdn bcac service update linkup	Triggers updates of the BCAC service states between peer nodes through exchange of SERV and SERV ACK messages.

Command	Description
isdn bcac service update provision	Enables the functionality of service status for provisioning ISDN PRI B channels.
isdn service	Takes an individual B channel or an entire PRI interface out of service or sets it to a different channel service state that is passed in to the switch.

isdn bcac service update linkup

To trigger updates of the B-Channel Availability Control (BCAC) service states between peer nodes through exchange of SERV and SERV ACK messages, use the **isdn bcac service update linkup** command in interface configuration mode. To disable triggering of updates, use the **no** form of this command.

isdn bcac service update linkup

no isdn bcac service update linkup

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

This command updates the service states of *all* the channels to the far side of the interface by exchanging SERV and SERV ACK messages whenever ISDN Layer 2 comes up.

Use the **isdn bcac service update linkup** command to bring the service state of the channels on the interface in synchronization with its peer through the exchange of SERV messages. This synchronizing of the service states will be triggered whenever ISDN Layer 2 comes up. This command can be used with the **isdn service** command in cases where the service state of the channels needs to be synchronized when the ISDN Layer 2 comes up, and in particular, when the ISDN Layer 2 comes up after the router has reloaded.

Examples

The following example shows how to trigger service state updates on serial interface 2:23:

```
interface serial 2:23
 isdn bcac service update linkup
```

Related Commands

Command	Description
isdn bcac service audit	Enables service audits on an interface configured for BCAC.
isdn bcac service audit interface	Specifies that the BCAC service audit needs to be triggered on the entire interface.
isdn bcac service audit trigger	Enables individual BCAC service triggers.

Command	Description
isdn bcac service retry in-serv-on-fail	Specifies that the BCAC service state of the channel needs to be changed to In Service because no acknowledgment was received.
isdn bcac service retry max	Specifies the maximum number of times a BCAC service message can be retransmitted when unacknowledged.
isdn bcac service timer	Changes the value of the BCAC T3M1 or T323 service message timer.
isdn bcac service update provision	Enables the functionality of service status for provisioning ISDN PRI B channels.
isdn service	Takes an individual B channel or an entire PRI interface out of service or sets it to a different channel service state that is passed in to the switch.

isdn bcac service update provision

To enable functionality of service status for provisioning the ISDN B channels, use the **isdn bcac service update provision** command in interface configuration mode. To disable provisioning, use the **no** form of this command.

isdn bcac service update provision

no isdn bcac service update provision

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

This command enables functionality of service status for provisioning the B channels, which for the Cisco implementation happens only on reboot.

Examples

The following example shows how to enable the service service status for provisioning the B channels on serial interface 2:23:

```
interface serial 2:23
 isdn bcac service update provision
```

Related Commands

Command	Description
isdn bcac service audit	Enables service audits on an interface configured for BCAC.
isdn bcac service audit interface	Specifies that the BCAC service audit needs to be triggered on the entire interface.
isdn bcac service audit trigger	Enables individual BCAC service triggers.
isdn bcac service retry in-serv-on-fail	Specifies that the BCAC service state of the channel needs to be changed to In Service because no acknowledgment was received.
isdn bcac service retry max	Specifies the maximum number of times a BCAC service message can be retransmitted when unacknowledged.
isdn bcac service timer	Changes the value of the BCAC T3M1 or T323 service message timer.

Command	Description
isdn bcac service update linkup	Triggers updates of the BCAC service states between peer nodes through exchange of SERV and SERV ACK messages.
isdn service	Takes an individual B channel or an entire PRI interface out of service or sets it to a different channel service state that is passed in to the switch.

isdn bchan-number-order

To configure an ISDN PRI interface to make outgoing call selection in ascending descending, or round-robin order, use the **isdn bchan-number-order** command in interface configuration mode. To restore the default, use the **no** form of this command or reconfigure the interface with the new value.

isdn bchan-number-order {**ascending** | **descending**} [**round-robin**]

no isdn bchan-number-order

Syntax Description

ascending	Makes the outgoing B-channel selection in ascending order as follows: • Channels 1 to 24 for a T1 controller • Channels 1 to 31 for an E1 controller
descending	Makes the outgoing B-channel selection in descending order as follows: • Channels 24 to 1 for a T1 controller • Channels 31 to 1 for an E1 controller
round-robin	(Optional) Enables a round-robin B-channel selection scheme.

Command Default

Selection default is ascending for the network side; descending for the user side.

Command Modes

Interface configuration

Command History

Release	Modification
11.3T	This command was introduced.
12.3(1)	The **round-robin** keyword was added.

Usage Guidelines

This command supports ascending, descending, and round-robin B-channel selection schemes. This command is for PRI configuration only.

This command supports ascending and descending B-channel selection by instructing the router to select the lowest or highest available B channel starting at either channel B1 (ascending) or channel B23 for a T1 and channel B31 for an E1 (descending).

In the ascending B-channel selection scheme, for example, if the channel selected for the last call was channel 14, then if channel *x*, where *x* is any channel number less than or equal to 14, becomes available by the time a channel is selected for the next call, that channel will be selected for the call.

In the round-robin B-channel selection scheme, the next channel selected is the current channel number *x* plus 1 for ascending, or current channel number *x* minus 1 for descending configuration.

When the channel selection software routine reaches channel 1 (the bottom for descending) or channel 23 for T1 and channel 31 for E1 (the top for ascending), the software routine wraps around. An example for a descending configuration: After reaching channel 1, the routine goes back to channel 31 or 23 and then decrements the count from there.

Examples

The following example configures the outgoing B-channel order on a PRI interface to be in ascending order. The router will select the lowest available B channel beginning with channel B1.

```
interface serial 5:10
 isdn bchan-number-order ascending
```

The following example configures the outgoing B-channel order on a PRI interface to be round-robin in ascending order.

```
interface serial 4:23
 isdn bchan-number-order ascending round-robin
```

isdn busy

To set a false busy signal on an ISDN B channel, use the **isdn busy** command in interface configuration mode. To remove this condition, use the **no** form of this command.

isdn busy dsl *number* **b_channel** *number*

no isdn busy dsl *number* **b_channel** *number*

Syntax Description

dsl *number*	Digital subscriber loop (DSL) number.
b_channel *number*	B channel or range of B channels to be set to the false busy signal. B channel numbers range from 1 to 24; 0 indicates the entire interface. The state of the channel, which is obtained using the **show isdn** command with the **status** keyword, can also be added to the command.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This command gives the impression that a call is active when the channel is actually idle.

Use the **b_channel 0** keywords to set a false busy signal on the entire interface.

Use the **show isdn** command with the **status** keyword to display the DSL number and channel state.

Examples

The following example sets the entire PRI interface to a false busy signal; the DSL number was obtained using the **show isdn** command with the **status** keyword, and then used in the command.

```
isdn busy dsl 3 b_channel 0 state 1
```

The following example sets the false busy signal on B channel 11; the DSL number was obtained using the **show isdn** command with the **status** keyword, and then used in the command.

```
isdn busy dsl 3 b_channel 11 state 2
```

Related Commands

Command	Description
isdn service	Takes an individual B channel or an entire PRI interface out of service or sets it to a different channel service state that is passed in to the switch.

isdn call interface

The **isdn call interface** command is replaced by the **isdn test call interface** command. See the **isdn test call interface** command for more information.

isdn caller

To configure ISDN caller ID screening and optionally to enable ISDN caller ID callback for legacy dial-on-demand routing (DDR), use the **isdn caller** command in interface configuration mode. To disable this feature, use the **no** form of this command.

isdn caller *phone-number* [**callback**] [**exact**]

no isdn caller *phone-number* [**callback**] [**exact**]

Syntax Description

phone-number	Remote telephone number for which to screen. Use the letter X to represent a single "don't care" digit. The maximum length of each number is 25 digits.
callback	(Optional) Enables callback.
exact	(Optional) Performs matching on incoming telephone number exactly as entered.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2F	This command was implemented on additional Cisco router and access server platforms.
12.1	The **exact** keyword was added.

Usage Guidelines

This command configures the router to accept calls from the specified number.

Note Caller ID screening requires a local switch or router that is capable of delivering the caller ID to the router. If you enable caller ID screening but do not have such a switch or router, no calls are allowed in. Caller ID screening is available on Cisco 7200 and 7500 series, Cisco 4000 series, Cisco 3000 series, and Cisco 2500 series routers that have one or more BRIs.

When the optional **callback** keyword is used and a call is received from one of the callback numbers, the initial call is rejected (hence, not subject to tolls) and a callback is initiated to that calling number.

When Xs are used in the callback number, dialer caller screening is based on a best match system that uses the *number* of Xs as a criterion. To make callback calls only to specified numbers or ranges of numbers but to accept any other incoming calls, make sure that the number of Xs in any configuration line that uses the **callback** keyword is less than the number of Xs in any configuration line that does not use the keyword.

For example, if you use at most four Xs in the configuration lines with the **callback** keyword, then to accept calls from other numbers use at least five Xs in a configuration line that does not use the keyword.

When a telephone number is entered *without* the **exact** keyword, the software compares each number going from right to left until matching numbers are detected. For example, if the *phone-number* argument is 4085550134, calls from telephone numbers 0134, 50134, 5550134, and 4085550134 would be accepted, but calls from telephone numbers 44 and 4155550134 would be rejected.

If you want to accept a telephone number *exactly* as it is configured, enter it with the **exact** keyword. For example, if the *phone-number* argument is 5550112 and the **exact** keyword is applied, only the telephone number 5550112 is accepted; calls from telephone numbers 408550112 and 50112 would be rejected.

The maximum length of each telephone number is 25 characters. There is no limit on the numbers you can specify per interface.

Examples

The following example configures the router to accept a call containing the numbers 415 555-0134:

```
isdn caller 4155550134
```

The following example configures the router to accept a call only from telephone number 555-0134:

```
isdn caller 5550134 exact
```

In the above example, a call from telephone number 415 555-0134 would be rejected.

The following example configures the router to accept a call with telephone number containing 415 555-01 and any numbers in the last two positions:

```
isdn caller 41555501xx
```

In the following example, callback calls will be made only to numbers in the 555 exchange, but any other telephone number can call in:

```
isdn caller 408555xxxx callback
isdn caller xxxxx
```

Related Commands

Command	Description
show dialer	Displays general diagnostic information for interfaces configured for DDR.

isdn calling-number

To configure an ISDN PRI or BRI interface to present the number of the device making the outgoing call, use the **isdn calling-number** command in interface configuration mode. To remove a previously configured calling number, use the **no** form of this command.

isdn calling-number *calling-number*

no isdn calling-number

Syntax Description

calling-number	Number of the device making the outgoing call; only one entry is allowed.

Command Default

No calling number is presented.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

An interface can have only one ISDN calling-number entry.

For ISDN BRI, this command is intended for use when the ISDN network offers TS014 tariffing, in which devices present the calling (billing) number.

For ISDN PRI, this command is intended for use when the network offers better pricing on calls in which devices present the calling number (that is, the billing number). The calling number information is included in the outgoing setup message.

Note This command cannot be used with German 1TR6 ISDN BRI switches. It can be used with all other switches, including all ISDN PRI switches.

Examples

The following example first configures the T1 interface, then configures the D channel interface to present the billing number 4233570925 when it makes outgoing calls:

```
controller t1 1/1
 framing esf
 linecode b8zs
 pri-group timeslots 1-23
 isdn switchtype primary-4ess
!
interface serial 1/1:23
 ip address 10.1.1.1 255.255.255.0
 encapsulation ppp
 isdn calling-number 4233570925
 dialer map ip 10.1.1.2 name mymap 14193460913
```

In the following example, the ISDN BRI interface is configured to present the number 5550112 when it makes outgoing calls:

```
interface bri 0
 isdn calling-number 5550112
```

Related Commands

Command	Description
interface dialer	Configures a BRI interface and enters interface configuration mode.
interface serial	Specifies a serial interface created on a channelized E1 or channelized T1 controller (for ISDN PRI, CAS, or robbed bit signaling).

isdn calling-party-num

To specify whether the network-provided or user-provided calling party number is selected when two calling party numbers are sent from a primary NET5 switch on ISDN, use the **isdn calling-party-num** command in interface configuration mode. To reset the default value, use the **no** form of this command.

isdn calling-party-num {**network-provided** | **user-provided**} [**first** | **last**]

no isdn calling-party-num

Syntax Description

network-provided	Network-provided calling party number.
user-provided	User-provided calling party number.
first	(Optional) Specifies that the first number provided as the calling number information element (IE) should be used to display the calling party number.
last	(Optional) Specifies that the last number provided as the calling number IE should be used to display the calling party number.

Command Default

The first user-provided calling party number is used to display the calling party number.

Command Modes

Interface configuration

Command History

Release	Modification
12.2	This command was introduced for the primary ISDN NET5 switch.
12.3(7)T	The **first** and **last** keywords were added and this command was integrated into this release.
12.3(7)	This command was integrated into this release.

Usage Guidelines

The **isdn calling-party-num** command is useful for customers who use network-provided and user-provided calling party numbers for accounting purposes. The selected number will be used by dialer filters, such as those configured with the **isdn caller** command.

Use the optional **first** and **last** keywords for instances when more than one calling number is sent. By default, the first number is used, and subsequent numbers are not recognized. If you specify **last** in the command syntax, the last calling number displays in the caller ID display.

An example application of the **last** keyword can be seen in an enterprise customer using multiple 800 numbers in an intelligent network service from a PSTN service provider. If a PSTN user dials (from 919-555-1111, for example) the customer's 800 number, the PSTN service provider routes the call to the customer's telephone number (for example, 408-555-0100) based on the 800 number. The incoming ISDN SETUP message from the PSTN has two user-provided calling party IEs:

- The 800 number that the user dialed
- The calling party number of the PSTN user (919-555-1111)

Because the Cisco IOS gateway always uses the first user-provided calling party number by default, the IP phone user is able to see only the 800 number and not the actual calling party number of the PSTN user, unless the **last** keyword is entered in the command syntax.

Examples

The following example shows how to configure the ISDN switch to accept network-provided calling party numbers. If more than one number is provided, the last number provided is used as the calling party number:

```
interface Serial0:23
 no ip address
 encapsulation ppp
 dialer rotary-group 1
 isdn switch-type primary-net5
 isdn protocol-emulate network
 isdn incoming-voice modem
 isdn calling-number 1111111
 isdn calling-party-num network-provided last
 isdn T310 40000
 no cdp enable
```

Related Commands

Command	Description
isdn caller	Configures ISDN caller ID screening and optionally enables ISDN caller ID callback for legacy DDR.
isdn calling-number	Configures an ISDN PRI or BRI interface to present the number of the device making the outgoing call.

isdn channel-id invert extended-bit

To invert the value of the extend bit (0x80) in the last octet of the channel ID information element, use the **isdn channel-id invert extended-bit** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

isdn channel-id invert extended-bit

no isdn channel-id invert extended-bit

Syntax Description

This command has no arguments or keywords.

Command Default

The last octet of the channel ID information element is not inverted.

Command Modes

Interface configuration

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

Use this command if you use a primary-DMS 100 switch type to ensure compatibility with a Setup or Call Proceeding message containing a channel ID information element. This command can be used only with ISDN PRI.

This command replaces the **isdn-flip-chan-flag** command.

Examples

The following example configures the router to invert the extended bit in the last octet of the channel ID information element:

```
isdn channel-id invert extended-bit
```

isdn conference-code

To activate three-way call conferencing, use the **isdn conference-code** command in interface configuration mode. To disable three-way call conferencing, use the **no** form of this command.

isdn conference-code *code*

no isdn conference-code

Syntax Description

code	Number from 0 to 999 (ISDN conference code).

Command Default

The default code is 60.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

Use this command if your ISDN line is connected to an NI1 or a Nortel DMS-100 Custom switch. Your telephone service provider should provide an ISDN conference code when you order three-way call conferencing.

Examples

The following example specifies 61 as the ISDN conference code:

```
isdn conference-code 61
```

isdn disconnect interface

The **isdn disconnect interface** command is replaced by the **isdn test disconnect interface** command. See the **isdn test disconnect interface** command for more information.

isdn disconnect-cause

To send a specific ISDN cause code to the switch, use the **isdn disconnect-cause** command in interface configuration mode. To return to the default condition, use the **no** form of this command.

isdn disconnect-cause {*cause-code-number* | **busy** | **not-available**}

no isdn disconnect-cause

Syntax Description

cause-code-number	Sends a cause code number (submitted as integer in the range of 1 through 127) to the switch.
busy	Sends the USER-BUSY code to the switch.
not-available	Sends the CHANNEL-NOT-AVAILABLE code to the switch.

Command Default

The default condition is no cause code override. If the **isdn disconnect-cause** command is not configured, the default cause codes for the application are sent.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

The **isdn disconnect-cause** command overrides specific cause codes (such as modem availability and resource pooling) that are sent to the switch by ISDN applications. When the **isdn disconnect-cause** command is implemented, the configured cause codes are sent to the switch; otherwise, the default cause codes for the application are sent. ISDN protocol errors are still reflected in the cause codes and are not overridden.

Examples

The following example sends the CHANNEL-NOT-AVAILABLE code to the ISDN switch:

```
interface serial0:20
 isdn disconnect-cause not-available
```

Related Commands

Command	Description
isdn disconnect-cause	Sends a specific ISDN cause code to the switch.

isdn fast-rollover-delay

To control the timing between successive dial attempts, use the **isdn fast-rollover-delay** command in interface configuration mode. To remove or change a value, use the **no** form of this command.

isdn fast-rollover-delay *seconds*

no isdn fast-rollover-delay

Syntax Description

seconds	Number of seconds between dial attempts.

Command Default

No default timer.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

This command provides a timer separate from the dialer wait-for-carrier timer to control the amount of time that elapses before calls are redialed. This delay is provided to allow the old call to be torn down completely before the new call is attempted.

The **isdn fast-rollover-delay** command is necessary on some ISDN switches because the new call may be attempted before the old call is completely torn down, which causes the second call or the callback to fail.

Use this command when *all* the following conditions are true:

- A BRI has two phone numbers configured, one for each B channel.
- You are dialing in to this BRI.
- You have a dialer map or dialer string for each phone number.
- The first call succeeds but the second call continuously fails.

When these conditions occur, set the **isdn fast-rollover-delay** command to 5 seconds and try again. A delay of 5 seconds should cover most cases. Configure sufficient delay to make sure that the ISDN RELEASE_COMPLETE message has been sent or received before the fast rollover call is made. Use the **debug isdn q931** command to display this information.

When the **isdn fast-rollover-delay** command is configured on a client requesting callback, the callback client first confirms whether the callback server has placed a call back to the callback client before dialing any subsequent numbers.

Examples

The following partial example sets the fast-rollover delay that is suggested when all the conditions specified in the list in the "Usage Guidelines" are true:

```
isdn fast-rollover-delay 5
```

Related Commands

Command	Description
dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites.
dialer wait-for-carrier-time (map-class)	Specifies the length of time to wait for a carrier when dialing out to the dial string associated with a specified map class.
ppp callback (DDR)	Enables a dialer interface that is not a DTR interface to function either as a callback client that requests callback or as a callback server that accepts callback requests.

isdn flip-chan-flag

The **isdn flip-chan-flag** command is replaced by the **isdn channel-id invert extended-bit** command. See the **isdn channel-id invert extended-bit** command for more information.

isdn guard-timer

To enable a managed timer for authentication requests, use the **isdn guard-timer** command in interface configuration mode. To reset the timer to its default value, use the **no** form of this command.

isdn guard-timer *milliseconds* [**on-expiry** {**accept** | **reject**}]

no isdn guard-timer

Syntax Description

milliseconds	Number of milliseconds that the network access server (NAS) waits for a response from the AAA security server. The valid range is from 1000 through 20,000.
on-expiry	(Optional) Determines whether calls are accepted or rejected after the specified number of milliseconds has expired. If no expiry action is selected, calls are rejected.
accept	(Optional) Calls are accepted if the guard-timer expires before AAA responds.
reject	(Optional) Calls are rejected if the guard-timer expires before AAA responds.

Command Default

The default timer value is eight (8) seconds and calls are rejected when the timer expires.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

The guard-timer starts when the DNIS number is sent to AAA for authentication. When the timer expires, authentication ends and the call is accepted or rejected based on the configured expiry action.

Examples

The following example sets the guard-timer to six (6) seconds and specifies that the call should be rejected if AAA does not respond within that interval:

```
interface serial 1/0/0:23
isdn guard-timer 6000 on-expiry reject
```

Related Commands

Command	Description
aaa preauth	Enables authentication using DNIS numbers.

isdn incoming alerting add-PI

To add a Progress Indicator (PI) in an incoming ALERTING messages during ISDN B-channel cut-through, use the **isdn incoming alerting add-PI** command in interface configuration mode. To remove the indicator, use the **no** form of this command.

isdn incoming alerting add-PI

no isdn incoming alerting add-PI

Syntax Description

This command has no arguments or keywords.

Command Default

On North American ISDN switches, the default behavior is to add the PI in incoming ALERTING messages. On ISDN switches compliant with the European Telecommunications Standards Institute (ETSI), the default behavior is to *not* add the PI in incoming ALERTING messages.

Command Modes

Interface configuration

Command History

Release	Modification
12.3	This command was introduced for ISDN BRI and PRI interfaces.

Usage Guidelines

The **isdn incoming alerting add-PI** and **no isdn incoming alerting add-PI** commands provide a way for switch types conforming to different standards to handle B-channel cut-through. These commands apply to both ISDN BRI and PRI connections.

North American switch types such as the 5ESS, 4ESS, DMS, and NI allow cut-through when an ALERTING message is received. ISDN B-channel cut-through for customer premises equipment (CPE) should happen upon receipt of a channel ID Information Element (IE) in the CALL_PROC message. For this reason, the default on North American ISDN switches is to add the PI in incoming ALERTING message.

On ETSI-compliant ISDN switches, the default behavior is to *not* add the PI in incoming ALERTING messages. But ETSI also specifies that when the remote device is playing tones or announcements, it should also include the PI in the ALERTING message. This is not the default behavior for ETSI-compliant switches, but the **isdn incoming alerting add-PI** command allows Cisco IOS software to support this behavior.

The **isdn incoming alerting add-PI** and **no isdn incoming alerting add-PI** commands can be used on switches that do not want to add the PI in incoming ALERTING messages and on those switches that cannot handle or do not want the PI in incoming ALERTING messages.

Examples

Because the the **isdn incoming alerting add-PI** command is the default for a North American ISDN switch, the following example shows that when the interface configuration is displayed, the **isdn incoming alerting add-PI** command is not listed, even if it was explicitly configured:

```
Router(config)# interface BRI1/0
Router(config-if)# no ip address
Router(config-if)# isdn switch-type basic-dms100
Router(config-if)# isdn spid1  40876726760101 5459374
Router(config-if)# isdn spid2 51076726760101 5459375
Router(config-if)# isdn incoming-voice voice
Router(config-if)# isdn incoming alerting add-PI
Router(config-if)# end
Router(config)# end
Router# show running interface BRI1/0
Building configuration...

Current configuration : 167 bytes
!
interface BRI1/0
 no ip address
 isdn switch-type basic-dms100
 isdn spid1  40876726760101 5459374
 isdn spid2 51076726760101 5459375
 isdn incoming-voice voice
end
```

The following example shows that when the the **no isdn incoming alerting add-PI** command is configured on a North American ISDN switch, the command is listed in the interface configuration:

```
Router(config)# interface BRI1/0
Router(config-if)# no isdn incoming alerting add-PI
Router(config-if)# end
Router(config)# end
Router# show running interface BRI1/0
Building configuration...

Current configuration : 201 bytes
!
interface BRI1/0
 no ip address
 isdn switch-type basic-dms100
 isdn spid1  4087672676 5459374
 isdn spid2 51076726760101 5459375
 isdn incoming-voice voice
 no isdn incoming alerting add-PI
end
```

Because the default for ETSI-compliant ISDN switches is **no isdn incoming alerting add-PI**, the following example shows that when the the **isdn incoming alerting add-PI** command is added to the configuration for a NET3 switch, the command is listed in the interface configuration:

```
Router(config-if)# no ip address
Router(config-if)# isdn switch-type basic-net3
Router(config-if)# isdn spid1  40876726760101 5459374
Router(config-if)# isdn spid2 51076726760101 5459375
Router(config-if)# isdn incoming-voice voice
Router(config-if)# isdn incoming alerting add-PI
Router(config-if)# end
Router(config)# end
Router# show running interface BRI1/0
Building configuration...
```

```
Current configuration : 165 bytes
!
interface BRI1/0
 no ip address
 isdn switch-type basic-net3
 isdn spid1 40876726760101 5459374
 isdn spid2 51076726760101 5459375
 isdn incoming-voice voice
 isdn incoming alerting add-PI
end
```

If the configuration for the NET3 switch were changed back to contain **no isdn incoming alerting add-PI**, the command would not be listed in the interface configuration, because this is the default behavior for ETSI-compliant switches:

```
Current configuration : 165 bytes
!
interface BRI1/0
 no ip address
 isdn switch-type basic-net3
 isdn spid1  40876726760101 5459374
 isdn spid2 51076726760101 5459375
 isdn incoming-voice voice
end
```

isdn incoming ie

To specify that the **channel-id** and **display** information elements (IEs) may be accepted in incoming ISDN messages, use the **isdn incoming ie** command in interface configuration mode. To indicate that one of these IEs may not be accepted in incoming ISDN messages, use the **no** form of this command.

isdn incoming ie {**channel-id** [**accept-qsig-variant**] | **display** {**dms250** | **transparent**}} [**redirecting-selection** {**first** | **last**}]

no isdn incoming ie {**channel-id** [**accept-qsig-variant**] | **display** {**dms250** | **transparent**}} [**redirecting-selection** {**first** | **last**}]

Syntax Description

channel-id	Information element pertaining to the channel ID.
accept-qsig-variant	(Optional) Specifies that the ISDN D channel supports QSIG switches that send a variant (the D-channel selector bit is not set) of the normal channel ID IE usage for calls that are "signaling only."
display	Information element pertaining to the text display.
dms250	(Optional) Configures the router to accept the ISDN incoming message when octet 3 of the display IE has been modified for compatibility with the DMS-250 switch type. **Note** This keyword is available only when the **display** keyword is entered. This option controls the handling of octet 3 of the display IE in the incoming message, and applies only when DMS-100 or DMS-250 switches must interoperate with other switch types.
transparent	(Optional) Configures the router to accept the ISDN message when the display IE has been packed in the incoming message without modifying or inserting octet 3. This is the default behavior for non-DMS switches. **Note** This keyword is available only when the **display** keyword is entered. This option controls the handling of octet 3 of the display IE in the incoming message, and applies only when DMS-100 or DMS-250 switches must interoperate with other switch types.
redirecting-selection	(Optional) Selects the first or the last redirect number (RDN) when multiple RDN IEs are received on an incoming ISDN call. The **first** keyword selects the first RDN received; the **last** keyword selects the last RDN received. **Note** The **first** and **last** keywords are available only when the **redirecting-selection** keyword is entered.

Command Default

Supported IEs are accepted in applicable incoming messages by default. The channel ID does not accept IEs with the QSIG variant, and the display IE for DMS-250 (transparent) is not altered. When multiple RDN IEs are received on an incoming ISDN call, the last RDN is automatically selected.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.4(7)	The **accept-qsig-variant** keyword was added.
12.4(8)	The **redirecting-selection**, **first**, and **last** keywords were added.

Usage Guidelines

Incompatibility between ISDN switch types at the originating and terminating gateways can prevent provided IEs from being passed end-to-end. Cisco devices can be configured to transparently accept incoming unsupported IEs, allowing full interworking between different switch types.

Use the **isdn incoming ie** command to configure a Cisco router to transparently accept unsupported IEs to its peer. IEs may be sent in any codeset. However IEs can be manually controlled using only the **isdn incoming ie** command when they are sent in codeset 0. IEs will be accepted only in applicable message types.

To configure the router so it will not accept channel ID and display IEs, use the **no isdn incoming ie** command.

Note If the **isdn gateway-max-interworking** command is enabled, IEs that are invalid for some destination switch types may be passed. This can result in the occurrence of undesirable events.

Note If the **isdn protocol-emulate** command is switched between the network and user configurations, the **isdn outgoing ie** command reverts to its default setting. The **isdn outgoing ie** command must be reissued to restore the manual configuration.

Examples

The following example configures the serial interface for the QSIG D channel to accept “malformed” channel-id IEs:

```
interface se3/0:3:23
isdn incoming ie channel-id accept-qsig-variant
end
```

The following example configures the serial interface to select the first RDN IE when multiple RDN IEs are received on an incoming ISDN call:

```
interface se3/0:3:23
isdn incoming ie redirecting-selection first
end
```

Related Commands

Command	Description
isdn gateway-max-interworking	Prevents an H.323 gateway from checking for ISDN protocol compatibility and dropping IEs in call messages.
isdn outgoing ie	Specifies that an IE may be passed in outgoing ISDN messages.
isdn protocol-emulate	Configures an ISDN data or voice port to emulate network or user functionality.

isdn incoming-voice

To route all incoming voice calls to the modem and determine how they will be treated, use the **isdn incoming-voice** command in interface configuration mode. To disable the setting or return to the default, use the **no** form of this command.

isdn incoming-voice {**voice** | **data** [**56** | **64**] | **modem** [**56** | **64**]}

no isdn incoming-voice {**voice** | **data** [**56** | **64**] | **modem** [**56** | **64**]}

Syntax Description

voice	Incoming voice calls bypass the modems and be handled as a voice call.
data	Incoming voice calls bypass the modems and will be handled as digital data. If the **data** keyword is selected, you can specify a B-channel bandwidth of either **56** kbps or **64** kbps.
modem	Incoming voice calls are passed over to the digital modems, where they negotiate the appropriate modem connection with the far-end modem. If this keyword is selected, you can specify a B-channel bandwidth of either **56** kbps or **64** kbps. If no argument is entered, the default value is 64.

Command Default

If you do not enter the **56** or **64** keywords after the **data** keyword, the default value will be 64 kbps.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced for ISDN PRI interfaces.
11.1AA	This command was implemented on ISDN BRI interfaces.
12.0(2)XC	This command was implemented on ISDN BRI interfaces.
11.2	This command was enhanced for channelized T1 and integrated into Cisco IOS Release 11.2.
11.3NA	This command was implemented on additional Cisco router and access server platforms.
12.0(3)T	This command was implemented on additional Cisco router and access server platforms.

Usage Guidelines

Unless you specify otherwise, all calls received by the router and characterized as voice calls are treated as normal ISDN calls, which are handled as digital data and not passed over to the modem. Ordinarily, a data device ignores incoming voice calls, but the tariff structure for data and voice calls might make it less expensive to do “data over voice” calls.

If you use the **voice** keyword, incoming ISDN voice calls will be treated as voice calls and handled by either a modem or a voice DSP as directed by CSM.

If the default value is configured and the bearer capability of the incoming call is the **voice** keyword, the call will be rejected.

To answer incoming voice calls at a configured rate (overriding the incoming data rate in the call), use the **data** keyword.

To establish speedier connections for analog calls to the router, use the **isdn incoming-voice** command with the **modem** keyword to have voice calls routed through digital modems (as pulse-code modulated analog data) instead of being treated as digital data.

Configure this command on each D channel in the access server or router. Incoming circuit-switched data calls are not affected by this command.

Note Use the **isdn incoming-voice modem** command only when you are using ISDN. You must use this command to carry voice over a modem when using ISDN PRI.

Examples

The following example designates incoming ISDN voice calls to be treated as voice calls:

```
interface 10
 isdn incoming-voice voice
```

The following example for channelized T1 configures the D channel (hence, all B channels) to answer all incoming voice calls at 56 kbps:

```
interface serial 0:23
 isdn incoming-voice data 56
```

The following example routes all incoming voice calls through the modem as analog data:

```
interface BRI 0/0
 isdn incoming-voice modem
```

The following example enables incoming and outgoing ISDN calls to route to the modems using the D channel serial interface:

```
interface serial 0:23
 isdn incoming-voice modem
```

isdn layer1-emulate

To configure the Layer 1 operation of a BRI voice port as clock master (NT) or slave (TE), use the **isdn layer1-emulate** command in interface configuration mode. To restore the default (user), use the **no** form of this command.

isdn layer1-emulate {**user** | **network**}

no isdn layer1-emulate

Syntax Description

user	Physical interface operation in clock slave mode (as TE).
network	Physical interface operation in clock master mode (as NT).

Command Default

Layer 1 port operation is as user (TE functionality as clock slave).

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on the MC3810.
12.1(3)XI	This command was implemented on the Cisco 2600 and Cisco 3600 series.

Usage Guidelines

If you use the **no isdn layer1-emulate network** command, the physical layer port operation defaults to user.

Examples

The following example configures the Layer 1 operation of a BRI voice port as QSIG clock slave (TE):

```
configure terminal
 interface bri 1
 isdn layer1-emulate user
```

Related Commands

Command	Description
isdn protocol-emulate (**dial**)	Configures the Layer 2 and Layer 3 port protocol of a BRI voice port or a PRI interface to emulate NT (network) or TE (user) functionality.
network-clock-priority	Specifies the clock-recovery priority for the BRI voice ports in a BVM.

isdn layer2-flap

To send RESTART or STATUS ENQUIRY messages over the ISDN PRI line when a Layer 2 link flap and recovery occurs, use the **isdn layer2-flap** command in interface configuration mode. To disable sending these messages, use the **no** form of this command.

isdn layer2-flap {**restart** | **status-enq**}

no isdn layer2-flap {**restart** | **status-enq**}

Syntax Description

restart	Sends a RESTART message to the remote peer.
status-enq	Sends a STATUS-ENQUIRY message to the remote peer.

Command Default

This command is disabled by default, in which case, no RESTART or STATUS-ENQUIRY messages are sent in the event of a Layer 2 flap and recovery.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

When you include the **isdn layer2-flap** command in the ISDN configuration, the router (as a user agent) sends a RESTART or STATUS-ENQUIRY message to the remote peer when a Layer 2 flap and recovery occurs. This notification enhances the gateway's ability to gracefully recover from a Layer 2 flap or failure error condition. This graceful recovery frees gateway resources to handle future calls and to increase the call completion rate.

Use the **isdn layer2-flap** command with the **isdn timer t309** command in your configuration. The **isdn timer t309** command enables the router to hold or drop calls. The effect of using these two commands in the event of a Layer 2 flap and recovery is summarized as follows:

- Layer 2 failure and then a Layer 2 recovery before the T309 timer expires (with T309 timer enabled)—STATUS-ENQUIRY message
- Layer 2 failure and then a Layer 2 recovery after the T309 timer expires or with the T309 timer not enabled—RESTART message

Examples

The following example shows how to enable the router to send a RESTART message when a Layer 2 flap or failure error condition occurs and recovery happens after the T309 timer has expired (or the T309 timer is not enabled):

```
isdn layer2-flap restart
```

Related Commands

Command	Description
isdn timer t309	Changes the value of the T309 timer to clear the network connection and to release the B channel and call reference when a data-link disconnection occurs.

isdn leased-line bri

To configure an ISDN BRI for leased-line service, or to configure both 64-kbps leased-line and ISDN service on the same BRI, use the **isdn leased-line bri** command in global configuration mode. To remove or change channel configurations, use the **no** form of this command.

isdn leased-line bri *number/number* [**b1** | **b2** | **128** | **144** | *Return-key*]

no isdn leased-line bri *number/number* [**b1** | **b2** | **128** | **144** | *Return-key*]

Syntax Description

number/number	BRI interface numbers (enter the slash to separate the physical interface numbers).
b1	(Optional) Uses channel B1 as a 64-kbps leased line and channel B2 for ISDN service on a single ETSI NET3 switch on a Cisco 800 series router.
b2	(Optional) Uses channel B2 as a 64-kbps leased line and channel B1 for ISDN service on a single ETSI NET3 switch on a Cisco 800 series router.
128	(Optional) Combines B1 and B2 channels for 128-kbps leased-line service.
144	(Optional) Combines B1 and B2 channels for 144-kbps leased-line service.
Return-key	(Optional) Configures two 64-kbps leased lines instead of two B channels. Press the Return or Enter key at the end of the **isdn leased-line bri** *number/numbe*r command instead of entering a keyword.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2F	This command was introduced.
12.2(4)T	The **b1** and **b2** keywords were added to allow the BRI channels on an ETSI NET3 switch on a Cisco 800 series router to be split into leased-line and ISDN services.

Usage Guidelines

Use the **isdn leased-line bri** command to configure an ISDN BRI for leased-line service by aggregating two BRI B channels into a single pipe at a speed of 128 or 144 kbps, or configuring both a 64-kbps leased line and ISDN service on a single European Telecommunications Standards Institute (ETSI) NET3 switch on Cisco 800 series routers.

This command also supports two separate 64-kbps leased lines, where the BRI interface is configured as two separate leased lines instead of two B channels. No keyword is required for this configuration; just press the Return or Enter key at the end of the **isdn leased-line bri** *number/number* command string. This configuration is different than using the **128** keyword, which configures a single 128-kbps leased line.

When you use the **no isdn leased-line bri** command to change the channel configuration, you must also perform a system reload in order for the change to take effect.

When you use an ISDN BRI interface for access over leased lines, configure the ISDN BRI as a synchronous serial interface and do not configure ISDN calling and called numbers.

Examples

The following example configures the BRI interface for leased-line access at 128 kbps in Japan:

```
isdn leased-line bri0/0 128
```

Because of the leased-line—not dialed—environment, configuration of ISDN called and calling numbers is not needed and not used. The BRI 0 interface is henceforth treated as a synchronous serial interface, with the default High-Level Data Link Control (HDLC) encapsulation.

The following example configures BRI channel B1 for 64-kbps leased-line service and channel B2 for ISDN service:

```
isdn switch-type basic-net3
isdn leased-line bri0/0 b1
!
interface bri0/0
 ip address 10.1.1.1 255.255.255.0
 no ip address
 dialer pool-member 1

interface bri0/0:1
 ip address 10.1.1.2 255.255.255.0
 encapsulation ppp
 no ip address
```

The following example configures two 64-kbps leased lines:

```
isdn leased-line bri0/0
```

Related Commands

Command	Description
isdn switch-type (BRI)	Specifies the central office switch type on the ISDN BRI interface.

isdn logging

To enable logging of ISDN syslog messages, use the **isdn logging** command in global configuration mode. To disable logging, use the **no** form of this command.

isdn logging

no isdn logging

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

This command supports syslog logging of the following ISDN events:

- ISDN Layer 2 Up and Down events at severity 3.
- ISDN SERV, SERV ACK, RESTART, RESTART ACK, and STATUS ENQ messages at severity 4.
- ISDN SERV status audit messages for various triggers at different severities.

Examples

The following example shows how to configure ISDN syslog logging:

```
isdn logging
```

Related Commands

Command	Description
isdn bchan-number-order	Configures an ISDN PRI interface to make outgoing call selection in ascending, descending, or round-robin order.
isdn protocol-emulate	Configures an ISDN data or voice port to emulate network or user functionality.

isdn map

To override the default ISDN type and plan generated by the router with custom values, use the **isdn map** command in interface configuration mode. To revert to the default ISDN type and plan, use the **no** form of this command.

isdn map address {{*address* | *reg-exp*} **plan** *plan* **type** *type* | **transparent**}

no isdn map address {{*address* | *reg-exp*} **plan** *plan* **type** *type* | **transparent**}

Syntax Description

address	Specifies that the default ISDN type and plan will be overridden.
address	Address map, which can be to either the calling number or the called number. This argument specifies the address for which the ISDN type and plan will be overridden.
reg-exp	Regular expression for pattern matching. This argument specifies that the ISDN type and plan will be overridden for addresses that match the regular expression.
plan *plan*	ISDN numbering plan. Valid values for the *plan* argument are as follows: • **any**—Any type of dialed number. • **data**—X.121 data numbering plan. • **ermes**—European Radio Message System numbering plan. • **isdn**—E.164 ISDN/Telephony numbering plan. • **national**—Number called to reach a subscriber in the same country, but outside the local network. • **private**—Private numbering plan. • **reserved**—Reserved for extension. • **telex**—F.69 telex numbering plan. • **unknown**—Number of a type that is unknown by the network.
type *type*	ISDN number type. Valid values for the *type* argument are as follows: • **abbreviated**—Abbreviated representation of the complete number as supported by this network. • **any**—Any type of called number. • **international**—Number called to reach a subscriber in another country. • **national**—Number called to reach a subscriber in the same country, but outside the local network. • **network**—Administrative or service number specific to the serving network. • **reserved**—Reserved for extension. • **subscriber**—Number called to reach a subscriber in the same local network. • **unknown**—Number of a type that is unknown by the network.
transparent	Specifies that the ISDN type and plan values received in raw messages from the ISDN originating gateway will take priority over the ISDN type and plan values received in the H.225 SETUP messages.

Command Default The default is the ISDN type and plan generated by the router.

Command Modes Interface configuration

Command History

Release	Modification
12.0(6)T	This command was introduced.
12.3(7)T	The **transparent** keyword was added.

Usage Guidelines The default ISDN type and plan can be overridden with custom values on a per-number basis or for numbers that match regular expression patterns.

If you use the **isdn map** command to configure custom values for the ISDN type and plan, these values take priority over any other ISDN type and plan values. The order of precedence for ISDN type and plan values is as follows, beginning with the highest precedence:

- Type and plan values configured with the **isdn map** command.
- Type and plan values from voice translation rules specified with the **rule (voice translation-rule)** command.
- Values received in the H.225 SETUP messages.
- Values received from the ISDN originating gateway in raw messages.

Configuring the **isdn map** command with the **transparent** keyword results in raw messages received from the ISDN originating gateway receiving priority over H.225 SETUP messages. When the **isdn map** command is configured with the **transparent** keyword, the order of precedence for ISDN type and plan values is as follows:

- Type and plan values configured with the **isdn map** command.
- Type and plan values from voice translation rules specified with the **rule (voice translation-rule)** command.
- Values received from the ISDN originating gateway in raw messages.
- Values received in the H.225 SETUP messages.

Examples The following example overrides any plan and type used for any ISDN calls with a called or calling number that exactly matches 123:

```
interface serial1:23
 isdn map address 123 plan isdn type unknown
```

The following example overrides any plan and type used for ISDN calls with a called or calling number that begins with the numerals 12:

```
interface serial1:23
 isdn map address 12.* plan data type subscriber
```

The following example matches any number that ends with the number 7:

```
interface serial1:23
 isdn map address .*7 plan data type subscriber
```

The following example reverses the precedence of ISDN type and plan values received from the ISDN originating gateway and from the H.225 SETUP message:

```
interface serial1:23
 isdn map address transparent
```

Related Commands

Command	Description
rule (voice translation-rule)	Defines a translation rule.

isdn modem-busy-cause

The **isdn modem-busy-cause** command is replaced by the **isdn disconnect-cause** command. See the **isdn disconnect-cause** command for more information.

isdn negotiate-bchan

To enable the router to accept a B channel that is different from the B channel requested in the outgoing call setup message, use the **isdn negotiate-bchan** command in interface configuration mode. To restore the default condition, use the **no** form of this command.

isdn negotiate-bchan [**resend-setup**] [**cause-codes** *cause-code1* [*cause-code2...cause-code16*]]

no isdn negotiate-bchan [**resend-setup**] [**cause-codes** *cause-code1* [*cause-code2...cause-code16*]]

Syntax Description

resend-setup	(Optional) Enables a single reattempt of a setup message if a disconnect message with a cause code of 44 is received before alerting. Supports NET5 and NI2 PRI switches only. (A Code 44 cause code means that the requested circuit or channel is not available. For more information, refer to the International Telecommunications Union [ITU] Q.850 standard.)
cause-codes *cause-code*	(Optional) Specifies up to 16 cause codes that will alert the gateway to reattempt a call. This reattempt may or may not be on the same B channel as the previous attempt. The value of each *cause-code* argument is a number from 1 to 127 corresponding to an ISDN cause code number. If the **cause-codes** keyword is entered, at least one cause code must be entered or the command will not be accepted. Separate multiple cause code entries with spaces. Once the **cause-codes** keyword is entered, cause code 44 will no longer cause a call reattempt unless 44 is specifically entered as one of the cause codes. **Note** The validity of each cause code is not checked by the gateway.

Command Default

B channel negotiation is not enabled. Most PRI switch types set the default channel ID to Exclusive in the setup message. An exception is the NI2 switch, which sets the default to Preferred.

If the **cause-codes** keyword is not entered, it is assumed that you want ISDN cause code 44.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2	The **resend-setup** keyword was implemented for NET5 and NI2 PRI switches.
12.2(15)T	The **cause-codes** keyword was implemented on the Cisco AS5350 and Cisco AS5400.

Usage Guidelines

The **isdn negotiate-bchan** command enables the router to negotiate the B channel by setting the channel ID information element to Preferred in the setup message. If this command is not configured, the channel ID is set to the default of the switch, which is usually Exclusive. Exclusive means that only the requested B channel is accepted. If the requested B channel is not available, the call is cleared.

The **isdn negotiate-bchan** command is supported for all PRI switch types. The **resend-setup** keyword is supported only for NET5 and NI2 switches. This command is not supported for BRI interfaces.

The **cause-codes** keyword allows you to configure the gateway to reattempt a call when a cause code other than 44 is received from the PSTN.

Refer to the "ISDN Cause Codes" table in the appendix of the *Cisco IOS Debug Command Reference* for a list of ISDN cause codes.

Examples

The following example enables a call to be reattempted when a disconnect with cause code of 44 is received before alerting:

```
interface serial0:23
 isdn negotiate-bchan resend-setup
```

The following example shows that cause codes 34, 44, and 63 have been configured:

```
interface serial0:23
 isdn negotiate-bchan resend-setup cause-codes 34 44 63
```

Related Commands

Command	Description
isdn bchan-number-order	Configures an ISDN PRI interface to make an outgoing call selection in ascending or descending order.
isdn switch-type (PRI)	Specifies the Central Office switch type on the ISDN PRI interface.

isdn not-end-to-end

To override the speed that the network reports it will use to deliver the call data, use the **isdn not-end-to-end** command in interface configuration mode. To disable the configured end-to-end speed, use the **no** form of this command.

isdn not-end-to-end {**56** | **64**}

no isdn not-end-to-end

Syntax Description

56	Answers all voice calls at 56 kbps.
64	Answers all voice calls at 64 kbps.

Command Default

The default line speed is 64 kbps.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

Note The **isdn not-end-to-end** command is valid only when an incoming Layer 3 Setup message contains a Progress Information Element in the message. The command is validated on a call-by-call basis, depending upon the message.

This command might be needed to handle incoming calls properly. Although a call might originate at a speed of 56 kbps, the network or internetworking networks might improperly deliver the call to the user at a speed of 64 kbps. This creates a speed mismatch and causes the data to be garbled. Enabling this command makes the router look more closely at the information elements of the incoming call to determine a speed.

A speed mismatch can occur when the source and destination ISDN ports do not belong to the same network.

Examples

The following example sets the line speed for incoming calls to 56 kbps:

```
isdn not-end-to-end 56
```

isdn nsf-service

To configure Network Specific Facilities (NSF) on an ISDN PRI for outgoing calls configured as voice calls, use the **isdn nsf-service** command in interface configuration mode. To remove NSF on an ISDN PRI, use the **no** form of this command.

isdn nsf-service {**megacom** | **sdn**}

no isdn nsf-service {**megacom** | **sdn**}

Syntax Description

megacom	Dial voice calls using AT&T Megacom NSF.
sdn	Dial voice calls using AT&T SDN NSF.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.3(5)T	This command was introduced.

Usage Guidelines

This command is used specifically on a PRI (channelized T1) to request NSF services supported on primary AT&T 4ESS (**primary-4ess**) switch types only.

Examples

The following example sets outgoing voice calls to use AT&T SDN NSF:

```
interface serial 0:23
 isdn-nsf-service sdn
```

Related Commands

Command	Description
dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites.
dialer voice-call	Configures the dialer map class for an NSF dialing plan to support outgoing voice calls.
map-class dialer	Defines a class of shared configuration parameters associated with the dialer map command for outgoing calls from an ISDN interface and for PPP callback.

isdn number

To change the maximum number of digits in a called number information element, use the **isdn number** command in interface configuration mode.

isdn number [**called enbloc** *limit*]

Syntax Description

called	Attributes for the ISDN number of the called party.
enbloc	Allows the ISDN terminal to send the ISDN number of the called party in a single SETUP message.
limit	Maximum number of digits allowed in a SETUP message, in the range from 1 to 32.

Command Default

20 digits

Command Modes

Interface configuration

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

The maximum number of digits sent in the initial call SETUP is defaulted to 20 digits. The default of 20 digits chosen because some switches cannot handle more than 20 digits. Some countries in Europe are changing their calling plans and will require calls to be made using more than 20 digits.

The **isdn number called enbloc** command is used when the maximum number of octets in the called number information element in a SETUP message must be changed from the 20-digit default to the user desired limit. With this command, the user can configure the maximum number from 1 to 32 digits. This command is available for ISDN interfaces and applicable to both BRI and PRI interfaces.

Note This command is enabled for only the following switch types:
BRI_NET3_STYPE
PRI_NET5_SYTPE

Examples

The following example configures the called number information element for 32 digits:

```
Router(config-if) isdn number called enbloc 32
```

isdn outgoing ie

To specify that an information element (IE) may be passed in outgoing ISDN messages, use the **isdn outgoing ie** command in interface configuration mode. To specify that an IE may not be passed in outgoing ISDN messages, use the **no** form of this command.

isdn outgoing ie *ie* [**codeset_0** {**message** *message-type* | **shiftcodeset codeset_6** } | **dms250** | **nooct3** | **transparent**]

no isdn outgoing ie *ie* [**codeset_0** {**message** *message-type* | **shiftcodeset codeset_6** } | **dms250** | **nooct3** | **transparent**]

Syntax Description

ie	The IE to pass in outgoing ISDN messages. Valid values for the *ie* argument are listed in Table 7.
codeset_0	(Optional) Specifies that the IE will be packed in ISDN codeset 0. Codeset 0 is the International Telecommunication Union (ITU) standard codeset. Codeset 0 is the default codeset; however you must issue the **codeset_0** keyword if you want to specify a message type.
message *message-type*	(Optional) Specifies a particular outgoing message to pass an IE in. Valid values for the *message-type* argument are listed in Table 8. If you do not specify a message type, the IE will be passed in all applicable message types.
dms250	(Optional) Specifies that octet 3 of the display IE is modified for compatibility with the DMS-250 switch type before it is packed in the setup message. **Note** This keyword is available only when **display** is entered for the *ie* argument.This option controls the handling of octet 3 of the display IE in the setup message, and applies only when DMS-100 or DMS-250 switches must interoperate with other switch types. See the "Usage Guidelines" section for more information.
nooct3	(Optional) Specifies that octet 3 of the display IE is stripped from the display IE before it is packed in the setup message. This is the default behavior for DMS-100 and DMS-250 switches. **Note** This keyword is available only when **display** is entered for the *ie* argument. This option controls the handling of octet 3 of the display IE in the setup message, and applies only when DMS-100 or DMS-250 switches must interoperate with other switch types. See the "Usage Guidelines" section for more information.

transparent	(Optional) Specifies that the display IE is packed in the setup message without modifying or inserting octet 3. This is the default behavior for non-DMS switches. **Note** This keyword is available only when **display** is entered for the *ie* argument. This option controls the handling of octet 3 of the display IE in the setup message, and applies only when DMS-100 or DMS-250 switches must interoperate with other switch types. See the "Usage Guidelines" section for more information.
shiftcodeset codeset_6	(Optional) Specifies that the display IE should be packed in codeset 6 in outgoing messages, rather than codeset 0. **Note** This keyword is available only when **display** is entered for the *ie* argument, and can be configured only for 4ESS or 5ESS switch types. See the "Usage Guidelines" section for more information.

Command Default

Supported IEs are passed in applicable outgoing messages by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(7)T	The **isdn outgoing ie** command was introduced and replaces the **isdn outgoing ie redirecting-number** command.

Usage Guidelines

Incompatibility between ISDN switch types at the originating and terminating gateways can prevent provided IEs from being passed end-to-end. Cisco devices can be configured to transparently pass unsupported IEs, allowing full interworking between different switch types.

Use the **isdn outgoing ie** command to configure a Cisco router to transparently pass unsupported IEs to its peer. IEs may be packed in any codeset. However, the **isdn outgoing ie** command can manually control IEs packed in codeset 0 only. IEs will be passed only in applicable message types.

The router can be configured to not pass IEs using the **no isdn outgoing ie** command.

You may use the **isdn gateway-max-interworking** command to globally configure the Cisco router to transparently pass all unsupported IEs to its peer. However, the **isdn outgoing ie** command provides much finer control.

Note If the **isdn gateway-max-interworking** command is enabled, IEs that are invalid for some destination switch types may be passed. This can cause undesirable events to occur.

Note If the **isdn protocol-emulate** command is switched between the **network** and **user** keyword configurations, the **isdn outgoing ie** command reverts to its default setting. The **isdn outgoing ie** command must be reissued to restore the manual configuration.

Options That Are Specific to the Display IE

DMS-100 and DMS-250 switch types format the display IE using an additional octet that is not used by other switch types, octet 3. Octet 3 specifies the calling party name, and is mandatory for DMS-100 and DMS-250 switch types. DMS-100 and DMS-250 switches each use a different value for octet 3. For these switch types to interoperate properly with each other or with other switch types, octet 3 must be modified. Use the **dms250**, **nooct3**, or **transparent** keyword to control the interoperation of a DMS-100 or DMS-250 switch with other switch types.

4ESS and 5ESS switch types do not support the display IE. If a message with a display IE packed in codeset 0 is passed out of a PRI interface with one of these switch types, the display IE will be dropped. However, these switches will pass any unknown IE that is packed in codeset 6. Use the **shiftcodeset codeset_6** keywords to specify that the display IE should be packed in codeset 6 before being sent out a PRI interface with a 4ESS or 5ESS switch.

Table 7 lists the IEs that can be entered for the *ie* argument. Not all IEs can be controlled using the **isdn outgoing ie** command.

Table 7 ISDN IE Values

IE	IE Description
called-number	The number the call is placed to.
called-subaddr	The subadress the call is placed to.
caller-number	The number the call originates from.
caller-subaddr	The subadress the call originates from.
connected-number	If a disconnect occurs during a conference, this indicates the number of the remaining caller.
connected-subaddr	If a disconnect occurs during a conference, this indicates the subadress of of the remaining caller.
display	Information about the text display.
extended-facility	Information about extended facility requests.
facility	Information about facility requests.
high-layer-compat	Information about higher layer compatibility.
low-layer-compat	Information about lower layer compatibility.
network-facility	Information about network facility requests.
notify-indicator	Information about notifications.
progress-indicator	Information about the call in progress.
redirecting-number	The number that is redirecting the call.
user-user	Information about the users at either end of the call.

Table 8 lists the ISDN messages that can be entered for the *message-type* argument.

Table 8 ISDN Outgoing Message Types

Outgoing Message Type	Message Type Description
alerting	Alerting message.
callproc	Call proceeding message.

Table 8 ISDN Outgoing Message Types (continued)

Outgoing Message Type	Message Type Description
connect	Connect message.
disconnect	Disconnect message.
facility	Facility message.
information	Information message.
progress	Progress message.
rel_comp	Release complete message.
release	Release message.
setup	Setup message.
setup-ack	Setup acknowledge message.

Examples

The following example enables the passing of the redirect number IE in for all applicable outgoing message types for a PRI-NI switch:

```
interface Serial 0:15
 no ip address
 isdn switch-type primary-ni
 isdn incoming-voice modem
 no cdp enable
 isdn outgoing ie redirecting-number
```

The following example enables the passing of the called number IE in an outgoing alert message for a PRI-NI switch:

```
interface Serial 0:15
 no ip address
 isdn switch-type primary-ni
 isdn incoming-voice modem
 no cdp enable
 isdn outgoing ie called-number codeset_0 message alerting
```

The following example configures a DMS-100 switch to reformat octet 3 for interoperability with a DMS-250 switch:

```
interface Serial 0:23
 no ip address
 dialer idle-timeout 999999
 isdn switch-type primary-dms100
 isdn incoming-voice modem
 no cdp enable
 isdn outgoing ie display dms250
```

The following example configures a DMS-100 switch to drop octet from the display IE:

```
interface Serial0:23
 no ip address
 dialer idle-timeout 999999
 isdn switch-type primary-dms100
 isdn incoming-voice modem
 no cdp enable
 isdn outgoing ie display nooct3
```

The following example configures a DMS-100 switch to pack the display IE without modifying octet 3:

```
interface Serial0:23
 no ip address
 dialer idle-timeout 999999
 isdn switch-type primary-dms100
 isdn incoming-voice modem
 no cdp enable
 isdn outgoing ie display transparent
```

The following example configures a switch to pack the display IE in codeset 6 before sending it out of an interface configured with a 4ESS switch:

```
interface Serial 0:23
 no ip address
 isdn switch-type primary-4ess
 isdn incoming-voice modem
 no cdp enable
 isdn outoing ie display codeset_0 shiftcodeset codeset_6
```

Related Commands

Command	Description
isdn gateway max-interworking	Prevents an H.323 gateway from checking for ISDN protocol compatibility and dropping IEs in call messages.
isdn outgoing display-ie	Enables the display IE to be sent in the outgoing ISDN message if provided by the upper layers, such as voice or modem.
isdn protocol-emulate	Configures an ISDN data or voice port to emulate network or user functionality.

isdn outgoing ie redirecting-number

Note Beginning in Cisco IOS Release 12.3(7)T, the **isdn outgoing ie redirecting-number** command is replaced by the **isdn outgoing ie** command. See the **isdn outgoing ie** command for more information.

To enable passing of the redirect number information element (IE) in the setup message from the Cisco router to its peer, use the **isdn outgoing ie redirecting-number** command in interface configuration mode. To disable passing of the redirect number IE in the setup message from the Cisco router to its peer, use the **no** form of this command.

isdn outgoing ie redirecting-number

no isdn outgoing ie redirecting-number

Syntax Description

This command has no arguments or keywords.

Command Default

The redirecting number IE will be passed in the setup message for the following switch types only by default:

- basic-dms100
- basic-ni
- primary-dms100
- primary-4ESS
- primary-5ESS
- primary-ni
- primary-ni2c

For all other switch types, the redirecting number IE will not be passed by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(15)T5	This command was introduced.
12.3(7)T	This command was replaced by the **isdn outgoing ie** command.

Usage Guidelines

Use the **isdn outgoing ie redirecting-number** command to enable passing of the redirect number IE in the setup message from the Cisco router to its peer. Some switch types do not support the redirect number IE, so to ensure compatibility with a peer that does support the redirect number IE you may enable the passing of the redirect number IE using the **isdn outgoing ie redirecting-number** command.

Note If the **isdn protocol-emulate** command is switched between the **network** and **user** keyword configurations, the **isdn outgoing ie** command reverts to its default setting. The **isdn outgoing ie** command must be reissued to restore the manual configuration.

Examples

The following example enables the passing of the redirect number IE for a NET5 switch on a serial interface:

```
interface Serial 0:15
 isdn outgoing ie redirecting-number
```

Related Commands

Command	Description
isdn outgoing ie	Specifies that an IE should be passed in outgoing ISDN messages.
isdn protocol-emulate	Configures an ISDN data or voice port to emulate network or user functionality.

isdn outgoing-voice

To set information transfer capability on outgoing calls for all switch types, use the **isdn outgoing-voice** command in interface configuration mode. To revert to the default state, use the **no** form of this command.

isdn outgoing-voice info-transfer-capability {**3.1kHz-audio** | **speech**}

no isdn outgoing-voice

Syntax Description

info-transfer-capability	Specifies information transfer capability for voice calls.
3.1kHz-audio	Sets capability to 3.1 kHz audio.
speech	Sets capability to speech.

Command Default

No information transfer capabilities set.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

This command is used on outgoing voice calls only, and sets standard information transfer capability.

Examples

The following example sets information transfer capability on outgoing voice calls to speech:

```
interface serial 0:23
 isdn outgoing-voice info-transfer-capability speech
```

Related Commands

Command	Description
isdn incoming-voice	Specifies how to process incoming ISDN voice and data calls.

isdn overlap-receiving

To enable overlap receiving on an ISDN interface, use the **isdn overlap-receiving** command in interface configuration mode. To disable overlap receiving on an ISDN interface, use the **no** form of this command.

isdn overlap-receiving [**T302** *milliseconds*]

no isdn overlap-receiving

Syntax Description

T302 *milliseconds*	(Optional) The number of milliseconds that the T302 timer should wait before expiring. Valid values for the *milliseconds* argument range from 500 to 20000. The default value is 10000 (10 seconds).

Command Default

Overlap receiving is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

In some situations, the default timer value of the T302 timer is too long. You can shorten the duration of the timer by specifying the **T302** keyword with the number of milliseconds necessary.

When configuring outbound peer matching and overlap receiving, use the **isdn overlap-receiving** command with the **destination-pattern** command. You must configure the commands to allow the router to wait for all the digits to be received before the call is routed. To do this, use the **T** control character after the digits in the destination pattern specified with the **destination-pattern** command. Optionally, you can shorten the duration of the T302 timer when you specify the **isdn overlap-receiving** command.

Examples

The following example shows how to enable overlap receiving on the ISDN interface:

```
interface serial 0:23
 isdn overlap-receiving
```

The following example shows how to enable overlap receiving on the ISDN interface and set the T302 timer to 2 seconds:

```
interface serial 0:23
 isdn overlap-receiving T302 2000
```

Related Commands

Command	Description
destination-pattern	Specifies either the prefix or full E.164 telephone number to be used for a dial peer.
isdn service	Takes an individual B channel or an entire PRI interface out of service or sets it to a different channel service state that is passed in to the switch.

isdn overlap-receiving calltypes all

To enable overlap receiving for all call types, use the **isdn overlap-receiving calltypes all** command in interface configuration mode. To disable overlap receiving for all call types, use the **no** form of this command.

isdn overlap-receiving calltypes all

no isdn overlap-receiving calltypes all

Syntax Description

This commands has no arguments or keywords.

Command Default

Overlap receiving is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

The **isdn overlap-receiving calltypes all** command enables overlap receiving for all nonvoice calls that use data dial peers, and it enables an ISDN interface to proceed with a call when a sufficient number of digits are received. These digits are determined by the **destination-pattern** command under the data dial peer configuration.

This command is supported on the Cisco AS5350, Cisco AS5400, and Cisco AS5850 routers.

Examples

The following example shows how to enable overlap receiving:

```
interface serial 0:23
 isdn overlap-receiving calltypes all
```

Related Commands

Command	Description
destination-pattern	Specifies either the prefix or full E.164 telephone number to be used for a dial peer.
dial-peer no-match disconnect-cause	Disconnects the incoming ISDN or CAS call when no inbound voice or modem dial peer is matched.
isdn overlap-receiving	Enables overlap receiving on an ISDN interface.

isdn piafs-enabled

To enable the PRI to take Personal Handyphone Internet Access Forum Standard (PIAFS) calls on MICA technologies modems, use the **isdn piafs-enabled** command in interface configuration mode. To disable the function, use the **no** form of this command.

isdn piafs-enabled

no isdn piafs-enabled

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(2)XH	This command was introduced on the Cisco AS5300.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T and support was added for the Cisco AS5800.
12.2(2)XA	Support was added for PIAFS version 2.1 using Cisco MICA 8.2.3.0 was added. **Note** PIAFS 2.1 is not supported on Cisco AS5800 universal access servers for this release.
12.2(2)XB1	This command was implemented on the Cisco AS5800 platform.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples

The following example shows how to enable the PRI to take PIAFS calls:

```
Router(config)# interface serial 0:23
Router(config-if)# isdn piafs-enabled
```

isdn point-to-point-setup

To configure the ISDN port to send SETUP messages on the static terminal endpoint identifier (TEI), use the **isdn point-to-point-setup** command in interface configuration mode. To restore the default, use the **no** form of this command.

isdn point-to-point-setup

no isdn point-to-point-setup

Syntax Description

This command has no arguments or keywords.

Command Default

The BRI port sends SETUP messages on the static TEI (TEI 127).

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)XI	This command was introduced.

Usage Guidelines

This command only applies if a static TEI has been activated with the **isdn static-tei command.**

Examples

The following example configures the BRI port to send SETUP messages on the static TEI:

```
interface bri 1
isdn point-to-point-setup
```

Related Commands

Command	Description
isdn tei-negotiation (global)	Configures when Layer 2 becomes active and ISDN TEI negotiation occurs.

isdn protocol-emulate

To emulate the network side of an ISDN configuration for a PRI Net5 or PRI NTT switch type, use the **isdn protocol-emulate** command in interface configuration mode. To disable ISDN emulation, use the **no** form of this command.

isdn protocol-emulate {**network** | **user**}

no isdn protocol-emulate {**network** | **user**}

Syntax Description

network	Network side of an ISDN configuration.
user	User side of an ISDN configuration.

Command Default

No default behavior or values

Command Modes

Interface configuration mode

Command History

Release	Modification
12.0(3)XG	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 concentrator.
12.1(1)T	This command was introduced in the T train.
12.2(2)XB	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was implemented on the Cisco IAD2420 series. This command is not supported on the access servers in this release.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.3	This command was enhanced to support network emulation capability on the Lucent 4ESS, 5ESS, and Nortel DMS-100 ISDN switch types. These switch types can be configured as a network, but no additional changes were made and not all network side features are supported.
12.3(8)T	Added support for the PRI NTT switch type.

Usage Guidelines

- The current ISDN signaling stack can emulate the ISDN network side, but it does not conform to the specifications of the various switch types in emulating the network side.
- This command enables the Cisco IOS software to replicate the public switched network interface to a Private Branch Exchange (PBX).
- To emulate NT (network) or TE (user) functionality, use this command to configure the layer 2 and layer 3 port protocol of a BRI voice port or a PRI interface.

- Use this command to configure the Cisco AS5300 PRI interface to serve as either the primary QSIG slave or the primary QSIG master. To disable QSIG signaling, use the **no** form of this command; the layer 2 and layer 3 protocol emulation defaults to **user**.
- This feature is supported for the PRI Net5 and PRI NTT switch types.

Examples

The following example configures the interface (configured for Net5) to emulate the network-side ISDN:

```
Router(config)# int s0:15
Router(config-if)# isdn protocol-emulate network
```

The following example configures the layer 2 and layer 3 function of T1 PRI interface 23 to act as the QSIG master (NT):

```
interface serial 1:23
 isdn protocol-emulate network
```

The following example configures the layer 2 and layer 3 function of a BRI voice port to operate as QSIG slave (TE):

```
interface bri 1
 isdn protocol-emulate user
```

The following example configures the layer 2 and layer 3 function of an E1 PRI interface to operate as QSIG slave (TE):

```
interface serial 4:23
 isdn protocol-emulate user
```

Related Commands

Command	Description
isdn bchan-number-order	Configures an ISDN PRI interface to make outgoing call selection in ascending, descending, or round-robin order.
isdn logging	Enables logging of ISDN syslog messages.
isdn switch-type (PRI)	Specifies the central office switch type on the ISDN PRI interface.
network-clock-priority	Specifies the clock-recovery priority for the BRI voice ports in a BVM.
pri-group nec-fusion	Configures the NEC PBX to support FCCS.
show cdapi	Displays the CDAPI.
show rawmsg	Displays the raw messages owned by the required component.

isdn reject

To reject an incoming ISDN BRI or PRI call based on type, use the **isdn reject** command in interface configuration mode. To re-allow the incoming call type, use the **no** form of this command.

isdn reject {**cause** *cause-code* | **data** [**56** | **64**] | **piafs** | **v110** | **v120** | **vod** | **voice** [**3.1khz** | **7khz** | **speech**]}

no isdn reject {**cause** *cause-code* | **data** [**56** | **64**] | **piafs** | **v110** | **v120** | **vod** | **voice** [**3.1khz** | **7khz** | **speech**]}

Syntax Description

cause *cause-code*	Rejects call based on cause code value.
data [**56** | **64**]	Rejects incoming data call. If the optional **56** or **64** keyword is not specified, all data calls, including data over voice, are rejected. Use the optional **56** keyword to reject data coming in at 56 kbps. Use the optional **64** keyword to reject data coming in at 64 kbps.
piafs	Rejects incoming Personal Handyphone Internet Access Forum Standard (PIAFS) calls.
v110	Rejects incoming V.110 calls.
v120	Rejects incoming V.120 calls.
vod	Rejects incoming voice-over-data calls, or calls characterized by 64 kbps unrestricted digital data. Although the bearer capability for these calls indicates an incoming data call, the call is treated as voice over data. See the "Usage Guidelines" for more information.
voice [**3.1khz** | **7khz** | **speech**]	Rejects incoming voice and modem calls characterized by one of three information transfer capability types: 3.1 kHz, 7 kHz, and speech, which are defined by using, in corresponding order, the **3.1khz**, **7khz**, and **speech** keywords. If none of the optional keywords is used, all voice calls except voice over data are rejected.

Command Default

Incoming calls are rejected based on D-channel bearer capability information (cause code 65).

Command Modes

Interface configuration

Command History

Release	Modification
12.0	This command was introduced.
12.2	The **cause** *cause-code* keyword and argument were added.

Usage Guidelines

The **isdn reject** command rejects incoming calls based on D-channel bearer capability information.

If this command is configured with the **cause** *cause-code* keyword and argument, it will override the default value and use the configured cause code specified to reject the call. For example, if the **isdn reject data** command is configured so that data calls are rejected with cause code set to 65 ("bearer

capability not implemented" and the default), you can change the cause code to 2, so that data calls will then be rejected with cause code 2. Refer to the *ISDN Switch Types, Codes, and Values* appendix in the *Cisco IOS Debug Command Reference* for a list of ISDN cause code values.

The settings for the **isdn incoming-voice** interface configuration command determine how the call is handled based on bearer capability information, as follows:

- **isdn incoming-voice voice**—Calls bypass the modem and are handled as a voice call.
- **isdn incoming-voice data**—Calls bypass the modem and are handled as digital data.
- **isdn incoming-voice modem**—Calls are passed to a digital modem and the call negotiates the appropriate modem connection with the far-end modem.

When the ISDN interface is configured for incoming voice with the **isdn incoming-voice voice** command and the ISDN bearer capability indicates the call as unrestricted digital data (i = 0x8890), the call is handled as voice over data.

You can assign as many reject incoming call type statements as needed to reject unwanted calls on the ISDN interface.

This command works on any Cisco platform that supports ISDN PRI and BRI interfaces.

Examples

The following example configuration rejects all incoming data and voice-over-data calls but accepts voice calls:

```
interface serial 2/0:23
  no ip address
  no logging event link-status
  dialer-group 1
  isdn switch-type primary-net5
  isdn incoming-voice voice
  isdn map address 222 plan isdn type national
  isdn T309 80000
  isdn reject data
  isdn reject vod
  isdn reject v120
  isdn reject v110
  isdn reject piafs
```

The following example sets the ISDN interface to reject incoming PIAFS calls:

```
interface serial 2/0:23
 isdn reject piafs
```

The following example sets cause code 21 to reject all incoming data calls:

```
interface serial 2/0:23
 isdn reject data
 isdn reject cause 21
```

Related Commands

Command	Description
isdn incoming-voice	Specifies how to process incoming ISDN voice and data calls.

isdn send-alerting

To specify that an Alerting message be sent before a Connect message when making ISDN calls, use the **isdn send-alerting** command in interface configuration mode. To disable the Alerting information element, use the **no** form of this command.

isdn send-alerting

no isdn send-alerting

Syntax Description

This command has no arguments or keywords.

Command Default'

This command is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

Some switches may want an Alerting message to be sent by the router before sending a Connect message. This is usually seen in a voice and data type of network.

Examples

In the following example, the **isdn send-alerting** command applies to an ISDN BRI interface:

```
interface BRI0
 description connected to PBX 61886
 ip address 172.26.1.1 255.255.255.0
 encapsulation ppp
 isdn send-alerting
 isdn sending-complete
 dialer idle-timeout 20
 dialer map ip 172.26.1.2 name name1 61884
 dialer map ip 172.26.1.3 name name2 61885
 dialer-group 1
 ppp authentication chap
```

Related Commands

Command	Description
isdn sending-complete	Specifies that the Sending Complete IE is included in the outgoing Setup message.

isdn sending-complete

To specify that the Sending Complete information element (IE) is included in the outgoing Setup message, use the **isdn sending-complete** command in interface configuration mode. To disable the Sending Complete information element, use the **no** form of this command.

isdn sending-complete

no isdn sending-complete

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The Sending Complete IE tells the switch that all the digits and information necessary for the call are contained in this Setup message.

Some switches in some countries want a Sending Complete information element to be included in the outgoing Setup message to indicate that the entire number is included. The Sending Complete IE is required in Hong Kong and Taiwan, and the **isdn sending-complete** command forces it to be sent.

Examples

In the following example, the **isdn sending-complete** command applies to an ISDN BRI interface:

```
interface BRI0
 description connected to PBX 61886
 ip address 172.31.1.1 255.255.255.0
 encapsulation ppp
 isdn sending-complete
 dialer idle-timeout 20
 dialer map ip 172.31.1.2 name name1 61884
 dialer map ip 172.31.1.3 name name2 61885
 dialer-group 1
 ppp authentication chap
```

The following example enables sending complete IE information on a serial interface:

```
interface serial 0:15
 description connected to PBX 61886
 ip address 10.1.1.1 255.255.255.0
 encapsulation ppp
 isdn sending-complete
 dialer idle-timeout 20
 dialer map ip 10.1.1.2 name name1 61884
```

```
dialer map ip 10.1.1.3 name name3 61885
dialer-group 1
ppp authentication chap
```

Related Commands

Command	Description
isdn send-alerting	Specifies that an Alerting message be sent before a Complete message when making ISDN calls.

isdn service

To take an individual B channel or an entire PRI interface out of service or set it to a different channel service state that is passed to a time-division multiplexing (TDM) switch at the Public Switched Telephone Network (PSTN), use the **isdn service** command in interface configuration mode. To remove the configuration, use the **no** form of the command.

isdn service [**dsl** *number* | **nfas-int** *number*] **b_channel** *number* **state** {**0** | **1** | **2**} [**hard** | **immediate** | **soft**]

no isdn service

Syntax Description

dsl *number*	(Optional) Digital subscriber loop number; displayed with the **show isdn status** command. DSL numbers range from 0 to 31.
nfas-int *number*	(Optional) The Non-Facility Associated Signaling (NFAS) member interface number that has a B channel or channels to which you want to do maintenance.
b_channel *number*	B channel, or a range of B channels separated by a dash, to be set with the passed-in state value. Specifying *number* as 0 sets the entire PRI interface to a specific state value. B channel numbers range from 0 to 31, or 0 for the complete interface.
state {**0** | **1** | **2**} [**hard** | **immediate** | **soft**]	Desired channel service state to be set on the channels. Note that the ISDN service messages are sent only for switch types that support them. A state change from lower availability to higher availability is possible only after a service acknowledgment (SERV ACK) message is received. The following channel service state values are supported: **0**—In Service. Restore a channel or channels to service. **1**—Maintenance. An intermediate state between In Service and Out of Service. **2**—Out of Service (OOS). Take a channel or channels out of service. The switch might drop calls on active channels. Additionally, you can provide one of the following optional keywords to control when to modify the state of the B channel or channels: • **hard**—(Optional) Sends the service (SERV) message immediately, even if the channel is active, and clears the call if there is any. If there is no active call, this keyword has the same effect as using the **immediate** keyword. • **immediate**—(Optional) This keyword is the default. It sends the service message, but does not clear the call. The switch might clear the active channels if the state is changed to Maintenance or OOS. • **soft**—(Optional) Moves the active channel or channels to a pending change state. The service message is sent after the channel becomes idle.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2	The **dsl** keyword was made optional.
12.3	The **hard**, **immediate**, and **soft** keywords were added as **state** keyword options.

Usage Guidelines

Use this command to manage channels on ISDN NFAS and Primary Rate Interfaces (PRI) on Cisco routers.

Use the **b_channel 0** keywords to set the entire PRI interface to the specified state value.

Use the optional **soft** and **immediate state** keywords to take switches down gracefully, without impacting calls in progress. The **hard** keyword sends an immediate service message to the connected switch that will disconnect active B channels and drop active calls.

To display the digital subscriber loop (DSL) number on NFAS interfaces, use the **show isdn service** EXEC command. To find the NFAS interface value, use the **pri-group** T1 controller configuration command.

This command can be used only on North American switch types, because it supports the service message.

Examples

The following example sets all the PRI B channel on the interface to the maintenance state:

```
isdn service b_channel 0 state 1
```

The following example restores B channels 2 through 4; the DSL number was obtained using the **show isdn** command with the **status** keyword, and the DSL number was then used in the command:

```
isdn service dsl 2 b_channel 2-4 state 0
```

The following example sets B channels 13 to 24 to the OOS state:

```
isdn service nfas-int 3 b_channel 13-24 state 1
```

In the following example, the first statement sets B channels 17 through 20 to the maintenance state and marks any busy B channel (or channels) as pending; the channel will change to the service state only when it becomes idle. The second statement will cause the service message to be sent immediately and will clear the call. If there is no call, the second statement will have the same effect as the **immediate** keyword, that is, it will send the service message, but will not clear the call.

```
isdn service b_channel 17-20 state 1 soft
isdn service b_channel 21 state 1 hard
```

Related Commands

Command	Description
isdn bcac service audit	Enables service audits on an interface configured for BCAC.
isdn bcac service audit interface	Specifies that the BCAC service audit needs to be triggered on the entire interface.

Command	Description
isdn bcac service audit trigger	Enables individual BCAC service triggers.
isdn bcac service retry in-serv-on-fail	Specifies that the BCAC service state of the channel needs to be changed to In Service because no acknowledgment was received.
isdn bcac service retry max	Specifies the maximum number of times a BCAC service message can be retransmitted when unacknowledged.
isdn bcac service timer	Changes the value of the BCAC T3M1 or T323 service message timer.
isdn bcac service update linkup	Triggers updates of the BCAC service states between peer nodes through exchange of SERV and SERV ACK messages.
isdn bcac service update provision	Enables the functionality of service status for provisioning ISDN PRI B channels.
show isdn	Displays the information about memory, Layer 2 and Layer 3 timers, and the status of PRI channels.

isdn silent-boot

To prevent the transmission and receipt of ISDN packets by the router during the boostrap loading process, use the **isdn silent-boot** command in global configuration mode. To allow the transmission and receipt of ISDN packets by the router during the boostrap loading process, use the **no** form of this command.

isdn silent-boot

no isdn silent-boot

Syntax Description

This command has no arguments or keywords.

Command Default

The transmission and receipt of ISDN packets by the router is allowed during the bootstrap process.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

ISDN traffic will not be sent from any interfaces on the router (ISDN BRI or PRI) when you use the **isdn silent-boot** command. Disabling the ISDN traffic on the router is appropriate when the router is part of a hunt group that is accepting incoming ISDN calls because you do not want the router to receive calls until after it has reloaded and is ready to accept the incoming calls.

Examples

The following example disables ISDN traffic:

```
Router(config)# isdn silent-boot
```

isdn snmp busyout b-channel

To enable PRI B channels to be busied out via Simple Network Management Protocol (SNMP), use the **isdn snmp busyout b-channel** command in interface configuration mode. To prevent B channels from being busied out via SNMP, use the **no** form of this command.

isdn snmp busyout b-channel

no isdn snmp busyout b-channel

Syntax Description

This command has no arguments or keywords.

Command Default

The default value is TRUE; that is, setting busyout using SNMP is allowed.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

To busy out B-channels on a PRI, the ISDN switch must support service messages. The **isdn snmp busyout b-channel** command sets the MIB object, cpmDS0BusyoutAllow, indicating whether or not the switch supports service messages, thereby allowing the busyout of B channels. When the network access server receives an SNMP request for a busyout, it checks the value of this object. If the **no isdn snmp busyout b-channel** command is configured, the busyout request fails.

Examples

The following example allows the busyout of B-channels for serial interface 0:23:

```
configure terminal
interface serial 0:23
isdn snmp busyout b-channel
```

isdn spid1, isdn spid2

To associate up to three ISDN local directory numbers (LDNs) provided by your telephone service provider to the first service profile identifier (SPID), use the **isdn spid1** command in interface configuration mode. To disable the specified SPID and prevent access to the switch, use the **no** form of this command.

isdn spid1 *spid-number ldn* [*ldn*] [*ldn*]

no isdn spid1 *spid-number ldn* [*ldn*] [*ldn*]

To associate up to three ISDN LDNs provided by your telephone service provider to the second service SPID, use the **isdn spid2** interface configuration command. To disable the specified SPID and prevent access to the switch, use the **no** form of this command.

isdn spid2 *spid-number ldn* [*ldn*] [*ldn*]

no isdn spid2 *spid-number ldn* [*ldn*] [*ldn*]

Syntax Description

spid-number	Number identifying the service to which you have subscribed. This value is assigned by the ISDN service provider and is usually a 10-digit telephone number with additional digits such as 40855501220101.
ldn	ISDN LDN, which is a 7-digit number assigned by the service provider. You can optionally specify a second and third LDN.

Command Default

A default SPID number and ISDN local directory numbers are not defined.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.3	This command was introduced.
12.0(3)T	This command was enhanced with the option of associating the SPID with up to three LDNs.

Usage Guidelines

This command applies only to North America and is required for DMS-100 and National ISDN switches. Typically, DMS-100 and National ISDN switch implementations using BRI interfaces with SPIDS require two terminal endpoint identifiers (TEIs), two SPIDS, and two phone numbers. If you want to take advantage of both B channels, it is advised you configure the router with the LDN value after the SPID.

Note Some DMS-100 and National ISDN switch installations may be configured as a "hunt group" whereby all calls are initially forwarded to the primary number. Under these circumstances, you should not configure the LDN. You can determine this by enabling the **debug isdn q931** command. If the endpoint identifier (EID) information element is delivered in the incoming setup message, then the switch is addressing the TEIs with the EID, instead of the LDN.

If you want the SPID to be automatically detected, you can specify 0 for the *spid-number* argument.

The ISDN switch checks for the LDN to determine whether both channels can be used to transmit and receive data. If there is not an LDN present, then only the B1 channel can be used for full-duplex communication. However, the B2 channel can still be used to make outgoing calls.

If you include the local directory number in the **no** form of this command, access to the switch is permitted, but the other B channel may not be able to receive incoming calls.

Examples

The following example defines, on the router, a SPID and LDN for the B1 channel:

```
isdn spid1 41555501130101 5550113
```

The following example shows how to specify that the SPID should be automatically detected, that the primary ISDN local directory number is 4085550111, and that the secondary number is 4085550122:

```
isdn spid1 0 4085550111 4085550122
```

The following example defines, on the router, a SPID and LDN for the B2 channel:

```
isdn spid2 41555501140101 5550114
```

The following example specifies that the SPID should be automatically detected, that the primary ISDN local directory number is 4085550111, and that the secondary number is 4085550122:

```
isdn spid2 0 4085550111 4085550122
```

Related Commands

Command	Description
isdn autodetect	Enables the automatic detection of ISDN SPIDs and switch type.

isdn spoofing

To enable ISDN spoofing so that loss of Layer 1 or Layer 2 connectivity of the ISDN BRI interface is not detected by the Trunk Group Resource Manager (TGRM) or similar application, use the **isdn spoofing** command in interface configuration mode. To disable ISDN spoofing so the TGRM or similar application can detect when the BRI interface is not operational (when the Layer 1 or Layer 2 connection is down), use the **no** form of this command.

isdn spoofing

no isdn spoofing

Syntax Description

This command has no arguments or keywords.

Command Default

The ISDN BRI interface is spoofing, which means that applications always see the BRI interface connection as operational (unless the interface has been manually shut down [ADMINDOWN state]).

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The ISDN BRI interface is spoofing by default. Spoofing makes the ISDN BRI interface available (up) for operation (for dialing in ISDN), even if the interface is down. For an ISDN BRI interface to be set to a down condition, the interface must be manually shut down (IDBS_ADMINDOWN state). Spoofing enables upper layers to dial out even when the interface is down.

Some upper layer modules, such as TGRM and similar applications, allow dial-out only if the channel is available. If the record for TGRM or similar application is notified of the actual status of BRI, then the TGRM or similar application can dial out accordingly. In this case, the **no isdn spoofing** command is appropriate.

Note ISDN spoofing can be applied only to BRI interfaces—it does not apply to PRI interfaces.

Examples

The following example shows how to configure an ISDN BRI interface to disable ISDN spoofing:

```
Router# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface bri0/0
Router(config-if)# no isdn spoofing
Router(config-if)#
```

Related Commands

Command	Description
interface bri	Configures a BRI interface and enters interface configuration mode.
show isdn status	Displays the status of all ISDN interfaces or a specific ISDN interface.

isdn static-tei

To configure a static ISDN Layer 2 terminal endpoint identifier (TEI) over the D channel, use the **isdn static-tei** command in interface configuration mode. To remove a static TEI configuration, use the **no** form of this command.

isdn static-tei *tei-number*

no isdn static-tei *tei-number*

Syntax Description

tei-number	Terminal endpoint identifier, in the range from 0 to 63.

Command Default

Dynamic TEI (**no isdn static-tei**)

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

Depending on the telephone company you subscribe to, you may have a dynamically or statically assigned TEI for your ISDN service. The default TEI behavior is dynamic, and the **isdn static-tei** command changes that behavior to static for the specified service.

When you reconfigure a TEI with the **isdn static-tei** command, you must activate the configuration using the **shutdow**n and **no shutdown** commands.

Examples

The following example configures German Anlagenanschluss ISDN lines. These lines are often provided in a group intended to be connected to single ISDN device such as a private branch exchange. To use the Anlagenanschluss ISDN lines on a Cisco router, you must set the TEI to 0, as follows:

```
Router# configure terminal
Router(config)# interface bri 0
Router(config-if)# isdn static-tei 0
Router(config-if)# shutdown
Router(config-if)# no shutdown
```

Related Commands

Command	Description
interface bri	Configures a BRI interface and enters interface configuration mode.
isdn x25 static-tei	Configure a static TEI for X.25 over the ISDN D channel.
shutdown	Disables an interface.

isdn switch-type (BRI)

To specify the central office switch type on the ISDN interface, use the **isdn switch-type** command in global or interface configuration mode. To remove an ISDN switch type, use the **no** form of this command.

isdn switch-type *switch-type*

no isdn switch-type *switch-type*

Syntax Description

switch-type	ISDN service provider switch type. Table 9 in the "Usage Guidelines" section lists the supported switch types.

Defaults

No ISDN switch type is specified.

Command Modes

Global configuration (config)
Interface configuration (config-if)

Command History

Release	Modification
9.21	This command was introduced as a global command.
11.3T	This command was introduced as an interface command.
12.0(3)XG	The **basic-qsig** and **primary-qsig s**witch type options were added to support BRI QSIG voice signaling.

Usage Guidelines

For the Cisco AS5300 access server, you have the choice of configuring the **isdn-switch-type** command to support Q.SIG in either global configuration mode or interface configuration mode. When entered in global configuration mode, the setting applies to the entire Cisco AS5300 access server. When entered in interface configuration mode, the setting applies only to the T1/E1 interface specified. The interface configuration mode setting overrides the global configuration setting.

Note This command can be entered in either global configuration or interface configuration mode. When entered in global configuration mode, the **basic-qsig** switch type command specifies that the Cisco MC3810 use QSIG signaling on all BRI interfaces; when entered in interface configuration mode, the command specifies that an individual BRI voice interface use QSIG signaling. The interface configuration mode setting overrides the global configuration setting on individual interfaces.

For example, if you have a Q.SIG connection on one line as well as on the PRI port, you can configure the ISDN switch type in one of the following combinations:

- Set the global **isdn-switch-type** command to support Q.SIG and set the interface **isdn-switch-type** command for **interface serial 0:23** to a PRI setting such as 5ess.
- Set the global **isdn-switch-type** command to support PRI 5ess and set the interface **isdn-switch-type** command for **interface serial 1:23** to support Q.SIG.
- Configure the global **isdn-switch-type** command to another setting (such as switch type VN3), set the interface **isdn-switch-type** command for **interface serial 0:23** to a PRI setting, and set the interface **isdn-switch-type** command for **interface serial 1:23** to support Q.SIG.

For the Cisco MC3810 router, if you are using different Cisco MC3810 BRI port interfaces with different ISDN switch types, you can use global and interface commands in any combination, as long as you remember that interface commands always override a global command.

For example, if you have a BRI QSIG switch interface on BRI voice ports 1, 2, 3 and 4, but a BRI 5ess switch interface on BRI backup port 0, you can configure the ISDN switch types in any of the following combinations:

- Enter the **isdn switch-type basic-qsig global configuration command**, and enter the **isdn switch-type bri-5ess command** on interface 0.
- Enter the **isdn switch-type bri-5ess** global configuration command, and enter the **isdn switch-type basic-qsig command** on interfaces 1, 2, 3, and 4 individually.
- Enter the **isdn switch-type bri-5ess** command on interface 0, and enter the **isdn switch-type basic-qsig command** on interfaces 1, 2, 3, and 4 individually.

If you use the **no isdn switch-type** global configuration command, any switch type that was originally entered in global configuration mode is canceled; however, any switch type originally entered on an interface is not affected. If you use the **no isdn switch-type** interface configuration command, any switch type configuration on the interface is canceled.

Note In the Cisco MC3810, ISDN BRI voice ports support *only* switch type **basic-qsig**; ISDN BRI backup ports support all other listed switch types, but *not* **basic-qsig**.

Note The dial-peer **codec** command must be configured before any calls can be placed over the connection to the PINX. The default codec type is G729a.

If you are using the Multiple ISDN Switch Types feature to apply ISDN switch types to different interfaces, refer to the chapters "Configuring ISDN BRI" and "Configuring ISDN PRI" in the *Cisco IOS Dial Technologies Configuration Guide* for additional details.

The Cisco IOS command parser accepts the following switch types: basic-nwnet3, vn2, and basic-net3; however, when viewing the NVRAM configuration, the basic-net3 or vn3 switch types are displayed, respectively.

To remove an ISDN switch type from an ISDN interface, specify **the no isdn switch-type** *switch-type command*.

Table 9 lists supported BRI switch types by geographic area.

Table 9 ISDN Service Provider BRI Switch Types

Keywords by Area	Switch Type
Voice/PBX Systems	
basic-qsig	PINX (PBX) switches with QSIG signaling per Q.931
Australia, Europe, UK	
basic-1tr6	German 1TR6 ISDN switch
basic-net3	NET3 ISDN BRI for Norway NET3, Australia NET3, and New Zealand NET3switch types; ETSI-compliant switch types for Euro-ISDN E-DSS1 signaling system
vn3	French ISDN BRI switches
Japan	
ntt	Japanese NTT ISDN switches
North America	
basic-5ess	Lucent (AT&T) basic rate 5ESS switch
basic-dms100	Northern Telecom DMS-100 basic rate switch
basic-ni	National ISDN switches
All Users	
none	No switch defined

Examples

The following example configures the French VN3 ISDN switch type:

```
isdn switch-type vn3
```

The following example uses the Multiple ISDN Switch Types feature and shows use of the global ISDN switch type **basic-ni** keyword (formerly **basic-ni1**) and the **basic-net3** interface-level switch type keyword. ISDN switch type **basic-net3** is applied to BRI interface 0 and overrides the global switch setting.

```
isdn switch-type basic-ni
!
interface BRI0
 isdn switch-type basic-net3
```

The following example configures the Cisco MC3810 router to use BRI QSIG signaling for all of its BRI voice ports:

```
isdn switch-type basic-qsig
```

The following example configures the Cisco MC3810 to use BRI QSIG signaling for BRI voice port 1. On port 1, this setting overrides any different signaling set in the previous example.

```
interface bri 1
 isdn switch-type basic-qsig
```

isdn switch-type (PRI)

To specify the central office switch type on the ISDN interface, or to configure the Cisco MC3810 PRI interface to support QSIG signaling, use the **isdn switch-type** command in global or interface configuration mode. To disable the switch or QSIG signaling on the ISDN interface, use the **no** form of this command.

isdn switch-type *switch-type*

no isdn switch-type *switch-type*

Syntax Description

switch-type	Service provider switch type; see Table 10 for a list of supported switches.

Command Default

The switch type defaults to **none**, which disables the switch on the ISDN interface.

Command Modes

Global configuration (confi)
Interface configuration (config-if)

Note This command can be entered in either global configuration mode or in interface configuration mode. When entered in global configuration mode, the setting applies to the entire Cisco MC3810. When entered in interface configuration mode, the setting applies only to the T1/E1 interface specified. The interface configuration mode setting overrides the global configuration setting.

Command History

Release	Modification
9.21	This command was introduced as a global command.
11.3T	This command was introduced as an interface command.
12.0(2)T	The **primary-qsig-slave** and **primary-qsig master** switch type options were added to support PRI QSIG signaling.

Usage Guidelines

You have a choice of configuring the **isdn-switch-type** command to support QSIG at either the global configuration level or at the interface configuration level. For example, if you have a QSIG connection on one line as well as on the BRI port, you can configure the ISDN switch type in one of the following combinations:

- Set the global **isdn-switch-type** command to support QSIG, and set the interface **isdn-switch-type** command for the **interface bri 0** command to a BRI setting such as 5ess.
- Set the global **isdn-switch-type** command to support BRI 5ess, and set the interface **isdn-switch-type** command for the **interface serial 1:23** command to support QSIG.
- Configure the global **isdn-switch-type** command to another setting (such as switch type VN3), and then set the interface **isdn-switch-type** command for the **interface bri 0** command to a BRI setting, and set the interface **isdn-switch-type** command for the **interface serial 1:23** command to support QSIG.

The voice-port **codec** command must be configured before any calls can be placed over the connection to the PINX. The default codec type is G729a.

To disable the switch on the ISDN interface, specify the **isdn switch-type none command**.

Table 10 lists supported PRI switch types by geographic area.

Note If you are using the Multiple ISDN Switch Types feature to apply the ISDN switch types to different interfaces, refer to the chapter "Setting Up Basic ISDN Service" in the *Cisco IOS Dial Technologies Configuration Guide* for additional details.

Table 10 ISDN Service Provider PRI Switch Types

Keywords by Area	Switch Type
Voice/PBX Systems	
primary-qsig	Supports QSIG signaling per Q.931. Network side functionality is assigned with the **isdn protocol-emulate** command.
Australia and Europe	
primary-net5	NET5 ISDN PRI switch types for Asia, Australia, and New Zealand; ETSI-compliant switches for Euro-ISDN E-DSS1 signaling system.
Japan	
primary-ntt	Japanese ISDN PRI switch.
North America	
primary-4ess	AT&T 4ESS switch type for the United States.
primary-5ess	AT&T 5ESS switch type for the United States.
primary-dms100	NT DMS-100 switch type for the United States.
primary-ni	National ISDN switch type.
All users	
none	No switch defined.

Examples

The following example demonstrates the Multiple ISDN Switch Type Feature. The global ISDN switch type setting is basic-net3. The PRI interface (channelized T1 controller), is configured to use the **isdn switch-type primary-net5** command and BRI interface 0 is configured for the **isdn switch-type basic-ni** command (formerly **isdn switch-type basic-ni1**).

```
isdn switch-type basic-net3
!
interface serial0:23
 isdn switch-type primary-net5
 ip address 172.21.24.85 255.255.255.0
!
interface BRI0
 isdn switch-type basic-ni
```

The following example configures T1 interface 23 on the Cisco AS5300 to support Q.SIG signaling:

```
interface serial 1:23
 isdn switch-type primary-qsig
```

Related Commands

Command	Description
isdn protocol-emulate (dial)	Configures the Layer 2 and Layer 3 port protocol of a BRI voice port or a PRI interface to emulate NT (network) or TE (user) functionality.
pri-group nec-fusion	Configures your NEC PBX to support FCCS.
show cdapi	Displays the CDAPI.
show rawmsg	Displays the raw messages owned by the required component.

isdn t306

Note Effective with Cisco IOS Release 12.4(11)T, the **isdn t306** command is replaced by the **isdn timer** command. See the **isdn timer** command for more information.

To set a timer for disconnect messages sent by a router, use the **isdn t306** command in interface configuration mode. To reset to the default, use the **default** or **no** form of this command.

isdn t306 *milliseconds*

default isdn t306

no isdn t306

Syntax Description

milliseconds	Time, in milliseconds, that the router waits before disconnecting a call after it receives a disconnect message with a progress indicator of 8. Range is from 1 to 400000.
default	This keyword resets the default value for the T306 timer.

Command Default

Default depends on the switch, usually from 5000 to 30000 ms.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(3)XI	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(2)XA	This command was implemented on the Cisco AS5400 and Cisco AS5350.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.4(11)T	This command was replaced by the **isdn timer** command.

Usage Guidelines

The T306 timer is designed for routers that are configured as an ISDN network-side switch. When a router sends out a disconnect message with a progress indicator of 8, it disconnects the call after waiting for the specified number of milliseconds (ms) while the in-band announcement or error tone is playing. Be sure to set the timer long enough for the announcement to be heard or the tone to be recognized. This command is used only for disconnect messages with a progress indicator of 8; otherwise, the T305 timer is used. The **default** and **no** forms of this command have the same result: the timer waits for the default number of ms before disconnecting the call.

Examples

The following example sets the T306 timer to 60000 ms for serial interface 0:23:

```
interface serial 0:23
 isdn t306 60000
```

Related Commands

Command	Description
isdn t309	Changes the value of the timer to clear the network connection, and release the B channel and call reference when a data-link disconnection has occurred.
isdn t310	Changes the value of the T310 timer for Call Proceeding messages.
isdn timer t321	Changes the value of the T321 timer for D channel switchover when the primary D channel fails.

isdn t310

Note Effective with Cisco IOS Release 12.4(11)T, the **isdn t310** command is replaced by the **isdn timer** command. See the **isdn timer** command for more information.

To set a timer for the call proceeding state, use the **isdn t310** comman in interface configuration mode. To reset to the default, use the **no** form of this command.

isdn t310 *milliseconds*

no isdn t310

Syntax Description

milliseconds	Time, in milliseconds, that the router waits before disconnecting a call after receiving a call proceeding message. Range is from 1 to 400000.

Command Default

Default depends on the switch; usually from 5000 to 30000 ms.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(3)XI	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.4(11)T	This command was replaced by the **isdn timer** command.

Usage Guidelines

The T310 timer starts when a router receives a call proceeding message; it stops when the call exits the call proceeding state, typically when the call moves to the alerting, connect, or progress state. If the timer expires while the call is in the call proceeding state, the router releases the call. Set the timer to match the specific characteristics of your network.

Examples

The following example sets the T310 timer to 40,000 ms for serial interface 0:23:

```
interface serial 0:23
 isdn t310 40000
```

Related Commands

Command	Description
isdn protocol-emulate	Sets a timer for disconnect messages.
isdn t306	Changes the value of the T306 timer to disconnect a call after the router sends a disconnect message.
isdn test call interface	Changes the value of the T309 timer to clear the network connection, and to release the B channel and call reference when a data-link disconnection has occurred.
isdn timer t321	Changes the value of the T321 timer for D-channel switchover when the primary D channel fails.

isdn tei-negotiation (global)

To configure when Layer 2 becomes active and ISDN terminal endpoint identifier (TEI) negotiation occurs, use the **isdn tei-negotiation** command in global configuration mode. To remove TEI negotiation configuration, use the **no** form of this command.

isdn tei-negotiation [**first-call** | **powerup**]

no isdn tei-negotiation

Syntax Description

first-call	(Optional) ISDN TEI negotiation should occur when the first ISDN call is placed or received.
powerup	(Optional) ISDN TEI negotiation should occur when the router is powered on.

Command Default

The **powerup** state is the default condition.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.21	This command was introduced as a global command.

Usage Guidelines

This command is for BRI configuration only.

This command is useful for switches that may deactivate Layers 1 and 2 when there are no active calls or primary DMS-100 switches which activate TEI when the first ISDN call is placed or received.

Examples

The following example applies the **isdn tei negotiation first-call** command to BRI interface 0. BRI interface 1 will use the **isdn tei negotiation powerup command**, which is the default setting. Defaults settings do not appear in the router configuration.

```
isdn switch-type basic-net
!
interface bri0
! Configure the ISDN switch type on this interface and set TEI negotiation to first-call.
 isdn switch-type basic-ni
 isdn tei-negotiation first-call
! BRI interface 1 uses the default TEI negotiation value.
interface bri1
```

isdn tei-negotiation (interface)

To configure when Layer 2 becomes active and ISDN terminal endpoint identifier (TEI) negotiation occurs, use the **isdn tei-negotiation** command in interface configuration mode. To remove TEI negotiation from an interface, use the **no** form of this command.

isdn tei-negotiation {**first-call** | **powerup**} {**preserve** | **remove**}

no isdn tei-negotiation

Syntax Description

first-call	ISDN TEI negotiation occurs when the first ISDN call is placed or received.
powerup	ISDN TEI negotiation occurs when the router is powered up.
preserve	Preserves dynamic TEI negotiation when ISDN Layer 1 flaps, and when the **clear interface** or the **shutdown** and **no shutdown** EXEC commands are executed.
remove	Removes dynamic TEI negotiation when ISDN Layer 1 flaps, and when the **clear interface** or the **shutdown** and **no shutdown** EXEC commands are executed.

Command Default

The **powerup** state is the default condition. Depending on the ISDN switch type configured, the default action is to preserve or remove the TEI negotiation options.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3T	This command was introduced as an interface command.
12.2	The **preserve** and **remove** keywords were added.

Usage Guidelines

This command is for BRI configuration only.

The **first-call** and **powerup**, and **preserve** and **remove** command pairs are mutually exclusive, that is, you must choose only one command from either the **first-call** and **powerup** or **preserve** and **remove** command pairs, per command line.

The **no isdn tei-negotiation** command returns the configuration to default to the **powerup** state.

Use of the **preserve** keyword causes different behavior depending on the ISDN switch type configured, that is, the TEI negotiation configured will be preserved during ISDN Layer 1 flaps, and when the **clear interface** or the **shutdown** and **no shutdown** EXEC commands are executed, on the switch types listed in Table 11.

Table 11 Switch Types with Preserved TEI Negotiation

Switch Type	Cisco IOS Keyword
French ISDN switch types	**vn2, vn3**
Lucent (AT&T) basic rate 5ESS switch	**basic-5ess**

Table 11 Switch Types with Preserved TEI Negotiation (continued)

Switch Type	Cisco IOS Keyword
Northern Telecom DMS-100 basic rate switch	**basic-dms100**
National ISDN basic rate switch	**basic-ni**
PINX (PBX) switches with QSIG signaling per Q.931	**basic-qsig**

For all other ISDN switch types, the TEI negotiation will be removed during ISDN Layer 1 flaps, and when the **clear interface** or the **shutdown** and **no shutdown** EXEC commands are executed. Use the **remove** keyword to specifically set one of the switches listed in Table 11 to the remove state.

The **first-call** keyword and its functionality are not supported on U.S. switch types (basic-ni, basic-5ess, basic-dms100, primary-ni, primary-4ess, primary-5ess, and primary-dms100), especially for service profile identifier (SPID) negotiations. The **first-call** keyword and its functionality are supported on European switch types (basic-net3 and primary-net5) to prevent Layer 2 activity when there are no Layer 3 calls.

Examples

The following example shows the ISDN TEI negotiation configuration with default settings. (Defaults settings do not appear in the router configuration.)

```
interface BRI0/0
 no ip address
 isdn switch-type basic-ni
 cdapi buffers regular 0
 cdapi buffers raw 0
 cdapi buffers large 0
```

The following example shows how to set TEI negotiation timing to the first call:

```
Router(config-if)# isdn tei-negotiation first-call
Router(config-if)# exit
Router(config)# exit
Router# show startup-config
.
.
.
interface BRI0/0
 no ip address
 isdn switch-type basic-ni
 isdn tei-negotiation first-call
 cdapi buffers regular 0
 cdapi buffers raw 0
 cdapi buffers large 0interface BRI0/0
```

The following example shows how to change TEI negotiation timing back to the default power-up state:

```
Router(config-if)# no isdn tei-negotiation
Router(config-if)# exit
Router(config)# exit
Router# show startup-config
.
.
.
interface BRI0/0
 no ip address
 isdn switch-type basic-ni
 cdapi buffers regular 0
 cdapi buffers raw 0
```

```
 cdapi buffers large 0
```

The following example shows how to remove TEI negotiation when ISDN Layer 1 flaps (the preserve state is the default for the National ISDN basic rate switch):

```
Router(config-if)# isdn tei-negotiation remove
Router(config-if)# exit
Router(config)# exit
Router# show startup-config
.
.
.
interface BRI0/0
 no ip address
 isdn switch-type basic-ni
 isdn tei-negotiation first-call
 isdn tei-negotiation remove
 cdapi buffers regular 0
 cdapi buffers raw 0
 cdapi buffers large 0
```

The following example shows how to return the National ISDN basic rate switch to its default preserve state:

```
Router(config-if)# no isdn tei-negotiation
Router(config-if)# exit
Router(config)# exit
Router# show startup-config
.
.
.
interface BRI0/0
 no ip address
 isdn switch-type basic-ni
 isdn tei-negotiation first-call
 cdapi buffers regular 0
 cdapi buffers raw 0
 cdapi buffers large 0
```

isdn test call interface

To make an ISDN data call, use the **isdn test call interface** command in privileged EXEC mode.

isdn test call interface *interface-number dialing-string* [**speed** {**56** | **64**}]

Syntax Description

interface-number	Interface number.
dialing-string	Telephone number used for making ISDN data call.
speed {**56** | **64**}	(Optional) Line speed (56 or 64 kbps) used for making ISDN data call.

Command Default

The default B-channel speed is 64 kbps.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

You can use the **isdn test call interface** command to test your DDR configuration. You can also use this command to verify the dialing string and speed without having to know the IP address of the remote router or without configuring a dialer map or string.

The **isdn test call interface** command replaces the **isdn call interface** command.

Examples

The following example makes an ISDN data call through interface bri 0 to 555-0111 and at a line speed of 56 kbps:

```
isdn test call interface bri 0 5550111 speed 56
```

Related Commands

Command	Description
isdn caller	Disconnects an ISDN data call without bringing down the interface.

isdn test disconnect interface

To disconnect an ISDN data call without bringing down the interface, use the **isdn test disconnect interface** command in privileged EXEC mode.

isdn test disconnect interface *type number* {**b1** | **b2** | **all**}

Syntax Description

type number	Interface type and number, such as bri 0.
b1	B channel 1.
b2	B channel 2.
all	B channels 1 and 2.

Command Default

A default interface is not defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

You can use the **isdn test disconnect interface** command to disconnect any ongoing data calls placed manually or caused by DDR.

The **isdn test disconnect interface** command replaces the **isdn disconnect interface** command.

Examples

The following example disconnects an ISDN data call through interface bri 0 and B channel 1:

```
isdn test disconnect interface bri 0 b1
```

Related Commands

Command	Description
isdn call interface	Makes an ISDN data call.

isdn test l2 flap interface

To simulate an ISDN Layer 2 interface flap without sending a DISC frame, use the **isdn test l2 flap interface** command in privileged EXEC mode.

isdn test l2 flap interface serial *slot/port*

Syntax Description

serial *slot/port*	Specifies the slot and port on the serial interface on which the flap will occur. The slash is required.

Command Default

No flaps are simulated.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Examples

The following example shows how to simulate an ISDN Layer 2 interface flap:

```
Router# isdn test l2 flap interface Serial 0/0
```

Related Commands

Command	Description
isdn layer 2-flap	Sends RESTART or STATUS ENQUIRY messages over the ISDN PRI line when a Layer 2 link flap and recovery occurs.

isdn timer

Note Effective with Cisco IOS Release 12.4(11)T, the **isdn timer** command replaces the **isdn t-activate**, **isdn t306**, **isdn t310**, **isdn timer t309**, and **isdn timer t321** commands. If any of these replaced commands are entered, the command-line interface responds with a message indicating the new syntax and a request that you update the startup configuration with the running configuration.

To identify and configure an ISDN timer and change the value of the timer for network and call connect and disconnect waiting periods, use the **isdn timer** command in interface configuration mode. To restore the default value, use the **no** form of this command.

isdn timer *timer milliseconds*

no isdn timer *timer milliseconds*

Syntax Description

timer	Type of ISDN timer to be configured. The timer is the wait period between two signficant events (the events vary according to the type of timer selected). The following are acceptable ISDN timers: **t-activate**, **t200**, **t203**, **t300s, t301**, **t303**, **t306**, **t307**, **t309**, **t310**, **t321**, and **t322**.
milliseconds	Number of milliseconds (ms) that the router or switch waits before taking action. Values for the different ISDN timers are as follows: • **t-activate**—The range is from 1000 to 15,000. The default is 4000 (5000 is recommended). • **t200**—The range is from 400 to 400,000. The default is 1000. • **t203**—The range is from 400 to 400,000. The default is 10,000. • **t300s**—The range is from 500 to 86,400,000. The default is 300,000. • **t301**—The range is from 180,000 to 86,400,000. The default is switch-dependent. • **t303**—The range is from 400 to 86,400,000. The default is 10,000. • **t306**—The range is from 400 to 86,400,000. The default is switch-dependent. • **t307**—The range is from 30,000 to 300,000. The default is 180,000. • **t309**—The range is from 0 to 86,400,000. The default is 90,000. • **t310**—The range is from 400 to 400,000. The default is 10,000. • **t321**—The range is from 0 to 86,400,000. The default is 30,000. • **t322**—The range is from 4,000 to 86,000,000. The default is 4,000. **Note** Setting the timer to 0 for the T309 and T321 timers causes the expiration time to be infinite so the wait period will never expire.

Command Default

The default values vary according to the type of ISDN timer and, in some cases, are switch-dependent. To restore a specific default value, use the **no isdn timer** command.

Command Modes Interface configuration

Command History

Release	Modification
12.4(11)T	This command was introduced. This command replaces the **isdn t-activate**, **isdn t306**, **isdn t310**, **isdn timer t309**, and **isdn timer t321** commands and standardizes the syntax for ISDN timer configuration.

Usage Guidelines Selection of the different timers serves different purposes in the ISDN configuration. The functions of the different ISDN timers are as follows:

- **t-activate**—The T-activate timer starts when the voice gateway sends a Facility message to the public switched telephone network (PSTN). If a response is not received within the specified time, the Tool Command Language (TCL) Interactive Voice Response (IVR) script for Malicious Call Identification (MCID) is notified. Depending on how the script is written, it could reinvoke MCID or perform some other action, such as playing a message if the MCID attempt fails. The ISDN interface must use the NET5 switch type, which is set using the **isdn switch-type primary-net5** command. Protocol emulation must be set to **user**, which is the default for the **isdn protocol-emulate** command.
- **t200**—The T200 timer defines the wait period until the retransmission of a message will occur. This wait period must exceed the time it takes to send a frame and receive its acknowledgment.
- **t203**—The T203 timer specifies the maximum wait period between exchanges of Q.921 frames. Although the default is 10,000 ms, most switches allow modification of this timer as needed. In cases of long distances and delay, this timer should be modified for continued operation.
- **t300s**—The T300S timer is specific to Cisco IOS software configurations. The T300S timer specifies the wait period between attempts to initiate ISDN Layer 2 communication.
- **t301**—The T301 timer is configured on the user side and the network side. On the user side, the timer indicates Call Delivered—Alerting Received. On the network side, this timer indicates Call Received—Alerting Received.
- **t303**—The T303 timer starts when a calling party initiates call establishment by transferring a setup message on the assigned signaling virtual channel across the interface. If no response to the setup message is received by the user side before the first expiry of the T303 timer, the setup message will be retransmitted and the T303 timer restarted. If the user side has not received any response to the setup message after the final expiry of timer T303, the user side manually clears the call internally.
- **t306**—The T306 timer is configured on the network side. The T306 timer defines a wait period only for disconnect messages with a progress indicator of 8. When a router sends out a disconnect message with a progress indicator of 8, it disconnects the call after waiting for the specified number of milliseconds while the in-band announcement or error tone is playing. The timer must be set with sufficient duration for the announcement to be heard or the tone to be recognized.
- **t307**—The T307 timer is configured on the network side for BRI switch-types (Primary-net5, Primary-NI, and Primary-NI2C) for Suspend—Remove message processing.

- **t309**—The T309 timer defines a wait period before clearing the network connection and releasing the B channel and call reference when a data-link disconnection has occurred. When a data link layer malfunction occurs, calls that are not in the active state are cleared. For calls that are not in the active state, the T309 timer is started. The timer is stopped when the data link is reconnected. If the T309 timer expires prior to the reestablishment of the data link, the network clears the connection and call to the remote user, sending a disconnect cause of 27 to indicate that the call destination is out of order. The network releases and disconnects the B channel and releases the call reference, thereby entering the Null state. The T309 timer is mandatory for routers that are configured as ISDN network-side switches. The implementation of the T309 timer is optional for the user side of the network.
- **t310**—The T310 timer starts when a router receives a call-proceeding message; it stops when the call exits the call proceeding state, typically when the call moves to the alerting, connect, or progress state. If the timer expires while the call is in the call-proceeding state, the router releases the call.
- **t321**—The T321 timer specifies a wait period for D-channel switchover when the primary D channel fails. The T321 timer must be implemented when you use the D-channel backup procedure involving D-channel switchover.
- **t322**—The T322 timer facilitates q.931 debug tracing during a flap because this tracing can cause unintended retransmissions. The T322 timer starts when a STATUS-ENQUIRY message is sent. If no response is received before the first expiry of the T322 timer, the STATUS-ENQUIRY message will be retransmitted. If no response is received after the final expiry of timer T322, the call is cleared.

Examples

The following example sets the T309 timer to 60,000 ms (60 seconds) for serial interface 0:24:

```
interface serial 0:24
 isdn timer t309 60000
```

The following example sets the T321 timer expiration to 0 ms so that it will never expire for serial interface 0:24:

```
interface serial 0:24
 isdn timer t321 0
```

Related Commands

Command	Description
isdn protocol-emulate	Configures the PRI interface to serve as either the primary slave (user) or the primary master (network).
isdn switch-type primary-net5	Specifies the central office switch type on the ISDN interface as NET5.
isdn t-activate	Specifies how long the gateway waits for a response from the PSTN after sending a MCID request.
isdn t306	Changes the value of the T306 timer to disconnect a call after the router sends a disconnect message.
isdn t310	Changes the value of the T310 timer for call proceeding messages.
isdn timer t309	Changes the value of the T309 timer to clear the network connection and to release the B channel and call reference when a data-link disconnection has occurred.
isdn timer t321	Changes the value of the T321 timer for D-channel switchover when the primary D channel fails.

isdn timer t309

Note Effective with Cisco IOS Release 12.4(11)T, the **isdn timer t309** command is replaced by the **isdn timer** command. See the **isdn timer** command for more information.

To change the value of the T309 timer to clear the network connection and to release the B channel and call reference when a data-link disconnection has occurred, use the **isdn timer t309** command in interface configuration mode. To restore the default value, use the **no** form of this command.

isdn timer t309 *milliseconds*

no isdn timer t309

Syntax Description

milliseconds	Number of milliseconds (ms) that the router waits before clearing the network connection, and releasing the B channel and call reference. Values are from 0 to 86,400,000 ms (0 to 86,400 seconds).

Command Default

90,000 ms (90 seconds)

Command Modes

Interface configuration

Command History

Release	Modification
12.2	This command was introduced.
12.4(11)T	This command was replaced by the **isdn timer** command.

Usage Guidelines

When a data link layer malfunction occurs, calls that are not in the active state are cleared. For calls that are not in the active state, the T309 timer is started. The timer is stopped when the data link is reconnected. If the T309 timer expires prior to the reestablishment of the data link, the network clears the connection and call to the remote user, sending a disconnect cause of 27 to indicate that the call destination is out of order. The network releases and disconnects the B channel, and releases the call reference, entering the Null state. The T309 timer is mandatory for routers that are configured as an ISDN network-side switch and by default the timer is set to expire after 90,000 ms (90 seconds). The implementation of the T309 timer is optional for the user side of the network. The **isdn timer t309** command is used for changing the value of the T309 timer.

Note Setting the timer to 0 causes the timer expiry to become infinite so the wait period never expires.

Examples

The following example sets the T309 timers to 60,000 ms (60 seconds) for serial interface 0:24:

```
interface serial 0:24
 isdn timer t309 60000
```

Related Commands

Command	Description
isdn t306	Changes the value of the T306 timer to disconnect a call after the router sends a disconnect message.
isdn t310	Changes the value of the T310 timer for call proceeding messages.
isdn timer t321	Changes the value of the T321 timer for D-channel switchover when the primary D channel fails.

isdn timer t321

Note Effective with Cisco IOS Release 12.4(11)T, the **isdn timer t321**command is replaced by the **isdn timer** command. See the **isdn timer** command for more information.

To change the value of the timer for D-channel switchover when the primary D channel fails, use the **isdn timer t321** command in interface configuration mode. To restore the default value, use the **no** form of this command.

isdn timer t321 *milliseconds*

no isdn timer t321

Syntax Description

milliseconds	Number of milliseconds (ms) that the router waits before sending a DL-ESTABLISH request on both D channels to request a switchover. Values are from 0 to 86,400,000.

Command Default

The default wait period is 30,000 ms.

Command Modes

Interface configuration

Command History

Release	Modification
12.2	This command was introduced.
12.4(11)T	This command was replaced by the **isdn timer** command.

Usage Guidelines

The T321 timer must be set when you use the D-channel backup procedure involving D-channel switchover. The **isdn timer t321** command is used for changing the value of the T321 timer.

Note Setting the timer to 0 causes the timer expiry to become infinite so that the wait period never expires.

Examples

The following example sets the T321 timers to 25 ms for serial interface 0:23:

```
interface serial 0:23
 isdn timer t321 25
```

Related Commands

Command	Description
isdn t306	Changes the value of the T306 timer to disconnect a call after the router sends a disconnect message.
isdn timer t309	Changes the value of the T309 timer to clear the network connection, and to release the B channel and call reference when a data-link disconnection has occurred.
isdn t310	Changes the value of the T310 timer for call proceeding messages.

isdn transfer-code

To activate call transferring, use the **isdn transfer-code** command in interface configuration mode. To disable call transferring, use the **no** form of this command.

isdn transfer-code *code*

no isdn transfer-code

Syntax Description

code	Number from 0 to 999 (ISDN transfer code).

Command Default

The default code is 61.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

Use this command if your ISDN line is connected to a NI1 or a Nortel DMS-100 Custom switch. Your telephone service provider should issue an ISDN transfer code when you order call transferring.

Examples

The following example specifies 62 as the ISDN transfer code:

```
isdn transfer-code 62
```

isdn transparent

To configure an ISDN interface to pass specified cause-code values transparently from VoIP to PSTN on the terminating gateway without mapping the values, use the **isdn transparent** command in interface configuration mode. To disable the transparent handling of specified cause codes, use the **no** form of this command.

isdn transparent cause-value *cause-value*

no isdn transparent cause-value *cause-value*

Syntax Description

cause-value	Sends a cause-code value number (submitted as an integer in the range of 1 through 127) to the switch. You can include up to 16 cause-code values in each command.

Command Default

When the **isdn transparent** command is not enabled, all ISDN cause-code values are mapped according to the configuration when they are passed from VoIP to PSTN on the terminating gateway.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(15)T9	This command was introduced.
12.3(7)XI	This command was integrated into this release.
12.3(8)T	This command was integrated into this release.
12.3(8)	This command was integrated into this release.

Usage Guidelines

This command must be enabled under the serial D-channel to pass specified cause-code values transparently. The command syntax allows you to configure up to 16 cause-code values to be passed transparently at the terminating gateway.

Examples

The following example shows how to configure the serial D-channel interface 7/7:23 to pass ISDN cause codes 4, 42, and 95 transparently at the terminating gateway:

```
Router# configure terminal
Router(config)# interface serial7/7:23
Router(config-if)# isdn transparent cause-value 4 42 95
Router(config-if)# end
```

Related Commands

Command	Description
interface serial	Specifies a serial interface created on a channelized E1 or channelized T1 controller (for ISDN PRI, CAS, or robbed-bit signaling).

isdn twait-disable

To delay a National ISDN BRI switch a random time before activating the Layer 2 interface when the switch starts up, use the **isdn twait-disable** command in interface configuration mode. To remove the delay, use the **no** form of this command.

isdn twait-disable

no isdn twait-disable

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

The random-length delay set by this command prevents mass power failures from causing the network ISDN switches to be overwhelmed when power returns and all the devices startup at the same time.

The random delay is in the range 1 to 300 seconds.

Examples

The following example configures a random wait period after a power failure:

```
isdn twait-disable
```

isdn v110 only

To selectively accept incoming V.110 calls based on data bit, parity, and stop bit modem communication settings, use the **isdn v110 only** command in interface configuration mode. To change or disable the expected incoming V.110 modem call configuration, use the **no** form of this command.

isdn v110 only [**databits** {**5** | **7** | **8**}] [**parity** {**even** | **mark** | **none** | **odd** | **space**}] [**stopbits** {**1** | **1.5** | **2**}]

no isdn v110 only

Syntax Description

databits {**5** | **7** | **8**}	(Optional) Allowed data bits, as follows: • **5**—Allow 5 data bits only. • **7**—Allow 7 data bits only. • **8**—Allow 8 data bits only.
parity {**even** | **mark** | **none** | **odd** | **space**}	(Optional) Allowed parity, as follows: • **even**—Allow even parity only. • **mark**—Allow mark parity only. • **none**—Allow no parity only. • **odd**—Allow odd parity only. • **space**—Allow space parity only.
stopbits {**1** | **1.5** | **2**}	(Optional) Allowed stop bits, as follows: • **1**—Allow 1 stop bit only. • **1.5**—Allow 1.5 stop bits only. • **2**—Allow 2 stop bits only.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)T	This command was introduced.

Usage Guidelines

The **isdn v110 only** command provides a way to screen incoming V.110 modem calls and reject any calls that do not have the communication settings configured as the network expects them to be.

Examples

The following example filters out all V.110 modem calls except those with communication settings of 8 data bits, no parity bit, and 1 stop bit:

```
interface serial 0:23
  isdn v110 only databits 8 parity none stopbits 1
```

isdn v110 padding

To enable the padded V.110 modem speed report required by the V.110 modem standard, use the **isdn v110 padding** command in interface configuration mode. To disable the padded V.110 modem speed report, use the **no** form of this command.

isdn v110 padding

no isdn v110 padding

Syntax Description

This command has no arguments or keywords.

Command Default

V.110 modem speed padding is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

The **no isdn v110 padding** command is useful for networks with devices such as terminal adapters (TAs) and global system for mobile communication (GSM) handsets that do not fully conform to the V.110 modem standard. The V.110 modem standard specifies that the incoming asynchronous data must be padded by adding stop elements to fit the nearest channel rate. For example, a 14400 bits per second (bps) user data signaling rate is adapted to a synchronous 19200-bps stream rate. The software reports the adapted rate (19200 bps) to the modem for an incoming V.110 call. However, for those devices that do not fully conform to the V.110 supplications, the software must report the speed as 14400 instead of 19200 to the modem for a successful connection. By setting the modem interface to **no isdn v110 padding**, padding is disabled and the actual bit rate can be reported to the modem.

Examples

The following example shows how to disable V.110 asynchronous-to-synchronous padding:

```
!
 interface Serial0:23
  no ip address
  isdn switch-type primary-ni
  isdn bchan-number-order ascending
  no isdn v110 padding
  no cdp enable
```

isdn voice-priority

To control the priority of data and voice calls for the telephones, fax machines, and modems connected to the router telephone ports, use the **isdn voice-priority** command in interface configuration mode. To disable a specified ISDN voice priority setting and to use the default setting, use the **no** form of this command.

isdn voice-priority *local-directory-number* {**in** | **out**} {**always** | **conditional** | **off**}

no isdn voice-priority *local-directory-number*

Syntax Description

local-directory-number	Local ISDN directory number assigned by your telephone service provider.
in	Incoming voice call.
out	Outgoing voice call.
always	Always bump a data call for a voice call.
conditional	Bump a data call only if there is more than one call to the same destination.
off	Never bump a data call for a voice call.

Command Default

A data call is never bumped for an incoming or outgoing voice call.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

If an ISDN circuit endpoint is busy with a data call or calls and either a voice call comes in (incoming) or you attempt to place a voice call (outgoing), the data call is handled according to the setting of **isdn voice-priority** command.

If you are in North America and have multiple ISDN directory numbers associated with a SPID, the outgoing voice priority that you set for any of these directory numbers applies to the other directory numbers. For example, if you enter the following commands, the outgoing voice priority for all directory numbers specified in the **isdn spid1** command is set to conditional:

```
isdn spid1 0 4085550111 4085550122 4085550133
isdn voice-priority 5550111 out conditional
```

The setting of the **pots dialing-method** command affects when you hear a busy signal in the following situation:

- A data call cannot be bumped.
- You are trying to make an outgoing call.

If the setting is **overlap**, you hear a busy signal when you pick up the handset. If the setting is **enblock**, you initially hear a dial tone and then a busy signal.

Examples

The following example specifies that a data call for the specified ISDN directory number never be bumped for an incoming or an outgoing voice call:

```
isdn voice-priority 5550111 in off
isdn voice-priority 5550111 out off
```

Related Commands

Command	Description
isdn spid1, isdn spid2	Defines the SPID number that has been assigned by the ISDN service provider for the B1 channel.
pots dialing-method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.

isdn x25 dchannel

To create a configurable interface for X.25 traffic over the ISDN D channel, use the **isdn x25 dchannel** command in interface configuration mode. To remove the interface, use the **no** form of this command.

isdn x25 dchannel [**q931-broadcast**]

no isdn x25 dchannel [**q931-broadcast**]

Syntax Description

q931-broadcast	(Optional) Enables a gateway to share the same terminal endpoint identifier (TEI) for sending X.25 Set Asynchronous Balanced Mode Extended (SABME) and ITU Q.931 packet mode responses.

Command Default

Command is disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.2F	This command was introduced.
12.4(6)T	This command was enhanced with the optional **q931-broadcast** keyword to enable the ITU Q.931 service access point identifier (SAPI) value 16 procedures for call setup that accepts X.25 calls on the BRI D channel on Japanese and some European telephone switches that require that procedure.

Usage Guidelines

This command creates a new, configurable interface, which can be specified as **interface bri*x*:0** in commands, where *x* is the original BRI interface number. For example, on a Cisco 4500 router with an MBRI, if the **isdn x25 dchannel** command is configured on interface BRI 5, the new interface is bri5:0 and can be used for configuring the other parameters for X.25 over the D channel. These parameters include the addresses and the map statements. To display the new interface, use the **more system:running-config** command.

The optional **q931-broadcast** keyword is supported only on the ISDN BRI interface user side. Although regular X.25 and ISDN configuration commands may be sufficient to enable this feature, the Japanese NTT ISDN switch types expect the same TEI to be shared. By default, Cisco gateways will try to use two different TEIs and expect the switch to establish an X.25 link on the TEI that responds. The Japanese NTT switch does not follow this procedure and expects the Cisco router to share the same TEI. Cisco recommends that deployments interworking with the Japanese NTT switch type use the optional **q931-broadcast** keyword to enable sharing of the TEI and avoid interworking incompatibilities. The optional **q931-broadcast** keyword can also be used in configurations for other switch types such as the European NET3 that require sharing of the TEIs.

You can verify the X.25 call accept procedure using the **debug isdn events**, **debug isdn** command with the optional **mgmnt** keyword, and **debug isdn q931** EXEC commands.

Examples

The following example creates BRI interface 0 and configures it for X.25 over the ISDN D channel. This example uses dynamic TEIs, not a static TEI.

```
interface bri1
 isdn x25 dchannel
interface bri1:0
 ip address 10.1.1.2 255.255.255.0
 x25 address 31107000000100
 x25 htc 1
 x25 suppress-calling-address
 x25 facility windowsize 2 2
 x25 facility packetsize 256 256
 x25 facility throughput 9600 9600
 x25 map ip 10.1.1.3 31107000000200
 x25 map ip 10.1.1.4 31107000000800
```

The following is a typical configuration that enables SAPI 0 procedures that accept X.25 calls on the ISDN D channel, on ISDN BRI interface 0:

```
isdn switch-type basic-ntt
x25 routing
!
interface BRI0
 no ip address
 no ip directed-broadcast
 dialer load-threshold 1 either
 isdn switch-type basic-net3
 isdn x25 dchannel q931-broadcast
!
interface BRI0:0
 ip address 192.168.1.1 255.255.255.252
 no ip directed-broadcast
 no ip mroute-cache
 x25 address 12503372501
 x25 htc 2
 x25 map ip 192.168.1.2 2231146
!
```

Related Commands

Command	Description
debug isdn	Displays messages about what is occurring in the structure and operation of ISDN in the Cisco IOS software.
debug isdn events	Displays ISDN events occurring on the user (router) side of the ISDN interface.
debug isdn q931	Displays information about call setup and teardown of ISDN Layer 3 network connection between the user (router) side and the network side.
interface bri	Configures a BRI interface and enters interface configuration mode.
isdn switch-type	Specifies the central office switch type on the ISDN interface.

isdn x25 static-tei

To configure a static ISDN Layer 2 terminal endpoint identifier (TEI) for X.25 over the ISDN D channel, use the **isdn x25 static-tei** command in interface configuration mode. Use the **no** form of this command if dynamic TEIs will be used on the interface that is to carry X.25 traffic over the D channel.

isdn x25 static-tei *tei-number*

no isdn x25 static-tei *tei-number*

Syntax Description

tei-number	Terminal endpoint identifier, in the range from 0 to 63.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.2F	This command was introduced.

Usage Guidelines

This command applies to ISDN BRI interfaces only. Only one static TEI is allowed per BRI interface. If a second static TEI is configured, the first static TEI is overwritten.

Some switches require a static TEI be used for X.25 over the ISDN D channel.

When the **isdn x25 dchannel** command is invoked without the **isdn x25 static-tei** command, a dynamic TEI is chosen.

Examples

The following example creates static TEI 8 on the X.25-over-ISDN-D channel:

```
interface bri0
 isdn x25 dchannel
 isdn x25 static-tei 8
```

Because the **isdn x25 static-tei** command is missing, the following example configuration sets dynamic TEIs for the ISDN channel:

```
interface bri0
 isdn x25 dchannel
```

Related Commands

Command	Description
interface bri	Configures a BRI interface and enters interface configuration mode.
isdn x25 dchannel	Creates a configurable interface for X.25 traffic over the ISDN D channel.

l2tp tunnel retransmit initial retries

To configure the number of times that the router will attempt to send out the initial Layer 2 Tunnel Protocol (L2TP) control packet for tunnel establishment before considering a peer busy, use the **l2tp tunnel retransmit initial retries** command in VPDN group or VPDN template configuration mode. To restore the default value, use the **no** form of this command.

l2tp tunnel retransmit initial retries *number*

no l2tp tunnel retransmit initial retries

Syntax Description

number	Number of retransmission attempts. Valid values range from 1 to 1000. The default value is 2.

Command Default

The router will resend the initial L2TP control packet twice.

Command Modes

VPDN group configuration
VPDN template configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)T	This command was implemented on the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Use the **l2tp tunnel retransmist initial retries** command to configure the number of times a device will attempt to resend the initial control packet used to establish an L2TP tunnel.

Examples

The following example configures the router to attempt to send the initial L2TP control packet five times for tunnels associated with the virtual private dialup network (VPDN) group named group1:

```
vpdn-group group1
 l2tp tunnel retransmit initial retries 5
```

Related Commands

Command	Description
l2tp tunnel busy timeout	Configures the amount of time that the router will wait before attempting to recontact a router that was previously busy.
l2tp tunnel retransmit initial timeout	Configures the amount of time that the router will wait before resending an initial L2TP control packet out to establish a tunnel.
l2tp tunnel retransmit retries	Configures the number of retransmission attempts made for a L2TP control packet.

Command	Description
l2tp tunnel retransmit timeout	Configures the amount of time that the router will wait before resending an L2TP control packet.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

limit base-size

To define the base number of simultaneous connections that can be done in a single customer or virtual private dialup network (VPDN) profile, use the **limit base-size** command in customer profile configuration or VPDN profile configuration mode. To remove the limitation, use the **no** form of this command.

limit base-size {*base-number* | **all**}

no limit base-size {*base-number* | **all**}

Syntax Description

base-number	Maximum number of simultaneous connections or sessions that can be used in a specified customer or VPDN profile, in the range from 0 to 1000.
all	Accept all calls (default). Use this keyword if you do not want to limit or apply overflow session counting to a customer or VPDN profile.

Command Default

The base size is set to **all**.

Command Modes

Customer profile configuration
VPDN profile configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **limit base-size** command to define the base number of simultaneous connections in a single customer or VPDN profile. The session limit applies to all the physical resource groups and pools configured in a single customer profile. If you want to define the number of overflow calls granted to a customer profile by using the **limit overflow-size** command, do *not* use the **all** keyword in the **limit base-size** command; instead, specify a base number.

Examples

The following example shows the total number of simultaneous connections limited to a base size of 48:

```
resource-pool profile customer customer1_isp
 limit base-size 48
```

Related Commands

Command	Description
limit overflow-size	Defines the number of overflow calls granted to one customer or VPDN profile.
resource-pool profile customer	Creates a customer profile.

limit overflow-size

To define the number of overflow calls granted to one customer or virtual private dialup network (VPDN) profile, use the **limit overflow-size** command in customer profile configuration or VPDN profile configuration mode. To remove the overflow configuration, use the **no** form of this command.

limit overflow-size {*overflow-calls* | **all**}

no limit overflow-size {*overflow-calls* | **all**}

Syntax Description

overflow-calls	Number of overflow calls to grant, in the range from 0 to 1000. Default is 0.
all	Accept all overflow calls.

Command Default

The overflow size is set to 0.

Command Modes

Customer profile configuration
VPDN profile configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **limit overflow-size** customer or VPDN profile configuration command to define the number of overflow calls granted to one customer or VPDN profile. The overflow is not applied if the **limit base-size** command is set using the **all** keyword.

Examples

The following example shows 20 overflow calls granted to the customer profile called customer1_isp:

```
resource-pool profile customer customer1_isp
 limit overflow-size 20
```

Related Commands

Command	Description
limit base-size	Defines the base number of simultaneous connections that can be done in a single customer or VPDN profile.
resource-pool profile customer	Creates a customer profile.

line-power

To configure an ISDN BRI port to supply line power to the terminal equipment (TE), use the **line-power** command in interface configuration mode. To disable the line power supply, use the **no** form of this command.

line-power

no line-power

Syntax Description

This command has no arguments or keywords.

Command Default

The BRI port does not supply line power.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810 access concentrator.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(3)XI	This command was implemented on the Cisco 2600 and Cisco 3600 series.

Usage Guidelines

This command is supported only if an installed BRI voice module (BVM) or BRI VIC is equipped to supply line power (phantom power).

This command is used only on a BRI port operating in NT mode. A BRI port operating in TE mode is automatically disabled as a source of line power, and the **line-power** command is rejected.

When you use the **line-power** command, the line power provision is activated on a BRI port if the port is equipped with the hardware to supply line power. When you enter the **no line-power command**, the line power provision is deactivated on a BRI port.

Note If the BRI port is operating in NT mode, the **line-power** command will be accepted, but will have no effect if a BVM is not equipped to supply line power.

Examples

The following example configures a BRI port to supply power to an attached TE device (only if the BVM is equipped to supply line power):

```
interface bri 1
 line-power
```

logging event nfas-status

To enable the production of log messages when ISDN layer 2 changes occur on NFAS D-channels. (Primary or Backup D-channels up/down, and active/alternate D-channel changes), use the **logging event nfas-status** command in interface configuration mode. To disable notification, use the no form of this command.

logging event nfas-status

no logging event nfas-status

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled (does not produce reports).

Command Modes

Interface configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

This configuration command should be entered on each ISDN serial interface.

This configuration command should be entered when the user wishes to see the NFAS D-channel status changes. Should “logging event link-status” not be configured, no indication may be provided when the NFAS D-channel status changes.

Examples

The following example shows how to enable the production of log messages when ISDN layer 2 changes occur on NFAS D-channels using the logging event nfas-status command.

```
Router(config-if)# logging event nfas-status
```

loopback (controller el)

To loop an entire E1 line (including all channel groups defined on the controller) toward the line and back toward the router or access server, use the **loopback** command in controller configuration mode. To remove the loop, use the **no** form of this command.

loopback

no loopback

Syntax Description

This command has no arguments or keywords.

Command Default

Loopback function is disabled.

Command Modes

Controller configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

This command is useful for testing the DCE channel service unit/data service unit (CSU/DSU) itself.

To display interfaces currently in loopback operation, use the **show interfaces loopback** EXEC command.

Examples

The following example configures the loopback test on the E1 line:

```
controller e1 0
 loopback
```

Related Commands

Command	Description
show interfaces loopback	Displays information about the loopback interface.

loopback local (controller)

To loop an entire T1 line (including all channel groups defined on the controller) toward the line and the router or access server, use the **loopback local** command in controller configuration mode. To remove the loop, use the **no** form of this command.

loopback local

no loopback local

Syntax Description

This command has no arguments or keywords.

Command Default

Loopback function is disabled.

Command Modes

Controller configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

This command is useful for testing the DCE channel service unit/data service unit (CSU/DSU) itself.

To display interfaces currently in loopback operation, use the **show interfaces loopback** EXEC command.

Examples

The following example configures the loopback test on the T1 line:

```
controller t1 0
 loopback local
```

Related Commands

Command	Description
show interfaces loopback	Displays information about the loopback interface.

loopback local (interface)

To loop a channelized T1 or channelized E1 channel group, use the **loopback local** command in interface configuration mode. To remove the loop, use the **no** form of this command.

loopback local

no loopback local

Syntax Description

This command has no arguments or keywords.

Command Default

Loopback function is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

This command is useful for looping a single channel group in a channelized environment without disrupting the other channel groups.

To display interfaces currently in loopback operation, use the **show interfaces loopback** EXEC command.

Examples

The following example configures the loopback test on the T1 line:

```
interface serial 1/0:22
 loopback local
```

Related Commands

Command	Description
show interfaces loopback	Displays information about the loopback interface.

loopback remote (controller)

To loop packets from a MultiChannel Interface Processor (MIP) through the channel service unit/data service unit (CSU/DSU), over a dedicated T1 link, to the remote CSU at the single destination for this T1 link and back, use the **loopback remote** command in controller configuration mode. To remove the loop, use the **no** form of this command.

loopback remote

no loopback remote

Syntax Description

This command has no arguments or keywords.

Command Default

Command is disabled.

Command Modes

Controller configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

This command applies only when the device supports the remote function. It is used for testing the data communication channels.

For MIP cards, this controller configuration command applies if *only one* destination exists at the remote end of the cloud, the entire T1 line is dedicated to it, and the device at the remote end is a CSU (not a CSU/DSU). This is an uncommon case; MIPs are not usually used in this way.

To display interfaces currently in loopback operation, use the **show interfaces loopback** EXEC command.

Examples

The following example configures a remote loopback test:

```
interface serial 0
 loopback remote
```

Related Commands

Command	Description
show interfaces loopback	Displays information about the loopback interface.

map-class dialer

To define a class of shared configuration parameters associated with the **dialer map** command for outgoing calls from an ISDN interface and for PPP callback, use the **map-class dialer** command in global configuration mode.

map-class dialer *class-name*

no map-class dialer *class-name*

Syntax Description

class-name	Unique class identifier.

Command Default

Command is disabled; no class name is provided.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

The *class-name* argument in the **map-class dialer** command used to specify the class must be the same as a *class-name* argument used in a **dialer map** command.

This command is used on the PPP callback server, not on the callback client.

This command is used to define classes of calls for PPP callback for dial-on-demand routing (DDR), for ISDN Advice of Charge, and for Network Specific Facilities (NSF) call-by-call dialing plans.

For NSF call-by-call support on ISDN Primary-4ESS switches only, use one of the dialing-plan keywords listed in Table 12.

Table 12 NSF Keywords and Supported Services

Keyword	NSF Dialing Plan	Data	Voice	International
sdnplan	SDN	Yes	Yes	GSDN (Global SDN)
megaplan	MEGACOMM	No	Yes	Yes
accuplan	ACCUNET	Yes	Yes	Yes

Examples

The following example configures the PPP callback server on an ISDN BRI interface on a router. The callback server requires an enable timeout and a map class to be defined.

```
interface BRI0
 ip address 10.1.1.7 255.255.255.0
 encapsulation ppp
 dialer callback-secure
 dialer enable-timeout 2
```

```
 dialer map ip 10.1.1.8 name mymap class dial1 81012345678901
 dialer-group 1
 ppp callback accept
 ppp authentication chap
!
map-class dialer dial1
 dialer callback-server username
```

The following example configures the ISDN switch type to Primary-4ESS and configures ISDN PRI on T1 controller 1/0, and sets the D channel for dialer map classes that reference the NSF dialing plans. Finally, the **map-class dialer** command uses a dialing plan keyword and the **dialer outgoing** command refers to the same plan.

```
isdn switch-type primary-4ess
!
!
controller T1 1/0
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
!
interface Serial1/0:23
 description This is the DMS D-channel 415-886-9503
 ip address 10.1.1.3 255.255.255.0
 encapsulation ppp
 no keepalive
 dialer map ip 10.1.1.1 name mymap class sdnplan 14155770715
 dialer map ip 10.1.1.2 name hermap class megaplan 14155773775
 dialer map ip 10.1.1.4 name hismap class accuplan 14155773778
 dialer-group 1
 ppp authentication chap
!
map-class dialer sdnplan
 dialer outgoing sdn
!
map-class dialer megaplan
 dialer voice-call
 dialer outgoing mega
!
map-class dialer accuplan
 dialer outgoing accu
```

The following partial example configures BRI interface 0 to function as the callback server on the shared network. The callback server requires an enable timeout and a map class to be defined.

```
interface BRI0
 ip address 10.2.1.7 255.255.255.0
 encapsulation ppp
 dialer callback-secure
 dialer enable-timeout 2
 dialer map ip 10.2.1.8 name mymap class dial1 81012345678901
 dialer-group 1
 ppp callback accept
 ppp authentication chap
!
map-class dialer dial1
 dialer callback-server username
```

The following example configures a map class named “mymap” and sets an ISDN speed of 56 kbps for the class.

```
map-class dialer mymap
 isdn speed 56
```

Related Commands

Command	Description
dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites.
dialer string (legacy DDR)	Specifies the destination string (telephone number) to be called for interfaces calling a single site.
show controllers e1	Displays information about the E1 links supported by the NPM (Cisco 4000) or MIP (Cisco 7500 series).

member

To alter the configuration of an asynchronous interface that is a member of a group, use the **member** command in interface configuration mode. To restore defaults set at the group master interface, use the **no** form of this command.

member *asynchronous-interface-number command*

no member *asynchronous-interface-number command*

Syntax Description

asynchronous-interface-number	Number of the asynchronous interface to be altered.
command	One or both of the following commands entered for this specific interface: • **peer default ip address** • **description**

Command Default

No individual configurations are set for member interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

You can customize a member interface by using the **member** command. Interfaces are designated as members of a group by using the **interface group-async** and **group-range** commands.

Examples

The following example defines interface 3 with a description of line 3, which is attached to a Hayes Optima modem:

```
interface group-async 0
  member 3 description line #3 Hayes Optima
```

Related Commands

Command	Description
group-range	Creates a list of member asynchronous interfaces (associated with a group interface).
interface group-async	Creates a group interface that will serve as master, to which asynchronous interfaces can be associated as members.

member (dial peer cor list)

To add a member to a dial peer class of restrictions (COR) list, use the **member** command in dial peer COR list configuration mode. To remove a member from a list, use the **no** form of this command.

member *class-name*

no member *class-name*

Syntax Description

class-name	Class name previously defined in dial peer COR custom configuration mode by using of the **name** command.

Command Default

No default behavior or values.

Command Modes

Dial peer COR list configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Examples

The following example adds three members to the COR list named list3:

```
dial-peer cor list list3
 member 900_call
 member 800_call
 member catchall
```

Related Commands

Command	Description
dial-peer cor list	Defines a COR list name.

modem always-on

To set a tty line to always be ready to interpret characters from network elements, use the **modem always-on** command in line configuration mode. To disable this function, use the **no** form of this command.

modem always-on

no modem always-on

Syntax Description

This command has no arguments or keywords.

Command Default

The tty line waits to recieve a data set ready (DSR), RING, or clear to send (CTS) signal before interpreting characters from network elements.

Command Modes

Line configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

To set the line as available to receive calls coming from the network via the router, you must also configure the line with the **autocommand x28** command.

Examples

The following example configures tty line 97 to interpret characters received from network elements without having to wait for other incoming signals:

```
Router(config)# line 97
Router(config-line)# modem always-on
```

Related Commands

Command	Description
autocommand	Automatically executes a command when a user connects to a particular line.
modem printer	Configures a line to receive a DSR signal before it will interpret incoming characters from a network element.
x28	Enters X.28 mode and accesses an X.25 network or sets X.3 PAD parameters.

modem answer-timeout

To set the amount of time that the Cisco IOS software waits for the Clear to Send (CTS) signal after raising the data terminal ready (DTR) signal in response to RING, use the **modem answer-timeout** command in line configuration mode. To revert to the default value, use the **no** form of this command.

modem answer-timeout *seconds*

no modem answer-timeout

Syntax Description

seconds	Timeout interval in seconds, in the range from 0 to 65535.

Command Default

15 seconds

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command is useful for modems that take a long time to synchronize to the appropriate line speed.

For more information, see the chapter "Creating and Using Modem Chat Scripts" in the *Cisco IOS Dial Technologies Configuration Guide*.

Examples

The following example sets the timeout interval to 20 seconds for the modem connected to lines 3 through 13:

```
line 3 13
 modem answer-timeout 20
```

Related Commands

Command	Description
modem callin	Supports dial-in modems that use the DTR signal to control the off-hook status of the modem.
modem inout	Configures a line for both incoming and outgoing calls.

modem at-mode

To open a directly connected session and enter AT command mode, which is used for sending AT (modem attention) commands to Microcom manageable modems, use the **modem at-mode** command in EXEC mode.

modem at-mode *slot/port*

no modem at-mode *slot/port*

Syntax Description

slot/port	Slot number and modem port number. Include the slash mark when entering this variable.

Command Default

Command is disabled.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Manageable modems return "OK" if the AT command you send is successfully enabled. Press Ctrl-C after sending an AT command to close the directly connected session.

Note This command does not apply to basic modems that have out-of-band ports.

Examples

The following example opens a directly connected session on modem 1/1, enters AT command mode on modem 1/1, and transmits the AT commands through the out-of-band feature of modem 1/1:

```
Router# modem at-mode 1/1

You are now entering AT command mode on modem (slot 1 / port 1).
Please type CTRL-C to exit AT command mode.
at%v

MNP Class 10 V.34/V.FC Modem Rev 1.0/85

OK
at\s

IDLE           000:00:00
LAST DIAL

NET ADDR:      FFFFFFFFFFFF
MODEM HW: SA 2W United States
4 RTS 5 CTS 6 DSR - CD 20 DTR - RI
```

```
MODULATION      IDLE
MODEM BPS       28800  AT%G0
MODEM FLOW      OFF    AT\G0
MODEM MODE      AUT    AT\N3
V.23 OPR.       OFF    AT%F0
AUTO ANS.       ON     ATS0=1
SERIAL BPS      115200 AT%U0
BPS ADJUST      OFF    AT\J0
SPT BPS ADJ.    0      AT\W0
ANSWER MESSGS   ON     ATQ0
SERIAL FLOW     BHW    AT\Q3
PASS XON/XOFF   OFF    AT\X0
PARITY          8N     AT
```

Related Commands

Command	Description
clear modem	Resets the hardware for one or more manageable modems on access servers and routers.

modem at-mode-permit

To permit a Microcom modem to accept a directly connected session, use the **modem at-mode-permit** command in line configuration mode. To disable permission for modems to accept a direct connection, use the **no** form of this command.

modem at-mode-permit

no modem at-mode-permit

Syntax Description

This command has no arguments or keywords.

Command Default

Command is enabled.

Command Modes

Line configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

After you enter this command, enter the **modem at-mode** command to enable a directly connected session on the modem. From AT command mode, you can enter AT (modem attention) commands directly from your terminal session.

For a complete list of supported AT commands, refer to the AT command documentation that came with your access server or router.

The **no modem at-mode-permit** command disables a modem from accepting a direct connection, which is useful for ensuring modem security.

Note This command does not apply to basic modems, which do not have out-of-band ports.

Examples

The following example permits the modem connected to TTY line 1 to accept a directly connected session:

```
line 1
 modem at-mode-permit
```

Related Commands

Command	Description
clear modem	Resets the hardware for one or more manageable modems on access servers and routers.
modem at-mode	Opens a directly connected session and enters AT command mode, which is used for sending AT commands to Microcom manageable modems.

modem autoconfigure discovery

To configure a line to discover which kind of modem is connected to the router and to configure that modem automatically, use the **modem autoconfigure discovery** command in line configuration mode. To disable this feature, use the **no** form of this command.

modem autoconfigure discovery

no modem autoconfigure discovery

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Line configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

The modem is identified each time the line is reset. If a modem cannot be detected, the line continues retrying for 10 seconds. When the modem type is determined, this information remains stored until the modem is recycled or disconnected. Using Discovery mode is much slower than configuring a line directly.

Each time the modem is reset (every time a chat reset script is executed), a string of commands is sent to the modem, the first one being "return to factory-defaults."

Examples

The following example automatically discovers which kind of modem is attached to the router or access server:

```
modem autoconfigure discovery
```

Related Commands

Command	Description
modem autoconfigure type	Directs a line to attempt to configure the attached modem using a predefined modemcap.

modem autoconfigure type

To direct a line to attempt to configure the attached modem using the entry for the *modem-type argument*, use the **modem autoconfigure type** command in line configuration mode. To disable this feature, use the **no** form of this command.

modem autoconfigure type *modem-type*

no modem autoconfigure type

Syntax Description

modem-type	Modem type, such as a Codex 3260.

Command Default

No default behavior or values.

Command Modes

Line configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

The modem is reconfigured each time the line goes down.

Examples

The following example automatically configures the attached modem using the codex_3260 modemcap entry:

```
modem autoconfigure type codex_3260
```

Related Commands

Command	Description
modem autoconfigure discovery	Configures a line to discover which kind of modem is connected to the router and to configure that modem automatically.

modem autotest

Support for the **modem autotest** command was removed in Cisco IOS Release 12.2(11)T. The use of this command is not recommended. In most cases, nonfunctional integrated modems will automatically be removed from service by the system. See the **modem recovery action** command and the **spe recovery** command for more configuration options for nonfunctional modems. For further information about MICA modem recovery, refer to the *Configuring MICA Modem Recovery* technical note. For further information about NextPort service processing element (SPE) recovery, refer to the *Configuring NextPort SPE Recovery* technical note.

modem bad

To remove an integrated modem from service and indicate it as suspected or proven to be inoperable, use the **modem bad** command in line configuration mode. To restore a modem to service, use the **no** form of this command.

modem bad

no modem bad

Syntax Description

This command has no arguments or keywords.

Command Default

Command is disabled.

Command Modes

Line configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

If you mark a modem as inoperable, it appears as Bad—without the asterisk (*)—in the Status column of the **show modem** command output. A modem marked inoperable by the **modem startup-test** command appears as Bad* in the **show modem** command output. Use the **no modem bad** command to unmark a modem as Bad* or Bad and restore it for dialup connection services.

Note Only idle modems can be marked bad by the **modem bad** command. If you want to mark a modem bad that is actively supporting a call, first issue the **modem shutdown** command then issue the **modem bad** command.

Examples

The first part of the following example shows a successful connection between modem 2/1 and modem 2/0, which verifies normal operating conditions between these two modems. However, when modem 2/1 is tested against modem 2/3, the back-to-back modem test fails. Therefore, modem 2/3 is suspected or proven to be inoperable. Modem 2/3 is removed from dialup services through the use of the **modem bad** command on line 28.

```
Router# test modem back-to-back 2/1 2/0

Repetitions (of 10-byte packets) [1]: 10

Router#

%MODEM-5-B2BCONNECT: Modems (2/1) and (2/0) connected in back-to-back test: CONN
ECT9600/REL-MNP
%MODEM-5-B2BMODEMS: Modems (2/0) and (2/1) completed back-to-back test: success/
packets = 20/20
```

```
Router# test modem back-to-back 2/1 2/3

Repetitions (of 10-byte packets) [1]: 10
Router#
%MODEM-5-BADMODEMS: Modems (2/3) and (2/1) failed back-to-back test: NOCARRIER

Router# configure terminal

Router(config)# line 28
Router(config-line)# modem bad
Router(config-line)# end
```

Related Commands

Command	Description
modem startup-test	Performs diagnostic testing on each integrated modem during the rebooting process.
show modem at-mode	Displays a high-level performance report for all the modems or a single modem.
test modem back-to-back	Diagnoses an integrated modem that may not be functioning properly.

modem buffer-size

To configure the size of the history event queue buffer for integrated modems installed in an access server or router, use the **modem buffer-size** command in global configuration mode.

modem buffer-size *events*

no modem buffer-size *events*

Syntax Description

events	Defined number of modem events that each manageable modem is able to store. Default is 100 events.

Command Default

100 modem events

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

A large buffer size uses substantial amounts of processing memory. If the processing memory is running low, reduce the modem buffer size.

To display modem events, use the **show modem log** command.

Note This command does not apply to basic modems that have out-of-band ports.

Examples

The following example enables each modem in the access server to store 150 modem events:

```
modem buffer-size 150
```

Related Commands

Command	Description
show modem log	Displays the modem history event status performed on a manageable modem or group of modems.

modem busyout

To gracefully disable a modem from dialing or answering calls, use the **modem busyout** command in line configuration mode. To reenable a modem, use the **no** form of this command.

modem busyout

no modem busyout

Syntax Description

This command has no arguments or keywords.

Command Default

Command is disabled.

Command Modes

Line configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The disabling action is not executed until the active modem returns to an idle state. No active connections are interrupted when you enter this command. If the **modem busyout-threshold** command is set, this command will be delayed until the DS0 lines to the exchange are taken out of service. For T3 cards the message "No Controller configured" might appear for unconfigured T1 links in the T3.

Examples

The following example disables the modem associated with line 1/0/5 from dialing and answering calls. You do not specify a slot or port number with this command.

```
line 1/0/5
 modem busyout
```

The following example busyouts a range of modems:

```
line 1/0/5 1/0/72
 modem busyout
```

The following example disables the modem associated with line 1 from dialing and answering calls. You do not specify a slot or port number with this command.

```
line 1
 modem busyout
```

Related Commands

Command	Description
busyout	Informs the central-office switch that a channel is out-of-service.
ds0 busyout (channel)	Forces a DS0 time slot on a controller into the busyout state.
modem shutdown	Abruptly shuts down an active or idle modem installed in an access server or router.

modem busyout-threshold

To define a threshold to maintain a balance between the number of DS0s and modems, use the **modem busyout-threshold** command in global configuration mode. To remove the threshold, use the **no** form of this command.

modem busyout-threshold *threshold-number*

no modem busyout-threshold *threshold-number*

Syntax Description

threshold-number	Number of modems that are free when the router should enforce the stipulation that the number of free DS0 lines is less than or equal to the number of modems.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3(2)AA	This command was introduced.

Usage Guidelines

The **modem busyout-threshold** command functionality is also often termed *autobusyout*. This command applies to all DS0 lines coming into the router and counts all free modems in all pools.

The **modem busyout-threshold** command periodically checks to determine if the number of free modems is less than the user specified threshold and if it is it ensures that the number of free DS0 channels is less than or equal to the number of modems.

This command should be used only where excess calls to one router are forwarded by the exchange to an additional router on the same exchange group number.

Because the **modem busyout-threshold** command checks only periodically, the threshold should be greater than the number of calls the user expects to receive in 1 minute plus a safety margin. For example, if the user receives an average of 10 calls per minute, then a threshold of 20 would be advised. Very small thresholds should be avoided because they do not allow sufficient time for the exchange to respond to out-of-service notifications from the router, and callers may receive busy signals when free modems are all used.

Caution The number of DS0 lines in normal operating conditions should be approximately equal to the number of modems (for example, within 30). If this is not the case, it will cause a lot of messaging traffic to the exchange and may cause active calls to be dropped. This caution is not a concern for short periods, that is, when modem cards are replaced.

On T3 controllers, any contained T1 controllers that are not in use should be undeclared to remove them from the autobusyout list.

Note On T3 controllers, any contained T1 controllers that are not in use should be undeclared to remove them from the autobusyout list.This command is the same as the **ds0 busyout-threshold** command for the Cisco AS5300 and AS5800 access servers.

Examples

The following example shows how you might configure the **modem busyout-threshold** command:

```
modem busyout-threshold 30
```

Related Commands

Command	Description
busyout	Informs the central-office switch that a channel is out-of-service.
ds0 busyout (channel)	Forces a DS0 timeslot on a controller into the busyout state.
modem busyout	Disables a modem from dialing or answering calls whereby the disabling action is not executed until the active modem returns to an idle state.
modem shutdown	Abruptly shuts down an active or idle modem installed in an access server or router.

modem callin

To support dial-in modems that use the data terminal ready (DTR) signal to control the off-hook status of the modem, use the **modem callin** command in line configuration mode. To disable this feature, use the **no** form of this command.

modem callin

no modem callin

Syntax Description

This command has no arguments or keywords.

Command Default

No modem control

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

In response to the RING signal, the router raises the DTR signal, which indicates to the modem that it should answer the call. At the end of the session, the Cisco IOS software lowers the DTR signal, which disconnects the modem. This command is useful for older modems that do not support autoanswer.

This command uses clear to send (CTS), whereas other modem commands in the Cisco IOS software use data set ready (DSR).

Only use the **modem callin** command on the ASM terminal server, where hardware flow control is not possible. If you have a Cisco 2500 or 3600 series router, use the **modem dialin** command instead.

Examples

The following example configures lines 10 through 16 for dial-in modems that can run at speeds from 300 to 19,200 bits per second:

```
line 10 16
 modem callin
 autobaud
```

Related Commands

Command	Description
modem answer-timeout	Sets the amount of time that the Cisco IOS software waits for the CTS signal after raising the DTR signal in response to RING.
modem inout	Configures a line for both incoming and outgoing calls.

modem callout

To configure a line for reverse connections, use the **modem callout** command in line configuration mode. To disable this feature, use the **no** form of this command.

modem callout

no modem callout

Syntax Description

This command has no arguments or keywords.

Command Default

No modem control

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command supports ports connected to computers that would normally be connected to modems. It causes the access server to act somewhat like a modem.

This command uses the clear to send (CTS) signal and should be used only on access servers that do not support hardware flow control. If you have an access server that is newer than the ASM terminal server (such as a Cisco 2500 or Cisco 3600 series routers, or a Cisco AS5100 or Cisco AS5200 access servers), use the **modem host** command instead. The **modem callout** command uses CTS, whereas the **modem host** command uses data set ready/ data carrier detect (DSR/DCD.) If CTS is used for modem control instead of DSR/DCD, it prevents CTS from being used by hardware flow control.

Examples

The following example configures lines 17 through 32 in reverse connection mode to a large terminal switch. By using Telnet to connect to a TCP port on this host, the user gets the next free line in the rotary group.

```
line 17 32
 rotary 1
 modem callout
```

Related Commands

Command	Description
modem inout	Configures a line for both incoming and outgoing calls.
show async-bootp	Displays the extended BOOTP request parameters that have been configured for asynchronous interfaces.

modem call-record

To activate the logging of a summary of modem events upon the termination of a call, use the **modem call-record** command in global configuration mode. To deactivate modem event logging of calls, use the **no** form of this command.

modem call-record terse [**quiet**] [**max userid** *character-max*]

no modem call-record

Syntax Description

terse	Specifies that only significant data is logged to the Modem Call Record (MCR).
quiet	(Optional) Specifies that the MCR is sent only to the syslog server and not to the console.
max userid *character-max*	(Optional) Sets the maximum number of characters of the user ID that will be entered into the MCR. The default length is 30 characters.

Command Default

Logging of modem events is off.

Command Modes

Global configuration

Command History

Release	Modification
11.3(6)AA	This command was introduced.
11.3(9)AA	The **max-userid** keyword was added.
12.0(4)T	The **max-userid** keyword was added.
12.1(1)	Support was added for NM-AM and NM-DM modem boards on the Cisco 2600 and Cisco 3600 series routers.
12.1(2)T	The **quiet** keyword was added.

Usage Guidelines

The modem management subsytem provides event logs for each modem at each major event during usage of the modems. The volume of event logs being generated makes the monitoring of modem calls for debugging purposes difficult. The MCR log, activated using the **modem call-record** command, will log a summary of a modem call to syslog upon termination of the call. If a call fails to establish a connection, the call will be summarized in a Modem Call Failed Record.

The MCR is written to the syslog and can be displayed using the **terminal monitor** or **show logging** command, or by examining files on a syslog server.

The **modem call-record** command is supported on Cisco AS5200, AS5300, AS5800, 2600, and 3600 routers with integrated MICA technologies and Microcom modems. For systems with NextPort modems, use the **spe call-record modem** command.

The information provided in the MCR log and the Modem Call Failed Record log varies depending on the type of modem being used. Table 13 describes the significant fields in the display for MICA technologies and Microcom modems.

Table 13 modem call-record Field Descriptions

Field	Description
Interface slot	Interface slot of device assigned for call.
Interface controller unit	Interface controller unit of device assigned for call.
Interface channel	Interface channel of device assigned for call.
Modem type	Modem type used for call.
Modem slot/port	Physical location for modem handling the call.
Call id	Unique Call Identifier assigned to the modem call by the call switching module.
Userid	User ID of caller.
IP address	IP address assigned for caller.
Calling number	Modem calling number.
Called number	Modem called number.
Connected standard	Standard used for connection. Possible values are Bell103, Bell212, K56Flex 1.1, V.17, V.21, V.22, V.22bis, V.23, V.27, V.29, V.32, V.32bis, V.32terbo. V.34, V.34+, and V.90.
Connect protocol	Protocol user for connection. Possible values are ARA1.0, ARA2.0, ASYNC Mode, FAX Mode, LAP-M, MNP, SS7/COT, and SYNC Mode.
Compression	Compression method used for connection. Possible values are MNP5 data, none, V.42bis both, V.42bis RX, and V.42bis TX.
Initial RX bit rate	Actual bit rate from the remote Digital Signal Processor (DSP) to the local DSP at connect.
Initial TX bit rate	Actual bit rate from the local DSP to the remote DSP at connect.
Final RX bit rate	Actual bit rate from the remote DSP to the local DSP at disconnect.
Final TX bit rate	Actual bit rate from the local DSP to the remote DSP at disconnect.
RBS pattern[1]	Actual robbed bit signaling (RBS) pattern observed by the modem. The six LSBs of the returned value indicate the periodic RBS pattern where a one denotes a pulse code modulation sample with a robbed bit. (Only reported for K56Flex).
Digital pad[1]	Amount of digital padding (attenuation) in downlink, in decibels (dB). (Only reported for V.90 and K56Flex.)
Total retrains[1]	Count of total retrains and speed shifts.
Signal quality value[1]	Signal quality values in a range from 0 to 7, where 0 is the worst. The units are arbitrary, approximating abs(log10(SNR)).
SNR	Signal-to-noise ratio, ranging from 0 to 70 in dB steps.
Characters received	Count of total characters received for SYNC/ASYNC connection.
Characters transmitted	Count of total characters sent for SYNC/ASYNC connection.
Characters received BAD[1]	Total number of parity errored characters received (for ASYNC connections).

Table 13 modem call-record Field Descriptions (continued)

Field	Description
Error correction frames received OK	Count of error-free Error Correction frames received. Incorrect or duplicate frames are not included.
Error correction frames transmitted	Count of unique Error Correction frames sent. Re-sent frames are not included.
Error correction frames received BAD/ABORTED[1]	Total error correction retransmissions requested by this modem during the course of the link.
Call timer	Duration of call, in seconds.
Final state	State of modem call before it terminated.
Disconnect reason	Reason for call being disconnected. Each modem type handles parameter differently.

1. These fields are displayed only for MICA technologies modems.

Examples

The following example shows the activation of MCR logging:

```
modem call-record terse
```

The following is the MCR of a successful call on a MICA technologies modem:

```
*Aug 15 01:34:08.775: %CALLRECORD-3-MICA_TERSE_CALL_REC:
DS0 slot/contr/channel=1/0/22 modem=mica slot/port=1/2 call_id=0x3
userid=user1 ip=124.34.45.120
calling=#4085550112 called=#4085550122
std=V.34+ prot=LAP-M comp=None
init-rx/tx b-rate=31200/33600 finl-rx/tx b-rate=33600/33600
rbs=0 d-pad=None retr=2 sq=2 snr=28
rx/tx chars=1067/0 bad=0 rx/tx ec=0/0 bad=0
time=139 finl-state=Steady
disc=0xA220
       Type (=5 ):  Rx (line to host) data flushing, not OK
      Class (=2 ):  EC condition, locally detected
     Reason (=32):  received DISC frame -- normal LAPM termination
```

The following is the MCR of a failed call on a MICA technologies modem:

```
*Aug 15 16:47:54.527: %CALLRECORD-3-MICA_TERSE_CALL_FAILED_REC:
DS0 slot/contr/channel=1/0/22 modem=mica slot/port=1/2 call_id=0x9
calling=4085550112# called=#4085550122
time=2 finl-state=Link
disc=0x7F06
       Type (=3 ):  Condition occurred during call setup
      Class (=31):  Requested by host
     Reason (=6 ):  network indicated disconnect
```

The following is the MCR of a successful call on a Microcom modem:

```
01:17:30: %CALLRECORD-3-MCOM_TERSE_CALL_REC:
DS0 slot/contr/channel=0/0/22 modem=microcom_server slot/port=0/2 call_id=0x3
userid=sque ip=124.34.46.111
calling=#4085550111 called=#4085550122
std=V34 prot=Normal comp=None
Init-RX/TX b-rate=33600/31200 Finl-RX/TX b-rate=33600/33600
SNR=47
RX/TX chars=0/0 RX/TX EC=0/0
time=73 Disc(local)=0x9 DTR Drop Disc(remote)=0x0 Unknown
```

The following is the MCR of a failed call on a Microcom modem:

```
Microcom Terse Modem Call Failed Record Log:
19:28:55: %CALLRECORD-3-MCOM_TERSE_CALL_FAILED_REC:
DS0 slot/contr/channel=0/0/0 modem=microcom_server slot/port=0/2 call_id=0xA003
calling=4085550111# called=#4085550122
time=0 finl-state=Dialing/Answering
disc(local)=0x9 DTR Drop disc(remote)=0x0 Unknown
```

Related Commands

Command	Description
calltracker call-record	Enables call record syslog generation for the purpose of debugging, monitoring, or externally saving detailed call record information.
show logging	Displays the state of logging (syslog).
spe call-record modem	Generates a modem call record at the end of each call.
terminal monitor	Displays **debug** command output and system error messages for the current terminal and session.

modem country mica

To configure the modem country code for a bank of MICA technologies modems, use the **modem country mica** command in global configuration mode. To remove a country code from service, use the **no** form of this command.

modem country mica *country*

no modem country mica *country*

Syntax Description

country	Country name. See Table 14 for a list of the supported country name keywords.

Command Default

Command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.

Usage Guidelines

Table 14 lists the supported codes for the *country* argument.

Table 14 MICA Country Names

australia
austria
belgium
china
cyprus
czech-republic (Czech/Slovak Republic)
denmark
e1-default (Default E1, a-law)
finland
france
germany
hong-kong
india
ireland
israel
italy

Table 14 MICA Country Names (continued)

japan
malaysia
netherlands
new-zealand
norway
poland
portugal
russia
singapore
south-africa
spain
sweden
switzerland
t1-default (Defaults T1, u-law)
taiwan
thailand
turkey
united-kingdom
usa

Examples

The following example sets the MICA technologies modems for operation in Sweden:

```
modem country mica sweden
```

Related Commands

Command	Description
modem country microcom_hdms	Configures the modem country code for a bank of Microcom modems.

modem country microcom_hdms

To configure the modem country code for a bank of Microcom High Density Management System (HDMS) modems, use the **modem country microcom_hdms** command in global configuration mode. To remove a country code from service, use the **no** form of this command.

modem country microcom_hdms *country*

no modem country microcom_hdms *country*

Syntax Description

country	Country name. See Table 15 for a list of the supported country name keywords.

Command Default

No country code is enabled.

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.
12.0	The **europe** keyword was added.

Usage Guidelines

Table 15 lists the supported codes for the *country* argument.

Table 15 Microcom Country Names

argentina
australia
austria
belgium
brazil
canada
chile
china
columbia
czech-republic (Czech/Slovak Republic)
denmark
europe
finland
france
germany

Table 15 Microcom Country Names (continued)

greece
hong-kong
hungary
india
indonesia
finland
israel
italy
japan
korea
malaysia
mexico
netherlands
norway
peru
philippines
poland
portugal
saudi-arabia
singapore
south-africa
spain
sweden
switzerland
taiwan
thailand
united-kingdom
usa

Examples

The following example shows the different duplex configuration options you can configure on a Cisco AS5300:

```
Router(config)# modem country microcom_hdms ?

  argentina       Argentina
  australia       Australia
  austria         Austria
  belgium         Belgium
  chile           Chile
  china           China
  columbia        Columbia
```

```
czech-republic  Czech/Slovak Republic
denmark         Denmark
europe          Europe
finland         Finland
france          France
germany         Germany
greece          Greece
hong-kong       Hong Kong
india           India
indonesia       Indonesia
ireland         Ireland
israel          Israel
italy           Italy
japan           Japan
korea           Korea
malaysia        Malaysia
mexico          Mexico
netherlands     Netherlands
new-zealand     New Zealand
norway          Norway
peru            Peru
philippines     Philippines
poland          Poland
portugal        Portugal
saudi-arabia    Saudi Arabia
singapore       Singapore
south-africa    South Africa
spain           Spain
sweden          Sweden
switzerland     Switzerland
taiwan          Taiwan
thailand        Thailand
united-kingdom  United Kingdom
usa             USA
```

Related Commands

Command	Description
modem country mica	Configures the modem country code for a bank of MICA technologies modems.

modem country smart_acf

To customize the modem firmware behavior according to the country of deployment, use the **modem country smart_acf** command in global configuration mode. To restore the default value, use the **no** form of this command.

modem country smart_acf *country-name*

no modem country smart_acf *country-name*

Syntax Description

country-name	Name of the country. For valid argument values, see the table in the "Usage Guidelines" section.

Command Default

United States and Canada

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T on Cisco 2600 series and Cisco 3700 series routers.

Usage Guidelines

Use this command to set the modem for use in a specific country. When a country name is specified, the firmware customizes the modem for use in the country where it is deployed. The following table includes valid values for the *country-name* argument and the country or countries associated with each argument value.

Valid Values for the *country-name* Argument	Country or Countries Where Located
argentina	Argentina
australia	Australia
austria	Austria
belgium	Belgium and Luxemburg
brazil	Brazil
bulgaria	Bulgaria
china	China
croatia	Croatia
czech	Czechoslovakia
denmark	Denmark and Iceland
finland	Finland
france	France

Valid Values for the *country-name* Argument	Country or Countries Where Located
germany	Germany
greece	Greece
hongkong	Hong Kong
hungary	Hungary
india	India
ireland	Ireland
israel	Israel
italy	Italy
japan	Japan
jordan	Jordan
korea	Korea
malaysia	Malaysia
mexico	Mexico
morocco	Morocco
netherlands	Netherlands
newzealand	New Zealand
norway	Norway
poland	Poland
portugal	Portugal
romania	Romania
russia	Russia
safrica	South Africa
singapore	Singapore
slovenia	Slovenia
spain	Spain
sweden	Sweden
switzerland	Switzerland
taiwan	Taiwan and Peru
thailand	Thailand
turkey	Turkey
uae	United Arab Emirates
uk	United Kingdom
usa	United States and Canada

Examples

The following example sets the modem for use in Turkey:

```
Router# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# modem country smart_acf turkey
```

Related Commands

Command	Description
show modem version	Displays the software version and the crash log of the modem.

modem country v12

To configure the modem country code for a bank of V12 modems, use the **modem country v12** command in global configuration mode. To remove a country code from service, use the **no** form of this command.

modem country v12 *country*

no modem country v12 *country*

Syntax Description

country	Country name. See Usage Guidelines for a list of the supported country names.

Command Default

Command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

The supported codes for the *country* argument are as follows:

- **australia**
- **austria**
- **belgium**
- **china**
- **cyprus**
- **czech-republic** (Czech/Slovak Republic)
- **denmark**
- **e1-default** (Default E1, a-law)
- **finland**
- **france**
- **germany**
- **hong-kong**
- **india**
- **ireland**
- **israel**
- **italy**
- **japan**

- **malaysia**
- **netherlands**
- **new-zealand**
- **norway**
- **poland**
- **portugal**
- **russia**
- **singapore**
- **south-africa**
- **spain**
- **sweden**
- **switzerland**
- **t1-default** (Defaults T1, u-law)
- **taiwan**
- **thailand**
- **turkey**
- **united-kingdom**
- **usa**

Examples

The following example sets the V12 modems for operation in Sweden:

```
modem country v12 sweden
```

modem cts-required

The **modem cts-required** command is replaced by the **modem printer** command. See the description of the **modem printer** command for more information.

modem dialin

To configure a line to enable a modem attached to the router to accept incoming calls only, use the **modem dialin** command in line configuration mode. To disable this feature, use the **no** form of this command.

modem dialin [**delay**]

no modem dialin

Syntax Description

delay	(Optional) Causes the operating system to delay assertion of the data terminal ready (DTR) signal until a network connection is established.

Command Default

Incoming calls to the modem are not permitted.

Command Modes

Line configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(4)T	The **delay** keyword was added to support the Cisco modem user interface.

Usage Guidelines

This command supports modems that can automatically handle telephone line activity, such as answering the telephone after a certain number of rings.

The **delay** keyword is useful when using the **modemui** EXEC command with software that requires a signal assertion to recognize that a connection has been established. It may be necessary to reroute the router DTR signal to an alternate EIA-232 pin such as Carrier Detect (CD) for the delay to work properly.

Examples

The following example configures a line for a high-speed modem:

```
line 5
 modem dialin
```

The following example shows how to set up a delay in a line configured for the Cisco modem user interface feature:

```
line aux 0
 login authentication modem
 modem dialin delay
 autocommand  modemui
 transport input all
 stopbits 1
 speed 38400
 flowcontrol hardware
```

Related Commands

Command	Description
modem inout	Configures a line for both incoming and outgoing calls.
modemui	Enters the Cisco modem user interface mode.
parity	Defines generation of a parity bit.

modem dialout controller

To specify a particular T1 or E1 controller through which to dial out, use the **modem dialout controller** command in line configuration mode. To disable the command, use the **no** form of this command.

modem dialout controller {**e1** | **t1**} *controller-list*

no modem dialout controller

Syntax Description

e1	Wide-area digital transmission scheme used predominantly in Europe.
t1	Wide-area digital carrier facility.
controller-list	List of controllers through which to dial out. The range is from 0 to 7. List the controllers individually (1, 2, 3, for example).

Command Default

All T1 and E1 controllers are used for dial out.

Command Modes

Line configuration

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

This command is only supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800.

Examples

In the following example, the router is configured to use the controller t1 0, t1 1, t1 3 (and no others) when dialing out from lines 1 through 60:

```
line 1 60
 modem dialout controller t1 0,1,3
```

modem dtr-active

To configure a line to leave data terminal ready (DTR) signals low, unless the line has an active incoming connection or an EXEC process, use the **modem dtr-active** command in line configuration mode. To disable this feature, use the **no** form of this command.

modem dtr-active

no modem dtr-active

Syntax Description

This command has no arguments or keywords.

Command Default

No modem control.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command does not use the Carrier Detect (CD) signal.

This command can be useful if the line is connected to an external device (for example, a time-sharing system) that must know whether a line is in active use. The **modem dtr-active** command is similar to the **no modem** line configuration command.

Examples

The following example configures a line for low DTR:

```
line 5
 modem dtr-active
```

Related Commands

Command	Description
modem printer	Configures a line to require a DSR signal instead of CTS.

modem enable

To enable backup dial capability through the console port (change the console port into an auxiliary port), use the **modem enable** command in line configuration mode. To return the auxiliary port to a console port, use the **no** form of this command.

modem enable [**autodetect**]

no modem enable

Syntax Description

autodetect	(Optional) Automatically senses the type of device connected on the console line.

Command Default

This command is not configured by default, and is applicable only on the console line.

Command Modes

Line configuration

Command History

Release	Modification
12.2(8)YN	This command was introduced.
12.2(13)ZG	The optional **autodetect** keyword was added to this command for Cisco 831, 836, and 837, and Cisco SOHO 91 and 97 routers.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.

Usage Guidelines

On the Cisco 831, 836, and 837, and SOHO 91 and 97 routers, the console port and the auxiliary port share the same physical RJ-45 port. The console port must be changed to act as a virtual auxiliary port using the **modem enable** [**autodetect**] command before the dial backup and remote management capabilities can be enabled.

Use the **show line autodetect** EXEC command to determine when a modem or a console has been detected. This command displays the following messages to indicate the type or state of connection on the console line:

- Detection State: Console Attached—A DTE console or terminal device is attached.
- Detection State: Modem Attached—A DCE asynchronous modem device is attached.
- Detection State: Nothing Attached—No cable is attached to the EIA/TIA--232 port on the router.
- Detection State: Init State—Autodetection has been enabled, but no changes have been detected.
- Detection State: Feature not enabled—No device connection is detected.

Note The auto detection capability on the Cisco 831, 836, and 837 routers that detects whether a modem or console is attached to its RJ-45 console port will not work when the router is booting up. The routers use the data set ready (DSR) and clear to send (CTS) pin statuses to detect whether a modem or console is attached.

Examples

The following example enables the line autodetect option:

```
Router(config-line)# modem enable autodetect
```

Use the **show line autodetect** command to determine when a modem or a console has been detected:

```
Router# show line autodetect
Detection State: Nothing Attached

Router# show line autodetect
Detection State: Console Attached
```

Related Commands

Command	Description
show line autodetect	Displays type or state of connection on the console line.

modem hold-reset

To reset and isolate integrated modems for extensive troubleshooting, use the **modem hold-reset** command in line configuration mode. To restart a modem, use the **no** form of this command.

modem hold-reset

no modem hold-reset

Syntax Description

This command has no arguments or keywords.

Command Default

Command is disabled.

Command Modes

Line configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The **modem hold-reset** command for the V.110 port module resets the processor on board the module only if the command is executed on all 12 ports. If the **modem hold-reset** command is issued on only a portion of the V.110 ports, the processor will not reset.

This command is also used to reset a modem that is frozen in a suspended state. Disable the suspended modem with the **modem hold-reset** command, and then restart initialization with the **no modem hold-reset** command.

Examples

The following example disables the suspended modem using tty line 4 and resets the modem's initialization:

```
line 4
 modem hold-reset
 no modem hold-reset
```

The following examples resets a 12-port V.110 port module. You must specify the entire tty line range for the entire bank of ports.

```
line 1 12
 modem hold-reset
 no modem hold-reset
```

Related Commands

Command	Description
modem autotest	Automatically and periodically performs a modem diagnostics test for modems inside the access server or router.

modem host

To configure a line for reverse connections where hardware flow control is also required, use the **modem host** command in line configuration mode. To disable the line modem control for reverse connections, use the **no** form of this command.

modem host

no modem host

Syntax Description

This command has no arguments or keywords.

Command Default

No modem control

Command Modes

Line configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

This command supports ports connected to computers that would normally be connected to modems. This command causes the access server to act like a modem.

The **modem host** command is identical in operation to the **modem callout** command except that data set ready/data carrier detect (DSR/DCD) is used for modem control instead of clear to send (CTS). This frees CTS for use by hardware flow control.

Examples

The following example configures a line to send a DSR/DCD active signal to the modem for data switches and hosts:

```
line 5
 modem host
```

Related Commands

Command	Description
modem callout	Configures a line for reverse connections.
modem printer	Configures a line to require a DSR signal instead of CTS.

modem inout

To configure a line for both incoming and outgoing calls, use the **modem inout** command in line configuration mode. To disable the configuration, use the **no** form of this command.

modem inout

no modem inout

Syntax Description

This command has no arguments or keywords.

Command Default

No modem control.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command uses DSR and RING signals for carrier detection.

The Cisco IOS software does not support any dialing protocols; therefore, the host system software or the user must provide any special dialing commands when using the modem for outgoing calls.

Examples

The following example configures a line for both incoming and outgoing calls:

```
line 5
 modem inout
```

Related Commands

Command	Description
parity	Defines generation of a parity bit.

modem cts-alarm

To enable the router to react to a Clear to Send (CTS) drop from a remote device, and to clear an existing EXEC session, use the **modem cts-alarm** command in line configuration mode. To disable the system from reacting to CTS drops from remote devices, and to have the router ignore to CTS drops, use the **no** form of this command.

modem cts-alarm

no modem cts-alarm

Syntax Description

This command does not have any keywords or arguments.

Command Default

The system does not react to CTS drops.

Command Modes

Line configuration (config-line)

Command History

Release	Modification
12.0T	This command was introduced.
12.2(4)T	This command was integrated into the Cisco IOS Release 12.2(4)T.

Usage Guidelines

This command allows a router to react to asynchronous devices that signal state changes via CTS. When an asynchronous line is used to connect to remote devices, the **modem cts-alarm** command allows the router to react to a CTS drop from the remote device and clear any existing EXEC session that it might have.

By default, the recovery and EXEC restart sessions are not triggered by CTS changes if the **modem-cts-alarm** command is not configured.

Examples

The following example shows how to configure a line for a modem:

```
Router# configure terminal
Router(config)# line 8 9
Router(config-line)# modem cts-alarm
Router(config)# end
Router#
```

modem firmware slot

To enable modem management configuration and specify the firmware used for the modem, the modem slot, and the name of the firmware file, use the **modem firmware slot** command in global configuration mode. To disable the modem management configuration, use the **no** form of this command.

modem firmware slot *slot-number* **location** *firmware-filename*

no modem firmware slot *slot-number* **location** *firmware-filename*

Syntax Description

slot-number	The modem slot number. The range is from 0 to 6.
location	Specifies the location of the firmware file.
firmware-filename	The name of the firmware file.

Command Default

The modem management configuration is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the **modem firmware slot** command to load a specified version of portware into specified modems, or to load any portware that is resident in flash memory and is older than the portware that is bundled with the Cisco IOS software image. The *slot-number* argument specifies the modem slot that contains the network module with the modem. The *firmware-filename* argument specifies the Cisco IOS file system (IFS) filename of the portware to be loaded into the modem.

Examples

The following example shows how to specify the firmware used for the modem, the modem slot number 3, and the firmware file named abcd:

```
Router(config)# modem firmware slot 1 location flash:pw2730.ios

This command will disconnect any active calls.
Modem Slot 1 :Started firmware download.
Modem Slot 1: Completed firmware download
```

Related Commands

Command	Description
show modem version	Displays version information about the modem firmware, controller and DSP ATM address field code (for 56K modems only), and boot code.

modem link-info poll time

To set the polling interval at which link statistics are retrieved from the MICA technologies modem, use the **modem link-info poll time** command in global configuration mode. To return to the default condition, use the **no** form of this command.

modem link-info poll time *seconds*

no modem link-info poll time *seconds*

Syntax Description

seconds	Number of seconds between polling intervals. The valid range is from 10 to 65535.

Command Default

Link statistics are not polled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

The **modem link-info poll time** command periodically polls active modem sessions to collect information such as attempted transmit and receive rates, maximum and minimum transmit and receive rates, and locally and remotely issued retrains and speedshift counters. This data is polled from MICA portware and passed unsolicited to Cisco IOS software.

Enabling the **modem link-info poll time** command disables the **modem poll time** command. Any **modem poll time** configuration is ignored because all modem events are sent to the access server unsolicited and no longer require polling by Cisco IOS software.

Note The **modem link-info poll time** command consumes a substantial amount of memory, approximately 500 bytes for each MICA modem call. You should use this command only if you require the specific data that it collects; for instance, if you have enabled Call Tracker on your access server using the **calltracker call-record** command.

Examples

The following example polls link statistics at 90 second intervals:

```
modem link-info poll time 300
```

Related Commands

Command	Description
calltracker call-record	Enables Call Tracker on the access server.
show call calltracker active	Displays the detailed data stored within Call Tracker for active calls.
show call calltracker handle	Displays the detailed data stored within Call Tracker for a specific call specified unique call handle identifier.
show call calltracker history	Displays the detailed data stored within Call Tracker for terminated calls.
show modem calltracker	Displays the detailed data stored within Call Tracker for the last call on the specified modem.

modem log

To configure the types of EIA/TIA events that are stored in the modem log, use the **modem log** command in line configuration mode. To prevent a type of EIA/TIA event from being stored in the modem log, use the **no** form of this command.

modem log {**cts** | **dcd** | **dsr** | **dtr** | **ri** | **rs232** | **rts** | **tst**}

no modem log {**cts** | **dcd** | **dsr** | **dtr** | **ri** | **rs232** | **rts** | **tst**}

Syntax Description

cts	Specifies that EIA/TIA clear to send (CTS) events are stored in the modem log.
dcd	Specifies that EIA/TIA data carrier detect (DCD) events are stored in the modem log.
dsr	Specifies that EIA/TIA data set ready (DSR) events are stored in the modem log.
dtr	Specifies that EIA/TIA data terminal ready (DTR) events are stored in the modem log.
ri	Specifies that EIA/TIA ring indication (RI) events are stored in the modem log.
rs232	Specifies that all EIA/TIA events are stored in the modem log.
rts	Specifies that EIA/TIA request to send (RTS) events are stored in the modem log.
tst	Specifies that EIA/TIA transmit signal timing (TST) events are stored in the modem log.

Command Default

No EIA/TIA events are logged.

Command Modes

Line configuration

Command History

Release	Modification
11.3AA	This command was introduced for the Cisco AS5300 access server.
12.0(5)T	This command was implemented on the Cisco AS5800 access server.

Usage Guidelines

Use the **modem log** command to suppress the storage of undesired EIA/TIA history events in the modem log.

Examples

The following example configures the storage of EIA/TIA CTS and DSR events on lines 1 through 120:

```
line 1 120
 modem log cts
 modem log dsr
```

Related Commands

Command	Description
show modem log	Displays the modem history event status performed on a manageable modem or group of modems.

modem min-speed max-speed

To configure various modem-service parameters, use the **modem min-speed max-speed** command in service profile configuration mode. To remove modem parameters, use the **no** form of this command.

modem min-speed {*bps* | **any**} **max-speed** {*bps* | **any** [**modulation** *value*][**error-correction** *value*][**compression** *value*]}

no modem min-speed {*bps* | **any**} **max-speed** {*bps* | **any** [**modulation** *value*][**error-correction** *value*][**compression** *value*]}

Syntax Description

bps	Minimum and maximum bit rate for the modems, which can be from 300 to 56,000 bits per second (bps). The bit rate must be in V.90 increments.
any	Any minimum or maximum speed.
modulation *value*	(Optional) Sets a maximum negotiated speed. Replace the *value* argument with one of the following choices: **any**, **k56flex**, **v22bis**, **v34**, or **v90**.
error-correction *value*	Replace the value argument with one of the following choices: **any**, **1apm**, **mnp4**, **none**.
compression *value*	Replace the value argument with one of the following choices: **any**, **mnp5**, **none**, **v42bis**.

Command Default

No modem service parameters are defined by default. Any default services provided by the modems will be available.

Command Modes

Service profile configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Examples

The following example shows the modem service parameters for the service profile named user1sample configured for any minimum or maximum and sets a maximum negotiated speed to **k56flex**.

```
resource-pool profile service user1sample
 modem min-speed any max-speed any modulation k56flex
```

modem poll retry

To set the maximum number of polling attempts used to retrieve performance statistics from a modem installed in an access server or router, use the **modem poll retry** command in global configuration mode. To change or remove the polling attempts, use the **no** form of the command.

modem poll retry *polling-attempts*

no modem poll retry *polling-attempts*

Syntax Description

polling-attempts	Maximum number of polling attempts. The configuration range is from 0 to 10 attempts, and the default is 3.

Command Default

Three polling attempts

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Higher settings cause the software to keep polling one modem for status and to avoid polling other modems, which decreases the amount of statistics that are gathered.

Note This command does not apply to basic modems that have out-of-band ports.

Examples

The following example configures the server to attempt to retrieve statistics from a local modem up to five times before discontinuing the polling effort:

```
modem poll retry 5
```

Related Commands

Command	Description
clear modem	Resets the hardware for one or more manageable modems on access servers and routers.
modem poll time	Sets the time interval between modem polls, which are used to periodically retrieve and report modem statistics.
modem status-poll	Polls for modem statistics through the out-of-band feature of a modem.

modem poll time

To set the time interval between modem polls, which are used to periodically retrieve and report modem statistics, use the **modem poll time** command in global configuration mode. To restore the 12-second default setting, use the **no** form of this command.

modem poll time *interval*

no modem poll time *interval*

Syntax Description

interval	Interval, in seconds, between polls. The configuration range is from 2 to 120 seconds, and the default is 12 seconds.

Command Default

12 seconds

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

This command does not apply to basic modems, which do not have out-of-band ports.

Examples

The following example sets the time interval between polls to 10 seconds:

```
modem poll time 10
```

Related Commands

Command	Description
modem min-speed max-speed	Sets the maximum number of polling attempts used to retrieve performance statistics from a modem installed in an access server or router.
modem status-poll	Polls for modem statistics through the out-of-band feature of a modem.

modem printer

To configure a line to require receipt of a data set ready (DSR) modem control signal, use the **modem printer** command in line configuration mode. To require the clear to send (CTS) modem control signal instead, use the **no** form of this command.

modem printer [**always-on**] [**delay**]

no modem printer [**always-on**] [**delay**]

Syntax Description

always-on	(Optional) Enables the line to interpret characters received from network elements after receiving a DSR signal. The line need not wait for a CTS signal.
delay	(Optional) Causes router to delay assertion of the data terminal ready (DTR) signal until a network connection has been established.

Command Default

The modem requires the CTS signal. Hardware flow control cannot be configured concurrently.

Command Modes

Line configuration mode.

Command History

Release	Modification
11.1	This command was introduced.
12.2(15)T	Support was added for the **delay** keyword.
12.4(4)T	Support was added for the **always-on** keyword.

Usage Guidelines

Use the **modem printer** command to set DSR as the modem control signal, leaving the CTS signal free for use with hardware flow control. This allows hardware flow control to be configured concurrently.

Although the **modem dialin** command supports modems concurrently with hardware flow control, the other auxiliary modem control options for printers, such as **modem cts-required**, use CTS instead of DSR/carrier detect (CD), as the CD signal.

To make the line available to receive calls coming from the network via the router with the **always- on** keyword, you must also configure that line with the **autocommand x28** command.

Examples

The following example configures a line to send a DSR signal to the modem:

```
Router(config)# line 5
Router(config-line)# modem printer
```

The following example configures a line to become ready to interpret characters from network elements when it receives a DSR signal:

```
Router(config)# line 5
Router(config-line)# modem printer always-on
```

Related Commands

Command	Description
autocommand	Automatically executes a command when a user connects to a particular line.
flowcontrol	Sets the method of data flow control between the router and a terminal or other serial device.
modem always-on	Sets a tty line to always be ready to interpret characters from network elements.
modem dialin	Configures a line to enable a modem attached to the router to accept incoming calls only.
x28	Enters X.28 mode and accesses an X.25 network or sets X.3 PAD parameters.

modem recovery action

To specify a modem recovery action, use the **modem recovery action** command in global configuration mode. To turn the modem recovery action off, use the **no** form of this command.

modem recovery action {**disable** | **download** | **none**}

no modem recovery action

Syntax Description

disable	Marks the modem bad.
download	Recovers by firmware download (default). Sets the modem into a recovery pending state, thus stopping the modem from accepting new calls.
none	Does not try to recover. Ignores the recovery threshold and just keeps running.

Command Default

The default setting is **download**.

Command Modes

Global configuration

Command History

Release	Modification
12.0	This command was introduced.
12.1(2.3)T	This command was no longer supported on Cisco AS5800 platforms.

Usage Guidelines

MICA technologies portware is downloaded on a modular basis and not on a modem basis. Thus, reloading MICA portware requires all 6 or 12 modems in a module to be reloaded.

Note Beginning with Cisco IOS Release 12.1(2.3)T1, the **modem recovery action** command is no longer supported for MICA technologies modems on the Cisco AS5800 platforms. To specify a modem recovery action for MICA technologies modems on the Cisco AS5800 platforms, use the **spe recovery** command.

After a modem has been deemed faulty, the configured action will take place on the modem. The following choices are possible: **disable**, **download**, and **none**.

Examples

The following example sets the recovery action to mark the modem as bad:

```
modem recovery action disable
```

Related Commands

Command	Description
modem recovery maintenance	Specifies the scheduled modem maintenance recovery behavior.
modem recovery threshold	Specifies the threshold, which starts the modem recovery process.
modem recovery-time	Sets the maximum amount of time the call-switching module waits for a local modem to respond to a request before it is considered locked in a suspended state.

modem recovery maintenance

To specify the modem maintenance recovery behavior, use the **modem recovery maintenance** command in global configuration mode. To change or turn off this behavior, use the **no** form of this command.

modem recovery maintenance {**action** {**disable** | **drop-call** | **reschedule**} | **max-download** *recovery-downloads* | **schedule** {**immediate** | **pending**} | **time** *hh*:*mm* | **window** *minutes*}

no modem recovery maintenance

Syntax Description

action	Mode of recovery. The default is set to **reschedule**.
disable	Marks the modem bad. Marks the originally faulty modem as bad and returns all other modems back into service.
drop-call	Forces firmware download by dropping holding calls. This action forces the recovery by dropping any active calls remaining on modems within the module.
reschedule	Reschedules firmware download to next maintenance time. Leaves the originally faulty modem as needing recovery and returns all other modems into service. Recovery will be attempted again on the following day. The default is set to **reschedule**.
max-download *recovery-downloads*	Maximum simultaneous recovery downloads. You must choose one number from 1 to 30. A range of values is not supported.
schedule	Scheduling method for modem recovery. Determines if the system should attempt module recovery as soon as a problem is found or wait for the maintenance window.
immediate	Immediately attempts modem recovery.
pending	Delays recovery until maintenance time (default).
time *hh*:*mm*	Time of day for scheduled modem recovery, in hours and minutes. This is the actual time of day when the modem recovery maintenance process wakes up and starts recovering MICA technologies modems. The default time is 3:00 a.m.
window *minutes*	Amount of time for normal recovery to take place. This is the delay timer in minutes, which is from 0 to 360.

Command Default

The default mode of recovery (**action**) is set to **reschedule**.
The default schedule is set to **pending**.
The default **time** for scheduled modem recovery is 3:00 a.m.

Command Modes

Global configuration

Command History

Release	Modification
12.0	This command was introduced.
12.1(2.3)T1	This command was no longer supported on Cisco AS5800 platforms.

Usage Guidelines

MICA portware is downloaded on a modular basis and not on a modem basis. Thus, reloading MICA portware requires all 6 or 12 modems in a module to be reloaded.

Note Beginning with Cisco IOS Release 12.1(2.3)T1, the **modem recovery maintenance** command is no longer supported for MICA technologies modems on the Cisco AS5800 platforms. To specify a modem recovery action for MICA technologies modems on the Cisco AS5800 platforms, use the **spe recovery** command.

Every 24 hours, the modem recovery maintenance process will wake up and attempt to recover any modems that are in the pending recovery state.

When a MICA module attempts to reload its portware, it must avoid taking down any modem connections that may exist. As such, the recovery process sets all modems currently not in use to recovery pending state. If any modems on the module are active, the recovery process waits for the calls to terminate normally. To avoid capacity problems from attempting recovery for an excessively long time period, a maintenance window is configured to require the modem recovery to take place within a specific timeframe. Otherwise, a given action is performed on that module when the window expires. The default window is 60 minutes. This behavior is set using the **modem recovery maintenance window** *minutes* command.

When the modem recovery maintenance window expires, one of the following actions is performed on the modem module awaiting recovery: **disable**, **reschedule**, or **drop-call**. The **disable** option is associated with the **modem recovery action** command.

When the modem recovery maintenance process starts, it attempts to recover all modems in the recovery pending state. This attempt can be on all modules on a given system. Thus, to avoid taking down all modems on a given system, only a maximum of simultaneous module recoveries can take place. The default is dynamically calculated to be 20 percent of the modules on a given system. This configuration allows that value to be overridden. These options are associated with the **modem recovery maintenance max-download** command.

Examples

The following examples show the available options for this command:

```
Router(config)# modem recovery maintenance ?

  action        Mode of recovery
  max-download  Maximum simultaneous recovery downloads
  schedule      Scheduling method for modem recovery
  time          Time of day for scheduled modem recovery
  window        Amount of time for normal recovery to take place

Router(config)# modem recovery maintenance action ?

  disable     Mark the modem bad
  drop-call   Force firmware download by dropping holding calls
  reschedule  Reschedule firmware download to next maintenance time

Router(config)# modem recovery maintenance max-download ?

  <1-30>  Number of MICA modules which can be simultaneously recovered

Router(config)# modem recovery maintenance schedule ?
  immediate  Attempt recovery immediately
  pending    Delay recovery until maintenance time
```

The following example shows how to set modem recovery maintenance to start immediately:

```
modem recovery maintenance schedule immediate
```

Related Commands

Command	Description
modem recovery action	Specifies the modem recovery mode when a modem has been identified as faulty.
modem recovery threshold	Specifies the threshold, which starts the modem recovery process.
modem recovery-time	Sets the maximum amount of time the call-switching module waits for a local modem to respond to a request before it is considered locked in a suspended state.

modem recovery threshold

To specify a failed call threshold that starts the modem recovery process, use the **modem recovery threshold** command in global configuration mode. To disable the threshold value, use the **no** form of this command.

modem recovery threshold *failed-calls*

no modem recovery threshold

Syntax Description

failed-calls	Number of consecutive call attempts that fail to queue up before the modem is deemed faulty, in the range from 1 to 1000.

Command Default

30 call attempts are enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0	This command was introduced.
12.1(2.3)T1	This command was no longer supported on Cisco AS5800 platforms.

Usage Guidelines

MICA technologies portware is downloaded on a modular basis and not on a modem basis. Thus, reloading MICA portware requires all 6 or 12 modems in a module to be reloaded.

Note Beginning with Cisco IOS Release 12.1(2.3)T1, the **modem recovery threshold** command is no longer supported for MICA technologies modems on the Cisco AS5800 platforms. To specify a modem recovery action for MICA technologies modems on the Cisco AS5800 platforms, use the **spe recovery** command.

Examples

The following example shows how to set the modem recovery threshold to 12 failed calls:

```
modem recovery threshold 12
```

Related Commands

Command	Description
modem recovery action	Specifies the modem recovery mode when a modem has been identified as faulty.
modem recovery maintenance	Specifies the scheduled modem maintenance recovery behavior.
modem recovery-time	Sets the maximum amount of time the call-switching module waits for a local modem to respond to a request before it is considered locked in a suspended state.

modem recovery-time

To set the maximum amount of time the call-switching module waits for a local modem to respond to a request before it is considered locked in a suspended state, use the **modem recovery-time** command in global configuration mode. To set a 5-minute response time, which is the default setting, use the **no** form of this command.

modem recovery-time *response-time*

no modem recovery-time

Syntax Description

response-time	Maximum amount of time, in minutes, for which local modems wait for a response; default is 5 minutes.

Command Default

5 minutes

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.1(2.3)T	This command was no longer supported on Cisco AS5800 platforms.

Usage Guidelines

This command does not apply to basic modems that do not have out-of-band ports.

After the call-switching module resets a suspended modem, it recovers to a default call switching module state.

Note Beginning with Cisco IOS Release 12.1(2.3)T, the **modem recovery-time command** is no longer supported for MICA technologies modems on the Cisco AS5800 platforms. To specify a modem recovery action for MICA technologies modems on the Cisco AS5800 platforms, use the **spe recovery** command.

Examples

The following example configures the call-switching module to wait for 8 minutes:

```
modem recovery-time 8
```

Related Commands

Command	Description
modem recovery action	Specifies the modem recovery mode when a modem has been identified as faulty.
modem recovery maintenance	Specifies the scheduled modem maintenance recovery behavior.
modem recovery threshold	Specifies the threshold, which starts the modem recovery process.

modem ri-is-cd

The **modem ri-is-cd** command is replaced by the **modem dialin** command. See the description of the **modem dialin** command for more information.

modem shutdown

To abruptly shut down an active or idle modem installed in an access server or router, use the **modem shutdown** command in line configuration mode. To take the modem out of a shutdown state and place it back in service, use the **no** form of this command.

modem shutdown

no modem shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

Command is disabled.

Command Modes

Line configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Enable the **no modem shutdown** command to restore to service a modem that has been shut down.

Examples

The following example abruptly shuts down the modem associated with line 1/0/6. All active calls on the modem are dropped immediately.

```
line 1/0/6
 modem shutdown
```

The following example abruptly shuts down a range of modems:

```
line 1/0/5 1/0/72
 modem shutdown
```

The following example abruptly shuts down the modem associated with line 2 on a Cisco AS5300. All active calls on the modem are dropped immediately.

```
 line 2
  modem shutdown
```

Related Commands

Command	Description
modem busyout	Disables a modem from dialing or answering calls whereby the disabling action is not executed until the active modem returns to an idle state.

modem startup-test

Support for the **modem startup-test** command was removed in Cisco IOS Release 12.2(11)T. The use of this command is not recommended. In most cases, nonfunctional integrated modems will automatically be removed from service by the system. See the **modem recovery action** command and the **spe recovery** command for more configuration options for nonfunctional modems. For further information about MICA modem recovery, refer to the *Configuring MICA Modem Recovery* technical note. For further information about NextPort service processing element (SPE) recovery, refer to the *Configuring NextPort SPE Recovery* technical note.

modem status-poll

To poll for modem statistics through a modem's out-of-band feature, use the **modem status-poll** command in line configuration mode. To disable status polling through the out-of-band feature for a specified modem, use the **no** form of this command.

modem status-poll

no modem status-poll

Syntax Description

This command has no arguments or keywords.

Command Default

Command is enabled.

Command Modes

Line configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

This command applies only to manageable modems that have out-of-band ports.

Note This command does not apply to basic modems that have out-of-band ports.

Examples

The following example enables modem status polling through TTY line 1:

```
line 1
 modem status-poll
```

Related Commands

Command	Description
modem min-speed max-speed	Sets the maximum number of polling attempts used to retrieve performance statistics from a modem installed in an access server or router.
modem poll time	Sets the time interval between modem polls, which are used to periodically retrieve and report modem statistics.

modemcap edit

To change a modem value that was returned from the **show modemcap** command, use the **modemcap edit** command in global configuration mode.

modemcap edit *modem-name attribute at-command*

Syntax Description

modem-name	Name of the modem whose values are being edited.
attribute	Modem capability, or attribute, as defined by the **show modemcap** command.
at-command	The AT command equivalent (such as **&F**).

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Modemcaps are printed within the configuration file. You can edit them using this command.

Configure one attribute of one modem at a time. See the modem-capability values defined by the **show modemcap** command.

Examples

The following example adds the factory default entry, **&F**, to the configuration file. This entry and others like it are stored in a database that is referenced by the configuration file.

```
modemcap edit codex_3250 factory-default &F
```

Related Commands

Command	Description
modemcap entry	Stores and compresses information about the capability of a specified modem.
show modemcap	Displays the values set for the current modem and lists the modems for which the router has entries.

modemcap entry

To store and compress information about the capability of a specified modem, use the **modemcap entry** command in global configuration mode. To disable this feature, use the **no** form of this command.

modemcap entry *modem-type*

no modemcap entry *modem-type*

Syntax Description

modem-type	Type of supported modem as specified in Table 16.

Command Default

The capability values that exist in the specified modem at the time that the command is issued

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.1(5)T	This command was implemented on the Cisco 2600 series and the Cisco 3600 series.

Usage Guidelines

This command displays the capability of the specified modem. Modemcaps are printed within the configuration file and are intended to be edited using the **modemcap edit** command. The **modemcap entry** command does not display values that are not set in the modem.

Use the **modemcap entry** command with the **show modemcap** command to interpret the capability of the specified modem. Table 16 lists the modemcap entries for supported modems.

Table 16 Modemcap Entries for Supported Modems

Modemcap Name	Modem Type
External Modems	
codex_3260	Motorola Codex 3260
default	Generic “Hayes” interface
global_village	Global Village Teleport
hayes_optima	Hayes Optima[1]
nec_piafs	NEC PIAFS TA
nec_v34	NEC V.34
nec_v110	NEC V.110 TA
telebit_t3000	Telebit T3000
usr_courier	U.S. Robotics Courier
usr_sportster	U.S. Robotics Sportster

Table 16 Modemcap Entries for Supported Modems (continued)

Modemcap Name	Modem Type
viva	Viva (Rockwell ACF with MNP)
Internal Modems	
cisco_v110	Cisco (NEC) internal V.110 TA (AS5200)
mica	Cisco MICA HMM/DMM digital
microcom_hdms	Microcom HDMS chassis
microcom_mimic	Cisco (Microcom) analog (NM-AM-2600/3600)
microcom_server	Cisco (Microcom) V.34/56K digital (AS5300)
nextport	Cisco NextPort CSMV/6 digital

1. This built-in modemcap is not recommended for use on an Optima because it sets the modem to automatic speed buffering. This modemcap disables error control and may result in poor performance. Instead, use modemcap **default.**

Examples

The following example shows how to select a U.S. Robotics Sportster modem type:

```
modemcap entry usr_sportster
```

Related Commands

Command	Description
modem hold-reset	Resets and isolates integrated modems for extensive troubleshooting.
show modemcap	Displays the values set for the current modem and lists the modems for which the router has entries.

modem-pool

To create a new modem pool or to specify an existing modem pool, use the **modem-pool** command in global configuration mode. To delete a modem pool from the access server configuration, use the **no** form of this command.

modem-pool *name*

no modem-pool *name*

Syntax Description

name	Name of a modem pool.

Command Default

All modems are configured to be part of one system default modem pool (displayed as System-def-Mpool by the **show modem-pool** command.). For example, if you have 120 MICA technologies modems loaded in your access server, 120 modems are in the default modem pool.

Command Modes

Global configuration

Command History

Release	Modification
11.2P	This command was introduced.

Usage Guidelines

Modem pools enable you to physically partition or virtually partition your access server for dial-in and dial-out access.

Physical partitioning makes one access server appear as if it is multiple access servers loaded with different types of modem services (for example, v.34 modems, fax capable modems, and point-of-sale (POS) modems). Each service is part of one modem pool and assigned a unique Dialed Number Information Service (DNIS) number.

Virtual partitioning creates one large modem pool on the access server, but enables different customers to dial in and share the modem resources. Each customer is assigned its own DNIS number. Each customer is given overflow protection, which guarantees a certain number of simultaneous connections.

Note MICA and Microcom modems support incoming analog calls over ISDN PRI. However, only MICA technologies modems support modem pooling for CT1 and CE1 configurations with channel-associated signaling.

Examples

The following example creates a modem pool called v90service. After the **modem-pool v90service** command is issued, modem pool configuration mode is accessed and the router prompt changes.

```
modem-pool v90service
```

Related Commands

Command	Description
called-number (modem pool)	Assigns a called party number to a pool of modems.
clear modempool-counters	Clears active or running counters associated with one or more modem pools.
pool-member	Assigns a range of modems to a modem pool.
show modem-pool	Displays the configuration and connection status for one or more modem pools.

modemui

To enter Cisco modem user interface mode and enter Hayes-compatible modem commands, use the **modemui** command in EXEC mode.

modemui [*modem-commands*]

Syntax Description

modem-commands	(Optional) Hayes-compatible modem commands. Table 17 lists the modem commands supported on Cisco routers. Multiple commands may be entered.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

Use the **modemui** command to enter interactive Cisco modem user interface mode, which allows the Hayes-compatible modem command subset listed in Table 17 to be entered.

The **modemui** EXEC command can also be entered with the **autocommand** line configuration command to configure the Cisco modem user interface feature as part of line configuration.

Note Before entering the modem command that dials the modem telephone number, you must map the telephone number to an appropriate IP host using the Cisco IOS **ip host** global configuration command.

Table 17 Cisco-Supported Hayes Modem Commands

Hayes Modem Commands	Description
AT	Attention command. Enters modem command execution mode. You can add any of the command settings listed in this table to the **AT** command.
DT*string* **DP***string*	Dials outbound tone (**T**) or pulse (**P**) call. The string following the **T** or **P** character is used as an argument to the Cisco IOS **connect** EXEC command. Before dialing, you must set up an appropriate IP host using the Cisco IOS **ip host** global configuration command. For example: `ip host t555-0112 4023 10.0.0.51` Valid characters for *string* are the same as the characters that are used in a host name for the Cisco IOS **connect** command, as follows: • The numbers 0 through 9 • Uppercase letters A through Z • Lowercase letters a through z • The . (period), - (hyphen), and _ (underscore) characters No other characters (such as # or *) are accepted in the dial string, and unsupported characters are stripped before dialing occurs.
E*n*	Echo mode. Values for *n* are as follows: • 0 turns off command echo. • 1 turns on command echo (default).
H*n*	Hangup mode. A value of 0 or 1 closes the connection.
I*n*	Information mode. The information displayed is set in a banner configured with the Cisco IOS **MODEMUI-VERSION** global configuration command. Acceptable values for *n* are the numbers 0 through 6.
O*n*	Online mode. A value of 0 or 1 resumes the connection.
Q*n*	Quiet mode. Values for *n* are as follows: • 0 displays modem result codes (default). • 1 inhibits modem result codes display (quiet mode).
S*n*=*v*	Set selected register (S-register). **Note** The standard Hayes modem S-register settings S0 through S53 are accepted by Cisco IOS software, but do not have any effect. Choose one of the following S-registers for *n*: • S201—Command mode parity sniffing. If the value (*v*) for S201 is 0 (default), parity for both the command and data portions of a call are controlled by the Cisco IOS **parity** and **databits** line configuration commands. If the value (*v*) for S201 is 1, mark or space parity for the command session will be taken from the Hayes **AT** part of the command, and the data portion will be 8-bit transparent.

Table 17 Cisco-Supported Hayes Modem Commands (continued)

Hayes Modem Commands	Description
	• S202—Output mask. This setting allows mark parity to be unconditionally implemented for the command characters. The default value for S202 is 0 (no parity). The value 128 causes command characters to be sent with mark parity. • S203—Connect delay. Allows a delay in seconds to be added to the time between when the **ATD** command is executed and when the call success or failure code is displayed. This delay is sometimes required because a Telnet connection is established more quickly than placing a telephone call. The value for S203 can be a number from 0 to 255. The actual value applied to the connect delay is 10 percent of the number entered for *v*. For example, a value of 300 sets a connect delay of 30 seconds. The default value is 0. • S204—Connect code. Allows the result code for a successful connection to be specified. The default is code 1 for the unextended mode, but you can configure one of the following numbers to display a selected line speed. For example, connection code 10 selects CONNECT 2400. By allowing the code to be expressed explicitly, you can allow for a "CONNECT 2400" response message to be displayed, regardless of the actual line speed. The default for *v* is 0, or choose one of the following connection codes: – 9—CONNECT 1200 – 10—CONNECT 2400 – 11—CONNECT 4800 – 12—CONNECT 9600 – 13—CONNECT 14400 – 14—CONNECT 19200 – 15—CONNECT 38400 – 16—CONNECT 57600
S*n*?	S-register query. The value for *n* is the number of the S-register to query (S201 through S204; see the preceding list).
V*n*	Result code format. Values for *n* are as follows: • 0 displays a short result report. • 1 displays a long result report (default).
X*n*	Extended result codes. The value for *n* is any nonzero number, which appends /NONE to the connect message. Also see the preceding description for S-register S204, for changing the reported connection speed.
Z **Z99**	Reset to default configuration. Choose one of the following reset options: • **ATZ** returns the Cisco modem user interface to its default state and re-executes the initialization string provided in the **modemui** command. • **ATZ99** returns to the standard Cisco IOS software user interface (EXEC) mode.

Examples

The following example shows how to configure a line for the Cisco modem user interface feature and set the modem in no-echo, short-response mode:

```
line aux 0
 login authentication modem
 modem dialin delay
 autocommand modemui ATE0V0
 transport input all
 stopbits 1
 speed 38400
 flowcontrol hardware
```

The following example shows how to enter Cisco modem user interface mode from the Cisco IOS EXEC mode and enter Hayes-compatible **AT** commands to dial and test the modem:

```
Router# modemui
AT
OK
ATDT4155551234
CONNECT
User Access Verification
Username:
```

Related Commands

Command	Description
autocommand	Configures the Cisco IOS software to automatically execute a command when a user connects to a particular line.
connect	Logs in to a host that supports Telnet, rlogin, or LAT.
ip host	Defines a static host name-to-address mapping in the host cache.
modemui-version	Displays a banner in response to the Hayes information mode command.

modemui-version

To display a banner as a response to the Hayes modem information command, use the **modemui-version** command in global configuration mode. To remove or change the banner display, use the **no** form of this command.

modemui-version *delimiter banner-text delimiter*

no modemui-version *delimiter banner-text delimiter*

Syntax Description

delimiter	Character that you choose, such as # or /, to signal the beginning and end of the banner message.
banner-text	Banner message text.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

Use the **modemui-version** command to configure banners for the Hayes information mode command *(***ATI***n)*.

Examples

The following example configures the modem user interface banner to display the modem model and code revision in response to the **ATI6** Cisco modem user interface command:

```
modemui-version / Telebit T3000, Version 1.5 /
```

Related Commands

Command	Description
modemui	Enters Cisco modem user interface mode.

multilink

To limit the total number multilink PPP (MLP) sessions for all virtual private dialup network (VPDN) multilink users, enter the **multilink** command in VPDN group configuration mode. To remove the MLP session limit, enter the **no** form of this command.

multilink {**bundle** *bundles* | **link** *links*}

no multilink {**bundle** *bundles* | **link** *links*}

Syntax Description

bundle *bundles*	Configures the number of MLP bundles supported for a VPDN group. In general, each user requires one bundle. Valid values for the *bundles* argument range from 0 to 32,767.
link *links*	Configures the number of sessions supported for each bundle. Valid values for the links argument range from 0 to 32,767.

Command Default

No MLP session limit is set.

Command Modes

VPDN group configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.

Usage Guidelines

Use the **multilink** VPDN group configuration command to limit the total number of sessions for all MLP users. Each user requires one bundle, regardless if the user is a remote modem client or an ISDN client.

One modem client using one B channel requires one link. One ISDN BRI node may require up to two links for one BRI line connection. The second B channel of an ISDN BRI node comes up when the maximum threshold is exceeded.

Examples

The following example configures a VPDN group called group1 to initiate Layer 2 Tunnel Protocol (L2TP) tunnels to the tunnel server at IP address 10.2.2.2. Ten MLP bundles are configured for users that dial in to the domain cisco.com. Each bundle is configured to support a maximum of 5 links, limiting the total number of MLP sessions to 50.

```
Router(config)# vpdn-group group1
Router(config-vpdn)# request-dialin
Router(config-vpdn-req-in)# protocol l2tp
Router(config-vpdn-req-in)# domain cisco.com
Router(config-vpdn-req-in)# exit
Router(config-vpdn)# initiate-to ip 10.2.2.2
Router(config-vpdn)# multilink bundle 10
Router(config-vpdn)# multilink link 5
```

Related Commands

Command	Description
request-dialin	Creates a request dial-in VPDN subgroup that configures a NAS to request the establishment of a dial-in tunnel to a tunnel server, and enters request dial-in VPDN subgroup configuration mode.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.

multilink bundle-name

To select a method for naming multilink bundles, use the **multilink bundle-name** command in global configuration mode. To remove the selection method, use the **no** form of this command.

multilink bundle-name {**authenticated** | **endpoint** | **both**}

no multilink bundle-name {**authenticated** | **endpoint** | **both**}

Syntax Description

authenticated	Authenticated name of the peer. This is the default.
endpoint	Endpoint discriminator of the peer.
both	Authenticated name and endpoint discriminator of the peer.

Command Default

Authenticated name of the peer.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

The **authenticated** keyword defines the selection criteria for the bundle name as the authenticated name, the endpoint discriminator if the link is not authenticated, or the caller ID if neither an authenticated name nor an endpoint is supplied.

The **endpoint** keyword defines the selection criteria for the bundle name as the endpoint discriminator, the authenticated name if no endpoint is supplied, or the caller ID if neither an authenticated name nor an endpoint is supplied.

The **both** keyword defines the selection criteria for the bundle name as an authenticated name-endpoint discriminator pair, the authenticated name if no endpoint is supplied, the endpoint discriminator if the link is not authenticated, or the caller ID if neither an authenticated name nor an endpoint is supplied.

Examples

The following example sets the selection criteria for the multilink bundle name as the endpoint discriminator:

```
multilink bundle-name endpoint
```

multilink max-fragments

The **multilink max-fragments** command is replaced by the **ppp multilink fragment maximum** command. See the description of the **ppp multilink fragment maximum** command for more information.

multilink virtual-template

To specify a virtual template from which the specified Multilink PPP (MLP) bundle interface can clone its interface parameters, use the **multilink virtual-template** command in global configuration mode. To remove the defined virtual template, use the **no** form of the command.

multilink virtual-template *number*

no multilink virtual-template *number*

Syntax Description

number	Number of the virtual template to be used to clone the MLP bundle interface. An integer in the range from 1 to the largest number of virtual templates the software image supports (typically 25).

Command Default

No template is specified.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Configuring a specific IP address in a virtual template can result in the establishment of erroneous routes and the loss of IP packets.

Examples

The following example specifies that virtual template 1 is to be used for MLP ,and then defines virtual template 1:

```
multilink virtual-template 1
interface virtual-template 1
 ip unnumbered ethernet 0
 encapsulation ppp
 ppp multilink
 ppp authentication chap
```

Related Commands

Command	Description
interface virtual-template	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.

multilink-group

The **multilink-group** command is replaced by the **ppp multilink group** command. See the description of the **ppp multilink group** command for more information.

name (dial peer cor custom)

To specify the name for a custom class of restrictions (COR), use the **name** command in dial peer COR custom configuration mode. To remove a specified COR, use the **no** form of this command.

name *class-name*

no name *class-name*

Syntax Description

class-name	Name that describes the specific COR.

Command Default

No default behavior or values.

Command Modes

Dial peer COR custom configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

The **dial-peer cor custom** and **name** commands define the names of capabilities on which to apply COR operation. Examples of names might include any of the following: call1900, call527, call9, or call 911. You must define the capabilities before you specify the COR rules.

You can define a maximum of 64 COR names.

Examples

The following example defines three COR names:

```
dial-peer cor custom
 name 900_call
 name 800_call
 name catchall
```

Related Commands

Command	Description
dial-peer cor custom	Specifies that named CORs apply to dial peers.
name	Assigns a name to the internal adapter.

netbios nbf

To enable the NetBIOS Frames Protocol (NBF) on an interface, use the **netbios nbf** command in interface configuration mode. To disable NetBIOS Frames Protocol support on an interface, use the **no** form of this command.

netbios nbf

no netbios nbf

Syntax Description

This command has no arguments or keywords.

Command Default

Command is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Examples

The following example enables NBF on asynchronous interface 1 (connected to remote access client using a NetBEUI application) and Ethernet interface 0 (connected to the remote router):

```
interface async 1
 netbios nbf
interface ethernet 0
 netbios nbf
```

Related Commands

Command	Description
netbios name-cache	Defines a static NetBIOS name cache entry, tying the server with the name netbios-name to the mac-address, and specifying that the server is accessible either locally through the interface-name specified, or remotely through the ring-group group-number specified.
show nbf sessions	Displays NetBEUI connection information.
show netbios cache	Displays a list of NetBIOS cache entries.

network-clock-priority

To specify the clock-recovery priority for the BRI voice ports in a BRI voice module (BVM), use the **network-clock-priority** command in interface configuration mode. To restore the default (low) clock-recovery priority, use the **no** form of this command.

network-clock-priority {**low** | **high**}

no network-clock-priority {**low** | **high**}

Syntax Description

low	The BRI port is second priority to recover clock.
high	The BRI port is first priority to recover clock.

Command Default

Each BRI voice port has low clock-recovery priority. The BRI VIC port provides clocking (high).

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810 concentrator.
12.1(3)XI	This command was implemented on the Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

Because the BRI voice interface card can support both ISDN NT and TE ports, this command allows a "local loop" to be configured for testing. By default the TE port on the BRI VIC receives the clock source to drive the whole BRI (**network-clock-priority high**). Setting the clock priority to **low** allows the connected port to provide clocking.

This command becomes effective only when the BVM is the clock source for the Cisco MC3810, which can happen in one of three ways:

- When the BVM is specified as the first-priority network clock source through the **network-clock-select** command.
- When the BVM is specified as a lower-priority network clock source, and a higher-priority network clock source is lost.
- When the BVM is the only network clock source.

The BRI voice port supplying clock operates as a line source; if there are other BRI voice ports configured as TE, they operate in loop-timed mode.

Regardless of the **network-clock-priority** setting, the first TE-configured BRI voice port that becomes active is automatically chosen to supply clock. The clock source does not change if another BRI voice port configured for **network-clock-priority high** becomes active.

If the chosen clocking port becomes inactive, the system searches for clock on the active TE-configured ports in the following order:

1. Ports configured as **network-clock-priority high** in order from lowest (1) to highest (4).
2. Ports configured as **network-clock-priority low** in order from lowest (1) to highest (4).

If the originally chosen port then reactivates, it resumes its role as clock source regardless of its **network-clock-priority** setting.

If you enter either the **no network-clock-priority low** or the **no network-clock-priority high** command, the network clock priority defaults to low.

Examples

The following example configures BRI voice port 1 as a first priority clock source:

```
interface bri 0/1
 network-clock-priority high
```

Related Commands

Command	Description
number	Specifies selection priority for the clock sources.

number

To add a Calling Line Identification (CLID) or Dialed Number Identification Service (DNIS) number to a dialer group, use the **number** command in CLID group configuration or DNIS group configuration mode followed by the specifying number. To remove a number from a group, use the **no** form of this command.

number *id-number*

no number *id-number*

Syntax Description

id-number	CLID or DNIS number, which can have up to 65 digits.

Note The CLID screening feature rejects this number if it matches the CLID of an incoming call. Valid CLID numbers are all numeric, or numbers that contain the wildcard *x*. You can use *x* (signifying a single number don't care state), *X* or **.** as wildcards within each CLID number. The asterisk (*) wildcard is not accepted.

Command Default

No default behavior or values.

Command Modes

CLID group configuration
DNIS group configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.
12.1(5)T	This command was enhanced to add CLID numbers to a CLID group and DNIS numbers to a DNIS group.

Usage Guidelines

You can organize CLID numbers for a customer or service type into a CLID group. You can add multiple CLID groups to a customer profile. Add all CLID numbers into one CLID group, or subdivide the CLID numbers using criteria such as call type, geographical location, or division.

The Cisco IOS software also includes a feature that streamlines the DNIS configuration process. By replacing any digit with an *X* (for example, issuing the **number 555222121*x*** command), clients dialing different numbers, such as 5552221214 or 5552221215, are automatically mapped to the same customer profile. The *X* variable is a placeholder for the digits 1 through 9.

Examples

The following example shows the command to use to assign a number to a CLID group named group1:

```
dialer clid group group1
 number 2121212121
```

The following example shows a DNIS group called dnis_isp_1 and DNIS numbers 1234 and 5678 assigned to the DNIS group:

```
dialer dnis group dnis_isp_1
 number 1234
 number 5678
```

Related Commands

Command	Description
clid group	Adds a CLID group to a discriminator.
dnis group	Includes a group of DNIS numbers in a customer profile.
resource-pool call treatment discriminator	Creates a call discrimination profile.

peer default ip address

To specify an IP address, an address from a specific IP address pool, or an address from the Dynamic Host Configuration Protocol (DHCP) mechanism to be returned to a remote peer connecting to this interface, use the **peer default ip address** command in interface configuration mode. To disable a prior peer IP address pooling configuration on an interface, or to remove the default address from your configuration, use the **no** form of this command.

peer default ip address {*ip-address* | **dhcp-pool** | **dhcp** | **pool** [*pool-name*]}

no peer default ip address

Syntax Description

ip-address	Specific IP address to be assigned to a remote peer dialing in to the interface. To prevent duplicate IP addresses from being assigned on more than one interface, this argument cannot be applied to a dialer rotary group nor to an ISDN interface.
dhcp-pool	Retrieves an IP address from an on-demand address pool. This option only supports remote access (PPP) sessions into MPLS VPNs.
dhcp	Retrieves an IP address from the DHCP server.
pool	Uses the global default mechanism as defined by the **ip address-pool** command unless the optional *pool-name* argument is supplied. This is the default.
pool-name	(Optional) Name of a local address pool created using the **ip local pool** command. DHCP retrieves an address from this pool regardless of the global default mechanism setting.

Command Default

The default is **pool**.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(8)T	The **dhcp-pool** keyword was added.

Usage Guidelines

This command applies to point-to-point interfaces that support the PPP or Serial Line Internet Protocol (SLIP) encapsulation. This command sets the address used on the remote (PC) side.

Note This command replaces the **async default ip address** command.

This command allows an administrator to configure all possible address pooling mechanisms on an interface-by-interface basis.

The **peer default ip address** command can override the global default mechanism defined by the **ip address-pool** command on an interface-by-interface basis, as follows:

- For all interfaces not configured with a peer default IP address mechanism (equivalent to selecting the **peer default ip address pool** command), the router uses the global default mechanism that is defined by the **ip address-pool** command.
- If you select the **peer default ip address pool** *pool-name* form of this command, then the router uses the locally configured pool on this interface and does not follow the global default mechanism.
- If you select the **peer default ip address** *ip-address* form of this command, the specified IP address is assigned to any peer connecting to this interface and any global default mechanism is overridden for this interface.
- If you select the **peer default ip address dhcp** form of this command, the DHCP proxy-client mechanism is used by default on this interface and any global default mechanism is overridden for this interface.
- If you select the **peer default ip address dhcp-pool** form of this command, the DHCP on-demand address pooling mechanism is used by default on this interface and any global default mechanism is overridden for this interface.

Examples

The following command specifies that this interface will use a local IP address pool named pool3:

```
peer default ip address pool pool3
```

The following command specifies that this interface will use the IP address 172.19.34.21:

```
peer default ip address 172.19.34.21
```

The following command reenables the global default mechanism to be used on this interface:

```
peer default ip address pool
```

The following example specifies address 192.168.7.51 for asynchronous interface 6:

```
line 20
 speed 115200
interface async 6
 peer default ip address 192.168.7.51
```

Related Commands

Command	Description
async dynamic address	Specifies dynamic asynchronous addressing versus default addressing.
encapsulation slip	Enables SLIP encapsulation.
exec	Allows an EXEC process on a line.
ip address-pool	Enables an address pooling mechanism used to supply IP addresses to dial in asynchronous, synchronous, or ISDN point-to-point interfaces.
ip dhcp-server	Specifies which DHCP servers to use on a network, and specifies the IP address of one or more DHCP servers available on the network.
ip local pool	Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.
ppp	Starts an asynchronous connection using PPP.

Command	Description
show cot dsp	Displays information about the COT DSP configuration or current status.
slip	Starts a serial connection to a remote host using SLIP.

peer ip address forced

To force the router to assign a peer the next available IP address in the pool for an interface, use the **peer ip address forced** command in interface configuration mode. To allow a peer to negotiate a specific IP address or to allow the router to attempt to assign a peer its previously assigned IP address, use the **no** form of this command.

peer ip address forced

no peer ip address forced

Syntax Description

This command has no arguments or keywords.

Command Default

When a network device dials in to a Cisco network access server (NAS) that is configured to assign an IP address to the network device, the NAS attempts to assign the device the address it was assigned previously. If that address is unavailable or if no address in the pool was assigned previously, the NAS then assigns the next available address in its pool.

Command Modes

Interface configuration

Command History

Release	Modification
12.2T	This command was introduced.

Usage Guidelines

The **peer ip address forced** command is used for point-to-point interfaces that support a link framing protocol such as PPP where the NAS will assign a peer IP address from an address pool as a result of the following conditions:

- The NAS is configured with a pool of network addresses at the interface supporting the peers (configured by use of the **ip local-pool** command).
- The NAS is configured to assign IP addresses to peers from a pool. A pool of IP addresses can be configured and applied at the interface by use of the **ip address-pool** command and the **peer default ip address pool** command or as a RADIUS server directive.
- The peer is configured to request an IP address from the NAS server (for example, as configured by use of the **ip address negotiated** command).

To force the NAS to allocate the next available IP address from the pool for the interface, use the **peer ip address forced** command. Any attempts to allocate a previously held IP address or a specifically requested IP address are suppressed; instead, the NAS allocates the next available IP address from the specified pool. This feature can be used to prevent users from obtaining the same IP address for each dial-in session.

Examples

The following example specifies that the interface will allocate the next available address from the pool whenever an address is requested from a pool:

```
interface Virtual-template 1
 peer default ip address pool poolA poolB
 peer ip address forced
```

The following example specifies that the interface will allow a peer to negotiate an IP address or will attempt to assign a previously assigned address:

```
interface Virtual-template 1
 peer default ip address pool poolA poolB
 no peer ip address forced
```

Related Commands

Command	Description
ip address negotiated	Specifies that the IP address for a particular interface is obtained via PPP IPCP address negotiation.
ip address-pool	Enables an address pooling mechanism used to supply IP addresses to dial-in asynchronous, synchronous, or ISDN point-to-point interfaces.
ip local-pool	Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.
peer default ip address	Specifies an IP address, an address from a specific IP address pool, or an address from the DHCP mechanism to be returned to a remote peer connecting to this interface.
ppp	Starts an asynchronous connection using PPP when you want to connect from a remote node computer to an EXEC session on the access server and want to connect from the access server to a device on the network.

peer match aaa-pools

To specify that any IP address pool name supplied by authentication, authorization, and accounting (AAA) servers must also be present in the list of pool names specified in the **peer default ip address pool** interface configuration command, use the **peer match aaa-pools** command in interface configuration mode. To configure the software to use any pool name supplied by the AAA server (default configuration), use the **no** form of this command.

peer match aaa-pools

no peer match aaa-pools

Syntax Description

This command has no arguments or keywords.

Command Default

Command is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(6)T	This command was introduced.

Usage Guidelines

This command provides the ability to control or restrict the use of pool names supplied by AAA to only those pool names that are configured on the router. This ability is useful in cases where the AAA server and the router and its local configuration are controlled by different administrators, as would be the case for a wholesale dial supplier where the AAA servers are owned by individual customers.

When the **peer match aaa-pools** command is configured on an interface, the IP address pool names used are those specified in the local configuration as part of the **peer default ip address** command and the pool names supplied by the AAA server.

When the **no peer match aaa-pools** command is used, pool name selection is controlled by the AAA server, as follows: When the AAA server supplies a pool name, that is the only pool used. If AAA does not supply a pool name, then the normal IP default pool name processing is used as described in the **peer default ip address** command page.

Examples

The following example shows how to configure pool name restrictions in a Resource Pool Management (RPM) customer profile template:

```
template Word
  multilink max-fragments
  peer match aaa-pools
  peer default ip address pool poolA poolB
  ppp ipcp dns 10.1.1.1
resource-pool profile customer WORD
  source template Word
  aaa group-configuration AAA-group1
```

```
template user_direct
  peer default ip address pool mypool
  ppp authentication chap isdn-users
  ppp multilink
```

Related Commands

Command	Description
ip local pool	Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.
peer default ip address	Specifies an IP address, an address from a specific IP address pool, or an address from the DHCP mechanism to be returned to a remote peer connecting to this interface.
peer pool backup	Directs the pool software to use the local pool name configured with the **peer default ip address** interface configuration command to supplement the pool names supplied by AAA.
peer pool static	Suppresses an attempt to load all dynamic pools from the AAA server when a missing pool name is encountered.

peer pool backup

To provide backup IP address pool names supplied by authentication, authorization, and accounting (AAA) with local pool names, use the **peer pool backup** command in interface configuration mode. To disable the local pool name backup feature, use the **no** form of this command.

peer pool backup

no peer pool backup

Syntax Description

This command has no arguments or keywords.

Command Default

No backup IP address pool names are configured

Command Modes

Interface configuration

Command History

Release	Modification
12.2(8)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The **peer pool backup** command is useful in large-scale dial-out environments with a large number of independently controlled AAA servers. Difficulties arise when the network access server (NAS) must provide IP address pool name resolution when a new pool is introduced by one of the AAA servers before that pool is set up on the NAS, or when an existing local pool becomes exhausted but the AAA server actually has other pools that would be acceptable as IP address sources.

The **peer pool backup** command uses the local pool names configured with the **peer default ip address pool** interface configuration command to supplement the pool names supplied by AAA. The problems of pool name resolution and exhaustion can be solved by configuring backup pool names on a per-interface basis using both the **peer default ip address pool** and **peer pool backup** interface configuration commands.

You may also configure local restrictions on the use of AAA-supplied pool names to a NAS-specified set by adding the **peer match aaa-pools** interface configuration command to the configuration. The **peer match aaa-pools** command specifies that any AAA-supplied pool name must match one of the pool names supplied with the **peer default ip address pool** command. See the “Examples” section for an example.

Examples

In the following example, the search order for backup pool names set by the **peer default ip address pool** command is pool1 then pool2. These pools will be used when the NAS cannot resolve a pool name or when an existing pool of IP addresses is exhausted.

```
interface Dialer1
 ip unnumbered FastEthernet0
 encapsulation ppp
 dialer pool 1
 dialer idle-timeout 3600
 dialer-group 1
 peer pool backup
 peer default ip address pool pool1 pool2
 no fair-queue
 no cdp enable
 ppp authentication chap
```

In the following example, assume that there is a AAA-supplied IP address pool named poolA. By adding the **peer match aaa-pools** command to the configuration, the AAA-supplied pool named poolA will not be used because it does not appear in the **peer default ip address pool** command; only the pools named pool1 and pool2 will be searched.

```
interface serial 1:23
 ip address 10.4.4.1 255.255.255.0
 encapsulation ppp
 ppp authentication chap
 dialer-group 1
 peer pool backup
 peer match aaa-pools
 peer default ip address pool pool1 pool2
 isdn switch-type primary-5ess
```

Related Commands

Command	Description
ip local pool	Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.
peer default ip address	Specifies an IP address, an address from a specific IP address pool, or an address from the DHCP mechanism to be returned to a remote peer connecting to this interface.
peer match aaa-pools	Specifies that any AAA-supplied pool name must match one of the pool names supplied with the **peer default ip address pool** command.
peer pool static	Suppresses an attempt to load all dynamic pools from a AAA server when a missing pool name is encountered.

peer pool static

To suppress an attempt to load all dynamic pools from an authentication, authorization, and accounting (AAA) server when a missing pool name is encountered, use the **peer pool static** command in interface configuration mode. To disable the suppression of dynamic pool loading and restore the normal dynamic pool loading behavior, use the **no** form of this command.

peer pool static

no peer pool static

Syntax Description

This command has no arguments or keywords.

Command Default

Dynamic pools are loaded

Command Modes

Interface configuration

Command History

Release	Modification
12.2(8)B	This command was introduced.
12.3(4)T	This feature was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The **peer pool static** command controls attempts by the pool software to load dynamic pools in response to a pool request from a specific interface. These dynamic pools are loaded at system startup and refreshed whenever a pool name not configured on the network access server (NAS) is specified for IP address allocation. Because the behavior of the NAS in response to a missing pool name can be changed using the **peer pool backup** interface configuration command, you may need to use the **peer pool static** command to control attempts to load all dynamic pools when the AAA-supplied pool name is not an existing local pool name. The **peer pool static** command provides a two-minute interval between attempts to download dynamic IP pools when a missing pool name is encountered.

Examples

The following partial example shows how to disable loading dynamic pools using the **peer pool static** command:

```
aaa new-model
aaa authentication ppp default group radius
aaa authorization exec default group radius
aaa authorization network default group radius
!
interface ATM0/0/0
 no ip address
 no ip directed-broadcast
 no ip route-cache
 no atm ilmi-keepalive
.
```

```
.
.
interface Virtual-Template1
 ip address 10.4.4.1 255.255.255.0
 encapsulation ppp
 ppp authentication chap
 no ip directed-broadcast
 peer pool static
 peer pool static
 peer default ip address pool pool3 pool4 pool5
 ip classless
 radius-server host 172.30.166.121
 radius-server key lab
 radius-server vsa send accounting
 radius-server vsa send authentication
!
 ip local pool pool2 10.4.4.2
 ip local pool pool3 10.4.4.3
 ip local pool pool4 10.4.4.4
 ip local pool pool5 10.4.4.5
```

In this configuration, any attempt to load a dynamic pool name is suppressed; only the backup pool names defined by the **peer default ip address pool** command will be used.

Related Commands

Command	Description
ip local pool	Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.
peer default ip address	Specifies an IP address, an address from a specific IP address pool, or an address from the DHCP mechanism to be returned to a remote peer connecting to this interface.
peer pool backup	Directs the pool software to use the local pool name configured with the **peer default ip address pool** interface configuration command to supplement the pool names supplied by AAA.

permission (dial peer voice)

To specify whether incoming or outgoing calls are permitted on the defined dial peer, use the **permission** command in dial peer voice configuration mode. To remove the specified permission, use the **no** form of this command.

permission {**orig** | **term** | **both** | **none**}

no permission {**orig** | **term** | **both** | **none**}

Syntax Description

orig	This dial peer is permitted to originate calls. Thus, the access server can accept incoming calls from the dial peer.
term	This dial peer is permitted to terminate calls. Thus, the access server can send outgoing calls to the dial peer.
both	This dial peer is permitted to originate and terminate calls. Both incoming and outgoing calls are permitted (default).
none	No incoming or outgoing calls can be made to or from this dial peer.

Command Default

Both incoming and outgoing calls are permitted.

Command Modes

Dial peer voice configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

After a dial peer is associated with an incoming call, the permission is checked to determine whether incoming calls are permitted on the dial peer. If permission is not set to **orig** or **both**, the incoming call is blocked.

After a dial peer is matched for an outgoing call, the permission is checked to determine whether outgoing calls are permitted on the dial peer. If permission is not set to **term** or **both**, the outgoing call using this dial peer fails.

Note The call may “rotary” to the next dial peer if the current dial peer does not have the **huntstop** command set.

Examples

The following example configures a dial peer and sets its permission to both originate and terminate calls:

```
dial-peer voice 526 pots
 answer-address 408526....
 corlist incoming list2
 direct-inward-dial
 permission both
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer voice configuration mode and defines a remote VoIP dial peer.

pool-range

To assign a range of modems to a modem pool, use the **pool-range** command in modem-pool configuration mode. To remove the range of modems, use the **no** form of the command.

pool-range [**tty**] {*modem1*-*modemN* | *x*/*y*}

no pool-range [**tty**] {*modem1*-*modemN* | *x*/*y*}

Syntax Description

tty	(Optional) Sets the range to terminal controller (TTY) lines.
modem1-*modemN*	Range of lines, which correspond to a range of modems or to a modem pool. A hyphen (-) is required between the two numbers. The range of modems you can choose from is equivalent to the number of modems in your access server that are not currently associated with another modem pool, up to a maximum of 48.
x/*y*	Slot/port numbers for an internal modem. A range of numbers is not accepted. The slash mark is required.

Command Default

Command is disabled. All modems are configured to be part of the system default modem pool.

Command Modes

Modem pool configuration

Command History

Release	Modification
11.2P	This command was introduced on the Cisco AS5200 and Cisco AS5300.

Usage Guidelines

For a complete description of modem pools and how they are configured on Cisco access servers, see the command page for the **modem-pool** command.

Replace the*modem1*-*modemN* arguments with the modem TTY line numbers that correspond with the range of modems you want in the modem pool. TTY line numbers start from 1, and they map to modem numbers that start from 0. For example, if you want to include modems 1/0 through 1/23 in a pool range, use the TTY line numbers 1 to 24. To verify the modem to TTY line numbering scheme, use the **show modem** *slot*/*port* command.

Note MICA technologies modems and Microcom modems support incoming analog calls over ISDN PRI. However, only MICA modems support modem pooling for CT1 and CE1 configurations with channel–associated signaling.

Examples

The following example assigns modem TTY line numbers 30 to 50 to a modem pool. The Dialed Number Information Service (DNIS) number is set to 2000. The customers dialing 2000 are guaranteed access to 21 modems. The 22nd client to dial in is refused connectivity because the maximum number of allowable connections is exceeded.

```
modem-pool v90service
 pool-range 30-50
 called-number 2000 max-conn 21
 exit
```

The following configuration rejects the **pool-range 30** command, because modem TTY line 30 is already a member of the modem pool v90service, which was configured in the previous example. Each modem in the access server is automatically assigned to a unique TTY line. TTY line numbers are assigned according to your shelf, slot, or port hardware configuration.

```
modem-pool v34service
 pool-range tty 30

% TTY 30 is already in another pool.
```

Related Commands

Command	Description
called-number (modem pool)	Assigns a called party number to a pool of modems.
clear modempool-counters	Clears active or running counters associated with one or more modem pools.
modem-pool	Creates a new modem pool or specifies an existing modem pool, which allows you to physically or virtually partition your access server for dial-in and dial-out access.
show modem-pool	Displays the configuration and connection status for one or more modem pools.

port (global)

To enter the port configuration mode, use the port command in global configuration mode. To exit port configuration mode, use the **no** form of this command.

Cisco AS5400 with NextPort DFC

port {*slot* | *slot*/*port*} [*slot* | *slot*/*port*]

no port {*slot* | *slot*/*port*} [*slot* | *slot*/*port*]

Cisco AS5800 with Universal Port Card

port {*shelf*/*slot* | *shelf*/*slot*/*port*} [*shelf*/*slot* | *shelf*/*slot*/*port*]

no port {*shelf*/*slot* | *shelf*/*slot*/*port*} [*shelf*/*slot* | *shelf*/*slot*/*port*]

Syntax Description

slot	All ports on the specified slot. For the Cisco AS5400, slot values range from 0 to 7. Entering a second slot value will specify a range of slots.
slot/*port*	All ports on the specified slot and SPE. For the Cisco AS5400, slot values range from 0 to 7 and port values range from 0 to 107. The slash mark is required. Entering a second slot and SPE value will specify a range of slots.
shelf/*slot*	All ports on the specified shelf and slot. For the Cisco AS5800, shelf values are 0 and 1, and UPC slot values range from 2 to 11. The slash mark is required. Entering a second shelf and slot value will specify a range of slots.
shelf/*slot*/*port*	All ports on the specified SPE. For the Cisco AS5800, shelf values are 0 and 1, slot values range from 2 to 11, and port values range from 0 to 323. The slash marks are required. Entering a second shelf, slot, and SPE value will specify a range of slots.

Command Default

Command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

The **port** command helps you to enter the port configuration mode. The port configuration mode allows you to shut down or put individual ports or ranges of ports in busyout mode.

Examples

The following example shows how to enter port configuration mode on ports 1 to 18 to perform further tasks on the ports:

```
Router(config)# port 1/1 1/18
Router(config-port)# shutdown
```

Related Commands

Command	Description
clear port	Resets the port and clears any active calls to the port.

port modem autotest

To automatically and periodically perform a modem diagnostics test for modems inside the universal gateway or router, use the **port modem autotest** command in global configuration mode. To disable or turn off the modem autotest service, use the **no** form of this command.

port modem autotest {**error** *threshold* | **minimum** *modems* | **time** *hh*:*mm* [*hours*]}

no port modem autotest

Syntax Description

error *threshold*	Maximum modem error threshold. When the system detects this many errors with the modems, the modem diagnostics test is automatically triggered. Specify a threshold count from 3 to 50.
minimum *modems*	Minimum number of modems that will remain untested and available to accept calls during each test cycle. You can specify from 5 to 48 modems. The default is 6 modems on the Cisco AS5400. The range for the Cisco AS5800 is from 73 to 756.
time *hh*:*mm*	Time you want the modem autotest to begin. You must use the military time convention and a required colon (:) between the hours and minutes variables for this feature. For example, 1:30 p.m. is issued as 13:30.
hours	(Optional) Long-range time variable used to set the modem autotest more than one day in advance. The range of hours is from 1 hour to 168 hours. For example, if you want to run the test once per week, issue 168. There are 168 hours in one week.

Command Default

Modem diagnostics tests are disabled.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.1(1)XD	This command was introduced on the Cisco AS5400 as the **port modem autotest** command and replaced the **modem autotest** command for the NextPort dial feature card (DFC) only.
12.1(3)T	This command was implemented on the Cisco AS5400 and Cisco AS5800.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.

Examples

The following example shows how to set the modem autotest to run once per week at 3:00 a.m. Additionally, the autotest activates if the system detects a modem error count higher than 40 errors.

Determine the current time set on the access server with the **show clock** EXEC command. In this example, the time and date set is 3:00 p.m, Monday, January 6, 2003:

```
Router# show clock
*15:00:01.031 EST Jan 06 2003
```

Enter global configuration mode and set the time you want the modem autotest to activate. In this example, the access server is configured to run the modem autotest at 3:00 a.m. and every 168 hours (week) thereafter:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# port modem autotest time 03:00 168
```

Configure the autotest to activate if the system detects a high modem error count. In this example, the autotest activates if the system detects a modem error count higher than 40 errors. For the list of modem errors that are monitored by the **modem autotest** command, see the **show modem call-stats** command.

```
Router(config)# port modem autotest error 40
```

Related Commands

Command	Description
modem autotest	Automatically and periodically performs a modem diagnostics test for modems inside the access server or router.
show clock	Displays the system clock.
show modem	Displays a high-level performance report for all the modems or a single modem inside Cisco AS5200 and Cisco AS5300 access servers.
show modem test	Displays the modem test log.

ppp

To start an asynchronous connection using PPP, use the **ppp** command in EXEC mode.

ppp {**/default** | {*remote-ip-address* | *remote-name*} [@*tacacs-server*]} [**/routing**] **negotiate**

Syntax Description

/default	Makes a PPP connection when a default address has been configured. The slash mark is required.
remote-ip-address	IP address of the client workstation or PC. This parameter can be specified only if the line is set for dynamic addresses using the **async address dynamic** line configuration command.
remote-name	Name of the client workstation or PC. This parameter can be specified if the line is set for dynamic addresses using the **async address dynamic** line configuration command.
@*tacacs-server*	(Optional) IP address or IP host name of the TACACS server to which the user's TACACS authentication request is sent. The at sign is required.
/routing	(Optional) Indicates that the remote system is a router and that routing messages should be exchanged over the link. The line must be configured for asynchronous routing using PPP encapsulation. The slash mark is required.
negotiate	Use PPP negotiated IP address.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When you connect from a remote node computer to an EXEC session on the access server and want to connect from the access server to a device on the network, issue the **ppp** command.

If you specify an address for the TACACS server (either **/default** or @*tacacs-server*), the address must be the first parameter in the command after you type **ppp**. If you do not specify an address or enter the **default keyword**, you are prompted for an IP address or host name. You can enter the **default keyword** at this point.

To terminate a session, disconnect from the device on the network using the command specific to that device. Then, exit from the EXEC by using the **exit** command.

Examples

The following example shows a line that is in asynchronous mode using PPP encapsulation. The name of the computer (ntpc in this example) must be in the Domain Name System (DNS) so that it can be resolved to a real IP address). The computer must be running a terminal emulator program.

```
Router# ppp ntpc@server1
```

ppp accm

To specify the Asynchronous Control Character Map (ACCM) to be negotiated with a mobile station or sent to a peer in PPP outbound requests, use the **ppp accm** command in interface configuration mode. To restore the default state, use the **no** form of this command.

ppp accm *hex-number*

no ppp accm

Syntax Description

hex-number	Specifies the initial value for the ACCM. The value must be a hexadecimal number in the range from 0x0 to 0xFFFFFFFF, where the bit positions from right to left correspond to the characters 0x00 through 0x1F. The default character map (0xA0000) escapes the characters represented by 0x11 (^Q, DC1, and X-on) and 0x13 (^S, DC3, and X-off). **Note** The leading 0x is not necessary when entering the *hex-number* argument , but is accepted by the software.

Command Default

0xA0000.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)XS	This command was introduced.
12.2	This command was integrated into Cisco IOS Release 12.2.

Usage Guidelines

The ACCM is a four octet hexadecimal number that is sent to a peer in a PPP outbound Config-Request packet, informing the peer of which characters need to be escaped during transmission of Asynchronous HDLC (AHDLC) frames containing control characters. The escaped characters set by the **ppp accm** command are useful for allowing data to pass uninterpreted through a network that would normally interpret the control sequences as a command.

For example, the ^Q and ^S characters are software flow control commands used by asynchronous modems to start and stop data transmissions. To allow these characters to be sent as part of a data stream and not be interpreted as control codes by intervening devices, the characters must be escaped, and the **ppp accm** command specifies which characters to use.

The TIA/EIA/IS-835-B requires that the PDSN propose an ACCM of 0x00000000. To be compliant with TIA/EIA/IS-835-B, **ppp accm 00000000** must be configured on the virtual template interface on Cisco PDSN.

The **ppp accm** command is meaningful only on asynchronous interfaces. If entered on other interface types, it will be ignored.

Examples

In the following example, all characters can be transmitted intact to the receiver so that it is not necessary for the transmitter to escape anything:

```
interface async 0
 encapsulation ppp
 ppp accm 0
```

Related Commands

Command	Description
ppp authentication	Specifies CHAP or PAP authentication.

ppp acfc local

To configure high-level data link control (HDLC) address and control field compression (ACFC) options in configuration requests, use the **ppp acfc local** command in interface configuration mode. To return the router to the default for ACFC handling, use the **no** form of this command.

ppp acfc local {**request** | **forbid**}

no ppp acfc local

Syntax Description

request	The ACFC option is included in outbound configuration requests.
forbid	The ACFC option is not sent in outbound configuration requests, and requests from a peer to add the ACFC option are not accepted.

Command Default

ACFC handling is automatically selected based on the type of link, as follows: For asynchronous links, the router responds as if the **request** keyword were selected and the router includes the ACFC option in outbound configuration requests. For synchronous links, the router responds as if the **forbid** keyword were selected and the ACFC option is not sent out in configuration outbound requests and requests from a peer to add the ACFC option are not accepted.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(7)	This command was introduced.
12.2(15)B	This command was integrated into Cisco IOS Release 12.2(15)B.

Usage Guidelines

This command configures ACFC requests in outbound configuration requests. The **ppp acfc local** command allows ACFC handling to be disabled, thus allowing the HDLC framing and the protocol field to remain uncompressed.

Prior to the introduction of the **ppp acfc local** command, negotiation and use of ACFC was entirely dependent upon the link type (synchronous or asynchronous) and was not under the independent control of a system administrator, and this is still the default condition. The **ppp acfc local** command allows the system administrator to control over when PPP negotiates the HDLC ACFC options during initial LCP negotiations, and how the results of the PPP negotiation are applied.

Note Using ACFC can result in minor gains in effective bandwidth because they reduce the amount of framing overhead for each packet. However, using ACFC changes the alignment of the network data in the frame, which in turn can impair the switching efficiency of the packets both at the local and remote ends of the connection. For these reasons, it is generally recommended that ACFC not be enabled without carefully considering the potential results.

Examples

The following example shows how to configure a router to exclude ACFC options from its configuration requests:

```
ppp acfc local forbid
```

Related Commands

Command	Description
ppp acfc remote	Configures the ACFC option in configuration requests received from a remote peer.
ppp pfc remote	Configures the PFC option in configuration requests received from a remote peer.
ppp pfc local	Configures the PFC option in configuration requests.

ppp acfc remote

To configure how high-level data link control (HDLC) address and control field compression (ACFC) options in configuration requests are received from a remote peer, use the **ppp acfc remote** command in interface configuration mode. To return the router to the default for ACFC handling, use the **no** form of this command.

ppp acfc remote {**apply** | **reject** | **ignore**}

no ppp acfc remote

Syntax Description

apply	ACFC options are accepted and ACFC may be performed on frames sent to the remote peer.
reject	ACFC options are explicitly ignored.
ignore	ACFC options are accepted, but ACFC is not performed on frames sent to the remote peer.

Command Default

ACFC handling is automatically selected based on the type of link, as follows: For asynchronous links, the router responds as if the **apply** keyword were selected and the router accepts ACFC options received from a remote peer and may perform ACFC on frames sent to the peer. For synchronous links, the router responds as if the **ignore** keyword were selected and ACFC options received from a remote peer are accepted, but ACFC is not performed on frames sent to the remote peer.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(7)	This command was introduced.
12.2(15)B	This command was integrated into Cisco IOS Release 12.2(15)B.

Usage Guidelines

If ACFC is negotiated during PPP negotiation, Cisco routers may omit the HDLC header on links using HDLC encapsulation. This command allows ACFC handling to be disabled during PPP negotiation, thus allowing the HDLC framing and the protocol field to remain uncompressed.

Prior to the introduction of the **ppp acfc remote** command, negotiation and use of ACFC was entirely dependent upon the link type (synchronous or asynchronous) and was not under the independent control of a system administrator, and this is still the default condition. The **ppp acfc remote** command allows the system administrator control over when PPP negotiates the HDLC ACFC options during initial LCP negotiations, and how the results of the PPP negotiation are applied.

Note Using ACFC can result in minor gains in effective bandwidth because they reduce the amount of framing overhead for each packet. However, using ACFC changes the alignment of the network data in the frame, which in turn can impair the switching efficiency of the packets both at the local and remote ends of the connection. For these reasons, it is generally recommended that ACFC not be enabled without carefully considering the potential results.

Examples

The following example configures ACFC options received from a remote peer to be rejected:

```
ppp acfc remote reject
```

Related Commands

Command	Description
ppp acfc local	Configures the ACFC option in configuration requests.
ppp pfc remote	Configures the PFC option in configuration requests received from a remote peer.
ppp pfc local	Configures the PFC option in configuration requests.

ppp bap call

To set PPP Bandwidth Allocation Protocol (BAP) call parameters, use the **ppp bap call** command in interface configuration mode. To disable processing of a specific type of incoming connection, use the **no** form of this command.

ppp bap call {**accept** | **request** | **timer** *seconds*}

no ppp bap call {**accept** | **request** | **timer**}

Syntax Description

accept	Peer initiates link addition. This is the default.
request	Local side initiates link addition.
timer *seconds*	Number of seconds to wait between call requests the router sends, in the range from 2 to 120 seconds. No default value is set.

Command Default

Peers can initiate the addition of links to a multilink bundle; the timer is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

This command can be included in a virtual interface template for configuring virtual interfaces or can be used to configure a dialer interface.

Examples

The following example configures a dialer interface to accept calls. Accepting calls is the default, but the command is included for the sake of the example.

```
interface dialer 1
 ip unnumbered ethernet 0
 encapsulation ppp
 ppp multilink bap
 ppp bap call accept
 ppp bap link types isdn analog
 dialer load threshold 30
 ppp bap timeout pending 60
```

Related Commands

Command	Description
ppp bap callback	Enables PPP BAP callback and set callback parameters.
ppp bap drop	Sets parameters for removing links from a multilink bundle.
ppp bap link types	Specifies the types of links that can be included in a specific multilink bundle.

ppp bap callback

To enable PPP Bandwidth Allocation Protocol (BAP) callback and set callback parameters, use the **ppp bap callback** command in interface configuration mode. To remove the PPP BAP callback configuration, use the **no** form of this command.

ppp bap callback {**accept** | **request** | **timer** *seconds*}

no ppp bap callback {**accept** | **request** | **timer**}

Syntax Description

accept	Local router initiates link addition upon peer notification.
request	Local router requests that a peer initiate link addition.
timer *seconds*	Number of seconds to wait between callback requests the router sends, in the range from 2 to 120 seconds. Disabled by default.

Command Default

Callback is disabled, and no callback parameters are set. The timer is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Examples

The following example configures a BRI interface for active mode BAP:

```
interface bri 0
 ip unnumbered ethernet 0
 dialer load-threshold 10 either
 dialer map ip 172.21.13.101 name bap-peer 14085778899
 encapsulation ppp
 ppp multilink bap
 ppp bap call request
 ppp bap callback accept
 no ppp bap call accept
 no ppp bap drop accept
 ppp bap pending timeout 30
 ppp bap number default 5664567
 ppp bap number secondary 5664568
```

Related Commands

Command	Description
ppp bap drop	Sets parameters for removing links from a multilink bundle.
ppp bap link types	Specifies the types of links that can be included in a specific multilink bundle.
show ppp bap	Displays the configuration settings and run-time status for a multilink bundle.

ppp bap drop

To set parameters for removing links from a multilink bundle, use the **ppp bap drop** command in interface configuration mode. To disable a specific type of default processing, use the **no** form of this command.

ppp bap drop {**accept** | **after-retries** | **request** | **timer** *seconds*}

no ppp bap drop {**accept** | **after-retries** | **request** | **timer**}

Syntax Description

accept	Peer can initiate link removal. Enabled by default.
after-retries	Local router can remove the link without Bandwidth Allocation Protocol (BAP) negotiation when no response to the drop requests arrives.
request	Local router can initiate removal of a link. Enabled by default.
timer *seconds*	Number of seconds to wait between drop requests sent.

Command Default

accept, **request**: Peers can initiate link removal and this router also can initiate link removal.
no ppp bap drop after-retries: The link is not dropped when there is no response to drop requests.
timer: Disabled, no default value is defined.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

The **no ppp bap drop accept** command disables the router's ability to respond favorably to link drop requests from a peer. However, the router can still remove the link when it receives such requests.

The **no ppp bap drop after-retries** command is the default behavior; the **ppp bap drop after-retries** command must be entered explicitly to be effective.

The **no ppp bap drop request** command disables the router's ability to send link drop requests to a peer. However, the peer can still remove the link on its own behalf; for example, when there is too little traffic to justify keeping the link up.

The **ppp bap max** command specifies the maximum number of requests and retries.

Examples

The following partial example sets a 60-second wait between drop requests:

```
ppp bap drop timer 60
```

Related Commands

Command	Description
ppp bap max	Sets upper limits on the number of retransmissions for PPP BAP.

ppp bap link types

To specify the types of links that can be included in a specific multilink bundle, use the **ppp bap link types** command in interface configuration mode. To remove a type of interface that was previously allowed to be added, use the **no** form of this command.

ppp bap link types [**isdn**] [**analog**]

no ppp bap link types [**isdn**] [**analog**]

Syntax Description

isdn	(Optional) ISDN interfaces can be added to a multilink bundle. This is the default.
analog	(Optional) Asynchronous serial interfaces can be added to a multilink bundle.

Command Default

ISDN interfaces are added to the multilink bundle (**isdn** keyword).

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

The choice of keywords must suit the interfaces configured for Multilink PPP. For example, if you have configured a dialer rotary with only ISDN interfaces, only the **isdn** keyword would be appropriate. If the configuration allows both ISDN and asynchronous interfaces, both **isdn** and **analog** keywords could be used; the multilink bundle could then consist of both ISDN and asynchronous links. Bandwidth Allocation Protocol (BAP) dynamically determines which interfaces are applicable.

Examples

The following example configures a dialer interface for passive mode BAP and for both ISDN and asynchronous serial links:

```
interface dialer 1
 ip unnumbered ethernet 0
 encapsulation ppp
 ppp multilink bap
 ppp bap call accept
 ppp bap link types isdn analog
 dialer load threshold 30
 ppp bap timeout pending 60
```

Related Commands

Command	Description
ppp bap callback	Enables PPP BAP callback and set callback parameters.
show ppp bap	Displays the configuration settings and run-time status for a multilink bundle.

ppp bap max

To set upper limits on the number of retransmissions for PPP Bandwidth Allocation Protocol (BAP), use the **ppp bap max** command in interface configuration mode. To remove any retry limit, use the **no** form of this command.

ppp bap max {**dial-attempts** *number* | **ind-retries** *number* | **req-retries** *number* | **dialers** *number*}

no ppp bap max {**dial-attempts** | **ind-retries** | **req-retries** | **dialers** *number*}

Syntax Description

dial-attempts *number*	Maximum number of dial attempts to any destination number, in the range from 1 to 3. The default is one dial attempt.
ind-retries *number*	Maximum number of retries of a call status indication message, in the range from 1 to 10. The default is three indication retries.
req-retries *number*	Maximum number of retries for a particular request, in the range from 1 to 5. The default is three request retries.
dialers *number*	Maximum number of free dialers logged, in the range from 1 to 10. The default is five free dialers.

Command Default

1 dial attempt
3 indication retries
3 request retries
5 searches for free dialers

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

In compliance with RFC 2125, the **no** form of this command explicitly removes any status indication retry limit and is displayed in the router configuration.

The **ppp bap max dialers** command works in conjunction with the **dialer rotor** and **dialer priority** interface commands**,** which can be used to determine free dialers based upon the priority or the best available. Dialers include all interfaces that are configured under the dialer group leader (the dialer interface itself). The dialer group leader is displayed as the Master Interface in the **show ppp bap group** output.

BAP bases its link type and phone number decisions upon the ordering of the interfaces. This decision is suited to a mixed media environment of both ISDN and analog interfaces, where it may be desirable to choose the ISDN link over the asynchronous or vice versa.

Note that this decision also will limit the number of potential phone numbers that can be included in a CallResponse or CallbackRequest; the maximum number is limited to 20. For example, ten BRI interfaces with two numbers per interface.

Examples

The following partial example accepts the default number of attempts to dial a number and the default number of indication retries, but configures a limit of four times to send requests:

```
ppp bap max req-retries 4
```

Related Commands

Command	Description
dialer priority	Sets the priority of an interface in a dialer rotary group.
dialer rotor	Specifies the method for identifying the outbound line to be used for ISDN or asynchronous DDR calls.
ppp bap drop	Sets parameters for removing links from a multilink bundle.
ppp bap monitor load	Validates peer requests to add or remove links against the current bundle load and the defined dialer load threshold.
ppp bap timeout	Specifies nondefault timeout values for PPP BAP pending actions and responses.
show ppp bap group	Displays the configuration settings and run-time status for a multilink bundle.

ppp bap monitor load

To validate peer requests to add or remove links against the current bundle load and the defined dialer load threshold, use the **ppp bap monitor load** command in interface configuration mode. To specify that incoming link addition requests are not to be subject to the bundle load threshold, use the **no** form of this command.

ppp bap monitor load

no ppp bap monitor load

Syntax Description

This command has no arguments or keywords.

Command Default

Command is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

If the load is being monitored and the incoming peer requests that a link be dropped when the current traffic load is above the dialer load (that is, there is enough traffic to justify the current number of links), the router will not drop the link. In addition, when the traffic falls below the threshold, Bandwidth Allocation Protocol (BAP) tries to drop a link.

The **no** form of this command indicates that incoming peer requests to add a link are not subject to the bundle load threshold. However, other criteria must be met before a favorable response is sent.

Examples

The following partial example configures BAP not to validate peer requests against the current bundle load and the configured dialer load threshold:

```
no ppp bap monitor load
```

Related Commands

Command	Description
dialer load-threshold	Configures bandwidth on demand by setting the maximum load before the dialer places another call to a destination.

ppp bap number

To specify a local telephone number that peers can dial to establish a multilink bundle, use the **ppp bap number** command in interface configuration mode. To remove a previously configured number, use the **no** form of this command.

ppp bap number {**default** *phone-number* | **secondary** *phone-number* | **prefix** *prefix-number* | **format** {**national** | **subscriber**}}

no ppp bap number {**default** *phone-number* | **prefix** *prefix-number* | **format** {**national** | **subscriber**}}

Syntax Description

default *phone-number*	Primary (base) phone number for the interface and the number that can be used for incoming dial calls.
secondary *phone-number*	Telephone number for the second B channel. Applies only to BRI interfaces that have a different number for each B channel or to dialer interfaces that are BRIs.
prefix *prefix-number*	Prefix number for the PPP phone number.
format national | **subscriber**	Format for the primary phone number to be dialed should be either national or subscriber where the number of digits assigned to the number is as follows: • Ten-digit number for a national format. • Seven-digit number for a subscriber format.

Command Default

No base number is provided.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
11.3T	The **prefix** and **format** keywords were added.

Usage Guidelines

Use this command to supply a local default number to be exchanged between peers in order to establish a multilink bundle.

This command is applicable on both the dialer interface and the individual physical interfaces.

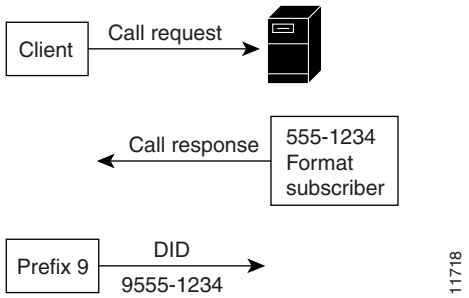
If a peer requests that a number be supplied and no PPP Bandwidth Allocation Protocol (BAP) default number is defined, it might not be possible for the peer to access the interface. However, the peer can access the interface if it has the number already or the number it dialed originally is the same as the number for establishing a Multilink PPP (MLP) bundle.

Note During BAP negotiations between peers, the called party indicates the number to call for BAP if it is different from the number the peer originally dialed. The called party responds with information about the phone number *delta* (the changes to be made in the right-most digits dialed). This information indicates the number of digits that are different from the number originally dialed and what those digits should be.

For example, if the remote peer dialed 5550159876, and the **ppp bap number** command had the default number 5550159912, the local router would respond "3 | 912." In the response, a vertical bar (|) is used to divide the number of digits to change from the number sequence to use instead. In the "3 | 912" response, the local router instructs the calling interface to replace the right-most three digits with "912" for BAP.

This command is used by the client side for dialing instructions when communicating with the server. Use the **prefix** keyword on the Always On/Dynamic ISDN (AO/DI) client side to specify what will precede any number dialed to a multilink peer. For example, the client issues a call request to the server whereby the server issues a call response that includes the dialing number the client should use and the format this number should be in (national or subscriber). The client then dials the number supplied by the server, preceded by any prefix information contained in the **ppp bap number prefix** command. Figure 1 shows an overview about the information exchange between the client and the server.

Figure 1 Client and Server Response Sequence



Use the **format** keyword on the AO/DI server side to specify how many digits should be returned by BAP. BAP will return the numbers based on either a national or subscriber format. The value that is returned is preceded by the prefix before dialing occurs. For example, if the **format national** keywords are configured, then the national format (which is equivalent to ten digits) is returned (during BAP negotiation) from the server.

Note The **ppp bap number prefix** and **ppp bap number format** keyword options cannot be combined to a single-string command line; they must be entered in two separate command strings.

Examples

In the following example, the AO/DI client uses a **ppp bap prefix** value of 9, which indicates that the dialed number of 5550134 will be preceded by a 9. The number that is actually dialed is 95550134. The AO/DI server uses a subscriber format, which indicates that when the client asks the server for the numbers to dial, BAP will return seven digits.

Client Router

```
interface dialer1
 ppp bap number prefix 9
```

Server Router

```
interface dialer1
 ppp bap number format subscriber
 ppp bap number default 5550134
```

In the following example, the AO/DI client uses a **ppp bap prefix** value of 1, which indicates that the dialed number of 5550178 will be preceded by a 1. The number that is actually dialed is 19195550178 because the server is using a national format, and BAP therefore, returns ten digits.

Client Router

```
interface dialer1
 ppp bap number prefix 1
```

Server Router

```
interface dialer1
 ppp bap number format national
 ppp bap number default 9195550178
```

The following example configures a physical interface with both a default number and a secondary number:

```
interface bri 0
 ip unnumbered ethernet 0
 dialer load-threshold 10 either
 dialer map ip 172.21.13.101 name bap-peer 14085550199
 encapsulation ppp
 ppp multilink bap
 ppp bap call request
 ppp bap callback accept
 no ppp bap call accept
 no ppp bap drop accept
 ppp bap pending timeout 30
 ppp bap number default 5550167
 ppp bap number secondary 5550168
```

Related Commands

Command	Description
ppp bap callback	Enables PPP BAP callback and set callback parameters.
show ppp bap	Displays the configuration settings and run-time status for a multilink bundle.

ppp bap timeout

To specify nondefault timeout values for PPP Bandwidth Allocation Protocol (BAP) pending actions and responses, use the **ppp bap timeout** command in interface configuration mode. To reset the response timeout to the default value, or to remove a pending timeout entirely, use the **no** form of this command.

ppp bap timeout {**pending** *seconds* | **response** *seconds*}

no ppp bap timeout {**pending** | **response**}

Syntax Description

pending *seconds*	Number of seconds to wait before timing out pending actions, in the range from 2 to 180 seconds. The default is 20 seconds.
response *seconds*	Number of seconds to wait for a response before timing out, in the range from 2 to 120 seconds. The default is 3 seconds.

Command Default

Enabled
pending: 20 seconds
response: 3 seconds

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

The **no ppp bap timeout response** command resets the timer to the default value.The **no ppp bap timeout pending** command removes the pending-action timeout entirely (in compliance with the BAP specification).

Examples

The following example configures BAP to wait 45 seconds before timing out pending actions:

```
interface dialer 1
 ip unnumbered ethernet 0
 encapsulation ppp
 ppp multilink bap
 ppp bap call accept
 ppp bap link types isdn analog
 dialer load threshold 30
 ppp bap timeout pending 45
```

Related Commands

Command	Description
ppp bap callback	Enables PPP BAP callback and set callback parameters.
ppp bap drop	Sets parameters for removing links from a multilink bundle.
ppp bap max	Sets upper limits on the number of retransmission for PPP BAP.
show ppp bap	Displays the configuration settings and run-time status for a multilink bundle.

ppp bridge appletalk

To enable half-bridging of AppleTalk packets across a serial interface, use the **ppp bridge appletalk** command in interface configuration mode. To disable AppleTalk packet half-bridging, use the **no** form of this command.

ppp bridge appletalk

no ppp bridge appletalk

Syntax Description

This command has no arguments or keywords.

Command Default

Command is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

When you configure a serial or ISDN interface for half-bridging, you configure it to function as a node on an Ethernet subnetwork. It communicates with a bridge on the subnetwork by sending and receiving bridge packets. The serial or ISDN interface converts bridge packets to routed packets and forwards them, as needed.

The serial interface must be configured with an AppleTalk address for communication on the Ethernet subnetwork, and the AppleTalk address must have the same AppleTalk cable range as the bridge.

You cannot configure a serial interface for both half-bridging and for transparent bridging. No more than one half-bridge should be on any subnetwork.

Examples

The following example configures serial interface 0 for half-bridging of AppleTalk. The remote bridge and other Ethernet nodes must be on the same network.

```
interface serial 0
 ppp bridge appletalk
 appletalk cable-range 301-301
 appletalk zone remote-lan
```

Related Commands

Command	Description
appletalk cable-range	Enables an extended AppleTalk network.
appletalk zone	Sets the zone name for the connected AppleTalk network.
ppp bridge ip	Enables half-bridging of IP packets across a serial interface.
ppp bridge ipx	Enables half-bridging of IPX packets across a serial interface.

ppp bridge ip

To enable half-bridging of IP packets across a serial interface, use the **ppp bridge ip** command in interface configuration mode. To disable IP packet half-bridging, use the **no** form of this command.

ppp bridge ip

no ppp bridge ip

Syntax Description

This command has no arguments or keywords.

Command Default

Command is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

When you configure a serial or ISDN interface for half-bridging, you configure it to function as a node on an Ethernet subnetwork. It communicates with a bridge on the subnetwork by sending and receiving bridge packets. The serial interface converts bridge packets to routed packets and forwards them, as needed.

The interface must be configured with an IP address for communication on the Ethernet subnetwork, and the IP address must be on the same subnetwork as the bridge.

You cannot configure a serial interface for both half-bridging and for transparent bridging.

No more than one half-bridge should be on any subnetwork.

Examples

The following example configures serial interface 0 for half-bridging of IP. The remote bridge and other Ethernet nodes must be on the same subnetwork.

```
interface serial 0
 ip address 172.19.5.8
 ppp bridge ip
```

Related Commands

Command	Description
ip address	Sets a primary or secondary IP address for an interface.
ppp bridge appletalk	Enables half-bridging of AppleTalk packets across a serial interfaces.
ppp bridge ipx	Enables half-bridging of IPX packets across a serial interfaces.

ppp bridge ipx

To enable half-bridging of Internetwork Packet Exchange (IPX) packets across a serial interface, use the **ppp bridge ipx** command in interface configuration mode. To return to the default Novell Ethernet_802.3 encapsulation, use the **no** form of this command.

ppp bridge ipx [**novell-ether** | **arpa** | **sap** | **snap**]

no ppp bridge ipx

Syntax Description

novell-ether	(Optional) Novell Ethernet_802.3 encapsulation. This is the default.
arpa	(Optional) Novell Ethernet_II encapsulation.
sap	(Optional) Novell Ethernet_802.2 encapsulation.
snap	(Optional) Novell Ethernet_Snap encapsulation.

Command Default

The default encapsulation is **novell-ether**.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

When you configure a serial interface for half-bridging, you configure it to function as a node on an Ethernet subnetwork. It communicates with a bridge on the subnetwork by sending and receiving bridge packets. The serial interface converts bridge packets to routed packets and forwards them, as needed.

The serial interface must be configured with an IPX address for communication on the Ethernet subnetwork, and the IPX address must be on the same subnetwork as the bridge.

You cannot configure a serial interface for both half-bridging and for transparent bridging.

No more than one half-bridge should be on any subnetwork.

Examples

The following example configures serial interface 0 for half-bridging of IPX. The remote bridge and other Ethernet nodes must be on the same subnetwork.

```
interface serial 0
 ppp bridge ipx
 ipx network 1800
```

Related Commands

Command	Description
ipx network	Enables IPX routing on a particular interface and optionally selects the type of encapsulation (framing).
ppp bridge appletalk	Enables half-bridging of AppleTalk packets across a serial interfaces.
ppp bridge ip	Enables half-bridging of IP packets across a serial interfaces.

ppp callback (DDR)

To enable a dialer interface to function either as a callback client that requests callback or as a callback server that accepts callback requests, use the **ppp callback** command in interface configuration mode. To disable a function, use the **no** form of this command.

ppp callback {**accept** | **permit** | **request**}

no ppp callback

Syntax Description

accept	Dialer interface accepts PPP callback requests (and functions as the PPP callback server).
permit	Dialer interface permits PPP callback (and functions as the PPP callback client).
request	Dialer interface requests PPP callback (and functions as the PPP callback client).

Command Default

Callback requests are neither accepted nor requested.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

An interface can request PPP callback only if the interface is configured for PPP authentication with Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP).

If an interface of the callback server is configured with **ppp callback accept** and the client attempts to cancel the callback and connect, Cisco IOS software will refuse the request and disconnect the client.

If a client is allowed to cancel callbacks and connects, the **ppp callback permit** command must be used instead of the **ppp callback accept** command on the callback server interface.

Examples

The following example configures a previously defined dialer interface to accept PPP callback requests:

```
ppp callback accept
```

Related Commands

Command	Description
dialer callback-secure	Enables callback security.
map-class dialer	Defines a class of shared configuration parameters associated with the **dialer map** command for outgoing calls from an ISDN interface and for PPP callback.
ppp callback (PPP client)	Enables a PPP client to dial in to an asynchronous interface and request a callback.

ppp callback (PPP client)

To enable a PPP client to dial in to an asynchronous interface and request a callback, use the **ppp callback** command in interface configuration mode. To disable callback acceptance, use the **no** form of this command.

ppp callback {**accept** | **initiate**}

no ppp callback

Syntax Description

accept	Accept callback requests from RFC 1570-compliant PPP clients on the interface.
initiate	Initiate a callback to non-RFC 1570-compliant PPP clients dialing in to an asynchronous interface.

Command Default

Callback requests are not accepted on asynchronous interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

PPP callback can be initiated only if the interface is configured for authentication using CHAP or PAP.

Examples

The following example accepts a callback request from an RFC-compliant PPP client:

```
ppp callback accept
```

The following example accepts a callback request from a non-RFC-compliant PPP client:

```
ppp callback initiate
```

Related Commands

Command	Description
arap callback	Enables an ARA client to request a callback from an ARA client.
autoselect ppp	Configures a line to start a SLIP session.
call progress tone country	Forces the Cisco IOS software to wait before initiating a callback to a requesting client.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.

Command	Description
ppp callback (DDR)	Enables a dialer interface to function either as a callback client that requests callback or as a callback server that accepts callback requests.
username	Establishes a username-based authentication system, such as PPP CHAP and PAP.

ppp caller name

To set the caller option when no Calling Line Identification (CLID) is available, use the **ppp caller name** command in interface configuration mode. To remove the name, use the **no** form of this command.

ppp caller name *name*

no ppp caller name *name*

Syntax Description

name	Username string for this call.

Command Default

Command is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.2T	This command was introduced.

Usage Guidelines

This command sets the username used when the CLID is not available. This username is used only in the case where the **ppp dnis** command is configured and the CLID is not available.

Examples

The following example shows how to configure a call to user1:

```
interface Serial0:15
 description "PRI D channel"
 ip unnumbered Loopback0
 encapsulation ppp
 no keepalive
 dialer pool-member 1 max-link 1
 isdn switch-type primary-net5
 isdn incoming-voice modem
 no fair-queue
 no cdp enable
 ppp caller name user1
 ppp authentication pap chap callin USERS&TUNNELS
 ppp chap hostname osh
```

Related Commands

Command	Description
ppp dnis	Sets the DNIS string for a PPP call.

ppp direction

To override the default direction of a PPP connection, use the **ppp direction** command in interface configuration mode. To disable an override setting, use the **no** form of this command.

ppp direction {**callin** | **callout** | **dedicated**}

no ppp direction {**callin** | **callout** | **dedicated**}

Syntax Description

callin	Treat the connection as a received call.
callout	Treat the connection as an initiated call.
dedicated	Treat the connection as a dedicated call.

Defaults

Disabled (no direction configured)

Command Modes

Interface configuration

Command History

Release	Modification
12.2T	This command was introduced.

Usage Guidelines

The **ppp direction** command is useful when a router is connected to an interface type where there is either no inherent call direction, such as with a back-to-back or leased-line connection, or where an external dial device such as a CSU/DSU or an ISDN terminal adapter is connected to the interface.

The configured call direction will always override the automatically detected direction, even on dial interfaces where the true direction is known.

The call direction is used mainly internally by PPP authentication, as follows:

- If doing bidirectional authentication, PPP will wait to send its authentication credentials to the peer if the direction is call-in, and the **no ppp chap wait**, **no ppp pap wait**, or **no ppp eap wait** commands are not configured.
- PPP uses the call direction internally to detect spoofed Challenge Handshake Authentication Protocol (CHAP) sessions.
- If the direction is call-in, PPP requires that the remote names used in a peer's CHAP challenge and CHAP response be the same.

The call direction is also used for callback processing.

Typically, you will not need to configure this command. If you do, you should configure the opposite of the command on the other side of the link, so one side is call-out and one side is call-in.

Examples

The following example determines the call direction on a back-to-back serial connection:

```
interface Serial2/0
 ip address 192.168.1.131 255.255.255.0
 encapsulation ppp
 peer default ip address pool local local_pool
 serial restart-delay 0
 ppp authentication chap
 ppp direction callin
```

Related Commands

Command	Description
ppp chap wait	Configures the router to delay the CHAP authentication until after the peer has authenticated itself to the router.
ppp eap wait	Configures the router to delay the EAP authentication until after the peer has authenticated itself to the server.
ppp pap wait	Configures the router to delay the PAP authentication until after the peer has authenticated itself to the router.

ppp dnis

To configure a set of dialed number identification service (DNIS) numbers to check an incoming call against to automatically authenticate and authorize a user, use the **ppp dnis** command in interface configuration mode. To remove the numbers, use the **no** form of this command.

ppp dnis *DNIS-number* [*DNIS-number*] [*DNIS-number...*]

no ppp dnis

Syntax Description

DNIS-number	Specifies the DNIS number that will be checked when a call comes in. Multiple DNIS numbers can be entered seperated by spaces.

Command Default

This command is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.2T	This command was introduced.

Usage Guidelines

This command enables a method of authenticating and authorizing a user based on the DNIS. The DNIS is the number dialed by the user. If the dialed number for this session matches one of the numbers configured in the **ppp dnis** command, the user is automatically authenticated and authorized for the session. Any other configured PPP authentication is not performed. In the case of DNIS authentication, the Calling Line Identification (CLID) is used as the username. If the CLID is unavailable, the username is the name configured with the **ppp caller name** command. If neither the CLID nor a caller name is configured, the username will automatically be set to “no-clid.”

Examples

The following example shows how to set the DNIS for a call:

```
interface Serial0:15
 description "PRI D channel"
 ip unnumbered Loopback0
 encapsulation ppp
 no keepalive
 dialer pool-member 1 max-link 1
 isdn switch-type primary-net5
 isdn incoming-voice modem
 no fair-queue
 no cdp enable
 ppp dnis 13693 132
 ppp authentication pap chap callin USERS&TUNNELS
 ppp chap hostname osh
```

Related Commands

Command	Description
ppp caller name	Sets the caller option when no CLID is available.

ppp encrypt mppe

To enable Microsoft Point-to-Point Encryption (MPPE) on the virtual template, use the **ppp encrypt mppe** command in interface configuration mode. To disable MPPE, use the **no** form of this command.

ppp encrypt mppe {**auto** | **40** | **128**} [**passive** | **required**] [**stateful**]

no ppp encrypt mppe

Syntax Description

auto	All available encryption strengths are allowed.
40	Only 40-bit encryption is allowed.
128	Only 128-bit encryption is allowed.
passive	(Optional) MPPE will not offer encryption, but will negotiate if the other tunnel endpoint requests encryption.
required	(Optional) MPPE must be negotiated, or the connection will be terminated.
stateful	(Optional) MPPE will negotiate only stateful encryption. If the **stateful** keyword is not used, MPPE will first attempt to negotiate stateless encryption, but will allow stateful mode if the other tunnel endpoint requests it.

Command Default

MPPE encryption is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)XE5	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.4(5)	This command was modified to explicitly disallow interleaving.

Usage Guidelines

PPP encapsulation must be enabled before you can use the **ppp encrypt mppe** command.

All of the configurable MPPE options must be identical on both tunnel endpoints.

The **auto** keyword is offered only on 128-bit images.

Note The **ppp authentication ms-chap** command must be added to the interface that will carry Point-to-Point Tunnel Protocol (PPTP)-MPPE traffic. All Windows clients using MPPE need the Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) application. This is a Microsoft design requirement.

Stateful encryption is not appropriate for links that have high loss rates because the state information is updated with each packet received, but cannot be updated correctly for packets that are not received. Losing a packet means loss of state (transmissions are no longer synchronous). Losing state triggers expensive resynchronization mechanisms, and more packets will be lost during the recovery period. Any link that experiences more than the occasional random drop is therefore unsuitable for stateful

encryption mechanisms. The same is also true for stateful compressions. For this reason, stateful encryption may not be appropriate for lossy network environments such as Layer 2 tunnels on the Internet.

The interleaving of packets among fragments of larger packets on a Multilink PPP (MLP) bundle (enabled with the **ppp multilink interleave** command) is not supported with this command.

Examples

The following example shows a virtual template configured to perform 40-bit MPPE encryption:

```
interface Virtual-Template1
 ip unnumbered FastEthernet0/0
 no ip directed-broadcast
 ip mroute-cache
 no keepalive
 ppp encrypt mppe 40
 ppp authentication ms-chap
```

Related Commands

Command	Description
encryption mppe	Enables MPPE encryption on the ISA card.
interface virtual-template	Creates a virtual template interface.
ppp authentication	Enables CHAP, PAP, MS-CHAP, or a combination of methods and specifies the order in which the authentication methods are selected on the interface.
ppp multilink interleave	Enables interleaving of packets among the fragments of larger packets on an MLP bundle.

ppp hold-queue

To specify the maximum number of packets to be queued to the PPP process across all interfaces, use the **ppp hold-queue** command in global configuration mode. To restore the default values, use the **no** form of this command.

ppp hold-queue *length*

no ppp hold-queue

Syntax Description

length	The number of packets to be queued. Values are from 1 to 1000000.

Command Default

The default length depends on the platform. That is, the default length is twice the maximum number of PPP-supported interfaces on that platform.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

The exact value of the packets queued depends on the number of PPP sessions supported. The default value works in most cases. It is not recommended to set a different value unless your Cisco technical support representative directs you to do so for deployment-specific tuning purposes.

The command specifies that only packets that are actually queued are counted; packets that are discarded at interrupt because they do not pass various checks are not counted. Preprocessed packets are also not counted. Any type of packet queued to the PPP process is counted.

Examples

The following example shows how to specify the maximum number of packets to be queued to the PPP process:

```
Router(config)# ppp hold-queue 64000
```

ppp ipcp

To configure PPP IP Control Protocol (IPCP) features such as the ability to provide primary and secondary Domain Name Server (DNS) and Windows Internet Naming Service (WINS) server addresses, and the ability to accept any address requested by a peer, use the **ppp ipcp** command in template or interface configuration mode. To disable a **ppp ipcp** feature, use the **no** form of this command.

ppp ipcp {**accept-address** | **address** {**accept** | **required** | **unique**} | **dns** {*primary-ip-address* [*secondary-ip-address*] [**aaa**] [**accept**] | **accept** | **reject** | **request** [**accept**]} | **header-compression ack** | **ignore-map** | **mask** {*subnet-mask* | **reject** | **request**} | **username unique** | **wins** {*primary-ip-address* [*secondary-ip-address*] [**aaa**] [**accept**] | **accept** | **reject** | **request** [**accept**]}}

no ppp ipcp {**accept-address** | **address** {**accept** | **required** | **unique**} | **dns** | **header-compression ack** | **ignore-map** | **mask** | **predictive** | **username unique** | **wins**}

Syntax Description

accept-address	Accepts any nonzero IP address from the peer.
address	Specifies IPCP IP address options: • **accept**—Accepts any nonzero IP address from the peer. • **required**—Disconnects the peer if no IP address is negotiated. • **unique**—Disconnects the peer if the IP address is already in use.
dns	Specifies DNS options: • *primary-ip-address*—IP address of the primary DNS server. – *secondary-ip-address*—(Optional) IP address of the secondary DNS server. – **aaa**—(Optional) Use DNS data from the AAA server. – **accept**—(Optional) Specifies that any nonzero DNS address will be accepted. • **accept**—Specifies that any nonzero DNS address will be accepted. • **reject**—Reject the IPCP option if received from the peer. • **request**—Request the DNS address from the peer.
header-compression ack	Enables IPCP header compression.
ignore-map	Ignores dialer map when negotiating peer IP address.
mask	Specifies IP address mask options: • *subnet-mask*—Specifies the subnet mask to offer the peer. • **reject**—Reject subnet mask negotiations. • **request**—Request the subnet mask from the peer.

username unique	Ignores a common username when providing an IP address to the peer.
wins	Specifies WINS options: • *primary-ip-address*—IP address of the primary WINS server. – *secondary-ip-address*—(Optional) IP address of the secondary WINS server. – **aaa**—(Optional) Use WINS data from the AAA server. – **accept**—(Optional) Specifies that any nonzero WINS address will be accepted. • **accept**—Specifies that any nonzero WINS address will be accepted. • **reject**—Reject the IPCP option if received from the peer. • **request**—Request the WINS address from the peer.

Command Default

No servers are configured, and no address request is made.

Command Modes

Template configuration
Interface configuration

Command History

Release	Modification
12.0(6)T	This command was introduced.
12.1(5)T	The **reject** and **accept** keywords were added.

Examples

The following examples show use of the **ppp ipcp** command:

```
ppp ipcp accept-address

ppp ipcp dns 10.1.1.3

ppp ipcp dns 10.1.1.3 10.1.1.4

ppp ipcp dns 10.1.1.1 10.1.1.2 accept

ppp ipcp dns accept

ppp ipcp dns reject

ppp ipcp ignore-map

ppp ipcp username unique

ppp ipcp wins 10.1.1.1 10.1.1.2

ppp ipcp wins accept
```

The following examples show how to use the **no** form of the **ppp ipcp** command:

```
no ppp ipcp wins

no ppp ipcp ignore-map
```

Related Commands

Command	Description
debug ppp	Displays information on traffic and exchanges in an internetwork implementing the PPP.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show ip interfaces	Displays the usability status of interfaces configured for IP.

ppp ipcp default route

To configure a default route through a PPP virtual access interface, use the **ppp ipcp default route** command in interface configuration mode. To disable a default route for a PPP virtual access interface, use the **no** form of this command.

ppp ipcp default route

no ppp ipcp default route

Syntax Description

This command has no arguments or keywords.

Command Default

No default route

Command Modes

Interface configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

This command allows a PPP virtual template to dynamically add a default route pointing to the virtual access interface created by the virtual template.

A customer premises equipment (CPE) router with PPP over an ATM or Frame Relay connection can access the Internet without turning on any other routing.

Examples

The following example shows how to configure the PPP default route on the virtual access interface:

```
interface virtual-template 1
 ip address negotiated
 ppp ipcp default route
```

Related Commands

Command	Description
debug ppp negotiation	Displays information on traffic and exchanges in an internetwork implementing PPP.

ppp ipcp predictive

To set the PPP Internet Protocol Control Protocol (IPCP) to a predictive state that reduces negotiation time by predicting responses from peers and sending expected reply and request packets in advance, use the **ppp ipcp predictive** command in interface configuration mode. To disable the IPCP predictive state, use the **no** form of this command.

ppp ipcp predictive

no ppp ipcp predictive

Syntax Description

This command has no arguments or keywords.

Command Default

The PPP IPCP is not set to a predictive state.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300, Cisco AS5400 and Cisco AS5800.

Usage Guidelines

The **ppp ipcp predictive** command is useful in networks that accept connections from devices that require a reduction in the IPCP negotiation cycle time. This command reduces the amount of time needed for PPP to negotiate with the peer so that connections can be made in an acceptable amount of time. The following changes to the IPCP negotiation strategy make this time reduction possible:

- Send an IPCP Configure-Ack packet after sending an IPCP Configure-Nak packet.
- Send IPCP Configure-Nak and Configure-Ack packets after rejecting certain configuration options.

These changes can reduce connection delay by approximately 40 percent.

Note Any Configure-Request packet received in the Open state is ignored until the software receives Configure-Request packets with identifying numbers greater than what was last acknowledged, in which case the software disables the predictive mode and processes the Configure-Request packet using normal IPCP negotiation operations.

The **ppp ipcp predictive** command is configured on group asynchronous and dialer interfaces running PPP or Multilink PPP.

Examples

The following example sets the link control protocol (LCP) and IPCP to predictive states on a group asynchronous interface:

```
interface group-async 1
 ip unnumbered loopback 0
 encapsulation ppp
 no ip mroute-cache
 dialer in-band
 dialer pool-member 1
 async dynamic address
 async dynamic routing
 async mode dedicated
 no fair-queue
 ppp lcp predictive
 ppp ipcp predictive
 group-range 1 48
 hold-queue 75 in
```

Related Commands

Command	Description
interface dialer	Defines a dialer rotary group.
interface group-async	Creates a group interface that will serve as master, to which asynchronous interfaces can be associated as members.
ppp lcp predictive	Sets LCP to a predictive state that reduces negotiation time by predicting responses from peers and sending expected reply and request packets in advance.

ppp iphc max-header

To set the maximum size of the largest IP header that may be compressed when configuring Internet Protocol Header Compression (IPHC) control options over PPP, use the **ppp iphc max-header** command in interface configuration mode. To change the configuration, use the **no** form of this command.

ppp iphc max-header *bytes*

no ppp iphc max-header *bytes*

Syntax Description

bytes	Maximum size, in bytes, of the largest IP header that may be compressed. The range is from 60 to 168 bytes, and the default is 168 bytes.

Command Default

168 bytes

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

There are two types of IP header compression used over PPP: Van Jacobsen header compression defined in RFC 1332 and enabled with the **ip tcp header-compression** command, and IPHC defined in RFC 2509 and enabled with the **ip rtp header-compression** command. The **ppp iphc** set of commands controls parameters that pertain to the form of IPHC described in RFC 2509.

The IPHC specification allows low speed links to run more efficiently by reducing the size of the IP headers as transmitted on the link. IPHC supports compressed Real-Time Transport Protocol (cRTP), compressed User Datagram Protocol (cUDP), and compressed Transaction Control Protocol (cTCP).

An IPHC-enabled interface sends only changes to the header instead of sending the entire header with every packet. At the beginning of a transmission, the transmitting end (the compressor) sends a full header packet to the receiving end (the decompressor). After the initial packet is sent, the compressor sends all other packets with headers that contain only the differences between them and the original full header. The decompressor maintains a copy of the original full header and reconstructs all the other packet headers by adding the changes to them.

The header data that is different with each packet is referred to as the session state, and is identified by a session ID or connection ID.

When the decompressor receives a compressed packet, it reconstructs the packet header by adding the difference to the saved uncompressed header. Typically, IPHC enables the header to be compressed to two bytes (four bytes if UDP checksums are used).

The following fields in a packet header usually remain the same throughout a transmission:

- IP source and destination addresses
- UDP and TCP source and destination ports
- RTP synchronization source (SSRC) fields

The following fields in a packet header usually change during a transmission:

- IP packet ID
- Checksum
- Sequence number
- RTP time stamp
- The RTP marker bit

Examples

The following example shows how to change the maximum size of the largest IP header that may be compressed from the default of 168 bytes to 114 bytes:

```
interface Multilink1
 ip address 10.100.253.1 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 ip tcp header-compression iphc-format
 no ip mroute-cache
 fair-queue 64 256 1000
 no cdp enable
 ppp multilink
 ppp multilink fragment-delay 20
 ppp multilink interleave
 multilink-group 1
 ip rtp header-compression iphc-format
 ip rtp priority 16384 50 64
 ppp iphc max-header 114
 ppp iphc max-time 10
 ppp iphc max-period 512
```

Related Commands

Command	Description
ip rtp header-compression	Enables TCP, UDP, and RTP (RFC 2509) header compression.
ip tcp header-compression	Enables TCP (RFC 1332) header compression.
ppp iphc max-period	Sets the maximum number of compressed packets that can be sent before a full header when configuring IPHC control options over PPP.
ppp iphc max-time	Sets the maximum time allowed between full headers when configuring IPHC control options over PPP.

ppp lcp delay

To configure the link control protocol (LCP) delay timer for initiating LCP negotiations after a link connects and to configure the router to discard incoming setup requests until the LCP delay timer expires, use the **ppp lcp delay** command in interface configuration mode. To disable the LCP delay timer, use the **no** form of this command.

ppp lcp delay *seconds* [*milliseconds*] [**random** *max-delay-seconds*] [**discard**]

no ppp lcp delay

Syntax Description

seconds	Delay, in seconds, before initiating LCP negotiations. Valid values for the *seconds* argument range from 0 to 255. The default value is 2 seconds.
milliseconds	(Optional) Delay, in milliseconds (ms), before initiating LCP negotiations. Valid values for the *milliseconds* argument range from 0 to 999. The default value is 0 ms.
random *max-delay-seconds*	(Optional) Specifies that a random amount of additional time will be added to the configured LCP delay timer. The additional amount of time will not exceed the number of seconds specified with the *max-delay-seconds* argument. Valid values for *max-delay-seconds* range from 1 to 255. Random delay is disabled by default.
discard	(Optional) Specifies that incoming configuration requests (CONFREQs) will be discarded until the LCP delay timer has expired. CONFREQs are not discarded by default.

Command Default

No LCP delay timer is configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T. The *milliseconds* argument was added.
12.3(11)YS	This command was integrated into Cisco IOS Release 12.3(11)YS. The **random** *max-delay-seconds* and **discard** keywords and argument were added.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Configure an LCP delay timer to allow the peer device a short amount of time to send the first packet after the PPP link comes up. If the LCP delay timer expires before a CONFREQ is received from the peer, the router can initiate LCP negotiations.

The LCP delay timer is applied only to incoming connections. PPP does not delay for outbound connections or connections where PPP cannot determine a direction.

Use the **random** *max-delay-seconds* keyword and argument combination to add a random amount of time to the LCP delay timer. Setting a random delay on the initiation of LCP negotiations prevents overload when many PPP links come up at the same time.

Use the **discard** keyword to specify that incoming CONFREQs should be discarded until the configured delay has expired. LCP negotiations will not be initiated until the LCP delay timer has expired.

Examples

The following example shows how to configure an LCP delay timer of 4 seconds. If a CONFREQ is not received before the LCP delay timer expires, LCP negotiations can be initiated by either peer.

```
Router(config-if)# ppp lcp delay 4
```

The following example shows how to configure an LCP delay timer that will expire at a random time between 5 and 15 seconds after the link comes up. If a CONFREQ is not received before the LCP delay timer expires, LCP negotiations can be initiated by either peer.

```
Router(config-if)# ppp lcp delay 5 random 10
```

The following example shows how to configure an LCP delay timer of 3.25 seconds and specifies that incoming CONFREQs will be discarded until the LCP delay timer has expired. After 3.25 seconds, LCP negotiations can be initiated by either peer.

```
Router(config-if)# ppp lcp delay 3 250 discard
```

The following example shows how to configure an LCP delay timer that will expire at a random time between 10 and 15 seconds after the link comes up, and specifies that incoming CONFREQs will be discarded until the LCP delay timer has expired. After the LCP delay timer expires, negotiations can be initiated by either peer.

```
Router(config-if)# ppp lcp delay 10 random 5 discard
```

Related Commands

Command	Description
debug ppp multilink negotiation	Displays information about events affecting multilink groups controlled by BACP.
show ppp multilink	Displays bundle information for MLP bundles.

ppp iphc max-period

To set the maximum number of compressed packets that can be sent before a full header when configuring Internet Protocol Header Compression (IPHC) control options over PPP, use the **ppp iphc max-period** command in interface configuration mode. To change the configuration, use the **no** form of this command.

ppp iphc max-period *packets*

no ppp iphc max-period *packets*

Syntax Description

packets	Maximum number of compressed packets that can be sent before a full header. The range is from 1 to 65,535 packets, and the default is 256 packets.

Command Default

256 packets

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

There are two types of IP header compression used over PPP: Van Jacobsen header compression, which is defined in RFC 1332, and a newer compression type described in RFC 2509. The **ppp iphc** set of commands controls parameters that pertain to the form of IPHC described in RFC 2509.

The IPHC specification allows low speed links to run more efficiently when IP headers are extremely large. IPHC supports compressed Real-Time Transport Protocol (cRTP), compressed User Datagram Protocol (cUDP), and compressed Transaction Control Protocol (cTCP).

An IPHC-enabled interface sends only changes to the header instead of sending the entire header with every packet. At the beginning of a transmission, the transmitting end (the compressor) sends a full header packet to the receiving end (the decompressor). After the initial packet is sent, the compressor sends all other packets with headers that contain only the differences between them and the original full header. The decompressor maintains a copy of the original full header and reconstructs all the other packet headers by adding the changes to them.

The header data that is different with each packet is referred to as the session state, and is identified by a session ID or connection ID.

When the decompressor receives a compressed packet, it reconstructs the packet header by adding the difference to the saved uncompressed header. Typically, IPHC enables the header to be compressed to two bytes (four bytes if UDP checksums are used).

The following fields in a packet header usually remain the same throughout a transmission:

- IP source and destination addresses
- UDP and TCP source and destination ports
- RTP synchronization source (SSRC) fields

The following fields in a packet header usually change during a transmission:

- IP packet ID
- Checksum
- Sequence number
- RTP time stamp
- RTP marker bit

The **ppp iphc max-period** command is specifically related to an IPHC frame format known as *compressed_non_TCP*. The recovery of lost compressed_non_TCP frames on lossy links is much improved by allowing more full headers to flow and by configuring less compression.

Examples

The following example shows how to increase the maximum number of compressed packets that can be sent before a full header from 256 to 512 packets when configuring IPHC control options over PPP:

```
interface Multilink1
 ip address 10.100.253.1 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 ip tcp header-compression iphc-format
 no ip mroute-cache
 fair-queue 64 256 1000
 no cdp enable
 ppp multilink
 ppp multilink fragment-delay 20
 ppp multilink interleave
 multilink-group 1
 ip rtp header-compression iphc-format
 ip rtp priority 16384 50 64
 ppp iphc max-header 114
 ppp iphc max-time 10
 ppp iphc max-period 512
```

Related Commands

Command	Description
ip rtp header-compression	Enables TCP, UDP, and RTP (RFC 2509) header compression.
ip tcp header-compression	Enables TCP (RFC 1332) header compression.
ppp iphc max-header	Sets the maximum size of the largest IP header that may be compressed when configuring IPHC control options over PPP.
ppp iphc max-time	Sets the maximum number of compressed packets that can be sent before a full header when configuring IPHC control options over PPP.

ppp iphc max-time

To set the maximum time allowed between full headers when configuring Internet Protocol Header Compression (IPHC) control options over PPP, use the **ppp iphc max-time** command in interface configuration mode. To change the configuration, use the **no** form of this command.

ppp iphc max-time *seconds*

no ppp iphc max-time *seconds*

Syntax Description

seconds	Maximum time, in seconds, allowed between full headers. The range is from 1 to 255 seconds, and the default is 5 seconds.

Command Default

5 seconds

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

There are two forms of IP header compression used over PPP: Van Jacobsen header compression, which is defined in RFC 1332, and a newer form of compression described in RFC 2509. The **ppp iphc** set of commands controls parameters that pertain to the form of IPHC described in RFC 2509.

The IPHC specification allows low speed links to run more efficiently by reducing the size of IP headers as transmitted on the link. IPHC supports compressed Real-Time Transport Protocol (cRTP), compressed User Datagram Protocol (cUDP), and compressed Transaction Control Protocol (cTCP).

An IPHC-enabled interface sends only changes to the header instead of sending the entire header with every packet. At the beginning of a transmission, the transmitting end (the compressor) sends a full header packet to the receiving end (the decompressor). After the initial packet is sent, the compressor sends all other packets with headers that contain only the differences between them and the original full header. The decompressor maintains a copy of the original full header and reconstructs all the other packet headers by adding the changes to them.

The header data that is different with each packet is referred to as the session state, and is identified by a session ID or connection ID.

When the decompressor receives a compressed packet, it reconstructs the packet header by adding the difference to the saved uncompressed header. Typically, IPHC enables the header to be compressed to two bytes (four bytes if UDP checksums are used).

The following fields in a packet header usually remain the same throughout a transmission:

- IP source and destination addresses
- UDP and TCP source and destination ports
- RTP synchronization source (SSRC) fields

The following fields in a packet header usually change during a transmission:

- IP packet ID
- Checksum
- Sequence number
- RTP time stamp
- RTP marker bit

The **ppp iphc max-time** command is specifically related to an IPHC frame format known as *compressed_non_TCP*. The recovery of lost compressed_non_TCP frames on lossy links is much improved by allowing more full headers to flow and by configuring less compression.

Examples

The following example shows how to change the number of compressed packets that can be sent before a full header from the default 5 seconds to 10 seconds:

```
interface Multilink1
 ip address 10.100.253.1 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 ip tcp header-compression iphc-format
 no ip mroute-cache
 fair-queue 64 256 1000
 no cdp enable
 ppp multilink
 ppp multilink fragment-delay 20
 ppp multilink interleave
 multilink-group 1
 ip rtp header-compression iphc-format
 ip rtp priority 16384 50 64
 ppp iphc max-header 114
 ppp iphc max-time 10
 ppp iphc max-period 512
```

Related Commands

Command	Description
ip rtp header-compression	Enables TCP, UDP, and RTP (RFC 2509) header compression.
ip tcp header-compression	Enables TCP (RFC 1332) header compression.
ppp iphc max-header	Sets the maximum size of the largest IP header that may be compressed when configuring IPHC control options over PPP.
ppp iphc max-period	Sets the maximum number of compressed packets that can be sent before a full header when configuring IPHC control options over PPP.

ppp lcp delay

To configure the link control protocol (LCP) delay timer for initiating LCP negotiations after a link connects and to configure the router to discard incoming setup requests until the LCP delay timer expires, use the **ppp lcp delay** command in interface configuration mode. To disable the LCP delay timer, use the **no** form of this command.

ppp lcp delay *seconds* [*milliseconds*] [**random** *max-delay-seconds*] [**discard**]

no ppp lcp delay

Syntax Description

seconds	Delay, in seconds, before initiating LCP negotiations. Valid values for the *seconds* argument range from 0 to 255. The default value is 2 seconds.
milliseconds	(Optional) Delay, in milliseconds, before initiating LCP negotiations. Valid values for the *milliseconds* argument range from 0 to 999. The default value is 0 milliseconds.
random *max-delay-seconds*	(Optional) Specifies that a random amount of additional time will be added to the configured LCP delay timer. The additional amount of time will not exceed the number of seconds specified with the *max-delay-seconds* argument. Valid values for *max-delay-seconds* range from 1 to 255. Random delay is disabled by default.
discard	(Optional) Specifies that incoming configuration requests (CONFREQs) will be discarded until the LCP delay timer has expired. CONFREQs are not discarded by default.

Command Default

No LCP delay timer is configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.1	This command was introduced.
12.2(13)T	Support for the *milliseconds* argument was added to this command.
12.3(11)YS	Support for the **random** *max-delay-seconds* and **discard** keywords and argument was added to this command.

Usage Guidelines

Configure an LCP delay timer to allow the peer device a short amount of time to send the first packet after the PPP link comes up. If the LCP delay timer expires before a CONFREQ is received from the peer, the router can initiate LCP negotiations.

The LCP delay timer is applied only to incoming connections. PPP does not delay for outbound connections or connections where PPP cannot determine a direction.

Use the **random** *max-delay-seconds* keyword and argument combination add a random amount of time to the LCP delay timer. Setting a random delay on the initiation of LCP negotiations prevents overload when many PPP links come up at the same time.

Use the **discard** keyword to specify that incoming CONFREQs should be discarded until the configured delay has expired. LCP negotiations will not be initiated until the LCP delay timer has expired.

Examples

The following example configures an LCP delay timer of 4 seconds. If a CONFREQ is not received before the LCP delay timer expires, LCP negotiations can be initiated by either peer.

```
ppp lcp delay 4
```

The following example configures an LCP delay timer that will expire at a random time between 5 and 15 seconds after the link comes up. If a CONFREQ is not received before the LCP delay timer expires, LCP negotiations can be initiated by either peer.

```
ppp lcp delay 5 random 10
```

The following example configures an LCP delay timer of 3.25 seconds and specifies that incoming CONFREQs will be discarded until the LCP delay timer has expired. After 3.25 seconds, LCP negotiations can be initiated by either peer.

```
ppp lcp delay 3 250 discard
```

The following example configures an LCP delay timer that will expire at a random time between 10 and 15 seconds after the link comes up, and specifies that incoming CONFREQs will be discarded until the LCP delay timer has expired. After the LCP delay timer expires, negotiations can be initiated by either peer.

```
ppp lcp delay 10 random 5 discard
```

ppp lcp fast-start

To allow a PPP interface to respond immediately to incoming packets once a connection is established, use the **ppp lcp fast-start** command in interface configuration mode. To specify that PPP delay before responding, use the **no** form of this command.

ppp lcp fast-start

no ppp lcp fast-start

Syntax Description

This command has no arguments or keywords.

Command Default

Command is enabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

Some systems, typically those with external modems, may have problems with slow or electrically noisy hardware. If the **no ppp lcp fast-start** command is specified, PPP starts a debounce timer and waits for it to expire before attempting to communicate with the peer system, thereby reducing the probability of a false start on the interface.

If the **no ppp lcp fast-start** command is not specified, PPP will not use a debounce timer and will respond immediately to incoming packets once a connection is made.

The default fast start enabled state should not be disabled unless there is a problem with slow or electronically noisy hardware. This setting prevents PPP from waiting for a debounce timer to expire before responding to inbound frames.

Examples

The following example disables fast start:

```
no ppp lcp fast-start
```

ppp lcp predictive

To set the PPP link control protocol (LCP) to a predictive state that reduces negotiation time by predicting responses from peers and sending expected reply and request packets in advance, use the **ppp lcp predictive** command in interface configuration mode. To disable the LCP predictive state, use the **no** form of this command.

ppp lcp predictive

no ppp lcp predictive

Syntax Description

This command has no arguments or keywords.

Command Default

The PPP LCP is not set to a predictive state.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300, Cisco AS5400 and Cisco AS5800.

Usage Guidelines

The **ppp lcp predictive** command is useful in networks that accept connections from devices that require a reduction in the LCP negotiation cycle time. This command reduces the amount of time needed for PPP to negotiate with the peer so that connections can be made in an acceptable amount of time. The following changes to the LCP negotiation strategy make this time reduction possible:

- Send an LCP Configure-Ack packet, then send the next-level LCP Configure-Request packet before receiving acknowledgment for the PPP Configure-Request packet.
- Send an LCP Configure-Ack packet after sending LCP Configure-Reject and Configure-Nak packets for certain configuration options.

These changes can reduce connection delay by approximately 40 percent.

The **ppp lcp predictive** command is configured on group asynchronous and dialer interfaces running PPP or Multilink PPP.

Examples

The following example sets LCP and Internet Protocol Control Protocol (IPCP) to predictive states on a dialer interface:

```
!
interface dialer 1
 ip unnumbered loopback 0
 encapsulation ppp
 dialer pool 1
 dialer idle-timeout 120000
```

```
dialer enable-timeout 6
dialer-group 1
peer default ip address pool LOCAL
no cdp enable
ppp lcp predictive
ppp ipcp predictive
ppp multilink
```

Related Commands

Command	Description
interface dialer	Defines a dialer rotary group.
interface group-async	Creates a group interface that will serve as master, to which asynchronous interfaces can be associated as members.
ppp ipcp predictive	Sets IPCP to a predictive state that reduces negotiation time by predicting responses from peers and sending expected reply and request packets in advance.

ppp link reorders

To set an advisory flag that indicates the serial interface may receive packets in a different order than a peer system sent them, use the **ppp link reorders** command in interface configuration mode. To turn this flag off, use the **no** form of this command.

ppp link reorders

no ppp link reorders

Syntax Description

This command has no arguments or keywords.

Command Default

Command is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

The **ppp link reorders** command indicates that a link can receive packets in a different order than the peer system sent them. This situation can be encountered with PPP tunneling mechanisms such as Layer 2 Forwarding (L2F) and the Layer 2 Transport Protocol (L2TP) that do not always enforce strictly serial delivery of frames from source to final destination. Such links can pose problems for PPP features that depend upon in-order delivery of packets, such as compression, encryption, network header compression, and Multilink PPP.

Setting this option allows some PPP systems to compensate to an extent for the nonserial delivery of packets, although this compensation can incur a performance penalty. It is not normally necessary to configure the **ppp link reorders** command. PPP automatically recognizes that the condition exists for Virtual Private Network (VPN) tunnels, and the misdelivery situation will not occur on normal serial interfaces.

Examples

The following example sets the **ppp link reorders** command advisory flag:

```
ppp link reorders
```

ppp loopback ignore

To disable PPP loopback detection, use the **ppp loopback ignore** command in interface configuration mode. To reenable PPP loopback detection (the default condition), use the **no** form of this command.

ppp loopback ignore

no ppp loopback ignore

Syntax Description

This command has no arguments or keywords.

Command Default

Loopback detection is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced as **ppp ignore-loopback**.
12.2(5)T	The **ppp loopback ignore** command replaced the **ppp ignore-loopback** command.

Usage Guidelines

A circuit loopback normally indicates faulty external switching equipment or wiring errors. The PPP protocol includes a mechanism that detects when a circuit is looped back, that is, when the circuit is fed back upon itself such that the router is reading its own output on that link. A first phase of loopback detection occurs during Link Control Protocol (LCP) negotiation when the circuit is being established. A loopback condition that occurs after the connection is made (after LCP negotiation) can be detected if link keepalives are enabled. If keepalives are disabled on the link, the second phase of loopback detection is not available.

The normal operation (default) is for PPP to check for a loopback condition and terminate the connection when a loopback is detected. There are, however, some situations where it is necessary to disable loopback detection, such as during certain testing situations, or when software detects problematic peers that do not implement the PPP protocol correctly. The **ppp loopback ignore** command disables normal operation; the **no ppp loopback ignore** command restores normal operation.

Note Loopback detection depends upon successful negotiation of the LCP Magic Number option during link establishment. Some implementations may not support this option.

Examples

The following example shows PPP loopback detection being disabled:

```
interface Serial0:15
 description "PRI D channel"
 ip unnumbered Loopback0
 encapsulation ppp
 ppp loopback ignore
```

Related Commands

Command	Description
keepalive	Configures a keepalive packet that is sent at a certain time interval, and for a certain number of retries if there is no response, to keep an interface active.

ppp max-bad-auth

To configure a point-to-point interface not to reset itself immediately after an authentication failure but instead to allow a specified number of authentication retries, use the **ppp max-bad-auth** command in interface configuration mode. To reset to the default of immediate reset, use the **no** form of this command.

ppp max-bad-auth *retries*

no ppp max-bad-auth

Syntax Description

retries	Number of retries after which the interface is to reset itself. Default is 0.

Command Default

The default is 0.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

This command applies to any serial interface (asynchronous serial, synchronous serial, or ISDN) on which PPP encapsulation is enabled.

Examples

The following example sets BRI interface 0 to allow two additional retries after an initial authentication failure (for a total of three failed authentication attempts):

```
interface bri 0
 encapsulation ppp
 ppp authentication chap
 ppp max-bad-auth 3
```

Related Commands

Command	Description
exec	Allows an EXEC process on a line.

ppp max-configure

To set the maximum number of attempts to send Configure-Request packets before it is assumed that the peer is unable to respond, use the **ppp max-configure** command in interface configuration mode. To return to the default, use the **no** form of this command.

ppp max-configure *attempts*

no ppp max-configure *attempts*

Syntax Description

attempts	Number of attempts allowed. Must be a number from 1 to 255. Default is 10 attempts with 1 packet sent per attempt.

Command Default

10 attempts (packets) and a default retry timeout period of 2 seconds

Command Modes

Interface configuration

Command History

Release	Modification
12.2T	This command was introduced.

Usage Guidelines

The **ppp max-configure** command sets the maximum number of Configure-Request packets that will be sent for any particular control protocol and that have gone unanswered before PPP will assume that the peer is unable to respond to the packets and will cease trying to negotiate that particular control protocol.

There is generally no reason to adjust the default maximum number of Configure-Request packets sent (attempts). The number might need to be increased slightly in the unlikely event that you are connecting to a peer that is slow to start negotiations of some protocol. Because the default is 10 packets (attempts), and the default retry timeout period is 2 seconds, a slow peer would be one that takes more than 20 seconds to start protocol negotiation.

For ordinary network control protocols (NCPs), the protocol will be put in a passive state whereby PPP will accept inbound negotiation packets, thereby giving the peer a chance to attempt negotiations later on.

If the Link Control Protocol (LCP) is used, then failure to negotiate LCP implies that the link will be reset. On a dialup connection, this reset will disconnect the call. For a leased-line connection, the reset will merely result in PPP attempting to restart after a short delay.

Note None of the supported PPP authentication protocols conform to RFC 1661-style control protocols, and the protocols are not affected by the **ppp max-configure** command. Rather, the authentication protocol commands have their own set of commands to fine-tune control.

Examples

The following example returns the maximum number of attempts to send a Configure-Request packet to the default of 10:

```
interface Serial2/0
 ip address 192.168.1.131 255.255.255.0
 encapsulation ppp
 peer default ip address pool local local_pool
 serial restart-delay 0
 no ppp max-configure
```

Related Commands

Command	Description
ppp max-failure	Sets the maximum number of attempts to send Configure-NAK packets before it is assumed the peer is not converging.
ppp max-terminate	Sets the maximum number of attempts to send a Terminate-Request packet before PPP gives up waiting for the Terminate-Ack packet and stops the protocol.
ppp timeout retry	Sets PPP timeout retry parameters.

ppp max-failure

To set the maximum number of attempts to send Configure-NAK packets before it is assumed the peer is not converging, use the **ppp max-failure** command in interface configuration mode. To return to the default, use the **no** form of this command.

ppp max-failure *attempts*

no ppp max-failure *attempts*

Syntax Description

attempts	Number of attempts allowed. Must be a number from 1 to 255. Default is 5 attempts with one packet sent per attempt.

Command Default

5 attempts

Command Modes

Interface configuration

Command History

Release	Modification
12.2T	This command was introduced.

Usage Guidelines

Unless you have reason to believe that a control protocol that is slow to converge will actually converge if given more chances, there is no reason to increase the default value of this command.

The **ppp max-failure** command sets the maximum number of successive Configure-NAK packets (attempts) that will be sent for any control protocol before PPP will assume that the peer is unwilling or incapable of converging (adapting to its own negotiation parameters), and that the negotiation parameters will never succeed.

Once the maximum limit is reached, PPP will start sending Configure-Reject packets rather than Configure-NAK packets for the offending parameters. The peer's response to this action should be to stop sending the offending parameters.

Note None of the supported PPP authentication protocols conform to RFC 1661-style control protocols, and the protocols are not affected by the **ppp max-failure** command. Rather, the authentication protocol commands have their own set of commands to fine-tune control.

Examples

The following example returns the maximum number of attempts to send a Configure-NAK packet to the default of 5:

```
interface Serial2/0
 ip address 192.168.1.131 255.255.255.0
 encapsulation ppp
 peer default ip address pool local local_pool
 serial restart-delay 0
 no ppp max-failure
```

Related Commands

Command	Description
ppp max-configure	Sets the maximum number of attempts to send Configure-Request packets before it is assumed that the peer is unable to respond.
ppp max-terminate	Sets the maximum number of attempts to send a Terminate-Request packet before PPP gives up waiting for the Terminate-Ack packet and stops the protocol.
ppp timeout retry	Sets PPP timeout retry parameters.

ppp max-terminate

To set the maximum number of attempts to send Terminate-Request packets before PPP gives up waiting for the Terminate-Ack packet and stops the protocol, use the **ppp max-terminate** command in interface configuration mode. To return to the default, use the **no** form of this command.

ppp max-terminate *attempts*

no ppp max-terminate *attempts*

Syntax Description

attempts	Number of attempts allowed. Must be a number from 1 to 255. Default is 2 attempts with 1 packet sent per attempt.

Command Default

2 attempts

Command Modes

Interface configuration

Command History

Release	Modification
12.2T	This command was introduced.

Usage Guidelines

There is little reason to change the default value of the **ppp max-terminate** command. The action of PPP sending a Terminate-Request packet is mainly a courtesy to the peer system; the protocol itself will be terminated whether or not the peer acknowledges the request. Sending the Terminate-Request packet twice makes an allowance that a single instance could be lost in transit.

When PPP wants to terminate a control protocol, it sends a Terminate-Request packet and waits for a limited time for the peer to respond with a Terminate-Ack packet. This command sets the maximum number of attempts that will be made, that is, the maximum number of Terminate-Request packets that will be sent, before PPP gives up waiting for the Terminate-Ack packet and automatically stops the protocol.

Note None of the supported PPP authentication protocols conform to RFC 1661-style control protocols, and the protocols are not affected by the **ppp max-terminate** command. Rather, the authentication protocol commands have their own set of commands to fine-tune control.

Examples

The following example returns the maximum number of attempts to send a Terminate-Request packet to the default of 2:

```
interface Serial2/0
 ip address 192.168.1.131 255.255.255.0
 encapsulation ppp
 peer default ip address pool local local_pool
 serial restart-delay 0
 no ppp max-terminate
```

Related Commands

Command	Description
ppp max-configure	Sets the maximum number of attempts to send Configure-Request packets before it is assumed that the peer is unable to respond.
ppp max-failure	Sets the maximum number of attempts to send Configure-NAK packets before it is assumed the peer is not converging.
ppp timeout retry	Sets PPP timeout retry parameters.

ppp microcode

To enable hardware (microcode) PPP framing on an asynchronous interface, use the **ppp microcode** command in interface configuration mode. To disable hardware PPP framing on an asynchronous interface, use the **no** form of this command.

ppp microcode

no ppp microcode

Syntax Description

This command has no arguments or keywords.

Command Default

Hardware PPP framing on an asynchronous interface is enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4	This command was introduced.

Usage Guidelines

Do not use the **no** form of this command unless instructed to do so by Cisco Technical Assistance Center (TAC) or Cisco technical support.

Examples

The following example shows how to disable the **ppp microcode** command in interface configuration mode:

```
no ppp microcode
```

Related Commands

Command	Description
async mode dedicated	Places a line into dedicated asynchronous mode using **SLIP** or PPP encapsulation.
async mode interactive	Returns a line that has been placed into dedicated asynchronous network mode to interactive mode, thereby enabling the slip and **ppp** EXEC commands.
encapsulation ppp	Sets PPP as the encapsulation method used on the specified interfaces.
ppp multilink	Enables MLP on an interface and, optionally, enables BACP and its BAP subset for dynamic bandwidth allocation.

ppp mru match

To trigger Link Control Protocol (LCP) renegotiation on a maximum receive unit (MRU) mismatch on a system acting as an L2TP network server (LNS) and thereby enforce strict matching, use the **ppp mru match** command in interface configuration mode. To remove this setting, use the **no** form of this command.

ppp mru match

no ppp mru match

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(12)T	This command was introduced.

Usage Guidelines

This command is configured only on virtual template interfaces.

By default, the LNS does not enforce matching of the MRU value advertised by the LAC with the MRU value that the LNS would advertise. Use the **ppp mru match** command to enforce strict matching of the MRU that is advertised by the Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) with the maximum transmission unit (MTU) of the relevant virtual template interface on the LNS. A mismatch can occur because the effective MRU size for a virtual access interface is not necessarily limited to the MTU size.

This command can be useful to inform the client PPP stack of the true MRU, when that PPP implementation is capable of adapting its MTU based on LCP MRU negotiation.

Examples

The following example shows LCP renegotiation being triggered on an MRU mismatch:

```
interface Virtual-Template1
 mtu 1454
 ppp mru match
 ip unnumbered GigabitEthernet0/1
 no keepalive
 peer default ip address pool mypool
 ppp authentication pap
```

Related Commands

Command	Description
ppp mtu adaptive	Defines autonegotiation of the MTU size for PPP.

ppp ms-chap refuse

To refuse Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) authentication from peers requesting it, use the **ppp ms-chap refuse** command in interface configuration mode. To allow MS-CHAP authentication, use the **no** form of this command.

ppp ms-chap refuse [**callin**]

no ppp ms-chap refuse [**callin**]

Syntax Description

callin	(Optional) Specifies that the router will refuse to answer MS-CHAP authentication challenges received from the peer, but will still require the peer to answer any MS-CHAP challenges the router sends.

Command Default

This command is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.2T	This command was introduced.

Usage Guidelines

This command specifies that MS-CHAP authentication is disabled for all calls, meaning that all attempts by the peer to force the user to authenticate using MS-CHAP will be refused. If the **callin** keyword is used, MS-CHAP authentication is disabled for incoming calls from the peer, but will still be performed on outgoing calls to the peer.

If outbound Password Authentication Protocol (PAP) has been enabled (using the **ppp pap sent-username** command), PAP will be suggested as the authentication method in the refusal packet.

Examples

The following example shows how to disable MS-CHAP authentication if a peer calls in requesting MS-CHAP authentication. The method of encapsulation on interface ISDN BRI number 0 is PPP.

```
interface bri 0
 encapsulation ppp
 ppp ms-chap refuse
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.

Command	Description
ppp authentication ms-chap-v2	Creates a pool of dialup routers that all appear to be the same host when authenticating with CHAP.
ppp chap password	Enables a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common CHAP secret password to use in response to challenges from an unknown peer.
ppp chap wait	Specifies that the router will not authenticate to a peer requesting CHAP authentication until after the peer has authenticated itself to the router.
ppp pap sent-username	Reenables remote PAP support for an interface and use the sent-username and password in the PAP authentication request packet to the peer.

ppp ms-chap-v2 refuse

To refuse Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) version 2 authentication from peers requesting it, use the **ppp ms-chap-v2 refuse** command in interface configuration mode. To allow MS-CHAP version 2 authentication, use the **no** form of this command.

ppp ms-chap-v2 refuse [**callin**]

no ppp ms-chap-v2 refuse [**callin**]

Syntax Description

callin	(Optional) Specifies that the router will refuse to answer MS-CHAP authentication challenges received from the peer, but will still require the peer to answer any MS-CHAP challenges the router sends.

Command Default

This command is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.2T	This command was introduced.

Usage Guidelines

This command specifies that MS-CHAP version 2 authentication is disabled for all calls, meaning that all attempts by the peer to force the user to authenticate using MS-CHAP version 2 will be refused. If the **callin** keyword is used, MS-CHAP version 2 authentication is disabled for incoming calls from the peer, but will still be performed on outgoing calls to the peer.

If outbound Password Authentication Protocol (PAP) has been enabled (using the **ppp pap sent-username** command), PAP will be suggested as the authentication method in the refusal packet.

Examples

The following example shows how to disable MS-CHAP version 2 authentication if a peer calls in requesting MS-CHAP version 2 authentication. The method of encapsulation on interface ISDN BRI number 0 is PPP.

```
interface bri 0
 encapsulation ppp
 ppp ms-chap-v2 refuse
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.

Command	Description
ppp authentication ms-chap-v2	Creates a pool of dialup routers that all appear to be the same host when authenticating with CHAP.
ppp chap password	Enables a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common CHAP secret password to use in response to challenges from an unknown peer.
ppp chap wait	Specifies that the router will not authenticate to a peer requesting CHAP authentication until after the peer has authenticated itself to the router.
ppp pap sent-username	Reenables remote PAP support for an interface and use the sent-username and password in the PAP authentication request packet to the peer.

ppp mtu adaptive

To allow the Layer 2 Network Server (LNS) to adapt to the Maximum Transmission Unit (MTU) size for PPP based on the value set by the customer premises equipment (CPE), use the **ppp mtu adaptive** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

ppp mtu adaptive [**proxy**]

no ppp mtu adaptive [**proxy**]

Syntax Description

proxy	(Optional) Adapts the MTU to the proxy MRU, that is, the MRU negotiated by a system such as an L2TP access concentrator (LAC) that has performed Link Control Protocol (LCP) negotiation on behalf of the Cisco router and forwarded the negotiated LCP options, including the MRU.

Command Default

Automatic adaption of the MTU size for PPP is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(7)	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T. The **proxy** keyword was added.
12.3(14)T	This command was modified. Support was added for serial interfaces when the **proxy** keyword is not used.

Usage Guidelines

By default, the Cisco IOS software will not adapt the interface MTU to the peer or proxy MRU.

Note By default, the LNS does not renegotiate Link Control Protocol (LCP). If the LNS has a different MTU defined, the call setup experiences a failure. Use the **ppp mtu adaptive** command to adjust the LNS MRU value to the CPE's negotiated value with the LAC.

Use this command on interfaces where a number of peers with different MRU settings may connect. In Cisco IOS Release 12.2(7) and later releases, this command is configured on virtual template interfaces and dialer interfaces. In Cisco IOS Release 12.3(14)T and later releases, the **ppp mtu adaptive** command *without* the **proxy** keyword can be configured on serial interfaces.

The **proxy** keyword is not typically required. It is used only as a workaround when the client PPP stack cannot correctly advertise its MRU requirements.

Examples

The following example defines autonegotiation of the MTU size on a virtual template:

```
interface Virtual-Template1
 no ip address
 no logging event link-status
 no snmp trap link-status
 ppp mtu adaptive
 ppp authentication chap callin
```

Related Commands

Command	Description
lcp renogtiation always	Allows the LNS to renegotiate the PPP LCP on dial-in calls, using L2TP or L2F.
ppp mtu match	Triggers LCP renegotiation on an MRU mismatch.

ppp multilink

To enable Multilink PPP (MLP) on an interface and, optionally, to enable Bandwidth Allocation Control Protocol (BACP) and its Bandwidth Allocation Protocol (BAP) subset for dynamic bandwidth allocation, use the **ppp multilink** command in interface configuration mode. To disable Multilink PPP or, optionally, to disable only dynamic bandwidth allocation, use the **no** form of this command.

ppp multilink [**bap**]

no ppp multilink [**bap** [**required**]]

Cisco 10000 Series Router

ppp multilink

no ppp multilink

Syntax Description

bap	(Optional) Specifies bandwidth allocation control negotiation and dynamic allocation of bandwidth on a link.
required	(Optional) Enforces mandatory negotiation of BACP for the multilink bundle. The multilink bundle is disconnected if BACP is not negotiated.

Defaults

This command is disabled. When BACP is enabled, the defaults are to accept calls and to set the timeout pending at 30 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.1	This command was introduced.
12.0(23)SX	This command was implemented on the Cisco 10000 series router.
12.2(16)BX	This command was implemented on the ESR–PRE2.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

This command applies only to interfaces that use PPP encapsulation.

MLP and PPP reliable links do not work together.

When the **ppp multilink** command is used, the first channel will negotiate the appropriate Network Control Protocol (NCP) layers (such as the IP Control Protocol and IPX Control Protocol), but subsequent links will negotiate only the link control protocol and MLP. NCP layers do not get negotiated on these links, and it is normal to see these layers in a closed state.

This command with the **bap** keyword must be used before configuring any **ppp bap** commands and options. If the **bap required** option is configured and a reject of the options is received, the multilink bundle is torn down.

The **no** form of this command without the **bap** keyword disables both MLP and BACP on the interface.

The **dialer load-threshold** command enables a rotary group to bring up additional links and to add them to a multilink bundle.

Before Cisco IOS Release 11.1, the **dialer-load threshold 1** command kept a multilink bundle of any number of links connected indefinitely, and the **dialer-load threshold 2** command kept a multilink bundle of two links connected indefinitely. If you want a multilink bundle to be connected indefinitely, you must set a very high idle timer.

Note By default, after changing hostnames, an MLP member link does not undergo failure recovery automatically. You must use the **ppp chap hostname** command to define the MLP bundle name on an endpoint. If this command is not configured and the hostname is changed, then a link flap will not return the link back to the bundle.

Cisco 10000 Series Router

The **ppp multilink** command has no arguments or keywords.

Examples

The following partial example shows how to configure a dialer for MLP:

```
interface Dialer0
 ip address 10.0.0.2 255.0.0.0
 encapsulation ppp
 dialer in-band
 dialer idle-timeout 500
 dialer map ip 10.0.0.1 name atlanta broadcast 81012345678901
 dialer load-threshold 30 either
 dialer-group 1
 ppp authentication chap
 ppp multilink
```

Related Commands

Command	Description
compress	Configures compression for LAPB, PPP, and HDLC encapsulations.
dialer fast-idle (interface)	Specifies the idle time before the line is disconnected.
dialer-group	Controls access by configuring an interface to belong to a specific dialing group.
dialer load-threshold	Configures bandwidth on demand by setting the maximum load before the dialer places another call to a destination.
encapsulation ppp	Enables PPP encapsulation.
ppp authentication	Enables CHAP or PAP or both, and specifies the order in which CHAP and PAP authentication is selected on the interface.
ppp bap timeout	Specifies nondefault timeout values for PPP BAP pending actions and responses.
ppp chap hostname	Enables a router calling a collection of routers that do not support this command to configure a common CHAP secret password to use in response to challenges from an unknown peer.

Command	Description
ppp multilink fragment delay	Specifies a maximum time for the transmission of a packet fragment on a MLP bundle.
ppp multilink fragment disable	Disables packet fragmentation.
ppp multilink fragmentation	Sets the maximum number of fragments a packet will be segmented into before being sent over the bundle.
ppp multilink group	Restricts a physical link to joining only a designated multilink-group interface.
ppp multilink interleave	Enables MLP interleaving.
ppp multilink mrru	Configures the MRRU value negotiated on an MLP bundle.
ppp multilink slippage	Defines the constraints that set the MLP reorder buffer size.
show ppp bap	Displays the configuration settings and run-time status for a multilink bundle.

ppp multilink endpoint

To override or change the default endpoint discriminator the system uses when negotiating the use of Multilink PPP (MLP) with the peer, use the **ppp multilink endpoint** command in interface configuration mode. To restore the default endpoint discriminator, use the **no** form of this command.

ppp multilink endpoint {**hostname** | **ip** *ip-address* | **mac** *lan-interface* | **none** | **phone** *telephone-number* | **string** *char-string*}

no ppp multilink endpoint

Syntax Description

hostname	Uses the host name configured for the router. This is useful when multiple routers are using the same username to authenticate, but have different host names.
ip *ip-address*	Uses the supplied IP address.
mac *lan-interface*	Uses the specified LAN interface whose MAC address is to be used.
none	Causes negotiation of the link control protocol without requesting the endpoint discriminator option. This is useful when the router is connected to a malfunctioning peer that does not handle the endpoint discriminator option properly.
phone *telephone-number*	Uses the supplied telephone number, and accepts E.164-compliant, full international telephone numbers.
string *char-string*	Uses the supplied character string.

Command Default

The default endpoint discriminator is the globally configured host name, or the Challenge Handshake Authentication Protocol (CHAP) host name or Password Authentication Protocol (PAP) sent-username configured on the interface. See the "Usage Guidelines" for additional information.

Command Modes

Interface configuration

Command History

Release	Modification
12.2	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

By default, PPP uses the same string for the endpoint discriminator that it would provide for authentication to negotiate use of MLP with the peer. The string (username) is configured for the interface with the **ppp chap hostname** or **ppp pap sent-username** command, or defaults to the globally configured host name (or stack group name, if the interface is a Stack Group Bidding Protocol, or SGBP, group member). The keywords supplied with the **ppp multilink endpoint** command allow a different endpoint discriminator to be defined. You can reset the default condition by entering the **no ppp multilink endpoint** command.

The difference between the **no ppp multilink endpoint** command and the **ppp multilink endpoint hostname** command is that for the first command, MLP supplies the name used for authentication (which may or may not be the router host name), and the second command always uses the router host name, regardless of any local authentication configuration.

Both the **hostname** and **string** keywords use the local endpoint class, the differences between them being that the **string** keyword allows you to enter a value, while the **hostname** keyword uses the configured (default) host name.

Note Do not configure the **ppp multilink endpoint** command on MLP bundle interfaces. Configure this command on each interface that will be an MLP bundle member, not on the bundle interface itself.

Refer to RFC 1990 for more information about MLP and the endpoint discriminator option.

Examples

The following partial example changes the endpoint discriminator from the CHAP host named group 1 to IP address 10.1.1.4:

```
.
.
.
interface Dialer0
 ip address 10.1.1.4 255.255.255.0
 encapsulation ppp
 dialer remote-name R-name
 dialer string 23456
 dialer pool 1
 dialer-group 1
 ppp chap hostname group 1
 ppp multilink endpoint ip 10.1.1.4
.
.
.
```

Related Commands

Command	Description
multilink bundle-name	Selects a method for naming multilink bundles.
ppp chap hostname	Creates a pool of dialup routers that all appear to be the same host when authenticating with CHAP.
ppp multilink group	Restricts a physical link to joining only a designated multilink-group interface.
ppp pap sent-username	Reenables remote PAP support for an interface and uses the sent-username and password in the PAP authentication request packet to the peer.
sgbp member	Specifies the host name and IP address of a router or access server that is a peer member of a stack group.

ppp multilink fragment delay

To specify a maximum time for the transmission of a packet fragment on a Multilink PPP (MLP) bundle, use the **ppp multilink fragment delay** command in interface configuration mode. To reset the maximum delay to the default value, use the **no** form of this command.

ppp multilink fragment delay *milliseconds* [*microseconds*]

no ppp multilink fragment delay

Syntax Description

milliseconds	Maximum amount of time, in milliseconds, that should be required to transmit a fragment. Valid values range from 0 to 1000 milliseconds. The default is 30 milliseconds. **Note** If the desired delay should be in microseconds, set the *milliseconds* argument to 0 and enter a value for the *microseconds* argument.
microseconds	(Optional) Maximum amount of time, in microseconds, that should be required to transmit a fragment. Valid values range from 1 to 999 microseconds.

Command Default

The default value is 30 milliseconds if interleaving is enabled or if the bundle contains links that have differing bandwidths. See the "Usage Guidelines" for more information.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced as **ppp multilink fragment-delay**.
12.2	This command was changed to **ppp multilink fragment delay**.
12.4(4)T	Support for the *microseconds* argument was added.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

By default, MLP has no fragment size constraint. Packets are divided into a number of fragments based on the number of links in the bundle. The size of any fragment is unconstrained, but the maximum number of fragments is constrained by the number of links. If interleaving is enabled, if the bundle contains links that have differing bandwidths, or if a fragment delay is explicitly configured with the **ppp multilink fragment delay** command, then MLP uses a different fragmentation algorithm. In this mode, the number of fragments is unconstrained, but the size of each fragment is limited to the fragment delay value, or 30 milliseconds if the fragment delay has not been configured.

The **ppp multilink fragment delay** command is useful when packets are interleaved and traffic characteristics such as delay, jitter, and load balancing must be tightly controlled.

The **ppp multilink fragment delay** command applies only to multilink interfaces that can configure a bundle interface, including multilink interfaces, virtual templates, dialer interfaces, and ISDN BRI or PRI interfaces.

The value assigned to the *milliseconds* or *microseconds* argument is scaled by the speed at which a link can convert the time value into a byte value. If a bundle has multiple links with varying speeds, the absolute size of a fragment will differ for each link.

MLP chooses a fragment size on the basis of the maximum delay allowed. If real-time traffic requires a certain maximum bound on delay, using this command to set that maximum time can ensure that a real-time packet will get interleaved within the fragments of a large packet.

Examples

The following example configures a maximum fragment delay of 20 milliseconds:

```
ppp multilink fragment delay 20
```

The following example configures a maximum fragment delay of 500 microseconds (1/2 millisecond):

```
ppp multilink fragment delay 0 500
```

Related Commands

Command	Description
ppp multilink	Enables MLP on an interface and, optionally, enables dynamic bandwidth allocation.
ppp multilink fragment disable	Enables or suppresses packet fragmentation on an MLP bundle.
ppp multilink fragment size	Specifies the maximum packet fragment size in bytes for a MLP link.
ppp multilink fragmentation	Sets the maximum number of fragments a packet will be segmented into before being sent over the bundle.
ppp multilink interleave	Enables MLP interleaving.

ppp multilink fragment disable

To disable packet fragmentation, use the **ppp multilink fragment disable** command in interface configuration mode. To enable fragmentation, use the **no** form of this command.

ppp multilink fragment disable

no ppp multilink fragment disable

Syntax Description

This command has no arguments or keywords.

Command Default

Fragmentation is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced as **ppp multilink fragmentation**.
12.2	The **no ppp multilink fragmentation** command was changed to **ppp multilink fragment disable**. The **no ppp multilink fragmentation** command was recognized and accepted through Cisco IOS Release 12.2.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

The **ppp multilink fragment delay** and **ppp multilink interleave** commands have precedence over the **ppp multilink fragment disable** command. Therefore, the **ppp multilink fragment disable** command has no effect if these commands are configured for a multilink interface and the following message displays:

```
Warning: 'ppp multilink fragment disable' or 'ppp multilink fragment maximum' will be
ignored, since multilink interleaving or fragment delay has been configured and have
higher precedence.
```

To completely disable fragmentation, you must do the following:

```
Router(config-if)# no ppp multilink fragment delay
Router(config-if)# no ppp multilink interleave
Router(config-if)# ppp multilink fragment disable
```

Disable multilink fragmentation using the **ppp multilink fragment disable** command if fragmentation causes performance degradation. Performance degradation due to multilink fragmentation has been observed with asynchronous member links.

Examples

The following example disables packet fragmentation:

```
ppp multilink fragment disable
```

Related Commands

Command	Description
ppp multilink fragment delay	Specifies a maximum size, in units of time, for packet fragments on an MLP bundle.
ppp multilink interleave	Enables MLP interleaving.
ppp multilink group	Restricts a physical link to joining only a designated multilink-group interface.
ppp multilink mrru	Configures the Maximum Receive Reconstructed Unit (MRRU) value negotiated on a Multilink PPP (MLP) bundle.

ppp multilink fragment maximum

To set the maximum number of fragments a packet will be segmented into before being sent over the bundle, use the **ppp multilink fragment maximum** command in interface configuration mode. To reset fragmentation to the default value, use the **no** form of this command.

ppp multilink fragment maximum *fragments*

no ppp multilink fragment maximum

Syntax Description

fragments	Maximum number of fragments in the range from 2 to 16.

Command Default

16 fragments

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced as **multilink max-fragments**.
12.2	This command was changed to **ppp multilink fragment maximum**. The **multilink max-fragments** command was accepted by the command line interpreter through Cisco IOS Release 12.2.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

Use the **ppp multilink fragment maximum** command to control the number of fragments into which a PPP frame may be fragmented. The **ppp multilink fragment maximum** command has been used to disable fragmentation entirely by setting the number of fragments to 1. This setting is better accomplished using the **ppp multilink fragment disable** command.

The limit set using the **ppp multilink fragment maximum** command applies only when Multilink PPP (MLP) is fragmenting packets in a mode where it is constraining the number of fragments rather than the size of the fragments. See the description about fragmentation modes in the section "Usage Guidelines" of the **ppp multilink fragment delay** command for more details.

Examples

The following example uses the **ppp multilink fragment maximum** command to fragment each frame into no more than four fragments:

```
ppp multilink fragment maximum 4
```

Related Commands

Command	Description
ppp multilink fragment delay	Specifies a maximum size, in units of time, for packet fragments on an MLP bundle.
ppp multilink fragment disable	Disables packet fragmentation.

ppp multilink fragment size

To specify the maximum packet fragment size in bytes for a Multilink PPP (MLP) link, use the **ppp multilink fragment size** command in interface configuration mode. To remove a configured fragment size limitation, use the **no** form of this command.

ppp multilink fragment size *bytes*

no ppp multilink fragment size

Syntax Description

bytes	Maximum number of bytes per fragment that will be transmitted over this link, not including link layer and multilink overhead.

Command Default

No maximum fragment size is set.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(4)T	The command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

Use the **ppp multilink fragment size** command to specify a maximum fragment size that is smaller than the size automatically computed by the value set with the **ppp multilink fragment delay** command. The **ppp multilink fragment size** command may be configured on the bundle interface or on the member links. If the command is configured on the bundle interface, the same fragment size is used by all of the links in the bundle. If it is configured in both places, the configuration on the member link takes precedence.

Examples

The following example configures a maximum fragment size of 100 bytes, not including link layer or multilink header overhead:

```
ppp multilink fragment size 100
```

Related Commands

Command	Description
ppp multilink	Enables MLP on an interface and, optionally, enables dynamic bandwidth allocation.
ppp multilink fragment delay	Specifies a maximum time for the transmission of a packet fragment on a MLP bundle.
ppp multilink fragment disable	Enables or suppresses packet fragmentation on an MLP bundle.

Command	Description
ppp multilink fragmentation	Sets the maximum number of fragments a packet will be segmented into before being sent over the bundle.
ppp multilink interleave	Enables MLP interleaving.

ppp multilink fragmentation

The **ppp multilink fragmentation** command is replaced by the **ppp multilink fragment disable** command. See the description of the **ppp multilink fragment disable** command for more information.

ppp multilink group

To restrict a physical link to joining only a designated multilink-group interface, use the **ppp multilink group** command in interface configuration mode. To remove the restrictions, use the **no** form of this command.

ppp multilink group *group-number*

no ppp multilink group

Syntax Description

group-number	Multilink-group number (a nonzero number).

Command Defaults

Command is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced as **multilink-group**.
12.0	This command was introduced on the PRE1 for the Cisco 10000 series router.
12.2	This command was changed to **ppp multilink group**. The **multilink-group** command was accepted by the command line interpreter through Cisco IOS Release 12.2.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(31)SB2	This command was introduced on the PRE3 for the Cisco 10000 series router.

Usage Guidelines

By default this command is disabled, which means the link can negotiate to join any bundle in the system.

When the **ppp multilink group** command is configured, the physical link is restricted from joining any but the designated multilink-group interface. If a peer at the other end of the link tries to join a different bundle, the connection is severed. This restriction applies when Multilink PPP (MLP) is negotiated between the local end and the peer system. The link can still come up as a regular PPP interface.

This command is primarily used with the MLP inverse multiplexer described in the "Configuring Media-Independent PPP and Multilink PPP" chapter in the *Cisco IOS Dial Technologies Configuration Guide*.

Cisco 10000 Series Router

- The *group-number* option of the **ppp multilink group** command identifies the multilink group. This number must be identical to the *multilink-bundle-number* you assign to a multilink interface. 1 to 9999 and 65,536 to 2,147,483,647 (Cisco IOS Release 12.2(31)SB2 and later releases)
- 1 to 9999 and 65,536 to 2,147,483,647 (Cisco IOS Release 12.2(31)SB2 and later releases)

Examples

The following example designates serial interface 1 as part of multilink bundle 1:

```
interface serial 1
 encapsulation ppp
 ppp multilink group 1
 ppp multilink
 ppp authentication chap
 pulse-time 3
```

Related Commands

Command	Description
interface multilink	Creates a multilink bundle or enters multilink interface configuration mode.

ppp multilink idle-link

To configure a multilink bundle so that the slowest link enters into receive-only mode when a link is added, use the **ppp multilink idle-link** command in interface configuration mode. To remove the idle link flag, use the **no** form of this command.

ppp multilink idle-link

no ppp multilink idle-link

Syntax Description

This command has no arguments or keywords.

Command Default

The idle link flag is not set.

Command Modes

Interface configuration

Command History

Release	Modification
11.3T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

When the idle link flag is enabled, Multilink PPP (MLP) places the slowest link in a bundle into an idle receive-only mode whenever the bundle has more than one link.

This mode is used for the Always On/Dynamic ISDN (AO/DI) feature, where a bundle contains one permanent slow-speed member link, which is on an X.25 circuit contained on an ISDN D channel. As additional and faster links join the MLP bundle, the D channel circuit will be idled and traffic will be confined to the faster links.

The **ppp multilink idle-link** command was intended specifically to enable the AO/DI feature. The command will work on any bundle, but normally should not be used outside the AO/DI environment.

Examples

The following example configures the interface (dialer interface 1) to add links to the MLP bundle once the traffic load on the primary link is reached:

```
interface dialer1
 ppp multilink idle-link
```

Related Commands

Command	Description
ppp multilink	Enables MLP on an interface and, optionally, enables dynamic bandwidth allocation.
ppp multilink fragment delay	Specifies a maximum time for the transmission of a packet fragment on an MLP bundle.
ppp multilink fragment disable	Disables packet fragmentation.

Command	Description
ppp multilink fragmentation	Sets the maximum number of fragments a packet will be segmented into before being sent over the bundle.
ppp multilink group	Restricts a physical link to joining only a designated multilink-group interface.
ppp multilink interleave	Enables MLP interleaving.

ppp multilink interleave

To enable interleaving of packets among the fragments of larger packets on a Multilink PPP (MLP) bundle, use the **ppp multilink interleave** command in interface configuration mode. To disable interleaving, use the **no** form of this command.

ppp multilink interleave

no ppp multilink interleave

Syntax Description

This command has no arguments or keywords.

Command Default

Interleaving is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.0(23)SX	This command was implemented on the Cisco 10000 series router.
12.2(4)T	This command was implemented on the Versatile Interface Processor (VIP)-enabled Cisco 7500 series routers as part of the Distributed Link Fragmentation and Interleaving (dLFI) feature. The Distributed Link Fragmentation and Interleaving feature introduced this command for ATM and Frame Relay only.
12.2(8)T	This command was implemented for leased lines on VIP-enabled Cisco 7500 series routers.
12.0(24)S	This command was implemented for leased lines on VIP-enabled Cisco 7500 series routers. This command cannot be used for ATM and Frame Relay using Cisco IOS Release 12.0S.
12.2(14)SX	This command was implemented for leased lines on the Cisco 7600 series routers and Catalyst 6500 series switches with a FlexWAN.
12.2(28)SB2	This command was integrated into Cisco IOS Release 12.2(28)SB2.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

The **ppp multilink interleave** command applies only to interfaces that can configure a bundle interface, such as virtual templates, dialer interfaces, multilink interfaces, and ISDN BRI or PRI interfaces.

Interleaving works only when the queuing mode on the bundle has been set to fair queuing (all platforms *except* the VIP-enabled Cisco 7500 series routers) or to distributed low latency queuing (dLLQ) for the VIP-enabled Cisco 7500 series routers.

On the VIP-enabled Cisco 7500 series routers, distributed Cisco Express Forwarding (dCEF) must be enabled, and dLLQ must be configured using the **priority** command in policy map configuration mode, before **ppp multilink interleave** command is used.

For all platforms except the VIP-enabled Cisco 7500 series routers, the **ppp multilink interleave** command should not be set unless weighted fair queuing (WFQ) has been configured using the default **fair-queue** command.

If interleaving is enabled when fragment delay is not configured, the default delay is 30 milliseconds. The fragment size is derived from that delay, depending on the bandwidths of the links.

Examples

The following example defines a virtual interface template that enables MLP interleaving and a maximum real-time traffic delay of 20 milliseconds, and then applies that virtual template to the MLP bundle:

```
interface virtual-template 1
 ip unnumbered ethernet 0
 ppp multilink
 ppp multilink interleave
 ppp multilink fragment delay 20
!
multilink virtual-template 1
```

The following example shows the configuration of LFI using MLP running on top of a PPP link over Frame Relay using a virtual template interface:

```
class-map voip
 match ip precedence 5
!
class-map business
 match ip precedence 3
!
policy-map llq-policy
 class voip
  priority 32
 class business
  bandwidth 32
!
policy-map shape-llq-policy
 class class-default
  shape average 80000 320 320
  service-policy llq-policy
!
policy-map input-policy
 class voip
  police 32000 1500 1500 conform-action transmit exceed-action drop
!
controller T1 5/1/0
 framing esf
 linecode b8zs
 channel-group 0 timeslots 1-2
!
interface Serial5/1/0:0
 no ip address
 encapsulation frame-relay
!
interface Serial5/1/0:0.1 point-to-point
 frame-relay interface-dlci 20 ppp Virtual-Template2
!
interface Virtual-Template2
 bandwidth 78
 ip unnumbered Loopback1
 no keepalive
 service-policy output llq-policy
 service-policy input input-policy
```

```
 ppp multilink
 ppp multilink fragment-delay 8
 ppp multilink interleave
```

The following example shows the configuration of LFI using MLP running on top of a PPPoATM link on an ATM interface. This configuration uses a virtual template interface.

```
class-map voip
 match ip precedence 5
!
class-map business
 match ip precedence 3
!
policy-map llq-policy
 class voip
  priority 32
 class business
  bandwidth 32
!
policy-map input-policy
 class voip
  police 32000 1500 1500 conform-action transmit exceed-action drop
!
interface ATM4/0/0
 no ip address
 no atm ilmi-keepalive
!
interface ATM4/0/0.1 point-to-point
 pvc 0/34
 abr 100 80
 protocol ppp Virtual-Template4
!
interface Virtual-Template4
 bandwidth 78
 ip unnumbered Loopback1
 service-policy output llq-policy
 service-policy input input-policy
 ppp multilink
!
class-map voip
 match ip precedence 5
!
class-map business
 match ip precedence 3
!
policy-map llq-policy
 class voip
  priority 32
 class business
  bandwidth 32
!
policy-map input-policy
 class voip
  police 32000 1500 1500 conform-action transmit exceed-action drop
!
interface ATM4/0/0
 no ip address
 no atm ilmi-keepalive
!
interface ATM4/0/0.1 point-to-point
 pvc 0/34
 abr 100 80
 protocol ppp Virtual-Template4
!
```

```
interface Virtual-Template4
 bandwidth 78
 ip address 10.0.0.2 255.0.0.0
 service-policy output llq-policy
 service-policy input input-policy
 ppp multilink
 ppp multilink fragment-delay 8
 ppp multilink interleave
```

The following example shows the configuration of LFI over a leased line:

```
class-map voip
 match ip precedence 5
!
class-map business
 match ip precedence 3
!
policy-map llq-policy
 class voip
  priority 32
 class business
  bandwidth 32
!
policy-map input-policy
 class voip
  police 32000 1500 1500 conform-action transmit exceed-action drop
!
controller T1 5/1/0
 channel group 0 timeslots 1-2
!
interface multilink 2
 ip address 172.16.0.0 255.0.0.0
 keepalive 5
 bandwidth 128
 ppp multilink
 ppp multilink fragment-delay 8
 ppp multilink interleave
 service-policy output llq-policy
 service-policy input input-policy
 multilink-group 2
!
interface serial5/0/0:0
 no ip address
 encapsulation ppp
 keepalive 5
 ppp chap hostname G2
 ppp multilink
 multilink-group 2
```

The following example shows a simple leased-line interleaving configuration using a virtual access interface bundle and default WFQ:

```
multilink virtual-template 10
!
interface serial0
 no ip address
 encapsulation ppp
 ppp multilink
!
interface virtual-template10
 ip unnumbered Ethernet0
 fair-queue
 ppp multilink
 ppp multilink interleave
```

The following example shows a simple leased-line interleaving configuration using a dedicated multilink interface:

```
interface serial1
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink-group 5
!
interface multilink5
 ip address 209.165.200.225 255.255.255.0
 fair-queue
 ppp multilink
 ppp multilink interleave
```

Related Commands

Command	Description
fair-queue	Enables WFQ for an interface.
ppp multilink fragment delay	Specifies a maximum size, in units of time, for packet fragments on an MLP bundle.
priority	Assigns the specified priority list to an interface.
show ppp multilink	Displays bundle information for the MLP bundles and their PPP links in the router.

ppp multilink links maximum

To limit the maximum number of links that Multilink PPP (MLP) can dial for dynamic allocation, use the **ppp multilink links maximum** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ppp multilink links maximum *links*

no ppp multilink links maximum

Syntax Description

links	Maximum number of links. Valid values range from 1 to 255. The default is 255.

Command Default

255 links

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced as **ppp multilink max-link**.
12.2	This command was changed to **ppp multilink links maximum**. The **ppp multilink max-link** command was accepted by the command-line interpreter through Cisco IOS Release 12.2.
12.2(13)T	The range of valid values for the *links* argument was changed from 1 to 255 to 1 to 64.
12.3(8)T	The range of valid values for the *links* argument was changed from 1 to 64 to 1 to 255.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

This command affects only dial-on-demand dynamic bandwidth environments.

The value configured in the **ppp multilink links maximum** command specifies the maximum number of links allowed in a bundle. When more links than the number assigned with the **ppp multilink links maximum** command try to enter the bundle, MLP hangs up its dialer channels to reduce the number of links.

Member links that are not dialer lines are not affected by settings in the **ppp multilink links maximum** command. If a bundle contains a mix of leased and dialer links, the leased lines count against the total, but the leased lines remain as permanent member links and will do so even if the value specified for the maximum number of links is exceeded.

Use this command to fine-tune the **ppp multilink load-threshold** command settings and to prevent runaway expansion of a bundle when a low threshold is set.

Examples

The following example sets the maximum number of links to 50:

```
ppp multilink links maximum 50
```

Related Commands

Command	Description
ppp multilink links minimum	Specifies the preferred minimum number of links in an MLP bundle.
ppp multilink load-threshold	Enables MLP to monitor traffic load and prompt dialer capability to adjust bandwidth to fit the load.
ppp multilink mrru	Configures the MRRU value negotiated on an MLP bundle.

ppp multilink links minimum

To specify the preferred minimum number of links in a Multilink PPP (MLP) bundle, use the **ppp multilink links minimum** command in interface configuration mode. To reset the default value, use the **no** form of this command.

ppp multilink links minimum *links* [**mandatory**]

no ppp multilink links minimum

Syntax Description

links	Minimum number of links. Valid values range from 0 to 255. The default is 0.
mandatory	(Optional) Specifies that the minimum number of links configured with the *links* argument is required to establish and maintain the Network Control Protocol (NCP) for the bundle.

Command Default

0 links

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced as **multilink min-links**.
12.1(11b)E	The **mandatory** keyword was added to the **multilink min-links** command.
12.2	The **multilink min-links** command was replaced by the **ppp multilink links minimum** command. The **multilink min-links** command was also accepted by the command-line interpreter in Cisco IOS Release 12.2.
12.2(13)T	Support was added for the **mandatory** keyword, and the range of valid values for the *links* argument was changed from 0 to 255 to 0 to 64.
12.2(14)S	This command, as modified in Cisco IOS Release 12.2(13)T, was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)B	This command, as modified in Cisco IOS Release 12.2(13)T, was integrated into Cisco IOS Release 12.2(15)B. Support was added for the Cisco 7401ASR and the Cisco 6400 series.
12.3(8)T	The range of valid values for the *links* argument was changed from 0 to 64 to 0 to 255.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

This command affects only dial-on-demand dynamic bandwidth environments.

The value configured for the *links* argument specifies the minimum number of links that MLP will try to keep in a bundle. If a bundle contains fewer links than the number specified by the *links* argument, and there is a means to establish additional channels (for example, available dialer channels), then MLP

attempts to increase the number of links up to the specified limit. MLP attempts to dial up additional links to obtain the number specified by the *links* argument, even if the load does not exceed the load threshold.

If the **mandatory** keyword is configured, the minimum number of links specified by the *links* argument must be in the bundle. Whenever a link is added to or removed from the bundle, the number of links is checked against the specified minimum number. If the number of links in the bundle falls below the specified minimum, all NCPs will be disabled for the bundle. NCPs will be established if the number of links meets the specified minimum.

If the **dialer max-call** command is configured, MLP will not exceed its value even if the **ppp multilink links maximum** command is configured for a higher value. This restriction does not affect the number of links that you can configure; rather it affects what happens at run time.

Examples

The following example sets the minimum number of links to 12:

```
ppp multilink links minimum 12
```

The following example sets the minimum number of links to 4 and specifies that the bundle must have at least four links to establish and maintain NCPs:

```
ppp multilink links minimum 4 mandatory
```

Related Commands

Command	Description
dialer max-call	Specifies the maximum number of calls to a remote destination that can be up at any one time for a dialer profile.
ppp multilink links maximum	Limits the maximum number of links that MLP can dial for dynamic allocation.

ppp multilink load-threshold

To enable Multilink PPP (MLP) to monitor traffic load and prompt dialer capability to adjust bandwidth to fit the load, use the **ppp multilink load-threshold** command in interface configuration mode. To disable this function, use the **no** form of this command.

ppp multilink load-threshold *load-threshold* [**outbound | inbound | either**]

no ppp multilink load-threshold *load-threshold* [**outbound | inbound | either**]

Syntax Description

load-threshold	Load threshold at which to consider adding or dropping a link, expressed as a value in the range from 1 to 255. A value of 255 indicates a 100 percent load. A value of 1 is a special case indicating any load at all; MLP will add as many links as it can, ignoring the actual traffic load.
outbound	(Optional) Only the outbound (transmit) traffic load is examined.
inbound	(Optional) Only the inbound (receive) traffic load is examined.
either	(Optional) Either the transmit traffic load or the receive traffic load can trigger a link addition or subtraction.

Command Default

No active dynamic bandwidth mechanisms. If a *load-threshold* argument is configured without any of the optional keywords, the link defaults to examining outbound traffic load (**outbound**).

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced as **multilink load-threshold**.
12.2	This command was changed to **ppp multilink load-threshold**. The **multilink load-threshold** command was accepted by the command-line interpreter through Cisco IOS Release 12.2.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

The **dialer load-threshold** command is generally configured instead of the **ppp multilink load-threshold** command, and MLP inherits the values set by the **dialer load-threshold** command when a bundle configuration is taken from a dialer interface.

Use the **ppp multilink load-threshold** command for dynamic bandwidth (dial-on-demand) systems in which MLP will need to dial additional links as needed to increase the bandwidth of a connection. When the load on the bundle interface exceeds the set value, links are added. When the load on the bundle interface drops below the set value, links are dropped.

Examples

The following example sets the MLP inbound load threshold to 10:

```
ppp multilink load-threshold 10 inbound
```

Related Commands

Command	Description
dialer load-threshold	Configures bandwidth on demand by setting the maximum load before the dialer places another call to a destination.
ppp multilink links maximum	Limits the maximum number of links that MLP can dial for dynamic allocation.
ppp multilink links minimum	Specifies the preferred minimum number of links in an MLP bundle.
ppp multilink mrru	Configures the MRRU value negotiated on an MLP bundle.

ppp multilink mrru

To configure the maximum receive reconstructed unit (MRRU) value negotiated on a Multilink PPP (MLP) bundle, use the **ppp multilink mrru** command in interface configuration mode. To remove the configured MRRU, use the **no** form of this command.

ppp multilink mrru [**local | remote**] *mrru-value*

no ppp multilink mrru [local | remote] *mrru-value*

Syntax Description

local	(Optional) Configures the local MRRU value.
remote	(Optional) Configures the minimum value that the software will accept from the peer when it advertises its MRRU.
mrru-value	MRRU value, in bytes. Valid value range is 128 to 16384.

Command Default

The default values for the local MRRU are the value of the multilink group interface maximum transmission unit (MTU) for multilink group members, and 1524 bytes for all other interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.0(28)S	This command was integrated into Cisco IOS Release 12.0(28)S.
12.2(27)SB	This command was integrated into Cisco IOS Release 12.2(27)SB.
12.2(28)S	This command was integrated into Cisco IOS Release 12.2(28)S.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.

Usage Guidelines

This command allows the MRRU value to be configured on MLP interfaces and member links. This command is useful for interfaces running an application such as IP Security (IPsec), where the addition of the IPsec header causes the packet to exceed the 1500-byte MTU of a typical IP packet.

When using a large-bundle interface MTU size, you must ensure that the individual frames-per-fragment size passed to the link interfaces is not greater than the link interface MTU setting or the peer MRRU setting. This size limit can be achieved in one of the following two ways:

- Configure the link interface MTU setting appropriately.
- Configure fragmentation such that the link MTU settings will never be violated.

When MLP is configured, several physical interfaces can constitute one logical connection to the peer. To represent the logical connection, software provides a logical interface, often called the bundle interface. This interface will have the IP address, for instance, and the MTU setting of the interface that

IP uses when it is deciding whether to fragment an IP datagram that needs to be forwarded. The physical interfaces simply forward individual MLP fragments or frames that are given to them by the bundle interface.

The result of having to decide whether to fragment a packet is that, whereas with simple PPP the interface MTU must not exceed the peer's MRRU, with MLP the MTU size of the bundle interface must not exceed the MRRU setting of the peer. The MRRU settings on both sides need not be equal, but the "must not exceed" rule just specified must be followed; otherwise a system might send several fragments that, when reconstructed as a frame, will be too large for the peer's receive buffer.

Once you configure the MRRU on the bundle interface, you enable the router to receive large reconstructed MLP frames. You may want to configure the bundle MTU so that the router can send large MLP frames, although it is not strictly necessary. The maximum recommended value for the bundle MTU is the value of the peer's MTU. The software will automatically reduce the bundle interface MTU if necessary to avoid violating the peer's MRRU.

When the bundle interface MTU is tuned to a higher number, then depending upon the fragmentation configuration, the link interface may be given larger frames to send. There are two possible solutions to this problem, as follows:

- Ensure that fragmentation is performed such that fragments are sized less than the link interface MTU (refer to the command pages for the **ppp multilink fragment disable** and **ppp multilink fragment delay** commands for more information about packet fragments).
- Configure the MTUs of the link interfaces such that they can send the larger frames.

Note Be careful when configuring MLP MRRU negotiation in a virtual private dialup network (VPDN) environment when an L2TP network server (LNS) is not running Cisco IOS Release 12.3(7)T. The software performs strict matching on the MRRU values in earlier versions of Cisco IOS software.

Examples

The following example shows how to configure MRRU negotiation on a virtual template with synchronous serial interfaces. The example also applies to asynchronous serial interfaces.

```
multilink virtual-template 1
!
interface virtual-template 1
 ip address 10.13.1.1 255.255.255.0
 mtu 1600
!
interface serial 0/0
 ppp multilink
 ppp multilink mrru local 1600
 mtu 1600
!
interface serial 0/1
 ppp multilink
 ppp multilink mrru local 1600
 mtu 1600
```

The following example shows how to configure MRRU negotiation on multilink groups:

```
interface multilink 10
 ip address 10.13.1.1 255.255.255.0
 ppp multilink mrru local 1600
 mtu 1600
!
```

```
interface serial 0/0
 ppp multilink
 multilink-group 10
 mtu 1600
!
interface serial 0/1
 ppp multilink
 multilink-group 10
 mtu 1600
```

The following example shows how to configure MRRU negotiation on dialer interfaces:

Note Dialer interfaces are not supported on the Cisco 7600 series router.

```
interface dialer 1
 ip address 10.13.1.1 255.255.255.0
 encapsulation ppp
 dialer remote-name 2610-2
 dialer idle-timeout 30 inbound
 dialer string 5550101
 dialer pool 1
 dialer-group 1
 no cdp enable
 ppp multilink
 ppp multilink mrru local 1600
```

Related Commands

Command	Description
encapsulation ppp	Sets the PPP encapsulation method.
interface dialer	Defines a dialer rotary group.
mtu	Adjusts the maximum packet size or MTU size.
multilink virtual-template	Specifies a virtual template from which the specified MLP bundle interface can clone its interface parameters.
ppp multilink	Enables MLP on an interface.
ppp multilink fragment delay	Specifies a maximum time for the transmission of a packet fragment on an MLP bundle.
ppp multilink fragment disable	Disables packet fragmentation.
ppp multilink fragmentation	Sets the maximum number of fragments a packet will be segmented into before being sent over the bundle.
ppp multilink group	Restricts a physical link to joining only a designated multilink-group interface.
ppp multilink interleave	Enables MLP interleaving.

ppp multilink multiclass

To enable Multiclass Multilink PPP on an interface, use the **ppp multilink multiclass** command in interface configuration mode. To disable Multiclass Multilink PPP, use the **no** form of this command.

ppp multilink multiclass

no ppp multilink multiclass

Syntax Description

This command has no arguments or keywords.

Command Default

Multiclass Multilink PPP is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(8)YN	This command was enhanced with quality of service (QoS) features for the following platforms: Cisco 1720, Cisco 1750, Cisco 1751, Cisco 1760, Cisco 2610XM through Cisco 2651XM, Cisco 3640A, Cisco 3640, and Cisco 3660.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T for the following platforms: Cisco 1721, Cisco 2610 through Cisco 2651, Cisco 2610XM through Cisco 2651XM, Cisco 2691, Cisco 3620, and Cisco 3660.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

This command applies only to interfaces that use PPP encapsulation.

Multiclass Multilink PPP and PPP reliable links do not work together.

When the **ppp multilink multiclass** command is used, the first channel will negotiate the appropriate Network Control Protocol (NCP) layers (such as the IP Control Protocol and IPX Control Protocol), but subsequent links will negotiate only the link control protocol and Multiclass Multilink PPP. NCP layers do not get negotiated. The **dialer load-threshold** command enables a rotary group to bring up additional links and to add them to a multilink bundle.

The **ppp multilink multiclass** command must be configured on each link that will be joining the bundle (that is, on member links, not on the bundle interface itself). Failure to configure this command could result in the peer refusing to allow mismatched links to join the bundle. The first link to join the bundle will determine whether Multiclass Multilink PPP is in effect for the bundle. Each subsequent link must negotiate the same Multiclass Multilink PPP parameters in order to join the bundle. In the case of PPP over ATM (PPPoA) or PPP over Frame Relay (PPPoFR), the command is entered on the virtual template.

When this command is configured (and assuming that the peer also supports and is configured for multiclass interleaving), interleaved packets are assigned sequence numbers so that they are kept in order at the receiving end. Without this command, interleaved packets are sent without multilink headers and are subject to reordering when sent over parallel links.

Examples

The following partial example shows the configuration for a dialer for Multiclass Multilink PPP; it does not show the configuration of the physical interfaces:

```
interface Dialer0
 ip address 10.0.0.2 255.0.0.0
 encapsulation ppp
 dialer in-band
 dialer idle-timeout 500
 dialer map ip 10.0.0.1 name router broadcast 81012345678901
 dialer load-threshold 30 either
 dialer-group 1
 ppp authentication chap
 ppp multilink
 ppp multilink multiclass
```

The following example shows a configuration that enables multilink PPP interleaving and Multiclass Multilink PPP on a dialer interface that controls a rotary group of BRI interfaces. This configuration permits IP packets to trigger calls.

```
interface BRI 0
 description connected into a rotary group
 encapsulation ppp
 dialer rotary-group 1
!
interface BRI 1
 no ip address
 encapsulation ppp
 dialer rotary-group 1
!
interface BRI 2
 encapsulation ppp
 dialer rotary-group 1
!
interface BRI 3
 no ip address
 encapsulation ppp
 dialer rotary-group 1
!
interface BRI 4
 encapsulation ppp
 dialer rotary-group 1
!
interface Dialer 0
 description Dialer group controlling the BRIs
 ip address 10.1.1.1 255.255.255.0
 encapsulation ppp
 dialer map ip 10.1.1.2 name router 14802616900
 dialer-group 1
 ppp authentication chap
! Enables Multilink Multiclass PPP interleaving on the dialer interface and reserves
! a special queue.
 ppp multilink
 ppp multilink multiclass
 ppp multilink interleave
 ip rtp reserve 32768 20 1000
! Keeps fragments of large packets small enough to ensure delay of 20 ms or less.
```

```
 ppp multilink fragment delay 20
dialer-list 1 protocol ip permit
```

The following example shows the configuration for defining a virtual interface template that enables Multilink PPP interleaving and a maximum real-time traffic delay of 20 milliseconds. The bundle interface will be a virtual access interface cloned from the virtual template. Multiclass Multilink PPP is then configured on a member link, Serial0.

```
interface virtual-template 1
 ip unnumbered ethernet 0
 ppp multilink
 ppp multilink interleave
 ppp multilink fragment delay 20
 ip rtp interleave 32768 20 1000
!
multilink virtual-template 1
!
interface Serial0
 encapsulation ppp
 ppp authentication chap
 ppp multilink
 ppp multilink multiclass
```

The following example shows the configuration for Multilink PPP interleaving and a maximum real-time traffic delay of 20 milliseconds on a multilink interface. Multiclass Multilink PPP is then configured on a member link, Serial1, and the member link is restricted to joining only the designated multilink group interface.

```
interface Multilink1
 ip address 10.2.3.4 255.255.255.0
 ppp multilink
 ppp multilink interleave
 ppp multilink fragment delay 20
!
interface Serial1
 encapsulation ppp
 ppp authentication chap
 ppp multilink
 ppp multilink multiclass
 ppp multilink group 1
```

The following example shows the configuration for interleaving on the bundle interface while multiclass is configured on the member links (in this case, any virtual access interfaces that are cloned from the virtual template):

```
interface Multilink1
 ip address 10.0.0.50 255.255.255.240
 fair-queue
 ppp multilink
 ppp multilink fragment-delay 10
 ppp multilink interleave
 multilink-group 2
!
interface Virtual-Template1
 no ip address
 ppp multilink
 ppp multilink multiclass
 multilink-group 2
```

Related Commands

Command	Description
dialer-group	Controls access by configuring an interface to belong to a specific dialing group.
dialer load-threshold	Configures bandwidth on demand by setting the maximum load before the dialer places another call to a destination.
encapsulation ppp	Enables PPP encapsulation.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication is selected on the interface.
ppp multilink	Enables MLP on an interface.
ppp multilink fragment-delay	Specifies a maximum size in units of time for packet fragments on a multilink PPP bundle.
ppp multilink group	Restricts a physical link to joining only a designated multilink-group interface.
ppp multilink interleave	Enables interleaving of packets among the fragments of larger packets on a multilink PPP bundle.
ppp multilink mrru	Configures the MRRU value negotiated on a multilink PPP bundle.
ppp multilink multiclass local	Configure the multiclass multilink PPP multilink header format option when negotiating class of service with a peer.
ppp multilink multiclass remote	Causes multilink to negotiate the multilink header format option if the peer requests it, and to use multiple multilink classes on transmitted packets (potentially including multilink headers on interleaved packets) if the option is negotiated.
show ppp multilink	Displays bundle information for the multilink PPP bundles.

ppp multilink multiclass local

To configure the multiclass multilink PPP multilink header format option when negotiating class of service with a peer, use the **ppp multilink multiclass local** command in interface configuration mode. To disable a local multilink header format option, use the **no** form of the command.

ppp multilink multiclass local {**request** [**initial** *init-value*] [**maximum** *max-value*] | **allow** [**maximum** *max-value*] | **forbid**}

no ppp multilink multiclass {**local** {**request** [**initial** *init-value*] [**maximum** *max-value*] | **allow** [**maximum** *max-value*] | **forbid**}

Syntax Description

request	Signals the Link Control Protocol (LCP) to request the multilink header format (multiclass) option when the interface is negotiating with the peer.
initial *init-value*	(Optional) The initial number of multilink classes to request, that is, the number of classes the multilink is initially prepared to accept in the receive path. The range is 1 to 16. The default is 2.
maximum *max-value*	(Optional) The maximum number of classes that can be requested, that is, the maximum number of classes the multilink will support in the receive path. Range is 2 to 16, except on distributed platforms, where the value is limited by platform capability). The default is 16.
allow	Causes the LCP to initially omit the multilink header format (multlink) option when negotiating with the peer, but to request the option in subsequent requests if the peer includes it in a configure-nak message.
forbid	Causes the LCP to omit the multilink header format (multiclass) option when negotiating with the peer.

Command Default

Initially omit the multilink header format option when negotiating with the peer, but request the option in a maximum of 16 subsequent requests when the peer includes it in a configure-nak message.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(31)SB2	This command was introduced on the Cisco 10000 series platform.

Usage Guidelines

This command applies only to interfaces that use PPP encapsulation.

Use this command paired with the **ppp multilink multiclass remote** command to configure the multiclass multilink PPP multilink header format option when negotiating with a peer. These commands extend the multiclass multilink PPP transmit logic to allow up to 16 transmit and receive classes, and up to 16 classes that can be negotiated with the peer. The **ppp multilink multiclass local** and **ppp multilink multiclass remote** commands use PPP link fragmentation and interleaving (LFI) to apply multilink headers to interleaved packets, which allows the packets to be kept in sequence when transmitted over multiple parallel links within a given multilink bundle.

MLP and PPP reliable links do not work together.

The **dialer load-threshold** command enables a rotary group to bring up additional links and to add them to a multilink bundle.

The **ppp multilink multiclass** command must be configured on each link that will be joining the bundle or on the multilink interface itself (members of the multilink group inherit any PPP configuration that is done on the multilink group master). Failure to configure this command could result in the peer refusing to allow mismatched links to join the bundle. The first link to join the bundle will determine whether multilink PPP is in effect for the bundle. Each subsequent link must negotiate the same multilink PPP parameters in order to join the bundle.

In the case of PPP over ATM (PPPoA) or PPP over Frame Relay (PPPoFR), the command is entered on the virtual template.

Effective with Cisco IOS Release 12.2(31)SB2, this command can be used only on the Cisco 10000 series platform.

Examples

The following example shows how to configure a multilink bundle for up to four receive classes and at least four transmit classes:

```
interface Multilink9
 ip address 10.0.0.161 255.255.255.240
 ppp multilink
 ppp multilink interleave
 ppp multilink group 9
 ppp multilink fragment delay 20
 ppp multilink multiclass local request maximum 4
 ppp multilink multiclass remote apply minimum 4
 no cdp enable
```

The following example shows how to configure a multilink bundle to not use multiple classes but allows the peer to request the option and transmit up to four classes when needed:

```
interface Multilink9
 ip address 10.0.0.161 255.255.255.240
 ppp multilink
 ppp multilink interleave
 ppp multilink group 9
 ppp multilink fragment delay 20
 ppp multilink multiclass local allow maximum 4
 ppp multilink multiclass remote ignore
 no cdp enable
```

The following example shows how to configure a multilink bundle to not use multiple classes, but allows the peer to request the option and inform the peer that the option is supported, allowing for up to four receive classes:

```
interface Multilink9
 ip address 10.0.0.161 255.255.255.240
 ppp multilink
 ppp multilink interleave
 ppp multilink group 9
 ppp multilink fragment delay 20
 ppp multilink multiclass local request initial 1 maximum 4
 ppp multilink multiclass remote ignore
 no cdp enable
```

The following example shows how to completely disable multiclass multilink PPP, rejecting the header and declining to allow the peer to transmit multiple classes:

```
interface Multilink9
 ip address 10.0.0.161 255.255.255.240
 ppp multilink
 ppp multilink interleave
 ppp multilink group 9
 ppp multilink fragment delay 20
 ppp multilink multiclass local forbid
 ppp multilink multiclass remote reject
 no cdp enable
```

Related Commands

Command	Description
dialer-group	Controls access by configuring an interface to belong to a specific dialing group.
dialer load-threshold	Configures bandwidth on demand by setting the maximum load before the dialer places another call to a destination.
encapsulation ppp	Enables PPP encapsulation.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication is selected on the interface.
ppp multilink	Enables MLP on an interface.
ppp multilink fragment delay	Specifies a maximum size in units of time for packet fragments on an multilink PPP bundle.
ppp multilink group	Restricts a physical link to joining only a designated multilink-group interface.
ppp multilink interleave	Enables interleaving of packets among the fragments of larger packets on an multilink PPP bundle.
ppp multilink mrru	Configures the MRRU value negotiated on an multilink PPP bundle.
ppp multilink multiclass	Enables multiclass multilink PPP on an interface.
ppp multilink multiclass remote	Causes multilink to negotiate the multilink header format option if the peer requests it, and to use multiple multilink classes on transmitted packets (potentially including multilink headers on interleaved packets) if the option is negotiated.
show ppp multilink	Displays bundle information for the multilink PPP bundles.

ppp multilink multiclass remote

To configure the multiclass multilink PPP multilink header format option when a peer requests class of service, use the **ppp multilink multiclass remote** command in interface configuration mode. To disable a remote multilink header format option, use the **no** form of the command.

ppp multilink multiclass remote {**apply** [**minimum** *min-value*] | **reject** | **ignore**}

no ppp multilink multiclass remote {**apply** [**minimum** *min-value*] | **reject** | **ignore**}

Syntax Description

apply minimum *min-value*	Causes the multilink: • To negotiate the multilink header format option if the peer requests it and attempts to induce the peer to request the option by including it in a configure-nak message if it does not. • To use multiple multilink classes on transmitted packets (potentially including multilink headers on interleaved packets) if the option is negotiated.
minimum *min-value*	Indicates the minimum number of classes that the peer is expected to request. This value indicates the number of classes the multilink will need in the transmit path. The range is 2 to 16 (except on distributed platforms, where the value is limited by platform capability). The default is 2.
reject	Causes the multilink to reject the option if the peer requests it.
ignore	Causes the multilink to acknowledge the multilink header format option if the peer requests it, but multiple classes will not be used. This is the default setting when a multiclass is not configured.

Command Default

Multilink PPP is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(31)SB2	This command was introduced on the Cisco 10000 series platform.

Usage Guidelines

This command applies only to interfaces that use PPP encapsulation.

Use this command paired with the **ppp multilink multiclass local** command to configure the multiclass multilink PPP multilink header format option when negotiating with a peer. These commands extend the multiclass multilink PPP transmit logic to allow up to 16 transmit and receive classes, and up to 16 classes that can be negotiated with the peer. The **ppp multilink multiclass local** and **ppp multilink multiclass remote** commands use PPP link fragmentation and interleaving (LFI) to apply multilink headers to interleaved packets, which allows the packets to be kept in sequence when transmitted over multiple parallel links within a given multilink bundle.

MLP and PPP reliable links do not work together.

The **dialer load-threshold** command enables a rotary group to bring up additional links and to add them to a multilink bundle.

The **ppp multilink multiclass** command must be configured on each link that will be joining the bundle or on the multilink interface itself (members of the multilink group inherit any PPP configuration that is done on the multilink group master). Failure to configure this command could result in the peer refusing to allow mismatched links to join the bundle. The first link to join the bundle will determine whether multilink PPP is in effect for the bundle. Each subsequent link must negotiate the same multilink PPP parameters in order to join the bundle.

In the case of PPP over ATM (PPPoA) or PPP over Frame Relay (PPPoFR), the command is entered on the virtual template.

Effective with Cisco IOS Release 12.2(31)SB2, this command can be used only on the Cisco 10000 series platform.

Examples

The following example shows how to configure a multilink bundle for up to four receive classes and at least four transmit classes:

```
interface Multilink9
 ip address 10.0.0.161 255.255.255.240
 ppp multilink
 ppp multilink interleave
 ppp multilink group 9
 ppp multilink fragment delay 20
 ppp multilink multiclass local request maximum 4
 ppp multilink multiclass remote apply minimum 4
 no cdp enable
```

The following example shows how to configure a multilink bundle to not use multiple classes but allows the peer to request the option and transmit up to four classes when needed:

```
interface Multilink9
 ip address 10.0.0.161 255.255.255.240
 ppp multilink
 ppp multilink interleave
 ppp multilink group 9
 ppp multilink fragment delay 20
 ppp multilink multiclass local allow maximum 4
 ppp multilink multiclass remote ignore
 no cdp enable
```

The following example shows how to configure a multilink bundle to not use multiple classes, but allows the peer to request the option and inform the peer that the option is supported, allowing for up to four receive classes:

```
interface Multilink9
 ip address 10.0.0.161 255.255.255.240
 ppp multilink
 ppp multilink interleave
 ppp multilink group 9
 ppp multilink fragment delay 20
 ppp multilink multiclass local request initial 1 maximum 4
 ppp multilink multiclass remote ignore
 no cdp enable
```

The following example shows how to configure a multilink bundle to not use multiple classes, but allows the peer to request the option and inform the peer that the option is supported, allowing for up to four receive classes:

```
interface Multilink9
 ip address 10.0.0.161 255.255.255.240
 ppp multilink
 ppp multilink interleave
 ppp multilink group 9
 ppp multilink fragment delay 20
 ppp multilink multiclass local request initial 1 maximum 4
 ppp multilink multiclass remote ignore
 no cdp enable
```

The following example shows how to completely disable multiclass multilink PPP, rejecting the header and declining to allow the peer to transmit multiple classes:

```
interface Multilink9
 ip address 10.0.0.161 255.255.255.240
 ppp multilink
 ppp multilink interleave
 ppp multilink group 9
 ppp multilink fragment delay 20
 ppp multilink multiclass local forbid
 ppp multilink multiclass remote reject
 no cdp enable
```

Related Commands

Command	Description
dialer-group	Controls access by configuring an interface to belong to a specific dialing group.
dialer load-threshold	Configures bandwidth on demand by setting the maximum load before the dialer places another call to a destination.
encapsulation ppp	Enables PPP encapsulation.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication is selected on the interface.
ppp multilink	Enables MLP on an interface.
ppp multilink fragment delay	Specifies a maximum size in units of time for packet fragments on a multilink PPP bundle.
ppp multilink group	Restricts a physical link to joining only a designated multilink-group interface.
ppp multilink interleave	Enables interleaving of packets among the fragments of larger packets on a multilink PPP bundle.
ppp multilink mrru	Configures the MRRU value negotiated on a multilink PPP bundle.
ppp multilink multiclass	Enables multiclass multilink PPP on an interface.
ppp multilink multiclass local	Configure the multiclass multilink PPP multilink header format option when negotiating class of service with a peer.
show ppp multilink	Displays bundle information for the multilink PPP bundles.

ppp multilink ncp sequenced

To control whether Network Control Protocol (NCP) packets are sent with or without multilink headers, use the **ppp multilink ncp sequenced** command in interface configuration mode. RFC 1990 requires that compliant peer implementations be able to receive NCP packets with or without the presence of multilink headers. The **ppp multilink ncp sequenced** command provides support for those remote peers not currently compliant with RFC 1990. To disable the control of multilink headers in NCP packets, use the **no** form of this command.

ppp multilink ncp sequenced {**if-needed | always | never**}

no ppp multilink ncp sequenced

Syntax Description

if-needed	Specifies that NCP packets are sent with multilink headers only if your bundle has multiple links, or you have configured Link Fragmentation and Interleaving (LFI).
always	Specifies that NCP packets are always sent with multilink headers. Use this keyword for any remote peer that requires multilink headers in NCP packet for processing.
never	Specifies that NCP packets are never sent with multilink headers. Use this keyword for any remote peer that requires NCP packets without multilink headers for processing.

Command Default

NCP packets are sent on an if-needed basis.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(31)SB2	This command was introduced.

Usage Guidelines

This command applies only to interfaces used for multilink bundles (multilink, virtual-templates, or dialer interfaces).

You must specify one keyword, unless you are using the **no** form of this command.

Some remote peers require the presence of multilink headers for NCP packet processing, while other remote peers require that NCP packets do not have multilink headers. Using the **ppp multilink ncp sequenced** command, you can control the presence of multilink headers in NCP packets.

Use this command with the **if-needed** keyword if your remote peers are RFC 1990 compliant. The **if-needed** specifies that remote peers are able to process NCP regardless of the existence of multilink headers. The **always** keyword specifies that multilink headers will always appear in all NCP packets. Use the **always** keyword for any remote peer that requires multilink headers in NCP packet for processing.

The **never** keyword specifies that multilink headers will never appear in any NCP packet. Use the **never** keyword for any remote peer that requires NCP packets without multilink headers for processing.

The **no** form of this command to disables the control of multilink headers appearing in NCP packets.

Examples

```
The following example shows how to configure a remote peer which is unable to process NCP
packets that have multilink headers:

ppp multilink ncp sequenced never

The following example shows how to configure a remote peer which is unable to process NCP
packets that do not have multilink headers:

ppp multilink ncp sequenced always
```

Related Commands

Command	Description
ppp multilink	Enables Multilink PPP (MLP) on an interface and, optionally, enables Bandwidth Allocation Control Protocol (BACP) and its Bandwidth Allocation Protocol (BAP) subset for dynamic bandwidth allocation.
ppp multilink interleave	Enables interleaving of packets among the fragments of larger packets on an MLP bundle.
ppp multilink fragment delay	Specifies a maximum time for the transmission of a packet fragment on an MLP bundle.
ppp multilink fragment size	Specifies the maximum packet fragment size in bytes for an MLP link.

ppp multilink slippage

To define the constraints that set the Multilink PPP (MLP) reorder buffer size, use the **ppp multilink slippage** command in interface configuration mode. To remove the restriction, use the **no** form of this command.

ppp multilink slippage [**mru** *value* | **msec** *value*]

no ppp multilink slippage [**mru** *value* | **msec** *value*]

Syntax Description

mru *value*	Specifies the buffer limit is at least this many maximum receive units (MRUs) worth of data, in bytes. Valid values are 2 to 32.
msec *value*	Specifies the buffer limit is at least this many milliseconds worth of data. Valid range is 1 to 16000.

Defaults

The **mru** *value* default is 8 bytes.

There is no default for **msec** *value*.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.

Usage Guidelines

The slippage constraints are interface-level configuration commands, which may be placed on any interface or configuration source ultimately providing the configuration for a multilink bundle interface like “interface Multilink” and “interface dialer.”

Limits are on a “per-link” basis. For example, issuing **ppp multilink slippage mru 4** means that the total amount of data which is buffered by the bundle is 4 times the MRU times the number of links in the bundle.

The reassembly engine is also affected by the lost fragment timeout, which is configured using the **ppp timeout multilink lost-fragment** command.

The buffer limit derived from the slippage constraints implies a corresponding tolerated differential delay between the links. Since it does not make sense to be declaring a fragment lost due to a timeout when it is within the delay window defined by the slippage, the timeout will be dynamically increased as necessary so that it is never smaller than the delay value derived from the slippage parameters.

Examples

The following example shows the total amount of data buffered by the bundle is four times the MRU times the number of links in the bundle:

```
Router(config)# interface multilink 8
Router(config-if)# ip address 172.16.48.209 255.255.0.0
Router(config-if)# ppp multilink slippage mru 4

Router(config)# interface dialer8
Router(config-if)# encapsulation ppp
Router(config-if)# ip address 172.16.48.209 255.255.0.0
Router(config-if)# ppp multilink slippage mru 4
Router(config-if)# ppp multilink slippage msec 16000
```

The following example shows configuring Multilink PPP over serial interface links on a multilink group interface. In this example, there are two serial interfaces that are members of "interface multilink8". It is assumed that Serial2 interface has the bandwidth of 64kbps and Serial3 interface has the bandwidth of 128kbps. With these two serial links, interface Multilink8 will have a bandwidth equal to 64kbps plus 128kbps which equals 196 kbps or 24.5 kBps [b=bit, B=byte]. The interface Multilink8 is configured with **ppp multilink slippage msec 2000** and therefore buffers at least 2000 milliseconds worth of data (2000 ms * 24.5 kBps = 49000 bytes).

```
Router(config)# interface Multilink8
Router(config-if)# ip address 172.16.48.209 255.255.0.0
Router(config-if)# ppp multilink
Router(config-if)# ppp multilink slippage msec 2000
Router(config-if)# ppp multilink group 8

Router(config)# interface Serial2
Router(config-if)# no ip address
Router(config-if)# encapsulation ppp
Router(config-if)# ppp multilink group 8

Router(config)# interface Serial3
Router(config-if)# no ip address
Router(config-if)# encapsulation ppp
Router(config-if)# ppp multilink group 8
```

Related Commands

Command	Description
ppp multilink	Enables MLP on an interface and, optionally, enables dynamic bandwidth allocation.
ppp multilink fragment delay	Specifies a maximum time for the transmission of a packet fragment on a MLP bundle.
ppp multilink fragment disable	Disables packet fragmentation.
ppp multilink fragmentation	Sets the maximum number of fragments a packet will be segmented into before being sent over the bundle.
ppp multilink group	Restricts a physical link to joining only a designated multilink-group interface.
ppp multilink interleave	Enables MLP interleaving.
ppp multilink mrru	Configures the MRRU value negotiated on a MLP bundle.

ppp pap wait

To configure the router to delay the Password Authentication Protocol (PAP) authentication until after the peer has authenticated itself to the router, use the **ppp pap wait** command in interface configuration mode. To allow the router to immediately send out its PAP request once the authentication phase starts, use the **no** form of this command.

ppp pap wait

no ppp pap wait

Syntax Description

This command has no arguments or keywords.

Command Default

Immediate PAP request transmission enabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2T	This command was introduced.

Usage Guidelines

This command is used only when the call direction is call-in. The **ppp pap wait** command specifies that the router will not authenticate to a peer requesting PAP authentication until the peer has authenticated itself to the router. The **no** form of this command specifies that the router will immediately send out its PAP request once the authentication phase starts.

Examples

The following example specifies ISDN BRI number 0. The method of encapsulation on the interface is PPP. The following example disables the default, meaning that the router will immediately send out its PAP request once the authentication phase starts.

```
interface bri 0
 encapsulation ppp
 no ppp pap wait
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
ppp pap refuse	Refuses a peer request to authenticate remotely with PPP using PAP.
ppp pap sent-username	Reenables remote PAP support for an interface and uses the sent username and password in the PAP authentication request packet to the peer.

ppp pfc local

To configure protocol field compression (PFC) in configuration requests, use the **ppp pfc local** command in interface configuration mode. To return the router to the default for PCF handling, use the **no** form of this command.

ppp pfc local {**forbid** | **request**}

no ppp pfc local

Syntax Description

forbid	The PFC option is not sent in outbound configuration requests, and requests from a peer to add the PFC option are not accepted.
request	The PFC option is included in outbound configuration requests.

Command Default

PFC handling is automatically selected based on the type of link. For asynchronous links, the router responds as if the **request** keyword were selected and the router includes the PFC option in outbound configuration requests. For synchronous links, the router responds as if the **forbid** keyword were selected and the PFC option is not sent out in outbound configuration requests and requests from a peer to add the PFC option are not accepted.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(7)	This command was introduced.
12.2(15)B	This command was integrated into Cisco IOS Release 12.2(15)B.

Usage Guidelines

When PFC is negotiated during PPP negotiation, Cisco routers may compress the PPP protocol field from two bytes to one byte. The **ppp pfc local** command configures how a router handles PFC in its outbound configuration request and allows PFC to be disabled during PPP negotiation, thus allowing the HDLC framing and the protocol field to remain uncompressed.

Prior to the introduction of the **ppp pfc local** command, negotiation and use of PFC was entirely dependent upon the link type (synchronous or asynchronous) and was not under the independent control of a system administrator, and this is still the default. The **ppp pfc local** command allows the system administrator to control when PPP negotiates the HDLC address and PFC options during initial LCP negotiations, and how the results of the PPP negotiation are applied.

Note Using PFC can result in minor gains in effective bandwidth because they reduce the amount of framing overhead for each packet. However, using PFC changes the alignment of the network data in the frame, which in turn can impair the switching efficiency of the packets both at the local and remote ends of the connection. For these reasons, it is generally recommended that PFC not be enabled without carefully considering the potential results.

Examples

The following example shows how to configure a router to exclude the PFC option from its outbound configuration requests:

```
ppp pfc local forbid
```

Related Commands

Command	Description
ppp acfc remote	Configures the ACFC options received from a remote peer.
ppp acfc local	Configures the ACFC option in configuration requests.
ppp pfc remote	Configures the PFC option in configuration requests received from a remote peer.

ppp pfc remote

To configure how the protocol field compression (PFC) option in configuration requests is received from a remote peer, use the **ppp pfc remote** command in interface configuration mode. To return to the default for PFC handling, use the **no** form of this command.

ppp pfc remote {**apply** | **ignore** | **reject**}

no ppp pfc remote

Syntax Description

apply	PFC options are accepted and PFC may be performed on frames sent to the remote peer.
ignore	PFC options are accepted, but PFC is not performed on frames sent to the remote peer.
reject	PFC options are explicitly rejected.

Command Default

PFC handling is automatically selected based on the type of link, as follows: For asynchronous links, the router responds as if the **apply** keyword were selected and the router accepts PFC options received from a remote peer and PFC may be performed on frames sent to the remote peer. For synchronous links, the router responds as if the **ignore** keyword were selected and PFC options are accepted but PFC is not performed on frames sent to the remote peer.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(7)	This command was introduced.
12.2(15)B	This command was integrated into Cisco IOS Release 12.2(15)B.

Usage Guidelines

When PFC is negotiated during PPP negotiation, Cisco routers may compress the PPP protocol field from two bytes to one byte. The **ppp pfc remote** command allows PFC to be disabled during PPP negotiation, thus allowing the HDLC framing and the protocol field to remain uncompressed.

Prior to the introduction of the **ppp pfc remote** command, negotiation and use of PFC was entirely dependent upon the link type (synchronous or asynchronous) and was not under the independent control of a system administrator, and this is still the default. The **ppp pfc remote** command allows the system administrator to control when PPP negotiates the HDLC address and PFC options during initial LCP negotiations, and how the results of the PPP negotiation are applied.

Note Using PFC can result in minor gains in effective bandwidth because they reduce the amount of framing overhead for each packet. However, using PFC changes the alignment of the network data in the frame, which in turn can impair the switching efficiency of the packets both at the local and remote ends of the connection. For these reasons, it is generally recommended that PFC not be enabled without carefully considering the potential results.

Examples

The following example shows how to configure a router to explicitly reject PFC options from a remote peer:

```
ppp pfc remote reject
```

Related Commands

Command	Description
ppp acfc local	Configures the ACFC option in configuration requests.
ppp acfc remote	Configures the ACFC option in configuration requests received from a remote peer.
ppp pfc local	Configures the PFC option in configuration requests.

ppp quality

To enable Link Quality Monitoring (LQM) on a serial interface, use the **ppp quality** command in interface configuration mode. To disable LQM, use the **no** form of this command.

ppp quality *percentage*

no ppp quality

Syntax Description

percentage	Specifies the link quality threshold. Range is from 1 to 100.

Command Default

Command is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The percentages are calculated for both incoming and outgoing directions. The outgoing quality is calculated by comparing the total number of packets and bytes sent to the total number of packets and bytes received by the destination node. The incoming quality is calculated by comparing the total number of packets and bytes received to the total number of packets and bytes sent by the destination node.

If the link quality percentage is not maintained, the link is deemed to be of poor quality and is taken down. LQM implements a time lag so that the link does not bounce up and down.

Examples

The following example enables LQM on serial interface 2:

```
interface serial 2
 encapsulation ppp
 ppp quality 80
```

Related Commands

Command	Description
exec	Allows an EXEC process on a line.
keepalive	Sets the keepalive timer for a specific interface.

ppp reliable-link

To enable Link Access Procedure, Balanced (LAPB) Numbered Mode negotiation for a reliable serial link, use the **ppp reliable-link** command in interface configuration mode. To disable negotiation for a PPP reliable link on a specified interface, use the **no** form of the command.

ppp reliable-link

no ppp reliable-link

Syntax Description

This command has no arguments and keywords.

Command Default

Command is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Enabling LAPB Numbered Mode negotiation as a means of providing a reliable link does not guarantee that all connections through the specified interface will in fact use a reliable link. It guarantees only that the router will attempt to negotiate reliable link on this interface.

PPP reliable link can be used with PPP compression over the link, but it does not require PPP compression.

PPP reliable link does not work with Multilink PPP.

You can use the **show interface** command to determine whether LAPB has been established on the link. You can troubleshoot PPP reliable link by using the **debug lapb** command and the **debug ppp negotiations**, **debug ppp errors**, and **debug ppp packets** commands.

Examples

The following example enables PPP reliable link and predictor compression on BRI interface 0:

```
interface bri 0
 description Enables predictor compression on BRI 0
 ip address 172.16.1.1 255.255.255.0
 encapsulation ppp
 dialer map ip 172.16.1.2 name mymap 15550191357
 compress predictor
 ppp authentication chap
 dialer-group 1
 ppp reliable-link
```

Related Commands

Command	Description
compress	Configures compression for LAPB, PPP, and HDLC encapsulations.
debug lapb	Displays all traffic for interfaces using LAPB encapsulation.
debug ppp	Displays information on traffic and exchanges in an internetwork implementing the PPP.
show interfaces	Displays statistics for all interfaces configured on the router or access server.

ppp timeout aaa

To support the idle direction for the timeout value set by authentication, authorization, and accounting (AAA), use the **ppp timeout aaa** command in interface configuration mode. To remove this setting, use the **no** form of this command.

ppp timeout aaa [**inbound**]

no ppp timeout aaa [**inbound**]

Syntax Description

inbound	(Optional) Specifies that the AAA server can set the PPP idle timeout parameters only for inbound traffic.

Command Default

The command is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2T	This command was introduced.

Usage Guidelines

Use this command to reset the idle timer based on inbound traffic only set by AAA, and to support the idle direction for the timeout value set by AAA.

Examples

The following example uses a virtual template to set the idle timer by AAA only when inbound traffic is detected:

```
interface Virtual-Template1
 ppp timeout idle 1800
 timeout absolute 180
 ppp timeout aaa inbound
```

Related Commands

Command	Description
ppp timeout idle	Sets PPP idle timeout parameters, in seconds.

ppp timeout authentication

To set the PPP authentication timeout value, use the **ppp timeout authentication** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ppp timeout authentication *seconds*

no ppp timeout authentication

Syntax Description

seconds	Maximum time, in seconds, to wait for a response to an authentication packet. Valid seconds are from 0 to 255 seconds. The default is 10 seconds.

Command Default

10 seconds

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

Cisco 10000 Series Router

To keep an L2TP network server (LNS) from timing out a PPP authentication process, we recommend that you configure the PPP authentication timeout to 100 seconds.

Examples

The following example changes the time to wait for a response to an authentication packet to 15 seconds:

```
ppp timeout authentication 15
```

Related Commands

Command	Description
ppp timeout retry	Sets PPP timeout retry parameters.

ppp timeout idle

To set the PPP timeout idle parameter, use the **ppp timeout idle** command in interface configuration mode. To reset the timeout value, use the **no** form of this command.

ppp timeout idle *seconds*

no ppp timeout idle *seconds*

Syntax Description

seconds	Line idle time, in seconds, allowed before disconnecting the line. Acceptable range is platform dependent.

Command Default

No PPP timeout idle parameter is set.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3	This command was introduced as **ppp idle-timeout**.
12.2	This command was modified. The command name was changed to **ppp timeout idle**.

Usage Guidelines

The **ppp timeout idle** command is used mainly on dialup interfaces and other temporary circuits to control how long the connection can be idle before it is terminated. All user traffic will reset the idle timer; however, nonnetwork traffic such as PPP control packets will not reset the timer. Also note that the dialer subsystem supports an alternate idle link detection mechanism that can be used instead of or with this PPP idle link detection mechanism.

The **ppp timeout idle** command name replaces the name **ppp idle-timeout**. The CLI will accept the **ppp timeout idle** name in Cisco IOS Release 12.2 and later releases.

Examples

The following example shows how to set the idle timer to 15 seconds:

```
ppp timeout idle 15
```

Related Commands

Command	Description
absolute-timeout	Sets the interval for closing user connections on a specific line or port.
dialer fast-idle (interface)	Specifies the amount of time that a line for which there is contention will stay idle before it is disconnected and the competing call is placed.

Command	Description
dialer hold-queue	Allows interesting outgoing packets to be queued until a modem connection is established.
dialer idle-timeout (interface)	Specifies the idle time before the line is disconnected.

ppp timeout idle (template)

To set PPP idle timeout parameters on a virtual template interface, use the **ppp timeout idle** command in interface configuration mode. To reset the time value, use the **no** form of this command.

ppp timeout idle *seconds*

no ppp timeout idle *seconds*

Syntax Description

seconds	Line idle time, in seconds, allowed before disconnecting the line.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(4)T	This command was introduced for virtual template interfaces.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300, Cisco AS5400 and Cisco AS5800.

Usage Guidelines

This version of the **ppp timeout idle** command is used on virtual template interfaces to control how long the connection can be idle before it is terminated.

Examples

The following example sets the PPP idle timeout to 45 seconds in virtual template interface 1:

```
interface Virtual-Template1
 ip unnumbered Loopback1
 peer default ip address pool local_pool
 ppp authentication chap callin
 ppp chap hostname name
 ppp timeout idle 45
 ip idle-group 101 in
 ip idle-group 102 in
 ppp multilink
```

Related Commands

Command	Description
absolute-timeout	Sets the interval for closing user connections on a specific line or port.
dialer fast-idle (interface configuration)	Specifies the amount of time that a line for which there is contention will stay idle before it is disconnected and the competing call is placed.

Command	Description
dialer hold-queue	Allows interesting outgoing packets to be queued until a modem connection is established.
dialer idle-timeout (template)	Specifies the idle time on a virtual template interface before the line is disconnected.

ppp timeout multilink link add

To limit the amount of time for which Multilink PPP (MLP) waits for a call to be established, use the **ppp timeout multilink link add** command in interface configuration mode. To remove the value, use the **no** form of this command.

ppp timeout multilink link add *seconds*

no ppp timeout multilink link add

Syntax Description

seconds	Wait period, in seconds, in the range from 1 to 65535 seconds.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

When MLP needs to increase the bandwidth of a bundle, it attempts to bring up an additional link by requesting that the dialer system place a call to the peer system, or if the Bandwidth Allocation Protocol (BAP) is used, the call may also be done by requesting that the peer system make the call. BAP can be used to either make the call or request that the peer system make the call, depending upon the configuration. The time value specified with the **ppp timeout multilink link add** command determines how long MLP waits for that call to be established. If a new link does not join the bundle within the specified time, it is assumed that the call failed, and the call is attempted again.

If there are not enough links to carry the load, and the call succeeds in less than the time specified with the **ppp timeout multilink link add** command, MLP can immediately request another link. The time value specified with the **ppp timeout multilink link add** command prevents flooding the dialer system with call requests because not enough time was provided for prior requests to finish.

If the **ppp timeout multilink link add** command is not configured but the **dialer wait-for-carrier-time** command is, MLP will use the time value set with the **dialer wait-for-carrier-time** command. If neither command is configured, MLP uses a default value of 30 seconds.

This command is used with dynamic bandwidth (dial-on-demand) bundles.

Examples

The following example sets the call timeout period to 45 seconds:

```
ppp timeout multilink link add 45
```

Related Commands

Command	Description
dialer wait-for-carrier-time (interface)	Specifies the length of time the interface waits for a carrier.
ppp timeout multilink link remove	Sets a timer that determines how long MLP waits to drop a link when traffic load goes below the configured load threshold.

ppp timeout multilink link remove

To set a timer that determines how long Multilink PPP (MLP) waits to drop a link when traffic load goes below the configured load threshold, use the **ppp timeout multilink link remove** command in interface configuration mode. To remove the value, use the **no** form of this command.

ppp timeout multilink link remove *seconds*

no ppp timeout multilink link remove

Syntax Description

seconds	Threshold wait period, in seconds, in the range from 1 to 65535 seconds.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

When traffic load goes below the threshold set with the **ppp multilink load-threshold** command, MLP waits for the time set with the **ppp timeout multilink link remove** command and, if the load still remains below that threshold, drops the link to reduce bandwidth.

MLP will reduce bandwidth but never remove the last link in a bundle. The complete severing of a connection is controlled by the idle timer value specified in the **dialer idle-timeout** command; however, the idle timer has no effect on when MLP will drop excess links in a bundle.

If the **ppp timeout multilink link remove** command is not configured but the **dialer wait-for-carrier-time** command is, MLP will use the time value set with the **dialer wait-for-carrier-time** command. If neither command is configured, MLP uses a default value of 30 seconds.

This command is used with dynamic bandwidth (dial-on-demand) bundles.

Examples

The following example sets the low traffic load threshold wait period to 45 seconds:

```
ppp timeout multilink link remove 45
```

Related Commands

Command	Description
dialer fast-idle (interface)	Specifies the idle time before the line is disconnected.
dialer wait-for-carrier-time (interface)	Specifies the length of time the interface waits for a carrier.
ppp timeout multilink link add	Limits the amount of time for which MLP waits for a call to be established.

ppp timeout multilink lost-fragment

To set a timer that determines how long Multilink PPP waits for an expected fragment to arrive before declaring it lost, use the **ppp timeout multilink lost-fragment** command in interface configuration mode. To reset the default value, use the **no** form of this command.

ppp timeout multilink lost-fragment *seconds* [*milliseconds*]

no ppp timeout multilink lost-fragment

Syntax Description

seconds	Wait period, in seconds, in the range from 1 to 255 seconds. **Note** If the desired delay should be in milliseconds, set the *seconds* argument to 0 and enter a value for the *milliseconds* argument.
milliseconds	(Optional) Wait period, in milliseconds, in the range from 1 to 999 milliseconds.

Command Default

The default value is 1 second.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.4(6)T	The optional *milliseconds* argument was added for a more precise setting and the command was integrated into Cisco IOS Release 12.4(6)T.
12.2(31)SB2	The command was integrated into Cisco IOS Release 12.2(31)SB2.

Examples

The following example sets a 5-second wait period for receiving expected fragments before declaring the fragments lost:

```
ppp timeout multilink lost-fragment 5
```

The following example sets a 300-millisecond wait period for receiving expected fragments before declaring the fragments lost:

```
ppp timeout multilink lost-fragment 0 300
```

The following example configures a wait period of 500 milliseconds (1/2 second):

```
ppp timeout multilink lost-fragment 0 500
```

Related Commands

Command	Description
ppp link reorders	Sets an advisory flag that indicates that the serial interface may receive packets in a different order than a peer system sent them.

ppp timeout ncp

To set a time limit for the successful negotiation of at least one network layer protocol after a PPP connection is established, use the **ppp timeout ncp** command in interface configuration mode. To reset the default condition, use the **no** form of this command.

ppp timeout ncp *seconds*

no ppp timeout ncp

Syntax Description

seconds	Maximum time, in seconds, PPP should wait for negotiation of a network layer protocol. If no network protocol is negotiated in the given time, the connection is disconnected.

Command Default

No time limit is imposed (**no ppp timeout ncp**).

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced as **ppp negotiation-timeout**.
12.2	This command was changed to **ppp timeout ncp**. The **ppp negotiation-timeout** command was accepted by the command line interpreter through Cisco IOS Release 12.2.

Usage Guidelines

The **ppp timeout ncp** command protects against the establishment of links that are physically up and carrying traffic at the link level, but are unusable for carrying data traffic due to failure to negotiate the capability to transport any network level data. This command is particularly useful for dialed connections, where it is usually undesirable to leave a telephone circuit active when it cannot carry network traffic.

Examples

The following example sets the Network Control Protocol (NCP) timer to 8 seconds:

```
ppp timeout ncp 8
```

Related Commands

Command	Description
absolute-timeout	Sets the interval for closing user connections on a specific line or port.
dialer idle-timeout (interface)	Specifies the idle time before the line is disconnected.

ppp timeout retry

To set the maximum waiting period for a response during PPP negotiation, use the **ppp timeout retry** command in interface configuration mode. To reset the time value to the default settings, use the **no** form of this command.

ppp timeout retry *seconds*

no ppp timeout retry

Cisco IOS Release 12.2(33)SRD

ppp timeout retry *seconds* [*milliseconds*]

no ppp timeout retry

Syntax Description

seconds	Maximum time, in seconds, to wait for a response during PPP negotiation. Valid values for the *seconds* argument range from 0 to 255. The default value is 2 seconds.
milliseconds	(Optional) Maximum time, in milliseconds (ms), to wait for a response during PPP negotiation. Valid values for the *milliseconds* argument range from 0 to 999. The default value is 0 ms.

Command Default

The default value waiting period for a response during PPP negotiation is 2 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD. The *milliseconds* argument was added.

Usage Guidelines

The **ppp timeout retry** command is useful for setting a maximum amount of time PPP should wait for a response to any control packet it sends.

Examples

The following example sets the retry timer to 100 seconds and 200 ms:

```
interface serial 2/0
encapsulation ppp
ppp timeout retry 100 200
```

Related Commands

Command	Description
ppp timeout authentication	Sets PPP authentication timeout parameters.
ppp timeout idle	Sets PPP idle timeout parameters.

pri-group timeslots

To specify an ISDN PRI group on a channelized T1 or E1 controller, and to release the ISDN PRI signaling time slot, use the **pri-group timeslots** command in controller configuration mode. To remove or change the ISDN PRI configuration, use the **no** form of this command.

pri-group timeslots *timeslot-range* [**nfas_d** {**backup nfas_int** *number* **nfas_group** *number* | **none nfas_int** *number* **nfas_group** *number* [**service mgcp**] | **primary nfas_int** *number* **nfas_group** *number* [**iua** *as-name* | **rlm-group** *number* | **service mgcp**]} | **service mgcp**]

no pri-group timeslots *timeslot-range* [**nfas_d** {**backup nfas_int** *number* **nfas_group** *number* | **none nfas_int** *number* **nfas_group** *number* [**service mgcp**] | **primary nfas_int** *number* **nfas_group** *number* [**iua** *as-name* | **rlm-group** *number* | **service mgcp**]} | **service mgcp**]

Syntax Description

timeslot-range	A value or range of values for time slots on a T1 or E1 controller that consists of an ISDN PRI group. Use a hyphen to indicate a range. **Note** Groups of time slot ranges separated by commas (1-4,8-23 for example) are also accepted.
nfas_d	(Optional) Configures the operation of the ISDN PRI D channel.
backup	The D-channel time slot is used as the Non-Facility Associated Signaling (NFAS) D backup.
none	The D-channel time slot is used as an additional B channel.
primary	The D-channel time slot is used as the NFAS D primary.
nfas_int *number*	Specifies the provisioned NFAS interface as a value. Valid values for the NFAS interface range from 0 to 44.
nfas_group *number*	Specifies the NFAS group. Valid values for the NFAS group number range from 0 to 31.
iua *as-name*	(Optional) Configures the ISDN User Adaptation Layer (IUA) application server (AS) name.
rlm-group *number*	(Optional) Specifies the Redundant Link Manager (RLM) group and release the ISDN PRI signaling channel. Valid values for the RLM group number range from 0 to 255.
service mgcp	(Optional) Configures the service type as Media Gateway Control Protocol (MGCP) service.

Command Default

No ISDN PRI group is configured. The switch type is automatically set to the National ISDN switch type (**primary-ni** keyword) when the **pri-group timeslots** command is configured with the **rlm-group** subkeyword.

Command Modes

Controller configuration

Command History

Release	Modification
11.0	This command was introduced.
11.3	This command was enhanced to support NFAS.
12.0(2)T	This command was implemented on the Cisco MC3810 multiservice concentrator.
12.0(7)XK	This command was implemented on the Cisco 2600 and Cisco 3600 series routers.
12.1(2)T	The modifications in Cisco IOS Release 12.0(7)XK were integrated into Cisco IOS Release 12.1(2)T.
12.2(8)B	This command was modified with the **rlm-group** subkeyword to support release of the ISDN PRI signaling channels.
12.2(15)T	The modifications in Cisco IOS Release 12.2(8)B were integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

The **pri-group** command supports the use of DS0 time slots for Signaling System 7 (SS7) links, and therefore the coexistence of SS7 links and PRI voice and data bearer channels on the same T1 or E1 span. In these configurations, the command applies to voice applications.

In SS7-enabled Voice over IP (VoIP) configurations when an RLM group is configured, High-Level Data Link Control (HDLC) resources allocated for ISDN signaling on a digital subscriber line (DSL) interface are released and the signaling slot is converted to a bearer channel (B24). The D channel will be running on IP. The chosen D-channel time slot can still be used as a B channel by using the **isdn rlm-group** interface configuration command to configure the NFAS groups.

NFAS allows a single D channel to control multiple PRI interfaces. Use of a single D channel to control multiple PRI interfaces frees one B channel on each interface to carry other traffic. A backup D channel can also be configured for use when the primary NFAS D channel fails. When a backup D channel is configured, any hard system failure causes a switchover to the backup D channel and currently connected calls remain connected.

NFAS is supported only with a channelized T1 controller and, as a result, must be ISDN PRI capable. Once the channelized T1 controllers are configured for ISDN PRI, only the NFAS primary D channel must be configured; its configuration is distributed to all members of the associated NFAS group. Any configuration changes made to the primary D channel will be propagated to all NFAS group members. The primary D channel interface is the only interface shown after the configuration is written to memory.

The channelized T1 controllers on the router must also be configured for ISDN. The router must connect to either an AT&T 4ESS, Northern Telecom DMS-100 or DMS-250, or National ISDN switch type.

The ISDN switch must be provisioned for NFAS. The primary and backup D channels should be configured on separate T1 controllers. The primary, backup, and B-channel members on the respective controllers should be the same configuration as that configured on the router and ISDN switch. The interface ID assigned to the controllers must match that of the ISDN switch.

You can disable a specified channel or an entire PRI interface, thereby taking it out of service or placing it into one of the other states that is passed in to the switch using the **isdn service** interface configuration command.

In the event that a controller belonging to an NFAS group is shut down, all active calls on the controller that is shut down will be cleared (regardless of whether the controller is set to primary, backup, or none), and one of the following events will occur:

- If the controller that is shut down is configured as the primary and no backup is configured, all active calls on the group are cleared.
- If the controller that is shut down is configured as the primary, and the active (In service) D channel is the primary and a backup is configured, then the active D channel changes to the backup controller.
- If the controller that is shut down is configured as the primary, and the active D channel is the backup, then the active D channel remains as backup controller.
- If the controller that is shut down is configured as the backup, and the active D channel is the backup, then the active D channel changes to the primary controller.

The expected behavior in NFAS when an ISDN D channel (serial interface) is shut down is that ISDN Layer 2 should go down but keep ISDN Layer 1 up, and that the entire interface will go down after the amount of seconds specified for timer T309.

Note The active D channel changeover between primary and backup controllers happens only when one of the link fails and not when the link comes up. The T309 timer is triggered when the changeover takes place.

Examples

The following example configures T1 controller 1/0 for PRI and for the NFAS primary D channel. This primary D channel controls all the B channels in NFAS group 1.

```
controller t1 1/0
 framing esf
 linecode b8zs
 pri-group timeslots 1-24 nfas_d primary nfas_int 0 nfas_group 1
```

The following example specifies ISDN PRI on T1 slot 1, port 0, and configures voice and data bearer capability on time slots 2 through 6:

```
isdn switch-type primary-4ess
controller t1 1/0
 framing esf
 linecode b8zs
 pri-group timeslots 2-6
```

The following example configures a standard ISDN PRI interface:

```
! Standard PRI configuration:
controller t1 1
 pri-group timeslots 1-23 nfas_d primary nfas_int 0 nfas_group 0
 exit

! Standard ISDN serial configuration:
interface serial1:23
! Set ISDN parameters:
 isdn T309 4000
 exit
```

The following example configures a dedicated T1 link for SS7-enabled VoIP:

```
controller T1 1
 pri-group timeslots 1-23 nfas_d primary nfas_int 0 nfas_group 0
 exit
```

```
! In a dedicated configuration, we assume the 24th timeslot will be used by ISDN.
! Serial interface 0:23 is created for configuring ISDN parameters.
interface Serial:24
! The D channel is on the RLM.
 isdn rlm 0
 isdn  T309 4000
 exit
```

The following example configures a shared T1 link for SS7-enabled VoIP. The **rlm-group 0** portion of the **pri-group timeslots** command releases the ISDN PRI signaling channel.

```
controller T1 1
 pri-group timeslots 1-3 nfas_d primary nfas_int 0 nfas_group 0 rlm-group 0
 channel group 23 timeslot 24
 end

! D-channel interface is created for configuration of ISDN parameters:
interface Dchannel1
 isdn T309 4000
 end
```

Related Commands

Command	Description
controller	Configures a T1 or E1 controller and enters controller configuration mode.
interface Dchannel	Specifies an ISDN D-channel interface for VoIP applications that require release of the ISDN PRI signaling time slot for RLM configurations.
interface serial	Specifies a serial interface created on a channelized E1 or channelized T1 controller for ISDN PRI signaling.
isdn rlm-group	Specifies the RLM group number that ISDN will start using.
isdn switch-type	Specifies the central office switch type on the ISDN PRI interface.
isdn timer t309	Changes the value of the T309 timer to clear network connections and release the B channels when there is no signaling channel active, that is, when the D channel has failed and cannot recover by switching to an alternate D channel. Calls remain active and able to transfer data when the D channel fails until the T309 timer expires. The T309 timer is canceled when D-channel failover succeeds.
show isdn nfas group	Displays all the members of a specified NFAS group or all NFAS groups.

profile incoming

To define a template formed by directives guiding the Call Service Module (CSM) to process the digit sequence for a signaling class, use the **profile incoming** command in global configuration mode.

profile incoming *template*

Syntax Description

template	String of special characters that are arranged in a certain order to process the digit sequence for the signaling class. Choose from the following list: • **S**—Starts the state machine. • **<***—Waits for the digit * to be detected. The digit to be detected is the next character in the template. If any other digit is detected, then that is a failure. If the digit is detected, then go to the next directive. • **a**—Digits are collected as the ANI until the first nondigit or a timeout occurs. • **d**—Digits are collected as the DNIS until the first nondigit or a timeout occurs. • **n**—Notifies the CSM of the collected ANI and DNIS.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

Arrange the directive special characters in the order necessary to process the digit sequence for your signaling class.

Examples

The following example enables the **profile incoming** command:

```
signaling-class cas test
 profile incoming S<*a<*d<*n
```

Related Commands

Command	Description
class (controller)	Activates the **signaling-class cas** command.
signaling-class cas	Defines a signaling class with a template formed by directives guiding the CSM to process the digit sequence.

range

To associate a range of modems or other physical resources with a resource group, use the **range** command in resource group configuration mode. To remove a range of modems or other physical resources, use the **no** form of this command.

range {**limit** *number* | **port** *slot* [*slot*]}

no range {**limit** *number* | **port** *slot* [*slot*]}

Cisco AS5200 and AS5300 Series Routers

range {**limit** *number* | **port** *slot*/*port* [*slot*/*port*]}

no range {**limit** *number* | **port** *slot*/*port* [*slot*/*port*]}

Syntax Description

limit *number*	Maximum number of simultaneous connections supported by the resource group. Replace the *number* argument with the session limit you want to assign. Your access server hardware configuration determines the maximum value of this limit. Applicable to ISDN B channels or HDLC controllers.
port *slot* [*slot*]	Slot or range of slots to use in the resource group.
port *slot*/*port* [*slot*/*port*]	Specific port or range of ports to use in the resource group. A forward slash must be used to separate the slot and port numbers.

Command Default

No range is configured.

Command Modes

Resource group configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **range** resource group configuration command to associate a range of modems or other physical resources with a resource group.

Specify the range for port-based resources by using the resource's physical location. Do not identify non-port-based resource ranges by using a location. Rather, specify the size of the resource group with a single integer limit.

Specify noncontiguous ranges by using multiple **range port** commands within the same resource group. Do not configure the same ports in more than one resource group and do not overlap multiple port ranges.

For resources that are not pooled and have a one-to-one correspondence between DS0s, B channels, and HDLC framers, use the **range limit** *number* command. Circuit-switched data calls and V.120 calls use these kinds of resources.

Note Do not put heterogeneous resources in the same group. Do not put MICA modems in the same group as Microcom modems. Do not put modems and HDLC controllers in the same resource group.

Do not configure “port” and “limit” parameters in the same resource group.

Examples

The following example shows the range limit set for 48 simultaneous connections being supported by the resource group:

```
resource-pool group resource hdlc1
 range limit 48
```

The following example shows the ports set for modem 1 ranging from port 0 to port 47:

```
resource-pool group modem1
 range port 1/0 1/47
```

rcapi number

To enable the Cisco 800 series router to distinguish between incoming CAPI calls and incoming non-CAPI calls such as POTS, PPP, and X.25, use the **rcapi number** command in global configuration mode. To release the specified directory number from the RCAPI interface, use the **no** form of this command.

rcapi number *directory-number*[**:***subaddress*]

no rcapi number

Syntax Description

directory-number	ISDN directory number.
:*subaddress*	(Optional) Subaddress of the router preceded by a colon (:).

Command Default

No directory number is set for the RCAPI interface.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XV	The commands **rcapi number** and **no rcapi number** were introduced on the Cisco 800 series router.

Usage Guidelines

The **rcapi number** command allows the Cisco 800 series router to reserve directory numbers exclusively for incoming calls.

The *directory-number* argument is the number assigned by the ISDN provider for the PC on which RCAPI is configured. The directory number should not be set to any other interfaces such as POTS and DOV. This command works only with the Net3 switch type.

Examples

The following example sets the router to recognize an ISDN number rather than a subaddress:

```
rcapi number 12345
```

Related Commands

Command	Description
debug rcapi events	Displays diagnostic DCP and driver messages.
rcapi server	Enables the RCAPI server on the 800 series router and, optionally, sets the TCP port number.
show rcapi status	Display statistics and details about RCAPI server operation.

rcapi server

To enable the RCAPI server on the 800 series router or to set the TCP port number, use the **rcapi server** command in global configuration mode. To disable the RCAPI server on the 800 series router, use the **no** form of this command.

rcapi server [**port** *number*]

no rcapi server

Syntax Description

port *number*	(Optional) TCP port number.

Command Default

If the router is configured for basic Net3 IDSN switch type, by default RCAPI is enabled, and the port number is set to 2578.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XV	This command was introduced on the Cisco 800 series router.

Usage Guidelines

This command works only with the Net3 switch type. The same port number must be configured on both the router and client PC.

Examples

The following example set the TCP port number to 2000:

```
rcapi server port 2000
```

Related Commands

Command	Description
debug rcapi events	Displays diagnostic DCP and driver messages.
rcapi number	Enables the Cisco 800 series router to distinguish between incoming CAPI calls and incoming non-CAPI calls such as POTS, PPP, and X.25.
show rcapi status	Display statistics and details about RCAPI server operation.

redundancy

To enter redundancy configuration mode, use the **redundancy** command in global configuration mode.

redundancy

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5)XV1	This command was introduced on the Cisco AS5800 universal access server.
12.2(4)XF	This command was introduced for the Cisco uBR10012 router.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.0(9)SL	This command was integrated into Cisco IOS Release 12.0(9)SL.
12.0(16)ST	This command was implemented on the Cisco 7500 series Internet routers.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	Support for this command was added for the Supervisor Engine 720.
12.2(18)S	This command was implemented on the Cisco 7500 series Internet routers.
12.2(20)S	This command was implemented on the Cisco 7304 router.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.3(7)T	This command was implemented on the Cisco 7500 series Internet routers.
12.2(8)MC2	This command was implemented on the MWR 1900 Mobile Wireless Edge Router (MWR).
12.3(11)T	This command was implemented on the MWR 1900 MWR.
12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
12.0(22)S	This command was implemented on the Cisco 10000 series Internet routers.
12.2(18)SXE2	This command was integrated into Cisco IOS Release 12.2(18)SXE2.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(44)SQ	This command was integrated into Cisco IOS Release 12.2(44)SQ. Support for the Cisco RF Gateway 10 was added.
12.2(33) SRE	This command was modified. The interchassis subconfiguration mode was added.

Usage Guidelines

Use the **redundancy** command to enter redundancy configuration mode, where you can define aspects of redundancy such as shelf redundancy for the Cisco AS5800 universal access server.

Cisco 10000 Series Router

Before configuring line card redundancy, install the Y-cables. Before deconfiguring redundancy, remove the Y-cables.

The following restrictions apply to line card redundancy on the Cisco 10000 series router:

- Port-level redundancy is not supported.
- Redundant cards must occupy the two subslots within the same physical line card slot.
- The line card that will act as the primary line card must be the first line card configured, and it must occupy subslot 1.

Cisco 7600 Series Router

From redundancy configuration mode, you can enter the main CPU submode to manually synchronize the configurations that are used by the two supervisor engines.

From the main CPU submode, you can use the **auto-sync** command to use all of the redundancy commands that are applicable to the main CPU.

To select the type of redundancy mode, use the **mode** command.

Nonstop forwarding (NSF) with stateful switchover (SSO) redundancy mode supports IPv4. NSF with SSO redundancy mode does not support IPv6, Internetwork Packet Exchange (IPX), and Multiprotocol Label Switching (MPLS).

After you enter redundancy configuration mode, you can use the **interchassis** command to specify the redundancy group number and enter interchassis redundancy mode. In the interchassis redundancy configuration mode, you can do the following:

- Specify a backbone interface for the redundancy group using the **backbone** command.
- Exit from interchassis configuration mode using the **exit** command.
- Specify the IP address of the remote redundancy group member using the **member ip** command.
- Specify the Multichassis LACP (mLACP) node ID, system MAC address, and system priority using the **node-id**, **system-mac**, and **system-priority** commands.
- Define the peer monitoring method using the **monitor** command.

Cisco uBR10012 Universal Broadband Router

After you enter redundancy configuration mode, you can use the **main-cpu** command to enter main-CPU redundancy configuration mode, which allows you to specify which files are synchronized between the active and standby Performance Routing Engine (PRE) modules.

Cisco RF Gateway 10

At the redundancy configuration mode, you can do the following:

- Set a command to its default mode using the **default** command.
- Exit from a redundancy configuration using the **exit** command.
- Enter the line card group redundancy configuration using the **linecard-group** command.
- Enter main-CPU redundancy configuration mode using the **main-cpu** command, which allows you to specify which files are synchronized between the active and standby Supervisor cards.
- Configure the redundancy mode for the chassis using the **mode** command.
- Enforce a redundancy policy using the **policy** command.

Examples

The following example shows how to enable redundancy mode:

```
Router(config)# redundancy
Router(config-red)#
```

The following example shows how to assign the configured router shelf to the redundancy pair designated as 25. This command must be issued on both router shelves in the redundant router-shelf pair:

```
Router(config)# redundancy
Router(config-red)# failover group-number 25
```

Cisco 10000 Series Router

The following example shows how to configure two 4-port channelized T3 half eight line cards that are installed in line card slot 2 for one-to-one redundancy:

```
Router(config)# redundancy
Router(config-r)# linecard-group 1 y-cable
Router(config-r-lc)# member subslot 2/1 primary
Router(config-r-lc)# member subslot 2/0 secondary
```

Cisco 7600 Series Router

The following example shows how to enter the main CPU submode:

```
Router(config)# redundancy
Router(config-r)# main-cpu
Router(config-r-mc)#
```

Cisco uBR10012 Universal Broadband Router

The following example shows how to enter redundancy configuration mode and display the commands that are available in that mode on the Cisco uBR10012 router:

```
Router# configure terminal
Router(config)# redundancy
Router(config-r)# ?

Redundancy configuration commands:
  associate  Associate redundant slots
  exit       Exit from redundancy configuration mode
  main-cpu   Enter main-cpu mode
  no         Negate a command or set its defaults
```

The following example shows how to enter redundancy configuration mode and displays its associated commands on the Cisco RFGW-10 chassis:

```
Router# configure terminal
Router(config)# redundancy
Router(config-r)#?

Redundancy configuration commands:
  default         Set a command to its defaults
  exit            Exit from redundancy configuration mode
  linecard-group  Enter linecard redundancy submode
  main-cpu        Enter main-cpu mode
  mode            redundancy mode for this chassis
  no              Negate a command or set its defaults
  policy          redundancy policy enforcement
```

The following example shows how to enter redundancy configuration mode and its associated commands in the interchassis mode:

```
Router# configure terminal
Router(config)# redundancy
Router(config-r)#?

Redundancy configuration commands:
  exit          Exit from redundancy configuration mode
  interchassis  Enter interchassis mode
  no            Negate a command or set its defaults

Router(config-r)# interchassis group 100
R1(config-r-ic)# ?

Interchassis redundancy configuration commands:
  backbone  specify a backbone interface for the redundancy group
  exit      Exit from interchassis configuration mode
  member    specify a redundancy group member
  mlacp     mLACP interchassis redundancy group subcommands
  monitor   define the peer monitoring method
  no        Negate a command or set its defaults
```

Related Commands

Command	Description
associate slot	Logically associates slots for APS processor redundancy.
auto-sync	Enables automatic synchronization of the configuration files in NVRAM.
clear redundancy history	Clears the redundancy event history log.
linecard-group y-cable	Creates a line card group for one-to-one line card redundancy.
main-cpu	Enters main-CPU redundancy configuration mode for synchronization of the active and standby PRE modules or Supervisor cards.
member subslot	Configures the redundancy role of a line card.
mode (redundancy)	Configures the redundancy mode of operation.
redundancy force-switchover	Switches control of a router from the active RP to the standby RP.
show redundancy	Displays information about the current redundant configuration and recent changes in states or displays current or historical status and related information on planned or logged handovers.

reload components

To request that the dial shelf controller (DSC) (or DSCs in a redundant configuration) be reloaded at the same time as a reload on the Router Shelf on the Cisco AS5800, use the **reload components** command in EXEC mode. To cancel a reload, use the **reload components cancel** command.

reload components {**all** | *description-line* | **at** *hh*:*mm* | **in** [*hhh*:]*mmm*}

reload components cancel

Syntax Description

all	Reloads all attached components.
description-line	Displays reason for the reload, 1 to 255 characters in length.
at *hh*:*mm*	Schedules when the software reload takes place using a 24-hour clock. If you specify the month and day, the reload is scheduled to take place at the specified time and date. If you do not specify the month and day, the reload takes place at the specified time on the current day (if the specified time is later than the current time), or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight. The reload must take place within approximately 24 days.
in [*hhh*:]*mmm*	Schedule a reload of the software to take effect in the specified minutes or (optionally) hours and minutes. The reload must take place within approximately 24 days.
cancel	Cancels a scheduled reload.

Command History

Release	Modification
12.1(3)T	This command was introduced.

Command Modes

EXEC

Usage Guidelines

On the Cisco AS5800 only, to request that the DSC (or DSCs in a redundant configuration) be reloaded at the same time as a reload on the Router Shelf, use the **reload components all** command.

You cannot reload from a virtual terminal if the system is not set up for automatic booting. This prevents the system from dropping to the ROM monitor and thereby taking the system out of remote user control.

If you modify your configuration file, the system prompts you to save the configuration. During a save operation, the system asks you if you want to proceed with the save if the CONFIG_FILE environment variable points to a startup configuration file that no longer exists. If you say “yes” in this situation, the system goes to setup mode upon reload.

When you schedule a reload to occur at a later time, it must take place within approximately 24 days.

The **at** keyword can only be used if the system clock has be set on the router (either through Network Time Protocol (NTP), the hardware calendar, or manually). The time is relative to the configured time zone on the router. To schedule reloads across several routers to occur simultaneously, the time on each router must be synchronized with NTP.

To display information about a scheduled reload, use the **show reload** command.

Examples

The following example reloads all components on a Cisco AS5800:

```
Router# reload components all
```

Related Commands

Command	Description
show reload	Displays the reload status on the router.

resource

To assign resources and supported call-types to a customer profile, use the **resource** command in customer profile configuration mode. To disable this function, use the **no** form of this command.

resource *name* {**digital | speech | v110 | v120**} [**service** *name*]

no resource *name* {**digital | speech | v110 | v120**} [**service** *name*]

Syntax Description

name	Name for a group of physical resources inside the access server. This name can have up to 23 characters.
digital	Accepts digital calls. Specifies circuit-switched data calls that terminate on a HDLC framers (unlike asynchronous analog modem call that use start and stop bits).
speech	Accepts speech calls. Specifies normal voice calls, such as calls started by analog modems and standard telephones.
v110	Accepts V.110 calls.
v120	Accepts V.120 calls. By specifying this keyword, the access server begins counting the number of v120 software encapsulations occurring in the system.
service *name*	(Optional) Name for a service profile. This option is not supported for digital or V.120 calls.

Command Default

No resources are assigned to the customer profile by default.

Command Modes

Customer profile configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **resource** customer profile configuration command to assign resources and supported call-types to a customer profile. This command specifies a group of physical resources to be used in answering an incoming call of a particular type for a particular customer profile. For example, calls started by analog modems are reciprocated with the **speech** keyword.

Examples

The following example shows a physical resource group called “modem1”. Forty-eight integrated modems are then assigned to modem1, which is linked to the customer profile called “customer1_isp”:

```
resource-pool group resource modem1
 range port 1/0 1/47
!
resource-pool profile customer customer1_isp
 resource modem1 speech
```

Related Commands

Command	Description
resource-pool profile customer	Creates a customer profile.

resource-pool

To enable or disable resource pool management, use the **resource-pool** command in global configuration mode.

resource-pool {**enable** | **disable**}

Syntax Description

enable	Enables resource pool management.
disable	Disables resource pool management.

Command Default

Resource management is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **resource-pool** global configuration command to enable and disable the resource pool management feature.

Examples

The following example shows how to enable RPM:

```
resource-pool enable
```

resource-pool aaa accounting ppp

To include enhanced start/stop resource manager records to authorization, authentication, and accounting (AAA) accounting, use the **resource-pool aaa accounting ppp** command in global configuration mode. To disable this feature, use the **no** form of this command.

resource-pool aaa accounting ppp

no resource-pool aaa accounting ppp

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled. The default of the **resource-pool enable** command is to *not* enable these new accounting records.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **resource-pool aaa accounting ppp** global configuration command to include enhanced start/stop resource manager records to AAA accounting. The **resource-pool aaa accounting ppp** command adds new resource pool management fields to the AAA accounting start/stop records. The new attributes in the start records are also in the stop records—in addition to those new attributes added exclusively for the stop records.

If you have configured your regular AAA accounting, this command directs additional information from the resource manager into your accounting records.

Note If you configure only this command and do not configure AAA accounting, nothing happens. The default functionality for the resource-pool enable command does not include this functionality.

Table 18 shows the new fields that have been added to the start and stop records.

Table 18 Start and Stop Resource Manager Records

New Start Record Fields	New Stop Record Fields
Call-type	ModemSpeed-receive
Customer-profile-name	ModemSpeed-transmit
Customer-profile-active-sessions	MLP-session-ID (multilink users)
MLP-session-ID (multilink users)	
Resource-group-name	
Overflow-flag	
VPDN-tunnel-ID (VPDN users)	
VPDN-homegateway (VPDN users)	
VPDN-domain-name (VPDN users)	
VPDN-group-active-session (VPDN users)	

Caution This list of newly supported start and stop fields is not exhaustive. Cisco reserves the right to enhance this list of records at any time. Use the **show accounting** command to see the contents of each active session.

Note Cisco recommends that you *thoroughly* understand how these new start/stop records affect your current accounting structure *before* you enter this command.

Examples

The following example shows the new AAA accounting start/stop records inserted into an existing AAA accounting infrastructure:

```
resource-pool aaa accounting ppp
```

Related Commands

Command	Description
show accounting	Allows display of the active accountable events on the network and helps collect information in the event of a data loss on the accounting server.

resource-pool aaa protocol

To specify which protocol to use for resource management, use the **resource-pool aaa protocol** command in global configuration mode. To disable this feature and go to local, use the **no** form of this command.

resource-pool aaa protocol {**local** | **group** *name*}

no resource-pool aaa protocol

Syntax Description

local	Local authorization.
group *name*	Use an external authorization, authentication, and accounting (AAA) server group. The Resource Pool Management Server (RPMS) is defined in a AAA server group.

Command Default

Default is set to local authorization.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **resource-pool aaa protocol** global configuration command to specify which protocol to use for resource management. The AAA server group is most useful when you want to have multiple RPMSs configured as a fall-back mechanism.

Examples

The following example shows how to specify local authorization protocol:

```
resource-pool aaa protocol local
```

resource-pool call treatment

To set up the signal sent back to the telco switch in response to incoming calls, use the **resource-pool call treatment** command in global configuration mode. To disable this function, use the **no** form of this command.

resource-pool call treatment {**profile** {**busy** | **no-answer**} | **resource** {**busy** | **channel-not-available**}}

no resource-pool call treatment {**profile** {**busy** | **no-answer**} | **resource** {**busy** | **channel-not-available**}}

Syntax Description

profile	Call treatment when profile authorization fails.
busy	Answers the call, then sends a busy signal when profile authorization or resource allocation fails.
no-answer	Does not answer the call when profile authorization fails.
resource	Call treatment when resource allocation fails.
channel-not-available	Sends channel not available (CNA) code when resource allocation fails.

Command Default

No answer for a customer profile; CNA for a resource.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **resource-pool call treatment** global configuration command to set up the signal sent back to the telco switch in response to incoming calls.

Examples

The following example configures the device to answer the call and send a busy signal when profile authorization or resource allocation fails:

```
resource-pool call treatment profile busy
```

resource-pool call treatment discriminator

To modify the signal (ISDN cause code) sent to the switch when a discriminator rejects a call, enter the **resource-pool call treatment discriminator** command in global configuration mode. To disable this function, use the **no** form of this command.

resource-pool call treatment discriminator {**busy** | **no-answer** | **channel-not-available**}

no resource-pool call treatment discriminator {**busy** | **no-answer** | **channel-not-available**}

Syntax Description

busy	Answers the call, then sends a busy signal when profile authorization or resource allocation fails.
no-answer	Does not answer the call when profile authorization fails.
channel-not-available	Sends channel not available (CNA) code when resource allocation fails.

Command Default

No answer for a customer profile; CNA for a resource.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.

Usage Guidelines

Use the **resource-pool call treatment discriminator** global configuration command to set up the signal sent back to the telco switch in response to incoming calls.

Examples

Use the following command to answer the call, but send a busy signal to the switch when profile authorization or resource allocation fails:

```
resource-pool call treatment discriminator busy
```

Use the following command to prevent the call from being answered when profile authorization fails and the discriminator rejects a call:

```
resource-pool call treatment discriminator no-answer
```

resource-pool group resource

To create a resource group for resource management, use the **resource-pool group resource** command in global configuration mode. To remove a resource group from the running configuration, use the **no** form of this command.

resource-pool group resource *name*

no resource-pool group resource *name*

Syntax Description

name	Name for the group of physical resources inside the access server. This name can have up to 23 characters.

Command Default

No resource groups are set up.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **resource-pool group resource** global configuration command to create a resource group for resource management. When calls come into the access server, they are allocated physical resources as specified within resource groups and customer profiles.

See the **range** command for more information.

If some physical resources are not included in any resource groups, then these remaining resources are not used and are considered to be part of the default resource group. These resources can be used in certain cases to answer calls before profile allocation occurs, but the resources are not used other than in the connection phase.

Note For standalone network access server environments, configure resource groups before using them in customer profiles. For external RPMS environments, configure resource groups on the network access server before defining them on external RPMS servers.

When enabling RPM for SS7 signaling, like resources in the network access server (NAS) must be in a single group:

- All modems must be in one group.
- All High-Level Data Link Control (HDLC) controllers must be in a different group.
- All V.110 ASICs must be put into another group.
- All V.120 resources must be in a separate group.

All resource group types must have the same number of resources and that number must equal the number of interface channels available from the public network switch. This grouping scheme prevents the CNA signal from being sent to the signaling point. For SS7 signaling, Microcom and MICA technologies modems must be in the *same* group. If SS7 signaling is not used, Cisco recommends assigning Microcom and MICA modems to separate groups to avoid introducing errors in RPM statistics.

Examples

The following example shows the configuration options within a resource group:

```
Router(config)# resource-pool group resource modem1
?
Resource Group Configuration Commands:
  default  Set a command to its defaults
  exit     Exit from resource-manager configuration mode
  help     Description of the interactive help system
  no       Negate a command or set its defaults
  range    Configure range for resource

Router(config-resource)# range ?
  limit  Configure the maximum limit
  port   Configure the resource ports

Router(config-resource)# range limit ?
  <1-192>  Maximum number of connections allowed

Router(config-resource)# range port ?
  <0-246>  First Modem TTY Number
  x/y      Slot/Port for Internal Modems
```

Related Commands

Command	Description
range	Associates a range of modems or other physical resources with a resource group.

resource-pool profile customer

To create a customer profile and to enter customer profile configuration mode, use the **resource-pool profile customer** command in global configuration mode. To delete a customer profile from the running configuration, use the **no** form of this command.

resource-pool profile customer *name*

no resource-pool profile customer *name*

Syntax Description

name	Customer profile name. This name can have up to 23 characters.

Command Default

No customer profiles are set up.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.
12.0(5)T	Support for this command was integerated into Cisco IOS Release 12.0(5)T.

Usage Guidelines

Use the **resource-pool profile customer** command to create a customer profile and enter customer profile configuration mode.

VPDN groups can be associated with a customer profile by issuing the **vpdn group** command in customer profile configuration mode.

A VPDN profile can be associated with a customer profile by issuing the **vpdn profile** command in customer profile configuration mode.

VPDN session limits for the VPDN groups associated with a customer profile can be configured in customer profile configuration mode using the **limit base-size** command.

Examples

The following example shows how to create two VPDN groups, configure the VPDN groups under a VPDN profile named profile1, then associate the VPDN profile with a customer profile named customer12:

```
Router(config)# vpdn-group 1
Router(config-vpdn)#
!
Router(config)# vpdn-group 2
Router(config-vpdn)#
!
Router(config)# resource-pool profile vpdn profile1
Router(config-vpdn-profile)# vpdn group 1
Router(config-vpdn-profile)# vpdn group 2
!
```

```
Router(config)# resource-pool profile customer customer12
Router(config-vpdn-customer)# vpdn profile profile1
```

Related Commands

Command	Description
dnis group	Includes a group of DNIS numbers in a customer profile.
limit base-size	Defines the base number of simultaneous connections that can be done in a single customer or VPDN profile.
limit overflow-size	Defines the number of overflow calls granted to one customer or VPDN profile.
resource	Assigns resources and supported call types to a customer profile.
resource-pool group resource	Creates a resource group for resource management.
vpdn group	Associates a VPDN group with a customer or VPDN profile.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn profile	Associates a VPDN profile with a customer profile.

resource-pool profile discriminator

To create a call discrimination profile and assign it a name, use the **resource-pool profile discriminator** command in global configuration mode. To remove a call discrimination profile from the running configuration, use the **no** form of this command.

resource-pool profile discriminator *name*

no resource-pool profile discriminator *name*

Syntax Description

name	Name of the call discrimination profile created. This name can have up to 23 characters. You can add a calling line ID (CLID) or DNIS group to the discriminator profile created.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.
12.1(5)T	This command was enhanced to add CLID groups and dialed number identification service (DNIS) groups to a discriminator.

Usage Guidelines

Discriminator profiles enable you to process calls differently based on the call type and DNIS or CLID combination. Use the **resource-pool profile discriminator** command to create a call discrimination profile, and then use the **clid group** command to add a CLID group to a discriminator.

To create a call discrimination profile, you must specify both the call type and CLID group. Once a CLID group is associated with a call type in a discriminator, it cannot be used in any other discriminator.

Examples

The following example shows a call discriminator named clid1 created and configured to block digital calls from the CLID group named clid3:

```
resource-pool profile discriminator clid1
 call-type digital
 clid group clid3
```

Related Commands

Command	Description
clid group	Configures a CLID group in a discriminator.
dnis group	Configures a DNIS group in a discriminator.

resource-pool profile service

To set up the service profile configuration, use the **resource-pool profile service** command in global configuration mode. To disable this function, use the **no** form of this command.

resource-pool profile service *name*

no resource-pool profile service *name*

Syntax Description

name	Service profile name. This name can have up to 23 characters.

Command Default

No service profiles are set up.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **resource-pool profile service** global configuration command to set up the service profile configuration.

Examples

The following example shows the creation of a service profile called user1:

```
resource-pool profile service user1
```

resource-pool profile vpdn

To create a virtual private dialup network (VPDN) profile and to enter VPDN profile configuration mode, use the **resource-pool profile vpdn** command in global configuration mode. To disable this function, use the **no** form of this command.

resource-pool profile vpdn *name*

no resource-pool profile vpdn *name*

Syntax Description

name	VPDN profile name.

Command Default

No VPDN profiles are set up.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.
12.0(5)T	Support for this command was integerated into Cisco IOS Release 12.0(5)T.

Usage Guidelines

Use the **resource-pool profile vpdn** command to create a VPDN profile and enter VPDN profile configuration mode, or to enter VPDN profile configuration mode for a VPDN profile that already exists.

VPDN groups can be associated with a VPDN profile using the **vpdn group** command in VPDN profile configuration mode. A VPDN profile will count VPDN sessions across all associated VPDN groups.

VPDN session limits for the VPDN groups associated with a VPDN profile can be configured in VPDN profile configuration mode using the **limit base-size** command.

Examples

The following example createss the VPDN groups named l2tp and l2f, and associates both VPDN groups with the VPDN profile named profile32:

```
Router(config)# vpdn-group l2tp
Router(config-vpdn)#
!
Router(config)# vpdn-group l2f
Router(config-vpdn)#
!
Router(config)# resource-pool profile vpdn profile32
Router(config-vpdn-profile)# vpdn group l2tp
Router(config-vpdn-profile)# vpdn group l2f
```

Related Commands

Command	Description
limit base-size	Defines the base number of simultaneous connections that can be done in a single customer or VPDN profile.
limit overflow-size	Defines the number of overflow calls granted to one customer or VPDN profile.
vpdn group	Associates a VPDN group with a customer or VPDN profile.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn profile	Associates a VPDN profile with a customer profile.

retry keepalive

To enable Redundant Link Manager (RLM) keepalive retries, use the **retry keepalive** command in RLM configuration mode. To disable this function, use the **no** form of this command.

retry keepalive *number-of-times*

no retry keepalive *number-of-times*

Syntax Description

number-of-times	Number of keepalive failures allowed before the link is declared down, from 1 to 100.

Command Default

Default retries is 3.

Command Modes

RLM configuration

Command History

Release	Modification
11.3(7)	This command was introduced.

Usage Guidelines

RLM allows keepalive failures in consecutive certain amounts of time configured using the command line interface (CLI) before it declares the link is down.

Examples

The following example sets RLM keepalive retries to 88:

```
retry keepalive 88
```

Related Commands

Command	Description
clear interface virtual-access	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
link (RLM)	Specifies the link preference.
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole rlm-group.
server (RLM)	Defines the IP addresses of the server.
show rlm group statistics	Displays the network latency of the RLM group.
show rlm group status	Displays the status of the RLM group.
show rlm group timer	Displays the current RLM group timer values.

Command	Description
shutdown (RLM)	Shuts down all of the links under the RLM group.
timer	Overwrites the default setting of timeout values.

rotary

To define a group of lines consisting of one or more virtual terminal lines or one auxiliary port line, use the **rotary** command in line configuration mode. To remove a group of lines from a rotary group, use the **no** form of this command.

rotary *group* [**queued** [**by-role**]] [**round-robin**]

no rotary *group* [**queued** [**by-role**]] [**round-robin**]

Syntax Description

group	Rotary group number.
queued	(Optional) Specifies queueing a connection request to a rotary group.
by-role	(Optional) Enables priority users to move to the head of the queue.
round-robin	(Optional) Selects a round-robin port selection algorithm instead of the default linear port selection algorithm.

Command Default

No group of lines is defined.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.1(1)T	The **queued** keyword was added.
12.1(2)T	The **round-robin** keyword was added.
12.2(15)T	The **by-role** keyword was added.

Usage Guidelines

Connections to a rotary group can take advantage of the following features:

- Clear To Send (CTS)—If a line in a rotary group is configured to require CTS, the Cisco IOS software ignores that line when CTS from the attached device is low. This feature enables the software to avoid inactive host ports automatically. To enable this feature, use the **modem bad** line configuration command.
- EIA/TIA-232 handshaking—Rotary groups are often associated with large terminal switches that require an EIA/TIA-232 handshake before forming a connection. In this case, use the **modem callout** line configuration command to configure the lines in the group. If the EIA/TIA-232 handshake fails on a line, the Cisco IOS software steps to the next free line in the rotary group and restarts the negotiation.
- Access control—You can use access lists for groups of virtual terminal lines.
- Session timeout—Use the **session-timeout** line configuration command to set an interval for a line so that if no activity occurs on a remotely initiated connection for that interval, the Cisco IOS software closes the connection. The software assumes that the host has crashed or is otherwise inaccessible.

Typically, rotary groups are used on devices with multiple modem connections to allow connection to the next free line in a hunt group. In the event that there are no free asynchronous ports, the **queued** keyword enables outgoing connection requests to be queued until a port becomes available. Periodic messages are sent to users to update them on the status of their connection request.

For a nonqueued connection request, the remote host must specify a particular TCP port on the router to connect to a rotary group with connections to an individual line. The available services are the same, but the TCP port numbers are different. Table 19 lists the services and port numbers for both rotary groups and individual lines.

Table 19 Services and Port Numbers for Rotary Groups and Lines

Services Provided	Base TCP Port for Rotaries	Base TCP Port for Individual Lines
Telnet protocol	3000	2000
Raw TCP protocol (no Telnet protocol)	5000	4000
Telnet protocol, binary mode	7000	6000
XRemote protocol	10000	9000

For example, if Telnet protocols are required, the remote host connects to the TCP port numbered 3000 (decimal) plus the rotary group number. If the rotary group identifier is 13, the corresponding TCP port is 3013.

If a raw TCP stream is required, the port is 5000 (decimal) plus the rotary group number. If rotary group 5 includes a raw TCP (printer) line, the user connects to port 5005 and is connected to one of the raw printers in the group.

If Telnet binary mode is required, the port is 7000 (decimal) plus the rotary group number.

The **by-role** keyword enables priority users to bypass the queue and access the first available line.

Note Priority users must have the privilege level of administrator(PRIV_ROOT) to take advantage of this option.

The round-robin selection algorithm enabled by the **round-robin** keyword improves the utilization of tty ports. When looking for the next available port, the default linear hunting algorithm will not roll over to the next port if the first port it finds is bad. This failure to roll over to the next port results in an inequitable utilization of the tty ports on a router. The round-robin hunting algorithm will roll over bad ports instead of retrying them.

Note The **round-robin** option must be configured for all the lines in a rotary group.

Examples

The following example establishes a rotary group consisting of virtual terminal lines 2 through 4 and defines a password on those lines. By using Telnet to connect to TCP port 3001, the user gets the next free line in the rotary group. The user need not remember the range of line numbers associated with the password.

```
line vty 2 4
 rotary 1
```

```
 password letmein
login
```

The following example enables asynchronous rotary line queueing:

```
line 1 2
 rotary 1 queued
```

The following example enables asynchronous rotary line queueing using the round-robin algorithm:

```
line 1 2
 rotary 1 queued round-robin
```

Related Commands

Command	Description
login (line)	Enables password checking at login and defines the method (local or TACACS+).
modem bad	Removes an integrated modem from service and indicates it as suspect or proven to be inoperable.
modem callout	Configures a line for reverse connections.
modem dialin	Configures a line to enable a modem attached to the router to accept incoming calls only.
session-timeout	Sets the interval for closing the connection when there is no input or output traffic.

rotary-group

To assign a request-dialout virtual private dialup network (VPDN) subgroup to a dialer rotary group, use the **rotary-group** command in request-dialout configuration mode. To remove the request-dialout VPDN subgroup from the dialer rotary group, use the **no** form of this command.

rotary-group *group-number*

no rotary-group [*group-number*]

Syntax Description

group-number	The dialer rotary group that this VPDN group belongs to.

Command Default

Disabled

Command Modes

Request-dialout configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

If the dialer pool or dialer rotary group that the VPDN group is in contains physical interfaces, the physical interfaces will be used before the VPDN group.

You must first enable the **protocol l2tp** command on the request-dialout VPDN subgroup before you can enable the **rotary-group** command. Removing the **protocol l2tp** command will remove the **rotary-group** command from the request-dialout subgroup.

You can only configure one dialer profile pool (using the **pool-member** command) or dialer rotary group (using the **rotary-group** command). If you attempt to configure a second dialer resource, you will replace the first dialer resource in the configuration.

Examples

The following example configures VPDN group 1 to request Layer 2 Tunnel Protocol (L2TP) dial-out to IP address 172.16.4.6 using dialer profile pool 1 and identifying itself using the local name router32.

```
vpdn-group 1
 request-dialout
  protocol l2tp
  rotary-group 1
 initiate-to ip 172.16.4.6
 local name router32
```

Related Commands

Command	Description
initiate-to	Specifies the IP address that will be tunneled to.
pool-member	Assigns a request-dialout VPDN subgroup to a dialer pool.
protocol (VPDN)	Specifies the L2TP that the VPDN subgroup will use.
request-dialout	Enables an LNS to request VPDN dial-out calls by using L2TP.

script activation

To specify that a chat script start on a physical terminal line any time the line is activated, use the **script activation** command in line configuration mode. To disable this feature, use the **no** form of this command.

script activation *regular-expression*

no script activation

Syntax Description

regular-expression	Regular expression that specifies the set of modem scripts that might be executed. The first script name that matches the *regular-expression* argument will be used.

Command Default

Not assigned to terminal lines

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command provides an asynchronous handshake to a user or device that activates the line. It can be activated by several events, such as a user issuing a carriage return on a vacant line, by a modem on the line sensing an incoming carrier, or an asynchronous device (such as another router) sending data. Each time an EXEC session is started on a line, the system checks to see if a **script activation** command is configured on the line. If so, and the *regular-expression* argument (a regular expression) matches an existing chat script name, the matched script is run on the line. For information about regular expressions, see the appendix "Regular Expressions" in the *Cisco IOS Dial Technologies Configuration Guide*.

The **script activation** command can mimic a login handshake of another system. For example, a system that dials into a line on a router and expects an IBM mainframe login handshake can be satisfied with an appropriate activation script.

This command also can send strings to asynchronous devices that are connecting or dialing into a router.

The **script activation** command functions only on physical terminal (tty) lines. It does not function on virtual terminal lines.

Examples

The following example specifies that the chat script with a name that includes "telebit" will be activated whenever line 4 is activated:

```
line 4
 script activation telebit
```

Related Commands

Command	Description
chat-script	Places calls over a modem and logs in to remote systems.
dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites.
script connection	Specifies that a chat script start on a physical terminal line when a remote network connection is made to a line.
script dialer	Specifies a default modem chat script.
script reset	Specifies that a chat script start on a physical terminal line when the specified line is reset.
script startup	Specifies that a chat script start on a physical terminal line when the router is powered up.
start-chat	Specifies that a chat script start on a specified line at any point.

script arap-callback

To specify that a chat script start on a line any time an AppleTalk Remote Access (ARA) client requests a callback, use the **script arap-callback** command in line configuration mode. To disable this feature, use the **no** form of this command.

script arap-callback *regular-expression*

no script arap-callback

Syntax Description

regular-expression	Regular expression that specifies the set of modem scripts that might be executed. The first script name that matches the *regular-expression* argument is used.

Command Default

Not assigned to terminal lines

Command Modes

Line configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

This command specifies that if an originating ARA client requests callback, the device will be disconnected and the chat script defined by the *regular-expression* argument will be executed to call back the client. The first available line specified for callback, and for which a chat script has been applied, will be used for the callback.

Create a chat script using the **chat script** command. The **script arap-callback** command functions only on physical terminal (tty) lines. It does not function on virtual terminal lines.

Examples

The following example specifies that a chat script with a name that includes *usr4* will be activated whenever a client requests a callback on line 4:

```
line 4
 script arap-callback usr4
```

Related Commands

Command	Description
chat-script	Places calls over a modem and logs in to remote systems.
script activation	Specifies that a chat script start on a physical terminal line when the line is activated.
script callback	Specifies that a chat script start on a line when a client requests a callback.
script connection	Specifies that a chat script start on a physical terminal line when a remote network connection is made to a line.

Command	Description
script dialer	Specifies a default modem chat script.
script reset	Specifies that a chat script start on a physical terminal line when the specified line is reset.
script startup	Specifies that a chat script start on a physical terminal line when the router is powered up.
chat-script	Places calls over a modem and logs in to remote systems.

script callback

To specify that a chat script start on a line any time a client requests a callback, use the **script callback** command in line configuration mode. To disable this feature, use the **no** form of this command.

script callback *regular-expression*

no script callback

Syntax Description

regular-expression	Regular expression that specifies the set of modem scripts that might be executed. The first script name that matches the *regular-expression* argument is used.

Command Default

Not assigned to terminal lines

Command Modes

Line configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

This command specifies that if an originating client requests callback, the device will be disconnected and the chat script defined by the *regular-expression* argument will be executed to call back the client. The first available line specified for callback, and for which a chat script has been applied, will be used for the callback. Regular expression characters and strings are described in the appendix "Regular Expressions" at the end of the *Cisco IOS Dial Technologies Configuration Guide*.

Create a chat script using the **chat script** command.

The **script callback** command functions only on physical terminal (tty) lines. It does not function on virtual terminal lines.

Examples

The following example specifies that the chat script with a name that includes supra4 will be activated whenever a client requests a callback on line 4:

```
line 4
 script callback supra4
```

Related Commands

Command	Description
chat-script	Places calls over a modem and logs in to remote systems.
script activation	Specifies that a chat script start on a physical terminal line when the line is activated.
script connection	Specifies that a chat script start on a physical terminal line when a remote network connection is made to a line.

Command	Description
script dialer	Specifies a default modem chat script.
script reset	Specifies that a chat script start on a physical terminal line when the specified line is reset.
script startup	Specifies that a chat script start on a physical terminal line when the router is powered up.
start-chat	Specifies that a chat script start on a specified line at any point.

service alignment

To configure service alignment issue detection and logging functionality, use the **service alignment** command in global configuration mode. To disable the service alignment configuration, use the **no** form of this command.

service alignment {**detection** | **logging**}

no service alignment {**detection** | **logging**}

Syntax Description

detection	Enables detection of the alignment issues.
logging	Enables logging of the alignment issues.

Command Default

The service alignment issue detection and logging functionality is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

Alignment Errors

Alignment errors are caused by misaligned reads and writes. For example, a two-byte read where the memory address is not an even multiple of two bytes is an alignment error. Alignment errors are caused by a software defect.

Alignment errors are reported in the system log and recorded by the router. Output from the **show alignment** command provides a record of these errors along with potentially useful traceback information. The traceback information for alignment errors can generally be decoded to reveal the function causing the alignment problems.

Spurious Memory Access Errors

Spurious memory access errors occur when a software process attempts to access memory in a restricted location. A read operation to this region of memory is usually caused when a nonexisting value is returned to a function in the software, or in other words, when a null pointer is passed to a function.

Spurious memory access errors are counted and recorded by the software. This information is displayed with the **show alignment** command.

Examples

The following example shows how to enable service alignment detection and logging:

```
Router# configure terminal
Router(config)# service alignment detection
Router(config)# service alignment logging
```

Related Commands

Command	Description
show alignment	Displays alignment errors and spurious memory access errors.

show caller

To display caller information, use the **show caller** command in user EXEC or privileged EXEC mode.

show caller [[[**interface** *interface-type interface-number* | **line** {[*line-modem-options*] *number* [*end-number*]}] [**full** | **timeouts**]] | [**summary** | **user** *name* [**detailed**]]]

Syntax Description

interface	(Optional) Displays a summary of caller information for the specified interface. • *interface-type*—Interface type for which to display caller information. • *interface-number*—Number of the interface for which caller information will be displayed. Valid values for the *interface-number* argument vary depending on the interface type and platform.
line	(Optional) Displays a summary of caller information for the specified line(s) or by line or modem options. • *number* [*end-number*]—Line number for which caller information will be displayed. Specifying a value for the optional *end-number* argument results in caller information being displayed for a range of line numbers. Valid values for the *number* [*end-number*] arguments vary depending on the platform. • *line-modem-options*—Type of line or modem option for which caller information will be displayed. Valid values for the *line-modem-options* argument are as follows: – **aux** *line-number*—Auxiliary line. – **console** *line-number*—Primary terminal line. – **tty** *line-number*—Terminal controller. – **v110**—V.110 modem. – **vty** *line-number*—Virtual terminal line. – *x*/*y*—Internal modem slot/port number.
full	(Optional) Provides expanded caller information and displays the total number of input and output packets on the virtual-access interface associated with a particular session.
timeouts	(Optional) Displays session and idle limits and disconnect time.
summary	(Optional) Displays total users logged, total ISDN users, total analog users, and total external signaling analog and digital calls since the last **reload** command was entered.
user *name*	(Optional) Displays a summary of caller information for the specified username. **detailed**—(Optional) Provides expanded information about the username.

Command Modes

User EXEC (>)
Privileged EXEC (#))

Command History

Release	Modification
11.3(5)AA	This command was introduced.
12.1(3)T	This command was modified. The **summary** keyword was added.
12.3(6)	This command was enhanced to display information about external signaling calls.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.
15.0(1)M	This command was modified. The **full** keyword was modified to display the details of the virtual-access interface and virtual call details of users associated with the virtual-access interface.

Usage Guidelines

The **show caller** command is used to:

- Display individual users and consumed resources on the network access server (NAS).
- Inspect active call statistics for large pools of connections. (Debugging commands produce too much output and tax the CPU too heavily.)
- Display the absolute and idle times for each user. The current values for both of these settings are displayed on the TTY line and the asynchronous interface. Users that have been idle for unacceptably long periods of time can be easily identified. By using this information, you can define timeout policies and multiple grades of services for different users.

In Multilink PPP (MLP) calls, if the MLP bundle is created on the remote home gateway, the total of unique users displayed by the **show caller summary** command is the same as the number of active B-channel calls. This is because the gateway does not know about the MLP bundle created on the other side. You can configure output modifiers for each option type of the **show caller** command.

Examples

The following example shows the caller information:

```
Router# show caller

Line      User                  Service       Active
  con 0     -                     TTY           00:08:21
  BR0:1     hatteras              PPP           00:00:14
  Vi1       hatteras              PPP   Bundle  00:00:13
```

The following example displays expanded information about the username. The output is self-explanatory.

```
Router# show caller user user_01@domain_3 detailed

User: user_01@domain_3, line Vi2.1, service PPPoE
        Connected for 01:24:59
  Timeouts:    Limit     Remaining Timer Type
               -         -         -
  PPP: LCP Open, CHAP (<-), IPCP
  NCP: Open IPCP
Vi2.1 LCP: [Open]
Our Negotiated Options
Vi2.1 LCP:    MRU 1492 (0x010405D4)
Vi2.1 LCP:    AuthProto CHAP (0x0305C22305)
Vi2.1 LCP:    MagicNumber 0x21F4CD31 (0x050621F4CD31)
Peer's Negotiated Options
```

```
Vi2.1 LCP:    MRU 1492 (0x010405D4)
Vi2.1 LCP:    MagicNumber 0x4A51A20E (0x05064A51A20E)
Vi2.1 IPCP: [Open]
Our Negotiated Options
Vi2.1 IPCP:    Address 10.0.0.1 (0x03060A000001)
Peer's Negotiated Options
Vi2.1 IPCP:    Address 12.0.0.1 (0x03060C000001)
  IP: Local 10.0.0.1, remote 12.0.0.1
  Counts: 1006 packets input, 72112 bytes
          2007 packets output, 168115 bytes
```

The following examples display details of the virtual-access interface and virtual call details of users associated with the virtual-access interface. The example also displays the total number of input and output packets on the virtual-access interface associated with a particular session. The output is self-explanatory.

```
Router# show caller user user_01@domain_3 full

User: user_01@domain_3, line Vi2.1, service PPPoE
        Connected for 01:25:05
  Timeouts:    Limit     Remaining Timer Type
               -         -         -
PPPoE Bound to ATM2/0/0.1 VCD: 4942, VPI: 42, VCI: 117
     121 packets input, 7173 bytes
     129 packets output, 12076 bytes
VCD: 4942 VBR-NRT, PeakRate: 1184, Average Rate: 1184, Burst Cells: 1
VCD: 4942 AAL5-LLC/SNAP, etype:0x0, Flags: 0x10000020, VCmode: 0x0
VCD: 4942 OAM frequency: 0 second(s)
VCD: 4942 InARP frequency: 15 minutes(s)
VCD: 4942 High Watermark: 512, Low Watermark: 256
VCD: 4942 InPkts: 116, OutPkts: 124, InBytes: 10887, OutBytes: 16004
VCD: 4942 InPRoc: 23, OutPRoc: 2, Broadcasts: 0
VCD: 4942 InFast: 0, OutFast: 0
VCD: 4942 InPktDrops: 0, OutPktDrops: 0
VCD: 4942 Out CLP=1 Pkts: 0
VCD: 4942 OAM cells received: 0
VCD: 4942 OAM cells sent: 0
VCD: 4942 Status: UPs

Router# show caller user user_01@domain_3

User: user_01@domain_3, line Vi2.1, service PPPoE
        Connected for 01:25:08
  Timeouts:    Limit     Remaining Timer Type
               -         -         -
  PPP: LCP Open, CHAP (<-), IPCP
  IP: Local 10.0.0.1, remote 12.0.0.1
  Counts: 1006 packets input, 72112 bytes
          2007 packets output, 168115 bytes
```

Each display from the **show caller** command is self-explanatory. See the “Usage Guidelines” section for more information.

script connection

To specify that a chat script will start on a physical terminal line any time a remote network connection is made to a line, use the **script connection** command in line configuration mode. To disable this feature, use the **no** form of this command.

script connection *regular-expression*

no script connection

Syntax Description

regular-expression	Set of modem scripts that can be executed. The first script name that matches the *regular-expression* argument will be used.

Command Default

Not assigned to terminal lines

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command provides modem dialing commands and commands for logging onto remote systems. The **script connection** command functions only on physical terminal (tty) lines. It does not function on virtual terminal lines.

This command can be used to initialize an asynchronous device sitting on a line to which a reverse network connection is made.

For information about regular expressions, see the appendix "Regular Expressions" in the *Cisco IOS Dial Technologies Configuration Guide*.

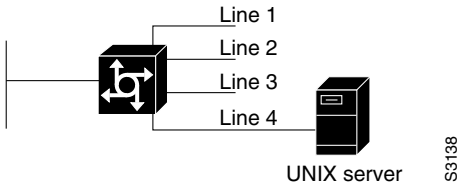
Examples

The following example specifies that the chat script with a name that includes "inband" will be activated whenever a remote connection to line 4 is established. The router can send a login string and password to the UNIX server when a network tunneling connection comes into line 4:

```
line 4
 script connection inband
```

Using this example and the topology in Figure 2, the access server or router can send a login string and password to the UNIX server when a network tunneling connection comes into line 4.

Figure 2 Network Tunneling Connection on an Asynchronous Line



Related Commands

Command	Description
chat-script	Places calls over a modem and logs in to remote systems.
dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites.
script activation	Specifies that a chat script start on a physical terminal line when the line is activated.
script dialer	Specifies a default modem chat script.
script reset	Specifies that a chat script start on a physical terminal line when the specified line is reset.
script startup	Specifies that a chat script start on a physical terminal line when the router is powered up.
start-chat	Specifies that a chat script start on a specified line at any point.

script dialer

To specify a default modem chat script, use the **script dialer** command in line configuration mode. To disable this feature, use the **no** form of this command.

script dialer *regular-expression*

no script dialer

Syntax Description

regular-expression	Set of modem scripts that can be executed. The first script that matches the *regular-expression* argument will be used.

Command Default

No chat script is defined.

Command Modes

Line configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

This command is used by DDR modules to provide modem dialing commands and commands to log in to remote systems.

The *regular-expression* argument is used to specify the name of the modem script that is to be executed. The first script that matches the argument in this command and the **dialer map** command will be used. For information about regular expressions, see the appendix "Regular Expressions" in the *Cisco IOS Dial Technologies Configuration Guide*.

If you adhere to the naming convention recommended for chat scripts (see the **chat-script** command), the modem lines (the *regular-expression* argument in the **script dialer** command) will be set to one of the following regular expressions to match patterns, depending on the kind of modem you have:

- **codex-.***
- **telebit-.***
- **usr-.***
- **xyz-.***

In the **dialer map** command, you can specify the modulation but leave the type of modem unspecified, as in *.*-v32bis*.

Examples

The following example shows line chat scripts being specified for lines connected to Telebit and US Robotics modems:

```
! Some lines have telebit modems
line 1 6
script dialer telebit.*
```

```
!
! Some lines have US robotics modems
line 7 12
script dialer usr.*
```

Related Commands

Command	Description
chat-script	Places calls over a modem and logs in to remote systems.
dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites.
script activation	Specifies that a chat script start on a physical terminal line when the line is activated.
script connection	Specifies that a chat script start on a physical terminal line when a remote network connection is made to a line.
script reset	Specifies that a chat script start on a physical terminal line when the specified line is reset.
script startup	Specifies that a chat script start on a physical terminal line when the router is powered up.
start-chat	Specifies that a chat script start on a specified line at any point.

script reset

To specify that a chat script will start on a physical terminal line any time the specified line is reset, use the **script reset** command in line configuration mode. To disable this feature, use the **no** form of this command.

script reset *regular-expression*

no script reset

Syntax Description

regular-expression	Set of modem scripts that might be executed. The first script name that matches the *regular-expression* argument will be used.

Command Default

Not assigned to terminal lines.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Chat scripts provide modem dialing commands and commands for logging onto remote systems. Use this command to reset a modem attached to a line every time a call is dropped.

The **script reset** command functions only on physical terminal (tty) lines. It does not function on virtual terminal lines.

For information about regular expressions, see the appendix "Regular Expressions" in the *Cisco IOS Dial Technologies Configuration Guide*.

Examples

The following example specifies that any chat script name with the word "linebackup" in it will be activated any time line 7 is reset:

```
line 7
 script reset linebackup
```

The following example resets a modem sitting on a line each time a call is dropped:

```
chat-script drop-line ""+++"" " " ATH OK "ATS0=1" OK "ATS9=21"
line 4
 script reset drop-line
```

Related Commands

Command	Description
chat-script	Places calls over a modem and logs in to remote systems.
dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites.
script activation	Specifies that a chat script start on a physical terminal line when the line is activated.
script connection	Specifies that a chat script start on a physical terminal line when a remote network connection is made to a line.
script dialer	Specifies a default modem chat script.
script startup	Specifies that a chat script start on a physical terminal line when the router is powered up.
start-chat	Specifies that a chat script start on a specified line at any point.

script startup

To specify that a chat script will start on a physical terminal line any time the router is powered up, use the **script startup** command in line configuration mode. To disable this feature, use the **no** form of this command.

script startup *regular-expression*

no script startup

Syntax Description

regular-expression	Set of modem scripts that might be executed. The first script that matches the *regular-expression* argument will be used.

Command Default

Not assigned to terminal lines

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command to initialize asynchronous devices connected to a line when the router is started up or reloaded. You can also use it to start up a banner other than the default banner on lines. The **script startup** command functions only on physical terminal (tty) lines. It does not function on virtual terminal lines.

For information about regular expressions, see the appendix "Regular Expressions" in the *Cisco IOS Dial Technologies Configuration Guide*.

Examples

The following example specifies that a chat script with the word "linestart" in its name will be activated whenever line 5 is started up:

```
line 5
 script startup linestart
```

Related Commands

Command	Description
chat-script	Places calls over a modem and logs in to remote systems.
dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites.
script activation	Specifies that a chat script start on a physical terminal line when the line is activated.
script connection	Specifies that a chat script start on a physical terminal line when a remote network connection is made to a line.

Command	Description
script dialer	Specifies a default modem chat script.
script reset	Specifies that a chat script start on a physical terminal line when the specified line is reset.
start-chat	Specifies that a chat script start on a specified line at any point.

set ip next-hop dynamic dhcp

To set the next hop to the gateway that was most recently learned by the Dynamic Host Configuration Protocol (DHCP) client, use the **set ip next-hop dynamic dhcp** command in route-map configuration mode. To restore the default setting, use the **no** form of this command.

set ip next-hop dynamic dhcp

no set ip next-hop dynamic dhcp

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

Route-map configuration (config-router)

Command History

Release	Modification
12.3(2)XE	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

The **set ip next-hop dynamic dhcp** command supports only a single DHCP interface. If multiple interfaces have DHCP configured, the gateway that was most recently learned among all interfaces running DHCP will be used by the route map.

Examples

The following example shows how to configure a local routing policy that sets the next hop to the gateway that was most recently learned by the DHCP client:

```
access list 101 permit icmp any host 172.16.23.7 echo
route map MY-LOCAL-POLICY permit 10
 match ip address 101
 set ip next-hop dynamic dhcp
!
ip local policy route-map MY-LOCAL-POLICY
```

Related Commands

Command	Description
access list (IP extended)	Defines an extended IP access list.

sgbp dial-bids

To allow the stack group to bid for dialout connection, use the **sgbp dial-bids** command in global configuration mode. To disable this function, use the **no** form of this command.

sgbp dial-bids

no sgbp dial-bids

Syntax Description

This command has no arguments or keywords.

Command Default

The stack group bid function is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Examples

The following example shows how to configure a stack group for large-scale dialout:

```
sgbp group forever
sgbp member NAS2 172.21.17.17
sgbp dial-bids
```

Related Commands

Command	Description
dialer congestion-threshold	Specifies congestion threshold in connected links.
dialer reserved-links	Reserves links for dialin and dialout.
sgbp group	Defines a named stack group and makes this router a member of that stack group.
sgbp member	Specifies the hostname and IP address of a router or access server that is a peer member of a stack group.

sgbp group

To define a named stack group and make this router a member of that stack group, use the **sgbp group** command in global configuration mode. To remove the definition, use the **no** form of this command.

sgbp group *name*

no sgbp group

Syntax Description

name	Name of the stack group the system belongs to.

Command Default

Disabled. No stack group name is provided.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Define the same stack group name across all the stack members.

Examples

The following example makes this system a member of the stack group named “stackq”:

```
sgbp group stackq
```

Related Commands

Command	Description
sgbp member	Specifies the host name and IP address of a router or access server that is a peer member of a stack group.
sgbp seed-bid	Sets the bidding level that a stack group member can be used to bid for a bundle.

sgbp member

To specify the hostname and IP address of a router or access server that is a peer member of a stack group, use the **sgbp member** command in global configuration mode. To remove the member association, use the **no** form of this command.

sgbp member *peer-name* [*peer-ip-address*]

no sgbp member *peer-name*

Syntax Description

peer-name	Hostname of the peer member.
peer-ip-address	(Optional) IP address of the peer member. If the domain name system (DNS) can perform a lookup on the *peer-name* value, the IP address is not required. Otherwise, it must be specified.

Defaults

Disabled. When enabled, names and IP addresses of peer routers or access servers in the stack group are not provided.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use this command to specify the names of peer hosts (other hosts, not the one being configured) in the specified stack group after you have entered the **sgbp dial-bids** command.

Note In Cisco IOS Release 15.1T and later releases, you cannot configure the peer hosts with invalid IP host addresses such as 0.0.0.0, 255.255.255.255, and so on..

Examples

The following example shows how to configure the current router to recognize the three routers (west, east, and south) as peer members of the stack group named mystackgroup:

```
sgbp group mystackgroup
sgbp member west 10.69.5.2
sgbp member east 172.16.6.3
sgbp member south 192.168.15.4
```

Related Commands

Command	Description
sgbp dial-bids	Defines a named stack group and makes this router a member of that stack group.
sgbp seed-bid	Sets the bidding level that a stack group member can be used to bid for a bundle.

sgbp ppp-forward

To enable forwarding of PPP calls—in addition to Multilink PPP (MLP) calls—to the winner of the Stack Group Bidding Protocol (SGBP) bid, use the **sgbp ppp-forward** command in global configuration mode. To return to the default state, use the **no** form of this command.

sgbp ppp-forward

no sgbp ppp-forward

Syntax Description

This command has no arguments or keywords.

Defaults

Only Multilink PPP calls are forwarded.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

When this command is enabled, both PPP and Multilink PPP calls are projected to the winner of the SGBP bid.

Examples

The following partial example enables forwarding of PPP calls, as well as MLP calls, to the winner of the SGBP bidding:

```
sgbp ppp-forward
```

Related Commands

Command	Description
sgbp member	Specifies the host name and IP address of a router or access server that is a peer member of a stack group.
sgbp seed-bid	Sets the bidding level that a stack group member can be used to bid for a bundle.

sgbp protocol

To set a specific tunneling protocol to use for Stack Group Bidding Protocol (SGBP), use the **sgbp protocol** command in global configuration mode. To change this command back to its default, use the **no** form of this command.

sgbp protocol {**any** | **l2f** | **l2tp**}

no sgbp protocol

Syntax Description

any	Negotiates which tunneling protocol to use. There is a preference for L2TP if both devices support it. This is the default.
l2f	Uses Layer 2 Forwarding (L2F) as the tunneling protocol.
l2tp	Uses Layer 2 Tunneling Protocol (L2TP) as the tunneling protocol.

Command Default

The **any** keyword is the default, which allows L2TP and L2F to be offered by a stack group member when bidding on a call, and allows bids with either L2TP or L2F to be accepted by the stack group member on which the call arrived.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.4(11)T	The **l2f** keyword was removed.

Usage Guidelines

This command is needed when both routers support both L2F and L2TP, but there is a preference that L2F be used between the stack group members instead of L2TP.

Note When two routers are trying to create a protocol-specific tunnel and each is explicitly set with different protocols—for example, one router is explicitly set for L2TP and the other is explicitly set for L2F—they will not be able to create the tunnel, and communication will fail.

Examples

The following example shows how to configure a stack group for large-scale dialout and set L2F as the tunneling protocol:

```
sgbp group forever
sgbp member NAS2 172.21.17.17
sgbp dial-bids
sgbp protocol l2f
```

Related Commands

Command	Description
sgbp group	Defines a named stack group and makes this router a member of that stack group.
sgbp member	Specifies the host name and IP address of a router or access server that is a peer member of a stack group.
sgbp seed-bid	Sets the bidding level that a stack group member can be bid with for a bundle.

sgbp seed-bid

To set the bidding level that a stack group member can bid with for a bundle, use the **sgbp seed-bid** command in global configuration mode. To return to the default state, use the **no** form of this command.

sgbp seed-bid {**default** | **offload** | **forward-only** | *bid*}

no sgbp ppp-forward

Syntax Description

default	If set across all members of a stack group, indicates that the member which receives the first call for a certain user always wins the bid and hosts the master bundle interface. All subsequent calls to the same user received by another stack group member will *project* to this stackgroup member. This is the default.
offload	Indicates that this router is a relatively higher powered stack group member, is to function as an offload server, and host the master bundle interface.
forward-only	Indicates that this router or access server is to forward calls to another system and never wins the bid to host a master interface. This router or access server should hang up—instead of answering a call—if all the offload servers are down.
bid	Bid level, an integer in the range 0 through 9999.

Command Default

The **default** keyword; no bid-level integer value is set.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

In the case of equivalent stack group members stacked to receive calls in a rotary group across multiple PRIs, use the **sgbp seed-bid default** command across all stack members. The stack member that receives the first call for a certain user always wins the bid and hosts the master bundle interface. All subsequent calls to the same user received by another stack member will project to this stack member. If the multiple calls come in concurrently over multiple stack members, the SGBP tie-breaking mechanism will break the tie.

To leverage the relative higher power of one stack member over another, you can set the designated stack member (of higher CPU power) as offload server with the **sgbp seed-bid offload command**. The bid that is sent is the precalibrated per-platform bid approximating the CPU power, minus the *bundle load.* In this case, the offload server hosts the master bundle. All calls from other stack members get projected to this stack member. One or more offload servers can be defined—if the bids are equal, the SGBP tie-breaking mechanism will break the tie.

The interfaces that received the calls are projected to the master bundle interface and are considered children of the master bundle interface for the call. See the output of the **show ppp multilink** command for an example of master bundle interface (shown as “Master link”) and the children of it.

You can also manually designate bid values with the **sgbp seed-bid** command. This value overrides the **default** or **offload** setting. The bid sent out is the user-configured value minus the *bundle load.* The *bundle load* is defined as the number of active bundles on the stack member. In effect, the more current active bundles on a router, the lower its bid for an additional bundle.

If you have assorted or exactly the same platforms and for some reason want to designate one or more as offload servers, you can *manually* set the bid value to be significantly higher than the rest. For example, you might use the **sgbp seed-bid 9999 command**. To determine the initial bid value associated with your particular platform**,** use the **show sgbp** command. This method allows you to manually designate the bid values when you have assorted platforms and want to designate one or more platforms as offload servers; for example, one Cisco 4700 (given the highest seed-bid), two Cisco 4000s and one Cisco 7000.

To check the bid value currently assigned on the system, use the **show sgbp queries** command.

Examples

The following example sets the SGBP bidding level to forward-only:

```
sgbp seed-bid forward-only
```

Related Commands

Command	Description
sgbp dial-bids	Defines a named stack group and makes this router a member of that stack group.
sgbp member	Specifies the host name and IP address of a router or access server that is a peer member of a stack group.
show ppp multilink	Displays bundle information for MLP bundles.
show sgbp	Displays the status of the stack group members.
show sgbp queries	Displays the current SGBP seed bid value.

sgbp source-ip

To specify the source IP address for a stack member that matches the locally defined IP address for the same stack member in the specified group, use the **sgbp source-ip** command in global configuration mode. To disable the configuration, use the **no** form of this command.

sgbp source-ip *source-ip-address*

no sgbp source-ip

Syntax for 12.4M and 12.2S Releases

sgbp source-ip *source-ip-address*

no sgbp source-ip *source-ip-address*

Syntax Description

source-ip-address	Source IP address of the stack member.

Defaults

The command is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
12.2S	This command was modified. The *source-ip-address* argument was added to the **no** form of the command.
12.4M	This command was integrated into Cisco IOS Release 12.4M.
15.1T	This command was modified. The *source-ip-address* argument was removed from the **no** form of the command.

Usage Guidelines

Use this command to specify the source IP address for a stack member in the specified stack group after you have entered the **sgbp dial-bids** and the **sgbp group** commands. This source IP address must match the source IP address of the other stack members. This source IP address will be used in outgoing messages.

This command is used to override the IP address of the physical interface when sending Stack Group Bidding Protocol (SGBP) packets. Configuring the **no** form of the command removes the command, and the IP address of the physical interface is used when sending the traffic.

Note In Cisco IOS Release 15.1T and later releases, you cannot configure invalid IP host addresses such as 0.0.0.0, 255.255.255.255, and so on.

Examples

The following example shows how to specify the source IP address for a stack member:

```
sgbp group mystackgroup
sgbp source-ip 192.168.2.1
```

Related Commands

Command	Description
sgbp dial-bids	Allows the stack group to bid for dialout connection.
sgbp group	Defines a named stack group and makes this router a member of that stack group.

shelf-id

To change the shelf number assigned to the router shelf or dial shelf on the Cisco AS5800, use the **shelf-id** command in global configuration mode. To return the shelf numbers to the default value, use the **no** form of this command.

shelf-id *number* {**router-shelf** | **dial-shelf**}

no shelf-id *number*

Syntax Description

number	Number to assign to the shelf. Range is from 0 to 9999.
router-shelf	Specified number to the router shelf.
dial-shelf	Specified number to the dial shelf.

Command Default

The default shelf number for the router shelf is 0.

The default shelf number for the dial shelf is 1, or one number higher than the specified router shelf number.

Command Modes

Global configuration

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The shelf number is used to distinguish between cards on the router shelf and cards on the dial shelf.

Caution You must reload the Cisco AS5800 for the shelf number to take effect. The shelf numbers are part of the interface names. When you reload the Cisco AS5800, all NVRAM interface configuration information is lost.

You can specify the shelf number through the setup facility during initial configuration of the Cisco AS5800. This is the recommended method to specify shelf numbers.

To display the shelf numbers, use the **show running-config** command. If a shelf number has been changed, the pending change is shown in the output of the **show version** command (for example, the dial-shelf ID is 87; will change to 2 on reload).

Examples

In the following example, the dial shelf is assigned the number 456:

```
Router(config)# shelf-id 456 dial-shelf
Router(config)# exit
```

Related Commands

Command	Description
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

show async status

To display the status of activity on all lines configured for asynchronous support, use the **show async status** command in privileged EXEC mode.

show async status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The display resulting from this command shows all asynchronous sessions, whether they are using Serial Line Internet Protocol (SLIP) or PPP encapsulation.

Examples

The following is sample output from the **show async status** command:

```
Router# show async status

Async protocol statistics:
  Rcvd: 5448 packets, 7682760 bytes
        1 format errors, 0 checksum errors, 0 overrun, 0 no buffer
  Sent: 5455 packets, 7682676 bytes, 0 dropped


 Tty           Local           Remote Qd InPack OutPac Inerr  Drops  MTU Qsz
   1     192.168.7.84          Dynamic  0      0      0     0      0 1500  10
*  3     192.168.7.98             None  0   5448   5455     1      0 1500  10
```

Table 20 describes the significant fields shown in the display.

Table 20 show async status Field Descriptions

Field	Description
Rcvd	Statistics on packets received.
5448 packets	Packets received.
7682760 bytes	Total number of bytes.
1 format errors	Spurious characters received when a packet start delimiter is expected.
0 checksum errors	Count of checksum errors.
0 overrun	Number of giants received.
0 no buffer	Number of packets received when no buffer was available.
Sent	Statistics on packets sent.

Table 20 show async status Field Descriptions (continued)

Field	Description
5455 packets	Packets sent.
7682676 bytes	Total number of bytes.
0 dropped	Number of packets dropped.
Tty	Line number.
*	Line currently in use.
Local	Local IP address on the link.
Remote	Remote IP address on the link; “Dynamic” indicates that a remote address is allowed but has not been specified; “None” indicates that no remote address is assigned or being used.
Qd	Number of packets on hold queue (Qsz is the maximum).
InPack	Number of packets received.
OutPac	Number of packets sent.
Inerr	Number of total input errors; sum of format errors, checksum errors, overruns and no buffers.
Drops	Number of packets received that would not fit on the hold queue.
MTU	Current maximum transmission unit size.
Qsz	Current output hold queue size.

show backup

To display interface backup status, use the **show backup** command in user EXEC or privileged EXEC mode.

show backup

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0	This command was introduced.
12.2(13)T	This command was enhanced to show primary and secondary interfaces configured as backup interfaces.
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.

Usage Guidelines

Use the **show backup** command to display the status of backup interfaces. This command is especially useful when dual serial X.25 interfaces are configured as primary and backup in a telco data communication network (DCN).

In Cisco IOS Release 12.2(33)SRB1 and later releases, you can use the command to display the status of a backup Gigabit Ethernet interface on the Cisco 7600 series router.

Examples

The following example shows a typical display from the **show backup** command. The output is self-explanatory.

```
Router# show backup

Primary Interface   Secondary Interface   Status
-----------------   -------------------   ------
Serial0/0           Serial0/1             active backup
```

The following example shows a single backup interface on the Cisco 7600 router:

```
Router# show backup

Primary Interface     Secondary Interface    Status
-----------------     -------------------    ------
GigabitEthernet3/0/0  GigabitEthernet3/0/11  normal operation
```

Related Commands

Command	Description
backup active interface	Activates primary and backup lines on specific X.25 interfaces.
debug backup	Monitors the transitions of an interface going down then back up.

show busyout

To display the busyout status for a card on the dial shelf, use the **show busyout** command in privileged EXEC mode.

show busyout *shelf*[**/***slot*[**/***port*]]

Syntax Description

shelf[**/***slot*[**/***port*]]	Shelf number and, optionally for a specific report about a card, a slot and a port number; for example, 1/0/5. Commands entered without the slot or port number provide reports about all cards on the dial shelf. The forward slash (**/**) is required.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.

Usage Guidelines

Use the **busyout** EXEC command or the **ds0 busyout** controller command to configure modem busyout.

Examples

The following is sample output from the **show busyout** command for a trunk card in slot 4 located in dial shelf 1, with busyout pending:

```
Router# show busyout 1/4

Controller t1 busyout status:
(s - static d - dynamic p - pending)
1/4/0  :ppppppppppppppppppppppp.
1/4/1  :sssssssssssssssssssss.
1/4/2  :ppppppppppppppppppppppp.
1/4/3  :ddddddddddddddddddddddd.
1/4/4  :ppppppppppppppppppppppp.
1/4/5  :ppppppppppppppppppppppp.
1/4/6  :ppppppppppppppppppppppp.
1/4/7  :sssssssssssssssssssss.
1/4/8  :ppppppppppppppppppppppp.
1/4/9  :ppppppppppppppppppppppp.
1/4/10 :ddddddddddddddddddddddd.
1/4/11 :ppppppppppppppppppppppp.
Router#
```

See Table 21 to further interpret the display.

The following is sample output from the **show busyout** command for a modem card in shelf 1, slot 9, and indicates the busyout is complete:

```
Router# show busyout 1/9

Slot 1/9: Busyout (no calls remaining)
```

The following is sample output from the **show busyout** command, the **busyout** command, the **ds0 busyout** command, and another **show busyout** command:

```
Router# show busyout 1/0

Controller t1 busyout status:
(s - static d - dynamic p - pending)
1/0/0  :ppppppppppppppppppppppp.
1/0/1  :ppppppppppppppppppppppp.
1/0/2  :ppppppppppppppppppppppp.
1/0/3  :ddddddddddddddddddddddd.
1/0/4  :ppppppppppppppppppppppp.
1/0/5  :ppppppppppppppppppppppp.
1/0/6  :ppppppppppppppppppppppp.
1/0/7  :sssssssssssssssssssss.
1/0/8  :ppppppppppppppppppppppp.
1/0/9  :ppppppppppppppppppppppp.
1/0/10 :ddddddddddddddddddddddd.
1/0/11 :ppppppppppppppppppppppp.


Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router (config)# controller t1 1/0/1
Router (config-controller)# busyout
Router (config-controller)# ds0 busyout 15-24
Router (config-controller)# end


Router# show busyout 1/0

Controller t1 busyout status:
(s - static d - dynamic p - pending)
1/0/0  :ppppppppppppppppppppppp.
1/0/1  :sssssssssssssssssssss.
1/0/2  :ppppppppppppppppppppppp.
1/0/3  :ddddddddddddddddddddddd.
1/0/4  :ppppppppppppppppppppppp.
1/0/5  :ppppppppppppppppppppppp.
1/0/6  :ppppppppppppppppppppppp.
1/0/7  :sssssssssssssssssssss.
1/0/8  :ppppppppppppppppppppppp.
1/0/9  :ppppppppppppppppppppppp.
1/0/10 :ddddddddddddddddddddddd.
1/0/11 :ppppppppppppppppppppppp.
```

Table 21 describes the significant fields shown in the **show busyout** displays.

Table 21 show busyout Field Descriptions

Field	Description
s - static	The channel is in an out-of-service state because of a **busyout** command.
d - dynamic	The channel is automatically put in an out-of-service state because of a preset and defined threshold. By default, this feature is disabled. This autobusyout function of the **modem busyout-threshold** global configuration command is used to define a threshold when you want to maintain a balance between the number of DS0s and modems.
p - pending	After you hang up, the established call is terminated because of a **busyout** command. After the call terminates, the DS0 is busied out.

Related Commands

Command	Description
busyout	Informs the central-office switch that a channel is out of service.
ds0 busyout (channel)	Forces a DS0 time slot on a controller into the busyout state.
modem busyout	Disables a modem from dialing or answering calls whereby the disabling action is not executed until the active modem returns to an idle state.
modem busyout-threshold	Maintains a balance between the number of DS0s and modems.
modem shutdown	Abruptly shuts down an active or idle modem installed in an access server or router.

show call calltracker active

To display all information stored within the Call Tracker active database for all active calls, use the **show call calltracker active** command in user EXEC or privileged EXEC mode.

show call calltracker active [**category** *call-type* | **service** *session-type*] [**reverse**]

Syntax Description

category	(Optional) Displays Call Tracker data for a specific type of call. The default is to display all calls, regardless of type. When the **category** keyword is specified with one of the values for the *call-type* argument, Call Tracker displays only calls whose records indicate that category.
call-type	(Optional) Call type for the calls stored within the Call Tracker active database table. Enter one of the following values: • **isdn**—Displays Call Tracker data for ISDN sync data calls. • **lapb-ta**—Displays Call Tracker data for Link Access Procedure, Balanced (LAPB) calls. • **modem**—Displays Call Tracker data for analog modem calls. • **other**—Displays Call Tracker data for other call categories. • **syncData**—Displays Call Tracker data for sync data calls for call control other than ISDN. • **v110**—Displays Call Tracker data for V.110 calls. • **v120**—Displays Call Tracker data for V.120 calls.
service	(Optional) Displays Call Tracker data with a filter restricting output based on the session type. When the **service** keyword is specified with one of the values for the *session-type* argument, Call Tracker displays only calls whose records indicate that session type.
session-type	(Optional) Session type for the calls stored within the Call Tracker active database table. Enter one of the following values: • **exec**—Displays Call Tracker data for EXEC sessions. • **l2f**—Displays Call Tracker data for Layer 2 Forwarding (L2F) sessions. • **l2tp**—Displays Call Tracker data for Layer 2 Tunnel Protocol (L2TP) sessions. • **mp**—Displays Call Tracker data for Multilink PPP (MLP) sessions. • **other**—Displays Call Tracker data for other sessions. • **ppp**—Displays Call Tracker data for PPP sessions. • **slip**—Displays Call Tracker data for Serial Line Internet Protocol (SLIP) sessions. • **tcpclear**—Displays Call Tracker data for TCP/Clear sessions. • **telnet**—Displays Call Tracker data for Telnet sessions.
reverse	(Optional) Displays Call Tracker data in inverted sorting order, from most recent to least recent.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.1(2)XH	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.2(2)XA	This command was implemented on the Cisco AS5350.
12.2(2)XB1	This command was integrated into Cisco IOS Release 12.2(2)XB1.
12.2(11)T	This command was modified. The **reverse** and **service** keywords were added.
12.3(7)YB	This command was modified. The signaling type field was added to the command output and the category field was modified to display V120, lapb, or syncData for autodetected calls.
12.4(6)T	This command was modified. Support for the signaling type field and the modified category field was added.

Usage Guidelines

Call Tracker is enabled by entering the **calltracker enable** command. If there is no call on the specified port, the information for the most recent call is displayed.

Issuing the **show call calltracker active** command displays all calls, regardless of type. The call history display can be filtered by call type or session type by issuing one of the optional keyword and argument pairs.

For all tabular forms of the **show call calltracker active** command, the sorting order may be inverted by using the **reverse** keyword to give most-recent to least-recent collation.

Examples

The following example shows all Call Tracker activity in reverse order, from most recent to least recent. The entries are sorted by call handle, from highest to lowest. The example is for an autodetected LAPB call.

```
Router# show call calltracker active reverse

-------------------------- call handle=        16 --------------------------
status=Active, service=PPP, origin=Answer, category=lapb,
DS0 slot/port/ds1/chan=1/0/0/22, called=5555, calling=(n/a)
userid=user1, ip=10.1.1.50, mask=0.0.0.0
setup=11/12/2000 20:30:50, conn=0.02, phys=0.12, service=0.78, authen=0.75
init rx/tx b-rate=64000/64000, rx/tx chars=2746/2719
resource slot/port=(n/a)/(n/a), mp bundle=0, charged units=0, account id=37
idb handle=0x656CA08C, tty handle=0x65AFD05C, tcb handle=0x00000000,
signaling=Auto
.
.
.
```

Table 22 describes the significant fields shown in the display.

Table 22 show call calltracker active reverse Field Descriptions

Field	Description
status	Status of the calls in the active database.
service	Session type for the call.
origin	Indicates how the call was created: • Originate—Dialout. The call was initiated locally, and the system sends the setup request. • Answer—Dialin. The call was initiated remotely, and the system receives the setup request.
category	Call type category. For autodetected calls, the values are V120, lapb, or syncData.
DS0 slot/port/ds1/chan	Number of the slot in the chassis, the applique that is being used (in the case of a card that supports multiple DS3 controllers), the DS1 trunk within the controller, and the channel, or time slot, within the DS1 trunk on which the call resides.
called	The called telephone number for this call.
calling	The calling telephone number for this call.
userid	The user login ID or zero-length string if unavailable.
ip	IP address assigned for the call, or 0.0.0.0 if not applicable or unavailable.
mask	The IP subnet mask assigned for this call. No IP subnet mask displays if the IP subnet mask is NULL.
setup	The time when the call was indicated to the NAS, for instance by the telecommunications network.
conn	The time, relative to the setup time, when the connection was established between the time slot of the incoming call and the appropriate local resources in the NAS such as the digital signal processor (DSP).
phys	The time, relative to the setup time, when the physical link became ready. For a modem, this time would be when the carrier came up and error control and compression were completely negotiated.
service	The time, relative to the setup time, when the service was determined for the call type.
authen	The time, relative to the setup time, when the user credentials were authenticated. Authentication may involve a Challenge Handshake Authentication Protocol (CHAP) challenge or response authentication for a PPP call, and the associated delay, through RADIUS or TACACS, in the external lookup.
signaling	Signaling type. Valid values are: • Auto—Autodetected calls. • LLC—ISDN signaled calls. • Xtrnl—External signaling protocols, such as Media Gateway Control Protocol (MGCP). • Unknwn—Unknown signaling types.

Related Commands

Command	Description
calltracker enable	Enables Call Tracker on the access server.
show call calltracker handle	Displays all information stored within the Call Tracker active or history database table for a specified unique call handle identifier.
show call calltracker history	Displays all information stored within the Call Tracker history database table for the most recent historical calls.
show call calltracker summary	Displays Call Tracker activity and configuration information such as the number of active calls and the history table attributes.

show call calltracker handle

To display all information stored within the Call Tracker active or history database table for a specified unique call handle identifier, use the **show call calltracker handle** command in privileged EXEC mode.

show call calltracker handle *call-identifier*

Syntax Description

call-identifier	Unique call identifier (*handle*) assigned by Call Tracker from the moment a DS0 B channel is requested. This identifier is a sequential number starting with handle 1.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

Each call managed by Call Tracker is assigned a unique call handle that is provided to users using the Simple Network Management Protocol (SNMP), the command line interface, or SYSLOG for all forms of data transfers. Knowing this call handle makes it easier to display the information desired for a given call than to manually search through all Call Tracker database tables for latest updates.

Examples

The following is sample output from the **show call calltracker handle** command:

```
Router# show call calltracker handle 30

------------------------- call handle=0000000030 -------------------------
status=History, service=None, origin=Answer, category=Other
DS0 slot/cntr/chan=0/0/22, called=71071, calling=6669999
userid=(n/a), ip=0.0.0.0, mask=0.0.0.0
setup=10/16/1999 18:29:20, conn=0.00, phys=0.00, service=0.00, authen=0.00
init rx/tx b-rate=0/0, rx/tx chars=0/0
resource slot/port=(n/a)/(n/a), mp bundle=0, charged units=0, account id=0
duration(sec)=0.00, disc subsys=CSM, disc code=0x1A
disc text=Failed to find DSP resource
---------------------------------------------------------------------------
```

See Table 22 on page 760 for a description of significant fields displayed by this command.

Related Commands

Command	Description
show call calltracker active	Displays all information stored within the Call Tracker active database for all active calls.
show call calltracker history	Displays all the information stored within the Call Tracker history database table for the most recent disconnected calls.
show call calltracker summary	Displays Call Tracker activity and configuration information such as the number of active calls and the history table attributes.

show call calltracker history

To display all information stored within the Call Tracker history database table for the most recent historical calls, use the **show call calltracker history** command in user EXEC or privileged EXEC mode.

show call calltracker history [**category** *call-type* | **service** *session-type* | **subsystem** *subsystem-type*] [**reverse**]

Syntax Description

category	(Optional) Displays Call Tracker data for a specific type of call. The default is to display all calls, regardless of type. When the **category** keyword is issued with one of the values for the *call-type* argument, Call Tracker displays only calls whose records indicate that category.
call-type	(Optional) Call type for the calls stored within the Call Tracker history database table. Enter one of the following values: • **isdn**—Displays Call Tracker data for ISDN calls. • **lapb-ta**—Displays Call Tracker data for Link Access Procedure, Balanced (LAPB) calls. • **modem**—Displays all of the information calls. • **other**—Displays Call Tracker data for other call categories. • **syncData**—Displays Call Tracker data for sync data calls for call control other than ISDN. • **v110**—Displays Call Tracker data for V.110 calls. • **v120**—Displays Call Tracker data for V.120 calls.
service	(Optional) Displays Call Tracker data with a filter restricting output based on the session type. When the **service** keyword is specified with one of the values for the *session-type* argument, Call Tracker displays only calls whose records indicate that session type.
session-type	(Optional) Session type for the calls stored within the Call Tracker history database table. Enter one of the following values: • **exec**—Displays Call Tracker data for EXEC sessions. • **l2f**—Displays Call Tracker data for Layer 2 Forwarding (L2F) sessions. • **l2tp**—Displays Call Tracker data for Layer 2 Tunnel Protocol (L2TP) sessions. • **mp**—Displays Call Tracker data for Multilink PPP (MLP) sessions. • **other**—Displays Call Tracker data for other sessions. • **ppp**—Displays Call Tracker data for PPP sessions. • **slip**—Displays Call Tracker data for Serial Line Internet Protocol (SLIP) sessions. • **tcpclear**—Displays Call Tracker data for TCP/Clear sessions.

subsystem	(Optional) Displays Call Tracker historical data with a filter restricting output based on the Cisco IOS subsystem that was responsible for terminating the call. When the **subsystem** keyword is specified with one of the values for the *subsystem-type* argument, Call Tracker displays only those historical calls whose records indicate that they were terminated by that type of subsystem.
subsystem-type	(Optional) Subsystem type responsible for terminating calls stored within the Call Tracker history database table. Enter one of the following values: • **admin**—Displays Call Tracker data for calls terminated by the Admin subsystem. • **csm**—Displays Call Tracker data for calls terminated by the Cisco Service Management subsystem. • **exec**—Displays Call Tracker data for calls terminated by the Exec subsystem. • **isdn**—Displays Call Tracker data for calls terminated by the ISDN subsystem. • **mica**—Displays Call Tracker data for calls terminated by the Mica Drivers subsystem. • **modem**—Displays Call Tracker data for calls terminated by the Modem Management subsystem. • **none**—Displays Call Tracker data for calls not terminated by a subsystem. • **ppp**—Displays Call Tracker data for calls terminated by the PPP subsystem. • **rpm**—Displays Call Tracker data for calls terminated by the Resource Pool Management (RPM) subsystem. • **vpn**—Displays Call Tracker data for calls terminated by the Virtual Private Network (VPN) subsystem. • **vtsp**—Displays Call Tracker data for calls terminated by the Voice Telephony Service Provider (VTSP) subsystem. **Note** Although this information requires a more detailed understanding of Cisco IOS software than the average user possesses, it is useful to Cisco Technical Support personnel for troubleshooting connection issues.
reverse	(Optional) Displays Call Tracker data in inverted sorting order, from most recent to least recent.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(11)T	This command was modified. The **reverse**, **service**, and **subsystem** keywords were added.
12.3(7)YB	This command was modified. The sig type field was added to the command output and the category field was modified to display V120, LAPB, or syncData for autodetected calls.
12.4(6)T	This command was modified. Support for the signaling type field and the modified category field was added.

Usage Guidelines

Call Tracker is enabled by entering the **calltracker enable** command.

Issuing the **show call calltracker history** command displays the call history for all calls, regardless of type. The call history display can be filtered by call type, session type, or by the Cisco IOS subsystem responsible for terminating the call by issuing one of the optional keyword and argument pairs.

For all tabular forms of the **show call calltracker history** command, the sorting order may be inverted by using the **reverse** keyword to give most-recent to least-recent collation.

Examples

The following sample shows Call Tracker historical data for an outgoing modem-to-Layer 2 Transport (L2TP) Virtual Private Network (VPN) tunneled call that was disconnected by the ISDN subsystem:

```
Router# show call calltracker history subsystem isdn

--------------------------- call handle=0000000002 ----------------------
status=History, service=L2TP, origin=Answer, category=Modem
DS0 slot/port/ds1/chan=7/0/2/0, called=70911, calling=(n/a)
userid=modem1_1@bmw.com, ip=172.16.0.0, mask=172.16.0.0
setup=08/01/2001 13:36:44, conn=0.02, phys=17.96, service=23.30, authen=22.26,
init rx/tx b-rate=33600/33600, rx/tx chars=201/247
resource slot/port=1/1, mp bundle=0, charged units=0, account id=6
duration(sec)=132.50, disc subsys=ISDN, disc code=0x10
disc text=Normal call clearing

-------------------------------------------------------------------------
protocol: last=LAP-M, attempted=LAP-M
compression: last=V.42bis-Both, attempted= V.42bis-RX V.42bis-TX
standard: last=V.34+, attempted=V.90, initial=V.34+

snr=40 dB, sq=5, rx/tx level=-15/-13 dBm
phase jitter: freq=12 Hz, level=2 degrees
far end echo level=-90 dBm, freq offset=0 Hz
phase roll=0 degrees, round-trip delay=0 msecs
digital pad=None dB, digital pad comp=0
rbs pattern=0, constellation=16 point
rx/tx: symbol rate=3429/3429, carrier freq=1959/1959
rx/tx: trellis code=16/16 preemphasis index=0/0
rx/tx: constellation shape=Off/Off, nonlinear encode=Off/Off
rx/tx: precode=Off/Off, xmit level reduct=0/0 dBm

rx/tx: chars=201/247, general info=0x0
rx/tx: link layer chars=172/214, NAKs=0/0
error corrected: rx/tx=9/5, rx bad=0
ec retransmissions=0, retransmitted frames=0
rx/tx ppp slip=4/4, bad ppp slip=0
```

```
rx/tx b-rate: last=33600/33600, lowest=33600/300, highest=33600/33600
phase 2 projected max rx b-rate: client=33600, host=33600
phase 4 desired rx/tx b-rate: client=33600/33600, host=33600/33600
retrains: local=0, remote=0, failed=0
speedshift: local up/down=0/0, remote up/down=0/0, failed=0

v110: rx good=0, rx bad=0, tx=0, sync lost=0
SS7/COT status=0x00
v90: status=No Attempt, client=(n/a), failure=None

rx/tx: max neg I frame=128/128, neg window=15/15
v42bis size: dictionary=4096, string=32
T401 timeouts=0, tx window closures=0, rx overruns=0
test err=0, reset=0, v0 synch loss=0
mail lost: host=0, sp=0
duration(sec)=116, disc reason=0x220
disc text= <unknown>/EC condition - locally detected/received DISC frame -- normal LAPM
termination

                --------5---------10--------15--------20--------25--------30
line shape  : 0x00000000000000000000000000000000000000000000000000000000
v8bis capab : 0x12C9808081C609B502009481834347CB00000000000000000000000000000000
v8bis mod sl: 0x00000000000000000000000000000000000000000000000000000000000000000000
v8 call menu: 0xC16513942A8D000000000000
v90 training: 0x00000000
v90 sgn ptrn: 0x00000000
state trnsn : 0x0102030410151920FF00000000000000000000000000000000000000000000
                0000
portwre diag: 0x00000000000000000000000000000000
phase 2 info: 0x02EFF41F120000003CEFF41F0200E0EF01040040860D1B083470600000EF
                1E041400E22D00003C07A707A70D650D658340834000000000000
phase 4 info: 0x02834083408340834000
total speedshifts: 0
qc exchange: No QC Requested
moh status: Modem is Not on Hold
moh count: 0, moh request count: 0
total moh time: 0, cur moh time: 0
call waiting retrains: 0
rx/tx codewords: 0/0, rx/tx string: 0/0
rx/tx history size: 0/0
encoder/decoder state: 0/0
rx/tx compression ratio: 0/0, rx/tx dictionary reset count: 0/0
diagnostic code: 0x0000000000000000
-------------------------------------------------------------------------------
```

The following sample shows Call Tracker historical data for an incoming autodetected Media Gateway Control Protocol (MGCP) network access server (NAS) V.120 call with a normal disconnect by the MGCP NAS subsystem:

```
Router# show call calltracker history category v120

------------------------- call handle=         1 --------------------------
status=History, service=PPP, origin=Answer, category=V120,
DS0 slot/port/ds1/chan=1/7/7/23, called=5555, calling=1000
userid=user1, ip=10.1.1.52, mask=0.0.0.0
setup=11/18/2004 09:34:04, conn=0.11, phys=0.11, service=0.80, authen=0.76
init rx/tx b-rate=56000/56000, rx/tx chars=36646/36533
resource slot/port=(n/a)/(n/a), mp bundle=0, charged units=0, account
id=(n/a)
duration(sec)=133.70, disc subsys=MGCP, disc code=0x66
disc text=User request, sig type=Auto
-------------------------------------------------------------------------------
.
.
```

.

Table 23 describes the significant fields shown in the previous two displays.

Table 23 show call calltracker history subsystem isdn Field Descriptions

Field	Description
status	Status of the calls in the active database.
service	Session type for the call.
origin	Indicates how the call was created: • Originate—Dialout. The call was initiated locally, and the system sends the setup request. • Answer—Dialin. The call was initiated remotely, and the system receives the setup request.
category	Call type category. For autodetected calls, the values are V120, lapb, or syncData.
DS0 slot/port/ds1/chan	Number of the slot in the chassis, the applique that is being used (in the case of a card that supports multiple DS3 controllers), the DS1 trunk within the controller, and the channel, or time slot, within the DS1 trunk on which the call resides.
called	The called telephone number for this call.
calling	The calling telephone number for this call.
userid	The user login ID or zero-length string if unavailable.
ip	IP address assigned for the call, or 0.0.0.0 if not applicable or unavailable.
mask	The IP subnet mask assigned for this call. No IP subnet mask displays if the IP subnet mask is NULL.
setup	The time when the call was indicated to the NAS, for instance by the telecommunications network.
conn	The time, relative to the setup time, when the connection was established between the time slot of the incoming call and the appropriate local resources in the NAS such as the digital signal processor (DSP).
phys	The time, relative to the setup time, at which the physical link became ready. For a modem, this time would be when the carrier came up and error control and compression were completely negotiated.
service	The time, relative to the setup time, when the service was determined for the call type.
authen	The time, relative to the setup time, at which the user credentials were authenticated. Authentication may involve a Challenge Handshake Authentication Protocol (CHAP) challenge or response authentication for a PPP call, and the associated delay, through RADIUS or TACACS, in the external lookup.
disc subsys	The subsystem that disconnected the call.
disc code	Disconnecting code—a numeric code unique within the disconnecting subsystem that is of local significance (internal and proprietary).

Table 23 show call calltracker history subsystem isdn Field Descriptions (continued)

Field	Description
disc text	Message that gives a textual explanation for why the disconnection occurred. This message is of local significance (internal and proprietary).
sig type	Signaling type. Valid values are: • Auto—Autodetected calls. • LLC—ISDN signaled calls. • Xtrnl—External signaling protocols, such as MGCP. • Unknwn—Unknown signaling types.

Related Commands

Command	Description
calltracker enable	Enables Call Tracker on the access server.
show call calltracker active	Displays all information stored within the Call Tracker active database for all active calls.
show call calltracker handle	Displays all information stored within the Call Tracker active or history database table for a specified unique call handle identifier.
show call calltracker summary	Displays Call Tracker activity and configuration information such as the number of active calls and the history table attributes.

show call calltracker summary

To display Call Tracker activity and configuration information such as the number of active calls and the history table attributes, use the **show call calltracker summary** command in privileged EXEC mode.

show call calltracker summary

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced.

Examples

The following is sample output from the **show call calltracker summary** command:

```
Router# show call calltracker summary

Call Tracker Status:
  Active Table:
    - 7 call(s)
    - 4473 bytes used (639 average, 639 maximum)
  History Table:
    - 50 of a maximum of 240 call(s) (20% full)
    - 45157 bytes used (903 average, 921 maximum)
    - 260000 minute(s) call retain time
  API Front-end:
    - event elements:512 total, 512 free, 0 in-use
    - free event elements' low watermark:467
    - events dropped due to unavailability of free elts:0
```

Table 24 describes the significant fields shown in the display.

Table 24 show call calltracker summary Field Descriptions

Field	Description
Active Table:	
call(s)	Number of active calls.
n bytes used (*m* average, *o* maximum)	*n* = total memory used for all active calls *m* = average memory usage per call (*n*/calls) *o* = highest single memory usage for a call

Table 24 show call calltracker summary Field Descriptions (continued)

Field	Description
History Table:	
x of a maximum of *n* calls (*o*% full)	Number of calls in the history table, the maximum allowed (as defined by the **calltracker history max-size** command), and the percentage of the history table that these calls consume.
n bytes used (*m* average, *o* maximum)	*n* = total memory used for all active calls *m* = average memory usage per call (*n*/calls) *o* = highest single memory usage for a call
minute(s) call retain time	Number of minutes, for which calls are retained in the history table. This parameter is configured using the **calltracker history retain-mins** command.
API Front-end:	
event elements	For Cisco internal use only.
free event elements' low watermark	For Cisco internal use only.
events dropped due to unavailability of free elts	For Cisco internal use only.

Related Commands

Command	Description
show call calltracker active	Displays all of the information stored within the Call Tracker active database for all active calls.
show call calltracker handle	Displays all information stored within the Call Tracker active or history database table for a specified unique call handle identifier.
show call calltracker history	Displays all the information stored within the Call Tracker history database table for the most recent disconnected calls.

show call progress tone

To display the contents of the internal call progress (CP) tone database for a specific country, use the **show call progress tone** command in EXEC mode.

show call progress tone *country* [*tone-type*]

Syntax Description

country	Enters the country code for the country's call progress tone database you want to display. For the supported country codes, see the **modem country mica** command and the **modem country microcom_hdms** command.
tone-type	(Optional) Enters the tone type parameters you want to see from Table 25.

Command Modes

EXEC

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Table 25 lists the supported tone type parameters.

Table 25 Supported Tone Type Parameters

busy—Busy tone
congestion—Congestion tone
dialtone—Dial tone
disconnect—Disconnect tone
error—Error tone
off-hook-alert—Off-hook alert tone
off-hook-notice—Off-hook notice tone
pbx-dialtone—PBX dialtone
ringback—Ringback tone
routing—Routing tone

Using this command enables you to display the exact settings as they are programmed in the call-progress-tone database.

Examples

When you enter the **show call progress tone** command, the contents of the internal CP tone database for a specific country appears as in the following example:

```
Router# show call progress tone japan

Call progress tone: Japan

Dial tone:
0     Forever       425Hz -15.0/-15.0/-15.0 dBm0

PBX Dial tone:
0     Forever       425Hz -15.0/-15.0/-15.0 dBm0

Busy tone:
0       250ms       425Hz -20.0/-20.0/-20.0 dBm0
1       250ms     Silence

Congestion tone:
0       250ms       425Hz -20.0/-20.0/-20.0 dBm0
1       250ms     Silence

Error tone:
0       330ms       950Hz -15.0/-15.0/-15.0 dBm0
1       330ms      1400Hz -15.0/-15.0/-15.0 dBm0
2       330ms      1800Hz -15.0/-15.0/-15.0 dBm0
3      5000ms     Silence

Routing tone:
0       125ms       600Hz -24.0/-24.0/-24.0 dBm0
1       125ms     Silence
2       125ms       600Hz -24.0/-24.0/-24.0 dBm0
3     Forever     Silence

Disconnect tone:
0       330ms       600Hz -15.0/-15.0/-15.0 dBm0
1       330ms     Silence
2       330ms       600Hz -15.0/-15.0/-15.0 dBm0
3     Forever     Silence

Ringback tone:
0      1000ms       425Hz -19.0/-19.0/-19.0 dBm0
1      4000ms     Silence

Off-hook Notice tone:
0       100ms 1400x2040Hz -24.0/-24.0/-24.0 dBm0 -24.0/-24.0/-24.0 dBm0
1       100ms     Silence

Off-hook Alert tone:
0       100ms 1400x2040Hz -15.0/-15.0/-15.0 dBm0 -15.0/-15.0/-15.0 dBm0
1       100ms     Silence
```

The following example shows a specific CP tone (Japan, busy):

```
Router# show call progress tone japan busy

Busy tone for Japan:
0      2000ms  440x480 Hz -17.0/-17.0/-19.0 dBm0 -17.0/-17.0/-19.0 dBm0
1      4000ms     Silence
```

Table 26 describes the significant fields shown in the display.

Table 26 show show call progress tone Field Descriptions

Field	Description
Cadence number	Call progress tones consist of cadences—periods of sound or silence with certain parameters that do not change during the call. The cadence number shows the number of a particular cadence within the CP tone definitions. Cadence numbers start at 0.
Cadence duration	Cadence duration. “Forever” means that the sound can be heard forever, as in a dialtone.
Cadence type	Silence—No tone is generated. 440Hz—A single frequency is generated. 440x530Hz—Two frequencies are added (mixed).
Amplitudes for corresponding frequency components	Amplitudes for the corresponding frequency components. Different amplitudes are used on different trunk types.

Related Commands

Command	Description
call progress tone country	Specifies the country code for retrieving the call progress tone parameters from the CP tone database.

show caller

To display caller information, use the **show caller** command in user or privileged EXEC mode.

show caller [[[**interface** *interface-type interface-number* | **line** {*number* [*end-number*]| *line-modem-options*}] [**full** | **timeouts**]] | [**summary** | **user** *name* [**detailed**]]]

Syntax Description

interface	(Optional) Displays a summary of caller information for the specified interface. • *interface-type*—Interface type for which to display caller information. Valid values for the *interface-type* argument are as follows: – **Async**—Async interface. – **Dialer**—Dialer interface. – **Serial**—Serial interface. • *interface-number*—Number of the interface for which caller information will be displayed. Valid values for the *interface-number* argument vary depending on the interface type and platform.
line	(Optional) Displays a summary of caller information for the specified line(s) or by line or modem options. • *number* [*end-number*]—Line number for which caller information will be displayed. Specifying a value for the optional *end-number* argument results in caller information being displayed for a range of line numbers. Valid values for the *number* [*end-number*] arguments vary depending on the platform. • *line-modem-options*—Type of line or modem option for which caller information will be displayed. Valid values for the *line-modem-options* argument are as follows: – **aux** *line-number*—Auxiliary line. – **console** *line-number*—Primary terminal line. – **tty** *line-number*—Terminal controller. – **v110**—V.110 modem. – **vty** *line-number*—Virtual terminal line. – *x*/*y*—Internal modem slot/port number.
full	(Optional) Provides expanded caller information.
timeouts	(Optional) Displays session and idle limits and disconnect time.
summary	(Optional) Displays total users logged, total ISDN users, total analog users, and total external signaling analog and digital calls since the last **reload** command was entered.
user *name*	(Optional) Displays a summary of caller information for the specified username. • **detailed**—(Optional) Provides expanded information about the username.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.3(5)AA	This command was introduced.
12.1(3)T	The **summary** keyword was added.
12.3(6)	This command was enhanced to display information about external signaling calls.

Usage Guidelines

The **show caller** command is used to:

- Display individual users and consumed resources on the network access server (NAS).
- Inspect active call statistics for large pools of connections. (Debugging commands produce too much output and tax the CPU too heavily.)
- Display the absolute and idle times for each user. The current values for both of these settings are displayed on the TTY line and the asynchronous interface. Users that have been idle for unacceptably long periods of time can be easily identified. By using this information, you can define timeout policies and multiple grades of services for different users.
- In Multilink PPP (MLP) calls, if the MLP bundle is created on the remote home gateway, the total of unique users displayed by the **show caller summary** command is the same as the number of active B-channel calls. This is because the gateway does not know about the MLP bundle created on the other side.

You can configure output modifiers for each option type of the **show caller** command.

Examples

The following is sample output from the **show caller** command:

```
Router# show caller

  Line      User                 Service       Active
  con 0     -                    TTY           00:08:21
  BR0:1     user 1               PPP           00:00:14
  Vi1       user 2               PPP   Bundle  00:00:13
```

The following is sample output from the **show caller** command with the **summary** keyword:

```
Router# show caller summary

      933   Analog calls (0 VPDN Calls)
           47   Ext-Sig Analog calls
        0   ISDN calls (0 VPDN Calls)
        0   Ext-Sig Digital calls
        0   VPDN calls
        0   PPPoA calls
        0   PPPoE calls
      980 Total unique users logged in
```

Each display from the **show caller** command is self-explanatory; see the "Usage Guidelines" section for more information.

show cca

To display various internal configuration relationships, use the **show cca** command in user EXEC or privileged EXEC mode.

show cca [**detail** [**ccb** *ccb-index* | **interface** *type number*] | [**interface** *type number*]]

Syntax Description

detail	(Optional) Displays detailed common configuration architecture (CCA) information.
ccb	(Optional) Displays detailed CCA configuration control block (CCB) information.
ccb-index	(Optional) CCA CCB index list.
interface *type number*	(Optional) Displays the specific bindings or sources of configuration for an interface.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(4)T	This command was introduced in a release earlier than Cisco IOS Release 12.0(4)T.
12.2(10)S	This command was integrated into Cisco IOS Release 12.2(10)S.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The **show cca** command shows information such as the software components (PPP, IP, and peer) that are registered with CCA.

Examples

The following is sample output from the **show cca** command with the optional **interface** keyword specified:

```
Router# show cca interface se1:23

Type        Name                    Component(s)
parent      Di1                     peer ppp
interface   Se1:23                  peer ppp
```

Table 27 describes the fields shown in the display.

Table 27 show cca interface Field Descriptions

Field	Description
Type	Type of interface.
Name	Template name.
Component(s)	Software components registered with CCA.

show controllers bri

To display information about the ISDN BRI, use the **show controllers bri** command in privileged EXEC mode.

Cisco MC3810 Routers

show controllers bri [*interface-number*]

Cisco 7200 Series Routers

show controllers bri *slot/port*

All Other Routers

show controllers bri *interface-number*

Syntax Description

interface-number	Interface number. The value is from 0 to 7 if the router has one 8-port BRI network interface module (NIM), or from 0 to 15 if the router has two 8-port BRI NIMs. Interface number values will vary, depending on the hardware platform used. The Cisco 3600 series router, for example, can have up to 48 interfaces. The *interface-number* argument is optional for the Cisco MC3810 router. Valid BRI controller numbers for the Cisco MC3810 router are from 1 to 4.
slot/port	Backplane slot number and port number on the interface. See your hardware installation manual for the specific slot and port numbers. The slash mark is required.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
11.2P	This command was enhanced to support slot and port syntax for the PA-8B-ST and PA-4B-U port adapters on the Cisco 7200 series.
12.0(3)XG	This command was implemented on the Cisco MC3810 universal access concentrator.

Usage Guidelines

If you use the **show controllers bri** command in the Cisco MC3810 without the slot-number keywords, information for all of the configured ISDN BRI controllers will be displayed. The BRI controller numbers match the physical ports numbers on the BRI voice module (BVM).

Examples

The following example shows controller statistics for interface BRI 1 on a Cisco MC3810 router:

```
Router# show controllers bri 1

BRI unit 1:
Layer 1 is DEACTIVATED. (ISDN L1 State F3)
S2084 registers:
Configuration register=0x1
QMC GLOBAL MULTICHANNEL PARAMETERS (at 0x30003C00)
[MCBASE]=0x1C4AE38, [QMCSTATE]=0x0, [MRBLR]=0x5F4
[TXSPTR]=0x1C20, [RXPTR]=0x1C24, [GRFTHR]=0x1
[GRFCNT]=0x1, [INTBASE]=0x1B04124, [INTPTR]=0x1B0413C
[RXSPTR]=0x1C20, [TXPTR]=0x1C3E, [CMASK32]=0xDEBB20E3
[TSATRX]=0x30003C20, [TSATTX]=0x30003C60, [CMASK16]=0xF0B8

QMC Timeslot Assignment Entries (Rx == Tx):
[ 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
0x0 0x0 0x0 0x0 0x540 0x8503 0x84C3 0x8483 0x0 0x400 0x400 0xC400 0xC000 ]

D Channel Information:

BVM unit 1,
qmc_channel: 18 timeslot: 26
idb at 0x1199FC8, driver data structure at 0x11D06D8
SCC Registers:
General [GSMR]=0x780:0x0000003A, Protocol-specific [PSMR]=0x80
Events [SCCE]=0x0000, Mask [SCCM]=0x000F, Status [SCCS]=0x0002
Transmit on Demand [TODR]=0x0, Data Sync [DSR]=0x7E7E
Interrupt Registers:
Config [CICR]=0x001B9981, Pending [CIPR]=0x00000240
Mask   [CIMR]=0x7A000400, In-srv  [CISR]=0x00000000
Command register [CR]=0x640
Port A [PADIR]=0x00F0, [PAPAR]=0xFFFF
    [PAODR]=0x00E0, [PADAT]=0x1AEF
Port B [PBDIR]=0x01333F, [PBPAR]=0x01033E
    [PBODR]=0x000030, [PBDAT]=0x00DFFC
Port C [PCDIR]=0x0C0C, [PCPAR]=0x0000
    [PCSO]=0x03F3,  [PCDAT]=0x00FF, [PCINT]=0x0000
Port D [PDDIR]=0x000760, [PDPAR]=0x00013F
    [PDDAT]=0x000CB0
SI      [SIMODE]=0x00480048,  [SIGMR]=0x0E, [SISTR]=0x00
    [SICR]=0x6D372E49
BRGC    [BRGC1]=0x00000000,  [BRGC2]=0x00000000

    [BRGC3]=0x00000000,  [BRGC4]=0x00000000

QMC CHANNEL PARAMETERS (at 0x30002480)
[TBASE]=0xBC0, [CHAMR]=0xB000, [TSTATE]=0x300C0FDE
[TBPTR]=0xBD0, [ZISTATE]=0xE1FF0FFF, [INTMSK]=0x3F
[RBASE]=0xB40, [MFLR]=0x5F4, [RSTATE]=0x31021C00
[RBPTR]=0xB70, [ZDSTATE]=0x25FFFFAE

buffer size 1524
RX ring with 16 entries at 0x1C4B978, Buffer size 1524
Rxhead = 0x1C4B9A8 (6), Rxp = 0x11D070C (6)
00 pak=0x145FDD0 buf=0x1CCE138 status=9000 pak_size=0
01 pak=0x145FBBC buf=0x1CCDA78 status=9000 pak_size=0
02 pak=0x145F9A8 buf=0x1CCD3B8 status=9000 pak_size=0
03 pak=0x145F794 buf=0x1CCCCF8 status=9000 pak_size=0
04 pak=0x14618D4 buf=0x1CD38F8 status=9000 pak_size=0
05 pak=0x14616C0 buf=0x1CD3238 status=9000 pak_size=0
06 pak=0x1461298 buf=0x1CD24B8 status=9000 pak_size=0
07 pak=0x1461084 buf=0x1CD1DF8 status=9000 pak_size=0
08 pak=0x1460E70 buf=0x1CD1738 status=9000 pak_size=0
```

```
09 pak=0x1460C5C buf=0x1CD1078 status=9000 pak_size=0
10 pak=0x1460A48 buf=0x1CD09B8 status=9000 pak_size=0
11 pak=0x1460834 buf=0x1CD02F8 status=9000 pak_size=0
12 pak=0x1460620 buf=0x1CCFC38 status=9000 pak_size=0
13 pak=0x146040C buf=0x1CCF578 status=9000 pak_size=0
14 pak=0x14601F8 buf=0x1CCEEB8 status=9000 pak_size=0
15 pak=0x145FFE4 buf=0x1CCE7F8 status=B000 pak_size=0

TX ring with 4 entries at 0x1C4B9F8, tx_count = 0
tx_head = 0x1C4BA08 (2), head_txp = 0x11D0818 (2)
tx_tail = 0x1C4BA08 (2), tail_txp = 0x11D0818 (2)
00 pak=0x0000000 buf=0x0000000 status=0000 pak_size=0
01 pak=0x0000000 buf=0x0000000 status=0000 pak_size=0
02 pak=0x0000000 buf=0x0000000 status=0000 pak_size=0
03 pak=0x0000000 buf=0x0000000 status=2000 pak_size=0
0 throttles, 0 enables
0 input aborts on receiving flag sequence
    0 missed datagrams, 0 overruns
    0 bad datagram encapsulations, 0 memory errors
    0 transmitter underruns

B1 Channel Information:

BVM unit 1,
qmc_channel: 0 timeslot: 0
idb at 0x119FEB0, driver data structure at 0x11D0B54
SCC Registers:
General [GSMR]=0x0:0x00000000, Protocol-specific [PSMR]=0x0
Events [SCCE]=0x0000, Mask [SCCM]=0x0000, Status [SCCS]=0x0000
Transmit on Demand [TODR]=0x9080, Data Sync [DSR]=0xA4
QMC CHANNEL PARAMETERS (at 0x0)
[TBASE]=0x0, [CHAMR]=0x0, [TSTATE]=0x7C6802A6
[TBPTR]=0x9080, [ZISTATE]=0x906000AC, [INTMSK]=0x9060
[RBASE]=0x4800, [MFLR]=0x5, [RSTATE]=0x7C8000A6
[RBPTR]=0x7C9B, [ZDSTATE]=0x3864FFDC

buffer size 1524
RX ring with 0 entries at 0x0, Buffer size 1524
Rxhead = 0x0 (0), Rxp = 0x0 (-4670172)

TX ring with 0 entries at 0x0, tx_count = 0
tx_head = 0x0 (0), head_txp = 0x0 (-4670243)
tx_tail = 0x0 (0), tail_txp = 0x0 (-4670243)
0 throttles, 0 enables
0 input aborts on receiving flag sequence
    0 missed datagrams, 0 overruns
    0 bad datagram encapsulations, 0 memory errors
    0 transmitter underruns

B2 Channel Information:

BVM unit 1,
qmc_channel: 0 timeslot: 0
idb at 0x11A5D98, driver data structure at 0x11D0F8C
SCC Registers:
General [GSMR]=0x0:0x00000000, Protocol-specific [PSMR]=0x0
Events [SCCE]=0x0000, Mask [SCCM]=0x0000, Status [SCCS]=0x0000
Transmit on Demand [TODR]=0x9080, Data Sync [DSR]=0xA4

QMC CHANNEL PARAMETERS (at 0x0)
[TBASE]=0x0, [CHAMR]=0x0, [TSTATE]=0x7C6802A6
[TBPTR]=0x9080, [ZISTATE]=0x906000AC, [INTMSK]=0x9060
[RBASE]=0x4800, [MFLR]=0x5, [RSTATE]=0x7C8000A6
[RBPTR]=0x7C9B, [ZDSTATE]=0x3864FFDC
```

```
buffer size 1524
RX ring with 0 entries at 0x0, Buffer size 1524
Rxhead = 0x0 (0), Rxp = 0x0 (-4670442)

TX ring with 0 entries at 0x0, tx_count = 0
tx_head = 0x0 (0), head_txp = 0x0 (-4670513)
tx_tail = 0x0 (0), tail_txp = 0x0 (-4670513)
0 throttles, 0 enables
0 input aborts on receiving flag sequence
    0 missed datagrams, 0 overruns
--More--           0 bad datagram encapsulations, 0 memory
>errors
    0 transmitter underruns
```

The following is sample output from the **show controllers bri** command:

```
Router# show controllers bri 0

BRI unit 0
D Chan Info:
Layer 1 is ACTIVATED
idb 0x32089C, ds 0x3267D8, reset_mask 0x2
buffer size 1524
RX ring with 2 entries at 0x2101600 : Rxhead 0
00 pak=0x4122E8 ds=0x412444 status=D000 pak_size=0
01 pak=0x410C20 ds=0x410D7C status=F000 pak_size=0
TX ring with 1 entries at 0x2101640: tx_count = 0, tx_head = 0, tx_tail = 0
00 pak=0x000000 ds=0x000000 status=7C00 pak_size=0
0 missed datagrams, 0 overruns, 0 bad frame addresses
0 bad datagram encapsulations, 0 memory errors
0 transmitter underruns
B1 Chan Info:
Layer 1 is ACTIVATED
idb 0x3224E8, ds 0x3268C8, reset_mask 0x0
buffer size 1524
RX ring with 8 entries at 0x2101400 : Rxhead 0
00 pak=0x421FC0 ds=0x42211C status=D000 pak_size=0
01 pak=0x4085E8 ds=0x408744 status=D000 pak_size=0
02 pak=0x422EF0 ds=0x42304C status=D000 pak_size=0
03 pak=0x4148E0 ds=0x414A3C status=D000 pak_size=0
04 pak=0x424D50 ds=0x424EAC status=D000 pak_size=0
05 pak=0x423688 ds=0x4237E4 status=D000 pak_size=0
06 pak=0x41AB98 ds=0x41ACF4 status=D000 pak_size=0
07 pak=0x41A400 ds=0x41A55C status=F000 pak_size=0
TX ring with 4 entries at 0x2101440: tx_count = 0, tx_head = 0, tx_tail = 0
00 pak=0x000000 ds=0x000000 status=5C00 pak_size=0
01 pak=0x000000 ds=0x000000 status=5C00 pak_size=0
02 pak=0x000000 ds=0x000000 status=5C00 pak_size=0
03 pak=0x000000 ds=0x000000 status=7C00 pak_size=0
0 missed datagrams, 0 overruns, 0 bad frame addresses
0 bad datagram encapsulations, 0 memory errors
0 transmitter underruns
B2 Chan Info:
Layer 1 is ACTIVATED
idb 0x324520, ds 0x3269B8, reset_mask 0x2
buffer size 1524
RX ring with 8 entries at 0x2101500 : Rxhead 0
00 pak=0x40FCF0 ds=0x40FE4C status=D000 pak_size=0
01 pak=0x40E628 ds=0x40E784 status=D000 pak_size=0
02 pak=0x40F558 ds=0x40F6B4 status=D000 pak_size=0
03 pak=0x413218 ds=0x413374 status=D000 pak_size=0
04 pak=0x40EDC0 ds=0x40EF1C status=D000 pak_size=0
05 pak=0x4113B8 ds=0x411514 status=D000 pak_size=0
```

```
06 pak=0x416ED8 ds=0x417034 status=D000 pak_size=0
07 pak=0x416740 ds=0x41689C status=F000 pak_size=0
TX ring with 4 entries at 0x2101540: tx_count = 0, tx_head = 0, tx_tail = 0
00 pak=0x000000 ds=0x000000 status=5C00 pak_size=0
01 pak=0x000000 ds=0x000000 status=5C00 pak_size=0
02 pak=0x000000 ds=0x000000 status=5C00 pak_size=0
03 pak=0x000000 ds=0x000000 status=7C00 pak_size=0
0 missed datagrams, 0 overruns, 0 bad frame addresses
0 bad datagram encapsulations, 0 memory errors
0 transmitter underruns
```

Table 28 describes the significant fields shown in the display.

Table 28 show controllers bri Field Descriptions

Field	Description
BRI unit 0	Interface type and unit number.
Chan Info	D and B channel numbers.
Layer 1 is ACTIVATED	Layer 1 status can be DEACTIVATED, PENDING ACTIVATION, or ACTIVATED.
idb ds reset_mask	Information about internal data structures and parameters (for use by Cisco technical personnel).
buffer size	Number of bytes allocated for buffers.
RX ring with - entries at -	Information about the Receiver Queue.
Rxhead	Start of the Receiver Queue.
pak ds status pak_size	Information about internal data structures and parameters.
TX ring with - entries at -	Information about the Transmitter Queue.
tx_count	Number of packets to transmit.
tx_head	Start of the transmit list.
tx_tail	End of the transmit list.
missed datagrams	Incoming packets missed due to internal errors.
overruns	Number of times the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
bad frame addresses	Frames received with a cyclic redundancy check (CRC) error and noninteger number of octets.
bad datagram encapsulations	Packets received with bad encapsulation.
memory errors	Internal direct memory access (DMA) memory errors.
transmitter underruns	Number of times that the transmitter has been running faster than the router can handle.

The following is a partial output example from the **show controllers bri** command on a Cisco 7200 series router:

```
Router# show controllers bri 2/0

BRI slot 2 interface 0 with integrated NT1
Layer 1 is ACTIVATED. (ISDN L1 State F7)
Master clock for slot 2 is bri interface 0.
Total chip configuration successes: 193, failures: 0, timeouts: 0
D Channel Information:
  Channel state: UP  Channel IDB: 6092AC64
  RX ring entries: 5, buffer size 512
  RX descriptor ring: head = 165F4D8, tail = 165F508
  RX buffer ring: head = 6093A260, tail = 6093A290
  00 params=0x2000000 status=0x0 data ptr=0x1650F84 next ptr=0x165F4D8
  01 params=0x2000000 status=0xC0080000 data ptr=0x1651884 next ptr=0x165F4E8
  02 params=0x2000000 status=0xC0080000 data ptr=0x1651644 next ptr=0x165F4F8
  03 params=0x2000000 status=0x0 data ptr=0x1651404 next ptr=0x165F508
  04 params=0x42000000 status=0x0 data ptr=0x16511C4 next ptr=0x165F4C8
  TX ring entries: 5, in use: 0, buffer size 512
  TX descriptor ring: head = 3C2049C0, tail = 3C2049C0
  TX buffer ring: head = 608EC0C4, tail = 608EC0C4
  00 params=0x80000000 data ptr=0x0000000 next ptr=0x4D0049A8
  01 params=0x80000000 data ptr=0x0000000 next ptr=0x4D0049B4
  02 params=0x80000000 data ptr=0x0000000 next ptr=0x4D0049C0
  03 params=0xC0000000 data ptr=0x0000000 next ptr=0x4D0049CC
  04 params=0x0 data ptr=0x0000000 next ptr=0x4D00499C
  List of timeslots (sw): 2
```

Table 29 describes the significant fields shown in the display.

Table 29 show controllers bri Field Descriptions (for Cisco 7200 Series Routers)

Field	Description
BRI slot 2 interface 0 with integrated NTI	Interface type and slot and port number.
Layer 1 is ACTIVATED	Layer 1 status can be DEACTIVATED, PENDING ACTIVATION, or ACTIVATED.
Master clock	The first interface that comes up on an MBRI port adapter holds the master clock. This clock is used for all interfaces on that port adapter. If the master clock interface goes down, the second interface that came up becomes the master clock interface.
Total chip configuration successes	Counters of successful chip configuration.
failures	Counters of bad chip configuration.
timeouts	Counters of failing to initialize chip.
D Channel Information	Information related to D-channel status.
Channel state	Channel state can be UNUSED, IDLE, DOWN, STANDBY, UP, THROTTLED, ILLEGAL.
Channel IDB	Internal interface channel description.
RX (or TX) ring entries	Internal receive queue.
RX (or TX) descriptor ring	Internal receive queue to manage hardware chip.
RX (or TX) buffer ring	Internal receive queue to hold inbound packets.
Rxhead	Start of the receiver queue.

Table 29 show controllers bri Field Descriptions (for Cisco 7200 Series Routers) (continued)

Field	Description
params, status, data ptr, next ptr	Information about internal data structures and parameters (for use by Cisco technical personnel.
List of timeslots (sw)	Time slots assigned to this channel.

show controllers e1 call-counters

To display the total number of calls and call durations on an E1 controller, use the **show controllers e1 call-counters** command in privileged EXEC mode.

show controllers e1 *controller-number* **call-counters**

Syntax Description

controller-number	Controller number (for example, 0, 1, 2, or 3).

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3T	This command was introduced.

Usage Guidelines

This command displays the E1 controller status as calls, such as switched 56K digital calls. It shows the total duration of all the previous calls on the specified timeslot in(hrs: mins:sec).

Examples

The following is sample output of the **show controllers e1 call-counters** command:

```
Router# show controllers e1 1 call-counters

E1 1:
  DS0's Active: 0
  DS0's Active High Water Mark: 0
  TimeSlot   Type   TotalCalls   TotalDuration
      1       cas           0       00:00:00
      2       cas           0       00:00:00
      3       cas           0       00:00:00
      4       cas           0       00:00:00
      5       cas           0       00:00:00
      6       cas           0       00:00:00
      7       cas           0       00:00:00
      8       cas           0       00:00:00
      9       cas           0       00:00:00
     10       cas           0       00:00:00
     11       cas           0       00:00:00
     12       cas           0       00:00:00
     13       cas           0       00:00:00
     14       cas           0       00:00:00
     15       cas           0       00:00:00
     16       cas           0       00:00:00
     17       cas           0       00:00:00
     18       cas           0       00:00:00
     19       cas           0       00:00:00
     20       cas           0       00:00:00
     21       cas           0       00:00:00
     22       cas           0       00:00:00
     23       cas           0       00:00:00
     24       cas           0       00:00:00
Total DS0's Active High Water Mark: 7
```

Table 30 describes the significant fields shown in the display.

Table 30 show controllers e1 call-counters Field Descriptions

Field	Description
E1 1:	Number of the E1 controller.
DS0's Active:	Displays the number of DS0s channels that are currently active.
DS0's Active High Water Mark:	Number of active DS0s that are approaching the threshold ceiling of the system.
TimeSlot	Time slot number used on the controller for the specified DS0.
Type	Type of call occupying the timeslot. This entry is usually channel-associated signaling (CAS) or ISDN PRI.
TotalCalls	How many calls came in on this time slot or DS0.
TotalDuration	Total duration of all the previous calls on the specified timeslot in(hrs: mins:sec).
Total DS0's Active High Water Mark:	Total number of active DS0s that are approaching the threshold ceiling of the system.

Related Commands

Command	Description
cas-group (E1 controller)	Configures CAS on an E1 controller.
show controllers e1 cas-data	Displays internal call switching module information about the switched 56K data channels.

show controllers e1 cas-data

To display internal call switching module information about the switched 56K data channels, use the **show controllers e1 cas-data** command in privileged EXEC mode.

show controllers e1 *controller-number* **cas-data**

Syntax Description

controller-number	Controller number (for example, 0, 1, 2, or 3).

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3T	This command was introduced.

Examples

The following is sample output from the **show controllers e1 cas-data** command:

```
router# show controllers e1 1 cas-data

Device Pool: Dev-SW56-pool
Number of SW56 vdev in pool: 48
Number of active connections: 0
No free SW56 device in pool: 0
SW56 max allocated messages: 96

E1 1:
 SW56(slot/subcont/bchan)=0/1/0, hwidb=0x00867348
  csm_state(0x00000100)=CSM_IDLE_STATE, csm_event_proc=0x0006CCC2
  total_call_duration=00:00:00
  invalid_event_count=0, wdt_timeout_count=0
  ic_failure=0, ic_complete=0, remote_link_disc=0
  csm_status(0): VDEV_STATUS_UNLOCKED
  wdt_timestamp_started is not activated
 SW56(slot/subcont/bchan)=0/1/1, hwidb=0x0086EC58
  csm_state(0x00000100)=CSM_IDLE_STATE, csm_event_proc=0x0006CCC2
  total_call_duration=00:00:00
  invalid_event_count=0, wdt_timeout_count=0
  ic_failure=0, ic_complete=0, remote_link_disc=0
  csm_status(0): VDEV_STATUS_UNLOCKED
  wdt_timestamp_started is not activated
 SW56(slot/subcont/bchan)=0/1/2, hwidb=0x00876568
  csm_state(0x00000100)=CSM_IDLE_STATE, csm_event_proc=0x0006CCC2
  total_call_duration=00:00:00
  invalid_event_count=0, wdt_timeout_count=0
  ic_failure=0, ic_complete=0, remote_link_disc=0
  csm_status(0): VDEV_STATUS_UNLOCKED
  wdt_timestamp_started is not activated
 SW56(slot/subcont/bchan)=0/1/3, hwidb=0x0087DE78
  csm_state(0x00000100)=CSM_IDLE_STATE, csm_event_proc=0x0006CCC2
  total_call_duration=00:00:00
  invalid_event_count=0, wdt_timeout_count=0
  ic_failure=0, ic_complete=0, remote_link_disc=0
  csm_status(0): VDEV_STATUS_UNLOCKED
  wdt_timestamp_started is not activated
```

```
SW56(slot/subcont/bchan)=0/1/4, hwidb=0x00885788
 csm_state(0x00000100)=CSM_IDLE_STATE, csm_event_proc=0x0006CCC2
 total_call_duration=00:00:00
 invalid_event_count=0, wdt_timeout_count=0
 ic_failure=0, ic_complete=0, remote_link_disc=0
 csm_status(0): VDEV_STATUS_UNLOCKED
 wdt_timestamp_started is not activated
```

Table 31 describes the significant fields shown in the display.

Table 31 show controllers e1 cas-data Field Descriptions

Field	Description
Device Pool:	Type of pool in service, which is a logical grouping used to achieve a specific service.
Number of SW56 vdev in pool:	Number of serial devices used in the pool.
Number of active connections:	Number of active switched 56K active connections.
No free SW56 device in pool:	Number of switched 56K channels available to accept calls.
SW56 max allocated messages:	Number of messages that are allocated to switched 56K services.
E1 1:	Number of the controller E1.
SW56(slot/subcont/bchan)=	Specified DS0 or time slot used for the switched 56K service.
csm_state(0x00000100)=	Call state machine register.
total_call_duration=	How long the call lasted (in hours: minutes: seconds).
invalid_event_count=	Number of invalid event counters for the specified channel.
ic_failure=	Number of incoming call failures.
csm_status(0):	Call state machine register.
wdt_timestamp_started is not activated	Watchdog timer.

Related Commands

Command	Description
cas-group (E1 controller)	Configures CAS on an E1 controller.
show controllers e1 call-counters	Displays the total number of calls and call durations on an E1 controller.

show controllers t1 call-counters

To display the total number of calls and call durations on a T1 controller, use the **show controllers t1 call-counters** command in privileged EXEC mode.

Cisco 4000 Series Routers

show controllers t1 *controller-number* **call-counters**

Cisco AS 53000 and AS5400 Access Servers

show controllers t1 *slot*/*port* **call-counters**

Syntax Description

controller-number	For Cisco 4000 series routers, enter just the controller number (for example, 0, 1, 2, or 3).
slot/*port*	For Cisco AS5300 and AS5400 series access servers, enter the controller number as *slot*/*port*. The slash marks are required.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3T	This command was introduced.
12.1(3)T	This command was introduced on the Cisco AS5300 and AS5400 series access servers.

Usage Guidelines

This command displays the T1 controller status as calls, such as switched 56K digital calls.

Examples

The following is partial sample output from the **show controllers t1 call-counters** command:

```
router# show controllers t1 1 call-counters

T1 1:
  DS0's Active: 0
  DS0's Active High Water Mark: 0
  TimeSlot   Type   TotalCalls   TotalDuration
      1       cas           0       00:00:00
      2       cas           0       00:00:00
      3       cas           0       00:00:00
      4       cas           0       00:00:00
      5       cas           0       00:00:00
      6       cas           0       00:00:00
      7       cas           0       00:00:00
      8       cas           0       00:00:00
      9       cas           0       00:00:00
     10       cas           0       00:00:00
     11       cas           0       00:00:00
     12       cas           0       00:00:00
     13       cas           0       00:00:00
```

```
     14       cas            0       00:00:00
     15       cas            0       00:00:00
     16       cas            0       00:00:00
     17       cas            0       00:00:00
     18       cas            0       00:00:00
     19       cas            0       00:00:00
     20       cas            0       00:00:00
     21       cas            0       00:00:00
     22       cas            0       00:00:00
.
.
.
Total DS0's Active High Water Mark: 7
```

Table 32 describes the significant fields shown in the display.

Table 32 show controllers t1 call-counters Field Descriptions

Field	Description
T1 1:	Number of the T1 controller.
DS0's Active:	Displays the number of DS0s channels that are currently active.
DS0's Active High Water Mark:	Number of active DS0s that are approaching the threshold ceiling of the system.
TimeSlot	Time slot number used on the controller for the specified DS0.
Type	Type of call occupying the time slot. This entry is usually channel-associated signaling (CAS) or ISDN PRI.
TotalCalls	How many calls came in on this time slot or DS0.
TotalDuration	Total active time for all previous successful calls on the specified time slot (in hours: minutes: seconds).
Total DS0's Active High Water Mark:	Total number of active DS0s that are approaching the threshold ceiling of the system.

Related Commands

Command	Description
cas-group (T1 controller)	Configures channel associated signaling on a T1 controller.
show controllers t1 cas-data	Displays internal call switching module information about the switched 56-kbps data channels.

show controllers t1 cas-data

To display internal call switching module information about the switched 56K data channels, use the **show controllers t1 cas-data** command in privileged EXEC mode.

Cisco 4000 Series Routers

show controllers t1 *controller-number* **cas-data**

Cisco AS 53000 and AS5400 Access Servers

show controllers t1 *slot/port* **cas-data**

Syntax Description

controller-number	For Cisco 4000 series routers, enter just the controller number (for example, 0, 1, 2, or 3).
slot/port	For Cisco AS5300 and AS5400 series access servers, enter the controller number as *slot/port*. The slash mark is required.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3T	This command was introduced.
12.1(3)T	This command was introduced on the Cisco AS5300 and AS5400 series access servers.

Examples

The following is sample output from the **show controllers t1 cas-data** command:

```
Router# show controllers t1 1 cas-data

Device Pool: Dev-SW56-pool
Number of SW56 vdev in pool: 48
Number of active connections: 0
No free SW56 device in pool: 0
SW56 max allocated messages: 96

T1 1:
 SW56(slot/subcont/bchan)=0/1/0, hwidb=0x00867348
  csm_state(0x00000100)=CSM_IDLE_STATE, csm_event_proc=0x0006CCC2
  total_call_duration=00:00:00
  invalid_event_count=0, wdt_timeout_count=0
  ic_failure=0, ic_complete=0, remote_link_disc=0
  csm_status(0): VDEV_STATUS_UNLOCKED
  wdt_timestamp_started is not activated
 SW56(slot/subcont/bchan)=0/1/1, hwidb=0x0086EC58
  csm_state(0x00000100)=CSM_IDLE_STATE, csm_event_proc=0x0006CCC2
  total_call_duration=00:00:00
  invalid_event_count=0, wdt_timeout_count=0
  ic_failure=0, ic_complete=0, remote_link_disc=0
  csm_status(0): VDEV_STATUS_UNLOCKED
  wdt_timestamp_started is not activated
```

```
SW56(slot/subcont/bchan)=0/1/2, hwidb=0x00876568
 csm_state(0x00000100)=CSM_IDLE_STATE, csm_event_proc=0x0006CCC2
 total_call_duration=00:00:00
 invalid_event_count=0, wdt_timeout_count=0
 ic_failure=0, ic_complete=0, remote_link_disc=0
 csm_status(0): VDEV_STATUS_UNLOCKED
 wdt_timestamp_started is not activated
SW56(slot/subcont/bchan)=0/1/3, hwidb=0x0087DE78
 csm_state(0x00000100)=CSM_IDLE_STATE, csm_event_proc=0x0006CCC2
 total_call_duration=00:00:00
 invalid_event_count=0, wdt_timeout_count=0
 ic_failure=0, ic_complete=0, remote_link_disc=0
 csm_status(0): VDEV_STATUS_UNLOCKED
 wdt_timestamp_started is not activated
SW56(slot/subcont/bchan)=0/1/4, hwidb=0x00885788
 csm_state(0x00000100)=CSM_IDLE_STATE, csm_event_proc=0x0006CCC2
 total_call_duration=00:00:00
 invalid_event_count=0, wdt_timeout_count=0
 ic_failure=0, ic_complete=0, remote_link_disc=0
 csm_status(0): VDEV_STATUS_UNLOCKED
 wdt_timestamp_started is not activated
```

Table 33 describes the significant fields in the display.

Table 33 show controllers t1 cas-data Field Descriptions

Field	Description
Device Pool:	Type of pool in service, which is a logical grouping used to achieve a specific service.
Number of SW56 vdev in pool:	Number of serial devices used in the pool.
Number of active connections:	Number of active switched 56K active connections.
No free SW56 device in pool:	Number of switched 56K channels available to accept calls.
SW56 max allocated messages:	Number of messages that are allocated to switched 56K services.
T1 1:	Number of the controller T1.
SW56(slot/subcont/bchan)=	Specified DS0 or time slot used for the switched 56K service.
csm_state(0x00000100)=	Call state machine register.
total_call_duration=	How long the call lasted (in hours: minutes: seconds).
invalid_event_count=	Number of invalid event counters for the specified channel.
ic_failure=	Number of incoming call failures.
csm_status(0):	Call state machine register.
wdt_timestamp_started is not activated	Watchdog timer.

Related Commands

Command	Description
cas-group (T1 controller)	Configures channel-associated signaling on a T1 controller.
show controllers t1 call-counters	Displays the total number of calls and call durations on a T1 controller.

show controllers t1 clock

To display the primary clock change history, use the **show controller t1 clock** command in privileged EXEC mode.

show controllers t1 *slot/port* **clock**

Syntax Description

slot/port	Controller number entered as *slot/port*. The slash mark is required.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco AS5300 and AS5400 series access servers.

Examples

The following example is a self-explanatory report for a Cisco AS5350 T1 controller clock:

```
Router# show controller t1 1/1 clock

Clock selected: Freerun clock


CLOCK CHANGE HISTORY
-------------------------

CLOCK        Event                                Time
-----        -----                                ----
Freerun   Firmware Initialization                 00:00:28 UTC Tue Nov 30 1999
```

Related Commands

Command	Description
clear controller	Resets the specified T1 or E1 controller.
clear controller t1 firmware-status	Clears the T1 controller crash history.

show controllers t1 firmware-status

To display the crash history of the New E1 And T1 (NEAT) controller, use the **show controller t1 firmware-status** command in privileged EXEC mode.

show controllers t1 *slot*/*port* **firmware-status**

Syntax Description

slot/*port*	Controller number entered as *slot*/*port*.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco AS5300 and AS5400 series access servers.

Examples

The following example is self-explanatory report crash history output from a Cisco AS5350 T1 controller:

```
Router# show controller t1 1/1 firmware-status

Trunk-1 hasn't restarted since last system reload
```

Related Commands

Command	Description
clear controller	Resets the specified T1 or E1 controller.
clear controller t1 firmware-status	Clears the T1 controller crash history.

show controllers t1 timeslots

To show the channel-associated signaling (CAS) and ISDN PRI state on the T1 controller in detail, use the **show controllers t1 timeslots** command in EXEC mode.

Cisco 4000 Series Routers

show controllers t1 *controller-number* **timeslots** *timeslot-range*

Cisco AS5300 and AS5400 Series Access Servers

show controllers t1 *slot*/*port* **timeslots** *timeslot-range*

Syntax Description

controller-number	For Cisco 4000 series: the controller number (for example, 0, 1, 2, or 3).
slot/*port*	For Cisco AS5300 series and Cisco AS5400 series: the controller number, as *slot*/*port*. The slash mark is required.
timeslot-range	Displays DS0 information. Time slot range for the T1 controller is from 1 to 24. Enter the range as a logical sequence of numbers separated by a dash.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.1(3)T	This command was introduced on the Cisco AS5300 series and Cisco AS5400 series.

Usage Guidelines

Use this command to display the CAS and ISDN PRI channel state in detail. On the Cisco access servers, the command shows whether the DS0 channels of a controller are in idle, in-service, maintenance, or busyout states. Use the command to display statistics about the T1 links.

Examples

The following example shows that the CAS state is enabled on the Cisco AS5300 universal access server with a T1 PRI card. The display is self-explanatory.

```
Router# show controllers t1 1 timeslots 1-24

SERVICE STATES                CAS CHANNEL STATES
insvc    = In Service         down       = Down
outofsvc = Out of Service     idle       = Idle
maint    = Maintenance        connected  = Call Connected
                              signaling  = Signaling
                              static-bo  = Static Busyout
                              dynamic-bo = Dynamic Busyout

                              ISDN CHANNEL STATES
                              idle       = Available
                              proposed   = Negotiating
                              busy       = Unavailable
```

```
                                reserved   = Reserved
                                restart    = Restart Pending
                                maint_pend = Maintenance Pending
                                reassigned = Reassigned
                                prop'd_1tr6= Net may change channel #

T1 1 is up:
Loopback: NONE
DS0  Type       Modem    <->     Service       Channel       Rx          Tx
                                 State         State        A B C D     A B C D
-------------------------------------------------------------------------------------
  1    cas-modem   1       in     insvc       connected    1  1  1  1    1  1  1  1
  2    cas         -       -      insvc       idle         0  0  0  0    0  0  0  0
  3    cas         -       -      insvc       idle         0  0  0  0    0  0  0  0
  4    cas         -       -      insvc       idle         0  0  0  0    0  0  0  0
  5    cas         -       -      insvc       idle         0  0  0  0    0  0  0  0
  6    cas         -       -      insvc       idle         0  0  0  0    0  0  0  0
  7    cas         -       -      insvc       idle         0  0  0  0    0  0  0  0
  8    cas         -       -      insvc       idle         0  0  0  0    0  0  0  0
  9    cas         -       -      insvc       idle         0  0  0  0    0  0  0  0
  10   cas         -       -      maint      static-bo     0  0  0  0    1  1  1  1
  11   cas         -       -      maint      static-bo     0  0  0  0    1  1  1  1
  12   cas         -       -      maint      static-bo     0  0  0  0    1  1  1  1
  13   cas         -       -      maint      static-bo     0  0  0  0    1  1  1  1
  14   cas         -       -      maint      static-bo     0  0  0  0    1  1  1  1
  15   cas         -       -      maint      static-bo     0  0  0  0    1  1  1  1
  16   cas         -       -      maint      static-bo     0  0  0  0    1  1  1  1
  17   cas         -       -      maint      static-bo     0  0  0  0    1  1  1  1
  18   cas         -       -      maint      static-bo     0  0  0  0    1  1  1  1
  19   cas         -       -      maint      dynamic-bo    0  0  0  0    1  1  1  1
  20   cas         -       -      maint      dynamic-bo    0  0  0  0    1  1  1  1
  21   cas         -       -      maint      dynamic-bo    0  0  0  0    1  1  1  1
  22   unused
  23   unused
  24   unused
```

The following example shows that the ISDN PRI state is enabled on the Cisco AS5300 universal access server with a T1 PRI card:

```
Router# show controllers t1 2 timeslots 1-24

T1 2 is up:
Loopback:NONE
DS0 Type          Modem    <->  Service   Channel     Rx        Tx
                                State     State       A B C D   A B C D
-------------------------------------------------------------------------
 1  pri           -        -    insvc     idle
 2  pri           -        -    insvc     idle
 3  pri           -        -    insvc     idle
 4  pri           -        -    insvc     idle
 5  pri           -        -    insvc     idle
 6  pri           -        -    insvc     idle
 7  pri           -        -    insvc     idle
. . .
20  pri           -        -    insvc     idle
21  pri-modem     2        in   insvc     busy
22  pri-modem     1        out  insvc     busy
23  pri-digi      -        in   insvc     busy
24  pri-sig       -        -    outofsvc  reserved
```

show cot dsp

To display configuration and current status information about the Continuity Test (COT) Digital Signal Processor (DSP), use the **show cot dsp** command in privileged EXEC mode.

Cisco AS5300 Series

show cot dsp {**config** | **status**} *hardware-unit/ds0*

Cisco AS5800 Series

show cot dsp {**config** | **status**} *shelf/slot/hardware-unit/ds0*

Syntax Description

config	Displays the COT DSP configuration.
status	Displays the COT DSP status.
hardware-unit/ds0	Hardware unit number that provides the external interface connections from a router to the network, followed by a slash mark and the number of the COT operation request. Refer to the hardware installation guide for the signal processor to determine argument numbers.
shelf/slot/hardware-unit/ds0	Shelf number of COT operation request, the slot number, hardware unit number that provides the external interface connections from a router to the network, and the number of the COT operation request, each separated by a slash mark. Refer to the hardware installation guide for the signal processor to determine argument numbers.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(7)	This command was introduced.

Examples

The following is sample output from the **show cot dsp** command that shows the COT DSP configuration:

```
Router# show cot dsp status 1/1

Rx Freq 2010 Hx
Tx Freq 1780 Hx
Tx then Rx mode
in WaitRxOn state

Router# show cot dsp config 1/1

Rx Freq 2010 Hx
Tx Freq 1780 Hx
Tx then Rx mode
Timeout value:0
```

Table 34 describes the significant fields shown in the displays.

Table 34 show cot dsp Field Descriptions

Field	Description
Rx Freq	The COT receive tone frequency.
Tx Freq	The COT transmit tone frequency.
Tx then Rx	Type of COT operation.
WaitRxOn	The state of the COT DSP.

Related Commands

Command	Description
clear cot summary	Resets the COT counters displayed by the **show cot summary** command.
debug cot	Troubleshoots COT operation.
show cot request	Displays COT request information.
show cot summary	Displays information about the COT activity.

show cot request

To display information about Continuity Test (COT) operation requests, use the **show cot request** command in privileged EXEC mode.

Cisco AS5300 Series

show cot request *hardware-unit/ds0*

Cisco AS5800 Series

show cot request *shelf/slot/hardware-unit/ds0*

Syntax Description

hardware-unit/ds0	Hardware unit number that provides the external interface connections from a router to the network, followed by a slash mark and the number of the COT operation request. Refer to the hardware installation guide for the signal processor to determine argument numbers.
shelf/slot/hardware-unit/ds0	Shelf number of COT operation request, the slot number, hardware unit number that provides the external interface connections from a router to the network, and the number of the COT operation request, each separated by a slash mark. Refer to the hardware installation guide for the signal processor to determine argument numbers.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(7)	This command was introduced.

Examples

The following is sample output from the **show cot request** command:

```
Router# show cot request 1/1

00:19:29:COT Request@ 0x61064A20, CDB@ 0x60EBB48C, Params@0x61123DBC
00:19:29:  request type = COT_CHECK_TONE_ON
00:19:29:  shelf 0 slot 0 appl_no 1 ds0 1
00:19:29:  duration 100000 key FFF1 freqTx 1780 freqRx 2010
00:19:29:  state COT_WAIT_TD_ON_CT
00:19:29:  event_proc(0x6093B55C)
```

Table 35 describes the significant fields shown in the display.

Table 35 show cot request Field Descriptions

Field	Description
COT Request	Internal COT operation request.
CDB	Internal controller information.
Params	Internal COT operation request parameters.
request type	Type of COT operation.
duration	Timeout duration of COT operation.
key	COT operation identifier.
freqTx	Transmit tone frequency.
freqRx	Receive tone frequency.
state	COT subsystem machine state.
event_proc	COT subsystem state machine function.

Related Commands

Command	Description
clear cot summary	Resets the COT counters displayed by the show cot summary command.
debug cot	Troubleshoots COT operation.
show cot dsp	Displays information about the COT DSP configuration or current status.
show cot summary	Displays information about the COT activity.

show cot summary

To display information about Continuity Test (COT) activity, use the **show cot summary** command in privileged EXEC mode.

show cot summary

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(7)	This command was introduced.

Examples

The following is sample output from the **show cot summary** command that shows the COT Digital Signal Processor (DSP) configuration:

```
Router# show cot summary

08:23:24:  COT Subsystem - Request Statistics

08:23:24: COT Request Type = COT_DS0_LOOPBACK_ON
08:23:24: # of request(s)           : 4         # of restart requests(s)  : 0
08:23:24: # of successful request(s): 4         # of invalid request(s)   : 0
08:23:24: # of cot timeout(s)       : 0         # of dsp error(s)         : 0
08:23:24: # of no dsp(s)            : 0

08:23:24: COT Request Type = COT_DS0_LOOPBACK_OFF
08:23:24: # of request(s)           : 4         # of restart requests(s)  : 0
08:23:24: # of successful request(s): 4         # of invalid request(s)   : 0
08:23:24: # of cot timeout(s)       : 0         # of dsp error(s)         : 0
08:23:24: # of no dsp(s)            : 0

08:23:24: COT Request Type = COT_CHECK_TONE_ON
08:23:24: # of request(s)           : 7         # of restart requests(s)  : 0
08:23:24: # of successful request(s): 3         # of invalid request(s)   : 2
08:23:24: # of cot timeout(s)       : 1         # of dsp error(s)         : 0
08:23:24: # of no dsp(s)            : 0

08:23:24: COT Request Type = COT_CHECK_TONE_OFF
08:23:24: # of request(s)           : 0         # of restart requests(s)  : 0
08:23:24: # of successful request(s): 0         # of invalid request(s)   : 0
08:23:24: # of cot timeout(s)       : 0         # of dsp error(s)         : 0
08:23:24: # of no dsp(s)            : 0


08:23:24: COT Request Type = COT_CUT_IN_TRANSPONDER
08:23:24: # of request(s)           : 0         # of restart requests(s)  : 0
08:23:24: # of successful request(s): 0         # of invalid request(s)   : 0
08:23:24: # of cot timeout(s)       : 0         # of dsp error(s)         : 0
08:23:24: # of no dsp(s)            : 0
```

```
08:23:24: COT Request Type = COT_CUT_OUT_TRANSPONDER
08:23:24: # of request(s)           : 0         # of restart requests(s)  : 0
08:23:24: # of successful request(s): 0         # of invalid request(s)   : 0
08:23:24: # of cot timeout(s)       : 0         # of dsp error(s)         : 0
08:23:24: # of no dsp(s)            : 0
```

Table 36 describes the significant fields shown in the display.

Table 36 show cot summary Field Descriptions

Field	Description
# of request(s)	Number of COT operation requests.
# of successful request(s)	Number of successful COT operation requests.
# of cot timeout(s)	Number of COT subsystem timeouts.
# of no dsp(s)	Number of COT operation requests rejected because of unavailable DSP.
# of restart request(s)	Number of COT operation requests restarted.
# of invalid request(s)	Number of invalid COT operation requests.
# of dsp error(s)	Number of DSP errors.

Related Commands

Command	Description
clear cot summary	Resets the COT counters displayed by the show cot summary command.
debug cot	Troubleshoots COT operation.
show cot dsp	Displays information about the COT DSP configuration or current status.
show cot request	Displays COT request information.

show dhcp

To display the current Dynamic Host Configuration Protocol (DHCP) settings on point-to-point interfaces, use the **show dhcp** command in privileged EXEC mode.

show dhcp {**server** | **lease** [**interface async** [*number*]]}

Syntax Description

server	Displays known DHCP servers.
lease	Displays DHCP addresses leased from a server.
interface async [*number*]	(Optional) Specifies asynchronous interfaces and, optionally, a specific interface number.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

If you omit the optional argument, the **show dhcp** command displays information about all interfaces.

You can use this command on any point-to-point type of interface (for example, serial, ISDN, and asynchronous) that uses DHCP for temporary IP address allocation.

Examples

The following is sample output from the **show dhcp server** command:

```
Router# show dhcp server

IP address pooling for Point to Point clients is: DHCP Proxy Client
DHCP Proxy Client Status:
   DHCP server: ANY (255.255.255.255)
    Leases:   0
    Offers:   0      Requests: 0     Acks: 0     Naks: 0
    Declines: 0      Releases: 0     Bad:  0
```

Table 37 describes the significant fields shown in the display.

Table 37 show dhcp Field Descriptions

Field	Description
Leases	Number of current leased IP addresses.
Offers	Number of offers for an IP address sent to a proxy-client from the server.
Requests	Number of requests for an IP address to the server.
Acks	Number of “acknowledge” messages sent by the server to the proxy-client.

Table 37 show dhcp Field Descriptions (continued)

Field	Description
Naks	Number of "not acknowledge" messages sent by the server to the proxy-client.
Declines	Number of offers from the server that are declined by the proxy-client.
Releases	Number of times IP addresses have been relinquished gracefully by the client.
Bad	Number of bad packets received from wrong length, wrong field type, and so on.

Related Commands

Command	Description
ip address-pool	Enables an address pooling mechanism used to supply IP addresses to dial-in asynchronous, synchronous, or ISDN point-to-point interfaces.
ip dhcp-server	Specifies which DHCP servers to use on a network, and specifies the IP address of one or more DHCP servers available on the network.
peer default ip address	Specifies an IP address, an address from a specific IP address pool, or an address from the DHCP mechanism to be returned to a remote peer connecting to this interface.

show dialer

To display general diagnostic information for interfaces configured for dial-on-demand routing (DDR), use th**e show dialer** command in EXEC mode.

show dialer [**interface** *type number*]

Syntax Description

interface	(Optional) Displays information for the interface specified by the *type* and *number* arguments. Refer to your hardware installation guide to determine the arguments for interface type and number.
type	(Optional) Interface type.
number	(Optional) Interface number.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

If you enter the **show dialer interface** command for the D channel of an ISDN BRI or PRI, the command output also displays the B channels. That is, the **show dialer interface bri 0** command displays information of interfaces bri 0, bri 0:1, and bri 0:2. The **show dialer interface serial 0:23** command (for a channelized T1 line configured for ISDN PRI) displays information for serial interfaces 0:23, 0:0, 0:1, and so forth to 0:22.

If you have defined a dialer group that consists of the interfaces serial 0, serial 1, and bri 2, the **show dialer interface dialer 1** command displays information for interfaces bri 0, bri 0:1, bri 0:2, serial 1, and serial 0.

Examples

The following is sample output from the **show dialer** command for a BRI interface when dialer profiles are configured:

```
Router# show dialer interface bri 0

BRI0 - dialer type = ISDN

Dial String      Successes   Failures    Last called   Last status

0 incoming call(s) have been screened.

BRI0: B-Channel 1
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)

Dialer state is data link layer up

Dial reason: ip (s=10.1.1.8, d=10.1.1.1)

Interface bound to profile Dialer0
```

```
Time until disconnect 102 secs
Current call connected 00:00:19
Connected to 5551212 (Device1)

BRI0: B-Channel 2
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle
```

Table 38 describes the significant fields shown in the display.

Table 38 show dialer interface bri Field Descriptions

Field	Description
BRI0 - dialer type = ISDN	ISDN dialer.
Dial String	Dial strings of logged calls (telephone numbers). On ISDN BRI interfaces, if you have specified a subaddress number in the **dialer string,** this number is included in the dial string after a colon.
Successes	Successful connections (even if no data is passed).
Failures	Failed connections; call not successfully completed.
Last called	Time that last call occurred to specific dial string.
Last status	Status of last call to specific dial string (successful or failed).
0 incoming call(s) have been screened.	Number of calls subjected to Dialer Profiles screening to determine how the call is to be treated.
BRI0: B-Channel 1	Header indicating the following data is for B channel 1.
Idle timer (120 secs), Fast idle timer (20 secs)	Settings (in seconds) for the idle timer and the fast idle timer.
Wait for carrier (30 secs), Re-enable (15 secs)	Settings (in seconds) for the wait for carrier timer and the reenable timer.
Dialer state is data link layer up	The message “data link layer up” suggests that the dialer came up properly; if it says anything else then dialer did not come up properly. The message “physical layer up” means the Line Control Protocol (LCP) came up, but the Network control Protocol (NCP) did not come up. The **show interfaces** command also provides similar information.
Dial reason: ip (s=10.1.1.8, d=10.1.1.1)	What initiated the dial, namely an IP packet, plus source and destination address in the packet.
Interface bound to profile Dialer0	Dialer profile that is bound to this interface or B channel.
Time until disconnect	Time, in seconds, until line is configured to disconnect.
Current call connected	Time, in hours: minutes: seconds, at which the current call was connected.
Connected to	Dial string to which the line is currently connected.

The following is sample output from the **show dialer** command for an asynchronous interface:

```
Router# show dialer interface async 1

Async1 - dialer type = IN-BAND NO-PARITY
Idle timer (900 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Time until disconnect 838 secs
Current call connected 0:02:16
Connected to 8986

 Dial String      Successes   Failures    Last called   Last status
 8986                   0          0     never                     Defaults
 8986                   8          3     0:02:16       Success     Defaults
```

Table 39 describes the significant fields shown in the display.

Table 39 show dialer interface async Field Descriptions for In-Band Dialers

Field	Description
Async 1	Name of an asynchronous interface.
dialer type = IN-BAND	Indicates that DDR is enabled.
Idle timer (900 secs)	Idle timeout specification (in seconds).
Fast idle timer (20 secs)	Fast idle timer specification (in seconds).
Wait for carrier (30 secs)	Wait for carrier timer specification (in seconds).
Re-enable (15 secs)	Enable timeout specification (in seconds).
Time until disconnect	Time, in seconds, until line is configured to disconnect.
Current call connected	Time, in hours: minutes: seconds, at which the current call was connected.
Connected to	Dial string to which the line is currently connected.
Dial String	Dial strings of logged calls (telephone numbers). On ISDN BRI interfaces, if you have specified a subaddress number in the **dialer string** or **dialer map** command, this number is included in the dial string after a colon.
Successes	Successful connections (even if no data is passed).
Failures	Failed connections; call not successfully completed.
Last called	Time, in hours: minutes: seconds, that last call occurred to specific dial string, or never if call has never been made.
Last status	Status of last call to specific dial string (Success or Failed).
Defaults	If the DDR facility is using the dial string specified with the **dialer string** command, the word *Defaults* is appended to the Last status entry.

When the **show dialer** EXEC command is issued for a synchronous serial interface configured for data terminal ready (DTR) dialing, output similar to the following is displayed:

```
Router# show dialer interface serial 0

Serial 0 - dialer type = DTR SYNC
Idle timer (120 secs), Fst idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
```

```
Dial String    Successes   Failures    Last called   Last status
----                   1          0        1:04:47      Success      DTR dialer
8986                   0          0        never                     Defaults
```

Table 40 describes additional fields shown in the display; see Table 39 for information about the other fields in the report.

Table 40 show dialer Field Descriptions for DTR Dialers

Field	Description
DTR SYNC	Indicates that DDR is enabled and that DTR dialing is enabled on this synchronous interface.
Last status: Success	Indicates that the last call was successful and that DTR dialing was used.
DTR dialer	Phrase appended to the Last status entry to indicate that this is a DTR dialer.

If an interface is connected to a destination, a display is provided that indicates the idle time before the line is disconnected. (The value decrements each second.) Then the duration of the current connection is displayed. The following is an example of this display:

```
Time until disconnect 596 secs
Current call connected 0:00:25
```

After a call disconnects, the system displays the time remaining before it can be dialed again. The following is an example of this display:

```
Time until interface enabled 8 secs
```

If the **show dialer** command is issued for an interface on which DDR is not enabled, the system displays an error message. The following is a sample error message:

```
Async 1 - Dialing not enabled on this interface.
```

If an interface is configured for DDR, the **show interfaces** command displays the following message:

```
Async1 is up, line protocol is up (spoofing)
Hardware is Async Serial
```

The word *spoofing* indicates that the line really is not up, but the dialer is forcing the line to masquerade as “up” so that upper level protocols will continue to operate as expected. Spoofing is a state added to allow DDR to work. The interface “dials on demand” in response to packets being routed to it. But because no packets are routed to down interfaces, the interface must pretend to be up (spoof) so packets will be routed to it when it is not connected. Spoofing is the normal idle state on a dial-on-demand interface.

If caller ID screening is configured on an ISDN BRI, the **show dialer** command display includes a line similar to the following:

```
1 incoming call(s) have been screened.
```

This line reports the number of calls that have been screened.

show dialer dnis

To see how many calls Dialed Number Information Service (DNIS) groups have had, use the **show dialer dnis** command in user EXEC mode or privileged EXEC mode.

show dialer dnis {**group** [*name*] | **number** [*number*] | **range** [*start-range end-range*]}

Syntax Description

group	Displays DNIS group statistics.
name	(Optional) DNIS group name.
number	Displays DNIS group number statistics.
number	(Optional) DNIS group number.
range	Displays DNIS range statistics.
start-range	(Optional) DNIS start range.
end-range	(Optional) DNIS end range.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(4)XI	This command was introduced.
12.2(10)S	This command was integrated into Cisco IOS Release 12.2(10)S.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

If no DNIS groups are configured and resource pooling is enabled, then no calls are accepted. All calls are identified by call type/DNIS combinations.

Use the **show dialer dnis** command to display how many calls DNIS groups have had or how many calls a specific DNIS group has had. You can configure each DNIS group with multiple numbers. Using this command displays tables of statistics for each DNIS number received at the network access server.

Examples

The following example shows the **show dialer dnis** command being used to display DNIS group and DNIS number statistics:

```
Router# show dialer dnis ?

  group   DNIS group statistics
  number  DNIS number statistics
  range   DNIS range statistics
```

```
Router# show dialer dnis group

List of DNIS Groups:
  default
  mdm_grp1

Router# show dialer dnis group mdm_grp1

DNIS Number:2001
  0 total connections
  0 peak connections
  0 calltype mismatches
DNIS Number:2002
  0 total connections
  0 peak connections
  0 calltype mismatches
DNIS Number:2003
  0 total connections
  0 peak connections
  0 calltype mismatches
DNIS Number:2004
  0 total connections
  0 peak connections
  0 calltype mismatches

Router# show dialer dnis number

List of Numbers:
  default
  2001
  2002
  2003
  2004

Router# show dialer dnis number 2001

DNIS Number:2001
  0 connections total
  0 peak connections
  0 call-type mismatches
```

Table 41 describes the significant fields shown in the display.

Table 41 show dialer dnis Field Descriptions

Field	Description
List of DNIS Groups	List of DNIS groups assigned.
List of Numbers	List of DNIS numbers currently assigned.
DNIS Number	DNIS number assigned to specific customers.
total connections	Cumulative number of connections since the last **clear** command was used.
peak connections	Cumulative number of peak connections since the last **clear** command was used.
call-type mismatches	Cumulative number of call-type mismatches since the last **clear** command was used.

Related Commands

Command	Description
clear dialer dnis	Resets the counter statistics associated with a specific DNIS group or number.

show dialer interface bri

To display general diagnostic information for ISDN BRI interfaces configured for dial-on-demand routing (DDR), use the **show dialer interface bri** command in EXEC mode.

show dialer interface bri *number*

Syntax Description

number	BRI interface number.

Command Modes

EXEC

Command History

Release	Modification
9.21	This command was introduced.

Usage Guidelines

If you enter the **show dialer interface bri** command for the D channel of an ISDN BRI, the command output also displays the B channels. That is, the **show dialer interface bri 0** command displays information of interfaces bri 0, bri 0:1, and bri 0:2. Similarly, use of the related **show dialer interface serial 0:23** command (for a channelized T1 line configured for ISDN PRI) displays information for serial interfaces 0:23, 0:0, 0:1, and so forth to 0:22.

If you have defined a dialer group that consists of the interfaces serial 0, serial 1, and bri 2, the **show dialer interface dialer 1** command displays information for interfaces bri 0, bri 0:1, bri 0:2, serial 1, and serial 0.

Examples

The following example shows the **show dialer interface bri** command report for a BRI interface when dialer profiles are configured:

```
Router# show dialer interface bri 0

BRI0 - dialer type = ISDN

Dial String      Successes   Failures    Last called   Last status

0 incoming call(s) have been screened.

BRI0: B-Channel 1
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)

Dialer state is data link layer up

Dial reason: ip (s=10.1.1.8, d=10.1.1.1)

Interface bound to profile Dialer0

Time until disconnect 102 secs
Current call connected 00:00:19
Connected to 5551212 (Device1)
```

```
BRI0: B-Channel 2
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle
```

Table 42 describes the significant fields shown in the display.

Table 42 show dialer interface bri Field Descriptions

Field	Description
BRI0 - dialer type = ISDN	ISDN dialer.
Dial string	Dial strings of logged calls (telephone numbers). On ISDN BRI interfaces, if you have specified a subaddress number in the **dialer string**, this number is included in the dial string after a colon.
Successes	Successful connections (even if no data is passed).
Failures	Failed connections; call not successfully completed.
Last called	Time that last call occurred to specific dial string.
Last status	Status of last call to specific dial string (successful or failed).
0 incoming call(s) have been screened.	Number of calls subjected to Dialer Profiles screening to determine how the call is to be treated.
BRI0: B-Channel 1	Header indicating the following data is for B channel 1.
Idle timer (120 secs), Fast idle timer (20 secs)	Settings (in seconds) for the idle timer and the fast idle timer.
Wait for carrier (30 secs), Reenable (15 secs)	Settings (in seconds) for the wait for carrier timer and the reenable timer.
Dialer state is data link layer up	The message “data link layer up” suggests that the dialer came up properly; if it says anything else then dialer did not come up properly. The message “physical layer up” means the line protocol (LCP) came up, but the NCP did not come up. The **show interfaces** command also provides the similar information.
Dial reason: ip (s=6.1.1.8, d=6.1.1.1)	What initiated the dial, namely an IP packet, plus source and destination address in the packet.
Interface bound to profile Dialer0	Dialer profile that is bound to this interface or B channel.
Time until disconnect	Time until line is configured to disconnect. This field is displayed if the interface is currently connected to a destination.
Current call connected	Time at which the current call was connected.
Connected to	Dial string to which line is currently connected.

If an interface is connected to a destination, a display is provided that indicates the idle time before the line is disconnected. (The value decrements each second.) Then the duration of the current connection is shown. The following shows an example of this display:

```
Time until disconnect 596 secs
Current call connected 0:00:25
```

After a call disconnects, the system displays the time remaining before being it can dial again. The following is an example of this display:

```
Time until interface enabled 8 secs
```

If caller ID screening is configured on an ISDN BRI, the **show dialer interface bri** command display includes a line similar to the following:

```
1 incoming call(s) have been screened.
```

This line reports the number of calls that have been screened.

Related Commands

Command	Description
show dialer	Displays general diagnostic information for interfaces configured for DDR.

show dialer maps

To display configured dynamic and static dialer maps and dynamically created PPP Bandwidth Allocation Control Protocol (BACP) temporary static dialer maps, use the **show dialer maps** command in user EXEC or privileged EXEC mode.

show dialer maps

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.2	This command was introduced.
12.2(10)S	This command was integrated into Cisco IOS Release 12.2(10)S.
12.2SX	This command is supported in Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 series routers.
12.2(33)SRE	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRE.

Examples

The following is sample output from the **show dialer maps** command. The dialer maps are grouped by network address. When multiple dialer maps exist for the same network address, the dialer maps differ only by phone number. In this output, the dialer maps marked “BAP” are temporary dialer maps the PPP BACP creates when a peer calls from a different phone number than is configured or when a peer calls from a number that does not appear in an existing map. The temporary dialer maps allows PPP BACP to make outgoing calls to the peers.

```
Router# show dialer maps

Static dialer map ip 10.1.1.1 name peer_1 on Dialer1
Static dialer map ip 10.1.1.2 name peer_2 on Dialer1
BAP dialer map ip 10.1.1.2 name peer_2 on Dialer1
Dynamic dialer map ip 10.1.1.3 name peer_3 on Dialer1
BAP dialer map ip 10.1.1.3 name peer_3 on Dialer1
```

Table 43 describes the significant fields shown in the display.

Table 43 show dialer map Field Descriptions

Field	Description
Static dialer map ip 10.1.1.1	A configured static dialer map to call the specified protocol address.
name peer_1	Name of the remote peer.
on Dialer1	The physical or logical dialer interface on which the static map is configured.
BAP dialer map ip 10.1.1.2	A temporary dialer map that was created by PPP BACP for the particular destination with a different phone number from that of any existing maps. It will be removed when the BACP group is removed or the last remaining map to that destination is removed.
Dynamic dialer map ip 10.1.1.3	Dialer map dynamically created when a peer called.
BAP dialer map ip 10.1.1.3 name peer_3	Temporary static dialer map created by PPP BACP when required. It will be removed when the BACP group is removed or when the dynamic dialer map disappears.

Related Commands

Command	Description
dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites.

show dialer sessions

To display all dialer sessions, use the **show dialer sessions** command in EXEC mode.

show dialer sessions

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced.

Examples

In the following example, a Cisco 5350 router is dialing out to a Cisco 5300 router. All dialer sessions are displayed.

```
Router# show dialer sessions

DSES 0xAF0: index = 0x0, state = 3, ip addr = 10.2.2.22, dialed number = 81067, name = p5
200_pri.cisco.com, connected interface = Serial0:22
```

Table 44 describes the significant fields shown in the display.

Table 44 show dialer sessions Field Descriptions

Field	Description
ip addr	IP address of the remote interface that has been dialed into.
dialed number	Number that was used to dial out.
name	Name of the interface dialed into. This can be different from the router name, because names can be changed on per-interface basis.
connected interface	The channel on which the call is connected.

Related Commands

Command	Description
clear dialer sessions	Removes all dialer sessions and disconnects links when connected.

show dial-shelf

To display information about the dial shelf, including clocking information, use the **show dial-shelf** command in privileged EXEC mode.

show dial-shelf [**clocks** | **slot** *slot-number* [**clocks**]]

Syntax Description

clocks	(Optional) Displays the current primary and backup clocks along with their priorities.
slot *slot-number*	(Optional) Displays information for a specific slot; refer to your hardware installation guide to determine the *slot-number*.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.

Usage Guidelines

To configure the clock source and priority of the clock source used by the time-division multiplexing (TDM) bus on the dial shelf, use the **dial-tdm-clock** global configuration command.

Examples

The following is sample output from the **show dial-shelf** command:

```
Router# show dial-shelf

Slot  Board     CPU          DRAM           I/O Memory   State          Elapsed
       Type     Util     Total (free)    Total (free)                 Time
 1      CT1    0%/0%  22034060 ( 88%)  8388608 ( 49%)  Up             00:37:31
 5    Modem    0%/0%   7353996 ( 57%)  6291456 ( 35%)  Up             00:37:29
 6    Modem    0%/0%   7353996 ( 58%)  6291456 ( 35%)  Up             00:37:34
 7    Modem    5%/5%   7353996 ( 57%)  6291456 ( 35%)  Up             00:37:29
 8    Modem  19%/19%   7353996 ( 57%)  6291456 ( 35%)  Up             00:37:33
 9    Modem    8%/8%   7353996 ( 57%)  6291456 ( 35%)  Up             00:37:33
11    Modem    0%/0%   7353996 ( 57%)  6291456 ( 35%)  Up             00:37:30
12      DSC    0%/0%  20830044 ( 91%)  8388608 ( 66%)  Up             00:37:35
```

When the router is in dial shelf split mode, the **show dial-shelf** command indicates that the router shelf is running in split mode and which slots the router shelf owns. The status of any cards in any owned slots will be displayed just as they are in the present command. Thus when in normal mode, this command is unchanged from the original version.

When in split mode, the output will be extended, as in the following example:

```
Router# show dial-shelf

System is in split dial shelf mode.
Slots owned: 0 2 3 4 5 6 (connected to DSC in slot 13)
Slot    Board     CPU       DRAM          I/O Memory   State   Elapsed
         Type     Util    Total (free)   Total (free)          Time
 0        CE1    0%/0%  21341728( 87%)  8388608( 45%)  Up      00:11:37
```

```
 2        CE1    0%/0%  21341728( 87%)  8388608( 45%)  Up       00:11:37
 4 Modem(HMM)  20%/20%   6661664( 47%)  6291456( 33%)  Up       00:11:37
 5 Modem(DMM)    0%/0%   6661664( 31%)  6291456( 32%)  Up       00:11:37
 6 Modem(DMM)    0%/0%   6661664( 31%)  6291456( 32%)  Up       00:11:37
13        DSC    0%/0%  20451808( 91%)  8388608( 66%)  Up       00:16:31
Dial shelf set for auto boot
```

Note that only the first two lines of output are new; the remaining information is the same that you would obtain from the system if there were no cards in the slots, which in the above example, are not owned.

Table 45 describes the significant fields shown in the display.

Table 45 show dial-shelf Field Descriptions

Field	Description
Slot	Slot number of the card.
Board Type	Type of card in the slot. Types include channelized T1/E1 trunk cards, modem cards, or Dial Shelf Controller (DSC) card.
CPU Util	Utilization ratio of the CPU.
DRAM Total (free)	Percent of free space.
I/O Memory Total (free)	Percent of free disk space.
State	Current state of the card. Can be Up or Down.
Elapsed Time	The elapsed time, in hours: minutes: seconds, for which the shelf has been up.

The following examples show output from the **show dial-shelf clocks** command, for comparison.

Display 1

```
Router# show dial-shelf clocks

Primary Clock:
--------------
Slot 12:
System primary is 1/3/1 of priority 3
TDM Bus Master Clock Generator State = NORMAL

Backup clocks:
Source  Slot    Port    Priority      Status      State
-------------------------------------------------------
Trunk   1       2       10             Good        Configured

Status of trunk clocks:
-----------------------
Slot    Type    11 10  9  8  7  6  5  4  3  2  1  0
1       T1       B  B  B  B  B  B  B  B  B  G  B  B
3       T1       B  B  B  B  B  B  B  B  B  B  G  B
```

Display 2

```
Router# show dial-shelf clocks

Slot 12:
System primary is 6/76/0 of priority 76
TDM Bus Master Clock Generator State = HOLDOVER
```

```
Backup clocks:
Source  Slot    Port    Priority      Status      State
-------------------------------------------------------

Slot    Type    11 10  9  8  7  6  5  4  3  2  1  0
0       E1       B  B  B  B  B  B  B  B  B  B  B  B
```

Related Commands

Command	Description
show diag	Displays advanced troubleshooting information about line cards.
show dial-shelf split	Displays information about the types of cards in nonowned dial shelf slots.

show dial-shelf split

To display information about the types of cards in nonowned dial shelf slots, use the **show dial-shelf split** command in privileged EXEC mode.

show dial-shelf split

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.

Examples

The following is sample output from the **show dial-shelf split** command:

```
Router# show dial-shelf split

System is in split dial shelf mode, connected to DSC in slot 13.
Slots owned: 0 2 3 4 5 6
Non owned slots:
Slot    Board Type
 1      CE1
 7      Modem(DMM)
 8      Modem(DMM)
 9      Modem(DMM)
10      Slot Empty
11      Slot Empty
12      DSC
```

The report is self-explanatory.

Related Commands

Command	Description
show dial-shelf	Displays information about the types of cards in nonowned dial shelf slots.

show dsc clock

To display information about the dial shelf controller clock, use the **show dsc clock** command in privileged EXEC mode with the line card execute (**execute-on**) command.

execute-on {**slot** *slot-number* | **all**} **show dsc clock**

Syntax Description

execute-on	Executes commands remotely on a line card.
slot *slot-number*	Displays information for a specific slot. Slot number (12 or 13) must be occupied by a DSC card.
all	Executes the command on all line cards.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You must use the **show dsc clock** command from the router using the **execute-on** command.

Examples

The following is sample output from the **show dsc clock** command:

```
Router# execute-on slot 12 show dsc clock

Router#
Primary Clock:
--------------
Slot: 3, Port 1, Line 0, Priority = 3 up since 00:37:56
Time elapsed since last failure of the primary = 00:38:59

Backup clocks:
Source  Slot    Port    Line    Priority    Status      State
-----------------------------------------------------------------
Trunk   1       2       0       10          Good        Configured

All feature boards present are getting good clock from DSC
```

Table 46 describes the significant fields shown in the display.

Table 46 show dcs clock Field Descriptions

Field	Description
Primary clock	The clock designated as the master timing clock.
Priority	The order in which a clock is designated to back up the primary clock or the next higher priority clock in case of its failure.
Backup Source	The clock signal source, such as a trunk, internal clock, or external generator.
Feature board	An application-specific card in the dial shelf, such as a line card.
Trunk	The trunk line connected to the ISP or central office.
Status	Whether the clock source is capable of providing a synch source signal.
State	Whether the clock source is connected and assigned a priority.

Related Commands

Command	Description
execute-on	Executes commands remotely on a line card.

show dsi

To display information about the dial shelf interconnect (DSI) port adapter parameters, use the **show dsi** command in privileged EXEC mode with the line card execute (**execute-on**) command.

execute-on {**slot** *slot-number* | **all**} **show dsi**

Syntax Description

execute-on	Executes commands remotely on a line card.
slot *slot-number*	Displays information for a specific slot. Slot number (12 or 13) must be occupied by a DSC card.
all	Executes the command on all line cards.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The dial shelf interconnect (DSI) port adapter connects the Cisco 5814 dial shelf to the Cisco 7206 router shelf. The DSI port adapter allows data transfers between the dial shelf and the router shelf. Data is converted into packets by the feature cards, transmitted to a hub on the dial shelf controller card, and from there sent to the router shelf. Conversely, packets from the router shelf are sent to the dial shelf controller card, where they are transmitted over the backplane to the modem and trunk cards. The **show dsi** command is used to show information about the dial shelf interconnect hardware, interface, physical link, PCI registers, and address filters.

Examples

The following is sample output from the **show dsi** command:

```
Router# execute-on slot 1 show dsi

DSI-Tx-FastEthernet0 is up, line protocol is up
  Hardware is DEC21140A, address is 0008.26b7.b008 (bia 0008.26b7.b008)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  Half-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 01:17:09, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     6 packets input, 596 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

```
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast
     0 input packets with dribble condition detected
     6170 packets output, 813483 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
DSI-Rx-FastEthernet1 is up, line protocol is up
Hardware is DEC21140A, address is 0008.26b7.b008 (bia 0008.26b7.b008)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     6280 packets input, 362493 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Interface DSI-Tx-FastEthernet0
Hardware is DEC21140A
 dec21140_ds=0x604C9FC4, registers=0x3C000000, ib=0x1912E00
 rx ring entries=128, tx ring entries=256
 rxring=0x1912F00, rxr shadow=0x604CA16C, rx_head=6, rx_tail=0
 txring=0x1913740, txr shadow=0x604CA398, tx_head=138, tx_tail=138, tx_count=0
 PHY link up
 CSR0=0xFE024882, CSR3=0x1912F00, CSR4=0x1913740, CSR5=0xFC660000
 CSR6=0x320CA002, CSR7=0xFFFFA261, CSR8=0xE0000000, CSR9=0xFFFDC3FF
 CSR11=0xFFFE0000, CSR12=0xFFFFFF09, CSR15=0xFFFFFEC8
 DEC21140 PCI registers:
  bus_no=0, device_no=1
  CFID=0x00091011, CFCS=0x02800006, CFRV=0x02000022, CFLT=0x0000FF00
  CBIO=0x00000001, CBMA=0x48000000, CFIT=0x28140100, CFDA=0x00000000
 MII registers:
  Register 0x00:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
  Register 0x08:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
  Register 0x10:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
  Register 0x18:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
 throttled=0, enabled=0, disabled=0
 rx_fifo_overflow=0, rx_no_enp=0, rx_discard=0
 tx_underrun_err=0, tx_jabber_timeout=0, tx_carrier_loss=0
 tx_no_carrier=0, tx_late_collision=0, tx_excess_coll=0
 tx_collision_cnt=0, tx_deferred=0, fatal_tx_err=0, tbl_overflow=0
 HW addr filter: 0x604CABC4, ISL Disabled
  Entry= 0:  Addr=FFFF.FFFF.FFFF
  Entry= 1:  Addr=FFFF.FFFF.FFFF
  Entry= 2:  Addr=FFFF.FFFF.FFFF
  Entry= 3:  Addr=FFFF.FFFF.FFFF
  Entry= 4:  Addr=FFFF.FFFF.FFFF
  Entry= 5:  Addr=FFFF.FFFF.FFFF
  Entry= 6:  Addr=FFFF.FFFF.FFFF
  Entry= 7:  Addr=FFFF.FFFF.FFFF
  Entry= 8:  Addr=FFFF.FFFF.FFFF
```

```
  Entry= 9:  Addr=FFFF.FFFF.FFFF
  Entry=10:  Addr=FFFF.FFFF.FFFF
  Entry=11:  Addr=FFFF.FFFF.FFFF
  Entry=12:  Addr=FFFF.FFFF.FFFF
  Entry=13:  Addr=FFFF.FFFF.FFFF
  Entry=14:  Addr=FFFF.FFFF.FFFF
  Entry=15:  Addr=0008.26B7.B008

Interface DSI-Rx-FastEthernet1
Hardware is DEC21140A
dec21140_ds=0x604DDA4C, registers=0x3C000800, ib=0x1A01FC0
rx ring entries=128, tx ring entries=256
 rxring=0x1A020C0, rxr shadow=0x604DDBF4, rx_head=55, rx_tail=0
 txring=0x1A02900, txr shadow=0x604DDE20, tx_head=2, tx_tail=2, tx_count=0
 PHY link up
 CSR0=0xFE024882, CSR3=0x1A020C0, CSR4=0x1A02900, CSR5=0xFC660000
 CSR6=0x320CA202, CSR7=0xFFFFA261, CSR8=0xE0000000, CSR9=0xFFFDC3FF
 CSR11=0xFFFE0000, CSR12=0xFFFFFF09, CSR15=0xFFFFFEC8
 DEC21140 PCI registers:
  bus_no=0, device_no=2
  CFID=0x00091011, CFCS=0x02800006, CFRV=0x02000022, CFLT=0x0000FF00
  CBIO=0x00000001, CBMA=0x48000800, CFIT=0x28140100, CFDA=0x00000000
 MII registers:
  Register 0x00:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
  Register 0x08:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
  Register 0x10:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
  Register 0x18:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
 throttled=0, enabled=0, disabled=0
 rx_fifo_overflow=0, rx_no_enp=0, rx_discard=0
 tx_underrun_err=0, tx_jabber_timeout=0, tx_carrier_loss=0
 tx_no_carrier=0, tx_late_collision=0, tx_excess_coll=0
 tx_collision_cnt=0, tx_deferred=0, fatal_tx_err=0, tbl_overflow=0
 HW addr filter: 0x604DE64C, ISL Disabled
  Entry= 0:  Addr=FFFF.FFFF.FFFF
  Entry= 1:  Addr=FFFF.FFFF.FFFF
  Entry= 2:  Addr=FFFF.FFFF.FFFF
  Entry= 3:  Addr=FFFF.FFFF.FFFF
  Entry= 4:  Addr=FFFF.FFFF.FFFF
  Entry= 5:  Addr=FFFF.FFFF.FFFF
  Entry= 6:  Addr=FFFF.FFFF.FFFF
  Entry= 7:  Addr=FFFF.FFFF.FFFF
  Entry= 8:  Addr=FFFF.FFFF.FFFF
  Entry= 9:  Addr=FFFF.FFFF.FFFF
  Entry=10:  Addr=FFFF.FFFF.FFFF
  Entry=11:  Addr=FFFF.FFFF.FFFF
  Entry=12:  Addr=FFFF.FFFF.FFFF
  Entry=13:  Addr=FFFF.FFFF.FFFF
  Entry=14:  Addr=FFFF.FFFF.FFFF
  Entry=15:  Addr=0008.26B7.B008
```

Table 47 describes the significant fields shown in the display.

Table 47 show dsi Field Descriptions

Field	Description
FastEthernet0 ... is up ... is administratively down	Indicates whether the interface hardware is currently active and if it has been taken down by an administrator.
line protocol is	Indicates whether the software processes that handle the line protocol consider the line usable or if it has been taken down by an administrator.

Table 47 show dsi Field Descriptions (continued)

Field	Description
Hardware	Hardware type (for example, MCI Ethernet, SCI,[1] CBus[2] Ethernet) and address.
Internet address	Internet address followed by subnet mask.
MTU	Maximum Transmission Unit of the interface.
BW	Bandwidth of the interface in kilobits per second.
DLY	Delay of the interface in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100% reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to interface.
ARP type:	Type of Address Resolution Protocol assigned.
loopback	Indicates whether loopback is set or not.
keepalive	Indicates whether keepalives are set or not.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface. Useful for knowing when a dead interface failed.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. Useful for knowing when a dead interface failed.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 2^{31}ms (and less than 2^{32}ms) ago.
Output queue, input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped due to a full queue.

Table 47 show dsi Field Descriptions (continued)

Field	Description
5 minute input rate, 5 minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic it sends and receives (rather than all network traffic). The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no input buffer events.
Received ... broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the medium's minimum packet size. For instance, any Ethernet packet that is less than 64 bytes is considered a runt.
giants	Number of packets that are discarded because they exceed the medium's maximum packet size. For example, any Ethernet packet that is greater than 1518 bytes is considered a giant.
input errors	Includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts. Other input-related errors can also cause the input errors count to be increased, and some datagrams may have more than one error; therefore, this sum may not balance with the sum of enumerated input error counts.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
overrun	Number of times the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.

Table 47 show dsi Field Descriptions (continued)

Field	Description
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be increased.
abort	Number of packets whose receipt was aborted.
watchdog	Number of times watchdog receive timer expired. It happens when receiving a packet with length greater than 2048.
multicast	Number of multicast packets received.
input packets with dribble condition detected	Dribble bit error indicates that a frame is slightly too long. This frame error counter is incremented just for informational purposes; the router accepts the frame.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the transmitter has been running faster than the router can handle. This may never be reported on some interfaces.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, as some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages retransmitted due to an Ethernet collision. This is usually the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once in output packets.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds. On a serial line, this can be caused by a malfunctioning modem that is not supplying the transmit clock signal, or by a cable problem. If the system notices that the carrier detect line of a serial interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down.
restarts	Number of times a Type 2 Ethernet controller was restarted because of errors.
babbles	The transmit jabber timer expired.
late collision	Number of late collisions. Late collision happens when a collision occurs after transmitting the preamble.
deferred	Deferred indicates that the chip had to defer while ready to transmit a frame because the carrier was asserted.
lost carrier	Number of times the carrier was lost during transmission.

Table 47 show dsi Field Descriptions (continued)

Field	Description
no carrier	Number of times the carrier was not present during the transmission.
output buffer failures	Number of failed buffers and number of buffers swapped out.

1. SCI = Single Cell Input
2. CBus = Command Bus

Related Commands

Command	Description
execute-on	Executes commands on a line card.
show dsip	Displays all information about the DSIP.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

show dsip

To display all information about the Distributed System Interconnect Protocol (DSIP) on a Cisco AS5800, use the **show dsip** command in EXEC mode.

show dsip

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Your Cisco AS5800 universal access server uses a protocol used by the Cisco 7206 router shelf to communicate back and forth with the Cisco 5814 dial shelf controller card(s) and feature cards. Although dial shelf interconnect (DSI) configuration is transparent to the user, there are several show commands to help you view your setup, and debug commands to help you troubleshoot your system.

To display a subset of this information, use the **show dsip clients**, **show dsip nodes**, **show dsip ports**, **show dsip queue**, **show dsip tracing**, **show dsip transport**, and **show dsip version** commands.

Examples

The following is sample output from the **show dsip** command. For a description of the fields shown in the sample output, refer to the individual **show dsip** commands listed in the "Usage Guidelines" section.

```
Router# show dsip

DSIP Transport Statistics:
 IPC : input msgs=8233, bytes=699488; output msgs=8233, bytes=483558
        total consumed ipc msgs=682;  total freed ipc msgs = 682
        transmit contexts in use = 11, free = 245, zombie = 0, invalid = 0
        ipc getmsg failures = 0, ipc timeouts=0
        core getbuffer failures=0, api getbuffer failures=0
           dsip test msgs rcvd = 2770, sent = 0
 CNTL: input msgs=1112, bytes=91272; output msgs=146, bytes=8760
        getbuffer failures=0
 DATA: input msgs=0, bytes=0; output msgs=426, bytes=5112

DSIP Private  Buffer Pool Hits  = 0

DSIP Registered Addresses:
 Shelf0 : Master: 00e0.b093.2238, Status=local
 Shelf1 : Slot1 : 0007.5387.4808, Status=remote
 Shelf1 : Slot5 : 0007.5387.4828, Status=remote
 Shelf1 : Slot6 : 0007.5387.4830, Status=remote
```

```
 Shelf1 : Slot7 : 0007.5387.4838, Status=remote
 Shelf1 : Slot8 : 0007.5387.4840, Status=remote
 Shelf1 : Slot9 : 0007.5387.4848, Status=remote
 Shelf1 : Slot11: 0007.5387.4858, Status=remote
 Shelf1 : Slot12: 0007.4b67.8260, Status=remote

DSIP Clients:
-------------
ID    Name
0   Console
1   Clock
2   Modem
3   Logger
4   Trunk
5   Async data
6   TDM
7   Dial shelf manager
8   Environment Mon
9   DSIP Test

Dsip Local Ports:
-----------------
Client:Portname             Portid    In-Msgs   Bytes     Last-i/p
Console:Master              10004     0         0         never
Clock:Master                10005     29        3464      00:00:40
Modem:Master                10006     90        70162     00:23:44
Logger:Master               10007     0         0         never
Trunk:Master                10008     1765      140480    00:00:08
Async data:Master           10009     0         0         never
TDM:Master                  1000A     7         112       00:24:19
Dial shelf manager:Master   1000B     28        4752      00:00:36
DSIP Test:Master            1000C     2922      2922      00:00:00

Dsip Remote Ports:
------------------
Client:Portname             Portid    Out-Msgs  Bytes     Last-o/p  Last-act
Clock:Slave1                101005F   1         24        00:24:21  00:24:21
Trunk:Slave1                1010061   12        1776      00:24:21  00:24:21
Modem:Slave5                1050050   96        2148      00:23:56  00:24:19
Modem:Slave6                1060050   105       2040      00:24:00  00:24:22
Modem:Slave7                1070050   106       2188      00:23:56  00:24:20
Modem:Slave8                1080050   112       2212      00:24:13  00:24:35
Modem:Slave9                1090050   115       2224      00:24:09  00:24:35
Modem:Slave11               10B0050   107       2192      00:24:09  00:24:32
Clock:Slave12               10C000D   1         24        00:24:37  00:24:37
Dial shelf manager:Slave12  10C000E   28        4752      00:00:49  00:24:35
DSIP Test:Slave12           10C000F   0         0         never     00:24:35

DSIP ipc queue:
---------------
There are 0 IPC messages waiting for acknowledgement in the transmit queue.
There are 0 messages currently in use by the system.

DSIP ipc seats:
---------------
There are 9 nodes in this IPC realm.
   ID     Type                Name                      Last  Last
                                                        Sent  Heard
   10000 Local       IPC Master                           0      0
 1060000 DSIP        Seat:Slave6                          10     10
 10C0000 DSIP        Seat:Slave12                         2963   13
 1080000 DSIP        Seat:Slave8                          10     10
 1090000 DSIP        Seat:Slave9                          10     10
 1010000 DSIP        Seat:Slave1                          16     16
```

```
 1070000 DSIP        Seat:Slave7                                10     10
 10B0000 DSIP        Seat:Slave11                               10     10
 1050000 DSIP        Seat:Slave5                                10     10

DSIP version information:
-------------------------
Local DSIP major version =  3,    minor version = 2

All DS slots are running DSIP versions compatible with RS

Local Clients Registered Versions:
-----------------------------------
Client Name      Major Version   Minor Version
Console          3               2
Clock            1               1
Modem            0               0
Logger           No version      No version
Trunk            No version      No version
Async data       No version      No version
TDM              No version      No version
DSIP Test        No version      No version

Mismatched  Remote Client Versions:
-----------------------------------
```

Related Commands

Command	Description
show dsip clients	Lists the clients registered with DSIP on a system.
show dsip nodes	Displays information about the processors running the DSIP.
show dsip ports	Displays information about local and remote ports.
show dsip queue	Displays the number of messages in the retransmit queue waiting for acknowledgment.
show dsip tracing	Displays DSIP tracing buffer information.
show dsip transport	Displays information about the DSIP transport statistics for the control/data and IPC packets and registered addresses.
show dsip version	Displays DSIP version information.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

show dsip clients

To display information about Distributed System Interconnect Protocol (DSIP) clients, use the **show dsip clients** command in EXEC mode.

show dsip clients

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to see whether a client is actually registered with DSIP and using its services.

Consider the following example: a client “Trunk” seems to be defunct on a particular node with absolutely no input/output activity. The command **show dsip ports** does not show any Trunk port among its local ports though all other client ports show up. The problem might be that the Trunk client did not even register with DSIP. To confirm this, use the **show dsip clients** command.

Examples

The following is sample output from the **show dsip clients** command. This command lists the clients.

```
Router# show dsip clients

ID    Name
0   Console
1   Clock
2   Modem
3   Logger
4   Trunk
5   Async data
6   TDM
7   Dial shelf manager
8   Environment Mon
9   DSIP Test
```

Related Commands

Command	Description
show dsip nodes	Displays information about the processors running the DSIP.
show dsip ports	Displays information about local and remote ports
show dsip queue	Displays the number of messages in the retransmit queue waiting for acknowledgment.
show dsip tracing	Displays DSIP tracing buffer information.
show dsip transport	Displays information about the DSIP transport statistics for the control/data and IPC packets and registered addresses.
show dsip version	Displays DSIP version information.

show dsip nodes

To display information about the processors running the Distributed System Interconnect Protocol (DSIP), use the **show dsip nodes** command in EXEC mode.

show dsip nodes

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use **show dsip nodes** to see the nodes (slots) connected by DSIP and the node specific sequence numbers. The former information is also available from **show dsip transport**. The sequence numbers are useful for support engineers while debugging a problem.

Examples

The following is sample output from the **show dsip nodes** command:

```
Router# show dsip nodes

DSIP ipc nodes:
---------------
There are 9 nodes in this IPC realm.
   ID     Type                 Name                          Last  Last
                                                             Sent  Heard
   10000 Local      IPC Master                                  0      0
 1130000 DSIP       Dial Shelf:Slave12                          12     12
 1080000 DSIP       Dial Shelf:Slave1                           1      1
 10A0000 DSIP       Dial Shelf:Slave3                           1      1
 10C0000 DSIP       Dial Shelf:Slave5                           1      1
 10D0000 DSIP       Dial Shelf:Slave6                           1      1
 10E0000 DSIP       Dial Shelf:Slave7                           1      1
 10F0000 DSIP       Dial Shelf:Slave8                           1      1
 1100000 DSIP       Dial Shelf:Slave9                           1      1
```

Table 48 describes the significant fields shown in the display.

Table 48 show dsip nodes Field Descriptions

Field	Description
ID	DSIP uses Cisco's IPC (Inter Process Communication) module for nondata related (client control messages etc.) traffic. A seat or node is a computational element, such as a processor, that can be communicated with using IPC services. A seat is where entities and IPC ports reside. The IPC maintains a seat table which contains the seatids of all the seats in the system. Normally this seatid is a function of the slot number.
Type	Local: Local node. DSIP: Remote DSIP node.
Name	Each seat (node) has a name to easily identify it. There is only one master node and rest are slave nodes. The master node name is "IPC Master" and the slave node name is "Seat:Slave X", where "X" is the slot number of the node.
Last Sent/Last Heard	Each node maintains two sequence numbers for the last sent and last heard.
Last Sent	Whenever a message is sent out, the "last sent" counter is updated.
Last Heard	Whenever a message is received from a remote node, "last heard" is updated.

Related Commands

Command	Description
show dsip clients	Lists the clients registered with DSIP on a system.
show dsip ports	Displays information about local and remote ports
show dsip queue	Displays the number of messages in the retransmit queue waiting for acknowledgment.
show dsip tracing	Displays DSIP tracing buffer information.
show dsip transport	Displays information about the DSIP transport statistics for the control/data and IPC packets and registered addresses.
show dsip version	Displays DSIP version information.

show dsip ports

To display information about local and remote ports, use the **show dsip ports** command in EXEC mode.

show dsip ports [**local** | **remote** [*slot*]]

Syntax Description

local	(Optional) Displays information for local ports. The local port is the port created at a seat's local end.
remote	(Optional) Displays information for remote ports. The remote port is the port residing on a remote seat to which DSIP IPC based connection is open.
slot	(Optional) Specifies a slot number to display information for a specific card on the dial shelf.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The DSIP communication going through the IPC stack uses ports. The creation of a port returns a 32-bit port ID which is the endpoint for communication between two IPC clients.

The **show dsip ports** command is used to check clients that are up and running:

- To see the local ports that are created and the activity on them.
- To see the remote ports which are connected and to see the activity on them.

If no options are specified, information is displayed for both local and remote ports.

Examples

The following is sample output from the **show dsip ports** command:

```
Router# show dsip ports

Dsip Local Ports:
----------------
Client:Portname             Portid    In-Msgs   Bytes     Last-i/p
Console:Master              10004     0         0         never
Clock:Master                10005     16        1800      00:00:05
Modem:Master                10006     90        70162     00:10:08
Logger:Master               10007     0         0         never
Trunk:Master                10008     792       62640     00:00:03
Async data:Master           10009     0         0         never
TDM:Master                  1000A     7         112       00:10:44
Dial shelf manager:Master   1000B     15        2256      00:00:27
DSIP Test:Master            1000C     1294      1294      00:00:00
```

```
Dsip Remote Ports:
------------------
Client:Portname             Portid    Out-Msgs  Bytes     Last-o/p  Last-act
Clock:Slave1                101005F   1         24        00:10:46  00:10:46
Trunk:Slave1                1010061   12        1776      00:10:46  00:10:46
Modem:Slave5                1050050   96        2148      00:10:21  00:10:44
Modem:Slave6                1060050   105       2040      00:10:25  00:10:48
Modem:Slave7                1070050   106       2188      00:10:21  00:10:45
Modem:Slave8                1080050   112       2212      00:10:25  00:10:47
Modem:Slave9                1090050   115       2224      00:10:39  00:11:05
Modem:Slave11               10B0050   107       2192      00:10:39  00:11:02
Clock:Slave12               10C000D   1         24        00:11:07  00:11:07
Dial shelf manager:Slave12  10C000E   15        2256      00:00:45  00:11:05
DSIP Test:Slave12           10C000F   0         0         never     00:11:05
```

Table 49 describes the significant fields shown in the display.

Table 49 show dsip ports Field Descriptions

Field	Description
Client:Portname	Client name and port name. Port Name. The port names can be determined because they are based on a uniform naming convention that includes the following elements: • Client name • Master/slave status • Slot number Any client can derive the port name of the other client it wants to talk to once it knows its physical location, using the following formula: Master/Slave Status — Port Name Syntax Master — *Client-Name***:Master,** for example, **Console:Master** Slave — *Client-Name***:Slave***Slot*, for example, **Clock:Slave1**
Portid	Port ID. The Port ID is a 32-bit identifier comprised of **seatid** and the **port-number**. The IPC maintains a seat table which contains the seatids of all the seats in the system. A seat is where clients and ports reside. The seat ID is a function of the slot number. Port number is the sequential number of the port that is being created on a particular seat, for example: 0,1, 2, etc.
In-Msgs/	The total number of input messages that were received on a particular port.
Out-Msgs	The total number of output messages that were sent to a particular remote port.
Bytes(in/out)	The total number of bytes that were received on a particular port or sent to a remote port. The number of bytes on this port up to the time of the execution of the **show** command.
Last-i/p	Elapsed time since the last input was received on a local port.
Last-o/p	Elapsed time since the last message was sent to a particular remote port.
Last-act	Elapsed time since the connection to a remote port was opened.

Related Commands

Command	Description
show dsip clients	Lists the clients registered with DSIP on a system.
show dsip nodes	Displays information about the nodes (slots) connected by DSIP on a system.
show dsip queue	Displays the number of messages in the retransmit queue waiting for acknowledgment.
show dsip tracing	Displays DSIP tracing buffer information.
show dsip transport	Displays information about the DSIP transport statistics for the control/data and IPC packets and registered addresses.
show dsip version	Displays DSIP version information.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

show dsip queue

To display the number of IPC messages in the transmission queue waiting for acknowledgment, use the **show dsip queue** command in EXEC mode.

show dsip queue

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

IPC is inter-process communication. Processes communicate by exchanging messages held in queue buffers. Use the show dsip queue to display the status of these queue buffers.

Examples

The following is sample output from the **show dsip queue** command when the system is operating correctly:

```
Router# show dsip queue

DSIP ipc queue:
---------------
There are 0 IPC messages waiting for acknowledgment in the transmit queue.
There are 0 messages currently in use by the system.
```

Related Commands

Command	Description
show dsip clients	Lists the clients registered with DSIP on a system.
show dsip nodes	Displays information about the nodes (slots) connected by DSIP on a system.
show dsip ports	Displays information about local and remote ports.
show dsip tracing	Displays DSIP tracing buffer information.
show dsip transport	Displays information about the DSIP transport statistics for the control/data and IPC packets and registered addresses.
show dsip version	Displays DSIP version information.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

show dsip tracing

To display Distributed System Interconnect Protocol (DSIP) tracing buffer information, use the **show dsip tracing** command in EXEC mode.

show dsip tracing [**control** | **data** | **ipc**] [*slot* | **entries** *entry-number* [*slot*]]

Syntax Description

control	(Optional) Displays the control tracing buffer.
data	(Optional) Displays the data tracing buffer.
ipc	(Optional) Displays the inter-process communication tracing buffer.
slot	(Optional) Specifies a specific slot number on the dial shelf. Slot number can range from 0 to 14.
entries *entry-number*	(Optional) Specifies the number of entries to trace. Entries can be 1 to 500.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This feature allows logging of DSIP media header information. Use the **show dsip tracing** command to obtain important information of the various classes of DSIP packets (Control/Data/IPC) coming in. You must first use the **debug dsip tracing** command then use the **show dsip tracing** command to display the logged contents. To clear the information, use the **clear dsip tracing** command.

Examples

The following is sample output from the **show dsip tracing** command:

```
Router# debug dsip tracing

DSIP tracing debugging is on
Router#

Router# show dsip tracing

Dsip Control Packet Trace:
--------------------------------------------------------------------------------
Dest:00e0.b093.2238 Src:0007.5387.4808 Type:200B SrcShelf:1 SrcSlot:1 MsgType:0 MsgLen:82
Timestamp: 00:00:03
--------------------------------------------------------------------------------
Dest:00e0.b093.2238 Src:0007.5387.4838 Type:200B SrcShelf:1 SrcSlot:7 MsgType:0 MsgLen:82
Timestamp: 00:00:03
--------------------------------------------------------------------------------
```

```
Dest:00e0.b093.2238 Src:0007.4b67.8260 Type:200B SrcShelf:1 SrcSlot:12 MsgType:0 MsgLen:82
Timestamp: 00:00:03
-------------------------------------------------------------------------------
Dest:00e0.b093.2238 Src:0007.5387.4858 Type:200B SrcShelf:1 SrcSlot:11 MsgType:0 MsgLen:82
Timestamp: 00:00:03
-------------------------------------------------------------------------------
Dest:00e0.b093.2238 Src:0007.5387.4848 Type:200B SrcShelf:1 SrcSlot:9 MsgType:0 MsgLen:82
Timestamp: 00:00:03
```

Table 50 describes the significant fields shown in the display.

Table 50 show dsip tracing Field Descriptions

Field	Description
Dest	The destination MAC address in the DSIP packet.
Src	The source MAC address in the DSIP packet.
Type	There are three types of DSIP packets: • Control—0x200B • IPC—0x200C • Data—0x200D
SrcShelf	The source shelf ID of the DSIP packet.
SrcSlot	The source slot of the DSIP packet.
MsgType	Used to further demultiplex Data packets. Not used for Control and IPC type packets.
MsgLen	Length of the message excluding the DSIP header.
Timestamp	Time elapsed since the packet was received.

Related Commands

Command	Description
clear dsip tracing	Clears DSIP tracing logs.
debug dsip tracing	Enables DSIP trace logging for use with the show dsip tracing commands.
show dsip clients	Lists the clients registered with DSIP on a system.
show dsip nodes	Displays information about the nodes (slots) connected by DSIP on a system.
show dsip ports	Displays information about local and remote ports.
show dsip queue	Displays the number of messages in the retransmit queue waiting for acknowledgment.
show dsip transport	Displays information about the DSIP transport statistics for the control/data and IPC packets and registered addresses.
show dsip version	Displays DSIP version information.

show dsip transport

To display information about the Distributed System Interconnect Protocol (DSIP) transport statistics for the control/data and IPC packets and registered addresses, use the **show dsip transport** command in EXEC mode.

show dsip transport

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show dsip transport** command:

```
Router# show dsip transport

DSIP Transport Statistics:
 IPC : input msgs=4105, bytes=375628; output msgs=4105, bytes=248324
        total consumed ipc msgs=669;  total freed ipc msgs = 669
        transmit contexts in use = 11, free = 245, zombie = 0, invalid = 0
        ipc getmsg failures = 0, ipc timeouts=0
        core getbuffer failures=0, api getbuffer failures=0
       dsip test msgs rcvd = 1200, sent = 0
 CNTL: input msgs=488, bytes=40104; output msgs=68, bytes=4080
        getbuffer failures=0
 DATA: input msgs=0, bytes=0; output msgs=426, bytes=5112

DSIP Private  Buffer Pool Hits  = 0

DSIP Registered Addresses:
 Shelf0 : Master: 00e0.b093.2238, Status=local
 Shelf1 : Slot1 : 0007.5387.4808, Status=remote
 Shelf1 : Slot5 : 0007.5387.4828, Status=remote
 Shelf1 : Slot6 : 0007.5387.4830, Status=remote
 Shelf1 : Slot7 : 0007.5387.4838, Status=remote
 Shelf1 : Slot8 : 0007.5387.4840, Status=remote
 Shelf1 : Slot9 : 0007.5387.4848, Status=remote
 Shelf1 : Slot11: 0007.5387.4858, Status=remote
 Shelf1 : Slot12: 0007.4b67.8260, Status=remote
Router#
```

Table 51 describes the significant fields shown in the display:

Table 51 show dsip transport Field Descriptions

Field	Description
DSIP Transport Statistics:	There are basically three kinds of communication channels between the DSIP modules running on two processors: 1. IPC: DSIP IPC-based reliable/best-effort channel. 2. CNTL: Control packet channel for DSIP modules to communicate between themselves. For example, keepalive messages and initial handshake messages between two DSIP modules are exchanged over this channel. 3. DATA: DSIP fast data packet channel.
input msgs/output msgs	The number of input/output packets on a particular channel.
bytes	The number of input bytes received or sent on a particular channel.
total consumed ipc msgs	The total number of IPC messages consumed so far from the IPC buffer pool.
total freed ipc msgs	The total number of IPC messages returned to the IPC buffer pool so far.
transmit contexts in use	DSIP for each active reliable connection to a remote port keeps a transmit context. This context holds all the important information pertaining to the remote connection, such as, destination portid, port name, number of message and bytes sent to that port etc. This is created when first time a connection is opened to a remote port and is reused for all subsequent communication to that port.
free	Free transmit context is available.
zombie	When DSIP tears down a connection to a remote slot, all the transmit contexts to that slot should return to the free pool. But instead of immediately returning to the free pool, all such contexts first end up on a zombie queue, spend their last few seconds here and then eventually return to the free queue.
invalid	Each transmit context has a magic number. While returning contexts to the free queue, if any transmit context is found to be corrupted, it is marked as invalid and is not returned to the free queue.
ipc getmsg failures	Number of times we failed to get an ipc message.
ipc timeouts	The retry timeouts of the reliable DSIP transport stack.
core getbuffer failures	The number of times DSIP transport layer has failed to allocate buffers for the IPC transport.
aip getbuffer failures	The number of times DSIP transport has failed to allocate buffers while preparing to transmit data received from the clients.
dsip test msgs received/sent	The DSIP test messages received and sent by invoking received/sent the “DSIP Test” client.

Table 51 show dsip transport Field Descriptions (continued)

Field	Description
DSIP Private Buffer Pool Hits	DSIP by default gets all its buffers from the public buffer pools. If for some reason, it runs out of those buffers, it falls back on a DSIP private pool. This number indicates the number of times DSIP has used this fallback pool.
DSIP Registered Addresses	The MAC addresses of nodes (slots) participating in DSIP communication including the local node. The master sees N slaves whereas slave sees only master (excluding themselves). The information is presented in the following form: Shelf*X*: Master | Slot*Y* : *MAC Address* : Status= local | remote

Related Commands

Command	Description
show dsip clients	Lists the clients registered with DSIP on a system.
show dsip nodes	Displays information about the nodes (slots) connected by DSIP on a system.
show dsip ports	Displays information about local and remote DSIP ports.
show dsip queue	Displays the number of messages in the retransmit queue waiting for acknowledgment.
show dsip tracing	Displays DSIP tracing buffer information.
show dsip version	Displays DSIP version information.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

show dsip version

To display Distributed System Interconnect Protocol (DSIP) version information, use the **show dsip version** command in EXEC mode.

show dsip version

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show dsip version** command:

```
Router# show dsip version

DSIP version information:
------------------------
Local DSIP major version = 5,    minor version = 2

All feature boards are running DSIP versions compatible with router shelf

Local Clients Registered Versions:
----------------------------------
Client Name      Major Version   Minor Version
Console          52
Clock            1               1
Modem            0               0
Logger           No version      No version
Trunk            No version      No version
Async data       No version      No version
TDM              No version      No version
DSIP Test        No version      No version

Mismatched  Remote Client Versions:
---------------------------------
```

DSIP is version-controlled software that should be identified and kept current.

Related Commands

Command	Description
show dsip clients	Lists the clients registered with DSIP on a system.
show dsip nodes	Displays information about the nodes (slots) connected by DSIP on a system.
show dsip ports	Displays information about local and remote DSIP ports.
show dsip queue	Displays the number of messages in the retransmit queue waiting for acknowledgment.
show dsip tracing	Displays DSIP tracing buffer information.
show dsip transport	Displays information about the DSIP transport statistics for the control/data and IPC packets and registered addresses.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

show interfaces bri

To display information about the BRI D channel or about one or more B channels, use the **show interfaces bri** command in privileged EXEC mode.

show interfaces bri *number*[[**:***bchannel*] | [*first*] [*last*]] [**accounting**]

Cisco 7200 Series Router

show interfaces bri *slot/port*

Syntax Description

number	Interface number. The value ranges from 0 to 7 if the router has one 8-port BRI NIM or from 0 to 15 if the router has two 8-port BRI NIMs. Interface number values will vary, depending on the hardware platform used. The Cisco 3600 series router, for example, can have up to 48 interfaces. Specifying just the number will display the D channel for that BRI interface.
slot/port	On the Cisco 7200 series, slot location and port number of the interface. The slash mark is required.
:*bchannel*	(Optional) Colon (:) followed by a specific B channel number.
first	(Optional) Specifies the first of the B channels; the value can be either 1 or 2.
last	(Optional) Specifies the last of the B channels; the value can only be 2, indicating B channels 1 and 2.
accounting	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
11.2P	This command was enhanced to support the slot/port syntax for the PA-8B-ST and PA-4B-U port adapters on the Cisco 7200 series.

Usage Guidelines

Use either the **:***bchannel* argument or the *first* or *last* arguments to display information about specified B channels.

Use the **show interfaces bri** *number* form of the command (without the optional **:***bchannel,* or *first* and *last* arguments) to obtain D channel information.

Use the command syntax sample combinations in Table 52 to display the associated output.

Table 52 Sample show interfaces bri Command Step Combinations

Command Syntax	Displays
show interfaces	All interfaces in the router
show interfaces bri 2	Channel D for BRI interface 2
show interfaces bri 2:1	Channel B1 on BRI interface 2
show interfaces bri 2:2	Channel B2 on BRI interface 2
show interfaces bri 4 1	Channel B1 on BRI interface 4
show interfaces bri 4 2	Channel B2 on BRI interface 4
show interfaces bri 4 1 2	Channels B1 and B2 on BRI interface 4
show interfaces bri	Error message: "% Incomplete command."

Examples

The following is sample output from the **show interfaces bri** command:

```
Router# show interfaces bri 0:1

BRI0:1 is down, line protocol is down
  Hardware is BRI
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive not set
  LCP Closed
  Closed: IPCP
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 7 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

The following is sample output from the **show interfaces bri** command on a Cisco 7200 series router:

```
Router# show interfaces bri 2/0

BRI2/0 is up, line protocol is up (spoofing)
  Hardware is BRI
  Internet address is 10.1.1.3/27
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set
  Last input 00:00:01, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/64/0 (size/threshold/drops)
     Conversations  0/1 (active/max active)
     Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
```

```
609 packets input, 2526 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
615 packets output, 2596 bytes, 0 underruns
0 output errors, 0 collisions, 5 interface resets
0 output buffer failures, 0 output buffers swapped out
3 carrier transitions
```

Table 53 describes the significant fields shown in the display.

Table 53 show interfaces bri Field Descriptions

Field	Description
BRI... is {up | down | administratively down}	Indicates whether the interface hardware is currently active (whether line signal is present) and whether it has been taken down by an administrator.
line protocol is {up | down | administratively down}	Indicates whether the software processes that handle the line protocol consider the line usable (that is, whether keepalives are successful).
Hardware is	Hardware type.
Internet address is	IP address and subnet mask, followed by packet size.
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface in kilobits per second.
DLY	Delay of the interface in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to interface.
loopback	Indicates whether loopback is set or not.
keepalive	Indicates whether keepalives are set or not.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface. Useful for knowing when a nonfunctioning interface failed.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the “last” fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks (**) are printed.
Output queue, drops Input queue, drops	Number of packets in output and input queues. Each number is followed by a slash (/), the maximum size of the queue, and the number of packets dropped due to a full queue.
Five minute input rate Five minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes.
packets input	Total number of error-free packets received by the system.

Table 53 show interfaces bri Field Descriptions (continued)

Field	Description
bytes	Total number of bytes, including data and media access control (MAC) encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no input buffer events.
broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the medium's minimum packet size.
giants	Number of packets that are discarded because they exceed the medium's maximum packet size.
input errors	Total number of no buffer, runts, giants, CRCs, frame, overrun, ignored, and abort counts. Other input-related errors can also increment the count, so this sum may not balance with the other counts.
CRC	Cyclic redundancy checksum generated by the originating station or far-end device does not match the checksum calculated from the data received. On a serial link, CRCs usually indicate noise, gain hits, or other transmission problems on the data link.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. Broadcast storms and bursts of noise can increase the ignored count.
abort	Illegal sequence of one bits on a serial interface. This usually indicates a clocking problem between the serial interface and the data link equipment.
packets output	Total number of messages sent by the system.
bytes	Total number of bytes, including data and MAC encapsulation, sent by the system.
underruns	Number of times that the transmitter has been running faster than the router can handle. This may never be reported on some interfaces.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of collisions. These can occur when you have several devices connected on a multiport line.

Table 53 show interfaces bri Field Descriptions (continued)

Field	Description
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds. On a serial line, this can be caused by a malfunctioning modem that is not supplying the transmit clock signal or by a cable problem. If the system recognizes that the carrier detect line of a serial interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down.
restarts	Number of times the controller was restarted because of errors.
carrier transitions	Number of times the carrier detect signal of a serial interface has changed state. Check for modem or line problems if the carrier detect line is changing state often.

show interfaces serial bchannel

To display information about the physical attributes of the ISDN PRI over channelized E1 or channelized T1 B and D channels, use the **show interfaces serial bchannel** command in EXEC mode.

show interfaces serial *slot/port* **bchannel** *channel-number*

show interfaces serial *number* **bchannel** *channel-number*

Syntax Description

slot/port	Backplane slot number and port number on the interface. See your hardware installation manual for the specific slot and port numbers.
number	Network processor module (NPM) number, in the range from 0 to 2.
channel-number	E1 channel number ranging from 1 to 31 or T1 channel number ranging from 1 to 23; 1 to 24 if using NFAS.

Command Modes

EXEC

Command History

Release	Modification
11.2F	This command was introduced.

show interfaces virtual-access

To display status, traffic data, and configuration information about a specified virtual access interface, use the **show interfaces virtual-access** command in privileged EXEC mode.

show interfaces virtual-access *number* [**configuration**]

Syntax Description

number	Number of the virtual access interface.
configuration	(Optional) Restricts output to configuration information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2F	This command was introduced.
11.3	The **configuration** keyword was added.
12.3(7)T	The output for this command was modified to indicate if the interface is a member of a multilink PPP bundle.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB. This command was implemented on the Cisco 10000 series router for the PRE3 and PRE4.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.3(33)SRE.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

To identify the number of the vty on which the virtual access interface was created, enter the **show users** command.

The counts of output packet bytes as reported by the L2TP access server (LAC) to the RADIUS server in the accounting record do not match those of a client. The following paragraphs describe how the accounting is done and how you can determine the correct packet byte counts.

Packet counts for client packets in the input path are as follows:

- For packets that are process-switched, virtual access input counters are incremented by the coalescing function by the PPP over Ethernet (PPPoE) payload length.
- For packets that are fast-switched, virtual access input counters are incremented by the fast-switching function by the formula:

  PPPoE payload length + PPP address&control bytes = = PPPoE payload length + 2
- For packets that are Cisco Express Forwarding switched, virtual access input counters are incremented by the Cisco Express Forwarding switching function by the formula:

  IP length + PPP encapbytes (4) = = PPPoE payload length + 2

Packet counts for client packets in the output path are as follows:

- For packets that are process-switched by protocols other than PPP, virtual access output counters are incremented in the upper layer protocol by the entire datagram, as follows:

Size = PPPoE payload + PPPoE hdr (6) + Eth hdr (14) + SNAP hdr (10) + media hdr (4 for ATM)

- For packets process-switched by PPP Link Control Protocol (LCP) and Network Control Protocol (NCP), virtual access output counters are incremented by PPP, as follows:

  PPP payload size + 4 bytes of PPP hdr

- For packets that are Cisco Express Forwarding fast-switched, virtual access counters are incremented by the PPPoE payload size.

Accounting is done for PPPoE, PPPoA PPP Termination Aggregation (PTA), and L2X as follows:

- For PPPoE PTA, the PPPoE payload length is counted for all input and output packets.
- For PPPoE L2X on a LAC, the PPPoE payload length is counted for all input packets. On an L2TP Network Server (LNS), the payload plus the PPP header (address + control + type) are counted.
- For PPP over ATM (PPPoA) PTA i/p packets, the payload plus the PPP address plus control bytes are counted. For PPPoA PTA o/p packets, the payload plus PPP address plus control plus ATM header are counted.
- For PPPoA L2X on a LAC for i/p packets, the payload plus PPP addr plus cntl bytes are counted. For PPPoA L2X on a LNS, the payload plus PPP header (address + control + type) are counted.

In Cisco IOS Release 12.2(33)SB and later releases, the router no longer allows you to specify a virtual access interface (VAI) as **vi***x.y* in the **show pxf cpu queue** and **show interfaces** commands. Instead, you must spell out the VAI as **virtual-access**.

For example, when you enter the following commands, the router accepts the command:

```
Router# show interfaces virtual-access 2.1
```

In releases prior to Cisco IOS Release 12.2(33)SB, the router accepts the abbreviated form of the VAI. For example, the router accepts the following commands:

```
Router# show interfaces vi2.1
```

Examples

The following is sample output from the **show interfaces virtual-access** command:

```
Router# show interfaces virtual-access 3

Virtual-Access3 is up, line protocol is up
  Hardware is Virtual Access interface
  MTU 1500 bytes, BW 149760 Kbit, DLY 100000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open, multilink Open
  Link is a member of Multilink bundle Virtual-Access4
  PPPoATM vaccess, cloned from Virtual-Template1
  Vaccess status 0x44
  Bound to ATM4/0.10000 VCD:16, VPI:15, VCI:200, loopback not set
  DTR is pulsed for 5 seconds on reset
  Last input never, output never, output hang never
  Last clearing of "show interfaces" counters 00:57:37
  Input queue:0/75/0/0 (size/max/drops/flushes); Total output drops:0
  Queueing strategy:fifo
  Output queue:0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     676 packets input, 12168 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     676 packets output, 10140 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
```

```
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
```

Table 54 describes the significant fields shown in the display.

Table 54 show interfaces virtual-access Field Descriptions

Field	Description
Virtual-Access ... is {up | down | administratively down}	Indicates whether the interface is currently active (whether carrier detect is present), is inactive, or has been taken down by an administrator.
line protocol is {up | down | administratively down}	Indicates whether the software processes that handle the line protocol consider the line to be usable (that is, whether keepalives are successful).
Hardware is	Type of interface. In this case, the interface is a dynamically created virtual access interface that exists on a vty line.
MTU	Maximum transmission unit for packets on the virtual access interface.
BW	Bandwidth of the virtual access interface, in kbps.
DLY	Delay of the virtual access interface, in microseconds.
reliability	Reliability of the virtual access interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over five minutes.
txload, rxload	Load on the virtual access interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes. The calculation uses the value from the **bandwidth** interface configuration command. • txload— Transmit load on the virtual access interface as a value of 1/255 calculated as an exponentioal average over 5 minutes. • rxload— Receive load on the virtual access interface as a value of 1/255 calculated as an exponentioal average over 5 minutes.
Encapsulation	Encapsulation method assigned to the virtual access interface.
loopback	Test in which signals are sent and then directed back toward the source at some point along the communication path. Used to test network interface usability.
DTR	Data terminal ready. An RS232-C circuit that is activated to let the DCE know when the DTE is ready to send and receive data.
LCP open | closed | req sent	Link Control Protocol (for PPP only; not for Serial Line Internet Protocol (SLIP)). LCP must come to the open state before any useful traffic can cross the link.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by a virtual access interface. This value indicates when a dead interface failed.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by a virtual access interface.

Table 54 show interfaces virtual-access Field Descriptions (continued)

Field	Description
output hang	Number of hours, minutes, and seconds (or never) since the virtual access interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is displayed. If that field overflows, asterisks are displayed.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. Asterisks (***) indicate that the elapsed time is too lengthy to be displayed. Zeros (0:00:00) indicate that the counters were cleared more than 2^{31} milliseconds (ms) and less than 2^{32} ms ago.
Input queue, drops	Number of packets in input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped because of a full queue.
Queueing strategy	Type of queueing selected to prioritize network traffic. The options are first-come-first-served (FCFS) queueing, first-in-first-out queueing (FIFO), weighted fair queueing, priority queueing, and custom queueing.
Output queue	Packets in output queues. Represented by the maximum size of the queue followed by a slash and the number of packets dropped because of a full queue. For example, if the output queue is 45/15, 45 is the maximum size of the queue and 15 is the number of packets dropped.
5 minute input rate, 5 minute output rate	Average number of bits and packets transmitted per second in the last five minutes.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no-input-buffer events.
broadcasts	Total number of broadcast or multicast packets received by the virtual access interface.
runts	Number of packets that are discarded because they are smaller than the medium's minimum packet size.
giants	Number of packets that are discarded because they exceed the medium's maximum packet size.
input errors	Total number of no-buffer, runts, giants, cyclic redundancy checks (CRCs), frame, overrun, ignored, and abort counts. Other input-related errors can also increment the count, so that this sum might not balance with the other counts.

Table 54 show interfaces virtual-access Field Descriptions (continued)

Field	Description
CRC	Counter that reflects when the cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from data received. On a LAN, this often indicates noise or transmission problems on the LAN interface or the LAN bus. A high number of CRCs is usually the result of collisions or a station transmitting bad data. On a serial link, CRCs often indicate noise, gain hits, or other transmission problems on the data link.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
overrun	Number of times the serial receiver hardware was unable to send received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the virtual access interface because the interface hardware ran low on internal buffers. These buffers are different from the system buffers mentioned in the description of the no buffer field. Broadcast storms and bursts of noise can cause the "ignored" count to be incremented.
abort	Illegal sequence of one bits on a virtual access interface. This usually indicates a clocking problem between the virtual access interface and the data link equipment.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times the far-end transmitter has been running faster than the near-end communication server's receiver can handle. Underruns may never be reported on some virtual access interfaces.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the virtual access interface being examined. Note that this might not balance with the sum of the enumerated output errors, because some datagrams might have more than one error, and others might have errors that do not fall into any of the tabulated categories.
collisions	Number of packets colliding.
interface resets	Number of times a virtual access interface has been completely reset. A reset can happen if packets queued for transmission were not sent within several seconds. Resetting can be caused by a malfunctioning modem that is not supplying the transmit clock signal or by a cable problem. If the system notices that the carrier detect line of a virtual access interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when a virtual access interface is looped back or shut down.
output buffer failures	Number of outgoing packets dropped from the output buffer.

Table 54 show interfaces virtual-access Field Descriptions (continued)

Field	Description
output buffers swapped out	Number of times the output buffer was swapped out.
carrier transitions	Number of times the carrier detect (CD) signal of a virtual access interface has changed state. Indicates modem or line problems if the CD line changes state often. If data carrier detect (DCD) goes down and comes up, the carrier transition counter increments two times.

Related Commands

Command	Description
clear interface virtual-access	Tears down the virtual access interface and frees the memory for other dial-in uses.
interface virtual-template	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.
show pxf cpu queue	Displays PXF queueing statistics.
show users	Displays information about the active lines on the router or information about lawful-intercept users.

show ip interface virtual-access

To display network layer IP information about a specified virtual access interface, use the **show ip interface virtual-access** command in EXEC mode.

show ip interface virtual-access *number*

Syntax Description

number	Number of the virtual access interface.

Command Modes

EXEC

Command History

Release	Modification
11.2F	This command was introduced.

Examples

The following is sample output from the **show ip interface virtual-access** command. This virtual access interface has been configured with a virtual template interface that applies the **ip unnumbered ethernet 0** command.

```
Router# show ip interface virtual-access 1

Virtual-Access1 is up, line protocol is up
  Interface is unnumbered. Using address of Ethernet0 (172.21.114.132)
  Broadcast address is 255.255.255.255
  Peer address is 20.0.0.1
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is enabled
  Outgoing access list is not set
  Inbound  access list is Virtual-Access1#0
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
```

Table 55 describes only the output fields that are significant to virtual access interfaces and that are not described in other IP commands.

Table 55 show ip interface virtual-access Field Descriptions

Field	Description
Virtual-Access1 is up, line protocol is up	Virtual access interface is up and the upper layers consider the line usable.
Interface is unnumbered. Using the address of Ethernet0 (172.21.114.132)	The **ip unnumbered ethernet 0** command was included in the virtual template interface cloned on this interface.

Related Commands

Command	Description
ip unnumbered	Enables IP processing on a serial interface without assigning an explicit IP address to the interface.

show ip local pool

To display statistics for any defined IP address pools, use the **show ip local pool** command in privileged EXEC mode.

show ip local pool [*poolname* | **group** [*group-name*]]

Syntax Description

poolname	(Optional) Named IP address pool.
group	(Optional) Displays statistics of all pools in the base system group.
group [*group-name*]	(Optional) Displays statistics of all pools in the named group.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.1(5)DC	This command was enhanced to allow pool group statistics to be displayed.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and support was added for the Cisco 6400 node route processor 25v (NRP-25v) Cisco 7400 platforms.

Usage Guidelines

If you omit the *poolname* argument, the command displays a generic list of all defined address pools and the IP addresses that belong to them. If you specify the *poolname* argument, the command displays detailed information about that pool.

When you supply the **group** keyword without the associated group name, the command displays all pools in the base system group. When you supply the **group** keyword with the associated group name, the command displays all pools in that group.

Examples

The following is sample output from the **show ip local pool** command when pool groups have not been created:

```
Router# show ip local pool

Scope    Begin           End             Free InUse
Dialin   172.30.228.11   172.30.228.26   16   0
Available addresses:
   172.30.228.12
   172.30.228.13
   172.30.228.14
   172.30.228.15
   172.30.228.16
   172.30.228.17
   172.30.228.18
   172.30.228.19
   172.30.228.20
   172.30.228.21
   172.30.228.22
```

```
   172.30.228.23
   172.30.228.24
   172.30.228.25
   172.30.228.26
   172.30.228.11        Async5

Inuse addresses:
     None
```

The following is sample output from the **show ip local pool** command when pool groups have been created:

```
Router# show ip local pool

 Pool                    Begin           End             Free  In use
 ** pool <p1> is in group <g1>
 p1                      10.1.1.1        10.1.1.10         10       0
                         10.1.1.21       10.1.1.30         10       0
 ** pool <p2> is in group <g2>
 p2                      10.1.1.1        10.1.1.10         10       0
 lcl1                    10.2.2.1        10.2.2.10         10       0
                         10.2.2.21       10.2.2.30         10       0
                         10.2.2.41       10.2.2.50         10       0
 ** pool <mypool> is in group <mygroup>
 mypool                  172.18.184.223  172.18.184.224     2       0
                         172.18.184.218  172.18.184.222     5       0
 ** pool <ccc> is in group <grp-c>
 ccc                     172.18.184.218  172.18.184.220     3       0
 ** pool <bbb> is in group <grp-b>
 bbb                     172.18.184.218  172.18.184.220     3       0
 ** pool <ddd> is in group <grp-d>
 ddd                     172.18.184.218  172.18.184.220     3       0
 ** pool <pp1> is in group <grp-pp>
 pp1                     172.18.184.218  172.18.184.220     2       1
```

The following is sample output from the **show ip local pool** command for the pool group named mygroup:

```
Router# show ip local pool mygroup

 Pool                    Begin           End             Free  In use
 ** pool <mypool> is in group <mygroup>
 mypool                  172.18.184.223  172.18.184.224     2       0
                         172.18.184.218  172.18.184.222     5       0
```

The following sample output from the **show ip local pool group** command shows the base system group (lcl1):

```
Router# show ip local pool group

 Pool                    Begin           End             Free  In use
 lcl1                    10.2.2.1        10.2.2.10         10       0
                         10.2.2.21       10.2.2.30         10       0
                         10.2.2.41       10.2.2.50         10       0
```

Table 56 describes the significant fields shown in the displays.

Table 56 show ip local pool Field Descriptions

Field	Description
Scope	The type of access.
Begin	The first IP address in the defined range of addresses in this pool.
End	The last IP address in the defined range of addresses in this pool.
Free	The number of addresses available.
InUse	The number of addresses in use.
Pool	Pool and group names and associations, if created.

Related Commands

Command	Description
ip address-pool	Enables an address pooling mechanism used to supply IP addresses to dial asynchronous, synchronous, or ISDN point-to-point interfaces.
ip local pool	Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.

show ipx compression

To show the current status and statistics of Internetwork Packet Exchange (IPX) header compression during PPP sessions, use the **show ipx compression** command in EXEC mode.

show ipx compression [*interface-type*]

Syntax Description

interface-type	(Optional) Interface type, as listed in Table 57.

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.2(13)T	The **detail** argument was removed because the NetWare Link Services Protocol (NLSP) is no longer available in Cisco IOS software.

Usage Guidelines

Table 57 lists the supported interface types.

Table 57 Interface Types

Keyword	Description
async	Asynchronous interface.
ethernet	Ethernet IEEE 802.3 interface.
null	Null interface.
serial	WAN serial interface.

Related Commands

Command	Description
ipx compression cipx	Enables compression of IPX packet headers in a PPP session.
show ipx interface	Displays the status of the IPX interfaces configured in the Cisco IOS software and the parameters configured on each interface.

show ipx spx-protocol

To view the status of the Sequenced Packet Exchange (SPX) protocol stack and related counters, use the **show ipx spx-protocol** command in EXEC mode.

show ipx spx-protocol

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.

Examples

The following is sample output from the **show ipx spx-protocol** command:

```
Router> show ipx spx-protocol

Next wake time:

SPX socket: 1D90
  state: 0  Connections: 2

   SPX Remote: A001500::0000.c047.ed5a:3A80   Local: ACBB::0000.0000.0001:2010
   state 1  flags 1
   Queue counts:  inq 0,  outQ 0,  unackedQ 0
   Sequence: 34,  Ack: 34,  local-alloc: 39,  remote-alloc: 35
   Abort Timer fires in 24 secs
   Verify Watchdog Timer fires in 3 secs

   SPX Remote: A001500::0000.c047.ed5a:C980   Local: ACBB::0000.0000.0001:2900
   state 1  flags 1
   Queue counts:  inq 0,  outQ 0,  unackedQ 0
   Sequence: 111,  Ack: 55,  local-alloc: 60,  remote-alloc: 112
   Abort Timer fires in 27 secs
   Verify Watchdog Timer fires in 0 secs
```

Table 58 describes significant fields shown in the display.

Table 58 show ipx spx-protocol Field Descriptions

Field	Description
SPX socket:	IPX/SPX socket number.
state	Internal state.
connections:	Number of open connections for this IPX/SPX socket.
SPX Remote: *xxxxxxx::yyyy:zzzz*	The SPX client address for each SPX connection on this IPX/SPX socket, where *xxxx* is the client IPX network number, *yyyy* is the client IPX MAC address, and *zzzz* is the client SPX connection number.

Table 58 show ipx spx-protocol Field Descriptions (continued)

Field	Description
SPX Local *xxxxxxx::yyyy:zzzz*	The local SPX address, where *xxxx* is local IPX network number, *yyyy* is the local IPX MAC address, and *zzzz* is the local SPX connection number.
state	Internal state.
flags	A status bit that is used internally to allow and close connections.
Queue counts	inQ, outQ, and unackedQ, as specified in the following three rows.
inq	Number of SPX packets available for the SPX application to read.
outQ	Number of SPX packets that must be sent to the remote client.
unackedQ	Number of SPX packets sent, but no packet was received by the client, so far.
Sequence:	SPX sequence number. Represents the sequence number of next packet of data to be sent by the router.
Ack:	SPX acknowledgment number. Represents the sequence number of the client's packet that the router has received, so far.
local-alloc:	Maximum packet sequence number that is acceptable from the client. This is a method of imposing flow control on the NASI client.
remote-alloc:	Maximum packet sequence number that the NASI client can accept from the router. This is the NASI client's way of imposing flow control on the router.
Abort Timer	Time in seconds until this SPX connection is closed and deleted if a watchdog packet is not received.
Verify Watchdog Timer fires in X secs	Indicates the time when you last sent a watchdog packet to the client.

Related Commands

Command	Description
aaa authentication nasi	Specifies AAA authentication for NASI clients connecting through the access server.
ipx nasi-server enable	Enables NASI clients to connect to asynchronous devices attached to a router.
nasi authentication	Enables AAA authentication for NASI clients connecting to a router.
show ipx nasi connections	Displays the status of NASI connections.

show isdn

To display the information about memory, Layer 2 and Layer 3 timers, and the status of PRI channels, use the **show isdn** command in user EXEC or privileged EXEC mode.

show isdn {**active** [**detail**] [*dsl* | *serial-number*] | **call rate** [**table**] | **answer** [*dsl* | *serial-number*] | **history** [**detail**] [*dsl* | *serial-number*] | **memory** | **service** [*dsl* | *serial-number*] | **status** [*dsl* | *serial-number*] | **timers** [*dsl* | *serial-number*]}

Syntax Description

active [**detail**] [*dsl* | *serial-number*]	Displays current call information of all ISDN interfaces or, optionally, a specific digital subscriber line (DSL) (created and configured as a serial interface) or a specific ISDN PRI interface. Values of *dsl* range from 0 to 15. Information includes the called number, the remote node name, the seconds of connect time, the seconds of connect time remaining, the seconds idle, and Advice of Charge (AOC) charging time units used during the call. The **detail** keyword provides additional information about active calls.
call rate [**table**]	Displays incoming and outgoing ISDN call switching rate. The optional **table** keyword presents the data in a tabular format.
answer [*dsl* | *serial-number*]	Displays whether a called-party or subaddress number has been configured in the incoming setup message for ISDN BRI calls.
history [**detail**] [*dsl* | *serial-number*]	Displays historic and current call information for all ISDN interfaces or, optionally, a specific DSL (created and configured as a serial interface) or a specific ISDN PRI interface. Values of *dsl* range from 0 to 15. Information displayed includes the called number, the remote node name, the seconds of connect time, the seconds of connect time remaining, the seconds idle, and AOC charging time units used during the call. The **detail** keyword provides additional information about historical calls.
memory	Displays ISDN memory pool statistics. This keyword is for use by technical development personnel only.
service [*dsl* | *serial-number*]	Displays the service status of all ISDN interfaces or, optionally, a specific DSL or a specific ISDN PRI interface (created and configured as a serial interface). Values of *dsl* range from 0 to 15.
status [*dsl* | *serial-number*]	Displays the status of all ISDN interfaces or, optionally, a specific DSL or a specific ISDN PRI interface (created and configured as a serial interface). Values of *dsl* range from 0 to 15.
timers [*dsl* | *serial-number*]	Displays the values of Layer 2 and Layer 3 timers for all ISDN interfaces or, optionally, a specific DSL or a specific ISDN PRI interface (created and configured as a serial interface). Values of *dsl* range from 0 to 15.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.1	This command was introduced.
12.2(8)B	This command was enhanced to display a report about D-channel and Redundant Link Manager (RLM) group status.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T, and implemented on the Cisco 2420, Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers, and Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 network access server (NAS) platforms.
12.3	This command was enhanced to display the message "%Q.931 is backhauled to BACKHAUL on DSL 0. Layer 3 output may not apply".
12.4	The **show isdn memory** output was modified to display information about Call Tables.
12.4	The **detail** keyword was added.
12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The **call rate** and **table** keywords were added.

Usage Guidelines

Native ISDN stacks do not know Layer 3 details because Layer 3 is backhauled to an external application. So informational message "%Q.931 is backhauled to BACKHAUL on DSL 0. Layer 3 output may not apply" is displayed for those users that expect ISDN commands to show the required output.

The following sections in the "Examples" section show how to display and interpret reports from the **show isdn** command options:

- show isdn active and show isdn history Command Examples, page 870
- show isdn answer Command Example, page 873
- show isdn memory Command Example, page 873
- show isdn service Command Examples, page 874
- show isdn status Command Examples, page 875
- show isdn timers Command Examples, page 879

Examples

show isdn active and show isdn history Command Examples

This section shows example output from the **show isdn active** and **show isdn history** commands on different Cisco routers. The commands report similar information about call activity, which is described in Table 59.

```
Router# show isdn active

%Q.931 is backhauled to BACKHAUL on DSL 0. Layer 3 output may not apply

-------------------------------------------------------------------------------
                              ISDN ACTIVE CALLS
-------------------------------------------------------------------------------
History Table MaxLength = 100 entries
History Retain Timer = 15 Minutes
-------------------------------------------------------------------------------
Call Calling and Called  Remote Node  Seconds  Seconds  Seconds Recorded Charges
Type Phone Number        Name         Used     Left     Idle    Units/Currency
-------------------------------------------------------------------------------
```

```
In +---Not Available----       Node1   684802  +499598     401
In +---Not Available----       Node2   363578  +499503     496
In +---Not Available----       Node3   253232  +499325     674
In +---Not Available----               194047  +499965      34
In +---Not Available----       Node4   189165  +499841     158
In +---Not Available----       Node5   110342               0
In +---Not Available----                 2603  +499997       2
In +---Not Available----                 1310  +499798     201


--------------------------------------------------------------------------------

Router# show isdn active ser3:23

%Q.931 is backhauled to IUA BACKHAUL on DSL 3. L3 output may not apply
--------------------------------------------------------------------------------
                              ISDN ACTIVE CALLS
--------------------------------------------------------------------------------
Call    Calling      Called       Remote  Seconds Seconds Seconds Charges
Type    Number       Number       Name    Used    Left    Idle    Units/Currency
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
```

The following example shows the output from the **show isdn history** command:

```
Router# show isdn history

--------------------------------------------------------------------------------
                            ISDN CALL HISTORY
--------------------------------------------------------------------------------
History Table MaxLength = 100 entries
History Retain Timer = 15 Minutes
--------------------------------------------------------------------------------
Call Calling and Called  Remote Node  Seconds  Seconds  Seconds Recorded Charges
Type Phone Number        Name         Used     Left     Idle    Units/Currency
--------------------------------------------------------------------------------
In +---Not Available----       Node1   684818  +499583     416
In +---Not Available----       Node2   363593  +499488     511
In +---Not Available----       Node3   253248  +499310     689
In +---Not Available----               194062  +499950      49
In +---Not Available----       Node4   189180  +499826     173
In +---Not Available----       Node5   110357               0
In +---Not Available           Node6     5244
In +---Not Available----                 2619  +499997       0
In +---Not Available----       Node7     1432
In +---Not Available----                 1325  +499783     216
In +---Not Available----       Node8      161


--------------------------------------------------------------------------------

Router# show isdn history ser2:23

%Q.931 is backhauled to IUA BACKHAUL on DSL 2. L3 output may not apply
--------------------------------------------------------------------------------
                            ISDN CALL HISTORY
--------------------------------------------------------------------------------
Call History contains all active calls, and a maximum of 100 inactive calls.
Inactive call data will be retained for a maximum of 15 minutes.
--------------------------------------------------------------------------------
Call    Calling      Called       Remote  Seconds Seconds Seconds Charges
Type    Number       Number       Name    Used    Left    Idle    Units/Currency
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
```

Table 59 show isdn active and show isdn history Field Descriptions

Field	Description
History Table MaxLength	Maximum number of entries that can be retained in the Call History table.
History Retain Timer	Maximum amount of time any entry can be retained in the Call History table.
Call Type	Type of call: In for incoming, Out for outgoing, or -- when direction of call cannot be determined.
Calling Number	For incoming calls, the number from which the call was received.
Called Number	For outgoing calls, the number to which the call was placed.
Duration Seconds	Number of seconds the call lasted. Indicates whether the call is still active, and how many seconds it has lasted so far.
Calling and Called Phone Number	For incoming calls, the number from which the call was received. For outgoing calls, the number to which the call was placed, or +---Not Available---- when a phone number is not available. The phone number display is limited to 20 digits. (+---Not Available---- is the truncated version of ----Not Available----. The + in the field means more data is available than can be displayed. The low-order data is displayed and the overflowing data is replaced by a +.)
Remote Node Name	Name of the host placing the call or the host called. The name display is limited to ten characters.
Seconds Used	Up to six digits of seconds (up to 999999) showing connect time used, or Failed when the connection attempt fails.
Seconds Left	Up to six digits of seconds (up to 999999) of connect time remaining when the **dialer idle-timeout** command is configured. The + in the field means more data is available than can be displayed. The low-order data is displayed and the overflowing data is replaced by a +.
Seconds Idle	Six digits of seconds (up to 999999) since the last interesting packet.
Time until Disconnect	Number of configured seconds before the call is disconnected because of the static idle timer for the map class or the interface.
Recorded Charges Units/Currency	For outgoing calls, number of ISDN Advice of Charge (AOC) charging units used or the currency cost of the call. Currency information display is limited to ten characters.
D-DSL	Digital subscriber line (DSL) number that received or sent the setup message.
DSL	DSL number on which the call completed.
Int-id	Non-Facility Associated Signalling (NFAS) interface number on which the call was completed.
B-chan	B-channel on the DSL used for the call.
Callid	Call-id value for the call.
Conn	Current connected state.
Disc Updated	Current state of the Disconnect updated indicator.
Call Type	Generic call type (for example, DATA, VOICE, or V110).

show isdn answer Command Example

The following report by the **show isdn answer** command indicates that no called-party or subaddress number has been configured:

```
Router# show isdn answer ser0:23 1234

%Q.931 is backhauled to IUA BACKHAUL on DSL 0. Layer 3 output may not apply

no isdn answer1 configured
no isdn answer2 configured
```

See the description for the **isdn answer1** command for more information about this report.

show isdn memory Command Example

The following is sample output from the **show isdn memory** command providing statistical information about memory resources:

```
Router# show isdn memory

MEMORY POOL STATISTICS
        BlockType          in use  limit max used
        mail descriptors        0   6720       32
        exec timer blocks       0   6720        0
        Modem_msg               0   1960        0
        LIF timers           1256      -     1256
        L2IF timers            42      -       42
        PRIM_BTYPE           1298      -     1313
        PKT_BTYPE               0      -       87
        HEADER_BTYPE            0      -       87
        SML_INFO_BTYPE          0      -        6
        LRG_INFO_BTYPE          0      -       20
        PKG_BTYPE               0      -       20
        Router_msg              0      -       20
        X25_msg                 0      -        0
        Tdial_msg               0      -        0
        Socket_msg              0      -        0
        Call Tables             0      -       21
        CCBs                    0      -       42
        DLCBs                  14      -       14
        NLCBs                  62      -       62
```

Table 60 describes the significant fields shown in the display.

Table 60 show isdn memory Field Descriptions

Field	Description
BlockType	The type of block for this line of information.
in use	The number of BlockType blocks that are current.
limit	The maximum number of BlockType blocks that can be allocated. A dash (-) indicates no limit.
max used	The maximum number of BlockType blocks that are allocated at one time.
mail descriptors	Intertask dispatch queue elements.
exec timer blocks	Intertask delay timer structures.
Modem_msg	Memory allocated to modem messages.
LIF timers	Layer-3 timer blocks (call related).

Table 60 show isdn memory Field Descriptions (continued)

Field	Description
L2IF timers	Layer-2 timer blocks (per message).
PRIM_BTYPE	Primitive block–ISDN internal (layer to layer) communication structure.
PKT_BTYPE	Packet block: ISDN internal (layer to layer) communication data structure.
HEADER_BTYPE	Header block: ISDN internal (layer to layer) communication structure.
SML_INFO_BTYPE	Small buffer: ISDN message block (up to 28 bytes).
LRG_INFO_BTYPE	Large buffer: ISDN message block (up to 1024 bytes).
PKG_BTYPE	Package block: ISDN internal (layer to layer) communication structure.
Router_msg	Queue of messages from another task in a router for ISDN.
X25_msg	Queue of messages for the X.25 internal interface for ISDN.
Tdial_msg	Queue of messages for Thunder dial/Thunder voice interface.
Socket_msg	Queue of messages used for socket interface.
Call Tables	Call redial block: ISDN redial structure.
CCBs	Call Control Blocks (CCB). Structures used by the Call Control layer.
DLCBs	Data Link Control Block (DLCB). Structures used by the Data Link layer (Q.921).
NLCBs	Network Layer Control Block (NLCB). Structures used by the Network layer (Q.931).

show isdn service Command Examples

The following example of the **show isdn service** command shows channel states when a PRI is configured on a T1 controller. Table 61 describes the significant fields shown in the display.

```
Router# show isdn service

%Q.931 is backhauled to IUA BACKHAUL on DSL 2. L3 output may not apply

PRI Channel Statistics:
ISDN Dc0 SC, Channel [1-31]
  Configured Isdn Interface (dsl) 0
   Channel State (0=Idle 1=Proposed 2=Busy 3=Reserved 4=Restart 5=Maint_Pend)
    Channel : 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4
    State   : 2 2 2 2 2 2 2 2 2 0 0 0 0 2 2 2 2 2 2 2 2 0 0
   Service State (0=Inservice 1=Maint 2=Outofservice)
    Channel : 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4
    State   : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
   Channel blocked? (0=No 1=Yes)
    Channel : 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4
              0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
```

Table 61 show isdn service Field Descriptions

Field	Description
ISDN Se1/0:23 ISDN Dc0 SC Channel [1-31]	ISDN interface type followed by the channel range. A range from 1 to 31 is a standard format for both T1 and E1 outputs, but the state value shown identifies whether the channel is used.
Configured Isdn Interface (dsl) 0	DSL value is 0.
Channel State (0=Idle 1=Propose 2=Busy 3=Reserved 4=Restart 5=Maint_Pend)	Current state of each channel. Channels 24 through 31 are marked as reserved when the output is from T1.
Service State (0=Inservice 1=Maint 2=Outofservice)	Service state assigned to each channel. Channel 24 is marked as out of service.[1]

1. If channel 24 (marked as out of service) is configured as the Non-Facility Associated Signaling (NFAS) primary D channel, NFAS will roll over to the backup D channel if one is configured. If channel 24 is a B channel, it will not accept calls.

show isdn status Command Examples

Table 62 describes the significant fields shown in the output of the following **show isdn status** command examples.

The following sample output from the **show isdn status** command shows a report about D-channel and Redundant Link Manager (RLM) group status for RLM configurations, and applications like Signaling System 7 (SS7) in integrated Signaling Link Terminal (SLT) configurations:

```
Router# show isdn status

%Q.931 is backhauled to BACKHAUL on DSL 0. L3 output may not apply

Global ISDN Switchtype = primary-ni
ISDN Dchannel0 interface   rlm-group = 1
    Transport Link Status:
    ACTIVE
    dsl 0, interface ISDN Switchtype = primary-ni : Primary D channel of nfas group 0
    Layer 1 Status:
    DEACTIVATED
    Layer 2 Status:
    TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
    0 Active Layer 3 Call(s)
    Active dsl 0 CCBs = 0
    The Free Channel Mask:  0x80000000
    Number of L2 Discards = 0, L2 Session ID = 43
ISDN Dchannel1 interface
    Transport Link Status :  Not Applicable
    dsl 1, interface ISDN Switchtype = primary-ni : Group member of nfas group 0
    Layer 1 Status:
    DEACTIVATED
    Layer 2 Status: Not Applicable
    Layer 3 Status:
    0 Active Layer 3 Call(s)
    Active dsl 1 CCBs = 0
    The Free Channel Mask:  0x80000000
    Number of L2 Discards = 0, L2 Session ID = 0
ISDN Serial2:15 interface
    dsl 2, interface ISDN Switchtype = primary-ni : Primary D channel of nfas group 1
    Layer 1 Status:
    DEACTIVATED
    Layer 2 Status:
```

```
    TEI = 0, Ces = 1, SAPI = 0, State = TEI_ASSIGNED
    Layer 3 Status:
    0 Active Layer 3 Call(s)
    Active dsl 2 CCBs = 0
    The Free Channel Mask:  0x0
    Number of L2 Discards = 0, L2 Session ID = 0
ISDN Serial3:15 interface
    dsl 3, interface ISDN Switchtype = primary-ni : Group member of nfas group 1
    Layer 1 Status:
    ACTIVATING
    Layer 2 Status: Not Applicable
    Layer 3 Status:
    0 Active Layer 3 Call(s)
    Active dsl 3 CCBs = 0
    The Free Channel Mask:  0x0
    Number of L2 Discards = 0, L2 Session ID = 0
    Total Allocated ISDN CCBs = 0
```

The following sample output from the **show isdn status** command shows when no calls are active for a Cisco 4500 router with eight BRIs and one E1 PRI:

```
Router# show isdn status

%Q.931 is backhauled to BACKHAUL on DSL 0. L3 output may not apply

Global ISDN Switchtype = basic-5ess
ISDN BRI0 interface
        dsl 0, interface ISDN Switchtype = basic-5ess
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 64, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Activated dsl 0 CCBs = 0
ISDN BRI1 interface
        dsl 1, interface ISDN Switchtype = basic-5ess
    Layer 1 Status:
        DEACTIVATED
    Layer 2 Status:
        Layer 2 NOT Activated
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Activated dsl 1 CCBs = 0
ISDN BRI2 interface
        dsl 2, interface ISDN Switchtype = basic-5ess
    Layer 1 Status:
        DEACTIVATED
    Layer 2 Status:
        Layer 2 NOT Activated
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Activated dsl 2 CCBs = 0
ISDN BRI3 interface
        dsl 3, interface ISDN Switchtype = basic-5ess
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 75, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Activated dsl 3 CCBs = 0
ISDN BRI4 interface
        dsl 4, interface ISDN Switchtype = basic-5ess
```

```
    Layer 1 Status:
        DEACTIVATED
    Layer 2 Status:
        Layer 2 NOT Activated
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Activated dsl 4 CCBs = 0
ISDN BRI5 interface
        dsl 5, interface ISDN Switchtype = basic-5ess
    Layer 1 Status:
        DEACTIVATED
    Layer 2 Status:
        Layer 2 NOT Activated
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Activated dsl 5 CCBs = 0
ISDN BRI6 interface
        dsl 6, interface ISDN Switchtype = basic-5ess
    Layer 1 Status:
        DEACTIVATED
    Layer 2 Status:
        Layer 2 NOT Activated
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Activated dsl 6 CCBs = 0
ISDN BRI7 interface
        dsl 7, interface ISDN Switchtype = basic-5ess
    Layer 1 Status:
        DEACTIVATED
    Layer 2 Status:
        Layer 2 NOT Activated
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Activated dsl 7 CCBs = 0
ISDN Serial0:15 interface
        dsl 8, interface ISDN Switchtype = primary-ni
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Activated dsl 8 CCBs = 0
    Total Allocated ISDN CCBs = 0
```

The following is partial sample output from the **show isdn status** command entered on a Cisco AS5300 with one active call on a PRI National ISDN switch type:

```
Router# show isdn status

%Q.931 is backhauled to BACKHAUL on DSL 0. L3 output may not apply

Global ISDN Switchtype = primary-ni
ISDN Serial0:23 interface       iua as5300-7-1
    Transport Link Status:
        ACTIVE
        dsl 0, interface ISDN Switchtype = primary-ni :Primary D channel of nfas group 1
        L2 Protocol = IUA  L3 Protocol(s) = Q.931
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:Not Applicable
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Active dsl 0 CCBs = 0
```

```
    The Free Channel Mask: 0x80FFFFFF
    Number of L2 Discards = 0, L2 Session ID = 1
ISDN Serial1:23 interface       iua as5300-7-2
    Transport Link Status:
.
.
.
```

The following example shows status of BRI interface 1/0/0:

```
Router# show isdn status bri 1/0/0

%Q.931 is backhauled to CCM MANAGER 0x0003 on DSL 8. Layer 3 output may not apply

Global ISDN Switchtype = primary-ni
ISDN BRI1/0/0 interface dsl 8, interface ISDN Switchtype = basic-net3
L2 Protocol = Q.921 0x0000  L3 Protocol(s) = CCM MANAGER 0x0003
Layer 1 Status:
        ACTIVE
Layer 2 Status:
TEI = 64, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Active dsl 8 CCBs = 0
    The Free Channel Mask:  0x80000003
    Total Allocated ISDN CCBs = 0
```

Table 62 show isdn status Field Descriptions

Field	Description
ISDN Dchannel0 interface rlm-group = 1	Status of D-channel interface and RLM group for RLM configurations and SS7 applications in integrated SLT configurations.
Transport Link Status	Displays ACTIVE or INACTIVE.
Layer 1 Status:	
ACTIVE, DEACTIVATED, ACTIVATING	Status of ISDN Layer 1.
Layer 2 Status:	
TEI = *n*, State = MULTIPLE_FRAME_ESTABLISHED	Status of ISDN Layer 2. Terminal endpoint identifier (TEI) number and multiframe structure state. **Note** The value (*n*) of the TEI will always be 0 for a D-channel interface.
SPID Status:	
TEI 65, ces = 1, state = 5(init)	Terminal endpoint identifier number and state.
spid1 configured, no LDN, spid1 sent, spid1 valid	Service profile identifier (SPID) configuration information. For example, local directory number is defined. **Note** There is no SPID report for a D-channel interface.
Endpoint ID Info: epsf = 0, usid = 3, tid = 7F	Endpoint identifier information.

Table 62 show isdn status Field Descriptions (continued)

Field	Description
Layer 3 Status:	
1 Active Layer 3 Call(s)	Number of active calls.
Activated dsl 0 CCBs =	Number of the DSL activated. Number of call control blocks in use.
CCB:callid=8003, callref=0, sapi=0, ces=1, B-chan=1	Information about the active call.
Number of active calls =	Number of active calls.
Number of available B-channels =	Number of B channels that are not being used.
Total Allocated ISDN CCBs =	Number of ISDN call control blocks that are allocated.

show isdn timers Command Examples

Cisco routers support an extensive list of ISDN switch types, which are listed in the "ISDN Service Provider BRI Switch Types" and "ISDN Service Provider PRI Switch Types" tables in the *Cisco IOS Dial Technologies Configuration Guide*.

The examples in this section show reports seen on Cisco routers connected to various ISDN switch types. Table 63 and Table 64 show typical and default values of the timers shown in the **show isdn timers** displays. The values of the timers depend on the switch type. Refer to the Q.921 specifications for detailed technical definitions of the Layer 2 timers; refer to the Q.931 specifications for detailed technical definitions of the Layer 3 timers.

The following is sample output from the **show isdn timers** command on a router connected to a PRI Lucent (AT&T) 5ESS ISDN switch type:

```
Router# show isdn timers

%Q.931 is backhauled to CCM MANAGER 0x0003 on DSL 8. Layer 3 output may not apply

ISDN Serial0:23 Timers (dsl 0) Switchtype = primary-5ess
        ISDN Layer 2 values
         K     =   7 outstanding I-frames
         N200  =   3 max number of retransmits
         T200  =   1.000 seconds
         T202  =   2.000 seconds
         T203  =  30.000 seconds
        ISDN Layer 3 values
         T303  =   4.000 seconds
         T304  =  20.000 seconds
         T305  =   4.000 seconds
         T306 =  30.000 seconds
         T307 = 180.000 seconds
         T308  =   4.000 seconds
         T309    Disabled
         T310 =  30.000 seconds
         T313 =   4.000 seconds
         T316  = 120.000 seconds
         T318  =   4.000 seconds
         T319  =   4.000 seconds
         T322  =   4.000 seconds
         T3OOS =   5.000 seconds
         TGUARD=   8.000 seconds, Expiry = REJECT_CALL
```

```
%Q.931 is backhauled to CCM MANAGER 0x0003 on DSL 8. Layer 3 output may not apply

    ISDN Serial1:23 Timers (dsl 1) Switchtype = primary-5ess
        ISDN Layer 2 values
         K     =   7 outstanding I-frames
         N200  =   3 max number of retransmits
         T200  =   1.000 seconds
         T202  =   2.000 seconds
         T203  =  30.000 seconds
        ISDN Layer 3 values
         T303  =   4.000 seconds
         T304  =  20.000 seconds
         T305  =   4.000 seconds
         T306 =  30.000 seconds
         T307 = 180.000 seconds
         T308  =   4.000 seconds
         T309    Disabled
         T310 =  30.000 seconds
         T313 =   4.000 seconds
         T316  = 120.000 seconds
         T318  =   4.000 seconds
         T319  =   4.000 seconds
         T322  =   4.000 seconds
         T3OOS =   5.000 seconds
         TGUARD=   8.000 seconds, Expiry = REJECT_CALL
        *** dsl 2 is not configured
        *** dsl 3 is not configured
        *** dsl 4 is not configured
        *** dsl 5 is not configured
        *** dsl 6 is not configured
        *** dsl 7 is not configured

%Q.931 is backhauled to CCM MANAGER 0x0003 on DSL 8. Layer 3 output may not apply

ISDN BRI0 Timers (dsl 0) Switchtype = basic-net3
        ISDN Layer 2 values
         K    = 1   outstanding I-frames
         N200 = 3   max number of retransmits
         N202 = 2   max number of retransmits of TEI ID Request
         T200 = 1   seconds
         T202 = 2   seconds
         T203 = 10  seconds
        ISDN Layer 3 values
         T303 = 4   seconds
         T305 = 30   seconds
         T308 = 4   seconds
         T310 = 40  seconds
         T313 = 4   seconds
         T316 = 0 seconds
         T318 = 4   seconds
         T319 = 4   seconds
```

The following is sample output from the **show isdn timers** command on a router connected to a BRI ETSI-compliant Euro-ISDN E-DSS1(NET3) ISDN signaling system:

```
Router# show isdn timers

%Q.931 is backhauled to CCM MANAGER 0x0003 on DSL 8. Layer 3 output may not apply

ISDN BRI0 Timers (dsl 0) Switchtype = basic-net3
        ISDN Layer 2 values
         K    = 1   outstanding I-frames
         N200 = 3   max number of retransmits
         N202 = 2   max number of retransmits of TEI ID Request
```

```
 T200 = 1   seconds
 T202 = 2   seconds
 T203 = 10  seconds
ISDN Layer 3 values
 T303 = 4   seconds
 T305 = 30   seconds
 T308 = 4   seconds
 T309 = 0  seconds
 T310 = 40  seconds
 T313 = 4   seconds
 T316 = 0 seconds
 T318 = 4   seconds
 T319 = 4   seconds
```

Table 63 show isdn timers Layer 2 Command Output

Timer Number Field	System Parameter (typical)
K = *n* outstanding I-frames	None
N200 = 3 max number of retransmits	3 seconds
T200 = 1.000 seconds	1 second
T202 = 2.000 seconds	2 seconds
T203 = 30.000 seconds	10 seconds

Table 64 show isdn timers Layer 3 Command Output

Timer Number Field	Network Side ITU Default Value	User Side ITU Default Value
T303 = 4.000 seconds	4 seconds	4 seconds
T304 = 20.000 seconds	20 seconds	30 seconds
T305 = 4.000 seconds	30 seconds	30 seconds
T306 = 30.000 seconds	30 seconds	None
T307 = 180.000 seconds	180 seconds (3 minutes)	None
T308 = 4.000 seconds	4 seconds	4 seconds
T309 Disabled	90 seconds	90 seconds
T310 = 30.000 seconds	10 seconds	30 to 120 seconds
T313 = 4.000 seconds	None	4 seconds
T316 = 120.000 seconds	120 seconds (2 minutes)	120 seconds (2 minutes)
T318 = 4.000 seconds	None	4 seconds
T319 = 4.000 seconds	None	4 seconds
T322 = 4.000 seconds	4 seconds	4 seconds

Table 64 show isdn timers Layer 3 Command Output (continued)

Timer Number Field	Network Side ITU Default Value	User Side ITU Default Value
T3OOS = 5.000 seconds	Time interval after which the software should attempt to recover from a Layer 2 failure. Default is 5 seconds	Time interval after which the software should attempt to recover from a Layer 2 failure. Default is 5 seconds
TGUARD = 8.000 seconds, Expiry = REJECT_CALL	Managed timer for authentication requests configured with the **isdn guard-timer** command. Default is 8 seconds.	Managed timer for authentication requests configured with the **isdn guard-timer** command. Default is 8 seconds.

Related Commands

Command	Description
clear ip sctp statistics	Clears statistics counts for SCTP.
isdn answer1, isdn answer2	Configures the router to verify a called-party or subaddress number in the incoming setup message for ISDN BRI calls when the number is delivered by the switch.
show ip sctp association list	Displays a list of all current SCTP associations.
show ip sctp association parameters	Displays the parameters configured for the association defined by the association ID.
show ip sctp association statistics	Displays the current statistics for the association defined by the association ID.
show ip sctp errors	Displays error counts logged by SCTP.
show ip sctp instances	Displays the currently defined SCTP instances.
show ip sctp statistics	Displays the overall statistics counts for SCTP.
show iua as	Displays information about the current condition of an AS.
show iua asp	Displays information about the current condition of an ASP.

show isdn nfas group

To display all the members of a specified Non-Facility Associated Signaling (NFAS) group or all NFAS groups, use the **show isdn nfas group** command in privileged EXEC mode.

show isdn nfas group [*id-number*]

Syntax Description

id-number	(Optional) Identifier number in the range from 1 to 24 of a specific NFAS group.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3	This command was introduced.
12.3	This command was enhanced to display the message "%Q.931 is backhauled to BACKHAUL on DSL 0. Layer 3 output may not apply".

Usage Guidelines

Native ISDN stacks do not know Layer 3 details because Layer 3 is backhauled to an external application. So informational message "%Q.931 is backhauled to IUA BACKHAUL on DSL 3. Layer 3 output may not apply" is displayed for those users that expect ISDN commands to show the required output.

Examples

The following is sample output from the **show isdn nfas group** command:

```
Router# show isdn nfas group 1

%Q.931 is backhauled to IUA BACKHAUL on DSL 3. L3 output may not apply

ISDN NFAS GROUP 1 ENTRIES:

The primary D is Serial1/0:23.
The backup D is Serial1/1:23.
The NFAS member is Serial2/0:23.

There are 3 total nfas members.
There are 93 total available B channels.
The primary D-channel is DSL 0 in state INITIALIZED.
The backup D-channel is DSL 1 in state INITIALIZED.
The current active layer 2 DSL is 1.
```

The following three examples show the D-channel state changes when rollover occurs from the primary NFAS D channel to the backup D channel. The first example shows the output with the primary D channel in service and the backup D channel in standby.

```
Router# show isdn nfas group 0

%Q.931 is backhauled to IUA BACKHAUL on DSL 3. L3 output may not apply

ISDN NFAS GROUP 0 ENTRIES:
```

```
The primary D is Serial1/0:23.
The backup D is Serial1/1:23.
The NFAS member is Serial2/0:23.

There are 3 total nfas members.
There are 70 total available B channels.
The primary D-channel is DSL 0 in state IN SERVICE.
The backup D-channel is DSL 1 in state STANDBY.
The current active layer 2 DSL is 0.
```

The following example shows the output during rollover. The configured primary D channel is in maintenance busy state and the backup D channel is waiting.

```
Router# show isdn nfas group 0

%Q.931 is backhauled to IUA BACKHAUL on DSL 3. L3 output may not apply

ISDN NFAS GROUP 0 ENTRIES:
The primary D is Serial1/0:23.
The backup D is Serial1/1:23.
The NFAS member is Serial2/0:23.

There are 3 total nfas members.
There are 70 total available B channels.
The primary D-channel is DSL 0 in state MAINTENANCE BUSY.
The backup D-channel is DSL 1 in state WAIT.
The current active layer 2 DSL is 1.
```

The following example shows the output when rollover is complete. The configured primary D channel is now in standby and the backup D channel is in service.

```
Router# show isdn nfas group 0

%Q.931 is backhauled to IUA BACKHAUL on DSL 3. L3 output may not apply

ISDN NFAS GROUP 0 ENTRIES:

The primary D is Serial1/0:23.
The backup D is Serial1/1:23.
The NFAS member is Serial2/0:23.

There are 3 total nfas members.
There are 70 total available B channels.
The primary D-channel is DSL 0 in state STANDBY.
The backup D-channel is DSL 1 in state IN SERVICE.
The current active layer 2 DSL is 1.
```

Table 65 describes the significant fields shown in the display.

Table 65 show isdn nfas group Field Descriptions

Field	Description
The primary D is Serial1/0:23.	Identifies the primary D channel.
The backup D is Serial1/1:23.	Identifies the backup D channel.
The NFAS member is Serial2/0:23.	Identifies the NFAS group.
There are 3 total nfas members.	Number of member interfaces in the group.
There are 70 total available B channels.	Number of B channels in this NFAS group.

Table 65 show isdn nfas group Field Descriptions (continued)

Field	Description
The primary D-channel is DSL 0 in state STANDBY.	Service state of the NFAS primary D channel; this D channel is in standby mode.
The backup D-channel is DSL 1 in state IN SERVICE.	Service state of the NFAS backup D channel; this D channel is in service. The states are IN SERVICE, STANDBY, OUT OF SERVICE, MAINTENANCE, WAIT, INITIALIZED, and BUSY.
The current active layer 2 DSL is 1.	Digital subscriber loop (DSL) identifier assigned by the service provider. If both D channels are out of service, the value displayed in this line is 1.

Related Commands

Command	Description
show isdn	Displays the information about memory, Layer 2 and Layer 3 timers, and the status of PRI channels.

show line async-queue

To display the status of connections currently waiting in the queue, use the **show line async-queue command in EXEC mode**.

show line async-queue [*rotary-group*]

Syntax Description

rotary-group	(Optional) Specifies a rotary group.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

Use this command to display all rotary line queues.

Examples

The following example shows all lines that are currently queued:

```
Router# show line async-queue

Showing async-queue for ALL rotary groups

Queue for Rotary Group 1:
    Pos    Waiting TTY    Dest Port    Source Host   Waiting Time
      1          tty69         7001       10.2.1.3       00:00:09
      2          tty70         7001       10.2.1.3       00:00:06


Queue for Rotary Group 2:
    Pos    Waiting TTY    Dest Port    Source Host   Waiting Time
      1          tty66         7002       10.2.1.3       00:00:36
      2          tty67         7002       10.2.1.3       00:00:29
      3          tty68         7002       10.2.1.3       00:00:26


Lines which have queuing enabled [tty (group)]:
tty33 (1)  tty34 (1)  tty35 (1)  tty36 (1)  tty37 (2)
tty38 (2)  tty39 (2)  tty40 (2)  tty41 (3)  tty42 (3)
tty43 (3)  tty44 (3)  tty45 (4)  tty46 (4)  tty47 (4)
Router#
```

Note that Waiting TTY may also be displayed as Waiting VTY and is equivalent.

show modem

To display a high-level performance report for all the modems or a single modem inside Cisco access servers, use the **show modem** command in EXEC mode.

show modem [*slot*/*port* | **group** *number*]

Syntax Description

slot/*port*	(Optional) Location of a slot and modem port. Remember to include the forward slash (/) when entering this variable.
group *number*	(Optional) Assigns the group to which a specified modem belongs. The group number range is from 1 to 200.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.1(5)T	This command was enhanced to display information about modems on the Cisco 3600 series routers that support the V.110 standard.
12.2(11)YT	This command was enhanced to display information about digital modems on the Cisco 3600 and 3700 series routers that support the V.92 and V.44 standards.
12.2(15)T	The Cisco IOS Release 12.2(11)YT enhancements were integrated into Cisco IOS Release 12.2(15)T.

Examples

The following is sample output from the **show modem** command for two V.34 modem cards inserted in a Cisco 3600 router:

```
Router# show modem

                Inc calls     Out calls     Busied   Failed  No       Succ
  Mdm  Usage    Succ   Fail   Succ   Fail   Out      Dial    Answer   Pct.
* 1/0    17%     74      3      0      0      0        0       0      96%
* 1/1    15%     80      4      0      0      0        1       1      95%
* 1/2    15%     82      0      0      0      0        0       0     100%
  1/3    21%     62      1      0      0      0        0       0      98%
  1/4    21%     49      5      0      0      0        0       0      90%
* 1/5    18%     65      3      0      0      0        0       0      95%
* 1/6    19%     58      2      0      0      0        0       0      96%
* 1/7    17%     67      5      0      0      0        1       1      93%
* 1/8    20%     68      3      0      0      0        0       0      95%
  1/9    16%     67      2      0      0      0        0       0      97%
  1/10   18%     56      2      0      0      0        1       1      96%
* 1/11   15%     76      3      0      0      0        0       0      96%
* 1/12   16%     62      1      0      0      0        0       0      98%
  1/13   17%     51      4      0      0      0        0       0      92%
  1/14   16%     51      5      0      0      0        0       0      91%
  1/15   17%     65      0      0      0      0        0       0     100%
  1/16   15%     73      3      0      0      0        0       0      96%
  1/17   17%     67      2      0      0      0        0       0      97%
  1/18   17%     61      2      0      0      0        0       0      96%
```

```
* 1/19   17%      74      2       0       0       0       0       0      97%
  1/20   16%      65      1       0       0       0       0       0      98%
* 1/21   16%      58      3       0       0       0       0       0      95%
* 1/22   18%      56      4       0       0       0       0       0      93%
* 1/23   20%      60      4       0       0       0       0       0      93%
```

The following is sample output from the **show modem** command for two V.110 modem cards inserted in a Cisco 3600 router:

```
Router# show modem

               Inc calls      Out calls   Busied   Failed  No       Succ
  Mdm  Usage    Succ   Fail    Succ   Fail   Out      Dial    Answer   Pct.
  0/0     0%       -      -       -      -       0       0       0      -
  0/1     0%       -      -       -      -       0       0       0      -
  0/2     0%       -      -       -      -       0       0       0      -
  0/3     0%       -      -       -      -       0       0       0      -
  0/4     0%       -      -       -      -       0       0       0      -
  0/5     0%       -      -       -      -       0       0       0      -
  0/6     0%       -      -       -      -       0       0       0      -
  0/7     0%       -      -       -      -       0       0       0      -
  0/8     0%       -      -       -      -       0       0       0      -
  0/9     0%       -      -       -      -       0       0       0      -
  0/10    0%       -      -       -      -       0       0       0      -
  0/11    0%       -      -       -      -       0       0       0      -
  1/0     0%       -      -       -      -       0       0       0      -
  1/1     0%       -      -       -      -       0       0       0      -
  1/2     0%       -      -       -      -       0       0       0      -
  1/3     0%       -      -       -      -       0       0       0      -
  1/4     0%       -      -       -      -       0       0       0      -
  1/5     0%       -      -       -      -       0       0       0      -
  1/6     0%       -      -       -      -       0       0       0      -
  1/7     0%       -      -       -      -       0       0       0      -
  1/8     0%       -      -       -      -       0       0       0      -
  1/9     0%       -      -       -      -       0       0       0      -
```

The following is sample output from the **show modem** command for a Cisco 3600 series router:

```
Router# show modem

  Codes:
  * - Modem has an active call
  R - Modem is being Reset
  D - Download in progress
  B - Modem is marked bad and cannot be used for taking calls
  b - Modem is either busied out or shut-down

       Avg Hold     Inc calls     Out calls    Busied   Failed    No      Succ
  Mdm     Time      Succ   Fail   Succ   Fail    Out      Dial   Answer   Pct.
* 0/0   00:21:01     132      0      0      0       0       0       0    100%
* 0/1      2d01h       1      0      0      0       0       0       0    100%
  0/2   00:00:34     130      0      0      0       0       0       0    100%
* 0/3   00:21:53     126      1      0      0       0       0       0     99%
* 0/4      2d01h       1      0      0      0       0       0       0    100%
  0/5   00:00:33     131      0      0      0       0       0       0    100%
* 0/6   00:21:12     131      0      0      0       0       0       0    100%
  0/7   00:00:34     131      0      0      0       0       0       0    100%
b 0/8   00:00:00       0      0      0      0       0       0       0      0%
b 0/9   00:00:00       0      0      0      0       0       0       0      0%
!.
!.
!.
b 0/29  00:00:00       0      0      0      0       0       0       0      0%
Total:  00:18:25     783      1      0      0       0       0       0     99%
```

Table 66 describes the significant fields shown in the previous displays of the **show modem** command.

Table 66 show modem Field Descriptions

Field	Description
Mdm	Slot and modem port number. Also, the following modem states can appear to the left of a slot/modem port number: • b—Modem was removed from service with the **modem shutdown** command or the **modem busyout** command. • B—Modem is suspected to be inoperable or bad. No calls can be made with this modem. The letter B can also mean that a modem firmware download failed for the specified modem. In this case, try unmarking the modem as bad with the **no modem bad** command and upgrading the modem firmware again. • d—The RAM-based Digital Signal Processor (DSP) code, which supports K56flex, is not configured. The modem will revert to transmitting at 33.6 kbps. • D—Modem is downloading firmware. • p—Firmware download is pending, typically because one or more modems is active. • R—Modem is held and isolated in a suspended state by the **modem hold-reset** command. • T—Modem is conducting a back-to-back test with another modem. • *—Modem is connected or dialing.
Usage	Percentage of the total system uptime that all modems are in use.
Inc calls	Number of incoming calls that successfully and unsuccessfully connected to a modem.
Out calls	Number of outgoing calls that successfully and unsuccessfully dialed out from an available modem.
Busied Out	Number of modems that have been manually removed from service.
Failed Dial	Number of modems that attempted to dial in to the network but failed to make a connection.
No Answer	Number of modems that detected an incoming ring but failed to answer the call.
Succ Pct.	Successful connection percentage of total available modems.

The following example shows the statistics and current configurations for the manageable modem 2/10, which exists on a V.34 modem card in a Cisco 3600 router. A dash (-) indicates a field that is not available on basic modems. An x indicates a field that is available and active on manageable modems. See Table 67 for a description of the fields displayed by the **show modem** command with slot and port designators.

```
Router# show modem 2/10

Mdm  Typ     Status      Tx/Rx     G  Duration  TX  RX  RTS  CTS  DSR  DCD  DTR
2/10 V34     Idle    33600/33600  1  00:00:00           x    x    x         x

Modem 2/10, Microcom MNP10 V34 Modem (Select), Async35, TTY35
Firmware (Boot) Rev: 2.1(9) (1.0(5))
Modem config: Incoming and Outgoing
Protocol: reliable/MNP, Compression: V42bis
Management port config: Status polling and AT session
```

```
Management port status: Status polling and AT session
TX signals: 0 dBm, RX signals: 0 dBm

  Last clearing of "show modem" counters never
    0 incoming completes, 0 incoming failures
    0 outgoing completes, 0 outgoing failures
    0 failed dial attempts, 0 ring no answers, 0 busied outs
    0 no dial tones, 0 dial timeouts, 0 watchdog timeouts
    0 no carriers, 0 link failures, 0 resets 0 recover oob
    0 protocol timeouts, 0 protocol errors, 0 lost events

Connection Speeds         75      300      600     1200     2400     4800
# of connections           0        0        0        0        0        0
Connection Speeds       7200     9600    12000    14400    16800    19200
# of connections           0        0        0        0        0        0
Connection Speeds      21600    24000    26400    28800    31200    33600
# of connections           0        0        0        0        0        1
```

The following is sample output for a basic V.34 modem module. Notice that unavailable fields are marked with dashes (-):

```
Router# show modem 1/1

Mdm  Typ  Status   Tx/Rx       G  Duration  TX  RX  RTS  CTS  DSR  DCD  DTR
1/1   -   Idle    19200/19200  0  00:01:05   -   -   -    -    -    -    -

Modem 1/1, C3600 Non-Manageable Modem
Firmware (Boot) Rev: Unknown
Modem config: Unknown
Management config: Not Manageable Modem

Last clearing of "show modem" counters never
- incoming completes, - incoming failures
- outgoing completes, - outgoing failures,
0 failed dial attempts, 0 ring no answers, 0 busied outs
0 no dial tones, 0 dial timeouts, 0 watchdog timeouts
- no carriers, - link failures, 0 resets
- protocol timeouts, - protocol errors, - lost events

Connection Speeds         75      300      600     1200     2400     4800
# of connections           0        0        0        0        0        0
Connection Speeds       7200     9600    12000    14400    16800    19200
# of connections           0        0        0        0        0        0
Connection Speeds      21600    24000    26400    28800    31200    33600
# of connections           0        0        0        0        0        0
```

The following is sample output from the **show modem** *slot*/*port* command for V.110 modem cards:

```
Router# show modem 0/1

Mdm  Typ    Status     Tx/Rx     G  Duration  TX  RX  RTS  CTS  DSR  DCD  DTR
0/1         Idle        -/-      1  00:00:00   -   -   -    -    -    -    -

Modem 0/1, V.110 Terminal Adaptor (Unmanaged), Async2, TTY2
Firmware (Boot) Rev: Unmanaged (Unmanaged)
Modem config: Incoming and Outgoing
Management config: Unmanaged

  Last clearing of "show modem" counters never
    - incoming completes, - incoming failures
    - outgoing completes, - outgoing failures
```

```
    0 failed dial attempts, 0 ring no answers, 0 busied outs
    - no dial tones, - dial timeouts, 0 watchdog timeouts
    - no carriers, - link failures, 0 resets, - recover oob
    - protocol timeouts, - protocol errors, - lost events

Connection Speeds          75      300      600     1200     2400     4800
# of connections           -        -        -        -        -        -
Connection Speeds        7200     9600    12000    14400    16800    19200
# of connections           -        -        -        -        -        -
Connection Speeds       21600    24000    26400    28800    31200    32000
# of connections           -        -        -        -        -        -
Connection Speeds       33600    34000    36000    38000    40000    42000
# of connections           -        -        -        -        -        -
Connection Speeds       44000    46000    48000    50000    52000    54000
# of connections           -        -        -        -        -        -
Connection Speeds       56000
# of connections           -
```

The type of display output generated from the **show modem** *slot*/*port* command depends on the version of Cisco IOS software running on the router or access server. For example, the following shows example output for a 56K modem card, which carries digital modems that transmit at 56 kbps. (In truth, 56K modems do not modulate or demodulate data. A pure digital-to-digital connection is made.) See Table 67 for a description of the fields displayed by this modem card.

```
Router# show modem 0/0

Mdm  Typ     Status      Tx/Rx     G  Duration  TX  RX  RTS  CTS  DSR  DCD  DTR
0/0          Idle         0/0      0  00:00:00           x    x    x         x

Modem 0/0, Microcom MNP10 K56 Modem (Select), TTY1
Firmware (Boot) Rev: 3.1(16) (3.0(4))
DSP Controller (SPX) Rev: 1.1(0) (1.1(0))
Modem config: Incoming and Outgoing
Protocol: Normal, Compression: None
Management port config: Status polling and AT session
Management port status: Status polling and AT session
TX signals: 0 dBm, RX signals: 0 dBm

  Last clearing of "show modem" counters never
    0 incoming completes, 0 incoming failures
    0 outgoing completes, 0 outgoing failures
    0 failed dial attempts, 0 ring no answers, 0 busied outs
    0 no dial tones, 0 dial timeouts, 0 watchdog timeouts
    0 no carriers, 0 link failures, 1 resets 0 recover oob
    0 protocol timeouts, 0 protocol errors, 0 lost events

Transmit Speed Counters:

Connection Speeds          75      300      600     1200     2400     4800
# of connections           0        0        0        0        0        0
Connection Speeds        7200     9600    12000    14400    16800    19200
# of connections           0        0        0        0        0        0
Connection Speeds       21600    24000    26400    28800    31200    32000
# of connections           0        0        0        0        0        0
Connection Speeds       33600    34000    36000    38000    40000    42000
# of connections           0        0        0        0        0        0
Connection Speeds       44000    46000    48000    50000    52000    54000
# of connections           0        0        0        0        0        0
Connection Speeds       56000
# of connections           0
```

```
Receive Speed Counters:

Connection Speeds         75      300      600     1200     2400     4800
# of connections           0        0        0        0        0        0
Connection Speeds       7200     9600    12000    14400    16800    19200
# of connections           0        0        0        0        0        0
Connection Speeds      21600    24000    26400    28800    31200    32000
# of connections           0        0        0        0        0        0
Connection Speeds      33600    34000    36000    38000    40000    42000
# of connections           0        0        0        0        0        0
Connection Speeds      44000    46000    48000    50000    52000    54000
# of connections           0        0        0        0        0        0
Connection Speeds      56000
# of connections           0
```

The following is sample output from the **show modem** *slot*/*port* command for digital modems on a Cisco 3600 series router that supports the V.92 and V.44 modem standards:

```
Router# show modem 3/0

Mdm  Typ    Status     Tx/Rx     G  Duration  TX  RX  RTS  CTS  DSR  DCD  DTR
3/0  V90/92 Idle    46666/31200  1  00:01:30   -   -             x

Modem 3/0 [line 97], Async97, TTY97
MICA-6DM Firmware: CP ver 2910 - 7/13/2001, SP ver 2910 - 7/13/2001.
Modem config: Incoming and Outgoing
Protocol: LAPM, Compression: V44

  Last clearing of "show modem" counters: never
    1 incoming completes, 1 incoming failures
    0 outgoing completes, 0 outgoing failures
    0 failed dial attempts, 0 ring no answers, 0 busied outs
    0 no dial tones, 0 dial timeouts, 0 watchdog timeouts
    0 no carriers, 0 link failures, 0 resets, 0 recover oob
    0 protocol timeouts, 0 protocol errors, 0 lost events
    0 TDM errors, 0 speed shifts (up/dn - 0/0), 0 retrains (hi/lo - 0/0)
    0 MOH

Modulation type       V90/92
# of connections           1

Protocol type           LAPM
# of connections           1

Transmit Speed Counters:

Connection Speeds      46667
# of connections           1

Receive Speed Counters:

Connection Speeds      31200
# of connections           1
```

Table 67 describes the fields in the previous four displays, which were created using the **show modem** *slot*/*port* command. This table applies to all modem module types.

Table 67 show modem slot/port Field Descriptions

Field	Description
Mdm	Slot and modem number.
Typ	Modulation type, which can be any of the following values: Bel103, Bel212, V21, V22, V22bis, V23, V32, V32bis, VFC, V34, V17, V27, V33, K56Flx, and V90/92.
Status	Current status of the modem. Possible values are as follows: • Conn—Modem is connected to a remote host. • B—Inoperable state, which is configured by the **modem bad** command. • B*—Inoperable state, which is configured by the **modem startup-test** command during initial power-up testing. • b—Modem is busied out. This can be manually configured by the **modem busyout** line configuration command. • Reset—Modem is in reset mode. • D/L—Modem is downloading firmware. • Bad FW—Downloaded modem firmware is not operational. • Busy—Modem is out of service and not available for calls. • Idle—Modem is ready for incoming and outgoing calls.
Tx/Rx	Transmission and receiving speed for the most recently connected call.
G	Modem group number assigned to the modem. The group number 0 means the modem is not part of any group.
Duration	Time duration (in hours: minutes: seconds) of the current or the last call.
Modem functions	The following modem functions are displayed on manageable modems. A field that is available and turned on is marked with an x. An unavailable field is marked with a dash (-). • TX—Transmit Data. The DTE device transmits data to the DCE device. • RX—Receive Data. The DCE device receives data from the DTE device. • RTS—Request To Send. The DTE device signals to the DCE device that the DTE device accepts data into its buffers. • CTS—Clear To Send. The DCE device signals to the DTE device that the DCE device accepts data into its buffers. • DSR—Data Set Ready. The modem is ready to start communication. • DCD—Data Carrier Detect. The DCE device indicates to the DTE device that a call is present and established with a remote modem. Dropping the DCD function terminates the session. • DTR—Data Terminal Ready. The DTE device indicates to the DCE device that it accepts calls.
Firmware	Installed modem firmware.
Modem config	Current modem configuration, which includes the fields Incoming, Outgoing, Incoming and Outgoing, Unknown, Protocol, and Compression.

Table 67 show modem slot/port Field Descriptions (continued)

Field	Description
Protocol	Protocol the modem is running such as Normal, Direct, reliable/Microcom Network Protocol (MNP)4, and reliable/LAPM (Link Access Procedure for Modems).
Compression	Compression algorithm running on the modem, such as None, V42*bis*, V.44, and MNP5.
Management config	Indicates if the modem is configured for out-of-band feature polling.
TX signals	Transmit signal levels. For modulations that do not support signal to noise calculations, the ratio is 0.
RX signals	Transmit signal levels.

Table 67 show modem slot/port Field Descriptions (continued)

Field	Description
Last clearing of "show modem" counters	Last time the modem's counters were cleared using the **clear modem counters** command. A summary of modem events also appears. • Incoming completes and failures—Total number of incoming connection requests that the modem answered and successfully or unsuccessfully connected with the remote DCE device. • Outgoing completes and failures—Total number of outgoing connection requests that the modem dialed and successfully or unsuccessfully connected with the remote DCE device. • Failed dial attempts—Number of times the modem attempted to dial out but the call failed to leave the modem. • Ring no answers—Number of times the integrated modem detected ringing but did not answer the incoming call. • Busied outs—Number of times the integrated modem was intentionally taken out of service (for example, the **modem busyout** command was enabled on the modem). • No dial tones—Number of times the dial-out attempt failed because the modem failed to detect a dial tone. • Dial timeouts—Number of times the modem has timed out while attempting to dial. • Watchdog timeouts—Number of times the modem internal watchdog timer has expired. • No carriers—Number of times the modem disconnected because no carrier was present. • Link failures—Number of times the modem has detected a link failure. • Resets—Number of times the modem has been reset. • Recover oob—Number of times the out-of-band feature has been cleared and reinitialized. • Protocol timeouts and errors—Number of times the modem protocol failed to make a call connection. • Lost events—Number of incomplete modem events performed by the modem. • MOH—Indicates V.92 Modem on Hold (MOH), which allows suspending a modem session to answer an incoming voice call or to place an outgoing call while engaged in a modem session.
Modulation type	Modulation type, which can be any of the following values: Bel103, Bel212, V21, V22, V22bis, V23, V32, V32bis, VFC, V34, V17, V27, V33, K56Flx, and V90/92.
Protocol type	Protocol the modem is running such as Normal, Direct, reliable/MNP4, and reliable/LAPM.
Transmit Speed Counters:	List of connection speeds that were sent by the modem.

Table 67 show modem slot/port Field Descriptions (continued)

Field	Description
Receive Speed Counters:	List of connection speeds that were received by the modem.
Connection Speeds # of connections	A complete summary of possible connection speeds and the actual number of connections that occurred at those speeds. Depending on which modem port module and version of software you are running, possible connection speeds range from 75 to 56000 bits per second (bps). The number of successful connections is displayed directly beneath the connection speed identifier. For example, the following output shows that three connections were made at 56 kbps: Connection Speeds 56000 # of connections 3

The following example shows the output for modem group 1, which comprises modem 1/0 through modem 1/23. The report is self explanatory.

```
Router# show modem group 1

              Incoming calls       Outgoing calls    Busied   Failed  No    Succ
Grp  Usage  Succ   Fail  Avail   Succ   Fail  Avail  Out      Dial    Ans   Pct.
1     0%     0      0     24      0      0     24       0        0    0     0%

Modem Group 1: 1/0, 1/1, 1/2, 1/3, 1/4, 1/5, 1/6, 1/7, 1/8, 1/9, 1/10, 1/11, 1/12, 1/13,
1/14, 1/15, 1/16, 1/17, 1/18, 1/19, 1/20, 1/21, 1/22, 1/23
```

Related Commands

Command	Description
show modem version	Displays version information about the modem firmware, controller and DSP code (for 56-kbps modems only), and boot code.

show modem at-mode

To display a list of the manageable Microcom modems that have open AT sessions and a list of users logged in to those sessions, use the **show modem at-mode** command in EXEC mode.

show modem at-mode

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Examples

The report from the show modem at-mode command is self-explanatory. The following output shows that modem 1/1 has one open AT directly connected session:

```
Router# show modem at-mode

Active AT-MODE management sessions:
Modem    User's Terminal
1/1 0    cty 0
```

show modem bundled-firmware

To display a a list of available modem firmware running in a Cisco AS5800 access server, use the **show modem bundled-firmware** command in EXEC mode.

show modem bundled-firmware

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3(5)AA	This command was introduced.

Usage Guidelines

Use this command instead of the the **show modem mapping** command on the Cisco AS5800 access servers. The **show modem bundled-firmware** command is useful for displaying a list of available modem firmware running in the access server.

Examples

The report from the **show modem bundled-firmware** command is self-explanatory. The following sample output shows firmware images by slot number:

```
Router# show modem bundled-firmware

List of bundled modem firmware images by slot
  Slot 4
    2.6.2.0
  Slot 5
    2.6.2.0
  Slot 6
    2.6.2.0
  Slot 7
    2.6.2.0
  Slot 8
    2.6.2.0
```

Related Commands

Command	Description
copy	Copies any file from a source to a destination, including a source or destination URL for a TFTP network server, or for Flash memory.
copy modem	Copies modem firmware to integrated modems in an access server.
show modem mapping	Displays a snapshot of all the firmware versions running on all the modems in access servers besides the AS5800.

show modem call-stats

To display the local disconnect reasons for all modems inside an access server or router, use the **show modem call-stats** command in EXEC mode.

show modem call-stats [*slot*]

Syntax Description

slot	(Optional) Slot number, which limits the display output to a particular range of modems in the system.

Command Modes

EXEC

Command History

Release	Modification
11.3	This command was introduced.
12.2(11)YT	This command was enhanced to display information about digital modems on the Cisco 3600 and 3700 series routers that support the V.92 and V.44 standards.
12.2(15)T	This enhanced command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

Use this command to find out why a modem ended its connection or why a modem is not operating at peak performance.

Local disconnect reasons for a particular modem are listed across the top of the screen display. For example, see lostCarr, dtrDrop, rmtLink, wdogTimr, compress, retrain, inacTout, and linkFail in the following output:

```
Router# show modem call-stats

  dial-in/dial-out call statistics

       lostCarr  dtrDrop  rmtLink wdogTimr compress  retrain inacTout linkFail
  Mdm
* 0/0
* 0/1
```

In the body of the screen display, the number of times an error occurred on a specific modem is displayed (see the # column). The % column shows the total running percent that a modem was logged for the specified disconnect reason with respect to the entire modem pool. For example, out of all the times that the lostCarr error occurred on all the modems in the system, the lostCarr error occurred 2 percent of the time on modem 0/0.

```
Router# show modem call-stats

  dial-in/dial-out call statistics

       lostCarr  dtrDrop  rmtLink wdogTimr compress  retrain inacTout linkFail
  Mdm     #   %    #   %    #   %    #   %    #   %    #   %    #   %    #   %
* 0/0     6   2    2   3    1   0    0   0    0   0    0   0    0   0    0   0
* 0/1     5   2    2   3    2   1    0   0    0   0    0   0    0   0    0   0
```

Bad or malfunctioning modems are detected by an unusually high number of disconnect counters for a particular disconnect reason. For example, if modem 1/0 had a high number of compression errors compared to the remaining modems in system, modem 1/0 would probably be bad or inoperable.

To reset the counters displayed by the **show modem call-stats** command, use the **clear modem counters** command.

Note Remote disconnect reasons are not described by this command.

Examples

The following example shows call statistics for the **show modem call-stats** command. Because of the screen size limitation of most terminal screen displays, all the possible disconnect reasons cannot be displayed at the same time. Only the top eight most frequently experienced disconnect reasons are displayed.

```
Router# show modem call-stats

dial-in/dial-out call statistics

         lostCarr  dtrDrop  rmtLink wdogTimr compress  retrain inacTout linkFail
   Mdm     #   %    #   %    #   %    #   %    #   %    #   %    #   %    #   %
* 0/0       6   2    2   3    1   0    0   0    0   0    0   0    0   0    0   0
* 0/1       5   2    2   3    2   1    0   0    0   0    0   0    0   0    0   0
  0/2       5   2    2   3    4   3    0   0    0   0    0   0    0   0    0   0
* 0/3       5   2    2   3    2   1    0   0    0   0    0   0    0   0    0   0
* 0/4       5   2    1   1    1   0    0   0    0   0    0   0    0   0    0   0
* 0/5       5   2    2   3    2   1    0   0    0   0    0   0    0   0    0   0
* 0/6       4   1    2   3    2   1    0   0    0   0    0   0    0   0    0   0
* 0/7       4   1    2   3    4   3    0   0    0   0    0   0    0   0    0   0
* 0/8       6   2    1   1    3   2    0   0    0   0    0   0    0   0    0   0
* 0/9       5   2    1   1    1   0    0   0    0   0    0   0    0   0    0   0
* 0/10      5   2    1   1    2   1    0   0    0   0    0   0    0   0    0   0
* 0/11      5   2    1   1    2   1    0   0    0   0    0   0    0   0    0   0
  0/12      5   2    2   3    2   1    0   0    0   0    0   0    0   0    0   0
* 0/13      5   2    1   1    1   0    0   0    0   0    0   0    0   0    0   0
* 0/14      5   2    1   1    1   0    0   0    0   0    0   0    0   0    0   0
* 0/15      5   2    1   1    1   0    0   0    0   0    0   0    0   0    0   0
* 0/16      5   2    1   1    1   0    0   0    0   0    0   0    0   0    0   0
* 0/17      5   2    1   1    2   1    0   0    0   0    0   0    0   0    0   0
* 0/18      5   2    1   1    2   1    0   0    0   0    0   0    0   0    0   0
* 0/19      5   2    1   1    3   2    0   0    0   0    0   0    0   0    0   0
* 0/20      5   2    1   1    1   0    0   0    0   0    0   0    0   0    0   0
* 0/21      5   2    1   1    1   0    0   0    0   0    0   0    0   0    0   0
* 0/22      5   2    1   1   11  10    0   0    0   0    0   0    0   0    0   0
* 0/23      5   2    1   1    2   1    0   0    0   0    0   0    0   0    0   0
* 2/0       4   1    2   3    2   1    0   0    0   0    0   0    0   0    0   0
* 2/1       5   2    1   1    2   1    0   0    0   0    0   0    0   0    0   0
* 2/2       5   2    2   3    0   0    0   0    0   0    0   0    0   0    0   0
* 2/3       5   2    1   1    2   1    0   0    0   0    0   0    0   0    0   0
* 2/4       5   2    1   1    2   1    0   0    0   0    0   0    0   0    0   0
* 2/5       5   2    1   1    2   1    0   0    0   0    0   0    0   0    0   0
* 2/6       4   1    1   1    1   0    0   0    0   0    0   0    0   0    0   0
* 2/7       5   2    1   1    1   0    0   0    0   0    0   0    0   0    0   0
* 2/8       5   2    1   1    1   0    0   0    0   0    0   0    0   0    0   0
* 2/9       4   1    1   1    2   1    0   0    0   0    0   0    0   0    0   0
* 2/10      5   2    1   1    0   0    0   0    0   0    0   0    0   0    0   0
* 2/11      5   2    1   1    5   4    0   0    0   0    0   0    0   0    0   0
* 2/12      5   2    1   1    2   1    0   0    0   0    0   0    0   0    0   0
* 2/13      5   2    1   1    1   0    0   0    0   0    0   0    0   0    0   0
* 2/14      5   2    1   1    2   1    0   0    0   0    0   0    0   0    0   0
```

```
* 2/15     4    1     1    1     3    2     0    0     0    0     0    0     0    0     0    0
* 2/16     4    1     1    1     3    2     0    0     0    0     0    0     0    0     0    0
* 2/17     5    2     2    3     9    8     0    0     0    0     0    0     0    0     0    0
* 2/18     4    1     1    1     1    0     0    0     0    0     0    0     0    0     0    0
* 2/19     3    1     1    1     2    1     0    0     0    0     0    0     0    0     0    0
* 2/20     7    3     1    1     8    7     0    0     0    0     0    0     0    0     0    0
* 2/21     5    2     1    1     1    0     0    0     0    0     0    0     0    0     0    0
* 2/22     4    1     1    1     2    1     0    0     0    0     0    0     0    0     0    0
* 2/23     5    2     1    1     2    1     0    0     0    0     0    0     0    0     0    0
 Total   233        59       110         0         0         0         0         0
```

```
  dial-out call statistics

           noCarr   noDitone  busy      abort    dialStrg autoLgon dialTout rmtHgup
  Mdm      #    %    #    %    #    %    #    %    #    %    #    %    #    %    #    %
* 0/0      1    1    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 0/1      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
  0/2      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 0/3      1    1    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 0/4      1    1    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 0/5      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 0/6      1    1    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 0/7      5    5    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 0/8      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 0/9      1    1    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 0/10     0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 0/11     5    5    0    0    0    0    0    0    0    0    0    0    0    0    0    0
  0/12     0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 0/13     0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 0/14     1    1    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 0/15     1    1    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 0/16     2    2    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 0/17     4    4    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 0/18     5    5    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 0/19     1    1    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 0/20     0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 0/21     0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 0/22     5    5    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 0/23     1    1    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 2/0      2    2    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 2/1      3    3    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 2/2      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 2/3      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 2/4      0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 2/5      1    1    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 2/6      1    1    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 2/7      4    4    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 2/8      7    8    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 2/9      4    1    1    1    2    1    0    0    0    0    0    0    0    0    0    0
* 2/10     1    1    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 2/11     1    1    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 2/12     1    1    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 2/13     1    1    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 2/14     4    4    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 2/15     1    1    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 2/16     1    1    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 2/17     5    5    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 2/18     5    5    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 2/19     3    3    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 2/20     0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 2/21     4    4    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 2/22     2    2    0    0    0    0    0    0    0    0    0    0    0    0    0    0
* 2/23     0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
 Total    84        0         0         0         0         0         0         0
```

The following is sample output from the **show modem call-stats** command for digital modems on a Cisco 3600 series router that supports the V.92 modem standard (see the "mohTrmnt" column for data about the V.92 Modem on Hold [MOH] function):

```
Router# show modem call-stats

  Codes:
  * - Modem has an active call
  R - Modem is being Reset
  D - Download in progress
  B - Modem is marked bad and cannot be used for taking calls
  b - Modem is either busied out or shut-down

  dial-in/dial-out call statistics

       mohTrmnt wdogTimr compress  retrain inacTout linkFail moduFail mnpProto
  Mdm     #   %    #   %    #   %    #   %    #   %    #   %    #   %    #   %
  3/0     1 100    0   0    0   0    0   0    0   0    0   0    0   0    0   0
* 3/1     0   0    0   0    0   0    0   0    0   0    0   0    0   0    0   0
  3/2     0   0    0   0    0   0    0   0    0   0    0   0    0   0    0   0
  3/3     0   0    0   0    0   0    0   0    0   0    0   0    0   0    0   0
  3/4     0   0    0   0    0   0    0   0    0   0    0   0    0   0    0   0
  3/5     0   0    0   0    0   0    0   0    0   0    0   0    0   0    0   0
  3/6     0   0    0   0    0   0    0   0    0   0    0   0    0   0    0   0
  3/7     0   0    0   0    0   0    0   0    0   0    0   0    0   0    0   0
  3/8     0   0    0   0    0   0    0   0    0   0    0   0    0   0    0   0
  3/9     0   0    0   0    0   0    0   0    0   0    0   0    0   0    0   0
  3/10    0   0    0   0    0   0    0   0    0   0    0   0    0   0    0   0
  3/11    0   0    0   0    0   0    0   0    0   0    0   0    0   0    0   0
 Total    1        0        0        0        0        0        0        0

  dial-out call statistics

        noCarr noDitone     busy    abort dialStrg autoLgon dialTout  rmtHgup
  Mdm     #   %    #   %    #   %    #   %    #   %    #   %    #   %    #   %
  3/0     0   0    0   0    0   0    0   0    0   0    0   0    0   0    0   0
* 3/1     0   0    0   0    0   0    0   0    0   0    0   0    0   0    0   0
  3/2     0   0    0   0    0   0    0   0    0   0    0   0    0   0    0   0
  3/3     0   0    0   0    0   0    0   0    0   0    0   0    0   0    0   0
  3/4     0   0    0   0    0   0    0   0    0   0    0   0    0   0    0   0
  3/5     0   0    0   0    0   0    0   0    0   0    0   0    0   0    0   0
  3/6     0   0    0   0    0   0    0   0    0   0    0   0    0   0    0   0
  3/7     0   0    0   0    0   0    0   0    0   0    0   0    0   0    0   0
  3/8     0   0    0   0    0   0    0   0    0   0    0   0    0   0    0   0
  3/9     0   0    0   0    0   0    0   0    0   0    0   0    0   0    0   0
  3/10    0   0    0   0    0   0    0   0    0   0    0   0    0   0    0   0
  3/11    0   0    0   0    0   0    0   0    0   0    0   0    0   0    0   0
 Total    0        0        0        0        0        0        0        0
```

Table 68 describes the significant fields shown in the display.

Table 68 show modem call-stats Field Descriptions

Field	Description
dial-in/dial-out call statistics	This category of disconnect reasons can happen only in dial-in or dial-out scenarios.
mohTrmnt	The number of times that a modem is disconnected because Modem on Hold (MOH) terminates. MOH will terminate for two reasons: • MOH clear down by the modem (MICA_DR_MOH_CLEAR_DOWN) • MOH time out (MICA_DR_MOH_TIMEOUT)
wdogTimr	Watchdog timeout. An obscure firmware problem occurred. This is a rare disconnect reason.
compress	Compression. An error was detected during decompression, which caused the internal decompression dictionary to overflow. This could be caused by a modem dialing in that is using a slightly different compression algorithm.
retrain	Retrain failure. A connection was lost and not reestablished after three attempts.
inacTout	Inactivity timeout. The time specified in the AT/T command has expired. No modem data transfers were detected during that period.
linkFail	Link failure. The protocol level link failed while using MNP-10 or LAPM (Link Access Procedure for Modems) in reliable mode.
moduFail	Modulation error. An error was detected at the Digital Signal Processor (DSP) chip level, which caused a disconnect.
mnpProto	MNP10 protocol error. An uncorrectable error occurred during an MNP-10 connection.
lapmProt	LAPM protocol error. An uncorrectable error occurred during a LAPM connection.
lostCarr	Lost carrier. The modem firmware detected a carrier drop during a connection. The cause for the carrier drop could be the loss of signal from the remote modem or the result of a error detection.
dtrDrop	DTR drop. The modem disconnected because the DTR signal from the host became inactive.
userHgup	User hang-up. The modem disconnected because a command such as ATH was detected.
rmtlink	Remote link disconnect. If an MNP-10 reliable link is established, the remote modem sends the disconnect reason across the link before disconnecting. The disconnect reason displayed is LOCAL (remote link disconnect) and REMOTE (the reason the remote modem disconnected).
trminate	Terminate. A password security error occurred in the Microcom High Density Management System (HDMS). This error occurs only with Microcom modems.
callBkfa	Callback failed. This error applies to leased line connections only. A switched line connection failed and a connection still cannot be made on the leased line.
dial-out call statistics	This category of disconnect reasons can happen only in a dial-out scenario.

Table 68 show modem call-stats Field Descriptions (continued)

Field	Description
noCarr	No carrier. The called number answered, but no answer tone was detected after the appropriate wait.
noDitone	No dial tone. No dial tone was detected after the modem went off hook.
busy	Busy. A busy signal was detected while the local modem was attempting to dial.
abort	Abort. A character was received from the remote host after the **dial** command was issued and before a connection was established.
dialStrg	Dial string error. An invalid character was detected in the dial string, which forced the dial attempt to terminate.
autoLgon	Autologon error. An autologon sequence did not successfully complete.
dialTout	Dial timeout. When a semicolon is used as a dial modifier, the modem returns to the command state as indicated by an "OK." This character allows a continuation of the dial string. If a period of time elapses as specified in the S7 register without the dial string completing, the attempt is aborted with dial timeout as the disconnect reason.
rmtHgup	Remote hang-up. The modem disconnected because the remote modem disconnected the call and dropped DTR.
blacklst	Blacklist. In a country that supports blacklisting, an attempt was made to go off hook with a null dial string (ATD).
ccpNssn	CCP not seen. The credit card prompt (also known as Bong) was not detected.
faxClasz	Fax class 2 error. An abnormal termination to a fax transmission was detected.
Total	Total number of times the disconnect reason occurred among all the modems in the system.

show modem calltracker

To display all information stored within the Call Tracker active or history database for the latest call assigned to a specified modem, use the **show modem calltracker** command in privileged EXEC mode.

show modem calltracker [*slot*/*port*]

Syntax Description

slot/*port*	(Optional) Location of a slot and modem port. Remember to include the slash mark when entering this argument.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

This command allows you to display all Call Tracker data for a given modem when you do not have the call handle readily available and do not want to search the Call Tracker database.

Examples

The following example shows Call Tracker data for the modem in slot 1, port 1:

```
Router# show modem calltracker 1/1

------------------------- call handle=0000000058 -------------------------
status=Active, service=PPP, origin=Answer, category=Modem
DS0 slot/cntr/chan=0/0/22, called=71071, calling=6669999
userid=router5200, ip=172.19.4.2, mask=255.255.255.0
setup=10/16/1999 18:29:20, conn=0.10, phys=17.00, service=24.71, authen=24.71
init rx/tx b-rate=28800/33600, rx/tx chars=0/0
resource slot/port=1/1, mp bundle=0, charged units=0, account id=75
idb handle=0x6185B968, tty handle=0x612F8598, tcb handle=0x0
-------------------------------------------------------------------------
protocol: last=LAP-M, attempted=LAP-M
compression: last=V.42bis-Both, supported= V.42bis-RX V.42bis-TX
standard: last=V.34+, attempted=V.34+, initial=V.34+

snr=35 dB, sq=3, rx/tx level=-16/-15 dBm
phase jitter: freq=0 Hz, level=0 degrees
far end echo level=-83 dBm, freq offset=0 Hz
phase roll=-99 degrees, round-trip delay=1 msecs
digital pad=None dB, digital pad comp=0
rbs pattern=0, constellation=16 point
rx/tx: symbol rate=3429/3429, carrier freq=1959/1959
rx/tx: trellis code=0/0, preemphasis index=6/0
rx/tx: constellation shape=Off/On, nonlinear encode=Off/On
rx/tx: precode=Off/On, xmit level reduct=2/2 dBm

rx/tx: chars=0/0, general info=0x0
rx/tx: link layer chars=0/0, NAKs=0/0
error corrected: rx/tx=0/0, rx bad=0
```

```
ec retransmissions=0, retransmitted frames=0
rx/tx ppp slip=0/0, bad ppp slip=0

rx/tx b-rate: last=28800/33600, lowest=28800/33600, highest=28800/33600
phase 2 projected max rx b-rate: client=19200, host=24000
phase 4 desired rx/tx b-rate: client=28800/33600, host=28800/33600
retrains: local=0, remote=0, failed=0
speedshift: local up/down=0/0, remote up/down=0/0, failed=0

v110: rx good=0, rx bad=0, tx=0, sync lost=0
SS7/COT status=0x00
v90: status=No Attempt, client=(n/a), failure=None

rx/tx: max neg I frame=128/128, neg window=15/15
v42bis size: dictionary=1024, string=64
T401 timeouts=0, tx window closures=0, rx overruns=0
test err=0, reset=0, v0 synch loss=0
mail lost: host=0, sp=0

duration(sec)=16, disc reason=0x0
disc text=(n/a)

                --------5---------10--------15--------20--------25--------30
line shape  : 0x19202121202021202020212020202020202020201F1D191100
v8bis capab : 0x00000000000000000000000000000000000000000000000000
v8bis mod sl: 0x00000000000000000000000000000000000000000000000000
v8 jnt menu : 0x01E0C14513942A0000000000000000000000000000000000
v8 call menu: 0x01C14513942A00000000000000000000000000000000000
v90 training: 0x00000000
v90 sgn ptrn: 0x00000000
state trnsn : 0x000102030410204042 43FF0000000000000000000000000000000000000000
                0000
portwre diag: 0x00000000000000000000000000000000
phase 2 info: 0x010000F4EF221FF37E0001E4EFA21FF2E30001A4EF980101B7CF98003C00
                00000024EF40000502160AE0304DFFFECE07A707A70D650D6500
phase 4 info: 0x01834070808340708000
--------------------------------------------------------------------------------
```

Related Commands

Command	Description
show call calltracker active	Displays all information stored within the Call Tracker active database for all active calls.
show call calltracker handle	Displays the detailed data stored within Call Tracker for a specific call having a specified unique call handle identifier.
show call calltracker history	Displays all the information stored within the Call Tracker history database table for the most recent disconnected calls.

show modem configuration

To display the current modem configuration for digital MICA technologies modems loaded inside an access server or router, use the **show modem configuration** command in EXEC mode.

show modem configuration [*slot*/*port*]

Syntax Description

slot/*port*	(Optional) Slot and modem port location. If this number is not specified, statistics for all connected modems are displayed. You must type in the forward slash (/).

Command Modes

EXEC

Command History

Release	Modification
11.2P	This command was introduced.
12.1(5)T	This command was enhanced to display information about digital modems on the Cisco 3600 series routers that support V.110.
12.2(2)XA	This command was implemented on Cisco AS5350 and Cisco AS5400 universal access servers running NextPort firmware. This command was implemented on Cisco AS5300 universal access servers running Cisco MICA Portware Version 2.9.1.0.
12.2(2)XB	This command was integrated into Cisco IOS Release 12.2(2)XB.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and was implemented on the Cisco AS5300 and Cisco AS5800 platforms.

Examples

The following is sample output from the **show modem configuration** command. A specific modem, 0/0, has been designated. V.110 information is highlighted in this example.

```
Router# show modem configuration 0/0

  S-Reg   Value   Meaning
 ---|---|----------------
    S-- = 1       Country Code is Default u-law
    S00 = 0       Auto Answer immediately
    S01 = 0       Reserved
    S02 = 43      escape character is 0x2B or '+'
    S03 = 13      carriage return character is 0xD
    S04 = 10      line feed character is 0xA
    S05 = 8       backspace character is 0x8
    S06 = 2       pause 2 seconds before blind dialing
    S07 = 60      wait up to 60 seconds for carrier after dialing
    S08 = 2       comma adds 2 second dial delay
    S09 = 317     BitMap register value = 0x13D
    S10 = 14      1.4 second delay for hangup after carrier loss
    S11 = 0       In Answer Mode
    S12 = 3       3 Data Bits
    S13 = 3       Space Parity
    S14 = 1       1 Stop Bits
    S15 = 1       V.42 ODP generation enabled
    S16 = 50      5.0 second Error Correction autodetect timeout
```

```
S17 = 100     10.0 second Error Correction negotiation timeout
S18 = 13      Error Correction fallback char is 0xD
S19 = 12      Error Correction retransmission limit is 12
S20 = 256     Error Correction frame length is 256 octets
S21 = 3       V42bis or MNP Data Compression
S22 = 0       ARA Error Correction is disabled
S23 = 1       V.42 Error Correction enabled
S24 = 1       MNP Error Correction enabled
S25 = 0       Link Protocol Fallback to Async framing
S26 = 0       Using TDM slice 0
S27 = 0       Calling Tone disabled
S28 = 0       Guard Tone disabled
S29 = 8       V.110 modem standard
S30 = 33600   Maximum connect rate of 33600 bps
S31 = 300     Minimum connect rate of 300 bps
S32 = 2       Bit Errors >= 1:1000 cause recovery
S33 = 500     Fallback/Fallforward Squelch Timer is 500ms
S34 = 2000    Fall Forward Timer is 20.0 seconds
S35 = 50      Fall Back Timer is 0.50 seconds
S36 = 20      Terminate timeout is 20 seconds
S37 = 60      Wait 60 seconds for data mode timeout
S38 = 14      1.4 second lost carrier to hang-up delay
S39 = 7       Transmit level setting of -13dBm
S40 = 4       4 consecutive retrains cause link disconnect
S41 = 5       V.34 maximum symbol rate of 3429 baud
S42 = 0       V.34 minimum symbol rate of 2400 baud
S43 = 2       V.34 carrier frequency is Auto Selection
S44 = 11      V.34 Preemphasis filter selection is Automatic
S45 = 0       Null transmit and receive Signalling Type
S46 = 0       No call progress tone detection
S47 = 2       +++ escape detection enabled for originate mode only
S48 = 1       AT command processor enabled
S49 = 0       no call setup delay
S50 = 60000   Maximum PCM connect rate of 60000 bps
S51 = 28000   Minimum PCM connect rate of 28000 bps
S52 = 1       Digital Pad Compensation is enabled
S53 = 3       V.8bis is enabled
S57 = 2400    User rate for V.110 connection is 2400 bps
configuration index = 59, value = 0x3
```

The following example uses the **show modem configuration** command to display the configuration for modem 0/1, which resides in slot 0/1 of a Cisco AS5300:

```
Router# show modem configuration 0/1

Modem(0/1) Configuration Block:
Country Code: 1
Originate/Answer Mode: Answer
Data Bits Selection: 8
Parity Selection: 0
Stop Bits Selection: 1
V.42 ODP generation: Generate ODP sequence when originating a call
Error Correction Autodetect Time-out value: 5000 ms
Protocol Negotiation Time-out value: 10000 ms
Protocol Negotiation Fallback Character:
Protocol Negotiation Retransmission Limit: 12
Error Correction Frame Length: 256 bytes
Data Compression: V.42bis and MNP5
ARA Error Correction: ARA1.0 & ARA2.0 Enabled for Answer only
V.42 Error Correction: V.42(LAP-M) Originate&Answer enabled
MNP Error Correction: MNP Originate&Answer enabled
Link Protocol Fallback: Asynchronous Framing (Start/Stop/Parity)
DSP processor MVIP TDM slice: 0
Calling Tone: Disabled
```

```
Guard Tone: Disabled
Modem Standard: V.34bis Automode, with terbo
Max. Connect Rate: 33600 bps
Min. Connect Rate: 300 bps
Signal Quality Threshold: Bit Errors >=1:1000 cause recovery
Fallback/Fallforward Squelch Timer: 500 ms
Fall Forward Timer: 10000 ms
Fall Back Timer: 500 ms
Terminate Time-out: 20 second(s)
Wait For Data Mode Time-out: 40 second(s)
Lost Carrier To Hang-up Delay: 1400 ms
Transmit Level Setting: -13 dBm
Retrain Limit: 4
V.34 Max. Symbol Rate: 3249 Baud
V.34 Min. Symbol Rate: 2400 Baud
V.34 Carrier Frequency: Auto Carrier Selection
V.34 Preemphasis Filter Selection: 11
Tx and RX Signaling Type: NULL signaling
Call Progress Tone Detection: No tone detection
+++ Escape Detection: Enabled-Originate-Mode-Only
AT Command Processor: Enabled
Call Set Up Delay: no delay before link initiation
Automatic Answer: delay 1 second(s)
Escape Detection Character: ASCII 43 ('+')
Carriage Return Character: ASCII 13 (CR)
Line Feed Character: ASCII 10 (LF)
Backspace Character: ASCII 8 (BS)
Pause Before Blind Dialing: 2 second(s)
Wait For Carrier After Dial: 40 second(s)
Comma Dial Modifier Time: 2 second(s)
Bit-mapped Register(S9=0x13D): E1Q2V1&D3X4
Delay For Hangup After Carrier Loss: 1400 ms
```

Table 69 describes the significant fields shown in the display.

Table 69 show modem configuration Field Descriptions for MICA Modems

Field	Description
Modem (0/1)	Slot and port for the specified modem.
Country Code:	Transmit level limits with respect to the S39 register. Default is 1 (U.S. domestic).
Originate/Answer Mode:	Answer or originate. Default is answer.
Data Bits Selection:	7, 8, or 9 data bits. Default is 8.
Parity Selection:	0 = no parity, 1 = even parity, 2 = odd parity. Default is no parity.
Stop Bits Selection:	1 or 2 stop bits. Default is 1 stop bit.
V.42 ODP generation:	Disabled or generated ODP sequence when originating a V.42 call. Default is Generate ODP sequence when originating a V.42 call.
Error Correction Autodetect Time-out value:	Maximum period (in milliseconds) during which the modem will run an automated detection machine upon the incoming data. Default is 5000 ms.
Protocol Negotiation Time-out value:	Maximum wait period (in ms) for error correction protocol negotiation before fallback. Default is 10,000 ms.
Protocol Negotiation Fallback Character:	0 to 127. Default is 13.

Table 69 show modem configuration Field Descriptions for MICA Modems (continued)

Field	Description
Protocol Negotiation Retransmission Limit:	0 = Do not disconnect on excessive retransmission; 1 to 255 = number of successive retransmissions to cause disconnect. Default is 12.
Error Correction Frame Length:	Buffer length; 64 to 1024 octets of data. Default is 256.
Data Compression:	Disabled, V.42bis, MNP5, or V.42bis or MNP5 (V.42 has precedence). Default is V.42bis or MNP5 (V.42 has precedence).
ARA Error Correction:	ARA1.0 & ARA2.0 Disabled, Enabled for Answer only, Enabled for Answer originate ARA1.0, and Enabled for Answer originate ARA2.0. Default is Enabled for Answer only.
V.42 Error Correction:	V.42(LAP-M) Disabled, V.42(LAP-M) Originate&Answer enabled. Default is disabled.
MNP Error Correction:	MNP Disabled or MNP Originate and Answer enabled. Default is MNP Originate&Answer enabled.
Link Protocol Fallback:	Asynchronous Framing (Start/Stop/Parity), Synchronous framing (Raw 8 bits to DSP), or Disconnect (Hang-up). Default is Asynchronous Framing (Start/Stop/Parity).
DSP processor MVIP TDM slice:	0 to 15.
Calling Tone:	Disabled or Send calling tone. Default is disable.
Guard Tone:	Guard tone disabled, Use Guard tone (V.22 and V.22bis only). Default is Disabled.
Modem Standard:	V.34bis Automode, with terbo; V.34bis Automode skip terbo; V.32 terbo Automode; V.32bis Automode; V.22bis Automode; or K56Flex 1.1. Default is V.34bis Automode, with terbo.
Max. Connect Rate:	75 to 56,000 bits per second (bps).
Min. Connect Rate:	75 to 56,000 bps.
Signal Quality Threshold:	No action on bit errors, Bit Errors >=1:100 cause recovery, Bit Errors >=1:1000 cause recovery, Bit Errors >=1:10000 cause recovery, Bit Errors >=1:100000 cause recovery, or Bit Errors >=1:1000000 cause recovery. Default is 1:1000.
Fallback/Fallforward Squelch Timer:	Time (in milliseconds) to delay after a speed shift before allowing another speed shift. Default is 500 ms.
Fall Forward Timer:	Elapsed time (in milliseconds) with continuous good signal quality to cause a fall forward. Default is 10,000 ms.
Fall Back Timer:	Elapsed time (in milliseconds) with bad signal quality to cause a fallback. Default is 500 ms.
Terminate Time-out:	Elapsed time (in seconds) after a disconnect request before forcing a link disconnect. During this period, the modem sends buffered data and then clears down the link. Default is 20 seconds.
Wait for Data Mode Time-out:	Maximum time (in seconds) during link establishment before disconnection. Default is 40; 60 for K56Flex.
Lost Carrier To Hang-up Delay:	Maximum time (in milliseconds) without a carrier to cause the link disconnect. Default is 1400 ms.

Table 69 show modem configuration Field Descriptions for MICA Modems (continued)

Field	Description
Transmit Level Setting:	6 dBm, 7 dBm, 8 dBm, –20 dBm, or –21 dBm. Default is 9 dBm.
Retrain Limit:	Maximum successive failed retrains to cause the link to disconnect. Default is 4.
V.34 Max. Symbol Rate:	2400 baud, 2743 baud, 2800 baud, 3000 baud, 3200 baud, or 3429 baud. Default is 3429 baud.
V.34 Min. Symbol Rate:	2400 baud, 2743 baud, 2800 baud, 3000 baud, 3200 baud, or 3429 baud. Default is 2400 baud.
V.34 Carrier Frequency:	Low Carrier, High Carrier, or Auto Carrier Selection. Default is High Carrier.
V.34 Preemphasis Filter Selection:	0 to 10 = a selected filter; 11 = Automatic Preemphasis Selection. Default is 11.
Tx and Rx Signaling Type:	NULL signaling, MF signaling, DTMF signaling, Lower band R2 signaling, Upper band R2 signaling, or R1 signaling. Default is NULL signaling.
Call Progress Tone Detection:	No tone detection, Dial tone detection, Ring-Back tone detection, or Busy tone detection. Default is No tone detection.
+++ Escape Detection:	Disabled, Enabled, or Enabled-Originate-Mode-Only. Default is Enabled-Originate-Mode-Only.
AT Command Processor:	Disabled or Enabled. Default is Disabled.
Call Set Up Delay:	No delay before link initiation, delay value (1 to 255). Default is no delay.
Automatic Answer:	Answer immediately, delay value (1 to 255 seconds). Default is 1 second.
Escape Detection Character:	ASCII value (0 to 127). Default is 43.
Carriage Return Character:	ASCII value (0 to 127). Default is 13.
Line Feed Character:	ASCII value (0 to 127). Default is 10.
Backspace Character:	ASCII value (0 to 127). Default is 8.
Pause Before Blind Dialing:	2 to 255 seconds. Default is 2.
Wait For Carrier After Dial:	Wait for data mode timeout (in seconds).
Comma Dial Modifier Time:	2 to 255 seconds. Default is 2.
Bit-mapped Register(S9=0x13D):	Bit mapped register.
Delay For Hangup After Carrier Loss:	Lost carrier to hang-up delay (in milliseconds).

Related Commands

Command	Description
show modem log	Displays the modem history event status performed on a manageable modem or group of modems.
show modem mica	Displays information about MICA technologies digital modems.
show modem operational-status	Displays the current modem operational status for MICA technologies digital modems loaded in access servers or routers.

show modem configuration (pvdm2)

To display the current modem configuration for digital modems on PVDM2-xxDM devices, use the **show modem configuration** command in privileged EXEC mode.

show modem configuration [*slot/modem number*]

Syntax Description

slot/modem number	(Optional) Slot and modem number. If this number is not specified, statistics for all connected modems are displayed. You must type in the forward slash (*/*).

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(11)XW	This command was introduced.

Examples

The following is sample output from the **show modem configuration** command for a V12 modem. A specific modem, 0/322, is designated.

```
Router# show modem configuration 0/322
Modem (0/322) Configuration Status:

  S-Reg   Value   Meaning
 -------|-------|-----------------------------------------------
    S00 = 0       Auto Answer disabled
    S01 = 0       Ring Counter is 0
    S02 = 43      escape character is 0x2B or '+'
    S03 = 13      carriage return character is 0xD
    S04 = 10      line feed character is 0xA
    S05 = 8       backspace character is 0x8
    S06 = 2       pause 2 seconds before blind dialing
    S07 = 70      wait up to 70 seconds for carrier after dialing
    S08 = 2       comma adds 2 second dial delay
    S09 = 6       0.6 second Carrier detect response time
    S10 = 14      1.4 second delay for hangup after carrier loss
    S11 = 95      0.095 second DTMF Tone Duration
    S11 = 50      Escape Prompt Delay (in .02s)
    S14 = 138     Command echo enabled (E1), Send result codes (Q0),
                  Result codes is verbose (V1), Tone (T), Originate,
    S16 = 0       Local analog loopback disabled
                  Local digital loopback disabled
                  Remote digital loopback not in progress RDL not requested
                  RDL with self test disabled
                  Local analog loopback with self test disabled
    S18 = 0       Test Timer = 0x0, test will not terminate if zero
    S21 = 52      Set by &J0 command but ignored otherwise,
                  CTS always on (&R1), DTR behavior &D2 selected,
                  RLSD (DCD) behavior &C1 selected,
                  DSR behavior &S0 selected Long space disconnect Y0,
    S22 = 119     Speaker/Results 0x77 not supported
    S23 = 54      RDL not allowed (&T5), DTE Rate 2400 bps,
                  Assumed DTE parity none, Guard tone none (&G0),
```

```
S24 = 0       0 second Sleep Inactivity Timer
S25 = 5       Delay 5 (sec for async; 0.01 sec otherwise) to ignore DTR
S26 = 1       Delay 0.01 seconds RTS to CTS Delay
S27 = 73      Sync./Async. selection &Q5 Dial up line (&L0),
              Internal clock (&X0), Bell mode (B1),
S28 = 0       39%-61% make/break ratio at 10 pulses per second (&P0)
S29 = 70      Flash Dial Modifier Time is 700 ms
S30 = 0       No Disconnect Inactivity Timer
S31 = 6       Single line connect message controlled by S95, Wn and Vn
              Auto line speed detection enabled(N1)
              Error correction progress messages full reporting (W1)
S32 = 17      XON character is 0x11
S33 = 19      XOFF character is 0x13
S36 = 7       Attempt MNP connection, if fails, Normal mode
S37 = 0       Attempt automode connection
S38 = 20      20 seconds Delay Before Forced Hang Up
S39 = 3       RTS/CTS (&K3)
S40 = 88      Disable extended services(-K0)
              Break Handling (\Kn) not supported
              NMP block size 128 chars (\A1)
S41 = 139     Compression selection is MNP 5 and V.42 bis
              Retrain and fallback/fall forward disabled
S46 = 138     Execute error correction protocol with compression
S48 = 7       V.42 negotiation enabled
S82 = 128     Break Handling Options/LAPM Break Control = 0x80
S82 = 21
S91 = 13      -13 dBm Transmit Level in analog modulations
S92 = 13      -13 dBm Transmit Level for the fax mode
S95 = 0       CONNECT result code indicates DTE speed
              Not append/ARQ to CONNECT 'rate' in error-correction
              Disable CARRIER 'rate' result code
              Disable PROTOCOL 'identifier' result code
              Disable COMPRESSION 'type' result code
S200 = 223    Enable K56Plus
S202 = 2      K56Plus protocol follows the setting of ATNn
              Enables V.90 digital pad compensation
              Disable Display Tx and Rx HNDSHK states
              No automatic CX802xx/CX803xx status response
              K56flex Tx level is -12 dBm V90 Tx level is -12 dBm
              Disable V.42 selective reject
S210 = 13     2400,2800,3000,3200,3429 V.34 asymmetric rates enabled
S220 = 11     Duration of Answer Tone is 0xB (in units of 450ms)
S221 = 50     500 ms Duration of Billing Delay
S222 = 0
S223 = 23     -12 dBm V.90 PCM Transmit Level
S224 = 0      Digital detect timer (100ms per unit)
```

Table 70 describes the S register fields shown in the display.

Table 70 show modem configuration Field Descriptions for V12 Modems

S Register	Field	Description
S00	Rings to Auto-Answer	0 to 255. Default is 0.
S01	Ring Counter	0 to 255. Default is 0.
S02	Escape Character	Default is 43.
S03	Carriage Return Character	Default is 13.
S04	Line Feed Character	Default is 10.
S05	Backspace Character	Default is 8.

Table 70 show modem configuration Field Descriptions for V12 Modems (continued)

S Register	Field	Description
S06	Wait Time Before Blind Dialing	2 to 255 seconds. Default/minimum is 2.
S07	Wait Time for Carrier, Silence, or Dial Tone	1 to 255 seconds. Default is 50.
S08	Pause Time for Dial Delay	0 to 255 seconds. Default is 2.
S09	Carrier Detect Response Time	1to 255 in 100 ms increments. Default is 6 (0.6 seconds).
S10	Lost Carrier to Hangup Delay	1 to 255 in 100 ms increments. Default is 14 (1.4 seconds).
S11	DTMF Tone Duration	Returns OK. Default is 95 (0.095 seconds).
S12	Escape Prompt Delay (EPD)	Returns OK. Default is 50 (1.00 seconds).
S14	General Bit Mapped Options Status	Sets/resets command echo, quiet mode, result codes, tone/pulse, originate/answer.
S16	General Bit Mapped Test Options Status	Status of analog and digital loopback tests.
S18	Test Timer	Length of test before returning to command mode. 0 to 255 seconds. Default is 0.
S21	V24/General Bit Mapped Options Status	Status of behavior of CTS, DTR, DCD, and DSR.
S22	Speaker/Results Options Status	Not supported.
S23	General Bit Mapped Options Status	Status of RDL, DTE rate, DTE parity, and guard tone.
S24	Sleep Inactivity Timer	0 to 255 seconds. Default is 0 (no sleep).
S25	Delay to DTR	0 to 255 in 10 ms increments (or full seconds for synchronous modes). Default is 5.
S26	RTS to CTS Delay	0 to 255 in 10 ms increments. Default is 1.
S27	Bit Mapped Options Status	Sync/async selection, leased line control, clock select, CCITT/Bell mode select.
S28	Bit Mapped Options Status	Pulse dialing make/break ratio. Default is 39 - 61% at 10 pulses/second.
S29	Flash Dial Modifier Time	0 to 255 in 10 ms increments. Default is 70 (0.7 seconds).
S30	Disconnect Inactivity Timer	0 to 255 in 10 second increments (0 to 2550 seconds). Default is 0 (disabled).
S31	Bit Mapped Options Status	Single line connect message, auto line speed detect, error correction progress message.
S32	XON Character	Default is 0x11.
S33	XOFF Character	Default is 0x17.
S36	LAPM Failure Control	Indicates activity on a LAPM failure.
S37	Desired Line Connection Speed	Default is 0 (automode connection).
S38	Delay Brfore Forced Hangup	0 to 255 seconds. Default is 20.

Table 70 show modem configuration Field Descriptions for V12 Modems (continued)

S Register	Field	Description
S39	Flow Control Bit Mapped Options Sta'tus	Status of flow control.
S40	General Bit Mapped Options Status	MNP extended services, block size, and break handling.
S41	General Bit Mapped Options Status	Compression selection, auto retrain, fallback/fall forward.
S46	Error Correction Protocol	Default is 138 (execute protocol with compression).
S48	V42 Negotiation	Default is 7 (negotiate).
S82	Break Handling Options	LAPM Break Control.
S86	Call Failure Reason Code	Default is 21 (clear previous reason value).
S91	PSTN Transmit Attenuation Level in Analog Modulations	0 to 20 (0 to -20 dBm transmit level). Default is 10 (-10 dBm).
S92	Fax Transmit Attenuation Level	10 to 15 (-10 to -15 dBm transmit level). Default is 10 (-10 dBm).
S95	Extended Result Codes	Indicates overriding of Wn command options.
S200	Disable K56Plus Protocol	Default is 223 (enables).
S202	CSM Bit Mapped Control Register	Controls K56flex/V90 Tx level and automatic CX802xx/CX803xx status response.
S210	Symbol Rate Limit	V34 symbol rate limit, symmetric or asymmetric.
S220	Duration of Answer Tone	Command is in units of 450 ms. Default is 11 (4950 ms).
S221	Duration of Billing Delay	0 to 255 in 10 ms increments. Default is 50 (500 ms).
S222	General Purpose Register	Status of Lucent negotiation with V.8bis.
S223	V.90 PCM Transmit Level Adjust	0 to -16 dBm. Default is 23 (-12 dBm).
S224	Digital Detect Timer	Autodetects incoming call from ISDN V110/V120 or analog modem. 0 to 100 in 100 ms increments. Default is 0.

Related Commands

Command	Description
show modem log (pvdm2)	Displays the modem history event status performed on a manageable modem or group of modems.
show modem operational-status (pvdm2)	Displays the current modem operational status for V12 digital modems on PVDM2-xxDM devices.

show modem connect-speeds

To display connection speed statistics for all the modems running in an access server or router, use the **show modem connect-speeds** command in EXEC mode.

show modem connect-speeds [*max-speed* [*slot*]]

Syntax Description

max-speed	(Optional) Maximum speed you want displayed in the shifting speed window. You can specify from 12000 to 56000 bits per second (bps), and the default is 12000 bps.
slot	(Optional) Slot number, which limits the display output to a particular range of modems in the system.

Defaults

The maximum speed displayed is 12000 bps.

Command Modes

EXEC

Command History

Release	Modification
11.3	This command was introduced.
12.1(5)T	This command was enhanced to display information about digital modems on the Cisco 3600 series routers that support V.110.

Usage Guidelines

Because most terminal screens are not wide enough to display the entire range of connection speeds at one time (for example, 75 to 56000 bps), the *max-speed* variable is used. This variable specifies the contents of a shifting baud-rate window, which provides you with a snapshot of modem connection speeds for your system. If you want to display a snapshot of lower baud rates, specify a lower connection speed. If you want to see a snapshot of higher baud rates, specify a higher connection speed.

The Cisco IOS software rounds up the *max-speed* variable to the nearest recognizable baud rate, so you need not memorize or enter exact connection speeds. For example, if you enter a maximum baud rate of 22059, the system software automatically rounds the value up to 24000.

To display a complete picture of all the connection speeds and counters on the system, you must enter a series of commands. Each time you issue the **show modem connect-speeds** *max-speed* command, only nine baud rate columns can be displayed at the same time.

Table 71 shows a range of commands that you can issue, one at a time, to display a complete picture of the total possible connection speeds on your access server.

Table 71 Connect Speed Displays for the show modem connect-speeds Command

Command	Connect Speed Range Displayed
show modem connect-speeds 56000	40000 to 56000 bps
show modem connect-speeds 38000	24000 to 38000 bps

Table 71 Connect Speed Displays for the show modem connect-speeds Command (continued)

Command	Connect Speed Range Displayed
show modem connect-speeds 21600	2400 to 21600 bps
show modem connect-speeds 1200	75 to 1200 bps

Note The Cisco IOS software does not accept commas (,) in the connect speed field. For example, enter **28000** not **28,000**.

The **show modem connect-speeds** command displays a log of connection speed statistics starting from the last time the access servers or router was power cycled or the **clear modem counters** command was issued. If you want to create a monthly report of the connection speeds achieved by the modems, issue the **clear modem counters** command at the beginning of the month and issue the **show modem connect-speeds** command at the end of the month.

Examples

The following is sample output from the **show modem connect-speeds** command on a Cisco 3600 series router:

```
Router# show modem connect-speeds

  Codes:
  * - Modem has an active call
  R - Modem is being Reset
  D - Download in progress
  B - Modem is marked bad and cannot be used for taking calls
  b - Modem is either busied out or shut-down

  Transmit connect speeds

   Mdm       75    300    600   1200   2400   4800   7200   9600  12000 TotCnt
* 0/0        0      0      0     36     35     61      0      0      0    132
* 0/1        0      0      0      1      0      0      0      0      0      1
  0/2        0      0      0     48     45     37      0      0      0    130
* 0/3        0      0      0     86     36      4      0      0      0    126
* 0/4        0      0      0      0      0      1      0      0      0      1
  0/5        0      0      0     20     33     78      0      0      0    131
* 0/6        0      0      0     25     57     49      0      0      0    131
  0/7        0      0      0     47     48     36      0      0      0    131
b 0/8        0      0      0      0      0      0      0      0      0      0
!.
!.
!.
b 0/29       0      0      0      0      0      0      0      0      0      0
 Tot         0      0      0    263    254    266      0      0      0    783
 Tot %       0      0      0     33     32     33      0      0      0

  Receive connect speeds

   Mdm       75    300    600   1200   2400   4800   7200   9600  12000 TotCnt
* 0/0        0      0      0     36     35     61      0      0      0    132
* 0/1        0      0      0      1      0      0      0      0      0      1
  0/2        0      0      0     48     45     37      0      0      0    130
* 0/3        0      0      0     86     36      4      0      0      0    126
* 0/4        0      0      0      0      0      1      0      0      0      1
  0/5        0      0      0     20     33     78      0      0      0    131
```

```
* 0/6       0      0      0     25     57     49      0      0      0    131
  0/7       0      0      0     47     48     36      0      0      0    131
b 0/8       0      0      0      0      0      0      0      0      0      0
!.
!.
!.
b 0/29      0      0      0      0      0      0      0      0      0      0
 Tot        0      0      0    263    254    266      0      0      0    783
 Tot %      0      0      0     33     32     33      0      0      0

Router# show modem connect-speeds ?

  <12000-64000>  Max baud connect speed to display to
  |              Output modifiers
  <cr>

Router# show modem connect-speeds 12000 ?

  <0-3>  Slot number
  |      Output modifiers
  <cr>

Router# show modem connect-speeds 12000 2

  Codes:
  * - Modem has an active call
  R - Modem is being Reset
  D - Download in progress
  B - Modem is marked bad and cannot be used for taking calls
  b - Modem is either busied out or shut-down

  Transmit connect speeds

  Mdm      75    300    600   1200   2400   4800   7200   9600  12000 TotCnt
 Tot        0      0      0    263    254    266      0      0      0    783
 Tot %      0      0      0     33     32     33      0      0      0

  Receive connect speeds

  Mdm      75    300    600   1200   2400   4800   7200   9600  12000 TotCnt
 Tot        0      0      0    263    254    266      0      0      0    783
 Tot %      0      0      0     33     32     33      0      0      0
```

The following example shows connection speed statistics up to 28000 bps:

```
Router# show modem connect-speeds 28800

  transmit connect speeds

  Mdm    9600  12000  14400  16800  19200  21600  24000  26400  28800 TotCnt
* 1/0       0      0      0      0      3      4      6     37     23     74
* 1/1       0      0      3      1      0      4      9     41     20     80
* 1/2       0      0      2      0      1      3     10     37     26     82
  1/3       1      0      0      0      0      3     15     35      7     62
  1/4       0      0      0      0      4      2      8     20     13     49
* 1/5       0      0      4      0      1      0      4     38     17     65
* 1/6       0      0      2      1      0      1      9     32     11     57
* 1/7       1      0      2      0      0      5     10     31     18     67
* 1/8       0      0      0      1      1      1     10     42     11     68
  1/9       0      0      2      1      2      4      4     30     23     67
  1/10      0      0      0      0      0      2      5     26     22     56
* 1/11      0      0      0      0      3      1     16     38     17     76
* 1/12      0      0      0      0      0      3      7     40     12     62
  1/13      0      0      0      1      2      3     11     20     14     51
```

```
  1/14      0      0      2      0      0      2      7     26     12     51
  1/15      0      0      1      1      1      2      6     29     25     65
  1/16      2      0      2      0      1      5     10     37     15     73
  1/17      0      0      0      0      0      2     10     33     22     67
  1/18      0      0      2      2      0      2     12     17     25     61
* 1/19      2      0      3      0      1      2      9     35     20     74
  1/20      0      0      2      2      2      2      8     28     21     65
* 1/21      0      1      2      0      1      2      5     23     21     58
* 1/22      0      0      1      0      1      1      5     27     21     56
* 1/23      0      0      2      0      0      4      8     30     15     60
 Tot        6      1     32     10     24     60    204    752    431   1546
 Tot %      0      0      2      0      1      3     13     48     27

  receive connect speeds

  Mdm    9600  12000  14400  16800  19200  21600  24000  26400  28800 TotCnt
* 1/0       0      0      1      0      1      2      9     35     25     74
* 1/1       0      0      3      0      1      3     10     42     18     80
* 1/2       0      0      2      0      1      4      8     40     26     82
  1/3       1      0      0      0      0      1     10     36     14     62
  1/4       0      0      1      0      2      2      8     22      8     49
* 1/5       0      1      4      0      0      0      9     32     17     65
* 1/6       0      0      2      0      0      0      7     33     14     57
* 1/7       0      0      2      1      1      0      6     39     18     67
* 1/8       0      0      0      0      1      0     11     43     12     68
  1/9       1      0      3      0      0      0      8     33     22     67
  1/10      0      0      0      0      1      1      6     31     17     56
* 1/11      0      0      0      1      1      1     14     43     16     76
* 1/12      0      0      0      0      0      0      5     43     12     62
  1/13      0      0      0      0      0      2     10     26     13     51
  1/14      0      0      2      1      0      0      5     27     14     51
  1/15      0      0      1      0      1      2      3     36     22     65
  1/16      1      0      3      1      2      0      8     37     20     73
  1/17      0      0      0      0      0      0      8     36     22     67
  1/18      0      1      1      0      0      2      4     30     20     61
* 1/19      0      0      3      2      1      1      6     42     18     74
  1/20      0      1      2      1      2      1      2     37     18     65
* 1/21      0      0      3      3      1      2      2     28     18     58
* 1/22      0      0      1      0      1      0      5     32     16     56
* 1/23      0      0      2      0      0      1      8     35     13     60
 Tot        3      3     36     10     17     25    172    838    413   1546
 Tot %      0      0      2      0      1      1     11     54     26
```

The following example shows connection speed statistics up to 56000 bps:

```
Router# show modem connect-speeds 56000

  transmit connect speeds

  Mdm   40000  42000  44000  46000  48000  50000  52000  54000  56000 TotCnt
  1/0       0      0      0      0      0      0      0      0      0      0
  1/1       0      0      0      0      0      0      0      0      0      0
  1/2       0      0      0      0      0      0      0      0      0      0
  1/3       0      0      0      0      0      0      0      0      0      0
  1/4       0      0      0      0      0      0      0      0      0      0
  1/5       0      0      0      0      0      0      0      0      0      0
  1/6       0      0      0      0      0      0      0      0      0      0
  1/7       0      0      0      0      0      0      0      0      0      0
  1/8       0      0      0      0      0      0      0      0      0      0
  1/9       0      0      0      0      0      0      0      0      0      0
  1/10      0      0      0      0      0      0      0      0      0      0
  1/11      0      0      0      0      0      0      0      0      0      0
  1/12      0      0      0      0      0      0      0      0      0      0
  1/13      0      0      0      0      0      0      0      0      0      0
```

```
 1/14       0       0       0       0       0       0       0       0       0       0
 1/15       0       0       0       0       0       0       0       0       0       0
 1/16       0       0       0       0       0       0       0       0       0       0
 1/17       0       0       0       0       0       0       0       0       0       0
 1/18       0       0       0       0       0       0       0       0       0       0
 1/19       0       0       0       0       0       0       0       0       0       0
 1/20       0       0       0       0       0       0       0       0       0       0
 1/21       0       0       0       0       0       0       0       0       0       0
 1/22       0       0       0       0       0       0       0       0       0       0
 1/23       0       0       0       0       0       0       0       0       0       0
Tot         0       0       0       0       0       0       0       0       0       0
Tot %       0       0       0       0       0       0       0       0       0

 receive connect speeds

 Mdm    40000   42000   44000   46000   48000   50000   52000   54000   56000 TotCnt
 1/0        0       0       0       0       0       0       0       0       0       0
 1/1        0       0       0       0       0       0       0       0       0       0
 1/2        0       0       0       0       0       0       0       0       0       0
 1/3        0       0       0       0       0       0       0       0       0       0
 1/4        0       0       0       0       0       0       0       0       0       0
 1/5        0       0       0       0       0       0       0       0       0       0
 1/6        0       0       0       0       0       0       0       0       0       0
 1/7        0       0       0       0       0       0       0       0       0       0
 1/8        0       0       0       0       0       0       0       0       0       0
 1/9        0       0       0       0       0       0       0       0       0       0
 1/10       0       0       0       0       0       0       0       0       0       0
 1/11       0       0       0       0       0       0       0       0       0       0
 1/12       0       0       0       0       0       0       0       0       0       0
 1/13       0       0       0       0       0       0       0       0       0       0
 1/14       0       0       0       0       0       0       0       0       0       0
 1/15       0       0       0       0       0       0       0       0       0       0
 1/16       0       0       0       0       0       0       0       0       0       0
 1/17       0       0       0       0       0       0       0       0       0       0
 1/18       0       0       0       0       0       0       0       0       0       0
 1/19       0       0       0       0       0       0       0       0       0       0
 1/20       0       0       0       0       0       0       0       0       0       0
 1/21       0       0       0       0       0       0       0       0       0       0
 1/22       0       0       0       0       0       0       0       0       0       0
 1/23       0       0       0       0       0       0       0       0       0       0
Tot         0       0       0       0       0       0       0       0       0       0
Tot %       0       0       0       0       0       0       0       0       0       0
```

Table 72 describes the significant fields shown in the displays.

Table 72 show modem connect-speeds Field Descriptions

Field	Description
transmit connect speeds	Connection speeds for calls initiated by the system.
Mdm *slot*/*port*	Specified slot and port number assigned to the modem.
speed counters	The transmit and receive speed counters are 75, 300, 600, 1200, 2400, 4800, 7200, 9600, 12000, 14400, 16800, 19200, 21600, 24000, 26400, 28800, 31200, 33600, 32000, 34000, 36000, 38000, 40000, 42000, 44000, 46000, 48000, 50000, 52000, 54000, and 56000 bps.
TotCnt	For the specified modem, the sum of the number of times a connection was initiated or received at one of the specified connection rates (75 to 56,000 bps).

Table 72 show modem connect-speeds Field Descriptions (continued)

Field	Description
Tot	For all modems loaded in the system, the total number of times a call was initiated or received at the specified speed.
Tot %	Percentage of the total number of calls that were initiated or received at the specified speed.
receive connect speeds	Connection speeds for incoming calls.

Related Commands

Command	Description
clear modem counters	Clears the statistical counters on one or more manageable modems on access servers or routers.

show modem cookie

To display information about the modem cookie, use the **show modem cookie** command in EXEC mode.

show modem cookie

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Examples

The following is sample output from the **show modem cookie** command for a V.34 carrier card and two modem cards:

```
Router# show modem cookie

 Hex dump of modem board HW version info:

 Slot 1:
   Carrier card:
     0000:  1802 0200 0000 0000 0000 0000 0000 0000
     0010:  0000 0000 0000 0000 0000 0000 0000 0000
   Modem Module 0:
     0000:  0C01 3033 3030 3031 4D69 6372 6F63 6F6D
     0010:  204D 4E50 3130 2056 3334 204D 6F64 656D
   Modem Module 1:
     0000:  0C01 3033 3030 3031 4D69 6372 6F63 6F6D
     0010:  204D 4E50 3130 2056 3334 204D 6F64 656D
```

Table 73 describes the significant fields shown in the display.

Table 73 show modem cookie Field Descriptions

Field	Description
Slot 1:	The slot carrying the carrier and modem card.
Carrier card:	Carrier card and its cookie parameters.
Modem Module 0:	Modem card and its cookie parameters.

show modem csm

To display the internal status of the call switching module for modems inside access servers or routers, use the **show modem csm** command in EXEC mode.

show modem csm [*slot*/*port* | **group** *number*]

Syntax Description

slot/*port*	(Optional) Slot and modem port location. If this number is not specified, statistics for all connected modems are displayed. (Include the forward slash (/) when entering this variable.)
group *number*	(Optional) Specific group of modems. If the modem group number is not specified, statistics for all modems in the access server are displayed. The group number range is from 1 to 200.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Examples

The following example displays the call switching module information for modem 1/2 on a Cisco AS5200:

```
Router# show modem csm 1/2

MODEM_INFO: slot 1, port 2, unit 130, modem_mask=0x0004, modem_port_offset=0
tty_hwidb=0x00000000, modem_tty=0x004370A8, mgmt_tty=0x004370A8, modem_pool=0x0041D99C
csm_status(0): CSM_STATUS_UNLOCKED
csm_state(0x00000000)=CSM_OC_STATE, csm_event_proc=0x0005B448
invalid_event_count=0, wdt_timeout_count=0
wdt_timestamp_started is not activated
wait_for_dialing:False, wait_for_bchan:False
pri_chnl=TDM_ISDN_STREAM(s0, c0), modem_chnl=TDM_ISDN_STREAM(s0, c0)
dchan_idb_start_index=0, dchan_idb_index=0, call_id=0x0000, bchan_num=0
csm_event=CSM_EVENT_NONE, cause=0x0000, phone_num=
ring_indicator=0, oh_state=0, oh_int_enable=0, modem_reset=0
ring_no_answer=0, ic_failure=0, ic_complete=0
dial_failure=0, oc_failure=0, oc_complete=0
oc_busy=0, oc_no_dial_tone=0, oc_dial_timeout=0
remote_link_disc=0, busyout=0, modem_reset=0
call_duration_started=00:00:00, call_duration_ended=00:00:00, total_call_duration=00:00:00
The calling party phone number = 4082968388
The called party phone number = 4085267406
```

Table 74 describes the significant fields shown in the display.

Table 74 show modem csm Field Descriptions

Field	Description
MODEM_INFO	Displays internal data structure information.
csm_status	Displays the status of the call switching module. Possible statuses include unlocked, active call, busyout req, shutdown, bad modem, modem hold, back-to-back, file downloading, and reset.
csm_state	Displays the current state of the call switching module. Possible states include idle and connected. Incoming calls are marked IC and outgoing calls are marked OC.
Modem counters	Counters for different modem events.
The calling party phone number The called party phone number	Phone numbers for the dialing integrated modem and the remote modem.

show modem log

To display the modem history event status performed on a manageable modem or group of modems, use the **show modem log** command in EXEC mode.

show modem log [*slot*/*port* | **group** *number*]

Syntax Description

slot/*port*	(Optional) Slot and modem port location. If this number is not specified, statistics for all connected modems are displayed. (Include the forward slash (/) when entering this variable.)
group *number*	(Optional) Specific group of modems. If the modem group number is not specified, statistics for all modems in the access server are displayed. The group number range is from 1 to 200.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.1(5)T	This command was enhanced to display information about the Cisco 3600 series digital modems that support V.110, and about the Cisco 2600 and Cisco 3600 series modems that support leased-line operation.

Examples

The following is sample output from the **show modem log** command issued on a Cisco AS5300, which is loaded with MICA technologies digital modems. See Table 75 for MICA modem field descriptions.

```
Router# show modem log 1/0

Modem 1/0 Events Log:
  01:54:02:Startup event:MICA Hex modem (Select)
       Modem firmware = 2.0.0.9
  01:54:02:RS232 event:
           noRTS, noDTR, CTS, noDCD
  01:54:02:RS232 event:
           RTS, DTR, CTS, noDCD
  01:54:02:RS232 event:
           RTS, DTR, CTS, noDCD
  01:54:02:RS232 event:
           noRTS, DTR, CTS, noDCD
  01:54:02:RS232 event:
           RTS, DTR, CTS, noDCD
  01:54:02:RS232 event:
           noRTS, noDTR, CTS, noDCD
  01:54:02:RS232 event:
           RTS, DTR, CTS, noDCD
  01:54:03:RS232 event:
           RTS, DTR, CTS, noDCD
  00:01:09: ISDN outgoing called number: 1000
  00:01:04:RS232 event:
           noRTS, DTR, CTS, noDCD
```

```
  00:01:04:RS232 event:
           RTS, DTR, CTS, noDCD
  00:01:06:Modem State event:
           State: Open
  00:01:06:Modem State event:
           State: Connect
  00:01:06:Modem State event:
           State: Link
  00:00:54:Modem State event:
           State: Training
  00:00:32:Modem State event:
           State: EC Correction
  00:00:32:Modem State event:
           State: Steady
  00:00:32:RS232 event:
           RTS, DTR, CTS, DCD
  00:00:32:Static event:
    Connect Protocol:  LAP-M
    Compression:  (invalid#3)
    Connected Standard:  Bell212
    TX,RX Symbol Rate:  3429, 3429
    TX,RX Carrier Frequency:  1959, 1959
    TX,RX Trellis Coding:  16, 16
    Frequency Offset:  0 Hz
    Round Trip Delay:  1 msecs
    TX,RX Bit Rate:  16800, 16800
  00:00:33:Dynamic event:
    Sq Value:  7
    Signal Noise Ratio:  35 dB
    Receive Level:  -8 dBm
    Phase Jitter Frequency:  0 Hz
    Phase Jitter Level:  0 degrees
    Far End Echo Level:  -73 dBm
    Phase Roll:  -98 degrees
    Total Retrains:  0
    EC Retransmission Count:  0
    Characters received, transmitted:  0, 32
    Characters received BAD:  0
    PPP/SLIP packets received, transmitted:  0, 0
    PPP/SLIP packets received (BAD/ABORTED):  0
    EC packets transmitted, received:  0, 0
    EC packets (Received BAD/ABORTED):  0
```

The following example shows a portion of the output display when using the **show modem log** command. Because no specific modem or range of modems is designated, the data from all modems is displayed. The V.110 information is highlighted in this example.

```
Router# show modem log

Modem 0/0 Mica: Event Log contains 100 Events:
1d21h MICA-Cfg issued S-Reg configuration change:
    configuration index = 59, value = 0x3
1d21h CSM: Incoming call from 9195555301 to Unknown
1d21h CSM: event-ISDN_CALL New State-IC_MODEM_RESERVED
    CSM: status-1 dchan-3/2 bchan-0
.
.
.
1d21h CSM: event-MODEM_CONNECTED New State-CONNECTED_STATE
1d21h MICA-Qry Static Link Information:
    Connect Protocol - V.110, Compression - None, Connected Standard - V110
    Tx/Rx Symbol Rate - 0/0, Tx/Rx Carrier Freq - 0/0
    Tx/Rx Trellis Coding - /, Frequency offset - 0Hz
```

```
    Round trip delay - 0ms, Tx/Rx bit rate - 2400/2400
    RBS pattern - 0x0, digital pad - , compensation - 0
1d21h MICA-Cmd Set Framing Mode to PPP.
.
.
.
1d21h MICA-Qry Final Link Information:
    Call Time - 00:00:34, Disconnect Reason (0x8001) - SOFTWARE_RESET command
    0 retrains and/or speed shifts, 0 ec retransmissions
    9454 chars tx, 6577 chars rx, 0 chars rx bad
    189 ppp packets tx, 129 ppp packets rx, 14 ppp packets rx bad
    0 ec packets tx, 0 ec packets rx, 0 ec packets rx bad
    0 v110 packets tx, 0 v110 packets rx, 0 v110 packets rx bad, 0 v110 sync loss
1d21h CSM: event-ASYNC_DTR_DOWN New State-IDLE_STATE
1d21h CSM: event-ASYNC_DTR_DOWN New State-IDLE_STATE
.
.
.
1d21h MICA-Cfg issued S-Reg configuration change:
    S29 = 8       V.110 modem standard
1d21h MICA-Cfg issued S-Reg configuration change:
    S57 = 3       User rate for V.110 connection is 3 bps
.
.
.
```

Table 75 describes the significant fields shown in the MICA modem display.

Table 75 show modem log Field Descriptions for MICA Modems

Field	Event State	Description
Modem <slot/port> Events Log:	—	The modem for which log events are currently displayed.
00:00:00:	—	Identifies the time elapsed (in hours: minutes: seconds) since each MICA modem event was performed (for example, 01:02:41 means the modem event occurred 1 hour, 2 minutes, and 41 seconds ago).
Startup event:	—	Type of specified MICA modem.
Modem firmware:	—	Modem firmware version.
RS232 event:	—	Detected modem signaling event.
ISDN outgoing called number:	—	Outgoing ISDN phone number dialed by the specified MICA modem.

Table 75 show modem log Field Descriptions for MICA Modems (continued)

Field	Event State	Description
Modem State event:	Current state of the MICA modem, which can be any of the following:	
	Connect	Modem is connected to a remote host.
	Open	Open modem event.
	Link	Link protocol event occurred.
	Training	Modem retraining event.
	EC Correction	Error correction frames transmitted or received.
	Steady	Steady modem event.
	Bad	Inoperable state, which is configured by the **modem bad** command.
	Bad*	Inoperable state, which is configured by the **modem startup-test** command during initial power-up testing.
	Reset	Modem is in reset mode.
	D/L	Modem is downloading firmware.
	Bad FW	Downloaded modem firmware is not operational.
	Busy	Modem is out of service and not available for calls.
	Idle	Modem is ready for incoming and outgoing calls.
Static event:	Current static event of the MICA modem, which can be any of the following:	
	Connect Protocol	Connection protocol used for the current session, which can be SYNC mode, ASYNC mode, ARA1.0, ARA2.0, Link Access Procedure for Modems (LAP-M), or Microcom Network Protocol (MNP).
	Compression	Type of compression used for the current session, which can be None, V.42*bis* TX, V.42*bis* RX, V.42*bis* both, or MNP5 data compression.
	Connected Standard	Standards protocol used to connect, which can be V.21, Bell103, V.22, V.22bis, Bell212, V.23, V.32, V.32bis, V.32terbo, V.34, V.34+, or K56Flex 1.1.
	TX, RX Symbol Rate	Symbol rate used to send samples to the line or receive samples off of the line.
	TX, RX Carrier Frequency	Carrier frequency used by the remote service provider.
	TX, RX Trellis Coding	Trellis coding received and transmitted.
	Frequency Offset	+/–32 in 1/8 Hz steps.
	Round Trip Delay	Total round trip propagation delay of the link, which is expressed in milliseconds.
	TX, RX Bit Rate	For RX, the bit rate from the remote service provider to the local service provider. For TX, the bit rate from the local service provider to the remote service provider.

Table 75 show modem log Field Descriptions for MICA Modems (continued)

Field	Event State	Description
Dynamic event:	Current dynamic event of the MICA modem, which can be any of the following:	
	Sq Value	Signal quality value, which can be from 0 to 7 (0 is the worst possible quality).
	Signal Noise Ratio	Expressed in decibels (dB), which can be from 0 to 70 dB steps.
	Receive Level	Expressed in decibels, which can be from 0 to –128 dBm steps.
	Phase Jitter Frequency	+/–32 in 1/8 Hz steps.
	Phase Jitter Level	0 to 90 degrees.
	Far End Echo Level	0 to –90 in dBm of far end echo level (that portion of the transmitted analog signal that has bounced off the remote modem's analog front end).
	Phase Roll	+/–32 in 1/8 Hz steps.
	Total Retrains	Count of total retrains.
	EC Retransmission Count	Count of total error correction retransmissions that occurred during the duration of the link.
	Characters received, transmitted	Count of total characters received and transmitted.
	Characters received BAD	A subset of the total Characters received, transmitted. Represents the total number of parity error characters.
	PPP/SLIP packets received, transmitted	Total count of PPP/SLIP packets transmitted and received. This total could include all PPP/SLIP packets, including BAD/ABORTED packets.
	PPP/SLIP packets received, (BAD/ABORTED)	Total count of the bad or aborted PPP/SLIP packets, which is a subset of the PPP/SLIP packets received, transmitted.
	EC packets transmitted, received	Count of total error correction frames transmitted or received. This total could include all error correction packets, including BAD/ABORTED packets.
	EC packets (Received BAD/ABORTED)	Total count of the bad or aborted error correction packets, which is a subset of the EC packets transmitted, received.

The following example displays the event log status for a V.34 Microcom manageable modem installed in a Cisco AS5200. To escape from the log display mode, press the keys Ctrl-c. See Table 76 for Microcom field descriptions.

```
Router# show modem log 1/0

Modem 1/0 Events Log:
  04:58:33: End connection event: Retransmits for EC block (TX/RX) = 86/33
            Duration = 0:10:21, Number of TX/RX char = 100183/34307
            Local Disc Reason = Remote Link Disc
            Remote Disc Reason = Unknown
  04:58:33: Modem State event: Idle
  04:58:33: DTR event: DTR Off
             04:58:33: RS232 event: RTS  noDTR* CTS* DSR* noDCD* noRI* noTST*
```

```
04:58:21: DTR event: DTR On
           04:58:21: RS232 event: RTS* DTR* CTS  DSR  noDCD  noRI  noTST
04:56:27: ISDN incoming calling number: 7039687666
04:56:27: ISDN incoming called number: 8366
04:56:21: Modem State event: Dialing/Answering
04:56:21: Modem State event: Incoming ring
04:56:21: Modem State event: Waiting for Carrier
           04:56:21: RS232 event: RTS  DTR  CTS  DSR  noDCD  noRI* noTST
04:56:09: Modem State event: Connected
04:56:09: Connection event: TX/RX Speed = 24000/26400, Modulation = V34
          Direction = Answer, Protocol = reliable/LAPM, Compression = V42bis
           04:56:09: RS232 event: RTS  DTR  CTS  DSR  DCD* noRI  noTST
04:55:57: Modem Analog signal event: TX = -13, RX = -17, Signal to noise = 40
04:55:21: Modem State event: Disconnecting
04:55:21: End connection event: Retransmits for EC block (TX/RX) = 0/0
          Duration = 0:00:46, Number of TX/RX char = 8911/7732
          Local Disc Reason = Remote Link Disc
          Remote Disc Reason = Unknown
04:55:23: Modem State event: Idle
04:55:23: DTR event: DTR Off
           04:55:23: RS232 event: RTS  noDTR* CTS* DSR* noDCD* noRI* noTST*
04:55:11: DTR event: DTR On
           04:55:11: RS232 event: RTS  DTR* CTS  DSR  noDCD  noRI  noTST
04:53:23: ISDN incoming calling number: 8477262725
04:53:23: ISDN incoming called number: 8366
04:53:22: Modem State event: Dialing/Answering
04:53:22: Modem State event: Incoming ring
           04:53:22: RS232 event: RTS  DTR  CTS  DSR  noDCD  noRI* noTST
04:53:10: Modem State event: Waiting for Carrier
           04:53:10: RS232 event: RTS  DTR  CTS  DSR  noDCD  noRI* noTST
04:52:58: Modem State event: Connected
04:52:58: Connection event: TX/RX Speed = 24000/24000, Modulation = V34
          Direction = Answer, Protocol = reliable/LAPM, Compression = V42bis
04:52:58: Modem Analog signal event: TX = -13, RX = -19, Signal to noise = 40
           04:52:58: RS232 event: RTS  DTR  CTS  DSR  DCD* noRI  noTST
04:52:46: Modem State event: Retrain Initiated
04:52:34: Connection update event: TX/RX Speed = 24000/24000, Modulation = V34
04:52:34: Modem State event: Connected
04:52:22: Modem Analog signal event: TX = -13, RX = -17, Signal to noise = 40
           04:52:12: RS232 event: RTS  DTR  CTS* DSR  DCD  noRI  noTST
           04:49:24: RS232 event: RTS  DTR  CTS* DSR  DCD  noRI  noTST
           04:49:12: RS232 event: RTS  DTR  CTS* DSR  DCD  noRI  noTST
           04:19:14: RS232 event: RTS  DTR  CTS* DSR  DCD  noRI  noTST
03:46:29: Modem State event: Disconnecting
03:46:29: End connection event: Retransmits for EC block (TX/RX) = 6/8
          Duration = 1:06:31, Number of TX/RX char = 114943/29854
          Local Disc Reason = Remote Link Disc
          Remote Disc Reason = Unknown
03:46:29: Modem State event: Idle
03:46:29: DTR event: DTR Off
03:46:29: DTR event: DTR On
           03:46:29: RS232 event: RTS  DTR* CTS* DSR* noDCD* noRI* noTST*
03:45:35: ISDN incoming calling number: 5124745911
03:45:35: ISDN incoming called number: 8366
03:45:29: Modem State event: Dialing/Answering
03:45:29: Modem State event: Incoming ring
03:45:29: Modem State event: Waiting for Carrier
```

Table 76 describes the significant fields shown in the Microcom modem display.

Table 76 show modem log Field Descriptions for Microcom Modems

Field	Description
Modem <slot/port> Events Log:	The modem for which log events are currently displayed.
00:00:00:	Identifies the time elapsed (in hours: minutes: seconds) since each Microcom modem event was performed (for example, 01:02:41 means the modem event occurred 1 hour, 2 minutes, and 41 seconds ago).
Startup Response:	List of information describing the modem type, modem firmware, and Digital Signal Processor (DSP) controller version (for 56K modems only).
Control Reply	Indicates the events the modem will be monitoring.
RS232 event	Detected modem signaling.
Modem State event	Current state of the modem, which can be any of the following: • Conn—Modem is connected to a remote host. • Bad—Inoperable state, which is configured by the **modem bad** command. • Bad*—Inoperable state, which is configured by the **modem startup-test** command during initial power-up testing. • Reset—Modem is in reset mode. • D/L—Modem is downloading firmware. • Bad FW—Downloaded modem firmware is not operational. • Busy—Modem is out of service and not available for calls. • Idle—Modem is ready for incoming and outgoing calls.

Table 76 show modem log Field Descriptions for Microcom Modems (continued)

Field	Description
End connection event	Descriptions or reasons why a connection was terminated: • Duration—Time (in hours: minutes: seconds) a connection was up between the local and remote devices. • Number of TX/RX char—Transmit and receive characters exchanged during the connection time. • Local or Remote Disc Reason—Reason the local or remote modem disconnected: – Lost Carrier—The modem firmware detects a drop in Carrier Detect during a connection. – DSP Task Hung—The DSP chip malfunctioned and failed to reset. – Link Access Procedure for Modems (LAPM) Timeout—Timed out waiting for a reply from remote. – Reliable link transmit timeout—Have not received a link acknowledgment in the first 30 seconds of the connection. – DSP access failure—Timed out trying to access the DSP chip. – CD off timeout—Timed out waiting for carrier to return after a retrain/rate renegotiation. – Code word size mismatched—The code word sizes are mismatched. – DSP code download Error—Error during the DSP code download. The time taken to recover and repeat the download would take too long to complete the handshake.
Phone number event	Descriptive information about the last dialed or current phone number.

The following example displays the event log status for a manageable modem. It also identifies the time elapsed since each modem event was performed (for example, 01:02:41 means the modem event occurred 1 hour, 2 minutes, and 41 seconds ago). To escape from the log display mode, press the keys Ctrl-c.

```
Router# show modem log 0/0

Modem 0/0 Events Log:
  01:03:03: Startup Response: Microcom MNP10 K56 Modem (Select)
            Modem (boot) firmware = 3.1(16) (3.0(4))
            DSP Controller (SPX) rev = 204.173(0) (143.191(0))
  01:03:03: Control Reply: 0xFF1F
  01:03:03: RS232 event: RTS  noDTR* CTS* DSR* noDCD* noRI  noTST
  01:03:03: RS232 event: RTS  noDTR  CTS  DSR  noDCD  noRI  noTST
  01:03:03: Modem State event: Idle
  01:03:03: End connection event: Retransmits for MNP block (TX/RX) = 0/0
            Duration = 0:00:00, Number of TX/RX char = 0/0
            Local Disc Reason = Lost Carrier
            Remote Disc Reason = Unknown
  01:03:04: Phone number event:
```

```
01:02:51: DTR event: DTR On
01:02:51: RS232 event: RTS  DTR* CTS  DSR  noDCD  noRI  noTST
00:39:52: Startup Response: Microcom MNP10 K56 Modem (Select)
          Modem (boot) firmware = 3.1(16) (3.0(4))
          DSP Controller (SPX) rev = 1.1(0) (1.1(0))
00:39:52: Control Reply: 0xFF1F
00:39:52: RS232 event: RTS  noDTR* CTS* DSR* noDCD* noRI  noTST
00:39:52: RS232 event: RTS  noDTR  CTS  DSR  noDCD  noRI  noTST
00:39:53: Modem State event: Idle
00:39:53: End connection event: Retransmits for MNP block (TX/RX) = 0/0
          Duration = 0:00:00, Number of TX/RX char = 0/0
          Local Disc Reason = Lost Carrier
          Remote Disc Reason = Unknown
00:39:53: Phone number event:
00:39:32: DTR event: DTR On
00:39:32: RS232 event: RTS  DTR* CTS  DSR  noDCD  noRI  noTST
```

Table 77 describes the significant fields shown in the display.

Table 77 show modem log Field Descriptions

Field	Description
Modem <slot/port> Events Log:	The modem for which log events are currently displayed.
Startup Response:	List of information describing the modem type, modem firmware, and DSP controller version (for 56K modems only).
Control Reply	Indicates the events the modem will be monitoring.
RS232 event	Detected modem signaling.
Modem State event	Current state of the modem, which can be any of the following: • Conn—Modem is connected to a remote host. • Bad—Inoperable state, which is configured by the **modem bad** command. • Bad*—Inoperable state, which is configured by the **modem startup-test** command during initial power-up testing. • Reset—Modem is in reset mode. • D/L—Modem is downloading firmware. • Bad FW—Downloaded modem firmware is not operational. • Busy—Modem is out of service and not available for calls. • Idle—Modem is ready for incoming and outgoing calls.

Table 77 show modem log Field Descriptions (continued)

Field	Description
End connection event	Descriptions or reasons why a connection was terminated: • Duration—Time a connection (in hours: minutes: seconds) was up between the local and remote devices. • Number of TX/RX char—Transmit and receive characters exchanged during the connection time. • Local or Remote Disc Reason—Reason the local or remote modem disconnected: – Lost Carrier—The modem firmware detects a drop in Carrier Detect during a connection. – DSP Task Hung—The DSP chip malfunctioned and failed to reset.
Phone number event	Descriptive information about the last dialed or current phone number.

The **show modem log** command shows the progress of leased line connections. The following example is taken from a Cisco 2600 series router configured for a leased line. Note the "LL Answering" state and "LL Answer" in the "Direction" field of the connection report:

```
Router# show modem log

  00:44:03.884 DTR set high
  00:44:02.888 Modem enabled
  00:43:57.732 Modem disabled
  00:43:52.476 Modem State: LL Answering
  00:43:52.476 CSM: event-MODEM_STARTING_CONNECT New State-CSM_CONNECT_INITIATED_STATE
  00:43:51.112 Modem State: Waiting for Carrier
  00:43:43.308 Modem State: Connected
  00:43:42.304 Connection: TX/RX Speed = 33600/33600, Modulation = V34
  Direction = LL Answer, Protocol = MNP, Compression = V42bis
  00:43:42.304 CSM: event-MODEM_CONNECTED New State-CONNECTED_STATE
  00:43:42.300 RS232: noCTS* DSR* DCD* noRI noRxBREAK TxBREAK*
  00:43:41.892 PPP mode active
  00:43:41.892 Modem enabled
  00:43:39.888 PPP escape maps set: TX map=00000000 RX map=FFFFFFFF
  00:43:39.724 PPP escape maps set: TX map=00000000 RX map=000A0000
  00:43:34.444 RS232: CTS* DSR DCD noRI noRxBREAK TxBREAK
  00:43:11.716 Modem Analog Report: TX = -20, RX = -34, Signal to noise = 61
```

Table 78 describes the significant fields shown in the display.

Table 78 show modem log Field Descriptions

Field	Description
Modem <slot/port> Events Log:	The modem for which log events are currently displayed.
Startup Response:	List of information describing the modem type, modem firmware, and DSP controller version (for 56K modems only).
Control Reply	Indicates the events the modem will be monitoring.
RS232 event	Detected modem signaling.

Table 78 show modem log Field Descriptions (continued)

Field	Description
Modem State event	Current state of the modem, which can be any of the following: • Conn—Modem is connected to a remote host. • Bad—Inoperable state, which is configured by the modem bad command. • Bad*—Inoperable state, which is configured by the modem startup-test command during initial power-up testing. • Reset—Modem is in reset mode. • D/L—Modem is downloading firmware. • Bad FW—Downloaded modem firmware is not operational. • Busy—Modem is out of service and not available for calls. • Idle—Modem is ready for incoming and outgoing calls.
End connection event	Descriptions or reasons why a connection was terminated: • Duration—Time a connection was up between the local and remote devices. • Number of TX/RX char—Transmit and receive characters exchanged during the connection time. • Local or Remote Disc Reason—Reason the local or remote modem disconnected: – Lost Carrier—The modem firmware detects a drop in Carrier Detect during a connection. – DSP Task Hung—The DSP chip malfunctioned and failed to reset. – Phone number event—Descriptive information about the last dialed or current phone number.

Related Commands

Command	Description
show modem configuration	Displays the current modem configuration for digital MICA technologies modems loaded inside access servers or routers.
show modem mica	Displays information about MICA technologies digital modems.
show modem operational-status	Displays the current modem operational status for MICA digital modems loaded in access servers or routers.
show modemcap	Displays the values set for the current modem and lists the modems for which the router has entries.

show modem log (pvdm2)

To display the modem history event status performed on a manageable modem on a PVDM2-xxDM device, use the **show modem log** command in privileged EXEC mode.

show modem log *slot/modem number*

Syntax Description

slot/modem number	(Optional) Slot and modem number. If this number is not specified, statistics for all connected modems are displayed. (Include the forward slash (**/**) when entering this variable.)

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(11)XW	This command was introduced.

Examples

The following is sample output from the **show modem log** command issued on a Cisco PVDMII-xxDM device with V12 digital modems. A specific modem, 0/323, is designated.

```
Router# show modem log 0/323
Modem 0/322 V12: Event Log contains 72 Events:
 00:15:31.116 CSM: Incoming call from Unknown to 223
 00:15:31.116 CSM: event-ISDN_CALL New State-IC_MODEM_RESERVED
    CSM: status-1 dchan-0/3 bchan-0
 00:15:31.068 Cmd: PCMENCODE
 00:15:31.068 Cmd: CMDDAT Config Change ATS
 5B 0D DF 17
 00:15:31.068 CSM: event-ISDN_CONNECTED New State-WAIT_FOR_CARRIER
 00:15:31.036 CSM: event-CSM_EVENT_MODEM_SETUP New State-WAIT_FOR_CARRIER
 00:15:31.036 Ntf: PCMENCODE
 00:15:31.032 Ntf: CMDDAT Config Acknowledge ATS
 Pass Pass
 00:15:31.032 Ntf: CMDREQ
 00:15:31.012 Cmd: LINECON
 00:15:31.012 Ntf: ANSDET
 00:15:14.092 Cmd: CMDDAT Statistic--Data Transfer Information

 00:15:14.092 CSM: event-MODEM_CONNECTED New State-CONNECTED_STATE
 00:15:14.092 Ntf: CHANCON
 00:15:14.088 Ntf: CMDDAT Statistic--Data Transfer Information
 Error correction               77    LAP-M
 Data compression               68    V44
 Modulation type                206   V.34
 receive speed                  16    33600
 transmit speed                 16    33600
 error correction frames sent   0
 error correction frames rcvd   0
 characters transmitted         0
 characters received            0
 synchronous frames sent        0
 synchronous frames rcvd        0
 bad synchronous frames rcvd    0
```

```
reject frames sent              0
reject frames rcvd              0
total retransmissions           0

00:15:16.080 Ntf: CMDREQ
00:15:16.076 Ntf: DCERPT
00:15:16.076 Cmd: SETSYNC
00:15:16.072 Ntf: CONFIGACK
00:15:13.844 Cmd: ACCMTX
00:15:13.844 Cmd: ACCMRX
00:15:13.840 Ntf: CONFIGACK
00:15:13.840 Ntf: CONFIGACK
00:15:13.600 Cmd: ACCMTX
00:15:13.600 Cmd: ACCMRX
00:15:13.600 Ntf: CONFIGACK
00:15:13.596 Ntf: CONFIGACK
00:13:24.384 Cmd: CMDDAT Statistic--Data Transfer Information


00:13:24.380 Ntf: CMDDAT Statistic--Data Transfer Information
Error correction                77    LAP-M
Data compression                68    V44
Modulation type                 206   V.34
receive speed                   16    33600
transmit speed                  16    33600
error correction frames sent    7
error correction frames rcvd    12
characters transmitted          218
characters received             487
synchronous frames sent         7
synchronous frames rcvd         12
bad synchronous frames rcvd     0
reject frames sent              0
reject frames rcvd              0
total retransmissions           0

00:13:44.996 Ntf: CMDREQ
00:13:44.996 Cmd: CMDDAT Statistic--Call Summary Information

00:13:44.992 Ntf: CMDDAT Statistic--Call Summary Information
Disconnect reason               21    Clears previous disconnect reason
Retrain/rate renegotiate reason 0     None
Connection time (hours)         0
Connection time (minutes)       1
Connection time (seconds)       53
Initial receive speed           16    33600
Initial transmit speed          16    33600
Maximum receive speed           16    33600
Maximum transmit speed          16    33600
Minimum receive speed           16    33600
Minimum transmit speed          16    33600
Max retransmit for one frame    1
Total retransmit during connect 0
Minimum EQM                     17
Maximum EQM                     24
Negative EQMs                   0
Minimum SNR                     27    31 dB
Maximum SNR                     27    31 dB
Retrains requested locally      0
Retrains requested remotely     0
Rate renegotiation req locally  0
Rate renegotiation req remotely 0

00:13:47.140 Ntf: CMDREQ
```

```
 00:13:45.436 Cmd: CMDDAT Statistic--DSP Information

 00:13:45.432 Ntf: CMDDAT Statistic--DSP Information
Raw AGC value                   94
 Last EQM                       20
 Transmit symbol rate           5     3429
 Receive symbol rate            5     3429
 Transmit carrier frequency     0     1959 (low)
 Receive carrier frequency      0     1959 (low)
 Minimum AGC reading            94
 Maximum AGC reading            94
 Transmit level                 13
 Remote req tx level reduction  2
 SNR                            27    31 dB
 Transmit non-linear encoding   1     On
 Receive non-linear encoding    1     On
 Transmit precoding             1     On
 Receive precoding              1     On
 Transmit shaping               16
 Receive shaping                16
 Trellis mapping                0     16-state
 Transmit pre-emphasis index    0
 Raw round trip delay           424
 EQM sum low                    0
 EQM sum medium                 0
 EQM sum high                   0

 00:14:18.796 Ntf: CMDREQ
 00:14:17.396 Cmd: CMDDAT Statistic--Digital Impairments

 00:14:17.392 Ntf: CMDDAT Statistic--Digital Impairments
 Ditital pad detected           0
 RBS pattern                    0
 Rate drop due to RBS           255
 V.90 minimum distance (high)   0
 V.90 minimum distance (low)    0
 Raw V.90 digital pad val (high) 255
 Raw V.90 digital pad val (low)  255

 00:14:17.392 Ntf: CMDREQ
 00:14:17.392 Cmd: CMDDAT Statistic--V.8bis(proprietary flex) Information

 00:14:17.388 Ntf: CMDDAT Statistic--V.8bis(proprietary flex) Information
 Negotiation status             74    RLSD on
                                      K56flex/K56Plus negotiation failed
                                      V.90 negotiation not tried
                                      V.90/K56flex negotiation failed
 Non-standard V.8bis Octet 13   148   K56flex (generic)
 Non-standard V.8bis Octet 14   129   Conexant Conexant-based
 Non-standard V.8bis Octet 15   131   K56flex capable, Last byte,
 Non-standard V.8bis Octet 16   66    flex version 0x2, Not prototype,
                                      Server, Not last byte,
 Non-standard V.8bis Octet 17   0     Not last byte,
                                      Conexant data pump revision 0x0
 Non-standard V.8bis Octet 18   0     u-law, x-law not forced,
                                      Not last byte,
                                      Conexant controller revision 0x0

 00:14:18.884 Ntf: CMDREQ
 00:12:09.636 Cmd: CMDDAT Statistic--Data Transfer Information

 00:12:09.632 Ntf: CMDDAT Statistic--Data Transfer Information
 Error correction               77    LAP-M
 Data compression               68    V44
```

```
Modulation type                 206   V.34
receive speed                   16    33600
transmit speed                  16    33600
error correction frames sent    7
error correction frames rcvd    12
characters transmitted          218
characters received             487
synchronous frames sent         7
synchronous frames rcvd         12
bad synchronous frames rcvd     0
reject frames sent              0
reject frames rcvd              0
total retransmissions           0

00:12:10.664 Ntf: CMDREQ
00:12:35.372 Cmd: CMDDAT Statistic--Call Summary Information

00:12:35.368 Ntf: CMDDAT Statistic--Call Summary Information
Disconnect reason               21    Clears previous disconnect reason
Retrain/rate renegotiate reason 0     None
Connection time (hours)         0
Connection time (minutes)       4
Connection time (seconds)       5
Initial receive speed           16    33600
Initial transmit speed          16    33600
Maximum receive speed           16    33600
Maximum transmit speed          16    33600
Minimum receive speed           16    33600
Minimum transmit speed          16    33600
Max retransmit for one frame    1
Total retransmit during connect 0
Minimum EQM                     17
Maximum EQM                     25
Negative EQMs                   0
Minimum SNR                     27    31 dB
Maximum SNR                     27    31 dB
Retrains requested locally      0
Retrains requested remotely     0
Rate renegotiation req locally  0
Rate renegotiation req remotely 0

00:12:36.400 Ntf: CMDREQ
00:12:35.596 Cmd: CMDDAT Statistic--DSP Information

00:13:01.796 Ntf: CMDDAT Statistic--DSP Information
Raw AGC value                   94
Last EQM                        19
Transmit symbol rate            5     3429
Receive symbol rate             5     3429
Transmit carrier frequency      0     1959 (low)
Receive carrier frequency       0     1959 (low)
Minimum AGC reading             94
Maximum AGC reading             94
Transmit level                  13
Remote req tx level reduction   2
SNR                             27    31 dB
Transmit non-linear encoding    1     On
Receive non-linear encoding     1     On
Transmit precoding              1     On
Receive precoding               1     On
Transmit shaping                16
Receive shaping                 16
Trellis mapping                 0     16-state
Transmit pre-emphasis index     0
```

```
Raw round trip delay            424
EQM sum low                     0
EQM sum medium                  0
EQM sum high                    0

00:13:02.832 Ntf: CMDREQ
00:13:01.792 Cmd: CMDDAT Statistic--Digital Impairments

00:13:01.788 Ntf: CMDDAT Statistic--Digital Impairments
Ditital pad detected            0
RBS pattern                     0
Rate drop due to RBS            255
V.90 minimum distance (high)    0
V.90 minimum distance (low)     0
Raw V.90 digital pad val (high) 255
Raw V.90 digital pad val (low)  255

00:13:02.784 Ntf: CMDREQ
00:13:01.748 Cmd: CMDDAT Statistic--V.8bis(proprietary flex) Information

00:13:01.744 Ntf: CMDDAT Statistic--V.8bis(proprietary flex) Information
Negotiation status              74    RLSD on
                                      K56flex/K56Plus negotiation failed
                                      V.90 negotiation not tried
                                      V.90/K56flex negotiation failed
Non-standard V.8bis Octet 13    148   K56flex (generic)
Non-standard V.8bis Octet 14    129   Conexant Conexant-based
Non-standard V.8bis Octet 15    131   K56flex capable, Last byte,
Non-standard V.8bis Octet 16    66    flex version 0x2, Not prototype,
                                      Server, Not last byte,
Non-standard V.8bis Octet 17    0     Not last byte,
                                      Conexant data pump revision 0x0
Non-standard V.8bis Octet 18    0     u-law, x-law not forced,
                                      Not last byte,
                                      Conexant controller revision 0x0

00:13:02.776 Ntf: CMDREQ
00:06:19.580 Cmd: CMDDAT Statistic--Data Transfer Information

00:06:21.296 Ntf: CMDDAT Statistic--Data Transfer Information
Error correction                77    LAP-M
Data compression                68    V44
Modulation type                 206   V.34
receive speed                   16    33600
transmit speed                  16    33600
error correction frames sent    7
error correction frames rcvd    12
characters transmitted          218
characters received             487
synchronous frames sent         7
synchronous frames rcvd         12
bad synchronous frames rcvd     0
reject frames sent              0
reject frames rcvd              0
total retransmissions           0

00:06:21.300 Ntf: CMDREQ
00:06:21.300 Cmd: CMDDAT Statistic--Call Summary Information

00:06:21.296 Ntf: CMDDAT Statistic--Call Summary Information
Disconnect reason               21    Clears previous disconnect reason
Retrain/rate renegotiate reason 0     None
Connection time (hours)         0
Connection time (minutes)       10
```

```
Connection time (seconds)       51
Initial receive speed           16    33600
Initial transmit speed          16    33600
Maximum receive speed           16    33600
Maximum transmit speed          16    33600
Minimum receive speed           16    33600
Minimum transmit speed          16    33600
Max retransmit for one frame    1
Total retransmit during connect 0
Minimum EQM                     17
Maximum EQM                     25
Negative EQMs                   0
Minimum SNR                     27    31 dB
Maximum SNR                     27    31 dB
Retrains requested locally      0
Retrains requested remotely     0
Rate renegotiation req locally  0
Rate renegotiation req remotely 0

00:07:22.856 Ntf: CMDREQ
00:07:21.828 Cmd: CMDDAT Statistic--DSP Information

00:07:21.824 Ntf: CMDDAT Statistic--DSP Information
Raw AGC value                   94
Last EQM                        21
Transmit symbol rate            5     3429
Receive symbol rate             5     3429
Transmit carrier frequency      0     1959 (low)
Receive carrier frequency       0     1959 (low)
Minimum AGC reading             94
Maximum AGC reading             94
Transmit level                  13
Remote req tx level reduction   2
SNR                             27    31 dB
Transmit non-linear encoding    1     On
Receive non-linear encoding     1     On
Transmit precoding              1     On
Receive precoding               1     On
Transmit shaping                16
Receive shaping                 16
Trellis mapping                 0     16-state
Transmit pre-emphasis index     0
Raw round trip delay            424
EQM sum low                     0
EQM sum medium                  0
EQM sum high                    0

00:07:23.216 Ntf: CMDREQ
00:07:22.180 Cmd: CMDDAT Statistic--Digital Impairments

00:07:22.176 Ntf: CMDDAT Statistic--Digital Impairments
Ditital pad detected            0
RBS pattern                     0
Rate drop due to RBS            255
V.90 minimum distance (high)    0
V.90 minimum distance (low)     0
Raw V.90 digital pad val (high) 255
Raw V.90 digital pad val (low)  255

00:07:22.176 Ntf: CMDREQ
00:07:23.208 Cmd: CMDDAT Statistic--V.8bis(proprietary flex) Information

00:07:24.824 Ntf: CMDDAT Statistic--V.8bis(proprietary flex) Information
Negotiation status              74    RLSD on
```

```
                                        K56flex/K56Plus negotiation failed
                                        V.90 negotiation not tried
                                        V.90/K56flex negotiation failed
 Non-standard V.8bis Octet 13    148    K56flex (generic)
 Non-standard V.8bis Octet 14    129    Conexant Conexant-based
 Non-standard V.8bis Octet 15    131    K56flex capable, Last byte,
 Non-standard V.8bis Octet 16    66     flex version 0x2, Not prototype,
                                        Server, Not last byte,
 Non-standard V.8bis Octet 17    0      Not last byte,
                                        Conexant data pump revision 0x0
 Non-standard V.8bis Octet 18    0      u-law, x-law not forced,
                                        Not last byte,
                                        Conexant controller revision 0x0

 00:07:25.856 Ntf: CMDREQ

Router#
```

Table 79 describes the major fields shown in the display.

Table 79 show modem log Field Descriptions for V12 Modems

Field	Description
CSM	PVDM2-xxDM internal state machine commands.
Cmd	Commands sent from Cisco IOS software to V12 modems.
Ntf	Notifications sent from V12 modems to Cisco IOS software.

Related Commands

Command	Description
show modem configuration (pvdm2)	Displays the current modem configuration for V12 digital modems on PVDM2-xxDM devices.
show modem operational-status (pvdm2)	Displays the current modem operational status for V12 digital modems on PVDM2-xxDM devices.
show modemcap	Displays the values set for the current modem and lists the modems for which the router has entries.

show modem mapping

To display a snapshot of all the firmware versions running on all the modems in the access server, use the **show modem mapping** command in EXEC mode.

show modem mapping

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3T	This command was introduced.

Usage Guidelines

This command is useful for managing and monitoring multiple versions of modem firmware running in an access server. This command also shows the source location of each version of firmware (for example, running out of Flash or boot Flash memory, or bundled with Cisco IOS software).

Firmware can also be copied from a local TFTP server to the onboard modems. For the Cisco AS5300, issue the **copy tftp flash** command followed by the **copy flash modem** command. The Cisco AS5300 stores individual firmware files that are not bundled with the Cisco IOS software in Flash memory. For the Cisco AS5200, issue the **copy tftp bootflash** command followed by the **copy bootflash modem** command. The Cisco AS5200 stores individual firmware files not bundled with the Cisco IOS software in boot Flash memory.

All the modems in a single MICA technologies modem module run the same version of firmware (for example, modems 1/0 through 1/5 in module 0). However, different versions of modem firmware can exist between different modem modules (for example, module 0 and module 1).

Individual firmware files cannot be erased from Flash or boot Flash memory. The entire contents of Flash or boot Flash memory must be deleted during the erase operation. If you do this delete, be sure to back up your Cisco IOS software and running configuration *before* you erase your system's Flash or boot Flash memory.

Note The Cisco AS5800 does not support the **show modem mapping** command. Use the **show modem bundled-firmware** command instead.

Examples

The following is sample output from the **show modem mapping** EXEC command. This access server is loaded with MICA and Microcom modems.

```
Router# show modem mapping

Slot 1 has Mica Carrier card.


        Modem       Firmware   Firmware
Module  Numbers     Rev        Filename
  0   1/0  - 1/5   2.0.1.7    IOS-Defaults
  1   1/6  - 1/11  2.0.1.7    IOS-Defaults
  2   1/12 - 1/17  2.0.1.7    IOS-Defaults
  3   1/18 - 1/23  2.0.1.7    IOS-Defaults
  4   1/24 - 1/29  2.0.1.7    IOS-Defaults
  5   1/30 - 1/35  2.0.1.7    IOS-Defaults
  6   1/36 - 1/41  2.0.1.7    IOS-Defaults
  7   1/42 - 1/47  2.2.3.0    flash:mica-modem-portware.2.2.3.0.bin

Slot 2 has Microcom Carrier card.

      Module  Firmware     Firmware
Mdm   Number  Rev          Filename
2/0      0    3.2(10)      flash:mcom-modem-code-3.2.10.bin
2/1      0    3.1(30)      IOS-Defaults
2/2      0    3.1(30)      IOS-Defaults
2/3      0    3.1(30)      IOS-Defaults
2/4      0    3.1(30)      IOS-Defaults
2/5      0    3.1(30)      IOS-Defaults
2/6      0    3.1(30)      IOS-Defaults
2/7      0    3.1(30)      IOS-Defaults
2/8      0    3.1(30)      IOS-Defaults
2/9      0    3.1(30)      IOS-Defaults
2/10     0    3.1(30)      IOS-Defaults
2/11     0    3.1(30)      IOS-Defaults
2/12     1    3.1(30)      IOS-Defaults
2/13     1    3.1(30)      IOS-Defaults
2/14     1    3.1(30)      IOS-Defaults
2/15     1    3.1(30)      IOS-Defaults
2/16     1    3.1(30)      IOS-Defaults
2/17     1    3.1(30)      IOS-Defaults
2/18     1    3.1(30)      IOS-Defaults
2/19     1    3.1(30)      IOS-Defaults
2/20     1    3.1(30)      IOS-Defaults
2/21     1    3.1(30)      IOS-Defaults
2/22     1    3.1(30)      IOS-Defaults
2/23     1    3.1(30)      IOS-Defaults

IOS Bundled Firmware Information:

Mica Boardware Version : 1.3.4.5
Mica Portware Version : 2.0.1.7
Microcom Firmware Version : 3.1.30
Microcom DSP Software Version : 1.01

 Firmware files on Boot Flash:

Firmware-file                                        Version  Firmware-Type
=============                                        =======  =============

Firmware files on System Flash:
```

```
Firmware-file                                    Version  Firmware-Type
=============                                    =======  =============
flash:mcom-modem-code-3.2.10.bin                 3.2.10   Microcom F/W and DSP
flash:mica-modem-portware.2.2.3.0.bin            2.2.3.0  Mica Portware
```

Table 80 describes the significant fields shown in the display.

Table 80 show modem mapping Field Descriptions

Field	Description
Slot *x* has card	Type of modem card inserted in the specified slot.
Module	Modem module number that corresponds with the specified modem or group of modems.
Modem numbers	Range of specified modems, which are displayed as slot/port.
Mdm	Specified modem number, which is displayed as slot/port.
Firmware Rev	Version of firmware running on the modem or module. Each time the access server reloads, this version of firmware is copied to the specified modem or range of modems. The field "Unknown" is displayed when a modem is upgrading its firmware.
Firmware Filename	Location or filename of the firmware that is downloaded to the modems. A firmware file located in Flash memory begins as flash:filename. A file located in boot Flash memory begins as bootflash:filename. If the firmware is embedded or bundled in the Cisco IOS image, the field IOS-Defaults appears. On the Cisco AS5300, firmware files are stored in the system Flash memory. On the Cisco AS5200, firmware files are stored in boot Flash memory.
IOS Bundled Firmware Information:	List of firmware versions that are bundled with the Cisco IOS software running on the system. If the firmware versions in this section are more current than the firmware running on your modems, you should upgrade the running modem firmware.
Firmware files on Boot Flash:	List of current firmware located on boot Flash memory. The categories are Firmware-file, Version, and Firmware-Type.
Firmware files on System Flash:	List of current firmware located on the system Flash memory. The categories are Firmware-file, Version, and Firmware-Type.

Related Commands

Command	Description
copy	Copies any file from a source to a destination, including a source or destination URL for a TFTP network server, or for Flash memory.
copy modem	Copies modem firmware to integrated modems in an access server.
show modem bundled-firmware	Displays a list of bundled modem firmware images by slot (Cisco AS5800 access server only).

show modem mica

To display information about MICA technologies digital modems, use the **show modem mica** command in EXEC mode.

show modem mica {*slot/port* | **all** | **slot** [*slot-number*]}

Syntax Description

slot/port	Single modem in a MICA digital modem board. The slash mark is required.
all	All the MICA modems in the system.
slot *slot-number*	A particular slot, which is mainly used for debugging purposes. The optional *slot-number* argument allows you to specify a slot number.

Command Modes

EXEC

Command History

Release	Modification
11.2P	This command was introduced.

Usage Guidelines

Each MICA modem has its own data channel port, which is tied to its own TTY line. For example, modem 0/1 is tied to TTY line 2. To display data channel information for a single MICA modem, issue the **show modem mica** *slot/port* command.

All the modems on each MICA modem card share three pseudochannels for modem management functions, for example, the DC session channel, status polling channel, and controlling channel. To display statistics for each modem management channel, issue the **show modem mica all** command. The first channel you see displayed is the status polling channel (shown as SLOT/PORT (0/61) TTYNUM=-1 (MM Status Port)). The second displayed channel is the DC session channel (shown as SLOT/PORT (0/60) TTYNUM=-1 (MM DC Port)). The third displayed port is the controlling channel (shown as SLOT/PORT (0/62) TTYNUM=-1 (Control Port)). No TTY lines are associated with the modem management ports, as indicated by the field display TTYNUM=-1. An extensive list of all the data channels for each MICA modem is also displayed.

Examples

The following example displays the data port channel for modem 0/1. For a description of the significant fields shown in this display, see Table 81.

```
Router# show modem mica 0/1

SLOT/PORT (0/1) TTYNUM=2 (Data Port)
Modem hardware state: CTS noDSR  DTR RTS
RX Queue count is 0
TX Queue count is 1
TTY outpak is 0
TX pending FALSE
RX pending FALSE
RX ring with 4 entries at 0x40093184, (RX_AVAILABLE) rx_count=4
Rx_pak_head=0x6082B030 Rx_BD_head=0x4009318C Rx_BD_base=0x40093184
INPUT count = 12
00 pak=0x60753064 buf=0x40067514 status=8000 pak_size=0
```

```
01 pak=0x6082B030 buf=0x4013F948 status=8000 pak_size=0
02 pak=0x60A4323C buf=0x4021A214 status=8000 pak_size=0
03 pak=0x60A32DA0 buf=0x40208E9C status=8800 pak_size=0

TX ring with 4 entries at 0x400943F0, (TX_READY) tx_count = 0
tx_head = 0x400943F0 , head_txp = 0x0
Tx_bd_tail=0x400943F0 , Tx_bd_base=0x400943F0
OUTPUT count = 12
00 pak=0x0000000 buf=0x0000000 status=0000 pak_size=0
01 pak=0x0000000 buf=0x0000000 status=0000 pak_size=0
02 pak=0x0000000 buf=0x0000000 status=0000 pak_size=0
03 pak=0x0000000 buf=0x0000000 status=0800 pak_size=0
```

The following is sample output from the **show modem mica all** command. For a description of the significant fields shown in this display, see Table 81.

```
Router# show modem mica all

SLOT/PORT (0/60) TTYNUM=-1 (MM DC Port)
Modem hardware state: CTS DSR  DTR RTS
Board is running boardware version 1.3.2.0
Boardware redirect state = DISABLE  size=4520 location=0x400968A8
Board INTR ON
RX[0]=0x0 RX[1]=0x0 RX[2]=0x0 RX[3]=0x0
TX[0]=0x0 TX[1]=0x0 TX[2]=0x0 TX[3]=0x0
Next Modem service is 0
Throttle count is 0, Throttle state is OFF
Data channel no buffer count is 0
Boardware crash count is 0
No crash dump available
Board state is RUNNING
Modules state are: R R R R R R R R
Modules crash count are: 0 0 0 0 0 0 0 0
Interval timer is 16

RX Queue count is 0
TX Queue count is 0
TTY outpak is 0
TX pending FALSE
RX pending FALSE
RX ring with 4 entries at 0x400938E4, (RX_AVAILABLE) rx_count=4
Rx_pak_head=0x60761CE0 Rx_BD_head=0x400938F4 Rx_BD_base=0x400938E4
INPUT count = 2
00 pak=0x60761920 buf=0x4009025C status=8000 pak_size=0
01 pak=0x60761740 buf=0x4008FBA4 status=8000 pak_size=0
02 pak=0x60761CE0 buf=0x40090FCC status=8000 pak_size=0
03 pak=0x6084311C buf=0x40150608 status=8800 pak_size=0

TX ring with 4 entries at 0x40094B50, (TX_READY) tx_count = 0
tx_head = 0x40094B60 , head_txp = 0x0
Tx_bd_tail=0x40094B60 , Tx_bd_base=0x40094B50
OUTPUT count = 2
00 pak=0x0000000 buf=0x0000000 status=0000 pak_size=0
01 pak=0x0000000 buf=0x0000000 status=0000 pak_size=0
02 pak=0x0000000 buf=0x0000000 status=0000 pak_size=0
03 pak=0x0000000 buf=0x0000000 status=0800 pak_size=0

SLOT/PORT (0/61) TTYNUM=-1 (MM Status Port)
Modem hardware state: CTS DSR  DTR RTS
Board is running boardware version 1.3.2.0
Boardware redirect state = DISABLE  size=4520 location=0x400968A8
Board INTR ON
RX[0]=0x0 RX[1]=0x0 RX[2]=0x0 RX[3]=0x0
TX[0]=0x0 TX[1]=0x0 TX[2]=0x0 TX[3]=0x0
```

```
Next Modem service is 0
Throttle count is 0, Throttle state is OFF
Data channel no buffer count is 0
Boardware crash count is 0
No crash dump available
Board state is RUNNING
Modules state are: R R R R R R R R
Modules crash count are: 0 0 0 0 0 0 0 0
Interval timer is 16
```

The following is sample output from the **show modem mica slot** command. For a description of the significant fields shown in this display, see Table 81.

```
Router# show modem mica slot

SLOT/PORT (0/62) TTYNUM=-1 (Control Port)
Modem hardware state: CTS DSR  DTR RTS
Board is running boardware version 1.3.2.0
Boardware redirect state = DISABLE  size=4520 location=0x400968A8
Board INTR ON
RX[0]=0x0 RX[1]=0x0 RX[2]=0x0 RX[3]=0x0
TX[0]=0x0 TX[1]=0x0 TX[2]=0x0 TX[3]=0x0
Next Modem service is 0
Throttle count is 0, Throttle state is OFF
Data channel no buffer count is 0
Boardware crash count is 0
No crash dump available
Board state is RUNNING
Modules state are: R R R R R R R R
Modules crash count are: 0 0 0 0 0 0 0 0
Interval timer is 16

RX Queue count is 0
TX Queue count is 0
TTY outpak is 0
TX pending FALSE
RX pending FALSE
RX ring with 4 entries at 0x40093924, (RX_AVAILABLE) rx_count=4
Rx_pak_head=0x6075D4D8 Rx_BD_head=0x40093934 Rx_BD_base=0x40093924
INPUT count = 1366
00 pak=0x6075CD58 buf=0x4008A2BC status=8000 pak_size=0
01 pak=0x6075D6B8 buf=0x4008C454 status=8000 pak_size=0
02 pak=0x6075D4D8 buf=0x4008BD9C status=8000 pak_size=0
03 pak=0x6075D2F8 buf=0x4008B6E4 status=8800 pak_size=0

TX ring with 4 entries at 0x40094B90, (TX_READY) tx_count = 0
tx_head = 0x40094BA0 , head_txp = 0x0
Tx_bd_tail=0x40094BA0 , Tx_bd_base=0x40094B90
OUTPUT count = 1894
00 pak=0x0000000 buf=0x0000000 status=0000 pak_size=0
01 pak=0x0000000 buf=0x0000000 status=0000 pak_size=0
02 pak=0x0000000 buf=0x0000000 status=0000 pak_size=0
03 pak=0x0000000 buf=0x0000000 status=0800 pak_size=0
```

The first channel you see displayed is the status polling channel (shown as SLOT/PORT (0/62) TTYNUM=-1 (MM Status Port)). The second displayed channel is the DC session channel (shown as SLOT/PORT (0/60) TTYNUM=-1 (MM DC Port)). The third displayed port is the controlling channel (shown as SLOT/PORT (0/62) TTYNUM=-1 (Control Port)). No TTY lines are associated with the modem management ports, as indicated by the field display TTYNUM=-1. An extensive list of all the data channels for each individual MICA modem is displayed.

Table 81 describes the significant fields shown in the displays.

Table 81 show modem mica Field Descriptions

Field	Description
SLOT/PORT (0/61) TTYNUM=-1 (MM Status Port)	Status polling channel.
SLOT/PORT (0/60) TTYNUM=-1 (MM DC Port)	DC session channel.
SLOT/PORT (0/62) TTYNUM=-1 (Control Port)	Controlling pseudochannel.
Modem hardware state:	State of the modem hardware, which can be CTS, DSR, DTR, and RTS.
Board is running boardware version	Version of boardware.
Boardware crash count	Number of times the board has crashed since the system was last power cycled.
Modules state are:	State of the modem modules. R means that the specified modem module is running.
Modules crash count are:	Number of times each modem module has crashed since the system was last power cycled.
INPUT count =	Count of packets received since the last power cycle.
OUTPUT count =	Count of packets transmitted since the last power cycle.

Related Commands

Command	Description
show modem configuration	Displays the current modem configuration for digital MICA technologies modems loaded inside access servers or routers.
show modem log	Displays the modem history event status performed on a manageable modem or group of modems.
show modem operational-status	Displays the current modem operational status for MICA technologies digital modems loaded in access servers or routers.

show modem operational-status

To display performance statistics for individual modems, use the **show modem operational-status** command in EXEC mode.

Cisco 3600 Series and Cisco AS5300 Universal Access Servers

show modem operational-status {*slot* | *slot*/*port*}

Cisco AS5800 Universal Access Servers

show modem operational-status [*shelf*/*slot*/*port*]

Syntax Description

slot	(Optional) Slot number.
slot/*port*	(Optional) Location of the slot and modem port. If these numbers are not specified, statistics for all connected modems are displayed. You must include the slash mark.
shelf/*slot*/*port*	(Optional) On Cisco AS5800 universal access servers, specifies the shelf, slot, and modem port. If these numbers are not specified, statistics for all connected modems are displayed. You must type in the forward slashes (/).

Command Modes

EXEC

Command History

Release	Modification
11.2(10)P	This command was introduced on the Cisco AS5400.
12.1(5)T	This command was enhanced to display information about modems on the Cisco 3600 series.
12.2(2)XA	This command was enhanced to display additional information on disconnection reasons and states.
12.2(2)XB	This command was integrated into Cisco IOS Release 12.2(2)XB.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for Cisco AS5300 and Cisco AS5800 platforms.

Usage Guidelines

The **show modem operational-status** command is supported on access servers with internal MICA technologies or Microcom analog (NM-AM) modems, but not on servers with internal Microcom digital modems.

To display performance statistics for Cisco AS3600 access servers with other modem types, use the following command sequence:

```
Router# modem at-mode s/p
AT@E1
```

Sample output and explanations of the **AT@E1** modem command are provided in the document *AT Command Set and Register Summary for Analog Modem Network Modules*, found in the Analog Modem Firmware index of the Cisco 3600 Series Router documentation on Cisco.com.

To display the operational status of a specific modem port or port range for the Cisco AS5400 and AS5800 access servers, use the **show port operational-status** command.

Examples

The following example shows performance statistics for modem 0/0 on a Cisco 3600 series router network module:

```
Router# show modem operational-status 0/0

Modem (0/0) Operational Status:
 Parameter #0  Disconnect Reason Info:  (0x0)
       Type (=0 ):  <unknown>
      Class (=0 ):  Other
     Reason (=0 ):  no disconnect has yet occurred
 Parameter #1  Connect Protocol:  ISDN Mode
 Parameter #2  Compression:  None
 Parameter #3  EC Retransmission Count:  0
 Parameter #4  Self Test Error Count:  0
 Parameter #5  Call Timer:  179077 secs
 Parameter #6  Total Retrains:  0
 Parameter #7  Sq Value:  7
 Parameter #8  Connected Standard:  ISDN
 Parameter #9  TX,RX Bit Rate:  2400, 2400
 Parameter #11 TX,RX Symbol Rate:  0, 0
 Parameter #13 TX,RX Carrier Frequency:  0, 0
 Parameter #15 TX,RX Trellis Coding:  (n/a), (n/a)
 Parameter #16 TX,RX Preemphasis Index:  0, 0
 Parameter #17 TX,RX Constellation Shaping:  (n/a), (n/a)
 Parameter #18 TX,RX Nonlinear Encoding:  (n/a), (n/a)
 Parameter #19 TX,RX Precoding:  (n/a), (n/a)
 Parameter #20 TX,RX Xmit Level Reduction:  0, 0 dBm
 Parameter #21 Signal Noise Ratio:  0 dB
 Parameter #22 Receive Level:  0 dBm
 Parameter #23 Frequency Offset:  0 Hz
 Parameter #24 Phase Jitter Frequency:  0 Hz
 Parameter #25 Phase Jitter Level:  0 degrees
 Parameter #26 Far End Echo Level:  0 dBm
 Parameter #27 Phase Roll:  0 degrees
 Parameter #28 Round Trip Delay:  0 msecs
 Parameter #30 Characters transmitted, received:  39483250, 41069212
 Parameter #32 General Portware Information:  0
 Parameter #33 PPP/SLIP packets transmitted, received:  774185, 774894
 Parameter #35 PPP/SLIP packets received (BAD/ABORTED):  0
 Parameter #36 EC packets transmitted, received OK:  0, 0
 Parameter #38 EC packets (Received BAD/ABORTED):  0
 Parameter #39 Robbed Bit Signalling (RBS) pattern:  0
 Parameter #40 Digital Pad:  (n/a),  Digital Pad Compensation: None
 Parameter #41 V110/PIAFS frames received bad:  0
 Parameter #42 V110/PIAFS frames received good:  0
 Parameter #43 V110/PIAFS frames transmitted:  0
 Parameter #44 V110/PIAFS sync lost:  0

Line Shape:
..............................................................................*
..............................................................................*
..............................................................................*
..............................................................................*
..............................................................................*
..............................................................................*
..............................................................................*
..............................................................................*
..............................................................................*
```

```
.....................................................................*
.....................................................................*
.....................................................................*
.....................................................................*
.....................................................................*
.....................................................................*
```

The following example shows performance statistics for modem 0/1 on a Cisco AS5300. This modem is located at slot 0, port 1. For a description of the output fields, refer to Table 82.

```
Router# show modem operational-status 0/1

 Modem(0/1) Operational-Status:
   Parameter #0 Disconnect Reason Info: (0xDF00)
                Type (=6 ): Tx (host to line) data flushing, OK
              Class (=31): Requested by host
            Reason (=0 ): non-specific host disconnect
   Parameter #1   Connect Protocol:   LAP-M
   Parameter #2   Compression:   V.42bis both
   Parameter #3   EC Retransmission Count:   1
   Parameter #4   Self Test Error Count:   0
   Parameter #5   Call Timer:   36 secs
   Parameter #6   Total Retrains:   1
   Parameter #7   Sq Value:   3
   Parameter #8   Connected Standard:   V.90
   Parameter #9   TX,RX Bit Rate:   48000, 28800
   Parameter #11   TX,RX Symbol Rate:   8000, 3200
   Parameter #13   TX,RX Carrier Frequency:   0, 1920
   Parameter #15   TX,RX Trellis Coding:   0, 16
   Parameter #16   TX,RX Preemphasis Index:   0, 6
   Parameter #17   TX,RX Constellation Shaping:   Off, Off
   Parameter #18   TX,RX Nonlinear Encoding:   Off, Off
   Parameter #19   TX,RX Precoding:   Off, Off
   Parameter #20   TX,RX Xmit Level Reduction:   0, 0 dBm
   Parameter #21   Signal Noise Ratio:   36 dB
   Parameter #22   Receive Level:   -19 dBm
   Parameter #23   Frequency Offset:   0 Hz
   Parameter #24   Phase Jitter Frequency:   0 Hz
   Parameter #25   Phase Jitter Level:   0 degrees
   Parameter #26   Far End Echo Level:   -65 dBm
   Parameter #27   Phase Roll:   0 degrees
   Parameter #28   Round Trip Delay:   3 msecs
   Parameter #30   Characters received, transmitted:   12, 0
   Parameter #32   Characters received BAD:   1
   Parameter #33   PPP/SLIP packets received, transmitted:   0, 0
   Parameter #35   PPP/SLIP packets received (BAD/ABORTED):   0
   Parameter #36   EC packets transmitted, received OK:   2, 0
   Parameter #38   EC packets (Received BAD/ABORTED):   1
   Parameter #39   Robbed bit Signalling (RBS) pattern:   0
   Parameter #40   Digital Pad:   4.125 dB, Digital Pad Compensation: None

Line Shape:
 ........................*
 .........................*
 .........................*
 .........................*
 .........................*
 .........................*
 .........................*
 .........................*
 .........................*
 .........................*
 .........................*
 .........................*
```

```
. . . . . .*
. . . . . .*
. . . . . .*
. . . . . .*
. . . . . .*
. . . . . .*
. . . . . .*
. . . . . .*
```

Table 82 show modem operational-status Field Descriptions for MICA Modems

Field	Description
Modem (slot/port) Operational Status:	This parameter identifies the modem.
Parameter #0 Disconnect Reason Info:	This parameter displays reasons for call disconnect.
Parameter #1 Connect Protocol:	This parameter displays the connect protocol for the current session, which can be synchronous (SYNC) mode, asynchronous (ASYNC) mode, AppleTalk Remote Access (ARA) 1.0, ARA 2.0, Link Access Procedure for Modems (LAP-M), Microcom Network Protocol (MNP), FAX mode, Signaling System 7/Continuity Test (SS7/COT), or ISDN Mode.
Parameter #2 Compression:	This parameter displays the compression protocol used for the current connection, which can be None, V.42*bis* TX (transmit), V.42*bis* RX (receive), V.42*bis* both, or MNP5 data compression.
Parameter #3 EC Retransmission Count:	This parameter displays the error correction (EC) retransmission count, or the number of times the MICA technologies modem has gone into error recovery in the TX direction for a particular connection. The higher the number, the worse the connection. However, compare this parameter against the count produced by Parameter #36 (EC packets transmitted, received) to determine if there really is a problem.
Parameter #4 Self Test Error Count:	This parameter displays the total errors generated during a self-test run.
Parameter #5 Call Timer:	This parameter displays the length of the call in seconds. The timer starts when the CONNECT modem state is reached.
Parameter #6 Total Retrains:	This parameter displays the count of total retrains and speed shifts.
Parameter #7 Sq Value:	This parameter displays the measure of the receive signal quality (SQ) bit error rate for the chosen modulation, as estimated by the Digital Signal Processor (DSP), where 0 is the highest BER value and 7 the lowest. Depending on the setting of the SQ Threshold (S32), the DSP seeks an SQ value somewhere between the highest and lowest levels. For example, if S32 = 2 (the default), an SQ value of 3 is sought. If the SQ value drops below the threshold for longer than the duration of S35, the DSP attempts a downward speed shift or retrain. Similarly, if the SQ value goes above the threshold for longer than S34, an upward speed shift or retrain is attempted.

Table 82 show modem operational-status Field Descriptions for MICA Modems (continued)

Field	Description
Parameter #8 Connected Standard:	This parameter displays the modulation, which can be V.21, Bell03, V.22, V.22*bis*, Bell212, V.23, V.32, V.32*bis*, V.32terbo, V.34, V.34+, K56Flex, V.90, V.110, or ISDN.
Parameter #9 TX, RX Bit Rate:	This parameter displays the TX bit rate from the local data communication equipment (DCE) to the remote DCE and the RX bit rate from the remote DCE to the local DCE. The following data carrier connect standards support the rates indicated in bits per second (bps): • V.21 TX, RX—300 bps • V.22 TX, RX—1200 bps • V.22*bis* TX, RX—2400 bps • V.23 TX (originate)—1200 bps • V.23 RX (originate)—75 bps • V.32 TX, RX—4800 and 9600 bps • V.32*bis* TX, RX—4800, 7200, 9600, 12000, and 14400 bps • V.34 TX, RX—2400, 4800, 7200, 9600, 12000, 14400, 16800, 19200, 21600, 24000, 26400, and 28800 bps • V.34+ TX, RX—2400, 4800, 7200, 9600, 12000, 14400, 16800, 19200, 21600, 24000, 26400, 28800, 31200, and 33600 bps • K56Flex TX—32000, 34000, 36000, 38000, 40000, 42000, 44000, 46000, 48000, 50000, 52000, 54000, 56000, 58000, and 60000 bps • K56Flex RX—2400, 4800, 7200, 9600, 12000, 14400, 16800, 19200, 21600, 24000, 26400, 28800, and 31200 bps • V.90 TX—28000, 29333, 30666, 32000, 33333, 34666, 36000, 37333, 38666, 40000, 41333, 42666, 44000, 45333, 46666, 48000, 49333, 50666, 52000, 53333, 54666, and 56000 bps • V.90 RX—2400, 4800, 7200, 9600, 12000, 14400, 16800, 19200, 21600, 24000, 26400, 28800, 31200, and 33600 bps • Bell103 TX, RX—Up to 300 bps • Bell212 TX, RX—0 to 300 and 1200 bps The following fax connect standards support the rates indicated in bps: • V.17 TX, RX—7200, 9600, 12000, and 14400 bps • V.27ter TX, RX—2400 and 4800 bps • V.29 TX, RX—7200 and 9600 bps

Table 82 show modem operational-status Field Descriptions for MICA Modems (continued)

Field	Description
Parameter #11 TX, RX Symbol Rate:	This parameter displays the TX symbol rate used to transmit samples to the line and the RX symbol rate used to receive samples from the line. The rates are synchronous with each other. The following data carrier connect standards support the indicated bit rates: • V.21 TX, RX—300 bps • V.22 TX, RX—600 bps • V.22*bis* TX, RX—600 bps • V.23 TX (originate)—1200 bps • V.23 RX (originate)—75 bps • V.23 TX (answer)—75 bps • V.23 RX (answer)—1200 bps • V.32 TX, RX—2400 bps • V.32*bis* TX, RX—2400 bps • V.34 TX, RX—2400, 2743, 2800, 3000, 3200, and 3429 bps • V.34+ TX,RX—2400, 2743, 2800, 3000, 3200, and 3429 bps • K56Flex TX—8000 bps • K56Flex RX—3200 bps • V.90 TX—8000 bps • V.90 RX—3000, 3200, and 3429 bps • Bell103 TX, RX—300 bps • Bell212 TX, RX—600 bps The following fax connect standards support the indicated bit rates: • V.17 TX, RX—2400 bps • V.27ter TX, RX—1800 bps • V.29 TX, RX—2400 bps

Table 82 show modem operational-status Field Descriptions for MICA Modems (continued)

Field	Description
Parameter #13 TX, RX Carrier Frequency:	This parameter displays the TX carrier frequency used by the local DCE and the RX carrier frequency used by the remote DCE. Data carrier frequencies are as follows: • V.21 TX RX—1080 Hz (originate) and 1750 Hz (answer) • V.22 TX, RX—1200 Hz (originate) and 2400 Hz (answer) • V.22*bis* TX, RX—1200 Hz (originate) and 2400 Hz (answer) • V.23 TX (originate)—1700 Hz • V.23 RX (originate)—420 Hz • V.23 TX (answer)—420 Hz • V.23 RX (answer)—1700 Hz • V.32 TX, RX—1800 Hz • V.32*bis* TX, RX—1800 Hz • V.34 TX, RX—1600, 1800, 1646, 1680, 1829, 1829, 1867, 1900, 1920, 1959 Hz • V.34+ TX, RX—1600, 1800, 1646, 1680, 1829, 1829, 1867, 1900, 1920, 1959 Hz • K56Flex TX—Does not apply. • K56Flex RX—1600, 1800, 1646, 1680, 1829, 1829, 1867, 1900, 1920, 1959 Hz • V90 TX—Does not apply. • V90 RX—1600, 1800, 1646, 1680, 1829, 1829, 1867, 1900, 1920, 1959 Hz • Bell103 TX, RX—1080 Hz (originate) and 1750 Hz (answer) • Bell212 TX, RX—1200 Hz (originate) and 2400 Hz (answer) Fax carrier frequencies are as follows: • V.17 TX, RX—1800 Hz • V.27ter TX, RX—1200 (originate) and 1600 (answer) • V.29 TX, RX—1700 Hz
Parameter #15 TX, RX Trellis Coding:	Trellis coding adds dependency between symbols to make the detection in noise more robust (Forward Error Correction). Trellis coding is displayed in values of 0, 8, 16, 32, or 64. Use the following key to correlate the trellis code values with the connection standard: • 0—V.22, V.22*bis*, V.21, Bell212, Bell103, V.29, or V.27 • 8—V.32, V.32*bis*, or V.17 • 16, 32, 64—V.34, V.34+, V.90, K56Flex **Note** MICA technologies modems do not support values of 32 or 64 in the RX direction, but do support values of 16, 32, and 64 in the TX direction.

Table 82 show modem operational-status Field Descriptions for MICA Modems (continued)

Field	Description
Parameter #16 TX, RX Preemphasis Index:	The preemphasis index involves shaping the raw transmit spectrum to deal with spectrum roll-offs. The preemphasis index can take on the values from 0 to 10. A zero denotes no reshaping. Typical values usually fall in the range from 0 to 2, or 6 to 7. This index is used with V.34 and V.34+ connection standards.
Parameter #17 TX, RX Constellation Shaping:	Constellation shaping is a technique for improving noise immunity by using a probability distribution for transmitted signal points. The signal states are used to predict the sensitivity to certain transmission impairments. Constellation shaping is used with the V.34 and V.34+ connection standards. Values displayed by this parameter are either none or active (Off or On).
Parameter #18 TX, RX Nonlinear Encoding:	Nonlinear encoding occurs during the training phase and moves the outer points of the constellation away to deal with nonlinear distortion. Nonlinear distortion (in the range from 0 to 200 Hz) tends to affect the higher-powered signals. Moving the outer constellation points out reduces the chance of error. Nonlinear encoding is used with the V.34 and V.34+ connection standards. Values displayed by this parameter are either none or active (Off or On). **Note** MICA technologies modems support nonlinear coding in both directions.
Parameter #19 TX, RX Precoding:	Precoding serves the same purpose as the preemphasis index, but instead manages the bits and not the raw transmit signals. This management is done only when asked for and therefore will occur only in the RX mode. Precoding is used with the V.34 and V.34+ connection standards. Values displayed by this parameter are either none or active (Off or On).
Parameter #20 TX, RX Xmit Level Reduction:	The Xmit (transmit) level affects the transmit signal with 0 to 15 in dBm of reduction. If nonlinear distortion is detected, the MICA technologies modem will request a lower-powered TX signal. If the remote end detects nonlinear distortion, it will also request a lower-powered TX signal. Xmit level reduction is used with the V.34 and V.34+ connection standards. Values displayed by this parameter are the transmit signal and reduction, in dBm.

Table 82 show modem operational-status Field Descriptions for MICA Modems (continued)

Field	Description
Parameter #21 Signal Noise Ratio:	A signal to noise ratio (SNR) is the ratio between the expected signal and the error signal. For example, consider a four-point constellation at (*x*,*y*) = (–1,1), (1,1), (1,–1), and (–1,–1). The receive signal comes in at (*x*^,*y*^) = (0.5,1.5). The expected value, although not guaranteed, is (1,1). The error vector is then calculated as follows: *e* = (*x* – *x*^, *y* – *y*^) = ([1–0.5], [1–1.5]) = (0.5,–0.5) and the SNR is calculated as follows: SNR = 20*log10 [magnitude(expected value *x*,*y* of constellation) / magnitude(error)] SNR = 20 log10 [magnitude(1,1) / magnitude(0.5,–0.5)] = 6.02 dB This parameter displays the ratio measurement of the desired signal to noise. MICA technologies modems measure the SNR in only the signal band that has a rate equal to the baud rate (that is, 3200 Hz, 2400 Hz, and so on). Note that a 28.8-kbps connection demands an SNR of about 37 dB. If the rate is lower than this value, the quality of the connection diminishes. A 33.6-kbps connection demands an SNR of 38 to 39 dB. A clean line has an SNR of about 41 dB. The values displayed by this parameter range from 0 to 70 decibels (dB) and change in 1-dB steps.
Parameter #22 Receive Level:	The receive level is the power of the received signal and ranges from 0 to –128 dBm in 1-dBm incremental steps. The ideal range is about –22 dBm in the United States and –12 dBm in Europe. In theory, MICA technologies modems can handle a receive level up to –4 dBm. However, the receive level they can handle is a function of the echo level. If there is absolutely no echo, the MICA modem should be able to handle a –4 dBm level. As the echo level goes up, the receive level that the MICA modem can handle moves from –4 dBm to –5 dBm, and so on. The optimum range for the receive level displayed by this parameter is from –12 dBm to –24 dBm.
Parameter #23 Frequency Offset:	Frequency offset is a difference between the modulation carriers—that is, the frequency shift in the receive spectrum between the expected RX carrier frequency and the actual RX carrier frequency. The values displayed by this parameter range from +/–32 in 0.125-Hz steps. The typical value is 0 Hz. **Note** Values of up to +/–7 Hz can be found on analog trunk circuits and will be compensated for by the MICA technologies modems.

Table 82 show modem operational-status Field Descriptions for MICA Modems (continued)

Field	Description
Parameter #24 Phase Jitter Frequency:	Phase jitter frequency is the peak-to-peak differential between two signal points. The following calculation models a typical RX carrier: $e\text{^}j(wt + a)$ but when phase jitter is detected, the RX carrier is modeled as follows: $e\text{^}j[wt + a + K \sin(bt + c)]$ where: w = carrier frequency a = carrier phase K = magnitude of sinusoidal phase jitter b = frequency of sinusoidal phase jitter c = phase of sinusoidal phase jitter Uncanceled phase jitter looks like "rocking" of the baseband QAM constellation. The points look like arcs with the outer points having longer arcs. The phase jitter measurements displayed by this parameter range from +/–32 in 0.125-Hz steps. The typical value is 0 degrees (that is, phase jitter is not normally present). **Note** This phase jitter value is found only on analog trunk circuits. Typical frequencies are power generation frequencies and their harmonics (that is, 60, 120 Hz within the United States; 50, 100 Hz international). MICA technologies modems cancel all known frequencies.
Parameter #25 Phase Jitter Level:	Phase jitter level is the amount of phase jitter measured and indicates how large the "rocking" is, in degrees. On an oscilloscope, the constellation points would look like crescent moons. The jitter level corresponds to magnitude K as described in Parameter #24. Values displayed by this parameter can range up to 15 degrees. The typical value is 0 degrees (that is, phase jitter is not normally present).

Table 82 show modem operational-status Field Descriptions for MICA Modems (continued)

Field	Description
Parameter #26 Far End Echo Level:	Over long connections, an echo is produced by impedance mismatches at 2-wire-to-4-wire and at 4-wire-to-2-wire hybrid circuitry. This parameter displays the far-end echo level (that portion of the transmitted analog signal that has bounced off of the analog front end of the remote modem), which can range from 0 to –90 dBm. A MICA modem cannot handle near-end echo if far-end echo is present and the round-trip delay is greater than 10 microseconds. This constraint comes from the number of taps in the echo canceler of MICA modems. Assuming that there is no near-end echo, the performance of the receiver varies as the ratio of the receive level divided by the far-end echo (RECEIVE LEVEL/FAR END ECHO). As the echo level rises, the receiver performance degrades. (This is why the MICA modem can handle "hotter" receive levels with less echo.) The technical reason for this degradation has to do with *dynamic range*. Every echo canceler has some residual echo (error) left in the signal. This residual echo adds to the power of the receive signal going through the rest of the MICA modem receiver. With little residual echo, there is more dynamic range for the actual receive signal. For a call to go from the MICA modem to the local switch and back into MICA, the reported far-end echo level must be less than –55 dBm. A greater echo level indicates a digital-to-analog conversion in the path between the MICA modem and the switch. MICA modems are not supported in this topology.
Parameter #27 Phase Roll:	This parameter displays the phase roll, which affects the echo signal coming back to the MICA modem. A certain constellation pattern is transmitted from a MICA modem when the echo signal reaches the central office (CO). Some echoed form of this signal/constellation pattern is sent back to the MICA modem; however, the constellation shape may be rotated from 0 to 359 degrees. This rotation is called the *phase roll*. The echoed signal consists of a frequency component and a phase component. If the frequency component changes at all, a correction is needed for echo cancellation to work correctly. A slight variance (an unknown amount that would have to be determined through experimentation) in the phase may not affect how the echo canceler performs. Too much change in phase also needs correcting for proper echo cancellation to occur. The phase roll value ranges from +/–32 in 0.125-Hz steps. The typical value is 0 or close to 0.

Table 82 show modem operational-status Field Descriptions for MICA Modems (continued)

Field	Description
Parameter #28 Round Trip Delay:	Round-trip delay is the total round-trip propagation delay of the link in microseconds. This delay is important for proper echo cancellation. This parameter displays the round-trip delay; the amount of delay varies with each network. **Note** The buffer speed for MICA modems is 4096 bps; therefore, at 2400 bps the delay is 1.7 seconds, and at 3429 bps, 1.19 seconds. Because round-trip delay is measured before the bps rate is chosen, round-trip delay is used to disable those bit rates for which the round-trip delay cannot be supported. For example, if the round trip-delay is 1.25 seconds, 3429 is disabled for that train attempt.
Parameter #30 Characters transmitted, received:	This parameter displays the total count of characters (before modem compression of any type) received and transmitted.
Parameter #32 General Portware Information:	Not used.
Parameter #33 PPP/SLIP packets transmitted, received:	This parameter displays the total count of Point-to-Point Protocol (PPP) and Serial Line Internet Protocol (SLIP) packets transmitted and received. This total could include all PPP/SLIP packets, including BAD/ABORTED packets.
Parameter #35 PPP/SLIP packets received (BAD/ABORTED):	This parameter displays the total count of the bad or aborted PPP/SLIP packets, and is a subset of the counter shown in Parameter #33 (PPP/SLIP packets received). A counted PPP packet has a bad FCS, or the SLIP packet has a transparency error. Errored PPP frames should be displayed only when asynchronous framing (no EC protocol) is being used.
Parameter #36 EC packets transmitted, received OK:	This parameter displays the number of EC packets transmitted (the number of TX frames that the client modem has accepted) and the number of EC packets received (the number of RX frames that the MICA modem has accepted).
Parameter #38 EC packets (Received BAD/ABORTED):	Parameter #38 is identical to Parameter #3 (EC Retransmission Count). It may read differently from Parameter #3, depending on how the software requests the parameter information.
Parameter #39 Robbed Bit Signalling (RBS) pattern:	This parameter displays the number of robbed bits detected in the connection. The robbed bits are used for in-band signaling. This information is reported only for K56Flex by the analog modem. The six least significant bits of the returned value indicate the periodic RBS pattern, where a 1 denotes a pulse code modulation sample with a robbed bit.

Table 82 show modem operational-status Field Descriptions for MICA Modems (continued)

Field	Description
Parameter #40 Digital Pad, Digital Pad Compensation:	A digital pad can be implemented by the CO to attenuate a "hot" signal. Compensation boosts the signal by the amount of the pad. This parameter displays values that usually range from 0 to 10 dB, with typical values being 0, 3, and 6 dB. **Note** A digital pad is mandatory for K56Flex, but configurable for V.90 using S52. K56Flex supports only 0, 3, and 6 dB. V.90 supports steps of 1/8192 dB, but it is reported to the host in steps of 0.125-dB granularity.
Line Shape:	The display at the end of the report shows line shaping as a frequency-response graph of the channel. The *Y* (vertical) axis represents frequencies from 150 Hz (top of chart) to 3750 Hz (bottom of chart) in 150-Hz steps. The *X* (horizontal) axis represents a normalized amplitude. The graph can help identify nulls, bandwidth, and distortion (irregular shape). A flat spectrum plot is best. This display is available only for V.34, V.90, and K56Flex connection standards.

Table 82 show modem operational-status Field Descriptions for MICA Modems (continued)

Field	Description
Parameter #9 TX, RX Bit Rate:	This parameter displays the TX bit rate from the local data communication equipment (DCE) to the remote DCE and the RX bit rate from the remote DCE to the local DCE. The following data carrier connect standards support the rates indicated in bits per second (bps): • V.21 TX, RX—300 bps • V.22 TX, RX—1200 bps • V.22*bis* TX, RX—2400 bps • V.23 TX (originate)—1200 bps • V.23 RX (originate)—75 bps • V.32 TX, RX—4800 and 9600 bps • V.32*bis* TX, RX—4800, 7200, 9600, 12000, and 14400 bps • V.34 TX, RX—2400, 4800, 7200, 9600, 12000, 14400, 16800, 19200, 21600, 24000, 26400, and 28800 bps • V.34+ TX, RX—2400, 4800, 7200, 9600, 12000, 14400, 16800, 19200, 21600, 24000, 26400, 28800, 31200, and 33600 bps • K56Flex TX—32000, 34000, 36000, 38000, 40000, 42000, 44000, 46000, 48000, 50000, 52000, 54000, 56000, 58000, and 60000 bps • K56Flex RX—2400, 4800, 7200, 9600, 12000, 14400, 16800, 19200, 21600, 24000, 26400, 28800, and 31200 bps • V.90 TX—28000, 29333, 30666, 32000, 33333, 34666, 36000, 37333, 38666, 40000, 41333, 42666, 44000, 45333, 46666, 48000, 49333, 50666, 52000, 53333, 54666, and 56000 bps • V.90 RX—2400, 4800, 7200, 9600, 12000, 14400, 16800, 19200, 21600, 24000, 26400, 28800, 31200, and 33600 bps • Bell103 TX, RX—Up to 300 bps • Bell212 TX, RX—0 to 300 and 1200 bps The following fax connect standards support the rates indicated in bits per second (bps): • V.17 TX, RX—7200, 9600, 12000, and 14400 bps • V.27ter TX, RX—2400 and 4800 bps • V.29 TX, RX—7200 and 9600 bps

Table 82 show modem operational-status Field Descriptions for MICA Modems (continued)

Field	Description
Parameter #11 TX, RX Symbol Rate:	This parameter displays the TX symbol rate used to transmit samples to the line and the RX symbol rate used to receive samples from the line. The rates are synchronous with each other. The following data carrier connect standards support the indicated bit rates: • V.21 TX, RX—300 bps • V.22 TX, RX—600 bps • V.22*bis* TX, RX—600 bps • V.23 TX (originate)—1200 bps • V.23 RX (originate)—75 bps • V.23 TX (answer)—75 bps • V.23 RX (answer)—1200 bps • V.32 TX, RX—2400 bps • V.32*bis* TX, RX—2400 bps • V.34 TX, RX—2400, 2743, 2800, 3000, 3200, and 3429 bps • V.34+ TX,RX—2400, 2743, 2800, 3000, 3200, and 3429 bps • K56Flex TX—8000 bps • K56Flex RX—3200 bps • V.90 TX—8000 bps • V.90 RX—3000, 3200, and 3429 bps • Bell103 TX, RX—300 bps • Bell212 TX, RX—600 bps The following fax connect standards support the indicated bit rates: • V.17 TX, RX—2400 bps • V.27ter TX, RX—1800 bps • V.29 TX, RX—2400 bps

The following Microcom example shows details for an 8-port analog modem module inside a Cisco 3640 router. (For an explanation of the fields seen in this display, refer to the description of the **AT@E1** modem command in the document *AT Command Set and Register Summary for Analog Modem Network Modules*.)

```
Router# show modem operational-status 1/0

MNP Class 10 V.34 Modem
MODEM HW: PC 2W ANALOG  United States
Firmware Rev 2.2.48/85
DSP C36 Part/Rev              3635 4241
DSP C58 Part/Rev              3635 2041
DSP Controller Rev            0.0
```

```
DSP Data Pump Rev             0.0
Connect Time                  000:00:00
- RTS 5 CTS 6 DSR - CD 20 DTR - RI
Disconnect  Remote -   Local -

Mod Type                      IDLE
TX/RX Spd                     *****  ***** BPS
TX/RX Spd Mask                   NA  0000 Hex
Symbol Rate                   2400 Hz
TX/RX Carrier Freq            1800  1800 Hz
TX/RX States                    16    16
TX/RX NLE                      OFF   OFF
TX/RX Precoding                OFF   OFF
TX/RX Shaping                  OFF   OFF
TX Preemphasis Index             0

TX Lvl REG                    - 13 dBm
TX Lvl RAM                    -  0 dB
TX Lvl Reduct                    0 dB
TX Lvl                        - 13 dBm
RX Lvl                        - 57 dBm
S/NR                             0
S/DR                             0
EQM                           0000 Hex
AVG EQM                       0000 Hex
Lower/Upper Edge                 0     0 Hz
Phase Jitter Freq                0 Hz
Phase Jitter Amp               0.0 deg
Far Echo Lvl                     0 N
Round Trip Delay                 0 msec
Dropouts > 5dB                   0
RTRNs Init/Accept                0     0
RRENs Init/Accept                0     0
BLER                          0000 Hex
RBS Counter                   0000 Hex
Digital Pad Detected             NA
Max SECRXB                    00
Max SECTXB                    00
OK
```

Related Commands

Command	Description
show modem configuration	Displays the current modem configuration for digital MICA modems loaded inside access servers or routers.
show modem log	Displays the modem history event status performed on a manageable modem or group of modems.
show modem mica	Displays information about MICA digital modems.
show port operational-status	Displays the operational status of a specific modem port or port range for the Cisco AS5400 and AS5800 access servers.

show modem operational-status (pvdm2)

To display performance statistics for individual digital modems on PVDM2-xxDM devices, use the **show modem operational-status** command in privileged EXEC mode.

show modem operational-status [*slot*/*port*]

Syntax Description

slot/*modem number*	(Optional) Location of the slot and modem number. If these numbers are not specified, statistics for all connected modems are displayed. You must include the slash mark.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(11)XW	This command was introduced.

Examples

The following example shows details for a V12 digital modem on a PVDMII-xxDM device. A specific modem, 0/322, is designated.

```
Router# show modem operational-status 0/322
Modem (0/322) Operational Status:

 Error correction               77    LAP-M
 Data compression               68    V44
 Modulation type                206   V.34
 receive speed                  16    33600
 transmit speed                 16    33600
 error correction frames sent   7
 error correction frames rcvd   12
 characters transmitted         218
 characters received            487
 synchronous frames sent        7
 synchronous frames rcvd        12
 bad synchronous frames rcvd    0
 reject frames sent             0
 reject frames rcvd             0
 total retransmissions          0

 Disconnect reason              21    Clears previous disconnect reason
 Retrain/rate renegotiate reason 0    None
 Connection time (hours)        0
 Connection time (minutes)      19
 Connection time (seconds)      15
 Initial receive speed          16    33600
 Initial transmit speed         16    33600
 Maximum receive speed          16    33600
 Maximum transmit speed         16    33600
 Minimum receive speed          16    33600
 Minimum transmit speed         16    33600
 Max retransmit for one frame   1
 Total retransmit during connect 0
```

```
 Minimum EQM                     17
 Maximum EQM                     26
 Negative EQMs                   0
 Minimum SNR                     27    31 dB
 Maximum SNR                     27    31 dB
 Retrains requested locally      0
 Retrains requested remotely     0
 Rate renegotiation req locally  0
 Rate renegotiation req remotely 0

 Raw AGC value                   94
 Last EQM                        21
 Transmit symbol rate            5     3429
 Receive symbol rate             5     3429
 Transmit carrier frequency      0     1959 (low)
 Receive carrier frequency       0     1959 (low)
 Minimum AGC reading             94
 Maximum AGC reading             94
 Transmit level                  13
 Remote req tx level reduction   2
 SNR                             27    31 dB
 Transmit non-linear encoding    1     On
 Receive non-linear encoding     1     On
 Transmit precoding              1     On
 Receive precoding               1     On
 Transmit shaping                16
 Receive shaping                 16
 Trellis mapping                 0     16-state
 Transmit pre-emphasis index     0
 Raw round trip delay            424
 EQM sum low                     0
 EQM sum medium                  0
 EQM sum high                    0

 Ditital pad detected            0
 RBS pattern                     0
 Rate drop due to RBS            255
 V.90 minimum distance (high)    0
 V.90 minimum distance (low)     0
 Raw V.90 digital pad val (high) 255
 Raw V.90 digital pad val (low)  255

 Negotiation status              74    RLSD on
                                       K56flex/K56Plus negotiation failed
                                       V.90 negotiation not tried
                                       V.90/K56flex negotiation failed
 Non-standard V.8bis Octet 13    148   K56flex (generic)
 Non-standard V.8bis Octet 14    129   Conexant Conexant-based
 Non-standard V.8bis Octet 15    131   K56flex capable, Last byte,
 Non-standard V.8bis Octet 16    66    flex version 0x2, Not prototype,
                                       Server, Not last byte,
 Non-standard V.8bis Octet 17    0     Not last byte,
                                       Conexant data pump revision 0x0
 Non-standard V.8bis Octet 18    0     u-law, x-law not forced,
                                       Not last byte,
                                       Conexant controller revision 0x0

Router#
```

Related Commands

Command	Description
show modem configuration (pvdm2)	Displays the current modem configuration for digital V12 modems on PVDM2-xxDM devices.
show modem log (pvdm2)	Displays the modem history event status performed on a manageable modem or group of modems.

show modem summary

To display a high-level report for all manageable modems dialing in to and out of the network, use the **show modem summary** command in EXEC mode.

show modem summary

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Examples

The following is sample output from the **show modem summary** command:

```
Router# show modem summary

         Incoming calls       Outgoing calls      Busied   Failed   No    Succ
Usage  Succ   Fail  Avail   Succ   Fail  Avail    Out      Dial     Ans   Pct.
  17%  1547     64     11      0      0     11        0        3     3     96%
```

Table 83 describes the significant fields shown in the display.

Table 83 show modem summary Field Descriptions

Field	Description
Incoming and Outgoing calls	Calls dialing into and out of the modem. • Usage—Percentage of the total system uptime that all the modems are in use. • Succ—Total calls successfully connected. • Fail—Total calls that did not successfully connect. • Avail—Total modems available for use in the system.
Busied Out	Total number of times the modems were taken out of service with the **modem busy** command or the **modem shutdown** command.
Failed Dial	Total number of attempts the modems did not hang up or there was no dial tone.
No Ans	Total number of times call ringing was detected, but the calls were not answered by a modem.
Succ Pct.	Successful connection percentage of total available modems.

show modem test

To display the modem test log, use the **show modem test** command in EXEC mode.

show modem test

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The modem test log displays the results of the modem diagnostics test, which is issued with the **modem autotest** global configuration command.

Examples

The following is sample output from the **show modem test** command for a V.34 modem card:

```
Router# show modem test

 Date Time          Modem  Test              Reason             State Result
 5/15 07:25:17 AM  1/0    Back-To-Back       TIME INTERVAL      Idle  FAIL
 5/15 07:25:17 AM  1/1    Back-To-Back       TIME INTERVAL      Idle  PASS
 5/15 07:25:17 AM  1/2    Back-To-Back       TIME INTERVAL      Idle  PASS
 5/15 07:25:17 AM  1/3    Back-To-Back       TIME INTERVAL      Idle  FAIL
 5/15 07:25:17 AM  1/4    Back-To-Back       TIME INTERVAL      Idle  PASS
 5/15 07:25:17 AM  1/5    Back-To-Back       TIME INTERVAL      Idle  PASS
 5/15 07:25:17 AM  1/6    Back-To-Back       TIME INTERVAL      Idle  PASS
 5/15 07:25:17 AM  1/7    Back-To-Back       TIME INTERVAL      Idle  PASS
 5/15 07:25:17 AM  1/8    Back-To-Back       TIME INTERVAL      Idle  PASS
 5/15 07:25:17 AM  1/9    Back-To-Back       TIME INTERVAL      Idle  PASS
.
.
.
```

Table 84 describes the significant field shown in the display.

Table 84 show modem test Field Descriptions

Field	Description
Date	Date the back-to-back test occurred for the specified modem.
Time	Time the test occurred.
Modem	Specified modem that performed a back-to-back test.
Test	Operation performed by the specified modem.
Reason	Reason the modem performed a back-to-back test.

Table 84 show modem test Field Descriptions (continued)

Field	Description
State	Current operational state of the modem.
Result	Result of the back-to-back test for the specified modem.

show modem version

To display version information about the modem firmware, controller and Domain Specific Part (DSP) ATM address field code (for 56K modems only), and boot code, use the **show modem version** command in EXEC mode.

show modem version

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.0(4)XI1	This command was enhanced to display service processing element (SPE) features. The "–/–" in the DSP REV field indicates that the **spe** configuration commands for firmware download are unavailable on that modem.

Usage Guidelines

This command is useful for verifying the version of modem firmware running on the system before or after a modem firmware upgrade. If there is a "-/-" in the DSP REV field, you cannot use the **spe** configuration commands for firmware download on that modem.

Examples

The following example displays information for modem firmware, which includes modem firmware version, boot code version, controller and DSP code version (56K modem modules only), modem board hardware version, and carrier card information. This particular example displays information for Microcom 56K modem cards (modules 0/0, 2/0, and 2/1) and V.34 cards (module 0/1) installed in a Cisco AS5200.

If the version number is displayed as 0.0.0, verify that out-of-band status polling is functioning.

```
Router# show modem version

          Modem module    Firmware    Boot           DSP
  Mdm     Number          Rev         Rev            Rev
  0/0               0       3.1(21)  3.0(4)    1.1(0)/1.1(0)
  0/1               0       3.1(21)  3.0(4)    1.1(0)/1.1(0)
  .
  .
  .
0/11              0       3.1(21)  3.0(4)    1.1(0)/1.1(0)
  0/12              1       2.2(8)   1.0(5)
  0/13              1       2.2(8)   1.0(5)
  .
  .
  .
0/23              1       2.2(8)   1.0(5)
         2/0                0       3.1(21)  3.0(4)    1.1(0)/1.1(0)
  2/1               0       3.1(21)  3.0(4)    1.1(0)/1.1(0)
  2/2               0       3.1(21)  3.0(4)    1.1(0)/1.1(0)
```

```
  .
  .
  .
2/21              1       3.1(21)  3.0(4)    1.1(0)/1.1(0)
  2/22              1       3.1(21)  3.0(4)    1.1(0)/1.1(0)
  2/23              1       3.1(21)  3.0(4)    1.1(0)/1.1(0)

 Modem board HW version info:

 Slot 0:
   Carrier card:
     hw version= 8, number_of_ports= 24, max_modules= 2, max_oob_ports= 2
   Modem Module 0:
     number_of_modems= 12, option_bits= 1,
     rev_num= 02.00, vendor_model_number= 02,
     vendor_banner= Microcom MNP10 K56 Modem
   Modem Module 1:
     number_of_modems= 12, option_bits= 1,
     rev_num= 03.00, vendor_model_number= 01,
     vendor_banner= Microcom MNP10 V34 Modem

 Slot 2:
   Carrier card:
     hw version= 7, number_of_ports= 24, max_modules= 2, max_oob_ports= 2
   Modem Module 0:
     number_of_modems= 12, option_bits= 1,
     rev_num= 02.00, vendor_model_number= 02,
     vendor_banner= Microcom MNP10 K56 Modem
   Modem Module 1:
     number_of_modems= 12, option_bits= 1,
     rev_num= 02.00, vendor_model_number= 02,
     vendor_banner= Microcom MNP10 K56 Modem
```

The following example displays modem version information for V.110 terminal adapter modules:

```
Router# show modem version

              Modem module       Firmware    Boot
  Mdm             Number         Rev         Rev
  0/0               0            Unmanaged   Unmanaged
  0/1               0            Unmanaged   Unmanaged
  0/2               0            Unmanaged   Unmanaged
  .
  .
  .
  0/11              0            Unmanaged   Unmanaged
  1/0               0            Unmanaged   Unmanaged
  .
  .
  .
  1/11              0            Unmanaged   Unmanaged
  1/12              1            Unmanaged   Unmanaged
  .
  .
  .
  1/22              1            Unmanaged   Unmanaged
  1/23              1            Unmanaged   Unmanaged
  2/0               0            Unmanaged   Unmanaged
  .
  .
  .
  2/11              0            Unmanaged   Unmanaged
  2/12              1            Unmanaged   Unmanaged
```

```
  .
  .
  .
  2/22              1            Unmanaged   Unmanaged

Modem board HW version info:

 Slot 0:
   Carrier card:
     hw version= 3, number_of_ports= 12, max_modules= 1, max_oob_ports= 1
   Modem Module 0:
     number_of_modems= 12, option_bits= 1,
     rev_num= 03.01, vendor_model_number= 01,
     vendor_banner= V.110 Terminal Adaptor

 Slot 1:
   Carrier card:
     hw version= 8, number_of_ports= 24, max_modules= 2, max_oob_ports= 2
   Modem Module 0:
     number_of_modems= 12, option_bits= 1,
     rev_num= 03.01, vendor_model_number= 01,
     vendor_banner= V.110 Terminal Adaptor
   Modem Module 1:
     number_of_modems= 12, option_bits= 1,
     rev_num= 03.01, vendor_model_number= 01,
     vendor_banner= V.110 Terminal Adaptor

 Slot 2:
   Carrier card:
     hw version= 8, number_of_ports= 24, max_modules= 2, max_oob_ports= 2
   Modem Module 0:
     number_of_modems= 12, option_bits= 1,
     rev_num= 03.00, vendor_model_number= 01,
     vendor_banner= V.110 Terminal Adaptor
   Modem Module 1:
     number_of_modems= 12, option_bits= 1,
     rev_num= 03.00, vendor_model_number= 01,
     vendor_banner= V.110 Terminal Adaptor
```

The following example shows the display from a Cisco AS5300. If there is a "-/-" in the DSP REV field, you cannot use the **spe** configuration commands for firmware download on that modem.

```
Router# show modem version

          Modem module     Firmware   Boot          DSP
 Mdm      Number           Rev        Rev           Rev
 1/0              0         2.6.1.0
 1/1              0         2.6.1.0
 1/2              0         2.6.1.0
 1/3              0         2.6.1.0
 1/4              0         2.6.1.0
 1/5              0         2.6.1.0
 1/6              1         2.6.1.0
 .
 .
 .
 1/41             6         2.6.1.0
 1/42             7         2.6.1.0
 1/43             7         2.6.1.0
 1/44             7         2.6.1.0
 1/45             7         2.6.1.0
 1/46             7         2.6.1.0
 1/47             7         2.6.1.0
 2/0              0         5.0(40)  3.0(4)    22.0/47.0
```

```
  2/1               0       5.0(40)  3.0(4)    22.0/47.0
  2/2               0       5.1(9)   3.0(4)    22.0/47.0
  .
  .
  .
  2/8               0       5.1(9)   3.0(4)    22.0/47.0
  2/9               0       5.0(40)  3.0(4)    22.0/47.0
  2/10              0       5.1(9)   3.0(4)    22.0/47.0
  2/11              0       5.1(9)   3.0(4)    22.0/47.0
  2/12              1       2.3(6)   1.0(5)       -/-
  2/13              1       2.3(6)   1.0(5)       -/-
  .
  .
  .
Modem board HW version info:

Slot 1:
Carrier card:
     number_of_ports= 48, max_modules= 10
Manufacture Cookie Info:
 EEPROM Type 0x0001, EEPROM Version 0x01, Board ID 0x47,
 Board Hardware Version 1.0, Item Number 73-2393-3,
 Board Revision A0, Serial Number 09361116,
 PLD/ISP Version 5.9, Manufacture Date 20-Jun-1998.

Modem Module 0
Manufacture Cookie Info:
 EEPROM Type 0x0101, EEPROM Version 0x01, Board ID 0x06,
 Board Hardware Version 1.0, Item Number 73-2522-2,
 Board Revision B48, Serial Number 06542204,
 PLD/ISP Version 255.255, Manufacture Date 23-Jun-1998.

Modem Module 1
Manufacture Cookie Info:
 EEPROM Type 0x0101, EEPROM Version 0x01, Board ID 0x06,
 Board Hardware Version 1.0, Item Number 73-2522-2,
 Board Revision B48, Serial Number 06478113,
 PLD/ISP Version 255.255, Manufacture Date 23-Jun-1998.
  .
  .
  .
Modem Module 7
Manufacture Cookie Info:
 EEPROM Type 0x0101, EEPROM Version 0x01, Board ID 0x06,
 Board Hardware Version 1.0, Item Number 73-2522-2,
 Board Revision B48, Serial Number 06478929,
 PLD/ISP Version 255.255, Manufacture Date 23-Jun-1998.

Modem Module 8

Modem Module 9

Slot 2:
   Carrier card:
     hw version= 2, pld= 0, number_of_ports= 24,
     max_modules= 2, max_oob_ports= 2
Manufacture Cookie Info:
 EEPROM Type 0x0001, EEPROM Version 0x01, Board ID 0x47,
 Board Hardware Version 1.0, Item Number 73-2522-2,
 Board Revision ^@2, Serial Number 05433763,
 PLD/ISP Version 255.255, Invalid Date code.

   Modem Module 0:
     number_of_modems= 12, option_bits= 1,
```

```
     rev_num= 03.30, vendor_model_number= 02,
     vendor_banner= Microcom MNP10 K56 Modem
   Modem Module 1:
     number_of_modems= 12, option_bits= 1,
     rev_num= 03.00, vendor_model_number= 01,
     vendor_banner= Microcom MNP10 V34 Modem
Router#

Router# write terminal

Building configuration...

Current configuration:
!
version 12.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname Router
!
aaa new-model
aaa group server radius aaa-server
 server 1.2.3.4
!
spe 1/0 1/7
 firmware location system:/ucode/mica_port_firmware
spe 2/0 2/1
 firmware location system:/ucode/microcom_firmware
spe 2/2 2/8
 firmware location flash:mcom-fw-dsp.5.1.9_47.22.bin
spe 2/9 2/9
 firmware location system:/ucode/microcom_firmware
spe 2/10 2/11
 firmware location flash:mcom-fw-dsp.5.1.9_47.22.bin
spe 2/12 2/23
 firmware location feature_card_flash
!

Router# termination length 0
```

Table 85 describes the significant fields shown in the displays of the **show modem version** command.

Table 85 show modem version Field Descriptions

Field	Description
Mdm	Slot and port number for the specified modem.
Modem module Number	Card number associated with the carrier card.
Firmware Rev	Modem firmware version, or one of the following: • Unknown—Indicates that the retrieved version is 0.0.0. • Unknown (F)—Indicates that the modem's out-of-band feature has failed. • Unknown (NP)—Indicates that the user has disabled the status polling for this modem using the **no modem status-polling** command.

Table 85 show modem version Field Descriptions (continued)

Field	Description
Boot Rev	Modem boot version, or one of the following: • Unknown—Indicates that the retrieved version is 0.0.0. • Unknown (F)—Indicates that the modem's out-of-band feature has failed. • Unknown (NP)—Indicates that the user has disabled the status polling for this modem using the **no modem status-polling** command.
DSP Rev	Controller and DSP version, which is displayed for the 56K modems only. The first set of numbers correspond to the controller version. The second set of numbers, which begin with a forward slash (/), corresponds to the DSP version.
Modem board HW version info:	Modem hardware board information.
Slot	Slot number used for the carrier card.
Carrier card	Modem carrier card.
hw version	Modem carrier card hardware version.
number_of_ports	Maximum number of modem ports that can be installed in the carrier card.
max_modules	Maximum number of modem cards that can be installed in a carrier card.
max_oob_ports	Maximum number of out-of-band ports used in the carrier card.
Modem Module	Modem card.
number_of_modems	Number of modems installed in the modem card.
option_bits	Signal level of the modem A-law and the U-law.
rev_num	Modem card version number.
vendor_model_number	Vendor modem model number.
vendor_banner	Type of banner displayed by the modem vendor.

show modem version (pvdm2)

To display version information about the modem firmware, controller, and boot code, use the **show modem version** command in Privileged EXEC mode.

show modem version

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(11)XW	This command was introduced.

Usage Guidelines

This command is useful for verifying the version of modem firmware running on the system before or after a modem firmware upgrade. If there is a "-/-" in the DSP REV field, you cannot use the **spe** configuration commands for firmware download on that modem.

Examples

The following example displays modem version information about PVDM2-xxDM digital modems. This example specifically shows information about a Cisco 2821 router with three PVDM2-36DMs, high-density pvdms holding 36 digital modems each.

```
Router# show modem version
Slot 0:
PVDM 0: PVDMII-36DM - HW Version 1, FPGA Version 3.3, NiOS(2) 5.0.1
 Modem 0/322-0/333:
    PCI Classid: 0x07800001 Bootrom Rev: 0x00005601 Diag Result: 0x0000007F
    Firmware: V3_09
 Modem 0/334-0/345:
    PCI Classid: 0x07800001 Bootrom Rev: 0x00005601 Diag Result: 0x0000007F
    Firmware: V3_09
 Modem 0/346-0/357:
    PCI Classid: 0x07800001 Bootrom Rev: 0x00005601 Diag Result: 0x0000007F
    Firmware: V3_09

PVDM 1: PVDMII-36DM - HW Version 1, FPGA Version 3.3, NiOS(2) 5.0.1
 Modem 0/386-0/397:
    PCI Classid: 0x07800001 Bootrom Rev: 0x00005601 Diag Result: 0x0000007F
    Firmware: V3_09
 Modem 0/398-0/409:
    PCI Classid: 0x07800001 Bootrom Rev: 0x00005601 Diag Result: 0x0000007F
    Firmware: V3_09
 Modem 0/410-0/421:
    PCI Classid: 0x07800001 Bootrom Rev: 0x00005601 Diag Result: 0x0000007F
    Firmware: V3_09

PVDM 2: PVDMII-36DM - HW Version 1, FPGA Version 3.3, NiOS(2) 5.0.1
 Modem 0/450-0/461:
    PCI Classid: 0x07800001 Bootrom Rev: 0x00005601 Diag Result: 0x0000007F
    Firmware: V3_09
```

```
Modem 0/462-0/473:
   PCI Classid: 0x07800001 Bootrom Rev: 0x00005601 Diag Result: 0x0000007F
   Firmware: V3_09
Modem 0/474-0/485:
   PCI Classid: 0x07800001 Bootrom Rev: 0x00005601 Diag Result: 0x0000007F
   Firmware: V3_09
```

Table 85 describes the significant fields shown in the displays of the **show modem version** command.

Table 86 show modem version Field Descriptions

Field	Description
PVDM	PVDM slot number where PVDM2-xxDM is present.
HW Version	Hardware revision number of PVDM2-xxDM.
FPGA Version	FPGA version loaded in the PVDM2-xxDM.
NiOS	The version number of the NiOS core soft processor in PVDM2-xxDM.
Modem	Slot and port number for the specified modem.
PCI Classid	PCI class id of the CSM V12 chipset present in PVDM2-xxDM.
Bootrom Rev	Bootrom revision number of PVDM2-xxDM.
Diag Result	Internal diagnostics result.
Firmware	CSM V12 Firmware version

show modemcap

To display the values set for the current modem and list the modems for which the router has entries, use the **show modemcap** command in EXEC mode. To display the attributes associated with a specific modem, use the **show modemcap** command in EXEC mode with the optional *modem-type* argument.

show modemcap [*modem-type*]

Syntax Description

modem-type	(Optional) Modem type, such as a Codex 3260.

Defaults

The list of modems for which the router has entries.

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

When a modem name is supplied, this command displays the available modem values.

As an alternative to repeatedly entering the same data, use templates as a way to join modemcap entries. For example, consider the following modemcap entries:

```
modemcap entry gv_basics:FD=&F:AA=S0=1:CD=&C1:DTR=&D2:NEC=E0:NRS=Q1
modemcap entry global_village:HFL=&K3\\X1:BCP=%C1:NCP=%C0:TPL=gv_basics
modemcap entry gv_teleport:NCP=%C0:TPL=gv_basics
```

To look up the factory default for a global_village modem, perform the following steps:

Step 1 Look at the global_village modemcap entry for the factory default (FD).

Step 2 If you fail to find FD in global_village, look at the global_village modemcap entry for a template (TPL).

Step 3 Find a TPL called “gv_basics.”

Step 4 Look in the gv_basics modemcap entry for the FD.

Step 5 Find FD=&F in the gv_basics modemcap entry.

Step 6 Use &F as the FD for the global_village.

Examples

The following example shows the modem values in a Codex 3260:

```
Router# show modemcap codex_3260

Modemcap values for codex_3260
Factory Defaults (FD):  &F
Autoanswer (AA):  S0=1
Carrier detect (CD):  &C1
Drop with DTR (DTR):  &D2
Hardware Flowcontrol (HFL):  *FL3
Lock DTE speed (SPD):  *SC1
DTE locking speed (DTE):  [not set]
Best Error Control (BER):  *SM3
Best Compression (BCP):  *DC1
No Error Control (NER):  *SM1
No Compression (NCP):  *DC0
No Echo (NEC):  E0
No Result Codes (NRS):  Q1
Software Flowcontrol (SFL):  [not set]
Caller ID (CID):  &S1
On-hook (ONH):  H0
Off-hook (OFH):  H1
Miscellaneous (MSC):  [not set]
Template entry (TPL):  default
Modem entry is built-in.
```

Table 87 identifies and describes the list of attributes.

Table 87 Modem Attributes

Modem Attribute	Description
Factory defaults (FD)	Returns the modem to factory default configuration. This is commonly "&F."
Autoanswer (AA)	Sets the modem to answer the phone if data terminal ready (DTR) is high, preferably on the first ring. This is commonly "S0=1."
Carrier detect (CD)	Instructs the modem to raise the CD signal when a carrier is detected. Cisco configures modems into auto-answer mode by default. This is not the default for most modems, which just raise CD and leave it high. This is commonly "&C1." In auto-answer mode, the modem waits until it detects a ring, then responds to the incoming call and negotiates an end-to-end connection with the other modem. At this point, the modem receiving the call informs the router that it has a call ready to be processed; this notification is performed by raising the signal on EIA/TIA-232 pin 8 (the Data Carrier Detect signal) to high.
Drop with DTR (DTR)	Drops the connection if DTR signal drops. There is frequently an option to reset the configuration while this drop occurs; however, this option should *not* be used. The connection should only drop. The correct value for this is commonly "&D2."
Set Hardware Flowcontrol (HFL)	Uses ready to send/clear to send (RTS/CTS) out-of-band flow control.
Set Software flowcontrol (SFL)	Uses transmit on/transmit off (XON/XOFF) in-band flow control.

Table 87 Modem Attributes (continued)

Modem Attribute	Description
Lock DTE speed (SPD)	Instructs the modem to lock the speed at which it communicates to the router to a single rate, preferably the highest. This attribute is important and is often hard to find in manuals. SPD is often linked to the hardware flow control variable. Look for phrases like "bps rate adjust" and "bit rate adjust." Some modems set the speed to a value that depends on an S-register; other modems simply lock to the speed that was used when the last AT command was issued. Locking to the speed that was last used is handled automatically. To enable the S-register to set the speed, you must include the proper S-register value for the fastest possible DTE speed.
Best Error Control (BER)	Instructs the modem to negotiate its best error control with remote modems. For ARAP users, this is Microcom Network Protocol (MNP) 5/Link Access Procedure, Balanced (LAPB), but not MNP4.
Best Compression (BCP)	Instructs the modem to negotiate its best compression with remote modems.
No Error Control (NER)	Instructs the modem to negotiate no error control with remote modems. This attribute will be used when placing outgoing (callback) AppleTalk Remote Access protocol (ARAP) calls.
No Compression (NCP)	Instructs the modem to negotiate no compression with remote modems. This attribute is used when placing outgoing (callback) ARAP calls.
No Echo (NEC)	Requests the modem *not* to echo characters. This attribute is commonly "E0."
No Result Codes (NRS)	Requests the modem *not* to send a response when you issue a command. This attribute is commonly "Q1."
Caller ID (CID)	Requests that Caller ID information be returned when dial in occurs. Not used.
Miscellaneous (MSC)	Sends any extra commands that are needed for the modem to work (possibly with specific platforms).
Template entry (TPL)	This is the name of another modem type. It is referenced as the value of any of the previously listed attributes if they are not set on the current modem type.

Related Commands

Command	Description
modemcap edit	Changes a modem value that was returned from the **show modemcap** command.
modemcap entry	Stores and compresses information about the capability of a specified modem.

show modem-pool

To display the configuration and connection status for one or more modem pools, use the **show modem-pool** command in EXEC mode.

show modem-pool [*pool-name*]

Syntax Description

pool-name	(Optional) Modem pool name.

Command Modes

EXEC

Command History

Release	Modification
11.2P	This command was introduced.

Usage Guidelines

The counters displayed by the **show modem-pool** command are cleared with the **copy modem** command.

Examples

In the following example, two modem pools are set up: v90service and v34service. Each pool contains one Dialed Number Information Service (DNIS) number: 1234 and 5678, respectively. Each DNIS number is allowed a maximum of 48 simultaneous connections. A total of 96 modems are assigned to the modem pools: 48 and 48, respectively. Modems that are left unassigned to modem pools are automatically put into the default modem pool (displayed as System-def-Mpool). The default pool is empty in this example.

```
Router# show modem-pool

modem-pool: System-def-Mpool
modems in pool: 0   active conn: 0
0 no free modems in pool

modem-pool: v90service
modems in pool: 48  active conn: 46
 8 no free modems in pool
 called_party_number: 1234
   max conn allowed: 48, active conn: 46
   8 max-conn exceeded, 8 no free modems in pool

modem-pool: v34service
modems in pool: 48  active conn: 35
 0 no free modems in pool
 called_party_number: 5678
   max conn allowed: 48, active conn: 35
   0 max-conn exceeded, 0 no free modems in pool
```

Table 88 describes the significant fields shown in the display.

Table 88 show modem-pool Field Descriptions

Field	Description
modem-pool	Name of the modem pool. In the previous example, there are three modem pools configured: System-def-Mpool, v34service, and v90service. To set modem pool name, see the **copy modem** command. All the modems not assigned to a modem pool are automatically assigned to the system default pool (displayed as System-def-Mpool).
modems in pool	Number of modems assigned to the modem pool. To assign modems to a pool, see the **copy modem** command.
active conn	Number of simultaneous active connections for the specified modem pool or called party DNIS number.
no free modems in pool	Number of times incoming calls were rejected because there were no more free modems in the pool to accept the call.
called_party_number	Specified called party DNIS number. This is the number that the remote clients use to dial in to the access server. You can have more than one DNIS number per modem pool. To set the DNIS number, see the **copy modem** command.
max conn allowed	Maximum number of modems that a called party DNIS number can use, which is an overflow protection measure. To set this feature, see the **copy modem** command.
max-conn exceeded	Number of times an incoming call using this called party DNIS number was rejected because the **max-conn** *number* parameter specified by the **called-number** command was exceeded.

Related Commands

Command	Description
called-number (modem pool)	Assigns a called party number to a pool of modems.
clear modempool-counters	Clears active or running counters associated with one or more modem pools.
copy modem	Copies modem firmware to integrated modems in access servers.
modem-pool	Creates a new modem pool or specifies an existing modem pool, which allows you to physically or virtually partition your access server for dial-in and dial-out access.
pool-member	Assigns a range of modems to a modem pool.

show nbf cache

To display NetBIOS name cache contents, use the **show nbf cache** command in EXEC mode.

show nbf cache

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.

Examples

The following is sample output from the **show nbf cache** command:

```
Router# show nbf cache

HW Addr           Name        How     Idle   NetBIOS Packet Savings
1000.5a89.449a    IKBA         E0      6      0
0000.0000.0000    NANOO        async1  21     0
```

Table 89 describes significant fields shown in the display.

Table 89 show nbf cache Field Descriptions

Field	Description
HW Addr	MAC address mapped to the NetBIOS name in this entry.
Name	NetBIOS name mapped to the MAC address in this entry.
How	Interface through which this information was learned.
Idle	Period of time (in seconds) since this entry was last accessed. A hyphen in this column indicates a static entry in the NetBIOS name cache.
NetBIOS Packet Savings	Number of packets to which local replies were made (thus preventing transmission of these packets over the network).

Related Commands

Command	Description
ppp multilink group	Restricts a physical link to joining only a designated multilink-group interface.
netbios access-list	Defines an IPX NetBIOS FindName access list filter.
netbios input-access-filter host	Defines a station access list filter on incoming messages. The access lists of station names are defined in **netbios access-list** host commands.

Command	Description
netbios name-cache	Defines a static NetBIOS name cache entry, tying the server with the name netbios-name to the mac-address, and specifying that the server is accessible either locally through the interface-name specified, or remotely through the ring-group group-number specified.
netbios output-access-filter host	Defines a station access list filter on outgoing messages.
show nbf sessions	Displays NetBEUI connection information.

show nbf sessions

To display NetBEUI connection information, use the **show nbf sessions** command in EXEC mode.

show nbf sessions‘

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.

Examples

The following is sample output from the **show nbf sessions** command:

```
Router> show nbf sessions

Async6 NetBIOS Session Table:
Srcnum   Destnum  Dest-Interface DestMAC
8        6         Ethernet0 00aa.005b.c17b

NetBIOS Global Session Table:
Srcnum   Destnum   Dest-Interface DestMAC  Src-Interface SrcMac(I)


6        8         Async7 0000.0000.0000  Ethernet0 00aa.005b.c17b(95)
ADD_[GROUP]NAME_QUERY queuesize=0
STATUS_QUERY queuesize=0
STATUS_RESPONSE queuesize=0
NAME_QUERY queuesize=0
NAME_RECOGNIZED queuesize=0
SESSION_INITIALIZE queuesize=0
SESSION_INITIALIZE (pending) queuesize=0
```

Table 90 describes the significant fields shown in the display.

Table 90 show nbf sessions Field Descriptions

Field	Description
Interface NetBIOS Session Table:	Summarizes Async/ISDN interface NetBIOS connection information.
Srcnum, Destnum	Source and destination connection numbers.
Dest-Interface, DestMAC	Destination interface and MAC address.
Global NetBIOS Session Table:	Summarizes LAN NetBIOS connection information.
Dest-Interface DestMAC	Destination interface (Async7 in this case) and MAC address (0000.0000.0000 in this case).

Table 90 show nbf sessions Field Descriptions (continued)

Field	Description
Src-Interface SrcMac	Source interface (Ethernet0 in this case) and MAC address (00aa.005b.c17b(95) in this case).
NetBIOS Datagram Queue Summary:	Summarizes NetBIOS pending datagram queues.
ADD_[GROUP]NAME_ QUERY	Add Group Name Query packets.
STATUS_QUERY	Status Query packets.
STATUS_RESPONSE	Status Response packets.
NAME_QUERY	Name Query packets.
NAME_RECOGNIZED	Name Recognized packets.
SESSION_INITIALIZE (pending)	NetBIOS session Initialize packets.

Related Commands

Command	Description
ppp multilink group	Restricts a physical link to joining only a designated multilink-group interface.
netbios access-list	Defines an IPX NetBIOS FindName access list filter.
netbios input-access-filter	Controls incoming IPX NetBIOS FindName messages.
netbios name-cache	Defines a static NetBIOS name cache entry, tying the server with the name netbios-name to the mac-address, and specifying that the server is accessible either locally through the interface-name specified, or remotely through the ring-group group-number specified.
netbios output-access-filter	Controls outgoing NetBIOS FindName messages.
show nbf cache	Displays NetBIOS name cache contents.

show plat hardware qfp active feature ess state pppoe

To display Quantum Flow Processor (QFP) edge switch services active instance state information for a PPP over Ethernet (PPPoE) client, use the **show plat hardware qfp active feature ess state pppoe** command in privileged EXEC mode.

show plat hardware qfp active feature ess state pppoe [**unknown-history**]

Syntax Description

unknown-history	(Optional) Displays information about the unknown session reporting history.

Command Default

Information about all PPPoE sessions are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.6	This command was modified. This command was extended to include PPPoE unknown session information.

Usage Guidelines

You can use the **show plat hardware qfp active feature ess state pppoe** command to display the number of data packets received in QFP for the unknown PPPoE sessions and the number of unknown sessions that have been reported to the Cisco IOS router. For example, if the QFP receives 100 data packets for one unknown PPPoE session, then the total number of packets received will be 100 and one session will be reported.

Cisco IOS router sends a PPPoE active discovery terminate (PADT) message to tear down reported unknown PPPoE sessions if the **sessions auto cleanup** command is configured in the Broadband Access Aggregation (BBA) group.

Examples

The following is sample output from the **show plat hardware qfp active feature ess state pppoe** command:

```
Router# show plat hardware qfp active feature ess state pppoe

ESS PPPOE State:
  Current number of segments: 0

PPPoE Session Lookup Depth:
  Distribution: 100%

PPPoE Unknown Session Handling:
  Reporting Rate(PPS)      : 100
  Refreshing Period(Second): 90
```

```
Current period:
  Start     : Dec 10 01:59:51
  Checked   : 0
  Reported  : 0
```

Table 91 describes the significant fields shown in the display.

Table 91 show plat hardware qfp active feature ess state pppoe Field Descriptions

Field	Description
ESS PPPOE State:	Current state of the Enterprise Storage Server (ESS).
Current number of segments:	Total number of segments.
PPPoE Session Lookup Depth:	Lookup depth of the PPPoE session, in percentage.
Distribution:	Distrubution value, in percentage.
PPPoE Unknown Session Handling:	Details about handling the PPPoE unknown sessions.
Reporting Rate(PPS):	Reporting rate in packets per second.
Refreshing Period(Second):	Time taken to refresh, in seconds.
Current period:	Current status.
Start:	Date and time at which the command was executed.
Checked:	Total number of data packets for the unknown PPPoE sessions received by the QFP.
Reported:	Total number of unknown sessions that have been reported to the Cisco IOS router.

Related Commands

Command	Description
sessions auto cleanup	Configures an aggregation device to attempt to recover PPPoE sessions that failed after reload by notifying CPE devices about the PPPoE session failures.

show port config

To display the configuration parameters of the active session for the specified port or the specified port range, use the **show port config** command in EXEC mode.

Cisco AS5400 with the NextPort Dial Feature Card (DFC)

show port config {*slot* | *slot*/*port*}

Cisco AS5800 with the Universal Port Card (UPC)

show port config {*shelf*/*slot* | *shelf*/*slot*/*port*}

Syntax Description

slot	All ports on the specified slot. For the Cisco AS5350 slot values range from 1to 3. For the Cisco AS5400, slot values range from 1to 7.
slot/*port*	All ports on the specified slot and service processing element (SPE). For the Cisco AS5350 slot values range from 1to 3. For the Cisco AS5400, slot values range from 1to 7. The port values range from 0 to one less than the number of ports supported by the card. You must include the slash mark.
shelf/*slot*	All ports on the specified shelf and slot. For the Cisco AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11. You must include the slash mark.
shelf/*slot*/*port*	All ports on the specified SPE. For the Cisco AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and port values range from 0 to one less than the number of ports supported by the card. You must include the slash marks.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5400 and Cisco AS5800.
12.2(2)XA	This command was implemented on the Cisco AS5350.
12.2(2)XB1	This command was integrated into Cisco IOS Release 12.2(2)XB1.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

The port should have an associated active session when the **show port config** command is executed.

Note The **show port config** command is similar to the **show modem config** MICA technologies modem command.

Examples

The following example shows output from the **show port config** command on the Cisco AS5400 with the NextPort DFC. This example shows port configuration for the modem service port slot 1, port 0.

```
Router# show port config 1/0

Service Type                              :Modem service
Originate/Answer Mode                     :Answer
Data Bits Selection                       :8
Parity Selection                          :No Parity
Stop bits Selection                       :1
V.42 ODP generation                       :Enabled
EC Autodetect Time-out                    :5000 ms
Protocol Negotiation Time-out             :10000 ms
Protocol Negotiation Fallback character   :13
Protocol Negotiation Retransmission Limit :12
EC Min, Max Octets Frame length           :256
Data Compression                          :V.44Tx   V.44Rx
ARA Error Correction                      :ARA1.0 & ARA2.0 Disabled
V.42 Error Correction                     :V.42(LAP-M) Originate&Answer enabled
MNP Error Correction                      :MNP Originate&Answer enabled
Link Protocol Fallback                    :Async Framing (Start/Stop/Parity)
Calling Tone                              :Disabled
Guard Tone                                :Disabled
Modem Standard                            :V.90 Automode
Max Non-PCM Connect Rate                  :33600 bps
Min Non-PCM Connect Rate                  :300 bps
Max PCM Connect Rate                      :60000 bps
Min PCM Connect Rate                      :28000 bps
Signal Quality Threshold                  :Bit Errors >= 1:1000 cause recovery
Fallback/Fallforward Squelch Timer        :500 ms
Fall Forward Timer                        :10000 ms
Fall Back Timer                           :500 ms
Terminate Time-out                        :20 secs
Wait for Data Mode Time-out               :60 secs
Lost Carrier To Hang-up Delay             :1400 ms
PCM Transmit Level Setting                :-13 dBm
Retrain Limit                             :4
V.34 Max Symbol Rate                      :3429 Baud
V.34 Min Symbol Rate                      :2400 Baud
V.34 Carrier Frequency                    :Auto Carrier Selection
V.34 Preemphasis Filter Selection         :11
+++ Escape Detection                      :Enabled-in-Originate-Mode-Only
AT Command Processor                      :Enabled
Call Setup Delay                          :0 ms
Automatic Answer Delay                    :2 secs
Escape Detection Character                :ASCII 43 (+)
Carriage Return Character                 :ASCII 13 (CR)
Line Feed Character                       :ASCII 10 (LF)
Backspace Character                       :ASCII 8 (BS)
Pause Before Blind Dialing                :2 secs
Comma Dial Modifier Time                  :2 secs
MOH Timeout                              :No limit
QC Configuration                         :Enabled ANSpcm Level -12dBm
V.44 Max Tx Codewords                     :256
V.44 Max Rx Codewords                     :256
V.44 Max Tx String Length                  :32
V.44 Max Rx String Length                  :32
V.44 Max Tx History Size                   :256
V.44 Max Rx History Size                   :256
```

The following example shows port configuration information for a digital service port slot 1, port 8 on the Cisco AS5800 with the UPC:

```
Router# show port config 1/8

Shelf/Slot/SPE/Port -- 1/8/27/165
Service Type                                : Modem service
Originate/Answer Mode                       : Answer
Data Bits Selection                         : 8
Parity Selection                            : No Parity
Stop bits Selection                         : 1
V.42 ODP generation                         : Enabled
EC Autodetect Time-out                      : 5000 ms
Protocol Negotiation Time-out               : 10000 ms
Protocol Negotiation Fallback character     : 13
Protocol Negotiation Retransmission Limit   : 12
EC Min, Max Octets Frame length             : 256
Data Compression                            : V.42bis or MNP5
ARA Error Correction                        : ARA1.0 & ARA2.0 Disabled
V.42 Error Correction                       : V.42(LAP-M) Originate&Answer enabled
MNP Error Correction                        : MNP Originate&Answer enabled
Link Protocol Fallback                      : Async Framing (Start/Stop/Parity)
Calling Tone                                : Disabled
Guard Tone                                  : Disabled
Modem Standard                              : V.90 Automode
Max Non-PCM Connect Rate                    : 33600 bps
Min Non-PCM Connect Rate                    : 300 bps
Max PCM Connect Rate                        : 60000 bps
```

Table 92 describes the significant fields shown in the displays.

Table 92 show port config Field Descriptions

Field	Description
Service Type	Digital or analog service type.
Originate/Answer Mode	Answer or originate. Default is answer.
Data Bits Selection	7, 8, or 9 data bits. Default is 8.
Parity Selection	0 = no parity, 1 = even parity, 2 = odd parity. Default is no parity.
Stop bits Selection	1 or 2 stop bits. Default is 1 stop bit.
V.42 ODP generation	Disabled or generate ODP sequence when originating a V.42 call. Default is Generate ODP sequence when originating a V.42 call.
EC Autodetect Time-out value	Maximum period, in milliseconds (ms), during which the modem will run an automated detection machine upon the incoming data. Default is 5000 ms.
Protocol Negotiation Time-out	Maximum wait (in ms) for error correction protocol negotiation before fallback. Default is 10000 ms.
Protocol Negotiation Fallback Character	0 to 127. Default is 13.
Protocol Negotiation Retransmission Limit	0 = Do not disconnect on excessive retransmission; 1 to 255 = number of successive retransmissions to cause disconnect. Default is 12.
EC Min, Max Octets Frame Length	Buffer length; 64 to 1024 octets of data. Default is 256.

Table 92 show port config Field Descriptions (continued)

Field	Description
Data Compression	Disabled, V.42bis, MNP5, or V.42bis or MNP5 (V.42 has precedence). Default is V.42bis or MNP5 (V.42 has precedence).
ARA Error Correction	ARA1.0 & ARA2.0 Disabled, Enabled for Answer only, Enabled for Answer originate ARA1.0, and Enabled for Answer originate ARA2.0. Default is Enabled for Answer only.
V.42 Error Correction	V.42(LAP-M) Disabled, V.42(LAP-M) Originate&Answer enabled. Default is Disabled.
MNP Error Correction	MNP Disabled or MNP Originate&Answer enabled. Default is MNP Originate&Answer enabled.
Link Protocol Fallback	Asynch Framing (Start/Stop/Parity), Synchronous framing (Raw 8 bits to DSP), or Disconnect (Hang-up). Default is Asynch Framing (Start/Stop/Parity).
DSP processor MVIP TDM slice	0 to 15.
Calling Tone	Disabled or Send calling tone. Default is Disabled.
Guard Tone	Disabled, Use Guard tone (V.22 & V.22bis only). Default is Disabled.
Modem Standard	V.34bis Automode with terbo, V.34bis Automode skip terbo, V.32 terbo Automode, V.32bis Automode, V.22bis Automode, or K56Flex 1.1. Default is V.34bis Automode with terbo.
Max. Connect Rate	75 to 56000 bits per second (bps).
Min. Connect Rate	75 to 56000 bps.
Signal Quality Threshold	No action on bit errors, Bit Errors >=1:100 cause recovery, Bit Errors >=1:1000 cause recovery, Bit Errors >=1:10000 cause recovery, Bit Errors >=1:100000 cause recovery, or Bit Errors >=1:1000000 cause recovery. Default is 1:1000.
Fallback/Fallforward Squelch Timer	Time to delay (in ms) after a speed shift before allowing another speed shift. Default is 500 ms.
Fall Forward Timer	Elapsed time (in ms) with continuous good signal quality to cause a fall forward. Default is 10000 ms.
Fall Back Timer	Elapsed time (in ms) with bad signal quality to cause a fallback. Default is 500 ms.
Terminate Time-out	Elapsed time (in seconds) after a disconnect request before forcing a link disconnection. During this period, the modem sends buffered data and then clears down the link. Default is 20 seconds.
Wait for Data Mode Time-out	Maximum time (in seconds) during link establishment before disconnection. Default is 40; 60 for K56Flex.
Lost Carrier To Hang-up Delay	Maximum time (in ms) without a carrier to cause the link disconnect. Default is 1400 ms.
PCM Transmit Level Setting	6d Bm, 7 dBm, 8 dBm, –20 dBm, or –21 dBm. Default is 9 dBm.
Retrain Limit	Maximum successive failed retrains to cause the link to disconnection. Default is 4.

Table 92 show port config Field Descriptions (continued)

Field	Description
V.34 Max. Symbol Rate	2400 baud, 2743 baud, 2800 baud, 3000 baud, 3200 baud, or 3429 baud. Default is 3429 baud.
V.34 Min. Symbol Rate	2400 baud, 2743 baud, 2800 baud, 3000 baud, 3200 baud, or 3429 baud. Default is 2400 baud.
V.34 Carrier Frequency	Low Carrier, High Carrier, or Auto Carrier Selection. Default is High Carrier.
V.34 Preemphasis Filter Selection	0 to 10 = a selected filter; 11 = Automatic Preemphasis Selection. Default is 11.
Tx and Rx Signaling Type	NULL signaling, MF signaling, DTMF signaling, Lower band R2 signaling, Upper band R2 signaling, or R1 signaling. Default is NULL signaling.
Call Progress Tone Detection	No tone detection, Dial tone detection, Ring-Back tone detection, or Busy tone detection. Default is No tone detection.
+++ Escape Detection	Disabled, Enabled, or Enabled-in-Originate-Mode-Only. Default is Enabled-in-Originate-Mode-Only.
AT Command Processor	Disabled or Enabled. Default is Disabled.
Call Set Up Delay	No delay before link initiation, delay value (1 to 255 ms). Default is No delay.
Automatic Answer	Answer immediately, delay value (1 to 255 seconds). Default is 1 second.
Escape Detection Character	ASCI value (0 to 127). Default is 43.
Carriage Return Character	ASCI value (0 to 127). Default is 13.
Line Feed Character	ASCI value (0 to 127). Default is 10.
Backspace Character	ASCI value (0 to 127). Default is 8.
Pause Before Blind Dialing	2 to 255 seconds. Default is 2.
Wait For Carrier After Dial	Wait for data mode timeout.
Comma Dial Modifier Time	2 to 255 seconds. Default is 2.

Related Commands

Command	Description
show port operational-status	Displays the operational status of a specific port or port range.

show port digital log

To display the data event log for digital modems, use the **show port digital log** command in EXEC mode.

show port digital log [**reverse** *slot*/*port*] [*slot* | *slot*/*port*]]

Syntax Description

reverse	(Optional) Displays a report with the most recent entry first.
slot	(Optional) All ports on the specified slot. For the Cisco AS5400, slot values range from 1to 7.
slot/*port*	(Optional) All ports on the specified slot and service processing element (SPE). For the Cisco AS5400, slot values range from 1to 7 and port values range from 0 to one less than the number of ports supported by the card. You must include the slash mark.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5400.
12.1(5)XM1	This command was implemented on the Cisco AS5350 universal gateway.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.

Usage Guidelines

Note This command is not supported on the Cisco AS5800 with the Universal Port DFC.

Examples

The following is sample output from the **show port digital log** command on the Cisco AS5400 with the NextPort DFC:

```
Router# show port digital log

Port 5/00 Events Log
  00:02:41: incoming called number: 35140
     Service type: DIGITAL_DATA
     Session State: IDLE
     Service type: DIGITAL_DATA
     Session State: ACTIVE
  00:02:41: Digital State event:
            State: Steady
  00:02:40: Digital Static event:
    Connect Protocol                        :   V.110
    Data Bits                               :   8
    Parity                                  :   0
```

```
    Stop Bits                              :   1
    TX,RX Bit Rate                         :   19200, 19200
Port 5/01 Events Log
  00:02:42: incoming called number: 35140
     Service type: DIGITAL_DATA
     Session State: IDLE
     Service type: DIGITAL_DATA
     Session State: ACTIVE
  00:02:41: Digital State event:
           State: Steady
  00:02:41: Digital Static event:
    Connect Protocol                       :   V.110
    Data Bits                              :   8
    Parity                                 :   0
    Stop Bits                              :   1
    TX,RX Bit Rate                         :   19200, 19200
Port 5/02 Events Log
  00:02:42: incoming called number: 35140
     Service type: DIGITAL_DATA
     Session State: IDLE
     Service type: DIGITAL_DATA
     Session State: ACTIVE
  00:02:42: Digital State event:
           State: Steady
  00:02:42: Digital Static event:
    Connect Protocol                       :   V.110
    Data Bits                              :   8
    Parity                                 :   0
    Stop Bits                              :   1
    TX,RX Bit Rate                         :   19200, 19200
Port 5/03 Events Log
  00:02:43: incoming called number: 35140
     Service type: DIGITAL_DATA
     Session State: IDLE
     Service type: DIGITAL_DATA
     Session State: ACTIVE
  00:02:43: Digital State event:
           State: Steady
  00:02:43: Digital Static event:
    Connect Protocol                       :   V.110
    Data Bits                              :   8
    Parity                                 :   0
    .
    .
    .
```

Table 93 describes the significant fields shown in the display.

Table 93 show port digital log Field Descriptions

Field	Description
Port	The port and slot with the events log of current session.
incoming called number	The incoming called number.
Service type	The type of digital service, data or voice.
Session State	The condition of the current state, active or idle.

Table 93 show port digital log Field Descriptions (continued)

Field	Description
Digital State event:	The digital state. Values are as follows: 0—IDLE state 10—CONNECTING state 30—Steady 50—TERMINATING state
Connect Protocol	The data carrier connect standard used to support the rates of bits per second (bps).
Data Bits	The number of data bits, 7, 8, or 9. Default is 8.
Parity	The parity selection of 0 = no parity, 1 = odd parity. Default is no parity.
Stop Bits	The selection of stop bits, 1 or 2. Default is 1.
TX, RX Bit Rate	The transmit and receive bit rate. For RX, the bit rate is from the remote service provider to the local service provider. For TX, the bit rate is from the local service provider to the remote service provider.
Events Log	Displays the log of events for that port.

Related Commands

Command	Description
clear port digital log	Clears specific service events.
clear port log	Clears all event entries in the port level history event log.
show port digital log	Displays port events with the most recent event first.

show port log

To display the service events generated by the sessions, use the **show port log** command in privileged EXEC mode.

show port {**fax** | **voice**} **log** [**reverse**] [*slot/port*] [*slot* | *slot/port*]

Syntax Description

fax	Displays the fax data event log.
voice	Displays the voice data event log.
reverse	(Optional) Displays the port history event log with the most recent event first.
slot/port	(Optional) Displays information for all ports on the specified slot and service processing element (SPE). Slot values range from 1 to 7 and port values range from 0 to 107. You must include the slash mark.
slot	(Optional) Displays information for all ports on the specified slot. Slot values range from 1 to 7.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5400 and Cisco AS5800.
12.1(5)XM2	This command was integrated into Cisco IOS Release 12.1(5)XM2.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350 and Cisco AS5400 platforms.
12.3(4)T	Voice activity detection (VAD) background noise, echo return loss (ERL) level, and Acombined (ACOM) level were replaced with average values for each statistic in the output. A new field was added for the average echo canceller (ECAN or EC) background noise.
12.3(14)T	T.38 fax relay call statistics were made available to Call Detail Records (CDRs) through Vendor-Specific Attributes (VSAs) and added to the call log.

Examples

The following example shows value averages for VAD background noise, ERL level, ACOM level, and EC background noise level. Relevant fields in the output are shown in bold.

```
Router# show port voice log 1/0

Port 1/00 Events Log
  *Aug 22 07:59:27.515:Voice Terminate event:
    Disconnect Reason                 :  normal call clearing (16)
    Call Timer                        :  57  secs
    Current playout delay             :  65  ms
    Min/Max playout delay             :  65/105  ms
    Clock offset                      :  142003  ms
    Predictive concealment            :  0  ms
```

```
  Interpolative concealment          :  0  ms
  Silence concealment                :  0  ms
  Buffer overflow discards           :  1
  End-point detection errors         :  0
  Tx/Rx Voice packets                :  2813/2816
  Tx/Rx signaling packets            :  0/0
  Tx/Rx comfort noise packets        :  0/0
  Tx/Rx duration                     :  56260/56260  ms
  Tx/Rx voice duration               :  0/0  ms
  Out of sequence packets            :  0
  Bad protocol headers               :  0
  Num. of late packets               :  0
  Num. of early packets              :  1
  Tx/Rx Power                        :  -87.0/-57.3  dBm
  Tx/Rx Mean                         :  -86.7/-57.0  dBm
  Average VAD Background noise level :  6.2  dBm
  Average ERL level                  :  127.0  dB
  Average ACOM level                 :  127.0  dB
  Tx/Rx current activity             :  silence/silence
  Tx/Rx byte count                   :  450080/450240
  Average ECAN Background noise level:  -83.4  dBm
*Aug 22 07:59:27.515:Voice SSRC change events:
  Latest ssrc value                  :  391643394
  Total ssrc changes                 :  1
```

The following example shows output for the Cisco AS5400 with the universal port Dial Feature Card (DFC). The example shows the port voice history event log for slot 4, port 0.

```
Router# show port voice log 4/0

03:36:26: incoming caller number: 11001
03:36:26: incoming called number: 21001
03:36:26: Voice Connect event:
Voice Codec : G.711 a-law
Echo Canceler Length : 64 taps
Digit detection enable : DTMF signaling - enabled
Echo Cancellation Control : Echo cancellation - enabled
Echo update - enabled
Non-linear processor - enabled
Echo reset coefficients -
disabled
High pass filter enable -
disabled
Comfort noise generation : Generate comfort noise
Voice activity detection : Disabled
Information field size : 20 ms
Digit relay enable : OOB Digit relay -
disabled
IB Digit relay -
disabled
Encapsulation protocol : RTP
Playout de-jitter mode : adaptive
Input Gain : 0 dB
Output Gain : 0 dB
Tx/Rx SSRC : 0/0
03:36:27: Voice Terminate event:
Disconnect Reason : Non-specific host disconnect
Call Timer : 122 secs
Current playout delay : 30 ms
Min/Max playout delay : 25/45 ms
Clock offset : 528623613 ms
Predictive concealment : 0 ms
Interpolative concealment : 0 ms
Silence concealment : 0 ms
```

```
Buffer overflow discards : 0
End-point detection errors : 0
Tx/Rx Voice packets : 6130/6130
Tx/Rx signaling packets : 0/0
Tx/Rx comfort noise packets : 0/0
Tx/Rx duration : 122615/122615
Tx/Rx voice duration : 90000/82000
:
Out of sequence packets : 0
Bad protocol headers : 0
Num. of late packets : 0
Num. of early packets : 0
Tx/Rx Power : 932/101 dBm
Tx/Rx Mean : 364/325 dBm
:
Background noise level : -1 dBm
ERL level : 623 dB
ACOM level : 586 dB
Tx/Rx current activity : silence/silence
```

Table 94 describes the significant fields shown in the display.

Table 94 show port log Field Descriptions

Field	Description
incoming caller number	The incoming caller number.
incoming called number	The incoming called number.
Voice Codec	Codec used for the current call.
Echo Canceler Length	Length of echo canceler in number of taps. Ranges from 1 to 1024 (128 milliseconds [ms]).
Digit detection enable	Bit mask where 1 = enabled, 0 = disabled, Bit 0 = dual tone multifrequency (DTMF) signaling detection.
Echo Cancellation Control	Bit mask where 1 = enabled, 0 = disabled. Bit 0: Echo cancellation enable. Bit 1: Echo update enable. Bit 2: Nonlinear processor enable. Bit 3: Echo reset coefficients (single shot). Bit 4: High pass filter disable. Bits 5—15: reserved (set to 0).
Echo update	Bit 1: Echo update enable.
Non-linear processor	Bit 2: Nonlinear processor enable.
Echo reset coefficients	Bit 3: Echo reset coefficients (single shot).
High pass filter enable	Bit mask where 1 = enabled, 0 = disabled Bit 0 = Echo cancellation enable. Bit 1: Echo update enable Bit 2: Nonlinear processor enable Bit 3: Echo reset coefficients (single shot) Bit 4: High pass filter disable Bits 5—15: reserved (set to 0)

Table 94 show port log Field Descriptions (continued)

Field	Description
Comfort noise generation	0 = generate silence - G.711 only, 1 = generate comfort noise.
Voice activity detection	0 = disabled, 1 = enabled.
Information field size	Maximum size (in ms) of information field in fax relay packets. The range is 0 to 90 ms.
Digit relay enable	Bit mask where 1 = enabled, 0 = disabled, Bit 0 = Digit Passthrough suppression.
IB Digit relay	Bit 1 = IB Digit Relay.
Encapsulation protocol	1 = RTP (VoIP), 2 = FRF.11 (VoFR), 3 = VoATM.
Playout de-jitter mode	0 = fixed, 1 = adaptive.
Input Gain	–6.0 to 6.0 in 0.1 decibel (dB) increments.
Output Gain	0 to –14.0 in 0.1 dB increments.
Disconnect Reason	Disconnect reason.
Call Timer	In seconds.
Current playout delay	Current playout delay estimate (in ms).
Min/Max playout delay	Minimum and Maximum playout delay encountered (in ms).
Clock offset	Clock offset value (in ms).
Predictive concealment	Cumulative duration (in ms).
Interpolative concealment	Cumulative duration (in ms).
Silence concealment	Cumulative duration (in ms).
Buffer overflow discards	Cumulative number buffer overflow errors.
End-point detection errors	Cumulative number of endpoint detection errors.
Tx/Rx SSRC	Value of Tx/Rx SSRC in the Routing Table Protocol (RTP) header.
Tx/Rx Voice packets	Cumulative count of voice packets sent and received.
Tx/Rx signaling packets	Cumulative count of signaling packets sent and received.
Tx/Rx comfort noise packets	Cumulative count of comfort noise packets sent and received.
Tx/Rx duration	Total duration of voice transmission and reception (in ms).
Tx/Rx voice duration	Total duration of voice transmission and reception (in ms).
Out of sequence packets	Cumulative count of packets received out of sequence.
Bad protocol headers	Cumulative count of packets received with bad protocol headers.
Num. of late packets	Cumulative count of packets received late.
Num. of early packets	Cumulative count of packets received early.
Tx/Rx Power	Current power of sent and received signal (to time-division multiplexing [TDM]) in 0.1 dBm increments.
Tx/Rx Mean	Average power of sent and received signal (to TDM) in 0.1 dBm increments.

Table 94 show port log Field Descriptions (continued)

Field	Description
Background noise level	Current background noise level estimate in 0.1 decibel (dB) increments.
ERL level	Current Echo Return Loss (ERL) level estimate in 0.1 dB increments.
ACOM level	Current ACOM level estimate in 0.1 dB increments. The term ACOM is used in G.165, *General Characteristics of International Telephone Connections and International Telephone Circuits: Echo Cancellers*. ACOM is the combined loss achieved by the echo canceller, which is the sum of the ERL, ERL enhancement, and nonlinear processing loss for the call.
Tx/Rx current activity	0 = silence, 1 = voice.

The following example shows output for the Cisco AS5400 with the universal port DFC. The example shows the port fax history event log for slot 1, port 0.

```
Router# show port fax log 1/0

Port 1/00 Events Log
Port 1/01 Events Log
Port 1/02 Events Log
  *Jan  1 18:39:30.499 UTC: Fax-relay Connect event:
    Max. transmission rate             :   4800 bps
    Information field size             :   20  ms
    TCF generation                     :   transparent
    Transmit level                     :   -10  dBm
    Encapsulation protocol             :   UDPTL
    IFP Payload Type                   :
    ECM Disable                        :   Disabled
```

The following example shows output for the Cisco AS5350 on shelf 1, slot 3 with the T.38 Fax Relay statistics:

```
Router# show port fax log 1/3

Port 1/03 Events Log
  May  7 21:32:22.556 UTC: Fax-relay Connect event:
    Max. transmission rate             :   14400 bps
    Information field size             :   20  ms
    TCF generation                     :   transparent
    Transmit level                     :   -10  dBm
    Encapsulation protocol             :   UDPTL
    ECM Disable                        :   Not disabled
    1 bytes of link info not formatted      :   0x01 0x00
Fax-relay Terminate event:
    Disconnect Reason                  : 0
    Call Timer                         : 55  secs
    Current playout delay              : 80  ms
    Min/Max playout delay              : 1/560  ms
    Buffer underflow discard           : 0
    Buffer overflow discard            : 0
    End-point detection errors         : 0
    Tx/Rx Fax packets                  : 1580/90
    Tx/Rx duration                     : 32856/6193  ms
    Tx/Rx pages                        : 1/0
    Out of sequence packets            : 0
    Bad protocol headers               : 0
    Fax state                          : Idle
!
```

```
    Current signal level               : 42  dBm
    Phase jitter                       : 0  degrees
    Frequency offset                   : 0  Hz
    EQM                                : 0
    Packet loss concealment count      : 0
    TX/RX Byte Count                   : 0/76
    Recent HS Modulation               : V.17/short/14400
    ECM in use                         : 1
```

The following example shows output for the Cisco AS5350 on shelf 1, slot 3 with the T.38 fax relay statistics:

```
Router# show port fax log 1/3

Port 1/03 Events Log
  May  7 21:32:22.556 UTC: Fax-relay Connect event:
    Max. transmission rate             :   14400 bps
    Information field size             :   20  ms
    TCF generation                     :   transparent
    Transmit level                     :   -10  dBm
    Encapsulation protocol             :   UDPTL
    ECM Disable                        :   Not disabled
    1 bytes of link info not formatted      :   0x01 0x00
Fax-relay Terminate event:
    Disconnect Reason                  : 0
    Call Timer                         : 55  secs
    Current playout delay              : 80  ms
    Min/Max playout delay              : 1/560  ms
    Buffer underflow discard           : 0
    Buffer overflow discard            : 0
    End-point detection errors         : 0
    Tx/Rx Fax packets                  : 1580/90
    Tx/Rx duration                     : 32856/6193  ms
    Tx/Rx pages                        : 1/0
    Out of sequence packets            : 0
    Bad protocol headers               : 0
    Fax state                          : Idle
!
    Current signal level               : 42  dBm
    Phase jitter                       : 0  degrees
    Frequency offset                   : 0  Hz
    EQM                                : 0
    Packet loss concealment count      : 0
    TX/RX Byte Count                   : 0/76
    Recent HS Modulation               : V.17/short/14400
    ECM in use                         : 1
```

Table 95 lists the significant fields displayed in the output of **show port fax log** command:

Table 95 show port fax log Field Descriptions

Field	Description
Max. transmission rate	0: No Limit. 1: 2400 bits per second (bps). 2: 4800 bps. 3: 7200 bps. 4: 9600 bps. 5: 12000 bps. 6: 14400 bps.
Information field size	Maximum size of information field in fax relay packets. The range is 0 to 90 ms.
TCF generation	0: transparent (remote). 1: controlled (local).
Transmit level	Transmit level of remodulator (in decibels per milliwatt [dBm]): –10 to –21.
Encapsulation protocol	1: UDPTL (T.38—VoIP) (default). 2: FRF.11 (VoFR). 3: RTP (IFP in RTP).
IFP Payload Type	0 to 127. Negotiated payload type for fax relay over RTP. (Valid only when encapsulation protocol is RTP.)
ECM Disable	0 - Error Correction Mode (ECM) is not disabled. 1 - ECM is disabled.
Disconnect Reason	Disconnect Reason.
Call Timer	Call timer in seconds.
Current playout delay	Current playout delay estimate in milliseconds (ms).
Min/Max playout delay	Minimum and maximum playout delay encountered in ms.
Buffer underflow discard	Cumulative number of buffer underflow errors.
Buffer overflow discard	Cumulative number of buffer overflow errors.
End-point detection errors	Cumulative number of endpoint detection errors.
Tx/Rx Fax packets	Cumulative count of fax packets sent and received.
Tx/Rx duration	Total duration of fax transmission and reception in ms.
Tx/Rx pages	Total pages of fax transmitted and received.
Out of sequence packets	Cumulative count of packets received out of sequence.
Bad protocol headers	Cumulative count of packets received with bad protocol headers.
Fax state	Idle.
Current signal level	Current sent and received signal level estimate in dBm.

Table 95 show port fax log Field Descriptions (continued)

Field	Description
Phase jitter	Measured amount of phase jitter which indicates how large the “rocking” is in degrees. On an oscilloscope, the constellation points would look like crescent moons. Values can range up to 15 degrees. The typical value is 0 (that is, phase jitter is not normally present).
Frequency offset	The difference (in hertz) between the expected RX carrier frequency and the actual RX carrier frequency.
EQM	Eye Quality Monitor (EQM) provides an assessment of line quality during transmission of both high speed (V.29, V.17, etc) and low speed (V.21) data.
Packet loss concealment count	Packet loss concealment count.
Tx/Rx Byte Count	Number of bytes sent and received.
Recent HS Modulation	Recent high-speed modulation used.
ECM in use	0 - Error Correction Mode (ECM) is not in use. 1 - ECM is in use.

Related Commands

Command	Description
clear port log	Clears all port log events.
show port operational-status	Displays active session statistics.

show port modem calltracker

To display the port-level information for an active modem, use the **show port modem calltracker** command in EXEC mode.

Cisco AS5350 and Cisco AS5400 with the NextPort Dial Feature Card (DFC)

show port modem calltracker [*slot* | *slot*/*port*]

Cisco AS5800 with the Universal Port Card (UPC)

show port modem calltracker [*shelf*/*slot* | *shelf*/*slot*/*port*]

Syntax Description

slot	(Optional) All ports on the specified slot. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7.
slot/*port*	(Optional) All ports on the specified slot and service processing element (SPE). For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7. Port values range from 0 to one less than the number of ports supported by the card. You must include the slash mark.
shelf/*slot*	(Optional) All ports on the specified shelf and slot. For the Cisco AS5800, shelf values range from 0 to 1 and Universal Port Card (UPC) slot values range from 2 to 11. You must include the slash mark.
shelf/*slot*/*port*	(Optional) The specified port range on a shelf and slot. For the Cisco AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 1to 323. You must type in the forward slashes (/).

Command Modes

EXEC

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5400 and Cisco AS5800.
12.1(5)XM1	This command was implemented on the Cisco AS5350 universal gateway.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.

Usage Guidelines

When there is no call on the specified port, the most recent call information is displayed. This command uses the Call Tracker database. To enable Call Tracker, enter the **calltracker enable** global configuration command.

Examples

The following is sample output from the **show port modem calltracker** command on the Cisco AS5400 with the NextPort DFC. This example shows output for slot 3, port 3:

```
Router# show port modem calltracker 3/3

------------------------- call handle=        62 -------------------------
status=Active, service=PPP, origin=Answer, category=Modem
DS0 slot/port/ds1/chan=4/7/7/0, called=124, calling=(n/a)
userid=as5300-ref2, ip=192.169.124.1, mask=255.255.255.0
setup=06/22/2000 21:50:47, conn=6.77, phys=25.00, service=29.83, authen=29.83
init rx/tx b-rate=33600/33600, rx/tx chars=0/0
resource slot/port=3/3, mp bundle=0, charged units=0, account id=0
idb handle=0x645B97CC, tty handle=0x622207BC, tcb handle=0x0
-------------------------------------------------------------------------
protocol: last=LAP-M, attempted=LAP-M
compression: last=V.42bis-Both, supported= V.42bis-RX V.42bis-TX
standard: last=V.34+, attempted=V.21, initial=V.21

snr=40 dB, sq=5, rx/tx level=-15/0 dBm
phase jitter: freq=1 Hz, level=2 degrees
far end echo level=-90 dBm, freq offset=0 Hz
phase roll=0 degrees, round-trip delay=0 msecs
digital pad=None dB, digital pad comp=0
rbs pattern=0, constellation=0 point
rx/tx: symbol rate=3429/3429, carrier freq=1959/1959
rx/tx: trellis code=0/0, preemphasis index=0/0
rx/tx: constellation shape=Off/Off, nonlinear encode=Off/Off
rx/tx: precode=Off/Off, xmit level reduct=0/0 dBm

rx/tx: chars=0/0, general info=0x0
rx/tx: link layer chars=0/0, NAKs=0/0
error corrected: rx/tx=0/0, rx bad=0
ec retransmissions=0, retransmitted frames=0
rx/tx ppp slip=0/0, bad ppp slip=0

rx/tx b-rate: last=33600/33600, lowest=0/0, highest=0/0
phase 2 projected max rx b-rate: client=0, host=33600
phase 4 desired rx/tx b-rate: client=16384/25987, host=25987/42765
retrains: local=0, remote=0, failed=0
speedshift: local up/down=0/0, remote up/down=0/0, failed=0

v110: rx good=0, rx bad=0, tx=0, sync lost=0
SS7/COT status=0x00
v90: status=(Invalid #141), client=(n/a), failure=None

rx/tx: max neg I frame=128/128, neg window=0/128
v42bis size: dictionary=0, string=16
T401 timeouts=0, tx window closures=0, rx overruns=0
test err=0, reset=0, v0 synch loss=0
mail lost: host=0, sp=0

duration(sec)=0, disc reason=0x0
disc text=(n/a)

                --------5---------10--------15--------20--------25--------30
line shape  : 0x00000000000000000000000000000000000000000000000000000000
v8bis capab : 0x12C9808081C609B502009481834347CB000000000000
v8bis mod sl: 0x00000000000000000000000000000000000000000000000000000000
v8 jnt menu : 0xC16513942A8D0000000000000000000000000000
v8 call menu: 0x00C16513942A000000000000000000000000000000
v90 training: 0x00000000
v90 sgn ptrn: 0x00000000
```

```
state trnsn : 0x0F0F010203041013151920FF00000000000000000000000000000000000000000
                0000
portwre diag: 0x00000000000000000000000000000000
phase 2 info: 0x0200EFF41F120000003CEFF41F0200E001EFB4014082050B083470200001
                1EEFB41440E1050008FCA707A707650D00000000000000000000
phase 4 info: 0x0DA70D65836583400040
-------------------------------------------------------------------------------
```

show port modem log

To display the events generated by the modem sessions, use the **show port modem log** command in EXEC mode.

Cisco AS5350 and Cisco AS5400 with the NextPort Dial Feature Card (DFC)

show port modem log [**reverse**] [*slot* | *slot*/*port*] [*slot* | *slot*/*port*]

Cisco AS5800 with the Universal Port Card (UPC)

show port modem log [**reverse**] [*shelf*/*slot* | *shelf*/*slot*/*port*] [*shelf*/*slot* | *shelf*/*slot*/*port*]

Syntax Description

reverse	(Optional) Displays the modem port history event log with the most recent event first.
slot	(Optional) All ports on the specified slot. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7. A range of slots can be specified by entering a second value for the *slot* argument
slot/*port*	(Optional) All ports on the specified slot and service processing element (SPE). For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7. Port values range from 0 to one less than the number of ports supported by the card. You must include the slash mark. A range of ports can be specified by entering a second value for the *slot*/*port* argument.
shelf/*slot*	(Optional) All ports on the specified shelf and slot. For the Cisco AS5800, shelf values range from 0 to 1 and Universal Port Card (UPC) slot values range from 2 to 11. You must include the slash mark. A range shelfs and slots can be specified by entering a second value for the *shelf*/*slot* argument.
shelf/*slot*/*port*	(Optional) All ports on the specified SPE. For the Cisco AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and port values range from 0 to one less than the number of ports supported by the card. You must type in the forward slashes (/). A range of ports can be specified by entering a second value for the *shelf*/*slot*/*port* argument.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5400 and Cisco AS5800.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(2)XA	Link and states information was added.
12.2(2)XB1	This command was integrated into Cisco IOS Release 12.2(2)XB1.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.

Usage Guidelines

The port modem test log displays the results of the SPE diagnostics tests.

Examples

The following is sample output for the Cisco AS5400 with the NextPort DFC. This example shows the port history event log for slot 5, port 47:

```
Router# show port modem log 5/47

Port 5/47 Events Log
     Service type: DATA_FAX_MODEM
     Service mode: DATA_FAX_MODEM
     Session State: IDLE
  00:02:23: incoming called number: 35160
     Service type: DATA_FAX_MODEM
     Service mode: DATA_FAX_MODEM
     Session State: IDLE
     Service type: DATA_FAX_MODEM
     Service mode: DATA_FAX_MODEM
     Session State: ACTIVE
  00:02:23: Modem State event:
            State: Connect
  00:02:16: Modem State event:
            State: Link
  00:02:13: Modem State event:
            State: Train Up
  00:02:05: Modem State event:
            State: EC Negotiating
  00:02:05: Modem State event:
            State: Steady
  00:02:05: Modem Static event:
    Connect Protocol                          :   LAP-M
    Compression                               :   V.42bis
    Connected Standard                        :   V.34+
    TX,RX Symbol Rate                         :   3429, 3429
    TX,RX Carrier Frequency                   :   1959, 1959
    TX,RX Trellis Coding                      :   16/16
    Frequency Offset                          :   0  Hz
    Round Trip Delay                          :   0  msecs
    TX,RX Bit Rate                            :   33600, 33600
    Robbed Bit Signalling (RBS) pattern       :   0
    Digital Pad                               :   None
    Digital Pad Compensation                  :   None
    4 bytes of link info not formatted        :   0x00 0x00 0x00 0x00 0x00
  00:02:06:Modem Dynamic event:
    Sq Value                                  :   5
    Signal Noise Ratio                        :   40  dB
    Receive Level                             :   -12  dBm
    Phase Jitter Frequency                    :   0  Hz
    Phase Jitter Level                        :   2  degrees
    Far End Echo Level                        :   -90  dBm
    Phase Roll                                :   0  degrees
    Total Retrains                            :   0
    EC Retransmission Count                   :   0
    Characters transmitted, received          :   0, 0
    Characters received BAD                   :   0
    PPP/SLIP packets transmitted, received    :   0, 0
    PPP/SLIP packets received (BAD/ABORTED)   :   0
    EC packets transmitted, received OK       :   0, 0
    EC packets (Received BAD/ABORTED)         :   0
```

The following example shows the port history event log with the most recent event first on slot 5, port 40:

```
Router# show port modem log reverse 5/40

Modem port 5/40 Events Log
  00:02:18:Modem Dynamic event:
    Sq Value                                :   5
    Signal Noise Ratio                      :   38  dB
    Receive Level                           :   -12  dBm
    Phase Jitter Frequency                  :   0  Hz
    Phase Jitter Level                      :   0  degrees
    Far End Echo Level                      :   0  dBm
    Phase Roll                              :   0  degrees
    Total Retrains                          :   0
    EC Retransmission Count                 :   0
    Characters transmitted, received        :   0, 0
    Characters received BAD                 :   0
    PPP/SLIP packets transmitted, received  :   0, 0
    PPP/SLIP packets received (BAD/ABORTED) :   0
    EC packets transmitted, received OK     :   0, 0
    EC packets (Received BAD/ABORTED)       :   0
  00:02:18: Modem Static event:
    Connect Protocol                        :   LAP-M
    Compression                             :   V.42bis
    Connected Standard                      :   V.90
    TX,RX Symbol Rate                       :   8000, 3200
    TX,RX Carrier Frequency                 :   1829, 1829
    TX,RX Trellis Coding                    :   16/16
    Frequency Offset                        :   0  Hz
    Round Trip Delay                        :   4  msecs
    TX,RX Bit Rate                          :   52000, 28800
    Robbed Bit Signalling (RBS) pattern     :   255
    Digital Pad                             :   None
    Digital Pad Compensation                :   Enabled
    4 bytes of link info not formatted      :   0x00 0x00 0x00 0x00 0x00
  00:02:23: Modem State event:
            State: Steady
  00:02:23: Modem State event:
            State: EC Negotiating
  00:02:36: Modem State event:
            State: Train Up
  00:02:39: Modem State event:
            State: Link
  00:02:46: Modem State event:
            State: Connect
  00:02:46: Port State Reached:
     Service type: DATA_FAX_MODEM
     Service mode: DATA_FAX_MODEM
     Session State: ACTIVE
  00:02:46: Port State Reached:
     Service type: DATA_FAX_MODEM
     Service mode: DATA_FAX_MODEM
     Session State: IDLE
  00:02:47: incoming called number: 6000
  00:02:47: incoming caller number: 90002
```

The following is sample output for the Cisco AS5800 with the UPC. This example shows the port history event log for slot 8, ports 0 to 6:

```
Router# show port modem log 1/8/0 1/8/6

Port 1/08/00 Events Log
  09:09:53: Service Type: DATA_FAX_MODEM
  09:09:53: Service Mode: DATA_FAX_MODEM
```

```
09:09:53: Session State: FLUSHING
09:09:53: Service Type: DATA_FAX_MODEM
09:09:53: Service Mode: DATA_FAX_MODEM
09:09:53: Session State: IDLE
09:09:53: Modem State event:
          State: Terminate
09:09:53: Modem End Connect event:
  Call Timer                              :   26  secs
  Disconnect Reason Info                  :   0x1F00
      Type (=0  ):  <unknown>
     Class (=31 ):  Requested by host
    Reason (=0  ):  non-specific host disconnect
  Total Retrains                          :   0
  EC Retransmission Count                 :   0
  Characters transmitted, received        :   2633, 485
  Characters received BAD                 :   0
  PPP/SLIP packets transmitted, received  :   0, 0
  PPP/SLIP packets received (BAD/ABORTED) :   0
  EC packets transmitted, received OK     :   27, 21
  EC packets (Received BAD/ABORTED)       :   0
09:09:54:Modem Link Rate event:
09:09:55: Service Type: DATA_FAX_MODEM
09:09:55: Service Mode: DATA_FAX_MODEM
09:09:55: Session State: IDLE
09:09:55: Service Type: DATA_FAX_MODEM
09:09:55: Service Mode: DATA_FAX_MODEM
09:09:55: Session State: ACTIVE
09:09:55: Modem State event:
          State: Connect
09:09:55: Modem State event:
          State: Link
09:09:55: Modem State event:
          State: Train Up
09:09:55: Modem State event:
          State: EC Negotiating
09:09:55: Modem State event:
          State: Steady
09:09:55: Modem Static event:
  Connect Protocol                        :   LAP-M
  Compression                             :   V.42bis
  Connected Standard                      :   V.34+
  TX,RX Symbol Rate                       :   3429, 3429
  TX,RX Carrier Frequency                 :   1959, 1959
  TX,RX Trellis Coding                    :   16/16
  Frequency Offset                        :   0  Hz
  Round Trip Delay                        :   1  msecs
  TX,RX Bit Rate                          :   31200, 28800
  Robbed Bit Signalling (RBS) pattern     :   0
  Digital Pad                             :   None
  Digital Pad Compensation                :   None
  4 bytes of link info not formatted      :   0x00 0x00 0x00 0x00 0x00
09:09:56: Modem Dynamic event:
  Sq Value                                :   5
  Signal Noise Ratio                      :   38  dB
  Receive Level                           :   -15  dBm
  Phase Jitter Frequency                  :   13  Hz
  Phase Jitter Level                      :   0  degrees
  Far End Echo Level                      :   -90  dBm
  Phase Roll                              :   0  degrees
  Total Retrains                          :   0
  EC Retransmission Count                 :   0
  Characters transmitted, received        :   0, 0
  Characters received BAD                 :   0
  PPP/SLIP packets transmitted, received  :   0, 0
```

```
  PPP/SLIP packets received (BAD/ABORTED) :   0
  EC packets transmitted, received OK     :   0, 0
  EC packets (Received BAD/ABORTED)       :   0
09:09:58: Service Type: DATA_FAX_MODEM
09:09:58: Service Mode: DATA_FAX_MODEM
09:09:58: Session State: FLUSHING
09:09:58: Service Type: DATA_FAX_MODEM
09:09:58: Service Mode: DATA_FAX_MODEM
09:09:58: Session State: IDLE
09:09:58: Modem State event:
          State: Terminate
.
.
.
```

Table 96 describes the significant fields shown in the displays.

Table 96 show port modem log Field Descriptions

Field	Description
Port 5/47 Events Log	Port number and slot is displayed.
Service type:	Data fax modem is displayed.
Service mode:	Data fax modem mode.
Session State:	Idle or busy state.
Incoming called number:	The number of the incoming call.
Modem <*slot/port*> Events Log:	The modem for which log events are currently displayed.
Modem State Event	Current state of the modem, which can be any of the following: • Connect—Modem is connected to a remote host. • Open—Open modem event. • Link—Link protocol event occurred. • Training—Modem retraining event. • EC correction—Error correction frames sent or received. • Steady—Steady modem event. • Bad—Inoperable state, which is configured by the **modem bad** command. • Bad*—Inoperable state, which is configured by the **modem startup-test** command during initial power-up testing. • Reset—Modem is in reset mode. • D/L—Modem is downloading firmware. • Bad FW—Downloaded modem firmware is not operational. • Busy—Modem is out of service and not available for calls • Idle—Modem is ready for incoming and outgoing calls.

Table 96 show port modem log Field Descriptions (continued)

Field	Description
Modem Static event:	Current static event of the MICA modem, which can be any of the following: • Connect Protocol—Connection protocol used for the current session, which can be SYNC mode, ASYNC mode, ARA1.0, ARA2.0, LAP-M, or MNP. • Compression—Type of compression used for the current session, which can be None, V.42*bis* TX, V.42*bis* RX, V.42*bis* both, or MNP5 data compression. • Connected Standard—Standards protocol used to connect, which can be V.21, Bell103, V.22, V.22*bis*, Bell212, V.23, V.32, V.32*bis*, V.32terbo, V.34, V.34+, or K56Flex 1.1. • TX, RX Symbol Rate—Symbol rate used to send samples to the line or receive samples off of the line. • TX, RX Carrier Frequency—Carrier frequency used by the remote service provider. • TX, RX Trellis Coding—Trellis coding received and sent. • Frequency Offset—+/–32 in 1/8 hertz (Hz) steps. • Round Trip Delay—Total round trip propagation delay of the link, which is expressed in milliseconds (ms). • TX, RX Bit Rate—For RX, the bit rate from the remote service provider to the local service provider. For TX, the bit rate from the local service provider to the remote service provider.

Table 96 show port modem log Field Descriptions (continued)

Field	Description
Modem Dynamic event:	Current dynamic event of the MICA modem, which can be any of the following: • Sq Value—Signal quality value, which can be from 0 to 7 (0 is the worst possible quality). • Signal Noise Ratio—Expressed in decibels, which can be from 0 to 70 dB steps. • Receive Level—Expressed in decibels, which can be from 0 to 128 dBm steps. • Phase Jitter Frequency—+/–32 in 1/8 Hz steps. • Phase Jitter Level—0 to 90 degrees. • Far End Echo Level—0 to –90 in dBm of far end echo level (that portion of the sent analog signal that has bounced off the analog front end of the remote modem). • Phase Roll—+/–32 in 1/8 Hz steps. • Total Retrains—Count of total retrains. • ECR retransmission Count—Count of total error correction retransmissions that occurred during the duration of the link. • Characters Transmitted, Received—Count of total characters sent and received. • Characters received BAD—A subset of the characters sent and received. Represents the total number of parity error characters. • PPP/SLIP packets transmitted, received—Total count of PPP/SLIP packets sent and received. This total could include all PPP/SLIP packets, including BAD/ABORTED packets. • PPP/SLIP packets received, (BAD/ ABORTED)—Total count of the bad or aborted PPP/Serial Line Internet Protocol (SLIP) packets, which is a subset of the above (PPP/SLIP packets received, transmitted). • EC packets transmitted, received—Count of total error correction frames sent and received. This total could include all error correction packets, including BAD/ABORTED packets. • EC packets (Received BAD/ ABORTED)—Total count of the bad or aborted error correction packets, which is a subset of the EC packets sent and received.

Related Commands

Command	Description
clear port log	Clears all event entries in the port level history event log.
port modem autotest	Automatically and periodically performs a modem diagnostics test for modems inside the access server or router.
port modem startup-test	Performs diagnostic testing for all modems.
show port modem log	Displays the events generated by the modem sessions.
show spe modem active	Displays active modem statistics of all SPEs, a specified SPE, or the specified SPE range.
test port modem back-to-back	Tests two specified ports back-to-back and transfers a specified amount of data between the ports.

show port modem test

To display the modem test log, use the **show port modem test** command in EXEC mode.

Cisco AS5400 with the NextPort Dial Feature Card (DFC)

show port modem test [*slot* | *slot*/*port*]

Cisco AS5800 with the Universal Port Card (UPC)

show port modem test [*shelf*/*slot* | *shelf*/*slot*/*port*]

Syntax Description

slot	(Optional) All ports on the specified slot. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7.
slot/*port*	(Optional) All ports on the specified slot and service processing element (SPE). For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7. Port values range from 0 to one less than the number of ports supported by the card. You must include the slash mark.
shelf/*slot*	(Optional) All ports on the specified shelf and slot. For the Cisco AS5800, shelf values range from 0 to 1 and Universal Port Card (UPC) slot values range from 2 to 11. You must include the slash mark.
shelf/*slot*/*port*	(Optional) The specified port range on a shelf and slot. For the Cisco AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 0 to 53. You must include the slash marks.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5400 and Cisco AS5800.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.

Usage Guidelines

The port modem test log displays the results of the SPE diagnostics tests.

Examples

The following is sample output for the Cisco AS5400 with the NextPort DFC. This example displays the results of the SPE startup test, SPE autotest, and SPE back-to-back test.

Note The Reason column indicates why the test was started. The TIME INTERVAL is one of the triggers under autotest, the other being the error threshold.

```
Router# show port modem test

Date Time             Modem  Test               Reason            State Result
 3/02 12:00:57 PM       2/01  Back-To-Back     :STARTUP TEST       Idle  PASS
 3/02 12:00:57 PM       2/00  Back-To-Back     :STARTUP TEST       Idle  PASS
 3/02 12:00:58 PM       2/02  Back-To-Back     :STARTUP TEST       Idle  PASS
 3/02 12:00:58 PM       2/03  Back-To-Back     :STARTUP TEST       Idle  PASS
 3/02 12:00:58 PM       2/04  Back-To-Back     :STARTUP TEST       Idle  PASS
 3/02 12:00:58 PM       2/05  Back-To-Back     :STARTUP TEST       Idle  PASS
 .
 .
 .
 3/02 12:01:14 PM       3/95  Back-To-Back     :STARTUP TEST       Idle  PASS
 3/02 12:01:14 PM       3/94  Back-To-Back     :STARTUP TEST       Idle  PASS
 3/02 12:01:15 PM       3/75  Back-To-Back     :STARTUP TEST       Idle  PASS
 3/02 12:01:15 PM       3/74  Back-To-Back     :STARTUP TEST       Idle  PASS
 3/02 12:13:52 PM       3/20  Back-To-Back     :USER INITIATED     Idle  PASS
 3/02 12:13:52 PM       2/10  Back-To-Back     :USER INITIATED     Idle  PASS
 .
 .
 .
3/02 12:44:00 PM      3/102  No Test (Time)   :MIN IDLE MODEMS    Idle  NOTST
 3/02 12:44:00 PM      3/103  No Test (Time)   :MIN IDLE MODEMS    Idle  NOTST
 3/02 12:44:00 PM      3/104  No Test (Time)   :MIN IDLE MODEMS    Idle  NOTST
 3/02 12:44:00 PM      3/105  No Test (Time)   :MIN IDLE MODEMS    Idle  NOTST
 3/02 12:44:00 PM      3/106  No Test (Time)   :MIN IDLE MODEMS    Idle  NOTST
 3/02 12:44:00 PM      3/107  No Test (Time)   :MIN IDLE MODEMS    Idle  NOTST
 3/02 12:44:21 PM       2/73  Back-To-Back     :TIME INTERVAL      Idle  PASS
 3/02 12:44:21 PM       2/72  Back-To-Back     :TIME INTERVAL      Idle  PASS
 3/02 12:44:21 PM       2/33  Back-To-Back     :TIME INTERVAL      Idle  PASS
 3/02 12:44:21 PM       2/32  Back-To-Back     :TIME INTERVAL      Idle  PASS
 3/02 12:44:21 PM       3/37  Back-To-Back     :TIME INTERVAL      Idle  PASS
```

Table 97 describes the significant fields shown in the display.

Table 97 show port modem test Field Descriptions

Field	Description
Date	Date the back-to-back test occurred for the specified modem.
Time	Time the test occurred.
Modem	Specified modem that performed a back-to-back test.
Test	Operation performed on the specified modem.
Reason	Reason the modem performed the back-to-back test.
State	Current operational state of the modem.
Result	Result of the back-to-back test for the specified modem.

Related Commands

Command	Description
clear port log	Clears all event entries in the port level history event log.
port modem autotest	Automatically and periodically performs a modem diagnostics test for modems inside the access server or router.
port modem startup-test	Performs diagnostic testing for all modems.
show port modem log	Displays the modem port history event log or modem test log.
show port log reverse	Displays the latest event first from the port history event log.

Command	Description
show port modem log	Displays the events generated by the modem sessions.
test port modem back-to-back	Tests two specified ports back-to-back and transfers a specified amount of data between the ports.

show port operational-status

To display the active session statistics, use the **show port operational-status** command in privileged EXEC mode.

Cisco AS5350 and Cisco AS5400 with the NextPort Dial Feature Card (DFC)

show port operational-status {*slot* | *slot*/*port*}

Cisco AS5800 with the Universal Port Card (UPC)

show port operational-status {*shelf*/*slot* | *shelf*/*slot*/*port*}

Syntax Description

slot	Displays information for all ports on the specified slot. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7.
slot/*port*	Displays information for all ports on the specified slot and service processing element (SPE). For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7. Port values range from 0 to one less than the number of ports supported by the card. You must include the slash mark.
shelf/*slot*	Displays information for all ports on the specified shelf and slot. For the Cisco AS5800, shelf values range from 0 to 1 and Universal Port Card (UPC) slot values range from 2 to 11. You must include the slash mark.
shelf/*slot*/*port*	Displays information for all ports on the specified SPE. For the Cisco AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and port values range from 0 to one less than the number of ports supported by the card. You must type in the forward slashes (/).

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)XD	This command was implemented on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5800.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(2)XA	Disconnect reasons and states information were added.
12.2(2)XB1	This command was integrated into Cisco IOS Release 12.2(2)XB1.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.
12.3(4)T	Configuration output was modified to show voice activity detection (VAD) background noise and echo canceller (EC or ECAN) background noise statistics.
12.3(14)T	T.38 fax relay call statistics were made available to Call Detail Records (CDRs) through Vendor-Specific Attributes (VSAs) and added to the call log.

Usage Guidelines

This command displays the operational status of a specific port or port range. The port should have an associated active modem session when the command is executed. The **show port operational-status** command is equivalent to the **show modem operational-status** MICA technologies modem command.

Examples

The following is sample output from the **show port operational-status** command on the Cisco AS5400 with the NextPort DFC. This example displays operational status for slot 2, SPE 0, port 1:

```
Router# show port operational-status 2/1

slot/spe/Port -- 2/0/1
Service Type                            :Modem service
Disconnect Reason Info                  :0x0
Type (=0  ): <unknown>
Class (=0  ): Other
Reason (=0  ): no disconnect has yet occurred
Modulation Standard                     :V.34+
TX/RX Bit Rate                          :31200/14400
Connect Protocol                        :LAP-M
Compression                             :V.42bis
Call Timer                              :47 secs
Link Signal Quality                     :7
SNR                                     :37 dB
TX/RX Symbol Rate                       :3429/3429
TX/RX Carrier Frequency                 :1959/1959
TX/RX Trellis Coding                    :16/16
TX/RX Preemphasis Index                 :0/1
TX/RX Constellation Shaping             :On-Active/On-Active
TX/RX Nonlinear Encoding                :On-Active/On-Active
TX/RX Precoding                         :On-Active/On-Active
TX/RX Xmit Level Reduction              :3/1 dBm
Receive Level                           :-15 dBm
Frequency Offset                        :0 Hz
Phase Jitter Frequency                  :2 Hz
Phase Jitter Level                      :2 degrees
Far End Echo Level                      :-90 dBm
Phase Roll                              :0 degrees
Round Trip Delay                        :0 msecs
>Total Retrains                          :0
Self Test Error count                   :0
EC Retransmission count                 :0
EC packets transmitted/received OK      :11/12
EC packets (Received BAD/ABORTED)       :0
Characters transmitted/received         :76/13
Characters received BAD                 :0
PPP/SLIP packets transmitted/received   :0/0
PPP/SLIP packets received (BAD/ABORTED) :0
RBS Pattern                             :0
Digital Pad                             :0
Digital Pad Compensation                :0
```

The following example displays operational status for a V.110 digital service for the Cisco AS5400 on slot 2, SPE 3, port 23:

```
Router# show port operational-status 2/23

slot/spe/Port -- 2/3/23
Service Type                            : Digital service
Connect Protocol                        : V110
Data Bits                               : 8
Parity                                  : 0
Stop Bits                               : 1
```

```
TX/RX Bit Rate                          : 19200/19200
Call Timer                              : 116 secs
EC packets transmitted/received OK      : 0/0
EC packets (Received BAD/ABORTED)       : 0
PPP/SLIP packets transmitted, received  : 8/8
PPP/SLIP packets received (BAD/ABORTED) : 0
Sync Loss                               : 0
```

The following example shows output from the **show port operational-status** command for the Cisco AS5800 on shelf 1, slot 8:

```
Router# show port operational-status 1/8

Shelf/Slot/SPE/Port -- 1/8/32/194
Service Type                            : Modem service
Disconnect Reason Info                  : 0x0
     Type (=0  ):  <unknown>
    Class (=0  ):  Other
   Reason (=0  ):  no disconnect has yet occurred
Modulation Standard                     : V.34+
TX/RX Bit Rate                          : 31200/31200
Connect Protocol                        : LAP-M
Compression                             : V.42bis
Call Timer                              : 18 secs
Link Signal Quality                     : 6
SNR                                     : 38 dB
TX/RX Symbol Rate                       : 3429/3429
TX/RX Carrier Frequency                 : 1959/1959
TX/RX Trellis Coding                    : 16/16
TX/RX Preemphasis Index                 : 0/1
TX/RX Constellation Shaping             : Off-None/On-Active
TX/RX Nonlinear Encoding                : Off-None/On-Active
TX/RX Precoding                         : Off-None/On-Active
TX/RX Xmit Level Reduction              : 6/5 dBm
Receive Level                           : -15 dBm
Frequency Offset                        : 0 Hz
Phase Jitter Frequency                  : 5 Hz
Phase Jitter Level                      : 2 degrees
Far End Echo Level                      : -90 dBm
Phase Roll                              : 0 degrees
Round Trip Delay                        : 1 msecs
Total Retrains                          : 0
Self Test Error count                   : 0
EC Retransmission count                 : 1
EC packets transmitted/received OK      : 34/14
EC packets (Received BAD/ABORTED)       : 0
Characters transmitted/received         : 9393/355
Characters received BAD                 : 0
PPP/SLIP packets transmitted/received   : 0/0
PPP/SLIP packets received (BAD/ABORTED) : 0
RBS Pattern                             : 0
Digital Pad                             : 0
Digital Pad Compensation                : 0
.
.
.
```

The following example shows VAD background noise and ECAN background noise statistics:

```
Router# show port operational-status 1/0

Slot/SPE/Port -- 1/0/0
Service Type                            :Voice service
Voice Codec                             :G.711 u-law
```

```
Echo Canceler Length                    :8 ms
Echo Cancellation Control               :Echo cancellation       - enabled
                                          Echo update            - enabled
                                          Non-linear processor   - enabled
                                          Echo reset coefficients - disabled
                                          High pass filter enable - disabled
Digit detection enable                  :DTMF signaling          - enabled
Voice activity detection                :Disabled
Comfort noise generation                :Generate comfort noise
Digit relay enable                      :OOB Digit relay         - disabled
                                          IB Digit relay         - disabled
Information field size                  :20 ms
Playout de-jitter mode                  :adaptive
Encapsulation protocol                  :RTP
Input Gain                              :0.0 dB
Output Gain                             :0.0 dB
Tx/Rx SSRC                              :20/0
Current playout delay                   :65 ms
Min/Max playout delay                   :65/105 ms
Clock offset                            :142003 ms
Predictive concealment                  :0 ms
Interpolative concealment               :0 ms
Silence concealment                     :0 ms
Buffer overflow discards                :1
End-point detection errors              :0
Tx/Rx Voice packets                     :1337/1341
Tx/Rx signaling packets                 :0/0
Tx/Rx comfort noise packets             :0/0
Tx/Rx duration                          :26745/26745 ms
Tx/Rx voice duration                    :0/0 ms
Out of sequence packets                 :0
Bad protocol headers                    :0
Num. of late packets                    :0
Num. of early packets                   :1
Tx/Rx Power                             :-87.0/-57.3 dBm
Tx/Rx Mean                              :-86.3/-57.0 dBm
VAD Background noise level              :6.2 dBm
ERL level                               :127.0 dB
ACOM level                              :127.0 dB
Tx/Rx current activity                  :silence/silence
Tx/Rx byte count                        :213920/214240
ECAN Background noise level             :-83.4 dBm
Latest SSRC value                       :391643394
Number of SSRC changes                  :1
Number of payload violations            :0
```

Table 98 describes the significant fields shown in the displays.

Table 98 show port operational-status Field Descriptions

Field	Description
slot/SPE/Port	Displays the slot and port designation for the SPE card location.
Service Type	Indicates the type of service.
Disconnect Reason Info	Displays the reason for disconnection.
Modulation Standard	Modulation standard can be V.21, Bell103, V.22, V.22*bis*, Bell 212, V.23, V.32, V.32*bis*, V.32terbo, V.34, V.34+, or K56Flex 1.1.
TX/RX Bit Rate	TX is the bit rate from the local DCE to the remote DCE. RX is the bit rate from the remote DCE to the local DCE. These rates may be asynchronous.

Table 98 show port operational-status Field Descriptions (continued)

Field	Description
Connect Protocol	Connect protocol for the current session, which can be SYNC mode, ARA1.0, ARA2.0, LAP-M, MNP, FAX mode, SS7/COT, or V.110.
Compression	Compression protocol used for the current connection, which can be None, V.42*bis* TX, V.42*bis* RX, V.42*bis* both, or MNP5 data compression.
Link Signal Quality	Measure of line quality for a given bit rate where 0 is the worst and 3 is steady state. If a 1 or 2 is present, the modem must shift down to a lower rate. Likewise, if the value is 4 to 7, the modem speeds shift up to a higher rate. If the value is high (for example, 7) and the bit rate is low, then there may be a problem at the remote end receiver.
SNR	The ratio measurement (in dB) of the desired signal to noise. This value can range from 0 to 70 dB and changes in 1 dB steps. Note that a 28.8-kbps connection demands an SNR of about 37 dB. Any values lower than this level result in a diminished quality of connection. A 33.6-kbps connection demands a signal-to-noise ratio (SNR) of 38 to 39 dB. Also note that a "clean" line has an SNR of about 41 dB.
TX/RX Symbol Rate	TX is symbol rate used to send samples to the line. RX is the symbol rate used to receive samples off of the line. The rates are synchronous with each other.
TX/RX Carrier Frequency	For TX, carrier frequency used by the local DCE. For RX, carrier frequency used by the remote DCE.
TX/RX Trellis Coding	Adds dependency between symbols in order to make the detection in noise more robust (Forward Error Correction). Modems may use 8 (V.32, V.32*bis*, V.17), 16, 32, 64 (V.34, V.34+, V.90, K56flex), or no trellis coding (V.22, V.22*bis*, V.21, Bell212, Bell103, V.29, V.27).
TX/RX Preemphasis Index	Involves shaping the raw transmit spectrum in order to deal with spectrum roll-offs. The preemphasis index can take on the values 0 to 10. A zero denotes no reshaping. Typical values usually fall in the ranges from 0 to 2 or 6 to 7. This technique is used with V.34 and V.34+ standards.
TX/RX Constellation Shaping	A method for improving noise immunity by using a probability distribution for sent signal points. The signal states used to predict the sensitivity to certain transmission impairments. Values may be either Off-none or On-active. This technique is used with V.34 and V.34+ standards.
TX/RX Nonlinear Encoding	Occurs during the training phase and moves the outer points of the constellation away in order to deal with nonlinear distortion. Nonlinear distortion (0 to 200 Hz) tends to affect the higher power signals. Moving the outer constellation points out reduces the chance of error. Values may be either Off-none or On-active. MICA modems support nonlinear coding in both directions. This technique is used with V.34 and V.34+ standards.

Table 98 show port operational-status Field Descriptions (continued)

Field	Description
TX/RX Precoding	Serves the same purpose as the preemphasis index but instead manages the bits and not the raw transmit signals. This is done only when requested and therefore will occur in the RX mode. The values may be either Off-none or On-active. This technique is used with V.34 and V.34+ standards.
TX/RX Xmit Level Reduction	Affects the transmit signal with 0 to 15 in dBm of reduction. If nonlinear distortion is detected, the modem prompts the client for a lower-powered TX signal. If the remote end detects nonlinear distortion, it may request that the sender lower the TX signal. This technique is used with V.34 and V.34+ standards.
Receive Level	The power of the received signal in dBm steps. It ranges from 0 to –128 dBm. Typically the range in the United States is about –22 dBm, and in Europe is –12 dBm. A good range is from –12 dBm to –24 dBm.
Frequency Offset	The difference (in hertz) between the expected RX carrier frequency and the actual RX carrier frequency.
Phase Jitter Frequency	Peak to peak differential (in hertz) between two signal points. Uncanceled phase jitter looks like “rocking” of the baseband quadrature amplitude modulation (QAM) constellation. The points look like arcs with the outer points having longer arcs.
Phase Jitter Level	Amount of phase jitter measured and indicates how large the “rocking” is in degrees. On an oscilloscope, the constellation points would look like crescent moons. Values can range up to 15 degrees. The typical value is zero (that is, phase jitter is not normally present).
Far End Echo Level	Over long connections, an echo is produced by impedance mismatches at 2-wire-to-4-wire and 4-wire-to-2-wire hybrid circuitry. The far-end echo level (that portion of the sent analog signal that has bounced off of the remote modem analog front end) may range from 0 to –90 in dBm.
Phase Roll	Phase roll affects the echo signal coming back. A certain constellation pattern is sent from a modem and arrives at to the central office. Some echoed form of this signal/constellation pattern is sent back. However, the constellation shape may be rotated from 0 to 359 degrees. This rotation is called the phase roll.
Round Trip Delay	Total round trip propagation delay of the link (in milliseconds). This is important for proper echo cancellation. The amount that the delay varies on the network.
Total Retrains	Count of total retrains and speed shifts.
Self Test Error count	Total errors generated during a self-test run.
EC Retransmission count	The number of times the NextPort has gone into error recovery in the TX direction for a particular connection. The larger the number, the worse the connection. However, this parameter should be weighed against the count produced by EC packets sent and received in order to determine if there should really be a concern.

Table 98 show port operational-status Field Descriptions (continued)

Field	Description
EC packets transmitted/received OK	Error correction (EC) packets sent is the number of TX frames that the client modem accepted. EC packets received is the number of data RX frames accepted.
EC packets (Received BAD/ABORTED)	This is identical to the EC Retransmission count field.
PPP/SLIP packets transmitted/received	Total count of PPP/Serial Line Internet Protocol (SLIP) packets sent and received. This total could include all PPP/SLIP packets, including BAD/ABORTED packets.
PPP/SLIP packets received (BAD/ABORTED)	Total count of the bad or aborted PPP/SLIP packets, which is a subset of PPP/SLIP packets received. A counted PPP packet has a bad frame check sequence (FCS), or the SLIP packet has a transparency error.
RBS Pattern	Reports the number of robbed bits detected in the connection. The robbed bits are used for inband signaling. This information is reported only for K56Flex (by the analog modem) and is found only on a channelized line such as T1 or E1. The six least significant bits (LSBs) of the returned value indicate the periodic robbed bit signaling (RBS) pattern where a 1 denotes a pulse code modulation (PCM) sample with a robbed bit.
VAD Background noise level	VAD background noise level, in 6.2 dBm increments.
ECAN Background noise level	ECAN background noise level, in –83.4 decibels per milliwatt (dBm) increments.

The following example shows output from the **show port operational-status** command for the Cisco AS5350 on shelf 1, slot 5 with the T.38 fax relay statistics:

```
Router# show port operational-status 1/5

Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 0
MGCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 1

 GENERIC:
SetupTime=10465510 ms
Index=1
PeerAddress=41023
PeerSubAddress=
PeerId=1
PeerIfIndex=242
LogicalIfIndex=180
ConnectTime=1046791
CallDuration=00:00:41 sec
CallState=4
CallOrigin=2
ChargedUnits=0
InfoType=fax
TransmitPackets=260
```

```
TransmitBytes=4396
ReceivePackets=1014
ReceiveBytes=40385

TELE:

ConnectionId=[0x37DF8CCA 0x9FA611D8 0x8007000A 0xF4107CA0]
!
IncomingConnectionId=[0x37DF8CCA 0x9FA611D8 0x8007000A 0xF4107CA0]
CallID=11
TxDuration=6640 ms
VoiceTxDuration=0 ms
FaxTxDuration=0 ms
FaxRate=disable bps
FaxRelayMaxJitBufDepth 0
FaxRelayJitterBufOverflow 0
Initial HS Modulation is UNKNOWN
Recent HS modulation is UNKNOWN
Number of pages 0
Direction of transmission is Unknown
Num of Packets TX'ed/RX'ed 0/0
Packet loss conceal is 0
Encapsulation protocol is T.38 (UDPTL)
ECM is DISABLED
NoiseLevel=0
ACOMLevel=0
OutSignalLevel=0
InSignalLevel=0
InfoActivity=0
ERLLevel=0
SessionTarget=
!
ImgPages=0
CallerName=Analog 41023
CallerIDBlocked=False
OriginalCallingNumber=
OriginalCallingOctet=0x80
OriginalCalledNumber=41021
OriginalCalledOctet=0xA1
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0xFF
TranslatedCallingNumber=41023
TranslatedCallingOctet=0x80
TranslatedCalledNumber=41021
TranslatedCalledOctet=0xA1
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwReceivedCalledNumber=41021
GwReceivedCalledOctet3=0xA1
GwOutpulsedCalledNumber=41021
```

Table 99 describes the significant fields showing T.38 fax relay statistics:

Table 99 show port operational-status Field Descriptions showing significant T.38 Fax Relay Satistics

Field	Description
Telephony call-legs	Type of call: Telephony.
SIP call-legs	Type of call: Session Initiation Protocol (SIP).
H323 call-legs	Type of call: H.323.

Table 99 show port operational-status Field Descriptions showing significant T.38 Fax Relay Satistics (continued)

Field	Description
MGCP call-legs	Type of call: Media Gateway Control Protocol (MGCP).
Multicast call-legs	Type of call: Multicast.
Total call-legs	Total calls.
PeerIfIndex	Voice port index number for this peer. For ISDN media, this would be the index number of the B channel used for this call.
LogicalIfIndex	Index number of the logical interface for this call.
TxDuration	Duration of transmit path open from this peer to the voice gateway for this call.
VoiceTxDuration	Duration of voice transmission from this peer to the voice gateway for this call in milliseconds (ms).
FaxTxDuration	Duration of fax transmission from this peer to the voice gateway for this call in ms.
FaxRate	Fax transmission rate from this peer to the specified dial peer in bps.
FaxRelayMaxJitBufDepth	Fax relay maximum jitter buffer depth in ms.
FaxRelayJitterBufOverflow	Fax relay jitter buffer overflow in ms.
Initial HS Modulation	Initial high speed modulation used.
Recent HS Modulation	Recent high-speed modulation used
ACOMLevel	Current ACOM level estimate in 0.1 dB increments. The term ACOM is used in G.165, "*General Characteristics of International Telephone Connections and International Telephone Circuits: Echo Cancellers*." ACOM is the combined loss achieved by the echo canceller, which is the sum of the ERL, ERL enhancement, and nonlinear processing loss for the call.
ERLLevel	Current Echo Return Loss (ERL) level estimate in 0.1 dB increments.
OriginalCallingNumber, OriginalCalling Octet, OriginalCalledNumber, OriginalCalledOctet, OriginalRedirectCalledNumber, OriginalRedirectCalledOctet	Original call information regarding calling, called, and redirect numbers, as well as octet-3s. Octet-3s are information elements (IEs) of Q.931 that include type of number, numbering plan indicator, presentation indicator, and redirect reason information.
TranslatedCallingNumber, TranslatedCallingOctet, TranslatedCalledNumber, TranslatedCalledOctet, TranslatedRedirectCalledNumber, TranslatedRedirectCalledOctet	Translated call information.
GwReceivedCalledNumber, GwReceivedCalledOctet3	Call information received at the gateway.

Related Commands

Command	Description
port modem autotest	Automatically and periodically performs a modem diagnostics test for modems inside the access server or router.
show modem operational-status	Displays the operational status of a specific port or port range.
show spe modem active	Displays active modem statistics of all SPEs, a specified SPE, or the specified range of SPEs.
test port modem back-to-back	Tests two specified ports back-to-back and transfers a specified amount of data between the ports.
voicecap configure	Applies a voicecap on NextPort platforms.

show ppp bap

To display the PPP Bandwidth Allocation Protocol (BAP) configuration settings and run-time status for a multilink bundle, use the **show ppp bap** command in privileged EXEC mode.

show ppp bap {**counters** [**reset**] | **group** [*name*] | **queues**}

Syntax Description

counters [**reset**]	Incoming and outgoing call counters and connection request data. The optional **reset** keyword resets the counters.
group [*name*]	All or, optionally, a specific BAP bundle group.
queues	BAP queues.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3	This command was introduced.
12.2T	This command was enhanced with a display of incoming and outgoing call counters and connection request data.

Examples

The following is sample output from the **show ppp bap group** command:

```
Router# show ppp bap group

Group bap-peer (multilink), id 35, peer has precedence, state Idle
Master interface: Dialer1
Outgoing requests: Call, Link Drop
Incoming requests: Call, Callback, Link Drop
Original number dialed 5550198
Transmit queue size threshold is not set
Peer link addition dependent upon load
Timers (secs): Call not set, Callback not set, Link Drop not set,
               Response 30, Pending 20
Retries: Request 3, Dial 1, Indication no limit
Link removal after 3 link drop retries not set
```

Table 100 describes the significant fields shown in the display of the ***show ppp bap group*** command.

Table 100 show ppp bap group Field Descriptions

Field	Description
Group bap-peer (multilink), id 35	Group name and internally assigned ID. “(multilink)” indicates the governing protocol.
peer has precedence	In cases where the remote and local peers issue simultaneous requests, the remote peer’s request takes precedence when the “peer has precedence” message is displayed. The local peer’s request takes precedence when the “precedence over peer” message is displayed.
state Idle	Internal state.

Table 100 show ppp bap group Field Descriptions (continued)

Field	Description
Outgoing requests	Current requests configured for outbound negotiation.
Incoming requests	Current requests allowed for inbound negotiation.
Peer link addition dependent upon load	Router is monitoring the load and subjecting requests to the load settings.
Timers (secs): Call not set, Callback not set, Link Drop not set, Response 30, Pending 20	Settings for specified timers.
Retries: Request 3, Dial 1, Indication no limit	Limits set on specified types of retransmissions.
Link removal after 3 link drop retries not set	The link will not be removed after no response to the link removal request because default behavior was not changed and the relevant link drop parameter was not set.

The display from the **show ppp bap counters** command shows fields of statistics gathered about request and response datagrams that allow endpoints to negotiate a connection and add or drop links from a multilink bundle, per RFC 2125:

- CallReq—Call-Request is a request for permission to add a link to a bundle.
- CallRsp—Call-Response is the required response to Callback-Request datagram.
- CallbackReq—Callback-Request is a request that the peer add a link to a bundle via a callback.
- CallbackRsp—Callback-Response is sent in response to a received Callback-Request.
- DropQueryReq—Link-Drop-Query-Request negotiates with the peer to drop a link from a bundle.
- DropQueryRsp—Link-Drop-Query-Response is sent to the peer to negotiate dropping a link.
- StatusInd—Call-Status-Indication is sent to its peer as a result of a Call-Request or a Callback-Request to indicate whether the attempt to add the link succeeded or failed.
- StatusRsp—Call-Status-Response is sent in response to a received Call-Status-Indication.

The counters record statistical information used by Cisco personnel for debugging purposes that is generally of no interest to end users. Following is sample output:

```
Router# show ppp bap counters

Incoming       inv-link  opt-err  rejects
                      0        4        2

Outgoing       inv-link  add-att  rem-att  add-fail  add-pass  dial-att  oob-ind
                      1        6        5         0         0         0        0

Incoming           off   pend  pend-add   wait  unf-req
CallReq              0      1         1      0        0
CallRsp              0      0         0      0        0
CallbackReq          0      0         0      0        0
CallbackRsp          0      0         0      0        0
DropQueryReq         0      0         0      0        0
DropQueryRsp         0      0         0      0        0
StatusInd            0      0         0      0        0
StatusRsp            0      0         0      0        0
```

```
Outgoing            off    pend  pend-add     unf  unf-req
CallReq               0       0         0       0        0
CallRsp               0       1         0       0        0
CallbackReq           0       0         0       0        0
CallbackRsp           0       0         0       0        0
DropQueryReq          0       0         0       0        0
DropQueryRsp          0       0         0       0        0
StatusInd             0       0         0       0        0
StatusRsp             0       0         0       0        0
```

Related Commands

Command	Description
show ppp multilink	Displays bundle information for the MLP bundles.

show ppp multilink

To display bundle information for Multilink PPP (MLP) bundles, use the **show ppp multilink** command in user EXEC or privileged EXEC mode.

show ppp multilink [**active** | **inactive** | **interface** *type number* | [**username** {*name* | **none**}] [**endpoint** {*discriminator* | **none**}]]

Syntax Description

active	(Optional) Displays information about active multilink bundles only.
inactive	(Optional) Displays information about inactive multilink bundles only.
interface	(Optional) Displays information for the specified bundle interface.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
number	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
username	(Optional) Displays information for all multilink bundles that have the specified peer username.
name	(Optional) Username of the multilink bundle.
none	(Optional) Displays information for multilink bundles with no remote username.
endpoint	(Optional) Displays information for all multilink bundles that have the specified endpoint discriminator.
discriminator	(Optional) Endpoint discriminator.
none	(Optional) Displays information for all multilink bundles with no endpoint discriminator.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.2	This command was introduced.
12.2(13)T	This command was modified. This command was updated to include per-class information when Multiclass Multilink PPP (MCMP) is negotiated.
12.3(7)T	This command was modified. The **active**, **inactive**, **endpoint**, and **username** keywords were added to enable information to be displayed for bundles that have specific parameters.
12.4(9)T	This command was modified. The output of the command was changed to include the following fields: Remote Endpoint Discriminator, Local Endpoint Discriminator, Bundle up for, total bandwidth, load, Receive buffer limit, frag timeout, fragments/bytes in reassembly list, lost fragments, reordered, discarded fragments/bytes, lost received, received sequence, sent sequence, Member links, BR2/0:1, since, weight, and frag size.

Release	Modification
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Examples

The following is sample output from the **show ppp multilink** command when no bundles are on a system:

```
Router# show ppp multilink

No active bundles
```

The following is an example of sample output when a single MLP bundle (named bundle1) is on a system:

```
Router# show ppp multilink

Bundle bundle1, 3 members, first link is BRI0: B-channel 1
0 lost fragments, 8 reordered, 0 unassigned, sequence 0x1E/0x1E rcvd/sent
```

The following is another example of sample output when a single MLP bundle (named 7206-3) is on a system:

```
Router# show ppp multilink

Virtual-Access4
Bundle name: 7206-3
Remote Endpoint Discriminator: [1] 7206-3
Local Endpoint Discriminator: [1] 7206-4
Bundle up for 00:00:07, total bandwidth 64, load 1/255
Receive buffer limit 12192 bytes, frag timeout 1000 ms
 0/0 fragments/bytes in reassembly list
 0 lost fragments, 0 reordered
 0/0 discarded fragments/bytes, 0 lost received
 0x0 received sequence, 0x0 sent sequence
Member links: 1 active, 0 inactive (max not set, min not set)
 BR2/0:1, since 01:59:35, 80 weight, 72 frag size
```

The following is sample output when two active bundles are on a system:

```
Router# show ppp multilink

Bundle bundle1, 3 members, first link is BRI0: B-Channel 1
  0 lost fragments, 8 reordered, 0 unassigned, sequence 0x1E/0x1E rcvd/sent
Bundle bundle2, 4 members, first link is BRI2: B-Channel 1
  0 lost fragments, 28 reordered, 0 unassigned, sequence 0x12E/0x12E rcvd/sent
```

The following example for a stack group member called systema shows output when a stack group has been created. On stack group member systema, the MLP bundle named bundle1 has bundle interface Virtual-Access4. Two child interfaces are joined to this bundle interface. The first is a local PRI channel (Serial 0:4), and the second is an interface from stack group member systemb.

```
Router# show ppp multilink

Virtual-Access4
  Bundle name: 7206-3
  Remote Endpoint Discriminator: [1] 7206-3
  Local Endpoint Discriminator: [1] 7206-4
  Bundle up for 00:00:07, total bandwidth 64, load 1/255
  Receive buffer limit 12192 bytes, frag timeout 1000 ms
  Using relaxed lost fragment detection algorithm.
```

```
    0/0 fragments/bytes in reassembly list
    0 lost fragments, 0 reordered
    0/0 discarded fragments/bytes, 0 lost received
    0x0 received sequence, 0x0 sent sequence
  Member links: 2 active, 0 inactive (max not set, min not set)
    BR2/0:1, since 01:59:35, 80 weight, 72 frag size
    systemb:Vi6 (10.1.1.1), since 00:00:42, unsequenced
```

The following is sample output when the PPP Bandwidth Allocation Control Protocol (BACP) is enabled for the multilink bundle:

```
Router# show ppp multilink

Virtual-Access4
  Bundle name: 7206-3
  Remote Endpoint Discriminator: [1] 7206-3
  Local Endpoint Discriminator: [1] 7206-4
  Bundle up for 00:00:07, total bandwidth 64, load 1/255
  Bundle under BAP control
  Dialer interface is Dialer1
  Receive buffer limit 12192 bytes, frag timeout 1000 ms
    0/0 fragments/bytes in reassembly list
    0 lost fragments, 0 reordered
    0/0 discarded fragments/bytes, 0 lost received
    0x0 received sequence, 0x0 sent sequence
  Member links: 1 active, 0 inactive (max not set, min not set)
    BR2/0:1, since 01:59:35, 80 weight, 72 frag size

  Discriminators Local Remote
    BR2/0:1         24      1
```

Table 101 describes the significant fields shown in the display.

Table 101 show ppp multilink Field Descriptions with PPP BACP Enabled

Field	Description
Bundle name	Configured name of the multilink bundle.
Member links	Number of interfaces in the group.
Bundle under BAP control	Multilink bundle is controlled and bandwidth is allocated by BACP.
Dialer Interface is	Name of the interface that dials the calls.
Member links	Number of child interfaces.
Discriminators Local Remote	Link Control Protocol (LCP) link discriminators, which are identifiers negotiated for each link in the bundle. This information is specific to BACP. BACP uses these discriminators to determine which link to drop during negotiations.

The following is sample output when MCMP is negotiated on a virtual access interface named Virtual-Access3:

```
Router# show ppp multilink interface Virtual-Access 3

Virtual-Access3, bundle name is bundle1
Bundle up for 01:59:35, 1/255 load, 2 receive classes, 2 transmit classes
Receive buffer limit 12192 bytes per class, frag timeout 1524 ms
Dialer interface is Dialer1
!
```

```
Receive Class 0:
0/0 fragments/bytes in reassembly list
0 lost fragments, 0 reordered
0/0 discarded fragments/bytes, 0 lost received
0x0 received sequence
!
Receive Class 1:
0/0 fragments/bytes in reassembly list
0 lost fragments, 0 reordered
0/0 discarded fragments/bytes, 0 lost received
0x0 received sequence
!
Transmit Class 0:
0x8 sent sequence
!
Transmit Class 1:
0x0 sent sequence
!
Member links: 1 (max not set, min not set)
BR2/0:1, since 01:59:35, 80 weight, 72 frag size
```

The following is sample output when Distributed MLP (DLMP) is enabled on Cisco MWR2941 router. The fragments would always contain zero because the counters do not exist in the DMLP output. This is only applicable on Cisco MWR series routers:

```
Bundle name: pas3_ep
  Remote Endpoint Discriminator: [1] pas3_ep
  Local Endpoint Discriminator: [1] pas1_ep
  Bundle up for 00:04:47, total bandwidth 31744, load 1/255
  Receive buffer limit 192000 bytes, frag timeout 1000 ms
  Interleaving disabled
    0/0 fragments/bytes in reassembly list
    0 lost fragments, 0 reordered
    0/0 discarded fragments/bytes, 0 lost received
    0xB received sequence, 0xC sent sequence
  Distributed MLP bundle status is: active
  Member links: 16 active, 0 inactive (max not set, min not set)
    Se0/4:0, since 00:04:48, 7440 weight, 1496 frag size
    Se0/5:0, since 00:04:48, 7440 weight, 1496 frag size
    Se0/6:0, since 00:04:48, 7440 weight, 1496 frag size
    Se0/7:0, since 00:04:48, 7440 weight, 1496 frag size
    Se0/8:0, since 00:04:48, 7440 weight, 1496 frag size
    Se0/0:0, since 00:04:47, 7440 weight, 1496 frag size
    Se0/1:0, since 00:04:47, 7440 weight, 1496 frag size
    Se0/2:0, since 00:04:47, 7440 weight, 1496 frag size
    Se0/3:0, since 00:04:49, 7440 weight, 1496 frag size
    Se0/9:0, since 00:04:47, 7440 weight, 1496 frag size
    Se0/10:0, since 00:04:47, 7440 weight, 1496 frag size
    Se0/11:0, since 00:04:47, 7440 weight, 1496 frag size
    Se0/12:0, since 00:04:47, 7440 weight, 1496 frag size
    Se0/13:0, since 00:04:47, 7440 weight, 1496 frag size
    Se0/14:0, since 00:04:47, 7440 weight, 1496 frag size
    Se0/15:0, since 00:04:47, 7440 weight, 1496 frag size
No inactive multilink interfaces
```

Table 102 describes the significant fields shown in the display when MCMP is enabled.

Table 102 show ppp multilink Field Descriptions with MCMP Enabled

Field	Description
bundle name is	Configured name of the multilink bundle.
Bundle up for	Time (in hh:mm:ss) for which the bundle has been up.
load	Load on the link in the range from 1/255 to 255/255 (255/255 is a 100 percent load).
receive classes, transmit classes	Number of data classes defined for the multilink bundle.
Receive buffer limit	Maximum number of bytes that will be buffered for reassembly for each class of data.
frag timeout	Amount of time, in milliseconds, the router will wait for the expected sequence number to arrive after receiving an out-of-order fragment.
Receive Class 0	Information about Class 0 (normal data) packets received by the router.
fragments/bytes in reassembly list	Number of fragments and bytes currently buffered and awaiting reassembly.
lost fragments	Number of fragments that have been lost.
reordered	Number of fragments that have been reordered.
discarded fragments/bytes	Number of fragments and bytes that have been discarded. This usually occurs only if the fragment is a part of a packet for which one or more fragments were lost.
lost received	Number of fragments that arrived after they were declared lost.
Receive Class 1	Information about Class 1 (high-priority) packets received by the router.
Transmit Class 0	Information about Class 0 (normal data) packets sent by the router.
Transmit Class 1	Information about Class 1 (high-priority) packets sent by the router.
Member links	Number of child interfaces.
BR2/0:1	Identity of the child interface.
since	Amount of time (in hh:mm:ss) the interface has been active.
weight	Relative weight of the link (calculated as bandwidth x fragment delay). This value is used to calculate the fragment size and for load balancing. Each fragment should be less than or equal to the weight, including all link layer headers.
frag size	Fragment size of packets sent over the link, not including link layer headers. The difference between the weight and the fragment size indicates how much link layer overhead is being calculated for each fragment.

The following sample output displays information about all the active multilink bundles:

```
Router# show ppp multilink active

Virtual-Access4, bundle name is 7200-4
  Endpoint discriminator is 7200-4
  Bundle up for 00:31:26, 1/255 load
```

```
Receive buffer limit 12192 bytes, frag timeout 1000 ms
  0/0 fragments/bytes in reassembly list
  0 lost fragments, 0 reordered
  0/0 discarded fragments/bytes, 0 lost received
  0x0 received sequence, 0x0 sent sequence
Member links:1 (max not set, min not set)
  Vi3, since 00:31:26
  PPPoATM link, ATM PVC 15/200 on ATM4/0.10000
  Packets in ATM PVC Holdq:0 , Particles in ATM PVC Tx Ring:1
```

Table 103 describes the significant fields shown in the display when information for all active bundles is displayed.

Table 103 show ppp multilink Field Descriptions for Active Bundles

Field	Description
bundle name is	Configured name of the multilink bundle.
Endpoint discriminator	Identifies the MLP bundle to which the PPP over ATM (PPPoA) session is associated.
Bundle up for	Time (in hh:mm:ss) for which the bundle has been up.
1/255 load	Load on the link in the range from 1/255 to 255/255 (255/255 is a 100 percent load).
Receive buffer limit	Maximum number of bytes that will be buffered for reassembly for each class of data.
frag timeout	Amount of time, in milliseconds, the router will wait for the expected sequence number to arrive after receiving an out-of-order fragment.
fragments/bytes in reassembly list	Number of fragments and bytes currently buffered and awaiting reassembly.
lost fragments	Number of fragments that have been lost.
reordered	Number of fragments that have been reordered.
discarded fragments/bytes	Number of fragments and bytes that have been discarded. This usually occurs only if the fragment is a part of a packet for which one or more fragments were lost.
lost received	Number of fragments that arrived after they were declared lost.
received sequence	Sequence number of the last MLP packet received.
sent sequence	Sequence number of the last MLP packet sent.
Member links	Number of child interfaces.
Vi3	Identity of the child interface.
since	Amount of time (in hh:mm:ss) the interface has been active.
Packets in ATM PVC Holdq	Number of packets in the ATM permanent virtual connection (PVC) hold queue.
Particles in ATM PVC Tx Ring	Number of particles in the transmission ring of the ATM PVC.

Related Commands

Command	Description
ppp multilink	Enables MLP on an interface and, optionally, enables BACP and its BAP subset for dynamic bandwidth allocation.

show queuing virtual-access

To display information about interleaving, use the **show queuing virtual-access** command in EXEC mode.

show queuing virtual-access *number*

Syntax Description

number	Virtual access interface number.

Command Modes

EXEC (>)

Command History

Release	Modification
11.3	This command was introduced.

Examples

The following is sample output from the **show queuing virtual-access** command:

```
Router# show queuing virtual-access 1

   Input queue: 0/75/0 (size/max/drops); Total output drops: 164974
   Queueing strategy: weighted fair
   Output queue: 315/64/164974/31191 (size/threshold/drops/interleaves)
      Conversations  5/8 (active/max active)
      Reserved Conversations 2/2 (allocated/max allocated)

   (depth/weight/discards/interleaves) 64/4096/38669/0
   Conversation 36, linktype: ip, length: 52
   source: 172.23.3.201, destination: 225.1.2.3, id: 0x0001, ttl: 254,
   TOS: 0 prot: 17, source port 6789, destination port 2345

   (depth/weight/discards/interleaves) 64/4096/0/0
   Conversation 2, linktype: ip, length: 52
   source: 172.23.3.201, destination: 225.1.2.4, id: 0x0001, ttl: 254,
   TOS: 0 prot: 17, source port 5432, destination port 9870
```

Table 104 describes the significant fields shown in the display.

Table 104 show queuing virtual-access Field Descriptions

Field	Description
Input queue: size, max, drops	Input queue used for virtual access interface 1, with the current size, the maximum size, and the number of dropped packets.
Total output drops	Number of output packets dropped.
Output queue: size/threshold/drops/interleaves	Output queue counters. Maximum number of packets allowed in the queue, number in the queue, the number of packets dropped due to a full queue, and the number of real-time packets interleaved among fragments of larger packets.
Conversations (active/max active)	Fair queue conversation statistics: number of conversations currently active and the maximum that have been active.

Table 104 show queuing virtual-access Field Descriptions (continued)

Field	Description
Reserved conversations (allocated, max allocated)	Reserved conversations in the weighted fair queue (current/maximum number allocated). Reserved conversations get the highest priority.
(depth/weight/discards/interleaves) 64/4096/38669/0	Depth of the queue, weight assigned to each packet in the queue, number of packets discarded in the queue so far, and the number of interleaves.
Conversation 36, linktype: ip, length: 52	Conversation identifier, protocol used on the link (IP), and the number of bytes.
source: 140.3.3.201, destination: 225.1.2.3,	Source IP address and destination IP address.
id: 0x0001	Protocol ID, identifying IP.
ttl: 254	Time to live, in seconds.
TOS: 0	Type of service.
prot: 17	Protocol field in IP. The value 17 indicates UDP.
source port 5432	Source TCP/UDP port.
destination port 9870	Destination TCP/UDP port.

show rcapi status

To display whether RCAPI is turned on or off, use the **show rcapi status** command in privileged EXEC mode.

show rcapi status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)XV	This command was introduced on the Cisco 800 series router.

Usage Guidelines

When RCAPI is running, details about the list of CAPI clients currently registered, the type of application that each client is running, and the status of each CAPI call at the time of the display.

This command works only with the Net3 switch type.

Examples

The following is sample output from the **show rcapi status** command:

```
Router# show rcapi status

RCAPI SERVER ON
RCAPI SERVER PORT 2578
RCAPI NUMBER 5553000 5553100

CLIENT           SESSION ID     LISTEN     CONNECTION     TYPE              CALL STATUS
                                           ID

172.18.100.3     16777212       ON

172.18.100.5     16777218       OFF        50333953       Bit Transparent   Connected

172.18.100.6     16777227       OFF        50333962       HDLC              Connected
```

Related Commands

Command	Description
debug rcapi events	Displays diagnostic DCP and driver messages.
rcapi number	Enables the Cisco 800 series router to distinguish between incoming CAPI calls and incoming non-CAPI calls such as POTS, PPP, and X.25.
rcapi server	Enables the RCAPI server on the 800 series router and, optionally, sets the TCP port number.

show resource-pool call

To display all active call information for all customer profiles and resource groups, use the **show resource-pool call** command in EXEC mode.

show resource-pool call

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **show resource-pool call** EXEC command to see all active call information for all customer profiles and resource groups. Use this command to see output when one call is up.

If no calls are up, there is no output. Enter the command to see valid information for all current calls.

Examples

The following is sample output from the **show resource-pool call** command:

```
Router# show resource-pool call

Shelf 0, slot 0, port 0, channel 2, state RM_RPM_RES_ALLOCATED
  Customer profile cp1, resource group isdn1
  DNIS number 71017
```

Table 105 describes the significant fields shown in the display.

Table 105 show resource-pool call Field Descriptions

Field	Description
Shelf	The shelf number where the call is being handled.
Slot	The slot number where the call is being handled.
Port	The port number where the call is being handled.
Channel	The channel number where the call is being handled.
State	The state of the call.
Customer profile	The customer profile name (alphanumeric).
Resource group	The name of the resource group being used for the call.
DNIS number	The DNIS number for the call.

show resource-pool customer

To display the contents of one or more customer profiles, use the **show resource-pool customer** command in EXEC mode.

show resource-pool customer [*name*]

Syntax Description

name	(Optional) Name of a specific customer profile. The name can have up to 23 characters.

Command Modes

EXEC

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Examples

The following example displays the contents of the customer profile named customer1-isp:

```
Router# show resource-pool customer customer1-isp

    5 active connections
    3 calls accepted
    8 max number of simultaneous connections
    0 calls rejected due to profile limits
    0 calls rejected due to resource unavailable
    0 overflow connections
    0 overflow states entered
    0 minutes spent in overflow
    28 minutes since last clear command
```

Table 106 describes the significant fields shown in the display.

Table 106 show resource-pool customer Field Descriptions

Field	Description
Active connections	Lists the number of active connections in the specified customer profile.
Calls accepted	Cumulative number of calls accepted since the last **clear** command in the customer profile—regardless of the call type.
Max number of simultaneous connections	Maximum number of simultaneous connections assigned for this customer profile.
Calls rejected due to profile limits	Cumulative number of calls rejected since the last **clear** command because the maximum number of allowable simultaneous connections was exceeded. You can configure each customer profile to not exceed a simultaneous call limit. This feature stops a single customer profile from consuming all the system resources.

Table 106 show resource-pool customer Field Descriptions (continued)

Field	Description
Calls rejected due to resource unavailable	Cumulative number of calls rejected since the last **clear** command because no system resources were available to accept the call (such as a free modem for an analog call or an HDLC framer for a circuit switched data call).
Overflow connections	Number of overflow connections active since the last **clear** command.
Overflow states entered	Number of overflow states processed since the last **clear** command.
Minutes spent in overflow	Number of minutes that the overflow session has been in process since the last **clear** command.
Minutes since last clear command	Number of minutes since the **clear** command has been used.
List of Customer Profiles	Lists the customer profiles set up on the access server.

show resource-pool discriminator

To see how many times an incoming call has been rejected due to a specific Calling Line Identification (CLID) or Dialed Number Identification Service (DNIS) call-type combination, use the **show resource-pool discriminator** command in privileged EXEC mode.

show resource-pool discriminator [*name*]

Syntax Description

name	(Optional) Name of the specific CLID or DNIS and call-type that will be rejected. The name can have up to 23 characters.

Command Default

No default behavior or values. You must configure a call discriminator for the command to work or appear.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(4)XI	This command was introduced.
12.1(5)T	This command was enhanced to include the CLID group when the discriminator contains CLID groups.

Usage Guidelines

Use the **show resource-pool discriminator** EXEC command to see how many times an incoming call has been rejected due to a specific CLID or DNIS and call-type combination.

If you enter the **show resource-pool discriminator** command without including a call discriminator name, a list of the current call discriminator profiles appears. If you enter a call discriminator profile name with the **show resource-pool discriminator** command, the number of calls rejected by the selected call discriminator appears.

Examples

The following command displays the list of call discriminator profiles configured.

```
Router# show resource-pool discriminator

List of Call Discriminator Profiles:
    cd1
    cd2
    cd3
    cd4
```

The following command displays the number of calls rejected by call discriminator **cd1** since the last clear command was used (this number is cumulative).

```
Router# show resource-pool discriminator cd1

    0 calls rejected
```

Table 107 describes the significant fields shown in the displays.

Table 107 show resource-pool discriminator Field Descriptions

Field	Description
List of Call Discriminator Profiles	A list of the Call Discriminator Profile names currently assigned.
Calls rejected	Number of calls rejected since the last **clear** command was used. (This is cumulative.)

Related Commands

Command	Description
resource-pool call treatment discriminator	Configures a CLID group in a discriminator.

show resource-pool resource

To see the resource groups configured in the network access server, use the **show resource-pool resource** command in EXEC mode.

show resource-pool resource [*name*]

Syntax Description

name	(Optional) Contents of a specifically named resource group, which was set up by using the **resource-pool group resource** *name* command. The name can have up to 23 characters.

Command Modes

EXEC

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Usage Guidelines

Use the **show resource-pool resource** EXEC command to see the resource groups configured in the network access server. To see the contents of a specific resource group, use the **show resource-pool resource** *name* command.

Examples

The following is sample output from the **show resource-pool resource** EXEC command:

```
Router# show resource-pool resource

List of Resources:
    modem1
    rg1
    hi
```

The following is sample output about **modem-group-1** from the **show resource-pool resource** EXEC command:

```
Router# show resource-pool resource modem-group-1

    2 resources in the resource group
    0 resources currently active
    0 calls accepted in the resource group
    0 calls rejected due to resource unavailable
    0 calls rejected due to resource allocation errors
```

Table 108 describes the significant fields shown in the display.

Table 108 show resource-pool resource name Field Descriptions

Field	Description
Resources in the resource group	Number of resources allocated to this pool. For example, you can limit a range of modems to five. You can limit a range of circuit-switched data calls to 50.
Resources currently active	Number of resources that are currently used in the resource group.
Calls accepted in the resource group	Number of calls accepted in the resource group (this is cumulative).
Calls rejected due to resource unavailable	Number of calls rejected because a resource was not available (this is cumulative).
Calls rejected due to resource allocation errors	Number of times the access server had an available resource, but the resource had an error when the access server tried to allocate it (for example, a bad modem). Therefore, the call was rejected. (This is cumulative.)

show resource-pool vpdn

To display information about a specific virtual private dialup network (VPDN) group or specific VPDN profile, use the **show resource-pool vpdn** command in EXEC mode.

show resource-pool vpdn {**group** | **profile**} [*name*]

Syntax Description

group	All the VPDN groups configured on the router.
profile	All the VPDN profiles configured on the router.
name	(Optional) Specific VPDN group or profile.

Command Modes

EXEC

Command History

Release	Modification
12.0(4)XI	This command was introduced.

Examples

Use the **show resource-pool vpdn group** command to display information about a specific VPDN group.

Example 1

This example displays specific information about the VPDN group named vpdng2:

```
Router# show resource-pool vpdn group vpdng2

VPDN Group vpdng2 found under Customer Profiles: customer2

Tunnel (L2TP)
--------
dnis:customer2-calledg
cisco.com

Endpoint        Session Limit Priority Active Sessions Status Reserved Sessions
--------        ------------- -------- --------------- ------ -----------------
172.21.9.97     *             1        0               OK
                ------------            ---------------        -----------------
Total           *                      0                      0
```

Example 2

The following example displays information about all the VPDN groups configured on the router:

```
Router# show resource-pool vpdn group

List of VPDN Groups under Customer Profiles
Customer Profile customer1: vpdng1
Customer Profile customer2: vpdng2
List of VPDN Groups under VPDN Profiles
VPDN Profile profile1: vpdng1
VPDN Profile profile2: vpdng2
```

Table 109 describes the significant fields shown in the displays.

Table 109 show resource-pool vpdn group Field Descriptions

Field	Description
Endpoint	IP address of HGW/LNS router.
Session Limit	Number of sessions permitted for the designated endpoint.
Priority	Loadsharing HGW/LNSs are always marked with a priority of 1.
Active Sessions	Number of active sessions on the network access server. These are sessions successfully established with endpoints (not reserved sessions).
Status	Only two status types are possible: OK and busy.
Reserved Sessions	Authorized sessions that are waiting to see if they can successfully connect to endpoints. Essentially, these sessions are queued calls. In most cases, reserved sessions become active sessions.
*	No limit is set.
List of VPDN Groups under Customer Profiles	A list of VPDN groups that are assigned to customer profiles. The customer profile name is listed first, followed by the name of the VPDN group assigned to it.
List of VPDN Groups under VPDN Profiles	A list of VPDN groups that are assigned to VPDN profiles. The VPDN profile name is listed first, followed by the VPDN group assigned to it.

Example 3

The following example displays a list of all VPDN profiles configured on the router:

```
Router# show resource-pool vpdn profile

% List of VPDN Profiles:
        profile1
        profile2
        profile3
```

Example 4

The following example displays details about a specific VPDN profile named vpdnp1:

```
Router# show resource-pool vpdn profile vpdnp1

         0 active connections
         0 max number of simultaneous connections
         0 calls rejected due to profile limits
         0 calls rejected due to resource unavailable
         0 overflow connections
         0 overflow states entered
         0 overflow connections rejected
         3003 minutes since last clear command
```

Table 110 describes the significant fields shown in the displays.

Table 110 show resource-pool vpdn profile Field Descriptions

Field	Description
List of VPDN Profiles	A list of the VPDN profiles that have been assigned.
Active connections	Number of active VPDN connections counted by the VPDN profile.
Max number of simultaneous connections	Maximum number of VPDN simultaneous connections counted by the VPDN profile. This value helps you determine how many VPDN sessions to subscribe to a specific profile.
Calls rejected due to profile limits	Number of calls rejected since the last **clear** command because the profile limit has been exceeded.
Calls rejected due to resource unavailable	Number of calls rejected since the last **clear** command because the assigned resource was unavailable.
Overflow connections	Number of overflow connections used since the last **clear** command.
Overflow states entered	Number of overflow states entered since the last **clear** command.
Overflow connections rejected	Number of overflow connections rejected since the last **clear** command.
Minutes since last clear command	Number of minutes elapsed since the last **clear** command was used.

Related Commands

Command	Description
resource-pool profile customer	Creates a customer profile and enters customer profile configuration mode.
resource-pool profile vpdn	Creates a VPDN profile and enters VPDN profile configuration mode.
vpdn group	Associates a VPDN group with a customer or VPDN profile.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.

show sessions

To display information about open local-area transport (LAT), Telnet, or rlogin connections, use the **show sessions** command in EXEC mode.

show sessions

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command display the host name, address, number of unread bytes for the user to receive, idle time, and connection name.

Examples

The following is sample output from the **show sessions** command:

```
Router# show sessions

Conn Host                Address          Byte    Idle  Conn Name
   1 MATHOM              192.168.7.21        0       0  MATHOM
*  2 CHAFF               172.25.12.19        0       0  CHAFF
```

The asterisk (*) indicates the current terminal session.

Table 111 describes significant fields shown in the display.

Table 111 show sessions Field Descriptions

Field	Description
Conn	Name or address of the remote host to which the connection is made.
Host	Remote host to which the router is connected through a Telnet session.
Address	IP address of the remote host.
Byte	Number of unread bytes displayed for the user to receive.
Idle	Interval (in minutes) since data was last sent on the line.
Conn Name	Assigned name of the connection.

Related Commands

Command	Description
protocol (VPDN)	Sets X.3 parameters for PAD connections.
where	Lists open sessions associated with the current terminal line.

show sgbp

To display the status of the stack group members, use the **show sgbp** command in EXEC mode.

show sgbp

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Examples

The following is sample output from the **show sgbp** command:

```
Router# show sgbp

Group Name: stack State: 0 Ref: 0xC07B060
  Member Name: systemb State: ACTIVE  Id: 1
  Ref: 0xC14256F
  Address: 10.1.1.1 Tcb: 0x60B34538

  Member Name: systemc State: ACTIVE  Id: 2
  Ref: 0xA24256D
  Address: 10.1.1.2 Tcb: 0x60B34439

  Member Name: systemd State: IDLE Id: 3
  Ref: 0x0
  Address: 10.1.1.3 Tcb: 0x0
```

Table 112 describes the significant fields shown in the display.

Table 112 show sgbp Field Descriptions

Field	Description
Group Name	Name of the stack group.
State	Status of the group or its member. The values are 0 for the stack group itself, and either ACTIVE or IDLE for each of the members of the group.
Member Name	Name of a specific host defined as a member of this stack group.
Id	Identifier used for each member of the group; typically the final digit of the host's IP address on the network they share.
Address	IP address of the stack group member.

show sgbp queries

To display the current seed bid value, use the **show sgbp queries** command in EXEC mode.

show sgbp queries

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Examples

The following example shows a bid of 50 from this system. Peers queried the system for the bid, the bid was accepted, and a connection was opened from a peer in the stack group.

```
Router# show sgbp queries

Seed bid: default, 50

Bundle: book State: Query_from_peers OurBid: 50
10.1.1.2         State: Open_from_peer   Bid: 050 Retry: 0
```

Table 113 describes the significant fields shown in the display.

Table 113 show sgbp queries Field Descriptions

Field	Description
Seed bid	The initial bid; in this case, the default 50.
Bundle	Name of the MMP bundle.
State	Activity that occurred. In this case, a peer queried this system for its bid for the specified bundle.
OurBid	What this system bid for the bundle. It bid 50.
10.1.1.2	The peer's IP address.
State Bid Retry	Activity that occurred on the bid. In this case, the stack-group peer 1.1.1.2 accepted this system's bid of 50 for the bundle and opened a connection with this system. Since the peer opened a connection, no retry was needed.

show snapshot

To display snapshot routing parameters associated with an interface, use the **show snapshot** command in EXEC mode.

show snapshot [*interface-type interface-number*]

Syntax Description

interface-type interface-number	(Optional) Interface type and number.

Command Modes

EXEC

Command History

Release	Modification
10.3	This command was introduced.

Examples

The following is sample output from the **show snapshot** command:

```
Router# show snapshot serial 1

Serial1 is up, line protocol is up, snapshot up
Options: dialer support
Length of each activation period: 3 minutes
Period between activations:       10 minutes
Retry period on connect failure:  10
For dialer address 240
 Current queue: active, remaining active time: 3 minutes
 Updates received this cycle: ip, ipx, appletalk
For dialer address 1
 Current queue: client quiet, time until next activation: 7 minutes
```

Table 114 describes the significant fields shown in the display.

Table 114 show snapshot Field Descriptions

Field	Description
Serial1 is up, line protocol is up	Indicates whether the interface hardware is currently active (whether carrier detect is present) and whether it has been taken down by an administrator.
snapshot up	Indicates whether the snapshot protocol is enabled on the interface.
Options:	Option configured on the **snapshot client** or **snapshot server** interface configuration command. It can be one of the following: • dialer support—Snapshot routing is configured with the **dialer** keyword. • stay asleep on carrier up—Snapshot routing is configured with the **suppress-statechange-updates** keyword.
Length of each activation period	Length of the active period.

Table 114 show snapshot Field Descriptions (continued)

Field	Description
Period between activations	Length of the quiet period.
Retry period on connect failure	Length of the retry period.
For dialer address	Displays information about each dialer rotary group configured with the **dialer map** command.
Current queue:	Indicates which period snapshot routing is currently in. It can be one of the following: • active—Routing updates are being exchanged. • client quiet—The client router is in a quiet period and routing updates are not being exchanged. • server quiet—The server router is in a quiet period, awaiting an update from the client router before awakening, and routing updates are not being exchanged. • post active—Routing updates are not being exchanged. If the server router receives an update from the client router, it processes it but does not begin an active period. This allows time for resynchronization of active periods between the client and server routers. • no queue—This is a temporary holding queue for new snapshot routing interfaces and for interfaces being deleted.
remaining active time time until next activation	Time remaining in the current period.
Updates received this cycle	Protocols from which routing updates have been received in the current active period. This line is displayed only if the router or access server is in an active period.

show spe

To display service processing element (SPE) status, use the **show spe** command in EXEC mode.

Cisco AS5350 and Cisco AS5400 with the NextPort Dial Feature Card (DFC)

show spe [*slot* | *slot*/*spe* | *slot*/*port*]

Cisco AS5800 with the Universal Port Card (UPC)

show spe [*shelf*/*slot* | *shelf*/*slot*/*spe*]

Syntax Description

slot	(Optional) All ports on the specified slot. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7.
slot/*spe*	(Optional) All ports on the specified slot and SPE. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7. and SPE values range from 1 to 17. You must include the slash mark.
slot/*port*	(Optional) The specified port range on a slot. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7. Port values range from 0 to one less than the number of ports supported by the card. You must include the slash mark.
shelf/*slot*	(Optional) The specified port range on a shelf and slot. For the Cisco AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11. You must include the slash mark.
shelf/*slot*/*spe*	(Optional) All ports on the specified SPE. For the Cisco AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 0 to 53. You must include the slash marks.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5800.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.1(5)XM2	This command was integrated into Cisco IOS Release 12.1(5)XM2.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350 and Cisco AS5400 platforms.

Usage Guidelines

Use the **show spe** command to display status and history statistics of all SPEs, a specified SPE, or the specified range of SPEs.

Examples

The following example displays history statistics for all SPEs after a busyout was executed on SPE 2/0 and a shutdown was executed on SPE 2/1 on the Cisco AS5400:

```
Router# show spe

SPE settings:
==============
Country code configuration: default T1 (u Law)
Polling interval: 12 secs.
History log events: 50(per port)
Port legends:
============
Port state: (s)shutdown (t)test (r)recovery (d)download
            (b)busiedout (p)busyout pending, (B)bad (a)active call
Call Type: (m)modem (d)digital (_)not in use

                     SPE          SPE     SPE  SPE   Port         Call
SPE#    Port #       State        Busyout Shut Crash State        Type
2/00    0000-0005    ACTIVE             0    0     0 aaaaaa       dddddd
2/01    0006-0011    ACTIVE             0    0     0 aaaaaa       dddddd
2/02    0012-0017    ACTIVE             0    0     0 aaaaaa       dddddd
2/03    0018-0023    ACTIVE             0    0     0 aaaaaa       dddmdm
2/04    0024-0029    ACTIVE             0    0     0 aaaaaa       dmmmmm
2/05    0030-0035    ACTIVE             0    0     0 aaa_aa       mmm_mm
2/06    0036-0041    ACTIVE             0    0     0 __aaaa       __mmmm
2/07    0042-0047    ACTIVE             0    0     0 aaa_aa       mmm_mm
2/08    0048-0053    ACTIVE             0    0     0 _aaa_a       _mmm_m
2/09    0054-0059    ACTIVE             0    0     0 _aa_aa       _md_mm
2/10    0060-0065    ACTIVE             0    0     0 _a_a_a       _m_m_m
2/11    0066-0071    ACTIVE             0    0     0 _a_aaa       _d_mmd
2/12    0072-0077    ACTIVE             0    0     0 aaaaaa       mdmmmd
2/13    0078-0083    ACTIVE             0    0     0 _aaaaa       _dmmdm
2/14    0084-0089    ACTIVE             0    0     0 _a_aaa       _m_ddd
2/15    0090-0095    ACTIVE             0    0     0 a_aaaa       m_dddd
2/16    0096-0101    ACTIVE             0    0     0 aaaaaa       ddddmd
2/17    0102-0107    ACTIVE             0    0     0 aaaaaa       dddddd
```

The following example shows output for the **show spe** command on the Cisco AS5800 with the universal port card. This example shows SPE settings for slot 2, SPEs 0 to 53:

```
Router# show spe

SPE settings
==============
Country code configuration default T1 (u Law)
Polling interval 12 secs.
History log events 50(per port)
Port legends
============
Port state (s)shutdown (t)test (r)recovery (d)download
            (b)busiedout (p)busyout pending, (B)bad (a)active call
Call type (m)modem (d)digital (_)not in use

                      SPE          SPE     SPE  SPE   Port         Call
SPE#    Port #       State        Busyout Shut Crash State        Type
1/02/00 0000-0005    ACTIVE             0    0     0 a_a_a_       m_m_m_
1/02/01 0006-0011    ACTIVE             0    0     0 aaa___       mmm___
1/02/02 0012-0017    ACTIVE             0    0     0 _a_aa_       _m_mm_
1/02/03 0018-0023    ACTIVE             0    0     0 _aaaaa       _mmmmm
1/02/04 0024-0029    ACTIVE             0    0     0 a_a_a_       m_m_m_
1/02/05 0030-0035    ACTIVE             0    0     0 ____a_       ____m_
1/02/06 0036-0041    ACTIVE             0    0     0 _aaa_a       _mmm_m
1/02/07 0042-0047    ACTIVE             0    0     0 a_____       m_____
```

```
1/02/08 0048-0053    ACTIVE              0     0      0 _aa_aa        _mm_mm
1/02/09 0054-0059    ACTIVE              0     0      0 _aa_aa        _mm_mm
1/02/10 0060-0065    ACTIVE              0     0      0 _a_a_a        _m_m_m
1/02/11 0066-0071    ACTIVE              0     0      0 a__aa_        m__mm_
1/02/12 0072-0077    ACTIVE              0     0      0 aaa___        mmm___
1/02/13 0078-0083    ACTIVE              0     0      0 aaaa_a        mmmm_m
1/02/14 0084-0089    ACTIVE              0     0      0 _aaa__        _mmm__
1/02/15 0090-0095    ACTIVE              0     0      0 a__aaa        m__mmm
1/02/16 0096-0101    ACTIVE              0     0      0 _aaaa_        _mmmm_
1/02/17 0102-0107    ACTIVE              0     0      0 _aaa_a        _mmm_m
1/02/18 0108-0113    ACTIVE              1     0      0 _aaaaa        _mmmmm
1/02/19 0114-0119    ACTIVE              1     0      0 aa_aa_        mm_mm_
1/02/20 0120-0125    ACTIVE              1     0      0 aa__aa        mm__mm
1/02/21 0126-0131    ACTIVE              1     0      0 aaa_aa        mmm_mm
1/02/22 0132-0137    ACTIVE              1     0      0 _a____        _m____
1/02/23 0138-0143    ACTIVE              1     0      0 a__aaa        m__mmm
1/02/24 0144-0149    ACTIVE              1     0      0 a_a_aa        m_m_mm
1/02/25 0150-0155    ACTIVE              1     0      0 ___aaa        ___mmm
1/02/26 0156-0161    ACTIVE              1     0      0 a_a__a        m_m__m
1/02/27 0162-0167    ACTIVE              1     0      0 a_a_aa        m_m_mm
1/02/28 0168-0173    ACTIVE              1     0      0 a___aa        m___mm
1/02/29 0174-0179    ACTIVE              1     0      0 _a____        _m____
1/02/30 0180-0185    ACTIVE              1     0      0 _aaaaa        _mmmmm
1/02/31 0186-0191    ACTIVE              1     0      0 _a_aa_        _m_mm_
1/02/32 0192-0197    ACTIVE              1     0      0 aaa__a        mmm__m
1/02/33 0198-0203    ACTIVE              1     0      0 a_a__a        m_m__m
1/02/34 0204-0209    ACTIVE              1     0      0 aaaaaa        mmmmmm
1/02/35 0210-0215    ACTIVE              1     0      0 _aa__a        _mm__m
1/02/36 0216-0221    ACTIVE              0     0      0 a_a_aa        m_m_mm
1/02/37 0222-0227    ACTIVE              0     0      0 a_aaaa        m_mmmm
1/02/38 0228-0233    ACTIVE              0     0      0 aaaaaa        mmmmmm
1/02/39 0234-0239    ACTIVE              0     0      0 aa_aa_        mm_mm_
1/02/40 0240-0245    ACTIVE              0     0      0 aa_aaa        mm_mmm
1/02/41 0246-0251    ACTIVE              0     0      0 a__a__        m__m__
1/02/42 0252-0257    ACTIVE              0     0      0 aa__aa        mm__mm
1/02/43 0258-0263    ACTIVE              0     0      0 aaa_aa        mmm_mm
1/02/44 0264-0269    ACTIVE              0     0      0 aaaa_a        mmmm_m
1/02/45 0270-0275    ACTIVE              0     0      0 aaa_a_        mmm_m_
1/02/46 0276-0281    ACTIVE              0     0      0 aaaaa_        mmmmm_
1/02/47 0282-0287    ACTIVE              0     0      0 _aaaa_        _mmmm_
1/02/48 0288-0293    ACTIVE              0     0      0 a_aa_a        m_mm_m
1/02/49 0294-0299    ACTIVE              0     0      0 aa_a_a        mm_m_m
1/02/50 0300-0305    ACTIVE              0     0      0 aa_aaa        mm_mmm
1/02/51 0306-0311    ACTIVE              0     0      0 aaaaa_        mmmmm_
1/02/52 0312-0317    ACTIVE              0     0      0 aaaaaa        mmmmmm
1/02/53 0318-0323    ACTIVE              0     0      0 aaaa_a        mmmm_m
```

Table 115 describes the significant fields shown in the display.

Table 115 show spe Field Descriptions

Field	Description
SPE #	Specifies the slot and port number of the SPE.
Port #	Displays the port number.
SPE State	Displays the state of the SPE port.
SPE Busyout	Displays the number of busyout calls.
SPE Shut	Indicates if the port is shut down.
SPE Crash	Specifies if the port has crashed.

Table 115 show spe Field Descriptions (continued)

Field	Description
Port State	Indicates if the port is active or idle.
Call Type	Data, modem, or fax call type.

Related Commands

Command	Description
show spe digital active	Displays active digital calls and digital statistics of all SPEs, a specified SPE, or the specified range of SPEs.
show spe modem active	Displays active modem statistics of all SPEs, a specified SPE, or the specified range of SPEs.
show spe voice active	Displays active voice statistics of all SPEs, a specified SPE, or the specified SPE range.

show spe digital

To display history statistics of all service processing elements (SPEs) for digital service, in summary form or for SPEs starting with a specified slot or a specified shelf/slot/range of SPEs, use the **show spe digital** command in EXEC mode.

show spe digital [*slot* | *slot*/*spe*]

Syntax Description

slot	(Optional) All ports on the specified slot. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7.
slot/*spe*	(Optional) All ports on the specified slot and SPE. For the Cisco AS5400, slot values range from 1 to 7 and SPE values range from 1 to 17. You must include the slash mark.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)XD	This command was introduced.
12.1(3)T	This command was implemented on the Cisco AS5400.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.

Usage Guidelines

Use the **show spe digital** command on the Cisco AS5350 and Cisco AS5400 with NextPort port dial feature card (DFC).

Note This command is not supported on the Cisco AS5800 with the universal port card (UPC).

Examples

The following example uses the starting slot/SPE version of the **show spe digital** command. This example shows statistics for slot 5, SPE 4:

```
Router# show spe digital 5/4

#SPE 5/04
Cisco Universal SPE; Fw: 0.06.07.03; Async5/24 - 5/29, TTY672 - 677
Last clearing of statistics counters          :  never
      11 incoming completes         24 incoming failures
       0 outgoing completes          0 outgoing failures
       0 failed dial attempts        0 ring no answers
       0 no dial tones               0 link failures
       0 watchdog timeouts           0 protocol errors
       0 dial timeouts
```

```
Transmit Speed Counters       :
 Speed    Calls  Speed    Calls  Speed    Calls  Speed    Calls
Speed    Calls
 64000        0  28800        0  14400        0   7200        0
1200        0
 56000        0  24000        0  12000        0   4800        1
600         0
 38400        0  19200       10   9600        0   2400        0

Receive Speed Counters        :
 Speed    Calls  Speed    Calls  Speed    Calls  Speed    Calls
Speed    Calls
 64000        0  28800        0  14400        0   7200        0
1200        0
 56000        0  24000        0  12000        0   4800        1
600         0
 38400        0  19200       10   9600        0   2400        0
```

Table 116 describes the significant fields shown in the display.

Table 116 show spe digital Field Descriptions

Field	Description
SPE #	Specifies the slot and port number of the SPE.
Cisco Universal SPE	Firmware version installed on the SPE.
Last clearing of statistics counters	Last time the modem counters were cleared using the **clear modem counters** command.
Transmit Speed Counters	List of connection speeds that were sent by the SPE.
Receive Speed Counters	List of connection speeds that were received by the SPE.

Related Commands

Command	Description
show spe digital active	Displays active digital calls and digital statistics of all SPEs, a specified SPE, or the specified range of SPEs.
show spe digital csr	Displays digital CSR statistics of all SPEs, a specified SPE, or the specified range of SPEs.
show spe digital disconnect-reason	Displays the local disconnection reasons for all digital calls on the SPEs, a specified SPE, or the specified range of SPEs.
show spe digital summary	Displays history statistics of all SPEs, a specified SPE, or the specified range of SPEs.

show spe digital active

To display active digital calls and digital statistics of all service processing elements (SPEs), a specified SPE, or the specified range of SPEs, use the **show spe digital active** command in EXEC mode.

show spe digital active [*slot* | *slot* /*spe*]

Syntax Description

slot	(Optional) All ports on the specified slot. For the Cisco AS5400, slot values range from 1 to 7.
slot/*spe*	(Optional) All ports on the specified slot and SPE. For the Cisco AS5400, slot values range from 1 to 7 and SPE values range from 1 to 17. You must include the slash mark.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)XD	This command was introduced.
12.1(3)T	This command was implemented on the Cisco AS5400.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.

Usage Guidelines

Use the **show spe digital active** command on the Cisco AS5350 and Cisco AS5400 with the NextPort dial feature card (DFC).

Note This command is not supported on the Cisco AS5800 with the universal port card (UPC).

Examples

The following is sample output from the **show spe digital active** command on the Cisco AS5400 with the NextPort DFC. This example displays active digital statistics for slot 5, SPE 06:

```
Router# show spe digital active 5

SPE 5/06
                        Char              Sync
Port  Prot    Duration  Tx/Rx       Cfg   Loss
41    V.110   188       19200/19200 In    0

SPE 5/09
                        Char              Sync
Port  Prot    Duration  Tx/Rx       Cfg   Loss
54    V.110   187       19200/19200 In    0
56    V.110   187       19200/19200 In    0
57    V.110   188       19200/19200 In    0
.
.
```

Table 117 describes the significant fields shown in the display.

Table 117 show spe digital active Field Descriptions

Field	Description
SPE #	Specifies the slot and port number of the SPE.
Port	Port that is active.
Prot	Protocol used for the call in progress.
Duration	Duration of call.
Char Tx/Rx	Characters sent and received.

Related Commands

Command	Description
show spe digital	Displays history statistics of all digital SPEs, in summary form or for SPEs starting with a specified slot or a specified shelf/slot/range of SPEs.
show spe digital csr	Displays digital calls CSR statistics of all SPEs, a specified SPE, or the specified range of SPEs.
show spe digital disconnect-reason	Displays the local disconnect reasons for all digital calls on the SPEs, a specified SPE, or the specified range of SPEs.
show spe digital summary	Display history statistics of all SPEs, a specified SPE, or the specified range of SPEs.

show spe digital csr

To display digital call success rate (CSR) statistics of all service processing elements (SPEs), a specified SPE, or the specified range of SPEs, use the **show spe digital csr** command in EXEC mode.

show spe digital csr {**summary** [*slot* | *slot*/*spe*] [*slot* | *slot*/*spe*] | {*slot* | *slot*/*spe*} [*slot* | *slot*/*spe*]}

Syntax Description

summary	Summary digital CSR statistics.
slot	All ports on the specified slot. For the Cisco AS5400, slot values range from 1 to 7. A range of slots can be specified by entering a second value for the *slot* argument.
slot/*spe*	(Optional) All ports on the specified slot and SPE. For the Cisco AS5400, slot values range from 1 to 7 and SPE values range from 1 to 17. You must include the slash mark. A range of ports can be specified by entering a second value for the *slot*/*spe* argument.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)XD	This command was introduced.
12.1(3)T	This command was implemented on the Cisco AS5400.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.

Usage Guidelines

Use the **show spe digital csr** command on the Cisco AS5350 and Cisco AS5400 with the NextPort dial feature card DFC.

Note This command is not supported on the Cisco AS5800 with the universal port DFC.

Examples

The following is sample output from the **show spe digital csr** command on the Cisco AS5400 with the NextPort DFC. This example displays the number of call success rate counters for slot 5:

```
Router# show spe digital csr 5

          Avg Hold     Inc calls     Out calls    Failed    No       Succ
SPE         Time      Succ   Fail   Succ   Fail   Dial    Answer    Pct
5/00      00:04:22       6      0      0      0       0       0    100%
5/01      00:04:22       6      0      0      0       0       0    100%
5/02      00:04:22       6      0      0      0       0       0    100%
5/03      00:04:22       6      0      0      0       0       0    100%
5/04      00:04:22       6      0      0      0       0       0    100%
5/05      00:04:21       6      0      0      0       0       0    100%
5/06      00:04:22       4      0      0      0       0       0    100%
```

```
5/07      00:04:22       1      0      0      0      0      0    100%
5/08      00:04:21       6      0      0      0      0      0    100%
5/09      00:04:23       5      0      0      0      0      0    100%
5/10      00:00:00       0      0      0      0      0      0      0%
5/11      00:04:21       5      0      0      0      0      0    100%
5/12      00:04:20       2      0      0      0      0      0    100%
5/13      00:00:00       0      0      0      0      0      0      0%
5/14      00:00:00       0      0      0      0      0      0      0%
5/15      00:00:00       0      0      0      0      0      0      0%
5/16      00:00:00       0      0      0      0      0      0      0%
5/17      00:00:00       0      0      0      0      0      0      0%
```

Table 118 describes the significant fields shown in the display.

Table 118 show spe digital csr Field Descriptions

Field	Description
SPE	The SPE slot and port number.
Avg Hold Time	The average hold time.
Inc calls, Succ/Fail	The cumulative number of incoming calls that have succeeded and failed in the configured time period.
Out calls, Succ/Fail	The cumulative number of outgoing calls that have succeeded and failed in the configured time period.
Failed Dial	The number of calls that failed when dialed.
No Answer	The number of calls that were not answered.
Succ Pct	The CSR of the carrier.

Related Commands

Command	Description
show spe digital	Displays history statistics of all digital SPEs, in summary form or for SPEs starting with a specified slot or a specified shelf/slot/range of SPEs.
show spe digital active	Displays active digital calls and digital statistics of all SPEs, a specified SPE, or the specified range of SPEs.
show spe digital disconnect-reason	Displays the local disconnect reasons for all digital calls on the SPEs, a specified SPE, or the specified range of SPEs.
show spe digital summary	Displays history statistics of all SPEs, a specified SPE, or the specified range of SPEs.

show spe digital disconnect-reason

To display the local disconnection reasons for all digital calls on the service processing elements (SPEs), a specified SPE, or the specified range of SPEs, use the **show spe digital disconnect-reason** command in EXEC mode.

show spe digital disconnect-reason [**summary** | *slot* | *slot*/*spe*]

Syntax Description

summary	(Optional) Summary of local disconnection reasons for digital ports.
slot	(Optional) All ports on the specified slot. For the Cisco AS5400, slot values range from 1 to 7.
slot/*spe*	(Optional) All ports on the specified slot and SPE. For the Cisco AS5400, slot values range from 1 to 7 and SPE values range from 1 to 17. You must include the slash mark.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)XD	This command was introduced.
12.1(3)T	This command was implemented on the Cisco AS5400.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.

Usage Guidelines

Use the **show spe digital disconnect-reason** command on the Cisco AS5350 and Cisco AS5400 with the NextPort dial feature card (DFC).

Note This command is not supported on the Cisco AS5800 with the universal port card (UPC).

Examples

The following is sample output from the **show spe digital disconnect-reason** command on the Cisco AS5400 with the NextPort DFC. This example displays reasons for digital call disconnections on slot 5:

```
Router# show spe digital disconnect-reason 5

#SPE 5/00   :
=====CLASS HOST======      =====CLASS SERVICE=====
NonSpecific          0  ATH                   0
Busy                 0  Aborted               0
No Answer            0  Connect Timeout       0
DTR                  0  Sync Loss             0
ATH                  0
NoDialTone           0
No Carrier           0
```

```
ACK                 0  TOTAL                0

#SPE 5/03   :
=====CLASS HOST======      =====CLASS SERVICE=====
NonSpecific         0  ATH                  0
Busy                1  Aborted              0
No Answer           0  Connect Timeout      0
DTR                 0  Sync Loss            0
.
.
.
```

Table 119 describes the significant fields shown in the display.

Table 119 show spe digital disconnect-reason Field Descriptions

Field	Description
SPE	The slot and port number of the SPE.
CLASS HOST	Disconnect reasons are as follows: • NonSpecific • Busy • No Answer—Number of times the SPE rang but did not answer the incoming call. • DTR • ATH • NoDialTone—Number of times the dial-out attempt failed because the SPE failed to detect a dial tone. • No Carrier • ACK
CLASS SERVICE	Disconnect reasons are a s follows: • ATH • Aborted • Connect Timeout • Sync Loss

Related Commands

Command	Description
show spe digital	Displays history statistics of all digital SPEs, in summary form or for SPEs starting with a specified slot or a specified shelf/slot/range of SPEs.
show spe digital active	Displays active digital calls and digital statistics of all SPEs, a specified SPE, or the specified range of SPEs.
show spe digital csr	Displays digital call success rate (CSR) statistics of all SPEs, a specified SPE, or the specified range of SPEs.
show spe digital summary	Displays history statistics of all SPEs, a specified SPE, or the specified range of SPEs.

show spe digital summary

To display history statistics of all service processing elements (SPEs), a specified SPE, or the specified range of SPEs, use the **show spe digital summary** command in EXEC mode.

show spe digital summary [*slot* | *slot*/*spe*]

Syntax Description

slot	(Optional) All ports on the specified slot. For the Cisco AS5400, slot values range from 1 to 7.
slot/*spe*	(Optional) All ports on the specified slot and SPE. For the Cisco AS5400, slot values range from 1 to 7 and SPE values range from 1 to 17. You must include the slash mark.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)XD	This command was introduced.
12.1(3)T	This command was implemented on the Cisco AS5400.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.

Usage Guidelines

Use the **show spe digital summary** command on the Cisco AS5350 and Cisco AS5400 with the NextPort dial feature card (DFC).

Note This command is not supported on the Cisco AS5800 with the universal port card (UPC).

Examples

The following is sample output from the **show spe digital summary** command on the Cisco AS5400 with the NextPort DFC. This example displays active digital statistics for slot 5:

```
Router# show spe digital summary 5

Async5/00 - 5/107, TTY648 - 755
     209 incoming completes        397 incoming failures
       0 outgoing completes          0 outgoing failures
       0 failed dial attempts        0 ring no answers
       0 no dial tones               0 link failures
       0 watchdog timeouts           0 protocol errors
       0 dial timeouts

Transmit Speed Counters       :
 Speed    Calls  Speed    Calls  Speed    Calls  Speed    Calls  Speed    Calls
 64000        0  28800        0  14400        0   7200        0  1200     20
 56000        0  24000        0  12000        0   4800       20  600      20
 38400        0  19200      149   9600        0   2400        0
```

```
Receive Speed Counters         :
 Speed    Calls  Speed    Calls  Speed    Calls  Speed    Calls  Speed    Calls
 64000        0  28800        0  14400        0   7200        0  1200     20
 56000        0  24000        0  12000        0   4800       20  600      20
 38400        0  19200      149   9600        0   2400        0
.
.
.
```

Table 120 describes the significant fields shown in the display.

Table 120 show spe digital summary Field Descriptions

Field	Description
A summary of SPE events also appears.	
incoming completes and failures	Total number of incoming connection requests that the SPE answered and successfully or unsuccessfully connected with the remote DCE device.
outgoing completes and failures	Total number of outgoing connection requests that the SPE dialed and successfully or unsuccessfully connected with the remote DCE device.
failed dial attempts	Number of times the SPE attempted to dial out but the call failed to leave the modem.
ring no answers	Number of times the SPE rang but did not answer the incoming call.
no dial tones	Number of times the dial-out attempt failed because the SPE failed to detect a dial tone.
link failures	Number of times the SPE detected a link failure.
watchdog timeouts	Number of times the SPE internal watchdog timer expired.
protocol errors	Number of times the SPE protocol failed to make a call connection
dial timeouts	Number of times the SPE timed out while attempting to dial.
Transmit Speed Counters	List of connection speeds that were sent by the SPE.
Receive Speed Counters	List of connection speeds that were received by the SPE.

Related Commands.

Command	Description
show spe digital	Displays history statistics of all digital SPEs, in summary form or for SPEs starting with a specified slot or a specified shelf/slot/range of SPEs.
show spe digital active	Displays active digital calls and digital statistics of all SPEs, a specified SPE, or the specified range of SPEs.
show spe digital csr	Displays digital call success rate (CSR) statistics of all SPEs, a specified SPE, or the specified range of SPEs.
show spe digital disconnect-reason	Displays the local disconnection reasons for all digital calls on the SPEs, a specified SPE, or the specified range of SPEs.

show spe log

To display the service processing element (SPE) system log, use the **show spe log** command in EXEC mode.

Cisco AS5350 and Cisco AS5400 with the NextPort Dial Feature Card (DFC)

show spe log [**reverse** | *slot*]

Cisco AS5800 with the Universal Port Card (UPC)

show spe log [**reverse** | *shelf/slot*]

Syntax Description

reverse	(Optional) Displays the SPE system log with the most recent event first.
slot	(Optional) All ports on the specified slot. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7.
shelf/slot	(Optional) All ports on the specified shelf and slot. For the Cisco AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11. You must include the slash mark.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5800.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.

Usage Guidelines

The **show spe log** command displays the slot history event log.

Examples

The following is sample output from the **show spe log** command on the Cisco AS5400 with the NextPort DFC:

```
Router# show spe log

Slot 3 Events Log
  2d15h   : SPE State Event:
     Address: 0x3000000
     SPE    : 3/00
     Command: SPE_IMMEDIATE_DISABLE Complete
  2d14h   : SPE State Event:
     Address: 0x3000100
     SPE    : 3/06
     Command: SPE_IMMEDIATE_DISABLE Complete
```

```
  2d13h   : SPE State Event:
     Address: 0x3000200
     SPE    : 3/12
     Command: SPE_IMMEDIATE_DISABLE Complete
  00:00:26: SPE State Event:
     Address: 0x3000001
     SPE    : 3/01
     Command: SPE_IMMEDIATE_DISABLE Complete
Slot 4 Events Log
  2d13h   : SPE State Event:
     Address: 0x4000000
     SPE    : 4/00
     Command: SPE_IMMEDIATE_DISABLE Complete
Slot 7 Events Log
  2d15h   : Diag Post event:
     Address    : 0x7000204
     SPE        : 7/16
     Result     : SPE_POST_TEST_FAILED
     Test ID    : SPE_POWER_ON_SELF_TEST
     Diag Code  : 0xFE01C004
     Data Format: ASCII
     Data Len   : 0
```

Table 121 describes the significant fields shown in the display.

Table 121 show spe log Field Descriptions

Field	Description
Address	Address of the SPE
SPE	The slot and port number of the SPE.

Related Commands

Command	Description
clear spe log	Clears all event entries in the slot history event log.
show spe log reverse	Displays the slot history event log, with the most recent event first.

show spe modem

To display the modem service history statistics for a specified service processing element (SPE), use the **show spe modem** command in EXEC mode.

Cisco AS5350 and Cisco AS5400 with the NextPort Dial Feature Card (DFC)

show spe modem {*slot* | *slot*/*spe*}

Cisco AS5800 with the Universal Port Card (UPC)

show spe modem {*shelf*/*slot* | *shelf*/*slot*/*spe*}

Syntax Description

slot	All ports on the specified slot. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7.
slot/*spe*	All ports on the specified slot and SPE. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7. SPE values range from 1 to 17. You must include the slash mark.
shelf/*slot*	All ports on the specified shelf and slot. For the Cisco AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11. You must include the slash mark.
shelf/*slot*/*spe*	All ports on the specified SPE. For the Cisco AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 1 to 53. You must include the slash mark.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5800.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.

Examples

The following is sample output from the **show spe modem** command on the Cisco AS5400 with the NextPort DFC:

```
Router# show spe modem 1/2

Async1/2/00 - 1/3/323, TTY972 - 1619
     4819 incoming completes        287 incoming failures
        0 outgoing completes          0 outgoing failures
        0 failed dial attempts        0 ring no answers          0 autotests
        0 no carriers                11 dial timeouts            0 autotest fails
        0 no dial tones               0 link failures            0 fail count
        0 watchdog timeouts        2784 protocol errors          0 recovers
Transmit Speed Counters
```

```
  Speed    Calls  Speed     Calls  Speed    Calls  Speed    Calls  Speed  Calls
 60000        0    48000       431  38400        0  30666        0  12000  143
 58000        0    46666         0  38000        4  29333        0   9600  5
 56000       15    46000        56  37333      110  28800      700   7200  11
 54666        0    45333       299  36000       84  28000        5   4800  2
 54000        0    44000       226  34666        0  26400      266   2400  0
 53333      122    42666         0  34000       39  24000       46   1200  3
 52000      562    42000        68  33600      323  21600       27    300  0
 50666        0    41333        38  33333        9  19200       38
 50000       59    40000        65  32000       20  16800       12
 49333      370    38666         0  31200      653  14400        5
Receive Speed Counters
  Speed    Calls  Speed    Calls  Speed    Calls  Speed    Calls   Speed Calls
 38400        0   26400     2280  16800       11   7200        1    300  2
 33600      113   24000      266  14400      139   4800        1
 31200      215   21600       56  12000        4   2400        3
 28800     1665   19200       47   9600       16   1200        0.
```

The following is sample output from the **show spe modem** command on the Cisco AS5800 with the universal port card:

```
Router# show spe modem 1/8/0

#SPE 1/08/00
Cisco Universal SPE; Fw: 0.00.06.81; Async1/8/00 - 1/8/05, TTY2916 - 2921
Last clearing of statistics counters          :  never
      90 incoming completes          0 incoming failures
       0 outgoing completes          0 outgoing failures
       0 failed dial attempts        0 ring no answers          0 autotests
       0 no carriers                 0 dial timeouts            0 autotest fails
       0 no dial tones               0 link failures            0 fail count
       0 watchdog timeouts           0 protocol errors

Transmit Speed Counters       :
 Speed    Calls  Speed    Calls  Speed    Calls  Speed    Calls  Speed    Calls
 60000        0  48000        0  38400        0  30666        0  12000        0
 58000        0  46666        0  38000        0  29333        0   9600        0
 56000        0  46000        0  37333        0  28800        0   7200        0
 54666        0  45333        0  36000        0  28000        0   4800        0
 54000        0  44000        0  34666        0  26400        0   2400        0
 53333        0  42666        0  34000        0  24000        0   1200        0
 52000        0  42000        0  33600        0  21600        0    300        0
 50666        0  41333        0  33333        0  19200        0
 50000        0  40000        0  32000        0  16800        0
 49333        0  38666        0  31200       90  14400        0

Receive Speed Counters        :
 Speed    Calls  Speed    Calls  Speed    Calls  Speed    Calls  Speed    Calls
 38400        0  26400        0  16800        0   7200        0    300        0
 33600       11  24000        0  14400        0   4800        0
 31200       25  21600        0  12000        0   2400        0
 28800       54  19200        0   9600        0   1200        0
```

Table 122 describes the significant fields shown in the display.

Table 122 show spe modem Command Field Descriptions

Field	Description
SPE	The slot and port number of the SPE.
Cisco Universal SPE	Firmware version installed on the SPE.
Last clearing of "show modem" counters	Last time the modem's counters were cleared using the **clear modem counters** command.
Summary of modem and SPE events as follows:	
incoming completes and failures	Total number of incoming connection requests that the SPE answered and successfully or unsuccessfully connected with the remote DCE device.
outgoing completes and failures	Total number of outgoing connection requests that the SPE dialed and successfully or unsuccessfully connected with the remote DCE device.
failed dial attempts	Number of times the SPE attempted to dial out but the call failed to leave the modem.
ring no answers	Number of times the SPE rang but did not answer the call.
autotests	Number of times an autotest was run on the SPE.
no carriers	Number of times the SPE disconnected because no carrier was present.
dial timeouts	Number of times the SPE timed out while attempting to dial.
autotest fails	Number of times the SPE failed an autotest.
no dial tones	Number of times the dial-out attempt failed because the SPE failed to detect a dial tone.
link failures	Number of times the SPE detected a link failure.
fail count	Number of times the SPE failed.
watchdog timeouts	Number of times the SPE internal watchdog timer expired.
protocol errors	Number of times the SPE protocol failed to make a call connection.
Transmit Speed Counters	List of connection speeds that were sent by the SPE.
Receive Speed Counters	List of connection speeds that were received by the SPE.

Related Commands

Command	Description
show modem	Displays modem service history statistics for the MICA technologies modem.
show spe	Displays history statistics of all SPEs, a specified SPE, or the specified range of SPEs.

show spe modem active

To display the modem service statistics of all active calls on specified service processing elements (SPEs), use the **show spe modem active** command in EXEC mode.

Cisco AS5350 and Cisco AS5400 with the NextPort Dial Feature Card (DFC)

show spe modem active {*slot* | *slot*/*spe*}

Cisco AS5800 with the Universal Port Card (UPC)

show spe modem active {*shelf*/*slot* | *shelf*/*slot*/*spe*}

Syntax Description

slot	All ports on the specified slot. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7.
slot/*spe*	All ports on the specified slot and SPE. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7. SPE values range from 1 to 17. You must include the slash mark.
shelf/*slot*	All ports on the specified shelf and slot. For the Cisco AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11. You must include the slash mark.
shelf/*slot*/*spe*	All ports on the specified SPE. For the Cisco AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 0 to 53. You must include the slash marks.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5800.
12.1(5)XM1	This command was introduced on the Cisco AS5350.
12.2(2)XA	This command was supported on the Cisco AS5350.
12.2(2)XB	This command was integrated into Cisco IOS Release 12.2(2)XB.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.

Examples

The following is sample output from the **show spe modem active** command on the Cisco AS5400 with the NextPort DFC. This example displays active modem statistics for slot 5, SPE 6:

```
Router# show spe modem active 5/6

SPE 5/06
Port  Type     Prot     Comp    Duration  Tx/Rx     Tx/Rx(Lvl) SNR Cfg  Retrain
37    V.90     LAP-M    V.42bis  95      3890/76     --/-11     38  In   0
```

The following is sample output from the **show spe modem active** command on the Cisco AS5800 with universal port card. This example displays active modem statistics for shelf 1, slot 8:

```
Router# show spe modem active 1/8

SPE 1/08/34
Port  Type     Prot     Comp    Duration  Tx/Rx(bps) Tx/Rx(Lvl) SNR Cfg  Retrain
209   V.34+    LAP-M    V.42bis  23      28800/31200  --/-13     37  In   0

SPE 1/08/35
Port  Type     Prot     Comp    Duration  Tx/Rx(bps) Tx/Rx(Lvl) SNR Cfg  Retrain
215   V.34+    LAP-M    V.42bis  12      28800/31200  --/-13     37  In   0

SPE 1/08/36
Port  Type     Prot     Comp    Duration  Tx/Rx(bps) Tx/Rx(Lvl) SNR Cfg  Retrain
216   V.34+    LAP-M    V.42bis  24      33600/31200  --/-36     38  In   0
217   ##       ##       ##       0       33600/300    --/19      37  In   0
218   ##       ##       ##       0       33600/300    --/19      37  In   0
219   ##       ##       ##       0       33600/300    --/19      35  In   0
```

Table 123 describes the significant fields shown in the display.

Table 123 show spe modem active Field Descriptions

Field	Description
SPE	The slot and port number of the SPE.
Port	Displays the port number.
Type	Modulation type.
Prot	The connection protocol used for the call.
Comp	The compression protocol used for the call.
Duration	Time duration of the call.
Tx/Rx(bps)	Transmission and receiving speed for the call in bits per second (bps).
Tx/Rx(Lvl)	Transmission and receiving level reduction for the call in decibels per milliwatt (dBm).
SNR	The signal-to-noise ratio for the call in dB.
Cfg	
Retrain	Number of retrain failures. A connection was lost and not reestablished after three attempts.

Related Commands

Command	Description
show port operational-status	Displays the operational status of a specific port or port range.
show spe	Displays history statistics of all SPEs, a specified SPE, or the specified range of SPEs.

show spe modem csr

To display the call success rate (CSR) for the specified service processing elements (SPEs), use the **show spe modem csr** command in EXEC mode.

Cisco AS5350 and Cisco AS5400 with the NextPort Dial Feature Card (DFC)

show spe modem csr {**summary** | *slot* | *slot*/*spe*}

Cisco AS5800 with the Universal Port Card (UPC)

show spe modem csr {**summary** | *shelf*/*slot* | *shelf*/*slot*/*spe*}

Syntax Description

summary	Displays all call success rate statistics for all SPEs.
slot	All ports on the specified slot. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7.
slot/*spe*	All ports on the specified slot and SPE. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7. SPE values range from 1 to 17. You must include the slash mark.
shelf/*slot*	All ports on the specified shelf and slot. For the Cisco AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11. You must include the slash mark.
shelf/*slot*/*spe*	All ports on the specified SPE. For the Cisco AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 0 to 53. You must include the slash mark.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5800.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(2)XA	This command was implemented on the Cisco AS5350.
12.2(2)X	This command was integrated into Cisco IOS Release 12.2(2)XB.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.

Usage Guidelines

The **show spe modem csr** command displays the modem CSR statistics for a specific SPE, range of SPEs, or all the SPEs. The **summary** keyword displays the CSR statistics for all SPEs.

Examples

The following are sample outputs from the **show spe modem csr** command on the Cisco AS5400 with the NextPort DFC:

```
Router# show spe modem csr 5/6

         Avg Hold     Inc calls     Out calls    Failed    No       Succ
SPE        Time      Succ   Fail   Succ   Fail   Dial    Answer    Pct
5/06     00:22:41       2      0      0      0       0       0    100%

Router# show spe modem csr 5/1 5/6

         Avg Hold     Inc calls     Out calls    Failed    No       Succ
SPE        Time      Succ   Fail   Succ   Fail   Dial    Answer    Pct
5/01     00:00:00       0      0      0      0       0       0      0%
5/02     00:00:00       0      0      0      0       0       0      0%
5/03     00:00:00       0      0      0      0       0       0      0%
5/04     00:00:00       0      0      0      0       0       0      0%
5/05     00:00:00       0      0      0      0       0       0      0%
5/06     00:22:48       2      0      0      0       0       0    100%
```

The following is sample output from the **show spe modem csr summary** command on the Cisco AS5800 with the universal port card:

```
Router# show spe modem csr summary

   Avg Hold          Inc  calls             Out  calls      Failed    No    Succ
   Time        Succ    Fail   Avail    Succ    Fail   Avail Dial    Answer  Pct
   002631    4827     285      93       0       0      93      5       0   94%
```

Table 124 describes the significant fields shown in the display.

Table 124 show spe modem csr Field Descriptions

Field	Description
SPE	The slot and port number of the SPE.
Avg Hold Time	The average hold time for the SPE.
Inc/Out calls	Calls dialing into and out of the modem: • Succ—Total call successfully connected. • Fail—Total calls that did not successfully connect. • Avail—Total modems available for use in the system.
Failed Dial	The number of attempts the SPE failed to make a connection.
No Answer	Number of times the SPE rang but did not answer the call.
Succ Pct	The percentage of calls that were successfully connected.

Related Commands

Command	Description
show spe	Displays history statistics of all SPEs, a specified SPE, or the specified range of SPEs.
show spe modem summary	Displays a summary of modem statistics for the specified SPE or range of SPEs.

show spe modem disconnect-reason

To display all modem disconnection reasons for the specified service processing element (SPE), use the **show spe modem disconnect-reason** command in EXEC mode.

Cisco AS5350 and Cisco AS5400 with the NextPort Dial Feature Card (DFC)

show spe modem disconnect-reason {**summary** | *slot* | *slot*/*spe*}

Cisco AS5800 with the Universal Port Card (UPC)

show spe modem disconnect-reason {**summary** | *shelf*/*slot* | *shelf*/*slot*/*spe*}

Syntax Description

summary	Displays the disconnect reasons for all SPEs.
slot	All ports on the specified slot. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7.
slot/*spe*	All ports on the specified slot and SPE. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7. SPE values range from 1 to 17. You must include the slash mark.
shelf/*slot*	All ports on the specified shelf and slot. For the Cisco AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11. You must include the slash mark.
shelf/*slot*/*spe*	All ports on the specified SPE. For the Cisco AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 1 to 53. You must include the slash marks.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5800.
12.1(5)XM1	This command was introduced on the Cisco AS5350.
12.2(2)XA	This command was implemented on the Cisco AS5350.
12.2(2)XB	This command was integrated into Cisco IOS Release 12.2(2)XB.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.

Usage Guidelines

Disconnection reasons are reasons why active calls are disconnected. The disconnect reasons are displayed with Class boundaries. The **show spe modem disconnect-reason** command is equivalent to the **show modem call stats** MCIA technologies modem command.

Examples

The following is sample output from the **show spe modem disconnect-reason** command on the Cisco AS5400 with the NextPort DFC:

```
Router# show spe modem disconnect-reason 5/6

#SPE 5/06   :
===CLASS OTHER====  =====CLASS DSP====  ===CLASS EC LCL===  ==CLASS EC FRMR===
Software Rst     0  No Carrier       0  No LR            0  Frmr Bad Cmd     0
EC Termntd       0  No ABT dtctd     0  LR Param1        0  Frmr Data        0
Bad MNP5 Rx      0  Trainup flr      0  LR Incmpt        0  Frmr Length      0
Bad V42B         0  Retrain Lt       0  Retrns Lt        0  Frmr Bad NR      0
Bad COP stat     0  ABT end flr      0  Inactivity       0
ATH              0                     Protocol Err     0  ===CLASS EC LD====
Aborted          0  ====CLASS HOST====  Fallbck Term     0  LD No LR         0
Connect Tout     0  Hst NonSpec      0  No XID           0  LD LR Param1     0
Reset DSP        0  Hst Busy         0  XID Incmpt       0  LD LR Incmpt     0
                    Hst No answr     0  Disc             0  LD Retrns Lt     0
===CLASS EC Cmd===  Hst DTR          1  DM               0  LD Inactivty     0
Bad Cmd          0  Hst ATH          0  Bad NR           0  LD Protocol      0
                    Hst NoDialTn     0  SABME Online     0  LD User          0
=====N O N E======  Hst No Carr      0  XID Online       0
None             0  Hst Ack          0  LR Online        0  TOTAL            1
```

The following is sample output from the **show spe modem disconnect-reason summary** command on the Cisco AS5800 with the universal port card:

```
Router# show spe modem disconnect-reason summary

===CLASS OTHER====  =====CLASS DSP====  ===CLASS EC LCL===  ==CLASS EC FRMR===
Software Rst     0  No Carrier      21  No LR            0  Frmr Bad Cmd     0
EC Termntd       0  No ABT dtctd     0  LR Param1        0  Frmr Data        0
Bad MNP5 Rx      0  Trainup flr     26  LR Incmpt        0  Frmr Length      0
Bad V42B        12  Retrain Lt       0  Retrns Lt       37  Frmr Bad NR      0
Bad COP stat     0  ABT end flr      0  Inactivity       0
ATH              0                     Protocol Err     5  ===CLASS EC LD====
Aborted          0  ====CLASS HOST====  Fallbck Term    22  LD No LR         0
Connect Tout    11  Hst NonSpec    799  No XID           5  LD LR Param1     0
Reset DSP        0  Hst Busy         0  XID Incmpt       0  LD LR Incmpt     0
                     Hst No answr     0  Disc          2718  LD Retrns Lt     0
===CLASS EC Cmd===  Hst DTR        870  DM               0  LD Inactivty     0
Bad Cmd          0  Hst ATH          0  Bad NR           0  LD Protocol      0
                     Hst NoDialTn     0  SABME Online     0  LD User          0
=====N O N E======  Hst No Carr      0  XID Online       0
None            29  Hst Ack          0  LR Online        0  TOTAL         4555
```

Related Commands

Command	Description
show spe	Displays history statistics of all SPEs, a specified SPE, or the specified range of SPEs.
show spe modem summary	Displays a summary of modem statistics for the specified SPE or range of SPEs.

show spe modem high speed

To display the total number of connections within each high-speed modulation or codec for a specific range of service processing elements (SPEs), use the **show spe modem high speed** command in EXEC mode.

Cisco AS5350 and Cisco AS5400 with the NextPort Dial Feature Card (DFC)

show spe modem high speed {**summary** | *slot* | *slot*/*spe*}

Cisco AS5800 with the Universal Port Card (UPC)

show spe modem high speed {**summary** | *shelf*/*slot* | *shelf*/*slot*/*spe*}

Syntax Description

summary	Displays a brief list of all modulation connections negotiated.
slot	All ports on the specified slot. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7.
slot/*spe*	All ports on the specified slot and SPE. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7. SPE values range from 1 to 17. You must include the slash mark.
shelf/*slot*	All ports on the specified shelf and slot. For the Cisco AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11. You must include the slash mark.
shelf/*slot*/*spe*	All ports on the specified SPE. For the Cisco AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 0 to 53. You must include the slash marks.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5800.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.

Examples

The following is sample output from the **show spe modem high speed** command on the Cisco AS5400 with the NextPort DFC:

```
Router# show spe modem high speed 1/0

#SPE 1/0      :
 Modln       V.FC            V.34          K56Flex           V.90      Modln
 Speed    Tx     Rx       Tx     Rx       Tx     Rx       Tx     Rx    Speed
 56000  ------ ------   ------ ------   000000 ------   000000 ------  56000
 54667  ------ ------   ------ ------        -      -        0      -  54667
```

```
 54000  ------ ------   ------ ------        0      -        -      -  54000
 53333  ------ ------   ------ ------        -      -        0      -  53333
 52000  ------ ------   ------ ------        0      -        0      -  52000
 50667  ------ ------   ------ ------        -      -        0      -  50667
 50000  ------ ------   ------ ------        0      -        -      -  50000
 49333  ------ ------   ------ ------        -      -        0      -  49333
 48000  ------ ------   ------ ------        0      -        0      -  48000
 46667  ------ ------   ------ ------        -      -        0      -  46667
 46000  ------ ------   ------ ------        0      -        -      -  46000
 45333  ------ ------   ------ ------        -      -        0      -  45333
 44000  ------ ------   ------ ------        0      -        0      -  44000
 42667  ------ ------   ------ ------        -      -        0      -  42667
 42000  ------ ------   ------ ------        0      -        -      -  42000
 41333  ------ ------   ------ ------        -      -        0      -  41333
 40000  ------ ------   ------ ------        0      -        0      -  40000
 38667  ------ ------   ------ ------        -      -        0      -  48667
 38000  ------ ------   ------ ------        0      -        -      -  38000
 37333  ------ ------   ------ ------        -      -        0      -  37333
 36000  ------ ------   ------ ------        0      -        0      -  36000
 34667  ------ ------   ------ ------        -      -        0      -  34667
 34000  ------ ------   ------ ------        0      -        -      -  34000
 33600  ------ ------        0      0        -      -        -      0  33600
 33333  ------ ------        -      -        -      -        0      -  33333
 32000  ------ ------        -      -        0      -        0      -  32000
 31200  ------ ------        0      0        -      0        -      0  31200
 30667  ------ ------        -      -        -      -        0      -  30667
 29333  ------ ------        -      -        -      -        0      -  29333
 28800       0      0        0      0        -      0        -      0  28800
 28000       -      -        -      -        -      -        0      -  28000
 26400       0      0        0      0        -      0        -      0  26400
 24000       0      0        0      0        -      0        -      0  24000
 21600       0      0        0      0        -      0        -      0  21600
 19200       0      0        0      0        -      0        -      0  19200
 16800       0      0        0      0        -      0        -      0  16800
 14400       0      0        0      0        -      0        -      0  14400
 12000       -      -        0      0        -      0        -      0  12000
  9600       -      -        0      0        -      0        -      0   9600
  7200       -      -        0      0        -      0        -      0   7200
  4800       -      -        0      0        -      0        -      0   4800
  2400       -      -        0      0        -      -        -      -   2400
 TOTAL     0000000         0000000         0000000         0000000     TOTAL
#SPE 1/1      :
 Modln       V.FC            V.34          K56Flex           V.90       Modln
 Speed    Tx     Rx       Tx     Rx       Tx     Rx       Tx     Rx    Speed
 56000  ------ ------   ------ ------   000000 ------   000000 ------  56000
 54667  ------ ------   ------ ------        -      -        0      -  54667
 54000  ------ ------   ------ ------        0      -        -      -  54000
 53333  ------ ------   ------ ------        -      -        0      -  53333
 52000  ------ ------   ------ ------        0      -        0      -  52000
 50667  ------ ------   ------ ------        -      -        0      -  50667
 50000  ------ ------   ------ ------        0      -        -      -  50000
 49333  ------ ------   ------ ------        -      -        0      -  49333
 48000  ------ ------   ------ ------        0      -        0      -  48000
 46667  ------ ------   ------ ------        -      -        0      -  46667
 46000  ------ ------   ------ ------        0      -        -      -  46000
 45333  ------ ------   ------ ------        -      -        0      -  45333
 44000  ------ ------   ------ ------        0      -        0      -  44000
 42667  ------ ------   ------ ------        -      -        0      -  42667
 42000  ------ ------   ------ ------        0      -        -      -  42000
 41333  ------ ------   ------ ------        -      -        0      -  41333
 40000  ------ ------   ------ ------        0      -        0      -  40000
 38667  ------ ------   ------ ------        -      -        0      -  48667
 38000  ------ ------   ------ ------        0      -        -      -  38000
 37333  ------ ------   ------ ------        -      -        0      -  37333
```

```
 36000  ------ ------    ------ ------        0      -        0      -  36000
 34667  ------ ------    ------ ------        -      -        0      -  34667
 34000  ------ ------    ------ ------        0      -        -      -  34000
 33600  ------ ------         0      0        -      -        -      0  33600
 33333  ------ ------         -      -        -      -        0      -  33333
 32000  ------ ------         -      -        0      -        0      -  32000
 31200  ------ ------         0      0        -      0        -      0  31200
 30667  ------ ------         -      -        -      -        0      -  30667
 29333  ------ ------         -      -        -      -        0      -  29333
 28800       0      0         0      0        -      0        -      0  28800
 28000       -      -         -      -        -      -        0      -  28000
 26400       0      0         0      0        -      0        -      0  26400
 24000       0      0         0      0        -      0        -      0  24000
 21600       0      0         0      0        -      0        -      0  21600
 19200       0      0         0      0        -      0        -      0  19200
 16800       0      0         0      0        -      0        -      0  16800
 14400       0      0         0      0        -      0        -      0  14400
 12000       -      -         0      0        -      0        -      0  12000
  9600       -      -         0      0        -      0        -      0   9600
  7200       -      -         0      0        -      0        -      0   7200
  4800       -      -         0      0        -      0        -      0   4800
  2400       -      -         0      0        -      -        -      -   2400
 TOTAL     0000000          0000000          0000000          0000000     TOTAL
```

The following is sample output from the **show spe modem high speed** command on the Cisco AS5800 with universal port card:

```
Router# show spe modem high speed 1/8/1

    --  Indicates an invalid speed for a standard
#SPE 1/08/01   :
 Modln       V.FC          V.34           K56Flex          V.90       Modln
 Speed    Tx     Rx      Tx     Rx      Tx     Rx       Tx     Rx    Speed
 60000  ------ ------   ------ ------  000000 ------   ------ ------  60000
 58000  ------ ------   ------ ------       0 ------   ------ ------  58000
 56000  ------ ------   ------ ------       0      -        0      -  56000
 54667  ------ ------   ------ ------       -      -        0      -  54667
 54000  ------ ------   ------ ------       0      -        -      -  54000
 53333  ------ ------   ------ ------       -      -        0      -  53333
 52000  ------ ------   ------ ------       0      -        0      -  52000
 50667  ------ ------   ------ ------       -      -        0      -  50667
 50000  ------ ------   ------ ------       0      -        -      -  50000
 49333  ------ ------   ------ ------       -      -        0      -  49333
 48000  ------ ------   ------ ------       0      -        0      -  48000
 46667  ------ ------   ------ ------       -      -        0      -  46667
 46000  ------ ------   ------ ------       0      -        -      -  46000
 45333  ------ ------   ------ ------       -      -        0      -  45333
 44000  ------ ------   ------ ------       0      -        0      -  44000
 42667  ------ ------   ------ ------       -      -        0      -  42667
 42000  ------ ------   ------ ------       0      -        -      -  42000
 41333  ------ ------   ------ ------       -      -        0      -  41333
 40000  ------ ------   ------ ------       0      -        0      -  40000
 38667  ------ ------   ------ ------       -      -        0      -  38667
 38400  ------ ------   ------ ------       -      -        -      -  38400
 38000  ------ ------   ------ ------       0      -        -      -  38000
 37333  ------ ------   ------ ------       -      -        0      -  37333
 36000  ------ ------   ------ ------       0      -        0      -  36000
 34666  ------ ------   ------ ------       -      -        0      -  34666
 34000  ------ ------   ------ ------       0      -        -      -  34000
 33600  ------ ------         0      1       -      -        -      0  33600
 33333  ------ ------         -      -       -      -        0      -  33333
 32000  ------ ------         -      -       0      -        0      -  32000
 31200  ------ ------         6      1       -      0        -      0  31200
 30667  ------ ------         -      -       -      -        0      -  30667
```

```
 29333  ------ ------        -      -        -      -        0      -  29333
 28800       0      0        0      4        -      0        -      0  28800
 28000       -      -        -      -        -      -        0      -  28000
 26400       0      0        0      0        -      0        -      0  26400
 24000       0      0        0      0        -      0        -      0  24000
 21600       0      0        0      0        -      0        -      0  21600
 19200       0      0        0      0        -      0        -      0  19200
 16800       0      0        0      0        -      0        -      0  16800
 14400       0      0        0      0        -      0        -      0  14400
 12000       -      -        0      0        -      0        -      0  12000
  9600       -      -        0      0        -      0        -      0   9600
  7200       -      -        0      0        -      0        -      0   7200
  4800       -      -        0      0        -      0        -      0   4800
  2400       -      -        0      0        -      -        -      -   2400
 TOTAL     0000000          0000012          0000000          0000000
```

Table 125 describes the significant fields shown in the display.

Table 125 show spe modem high speed Field Descriptions

Field	Description
SPE	The slot and port number of the SPE.
Modln Speed	Modem line speed, in bits per second.
Tx	The number of sent calls that occurred at this speed.
Rx	The number of received calls that occurred at this speed.

Related Commands

Command	Description
show spe modem low speed	Displays the total number of connections within each low modulation or codec for the specified SPEs.

show spe modem high standard

To display the total number of connections within each high modulation or codec for a specific range of service processing element (SPE), use the **show spe modem high standard** command in EXEC mode.

Cisco AS5350 and Cisco AS5400 with the NextPort Dial Feature Card (DFC)

show spe modem high standard {**summary** | *slot* | *slot*/*spe*}

Cisco AS5800 with the Universal Port Card (UPC)

show spe modem high standard {**summary** | *shelf*/*slot* | *shelf*/*slot*/*spe*}

Syntax Description

summary	Displays a brief list of all modulation connections negotiated.
slot	All ports on the specified slot. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7.
slot/*spe*	All ports on the specified slot and SPE. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7. SPE values range from 1 to 17. You must include the slash mark.
shelf/*slot*	All ports on the specified shelf and slot. For the Cisco AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11. You must include the slash mark.
shelf/*slot*/*spe*	All ports on the specified SPE. For the Cisco AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 0 to 53. You must include the slash marks.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5800.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.

Examples

The following is sample output from the show spe modem high standard command on the Cisco AS5400 with the NextPort DFC. This example displays standard low-speed connections for SPEs in slot 5:

```
Router# show spe modem high standard 5

SPE/Mod->     V.FC     V.34  K56Flex     V.90
5/00             0        1        2        1
5/01             0        0        0        0
5/02             0        0        0        0
5/03             0        0        0        0
```

```
5/04              0        0        0        0
5/05              0        0        0        0
5/06              0        0        0        2
5/07              0        0        0        0
5/08              0        0        0        0
5/09              0        0        0        0
5/10              0        0        0        0
5/11              0        0        0        0
5/12              0        0        0        0
5/13              0        0        0        0
5/14              0        0        0        0
5/15              0        0        0        0
5/16              0        0        0        0
5/17              0        0        0        0
TOTAL      00000000 00000001 00000002 00000003
```

The following is sample output from the **show spe modem high standard** command on the Cisco AS5800 with the universal port card. This example displays standard low-speed connections for SPEs in slot 8:

```
Router# show spe modem high standard 1/8/1

SPE/Mod->     V.FC     V.34  K56Flex     V.90
1/08/01          0        6        0        0
TOTAL      00000000 00000006 00000000 00000000
```

Table 126 describes the significant fields shown in the display.

Table 126 show spe modem high standard Field Descriptions

Field	Description
SPE	The slot and port number of the SPE.
Mod	The modem type.

Related Commands

Command	Description
show spe modem low standard	Displays the total number of connections within each low modulation or codec for the SPE.

show spe modem low speed

To display the total number of connections within each low-speed modulation or codec for the specified service processing elements (SPEs), use the **show spe modem low speed** command in EXEC mode.

Cisco AS5350 and Cisco AS5400 with the NextPort Dial Feature Card (DFC)

show spe modem low speed {**summary** | {*slot* | *slot*/*spe*} [*slot* | *slot*/*spe*]}

Cisco AS5800 with the Universal Port Card (UPC)

show spe modem low speed {**summary** | {*shelf*/*slot* | *shelf*/*slot*/*spe*} [*shelf*/*slot* | *shelf*/*slot*/*spe*]}

Syntax Description

summary	Displays a brief list of all modulation connections negotiated.
slot	All ports on the specified slot. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7. A range of slots can be specified by entering a second value for the *slot* argument.
slot/*spe*	Ports on the specified slot and SPE. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7. SPE values range from 1 to 17. You must include the slash mark. A range of ports can be specified by entering a second value for the *slot*/*spe* argument.
shelf/*slot*	Ports on the specified shelf and slot. For the Cisco AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11. You must include the slash mark. A range of slots can be specified by entering a second value for the *shelf*/*slot* argument.
shelf/*slot*/*spe*	Ports on the specified SPE. For the Cisco AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 0 to 53. You must include the slash marks. A range of ports can be specified by entering a second value for the *shelf*/*slot*/*spe* argument.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5800.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.

Examples

The following is sample output from the **show spe modem low speed** command on the Cisco AS5400 with the NextPort DFC. This example displays standard low-speed connections:

```
Router# show spe modem low speed 1/0
```

```
#SPE 1/0    :                                <--     MODEM   FAX       -->
 Speed   B103   V.21   B212   V.22  V.22b   V.32  V.32b    V.27t   V.29   V.17
 14400 ------ ------ ------ ------ ------ ------     30   ------ ------      0
 12000 ------ ------ ------ ------ ------ ------      0   ------ ------      0
  9600 ------ ------ ------ ------ ------      0      0   ------      0      0
  7200 ------ ------ ------ ------ ------      -      0   ------      0      0
  4800 ------ ------ ------ ------ ------      0      0        0      0 ------
  2400 ------ ------ ------ ------      0 ------ ------        0 ------ ------
  1200 ------ ------      0      0      6 ------ ------   ------ ------ ------
   600 ------ ------ ------ ------ ------ ------ ------   ------ ------ ------
   300      0      0 ------ ------ ------ ------ ------   ------ ------ ------
 TOTAL 000000 000000 000000 000000 000006 000000 000030   000000 000000 000000
#SPE 1/1    :                                <--     MODEM   FAX       -->
 Speed   B103   V.21   B212   V.22  V.22b   V.32  V.32b    V.27t   V.29   V.17
 14400 ------ ------ ------ ------ ------ ------     30   ------ ------      0
 12000 ------ ------ ------ ------ ------ ------      0   ------ ------      0
  9600 ------ ------ ------ ------ ------      0      0   ------      0      0
  7200 ------ ------ ------ ------ ------      -      0   ------      0      0
  4800 ------ ------ ------ ------ ------      0      0        0      0 ------
  2400 ------ ------ ------ ------      0 ------ ------        0 ------ ------
  1200 ------ ------      0      0      6 ------ ------   ------ ------ ------
   600 ------ ------ ------ ------ ------ ------ ------   ------ ------ ------
   300      0      0 ------ ------ ------ ------ ------   ------ ------ ------
 TOTAL 000000 000000 000000 000000 000006 000000 000030   000000 000000 000000
```

The following is sample output from the **show spe modem low speed** command on the Cisco AS5800 with the universal port card. This example displays standard low-speed connections for SPEs in slot 8:

```
Router# show spe modem low speed 1/8/0 1/8/6

    --  Indicates an invalid speed for a standard
#SPE 1/08/00   :                          <--       MODEM   FAX       -->
 Speed   B103  V.21  B212  V.22 V.22b  V.23  V.32 V.32b   V.27t  V.29  V.17
 14400  ----- ----- ----- ----- ----- ----- -----     0   ----- -----     0
 12000  ----- ----- ----- ----- ----- ----- -----     0   ----- -----     0
  9600  ----- ----- ----- ----- ----- -----     0     0   -----     0     0
  7200  ----- ----- ----- ----- ----- -----     -     0   -----     0     0
  4800  ----- ----- ----- ----- ----- -----     0     0       0     0 -----
  2400  ----- ----- ----- -----     0 ----- ----- -----       0 ----- -----
  1200  ----- -----     0     0     0     0 ----- -----   ----- ----- -----
   300      0     0 ----- ----- ----- ----- ----- -----   ----- ----- -----
 TOTAL  00000 00000 00000 00000 00000 00000 00000 00000   00000 00000 00000
```

Table 127 describes the significant fields shown in the display.

Table 127 show spe modem low speed Field Descriptions

Field	Description
SPE	The slot and port number of the SPE.
Speed	The modem line speed, in bits per second.
MODEM	The modem type.
FAX	The fax type.

Related Commands

Command	Description
show spe modem high standard	Displays the total number of connections within each high modulation or codec for a specific range of SPEs.

show spe modem low standard

To display the total number of connections within each low modulation or codec for the specified service processing elements (SPEs), use the **show spe modem low standard** command in EXEC mode.

Cisco AS5350 and Cisco AS5400 with the NextPort Dial Feature Card (DFC)

show spe modem low standard {**summary** | *slot* | *slot*/*spe*}

Cisco AS5800 with the Universal Port Card (UPC)

show spe modem low standard {**summary** | *shelf*/*slot* | *shelf*/*slot*/*spe*}

Syntax Description

summary	Displays a brief list of all modulation connections negotiated.
slot	All ports on the specified slot. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7.
slot/*spe*	All ports on the specified slot and SPE. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7. SPE values range from 1 to 17. You must include the slash mark.
shelf/*slot*	All ports on the specified shelf and slot. For the Cisco AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11. You must include the slash mark.
shelf/*slot*/*spe*	All ports on the specified SPE. For the Cisco AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 0 to 53. You must include the slash marks.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5800.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.

Examples

The following example displays standard low-speed connections for SPEs in slot 5 on the Cisco AS5400:

```
Router# show spe modem low standard 5
                                                <--        MODEM   FAX       -->
SPE/Mod->  B103  V.21  B212  V.22 V.22b  V.23  V.32 V.32b   V.27t  V.29  V.17
5/00          0     0     0     0     0     0     0     0       0     0     0
5/01          0     0     0     0     0     0     0     0       0     0     0
5/02          0     0     0     0     0     0     0     0       0     0     0
5/03          0     0     0     0     0     0     0     0       0     0     0
5/04          0     0     0     0     0     0     0     0       0     0     0
```

```
5/05          0     0     0     0     0     0     0     0        0     0     0
5/06          0     0     0     0     0     0     0     0        0     0     0
5/07          0     0     0     0     0     0     0     0        0     0     0
5/08          0     0     0     0     0     0     0     0        0     0     0
5/09          0     0     0     0     0     0     0     0        0     0     0
5/10          0     0     0     0     0     0     0     0        0     0     0
5/11          0     0     0     0     0     0     0     0        0     0     0
5/12          0     0     0     0     0     0     0     0        0     0     0
5/13          0     0     0     0     0     0     0     0        0     0     0
5/14          0     0     0     0     0     0     0     0        0     0     0
5/15          0     0     0     0     0     0     0     0        0     0     0
5/16          0     0     0     0     0     0     0     0        0     0     0
5/17          0     0     0     0     0     0     0     0        0     0     0
TOTAL     00000 00000 00000 00000 00000 00000 00000 00000    00000 00000 00000
```

The following example displays standard low-speed connections for SPEs in slot 8 on the Cisco AS5800:

```
Router# show spe modem low standard 1/8
                                                <--        MODEM    FAX        -->
SPE/Mod->  B103  V.21  B212  V.22 V.22b  V.23  V.32 V.32b   V.27t  V.29  V.17
1/08/00       0     0     0     0     0     0     0     0        0     0     0
1/08/01       0     0     0     0     0     0     0     0        0     0     0
1/08/02       0     0     0     0     0     0     0     0        0     0     0
1/08/03       0     0     0     0     0     0     0     0        0     0     0
1/08/04       0     0     0     0     0     0     0     0        0     0     0
1/08/05       0     0     0     0     0     0     0     0        0     0     0
1/08/06       0     0     0     0     0     0     0     0        0     0     0
1/08/07       0     0     0     0     0     0     0     0        0     0     0
1/08/08       0     0     0     0     0     0     0     0        0     0     0
1/08/09       0     0     0     0     0     0     0     0        0     0     0
1/08/10       0     0     0     0     0     0     0     0        0     0     0
1/08/11       0     0     0     0     0     0     0     0        0     0     0
1/08/12       0     0     0     0     0     0     0     0        0     0     0
1/08/13       0     0     0     0     0     0     0     0        0     0     0
1/08/14       0     0     0     0     0     0     0     0        0     0     0
1/08/15       0     0     0     0     0     0     0     0        0     0     0
1/08/16       0     0     0     0     0     0     0     0        0     0     0
1/08/17       0     0     0     0     0     0     0     0        0     0     0
1/08/18       0     0     0     0     0     0     0     0        0     0     0
1/08/19       0     0     0     0     0     0     0     0        0     0     0
1/08/20       0     0     0     0     0     0     0     0        0     0     0
                                                <--        MODEM    FAX        -->
SPE/Mod->  B103  V.21  B212  V.22 V.22b  V.23  V.32 V.32b   V.27t  V.29  V.17
1/08/21       0     0     0     0     0     0     0     0        0     0     0
1/08/22       0     0     0     0     0     0     0     0        0     0     0
1/08/23       0     0     0     0     0     0     0     0        0     0     0
1/08/24       0     0     0     0     0     0     0     0        0     0     0
1/08/25       0     0     0     0     0     0     0     0        0     0     0
1/08/26       0     0     0     0     0     0     0     0        0     0     0
1/08/27       0     0     0     0     0     0     0     0        0     0     0
1/08/28       0     0     0     0     0     0     0     0        0     0     0
1/08/29       0     0     0     0     0     0     0     0        0     0     0
1/08/30       0     0     0     0     0     0     0     0        0     0     0
1/08/31       0     0     0     0     0     0     0     0        0     0     0
1/08/32       0     0     0     0     0     0     0     0        0     0     0
1/08/33       0     0     0     0     0     0     0     0        0     0     0
1/08/34       0     0     0     0     0     0     0     0        0     0     0
1/08/35       0     0     0     0     0     0     0     0        0     0     0
1/08/36       0     0     0     0     0     0     0     0        0     0     0
1/08/37       0     0     0     0     0     0     0     0        0     0     0
1/08/38       0     0     0     0     0     0     0     0        0     0     0
1/08/39       0     0     0     0     0     0     0     0        0     0     0
1/08/40       0     0     0     0     0     0     0     0        0     0     0
```

```
1/08/41        0      0      0      0      0      0      0      0        0      0      0
1/08/42        0      0      0      0      0      0      0      0        0      0      0
                                                <--         MODEM    FAX         -->
SPE/Mod->   B103   V.21   B212   V.22 V.22b   V.23   V.32 V.32b    V.27t   V.29   V.17
1/08/43        0      0      0      0      0      0      0      0        0      0      0
1/08/44        0      0      0      0      0      0      0      0        0      0      0
1/08/45        0      0      0      0      0      0      0      0        0      0      0
1/08/46        0      0      0      0      0      0      0      0        0      0      0
1/08/47        0      0      0      0      0      0      0      0        0      0      0
1/08/48        0      0      0      0      0      0      0      0        0      0      0
1/08/49        0      0      0      0      0      0      0      0        0      0      0
1/08/50        0      0      0      0      0      0      0      0        0      0      0
1/08/51        0      0      0      0      0      0      0      0        0      0      0
1/08/52        0      0      0      0      0      0      0      0        0      0      0
1/08/53        0      0      0      0      0      0      0      0        0      0      0
TOTAL      00000  00000  00000  00000  00000  00000  00000  00000    00000  00000  00000
```

Table 128 describes the significant fields shown in the displays.

Table 128 show spe modem low standard Field Descriptions

Field	Description
SPE	The slot and port number of the SPE.
MODEM	The modem type.
FAX	The fax type.

Related Commands

Command	Description
show spe modem high standard	Displays the total number of connections within each high modulation or codec for a specific range of SPE.

show spe modem summary

To display a summary of modem statistics for the specified service processing element (SPE) or range of SPEs, use the **show spe modem summary** command in EXEC mode.

Cisco AS5350 and Cisco AS5400 with the NextPort Dial Feature Card (DFC)

show spe modem summary [*slot* | *slot*/*spe*]

Cisco AS5800 with the Universal Port Card (UPC)

show spe modem summary [*shelf*/*slot* | *shelf*/*slot*/*spe*]

Syntax Description

slot	(Optional) All ports on the specified slot. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7.
slot/*spe*	(Optional) All ports on the specified slot and SPE. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7. SPE values range from 1 to 17. You must include the slash mark.
shelf/*slot*	(Optional) All ports on the specified shelf and slot. For the Cisco AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11. You must include the slash mark.
shelf/*slot*/*spe*	(Optional) All ports on the specified SPE. For the Cisco AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 0 to 53. You must include the slash marks.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5800.
12.1(5)XM1	This command was introduced on the Cisco AS5350.
12.2(2)XA	Disconnection reasons and states information were added.
12.2(2)XB	This command was integrated into Cisco IOS Release 12.2(2)XB.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.

Examples

The following is sample output from the **show spe modem summary** command on the Cisco AS5400:

```
Router# show spe modem summary

Async1/00 - 5/107, TTY216 - 755
     786 incoming completes          4 incoming failures
       0 outgoing completes          0 outgoing failures
       0 failed dial attempts        0 ring no answers          0 autotests
```

```
       0 no carriers                0 dial timeouts            0 autotest fails
       0 no dial tones              0 link failures            0 fail count
       0 watchdog timeouts          0 protocol errors          0 recovers

Transmit Speed Counters       :
 Speed    Calls  Speed    Calls  Speed    Calls  Speed    Calls  Speed    Calls
 60000        0  48000        0  38400        0  30666        0  12000        0
 58000        0  46666        0  38000        0  29333        0   9600        0
 56000        0  46000        0  37333        0  28800       10   7200        0
 54666        0  45333        0  36000        0  28000        0   4800        0
 54000        0  44000        0  34666        0  26400        0   2400        0
 53333        0  42666        0  34000        0  24000        0   1200        0
 52000        0  42000        0  33600      631  21600        0    300        0
 50666        0  41333        0  33333        0  19200        0
 50000        0  40000        0  32000        0  16800        0
 49333        0  38666        0  31200      145  14400        0

Receive Speed Counters        :
 Speed    Calls  Speed    Calls  Speed    Calls  Speed    Calls  Speed    Calls
 38400        0  26400        0  16800        0   7200        0    300        0
 33600      786  24000        0  14400        0   4800        0
 31200        0  21600        0  12000        0   2400        0
 28800        0  19200        0   9600        0   1200        0
```

The following is sample output from the **show spe modem summary** command on the Cisco AS5800:

```
Router# show spe modem summary

Async1/2/00 - 1/3/323, TTY972 - 1619
     4827 incoming completes        284 incoming failures
        0 outgoing completes          0 outgoing failures
        0 failed dial attempts        0 ring no answers          0 autotests
        0 no carriers                11 dial timeouts           0 autotest fails
        0 no dial tones               0 link failures            0 fail count
        0 watchdog timeouts        2787 protocol errors          0 recovers
Transmit Speed Counters
  Speed    Calls  Speed    Calls  Speed    Calls  Speed    Calls  Speed Calls
  60000        0  48000      432  38400        0  30666        0  12000 143
  58000        0  46666        0  38000        4  29333        0   9600 5
  56000       15  46000       56  37333      111  28800      700   7200 11
  54666        0  45333      299  36000       84  28000        5   4800 2
  54000        0  44000      227  34666        0  26400      267   2400 0
  53333      123  42666        0  34000       39  24000       46   1200 3
  52000      563  42000       68  33600      323  21600       27    300 0
  50666        0  41333       38  33333        9  19200       38
  50000       59  40000       65  32000       20  16800       12
  49333      371  38666        0  31200      654  14400        5

Receive Speed Counters
  Speed    Calls  Speed    Calls  Speed    Calls  Speed    Calls  Speed Calls
  38400        0  26400     2286  16800       11   7200        1    300 2
  33600      113  24000      267  14400      139   4800        1
  31200      216  21600       56  12000        4   2400        3
  28800     1665  19200       47   9600       16   1200        0
```

Table 129 describes the significant fields shown in the display.

Table 129 show spe modem summary Field Descriptions

Field	Description
Summary of modem and SPE events follows:	
incoming completes and failures	Total number of incoming connection requests that the SPE answered and successfully or unsuccessfully connected with the remote DCE device.
outgoing completes and failures	Total number of outgoing connection requests that the SPE dialed and successfully or unsuccessfully connected with the remote DCE device.
failed dial attempts	Number of times the SPE attempted to dial out but the call failed to leave the modem.
ring no answers	Number of times the SPE rang but did not answer the call.
autotests	Number of times an autotest was run on the SPE.
no carriers	Number of times the SPE disconnected because no carrier was present.
dial timeouts	Number of times the SPE timed out while attempting to dial.
autotest fails	Number of times the SPE failed an autotest.
no dial tones	Number of times the dial-out attempt failed because the SPE failed to detect a dial tone.
link failures	Number of times the SPE detected a link failure.
fail count	Number of times the SPE failed.
watchdog timeouts	Number of times the SPE internal watchdog timer expired.
protocol errors	Number of times the SPE protocol failed to make a call connection.
recovers	Number of times the SPE recovered.
Transmit Speed Counters	List of connection speeds that were sent by the SPE.
Receive Speed Counters	List of connection speeds that were received by the SPE.
Transmit Speed Counters	List of connection speeds that were sent by the SPE.
Receive Speed Counters	List of connection speeds that were received by the SPE.

Related Commands

Command	Description
show port operational-status	Displays the operational status of a specific port or range of ports.
show spe	Displays history statistics of all SPEs, a specified SPE, or the specified range of SPEs.
show spe digital	Displays history statistics of all digital SPEs, in summary form or for SPEs starting with a specified slot or a specified shelf/slot/range of SPEs.
show spe modem disconnect-reason	Displays all modem disconnection reasons for the specified SPE or range of SPEs.

show spe recovery

To display service processing element (SPE) recovery statistics, use the **show spe recovery** command in EXEC mode.

Cisco AS5350 and Cisco AS5400 with the NextPort Dial Feature Card (DFC)

show spe recovery [*slot* | *slot*/*spe*]

Cisco AS5800 with the Universal Port Card (UPC)

show spe recovery [*shelf*/*slot* | *shelf*/*slot*/*spe*]

Syntax Description

slot	(Optional) All ports on the specified slot. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7.
slot/*spe*	(Optional) All ports on the specified slot and SPE. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7. SPE values range from 1 to 17. You must include the slash mark.
shelf/*slot*	(Optional) All ports on the specified shelf and slot. For the Cisco AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11. You must include the slash mark.
shelf/*slot*/*spe*	(Optional) All ports on the specified SPE. For the Cisco AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 0 to 53. You must include the slash marks.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5800.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.

Usage Guidelines

Use this command to display a list of recovered SPEs.

Examples

The following is sample output from the **show spe recovery** command on the Cisco AS5400:

```
Router# show spe recovery

SPE#      Session Abort   Session NAK   Call Failure
1/00                  0             0              0
1/01                  0             0              0
1/02                  0             0              0
1/03                  0             0              0
```

```
1/04                    0               0               0
1/05                    0               0               0
1/06                    0               0               0
1/07                    0               0               0
1/08                    0               0               0
1/09                    0               0               0
1/10                    0               0               0
1/11                    0               0               0
1/12                    0               0               0
1/13                    0               0               0
1/14                    0               0               0
1/15                    0               0               0
1/16                    0               0               0
1/17                    0               0               0
```

The following is sample output from the **show spe recovery** command on the Cisco AS5800:

```
Router# show spe recovery 1/8

SPE#       Session Abort   Session NAK   Call Failure
1/08/00                 0             0              0
1/08/01                 0             0              0
1/08/02                 0             0              0
1/08/03                 0             0              0
1/08/04                 0             0              0
1/08/05                 0             0              0
1/08/06                 0             0              0
1/08/07                 0             0              0
1/08/08                 0             0              0
1/08/09                 0             0              0
1/08/10                 0             0              0
1/08/11                 0             0              0
1/08/12                 0             0              0
1/08/13                 0             0              0
1/08/14                 0             0              0
1/08/15                 0             0              0
1/08/16                 0             0              0
1/08/17                 0             0              0
1/08/18                 0             0              0
1/08/19                 0             0              0
1/08/20                 0             0              0
1/08/21                 0             0              0
1/08/22                 0             0              0
1/08/23                 0             0              0
1/08/24                 0             0              0
1/08/25                 0             0              0
1/08/26                 0             0              0
1/08/27                 0             0              0
1/08/28                 0             0              0
1/08/29                 0             0              0
1/08/30                 0             0              0
1/08/31                 0             0              0
1/08/32                 0             0              0
1/08/33                 0             0              0
1/08/34                 0             0              0
1/08/35                 0             0              0
1/08/36                 0             0              0
1/08/37                 0             0              0
1/08/38                 0             0              0
1/08/39                 0             0              0
1/08/40                 0             0              0
1/08/41                 0             0              0
1/08/42                 0             0              0
1/08/43                 0             0              0
```

```
1/08/44          0          0          0
1/08/45          0          0          0
1/08/46          0          0          0
1/08/47          0          0          0
1/08/48          0          0          0
1/08/49          0          0          0
1/08/50          0          0          0
1/08/51          0          0          0
1/08/52          0          0          0
1/08/53          0          0          0
```

Related Commands

Command	Description
show spe	Displays SPE status.

show spe version

To display the firmware version on a service processing element (SPE), use the **show spe version** command in EXEC mode.

Cisco AS5350 and Cisco AS5400 with the NextPort Dial Feature Card (DFC)

show spe version [*slot* | *slot*/*spe*] [*slot* | *slot*/*spe*]

Cisco AS5800 with the Universal Port Card (UPC)

show spe version [*shelf*/*slot* | *shelf*/*slot*/*spe*] [*shelf*/*slot* | *shelf*/*slot*/*spe*]

Syntax Description

slot	(Optional) All ports on the specified slot. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7. A range of slots can be specified by entering a second value for the *slot* argument.
slot/*spe*	(Optional) All ports on the specified slot and SPE. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7. SPE values range from 1 to 17. You must include the slash mark. A range of ports can be specified by entering a second value for the *slot*/*spe* argument.
shelf/*slot*	(Optional) All ports on the specified shelf and slot. For the Cisco AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11. You must include the slash mark. A range of slots can be specified by entering a second value for the *shelf*/*slot* argument.
shelf/*slot*/*spe*	(Optional) All ports on the specified SPE. For the Cisco AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 0 to 53. You must include the slash marks. A range of ports can be specified by entering a second value for the *shelf*/*slot*/*spe* argument.

Command Modes

EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.1(1)XD	This command was implemented on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5800.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.

Usage Guidelines

Use the **show spe version** command to display the firmware version running on a specific SPE. If the *shelf*/*slot*/*spe* argument is specified, the firmware version for the identified SPE or range of SPEs is displayed. If the *slot* argument is specified, the firmware version for the identified SPEs in this slot or range of slots is displayed. If no argument is specified, all SPE versions are displayed.

The **show spe version** command also displays the version to firmware file mappings.

The **show spe version** command is similar to the **show modem mapping** MICA technologies modem command.

Examples

The following is sample output from the **show spe version** command on a Cisco AS5400:

```
Router# show spe version

IOS-Bundled Default Firmware-Filename              Version  Firmware-Type
===================================               =======  =============
system:/ucode/np_spe_firmware1                    0.6.5.5  SPE firmware
                                                  0.0.0.0  Portware

On-Flash Firmware-Filename                        Version  Firmware-Type
==========================                        =======  =============
flash:np.spe                                      0.6.4.5  SPE firmware

  SPE-# SPE-Type   SPE-Port-Range     Version    UPG Firmware-Filename
   4/00    CSMV6         0000-0005     0.6.5.5    N/A np.spe
   4/01    CSMV6         0006-0011     0.6.5.5    N/A ios-bundled default
   4/02    CSMV6         0012-0017     0.6.5.5    N/A ios-bundled default
   4/03    CSMV6         0018-0023     0.6.5.5    N/A ios-bundled default
   4/04    CSMV6         0024-0029     0.6.5.5    N/A ios-bundled default
   4/05    CSMV6         0030-0035     0.6.5.5    N/A ios-bundled default
   4/06    CSMV6         0036-0041     0.6.5.5    N/A ios-bundled default
   4/07    CSMV6         0042-0047     0.6.5.5    N/A ios-bundled default
   4/08    CSMV6         0048-0053     0.6.5.5    N/A ios-bundled default
   4/09    CSMV6         0054-0059     0.6.5.5    N/A ios-bundled default
   4/10    CSMV6         0060-0065     0.6.5.5    N/A ios-bundled default
   4/11    CSMV6         0066-0071     0.6.5.5    N/A ios-bundled default
   4/12    CSMV6         0072-0077     0.6.5.5    N/A ios-bundled default
   4/13    CSMV6         0078-0083     0.6.5.5    N/A ios-bundled default
   4/14    CSMV6         0084-0089     0.6.5.5    N/A ios-bundled default
   4/15    CSMV6         0090-0095     0.6.5.5    N/A ios-bundled default
   4/16    CSMV6         0096-0101     0.6.5.5    N/A ios-bundled default
   4/17    CSMV6         0102-0107     0.6.5.5    N/A ios-bundled default
```

The following is sample output from the **show spe version** command on a Cisco AS5800:

```
Router# show spe version 1/8

IOS-Bundled Default Firmware-Filename              Version  Firmware-Type
===================================               =======  =============
system:/ucode/np_spe_firmware1                    0.0.6.81 SPE firmware
system:/ucode/mica_board_firmware                 2.7.2.0  Mica Portware

On-Flash Firmware-Filename                        Version  Firmware-Type
==========================                        =======  =============
slot0:np_6_81.spe                                 0.0.6.81 SPE firmware
slot0:np_6_80.spe                                 0.0.6.80 SPE firmware
slot0:mica-modem-pw.2.7.1.1.bin                   2.7.1.0  Mica Portware
slot0:mica-modem-pw.2.7.2.0.bin                   2.7.2.0  Mica Portware

  SPE-# SPE-Type   SPE-Port-Range     Version    UPG Firmware-Filename
1/08/00    CSMV6         0000-0005    0.0.6.81    N/A ios-bundled default
1/08/01    CSMV6         0006-0011    0.0.6.81    N/A ios-bundled default
1/08/02    CSMV6         0012-0017    0.0.6.81    N/A ios-bundled default
1/08/03    CSMV6         0018-0023    0.0.6.81    N/A ios-bundled default
1/08/04    CSMV6         0024-0029    0.0.6.81    N/A ios-bundled default
1/08/05    CSMV6         0030-0035    0.0.6.81    N/A ios-bundled default
1/08/06    CSMV6         0036-0041    0.0.6.81    N/A ios-bundled default
1/08/07    CSMV6         0042-0047    0.0.6.81    N/A ios-bundled default
1/08/08    CSMV6         0048-0053    0.0.6.81    N/A ios-bundled default
```

```
1/08/09    CSMV6        0054-0059    0.0.6.81    N/A ios-bundled default
1/08/10    CSMV6        0060-0065    0.0.6.81    N/A ios-bundled default
1/08/11    CSMV6        0066-0071    0.0.6.81    N/A ios-bundled default
1/08/12    CSMV6        0072-0077    0.0.6.81    N/A ios-bundled default
1/08/13    CSMV6        0078-0083    0.0.6.81    N/A ios-bundled default
1/08/14    CSMV6        0084-0089    0.0.6.81    N/A ios-bundled default
1/08/15    CSMV6        0090-0095    0.0.6.81    N/A ios-bundled default
1/08/16    CSMV6        0096-0101    0.0.6.81    N/A ios-bundled default
1/08/17    CSMV6        0102-0107    0.0.6.81    N/A ios-bundled default
1/08/18    CSMV6        0108-0113    0.0.6.81    N/A ios-bundled default
1/08/19    CSMV6        0114-0119    0.0.6.81    N/A ios-bundled default
1/08/20    CSMV6        0120-0125    0.0.6.81    N/A ios-bundled default
1/08/21    CSMV6        0126-0131    0.0.6.81    N/A ios-bundled default
1/08/22    CSMV6        0132-0137    0.0.6.81    N/A ios-bundled default
1/08/23    CSMV6        0138-0143    0.0.6.81    N/A ios-bundled default
1/08/24    CSMV6        0144-0149    0.0.6.81    N/A ios-bundled default
1/08/25    CSMV6        0150-0155    0.0.6.81    N/A ios-bundled default
1/08/26    CSMV6        0156-0161    0.0.6.81    N/A ios-bundled default
1/08/27    CSMV6        0162-0167    0.0.6.81    N/A ios-bundled default
1/08/28    CSMV6        0168-0173    0.0.6.81    N/A ios-bundled default
1/08/29    CSMV6        0174-0179    0.0.6.81    N/A ios-bundled default
1/08/30    CSMV6        0180-0185    0.0.6.81    N/A ios-bundled default
1/08/31    CSMV6        0186-0191    0.0.6.81    N/A ios-bundled default
1/08/32    CSMV6        0192-0197    0.0.6.81    N/A ios-bundled default
1/08/33    CSMV6        0198-0203    0.0.6.81    N/A ios-bundled default
1/08/34    CSMV6        0204-0209    0.0.6.81    N/A ios-bundled default
1/08/35    CSMV6        0210-0215    0.0.6.81    N/A ios-bundled default
1/08/36    CSMV6        0216-0221    0.0.6.81    N/A ios-bundled default
1/08/37    CSMV6        0222-0227    0.0.6.81    N/A ios-bundled default
1/08/38    CSMV6        0228-0233    0.0.6.81    N/A ios-bundled default
1/08/39    CSMV6        0234-0239    0.0.6.81    N/A ios-bundled default
1/08/40    CSMV6        0240-0245    0.0.6.81    N/A ios-bundled default
1/08/41    CSMV6        0246-0251    0.0.6.81    N/A ios-bundled default
1/08/42    CSMV6        0252-0257    0.0.6.81    N/A ios-bundled default
1/08/43    CSMV6        0258-0263    0.0.6.81    N/A ios-bundled default
1/08/44    CSMV6        0264-0269    0.0.6.81    N/A ios-bundled default
1/08/45    CSMV6        0270-0275    0.0.6.81    N/A ios-bundled default
1/08/46    CSMV6        0276-0281    0.0.6.81    N/A ios-bundled default
1/08/47    CSMV6        0282-0287    0.0.6.81    N/A ios-bundled default
1/08/48    CSMV6        0288-0293    0.0.6.81    N/A ios-bundled default
1/08/49    CSMV6        0294-0299    0.0.6.81    N/A ios-bundled default
1/08/50    CSMV6        0300-0305    0.0.6.81    N/A ios-bundled default
1/08/51    CSMV6        0306-0311    0.0.6.81    N/A ios-bundled default
1/08/52    CSMV6        0312-0317    0.0.6.81    N/A ios-bundled default
1/08/53    CSMV6        0318-0323    0.0.6.81    N/A ios-bundled default
```

The following examples show various implementations of the **show spe version** command to display information about the available SPE sources and modem resources:

```
Router# show spe version

IOS-Bundled Default Firmware-Filename             Version  Firmware-Type
 ====================================              =======  =============
 system:/ucode/mica_board_firmware                 2.0.2.0  Mica Boardware
 system:/ucode/mica_port_firmware                  2.6.2.0  Mica Portware
 system:/ucode/microcom_firmware                   5.1.20   Microcom F/W and DSP

 On-Flash Firmware-Filename                        Version  Firmware-Type
 ==========================                        =======  =============
 flash:portware.2620.ios                           2.6.2.0  Mica Portware
 flash:mcom-modem-firmware.3.1.30.bin              3.1.30   Microcom Firmware
 flash:mcom-fw-dsp.5.1.9_47.22.bin                 5.1.9    Microcom F/W and DSP
 flash:R0620.ios                                   0.6.2.0  Mica Portware
```

```
 flash:pw2710.ios                                        2.7.1.0  Mica Portware
 flash:mica-modem-pw_2_7_1_0.bin                         2.7.1.0  Mica Portware

 SPE-# SPE-Type   SPE-Range     Version    Upgrade Firmware-Filename
 1/0   MICA-HMM   1/0   - 1/5   2.7.1.0    N/A     flash:mica-modem-pw_2_7_1_0.bin
 1/1   MICA-HMM   1/6   - 1/11  2.7.1.0    N/A     flash:mica-modem-pw_2_7_1_0.bin
 1/2   MICA-HMM   1/12  - 1/17  2.7.1.0    N/A     flash:mica-modem-pw_2_7_1_0.bin
 1/3   MICA-HMM   1/18  - 1/23  2.7.1.0    N/A     flash:mica-modem-pw_2_7_1_0.bin
 1/5   MICA-HMM   1/30  - 1/35  2.7.1.0    N/A     system:/ucode/mica_port_firmware
 1/6   MICA-HMM   1/36  - 1/41  2.7.1.0    N/A     system:/ucode/mica_port_firmware
 1/7   MICA-HMM   1/42  - 1/47  2.7.1.0    N/A     system:/ucode/mica_port_firmware
 1/9   MICA-HMM   1/54  - 1/59  2.7.1.0    N/A     flash:/pw2710.ios

 2/0   MCOM-V90   2/0           5.1(20)    N/A     system:/ucode/microcom_firmware
 2/1   MCOM-V90   2/1           5.1(20)    N/A     system:/ucode/microcom_firmware
 2/2   MCOM-V90   2/2           5.1(20)    N/A     system:/ucode/microcom_firmware
 2/3   MCOM-V90   2/3           5.1(20)    N/A     system:/ucode/microcom_firmware
 2/4   MCOM-V90   2/4           5.1(9)     N/A     flash:/mcom-fw-dsp.5.1.9_47.22.bin
 2/5   MCOM-V90   2/5           5.1(9)     N/A     flash:/mcom-fw-dsp.5.1.9_47.22.bin
 2/6   MCOM-V90   2/6           5.1(9)     N/A     flash:/mcom-fw-dsp.5.1.9_47.22.bin
 2/7   MCOM-V90   2/7           5.1(9)     N/A     flash:/mcom-fw-dsp.5.1.9_47.22.bin
 2/8   MCOM-V90   2/8           5.1(9)     N/A     flash:/mcom-fw-dsp.5.1.9_47.22.bin
 2/9   MCOM-V90   2/9           5.1(9)     N/A     flash:/mcom-fw-dsp.5.1.9_47.22.bin
 2/10  MCOM-V90   2/10          5.1(9)     N/A     flash:/mcom-fw-dsp.5.1.9_47.22.bin
 2/11  MCOM-V90   2/11          5.1(9)     N/A     flash:/mcom-fw-dsp.5.1.9_47.22.bin
 2/12  MCOM-V34   2/12          2.3(6)     N/A     feature_card_flash
 2/13  MCOM-V34   2/13          2.3(6)     N/A     feature_card_flash
 2/14  MCOM-V34   2/14          2.3(6)     N/A     feature_card_flash
 2/15  MCOM-V34   2/15          2.3(6)     N/A     feature_card_flash
 2/16  MCOM-V34   2/16          2.3(6)     N/A     feature_card_flash
 2/17  MCOM-V34   2/17          2.3(6)     N/A     feature_card_flash
 2/18  MCOM-V34   2/18          2.3(6)     N/A     feature_card_flash
 2/19  MCOM-V34   2/19          2.3(6)     N/A     feature_card_flash
 2/20  MCOM-V34   2/20          2.3(6)     N/A     feature_card_flash
 2/21  MCOM-V34   2/21          2.3(6)     N/A     feature_card_flash
 2/22  MCOM-V34   2/22          2.3(6)     N/A     feature_card_flash
 2/23  MCOM-V34   2/23          2.3(6)     N/A     feature_card_flash

Router# show spe version 1

 SPE-# SPE-Type   SPE-Range     Version    Upgrade Firmware-Filename
 1/0   MICA-HMM   1/0   - 1/5   2.7.1.0    N/A     flash:mica-modem-pw_2_7_1_0.bin
 1/1   MICA-HMM   1/6   - 1/11  2.7.1.0    N/A     flash:mica-modem-pw_2_7_1_0.bin
 1/2   MICA-HMM   1/12  - 1/17  2.7.1.0    N/A     flash:mica-modem-pw_2_7_1_0.bin
 1/3   MICA-HMM   1/18  - 1/23  2.7.1.0    N/A     flash:mica-modem-pw_2_7_1_0.bin
 1/5   MICA-HMM   1/30  - 1/35  2.7.1.0    N/A     system:/ucode/mica_port_firmware
 1/6   MICA-HMM   1/36  - 1/41  2.7.1.0    N/A     system:/ucode/mica_port_firmware
 1/7   MICA-HMM   1/42  - 1/47  2.7.1.0    N/A     system:/ucode/mica_port_firmware
 1/9   MICA-HMM   1/54  - 1/59  2.7.1.0    N/A     flash:/pw2710.ios

Router# show spe version 1/2

 SPE-# SPE-Type   SPE-Range     Version    Upgrade Firmware-Filename
 1/2   MICA-HMM   1/12  - 1/17  2.7.1.0    N/A     flash:mica-modem-pw_2_7_1_0.bin
```

The following two examples show implementation of the **show spe version** command to display information about a range of SPEs:

```
Router# show spe version 1/2 2

 SPE-# SPE-Type   SPE-Range     Version    Upgrade Firmware-Filename
 1/2   MICA-HMM   1/12  - 1/17  2.7.1.0    N/A     flash:mica-modem-pw_2_7_1_0.bin
 1/3   MICA-HMM   1/18  - 1/23  2.7.1.0    N/A     flash:mica-modem-pw_2_7_1_0.bin
```

```
 1/5   MICA-HMM   1/30  - 1/35  2.7.1.0    N/A     system:/ucode/mica_port_firmware
 1/6   MICA-HMM   1/36  - 1/41  2.7.1.0    N/A     system:/ucode/mica_port_firmware
 1/7   MICA-HMM   1/42  - 1/47  2.7.1.0    N/A     system:/ucode/mica_port_firmware
 1/9   MICA-HMM   1/54  - 1/59  2.7.1.0    N/A     flash:/pw2710.ios
 2/0   MCOM-V90   2/0           5.1(20)    N/A     system:/ucode/microcom_firmware
 2/1   MCOM-V90   2/1           5.1(20)    N/A     system:/ucode/microcom_firmware
 2/2   MCOM-V90   2/2           5.1(20)    N/A     system:/ucode/microcom_firmware
 2/3   MCOM-V90   2/3           5.1(20)    N/A     system:/ucode/microcom_firmware
 2/4   MCOM-V90   2/4           5.1(9)     N/A     flash:/mcom-fw-dsp.5.1.9_47.22.bin
 2/5   MCOM-V90   2/5           5.1(9)     N/A     flash:/mcom-fw-dsp.5.1.9_47.22.bin
 2/6   MCOM-V90   2/6           5.1(9)     N/A     flash:/mcom-fw-dsp.5.1.9_47.22.bin
 2/7   MCOM-V90   2/7           5.1(9)     N/A     flash:/mcom-fw-dsp.5.1.9_47.22.bin
 2/8   MCOM-V90   2/8           5.1(9)     N/A     flash:/mcom-fw-dsp.5.1.9_47.22.bin
 2/9   MCOM-V90   2/9           5.1(9)     N/A     flash:/mcom-fw-dsp.5.1.9_47.22.bin
 2/10  MCOM-V90   2/10          5.1(9)     N/A     flash:/mcom-fw-dsp.5.1.9_47.22.bin
 2/11  MCOM-V90   2/11          5.1(9)     N/A     flash:/mcom-fw-dsp.5.1.9_47.22.bin
 2/12  MCOM-V34   2/12          2.3(6)     N/A     feature_card_flash
 2/13  MCOM-V34   2/13          2.3(6)     N/A     feature_card_flash
 2/14  MCOM-V34   2/14          2.3(6)     N/A     feature_card_flash
 2/15  MCOM-V34   2/15          2.3(6)     N/A     feature_card_flash
 2/16  MCOM-V34   2/16          2.3(6)     N/A     feature_card_flash
 2/17  MCOM-V34   2/17          2.3(6)     N/A     feature_card_flash
 2/18  MCOM-V34   2/18          2.3(6)     N/A     feature_card_flash
 2/19  MCOM-V34   2/19          2.3(6)     N/A     feature_card_flash
 2/20  MCOM-V34   2/20          2.3(6)     N/A     feature_card_flash
 2/21  MCOM-V34   2/21          2.3(6)     N/A     feature_card_flash
 2/22  MCOM-V34   2/22          2.3(6)     N/A     feature_card_flash
 2/23  MCOM-V34   2/23          2.3(6)     N/A     feature_card_flash
```

```
Router# show spe version 1/2 2/6

 SPE-# SPE-Type   SPE-Range     Version    Upgrade Firmware-Filename
 1/2   MICA-HMM   1/12  - 1/17  2.7.1.0    N/A     flash:mica-modem-pw_2_7_1_0.bin
 1/3   MICA-HMM   1/18  - 1/23  2.7.1.0    N/A     flash:mica-modem-pw_2_7_1_0.bin
 1/5   MICA-HMM   1/30  - 1/35  2.7.1.0    N/A     system:/ucode/mica_port_firmware
 1/6   MICA-HMM   1/36  - 1/41  2.7.1.0    N/A     system:/ucode/mica_port_firmware
 1/7   MICA-HMM   1/42  - 1/47  2.7.1.0    N/A     system:/ucode/mica_port_firmware
 1/9   MICA-HMM   1/54  - 1/59  2.7.1.0    N/A     flash:/pw2710.ios
 2/0   MCOM-V90   2/0           5.1(20)    N/A     system:/ucode/microcom_firmware
 2/1   MCOM-V90   2/1           5.1(20)    N/A     system:/ucode/microcom_firmware
 2/2   MCOM-V90   2/2           5.1(20)    N/A     system:/ucode/microcom_firmware
 2/3   MCOM-V90   2/3           5.1(20)    N/A     system:/ucode/microcom_firmware
 2/4   MCOM-V90   2/4           5.1(9)     N/A     flash:/mcom-fw-dsp.5.1.9_47.22.bin
 2/5   MCOM-V90   2/5           5.1(9)     N/A     flash:/mcom-fw-dsp.5.1.9_47.22.bin
 2/6   MCOM-V90   2/6           5.1(9)     N/A     flash:/mcom-fw-dsp.5.1.9_47.22.bin
```

```
Router# show spe version

IOS-Bundled Default Firmware-Filename              Version  Firmware-Type
====================================              =======  =============
system:/ucode/mica_board_firmware                 2.0.2.0  Mica Boardware
system:/ucode/mica_port_firmware                  2.6.2.0  Mica Portware
system:/ucode/microcom_firmware                   5.1.20   Microcom F/W and DSP

On-Flash Firmware-Filename                        Version  Firmware-Type
==========================                        =======  =============
flash:portware.2620.ios                           2.6.2.0  Mica Portware
flash:mcom-modem-firmware.3.1.30.bin              3.1.30   Microcom Firmware
flash:mcom-fw-dsp.5.1.9_47.22.bin                 5.1.9    Microcom F/W and DSP
flash:R0620.ios                                   0.6.2.0  Mica Portware
flash:pw2710.ios                                  2.7.1.0  Mica Portware
flash:mica-modem-pw_2_7_1_0.bin                   2.7.1.0  Mica Portware
```

```
SPE-# SPE-Type   SPE-Range     Version    Upgrade Firmware-Filename
1/0   MICA-HMM   1/0   - 1/5   2.7.1.0    N/A     flash:mica-modem-pw_2_7_1_0.bin
1/1   MICA-HMM   1/6   - 1/11  2.7.1.0    N/A     flash:mica-modem-pw_2_7_1_0.bin
1/2   MICA-HMM   1/12  - 1/17  2.7.1.0    N/A     flash:mica-modem-pw_2_7_1_0.bin
1/3   MICA-HMM   1/18  - 1/23  2.7.1.0    N/A     flash:mica-modem-pw_2_7_1_0.bin
```

For the Cisco AS5800, the **show spe version** command display will be different. Note that the SPE-Port-Range field indicates the shelf/slot/port of the SPE.

```
Router# show spe version

Firmware-Filename                              Version  Firmware-Type
=================                              =======  =============
IOS-Bundled Default                            2.6.2.0  Mica Portware
slot0:/pw2710.ios                              2.7.1.0  Mica Portware
slot0:/pw3102.ios                              3.1.0.2  Mica Portware
slot0:/pw3101.ios                              3.1.0.1  Mica Portware

SPE-# SPE-Type   SPE-Port-Range    Version    Upgrade Firmware-Filename
3/0   MICA-DMM   1/3/00 - 1/3/11   2.7.1.0    N/A     slot0:/pw2710.ios
3/1   MICA-DMM   1/3/12 - 1/3/23   2.7.1.0    N/A     slot0:/pw2710.ios
3/2   MICA-DMM   1/3/24 - 1/3/35   2.7.1.0    N/A     slot0:/pw2710.ios
3/3   MICA-DMM   1/3/36 - 1/3/47   2.7.1.0    N/A     slot0:/pw2710.ios
3/4   MICA-DMM   1/3/48 - 1/3/59   2.7.1.0    N/A     slot0:/pw2710.ios
3/5   MICA-DMM   1/3/60 - 1/3/71   2.7.1.0    N/A     slot0:/pw2710.ios
3/6   MICA-DMM   1/3/72 - 1/3/83   2.7.1.0    N/A     slot0:/pw2710.ios
3/7   MICA-DMM   1/3/84 - 1/3/95   2.7.1.0    N/A     slot0:/pw2710.ios
3/8   MICA-DMM   1/3/96 - 1/3/107  2.7.1.0    N/A     slot0:/pw2710.ios
```

Table 130 describes the significant fields for the **show spe version** command on the Cisco AS5800 access server.

Table 130 show spe version Field Descriptions

Field	Description
SPE-#	The slot and port number of the SPE.
SPE-Type	The type of the SPE.
SPE-Port-Range	The range of ports within the specific SPE.
Version	The version of firmware loaded on the SPE.
Upgrade	The method used to reboot the SPE—choices are: busyout (default), N/A, reboot, or recover.
Firmware-Filename	Name of the firmware. You can use the **dir** command at the prompt to display available firmware filenames.
IOS-Bundled Default Firmware-Filename	The firmware filenames bundled with the Cisco IOS software (system:/ucode).
Firmware-Type	The type of modem associated with the firmware version.
On-Flash Firmware-Filename	The firmware filenames on the Flash (flash:).

Related Commands

Command	Description
firmware location	Upgrades SPE firmware after the new SPE firmware image is retrieved from Cisco.com or elsewhere.
show modem mapping	Displays a snapshot of all the firmware versions running on all the modems in the access server.
show spe	Displays history statistics of all SPEs, a specified SPE, or the specified range of SPEs.

show tech-support modem

To create a modem ISDN channel aggregation (MICA) modem functionality report on a Cisco AS5300 or AS5800 access server, use the **show tech-support modem** command in privileged EXEC mode.

show tech-support modem [**detail**]

Syntax Description

detail	(Optional) Produces an extensive modem functionality report.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced for MICA technologies modems on the Cisco AS5300 and AS5800.

Usage Guidelines

This command is useful when information is required to troubleshoot a problem with MICA modems in the field. Customers are typically asked to send the output for a number of Cisco IOS EXEC commands. The **show tech-support modem** command provides extensive output of many EXEC commands through entry of a single command.

The report displayed by the **show tech-support modem** command is the successive output of many commands. The report takes some time to run and, when captured in a buffer, can be over 100 pages in length. The following commands are run by the **show tech-support modem** command. The commands are shown in the order run:

- **show version**
- **show running-config**
- **show modem version**
- **show modem**
- **show modem summary**
- **show spe version**
- **show controllers t1 call-counters**
- **show controllers e1 call-counters**
- **show modem connect-speeds**
- **show modem mapping**
- **show line**
- **show caller**
- **show users all**

The following additional commands are run by the **show tech-support modem detail** command. The commands are shown in the order run:

- **show modem configuration**
- **show modem operational-status**
- **show modem mica all**
- **show modem csm**
- **show modem log**

To interpret the modem reports, refer to the descriptions for each command in the appropriate command reference manual.

Examples

The following example shows how to display a basic list of modem reports:

```
Router# show tech-support modem
```

The following example shows how to display an extensive list of modem reports:

```
Router# show tech-support modem detail
```

Related Commands

Command	Description
execute-on	Executes a command on a line card to monitor and maintain information on the card (for example, a line card on a dial shelf).

show tech-support spe

To create a NextPort service processing element (SPE) modem functionality report on a Cisco AS5350, AS5400, AS5800, or AS5850 access server, use the **show tech-support spe** command in privileged EXEC mode.

show tech-support spe [**detail**]

Syntax Description

detail	(Optional) Produces an extensive modem functionality report.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced for SPE modems on the Cisco AS5350, AS5400, AS5800, and AS5850.

Usage Guidelines

This command is useful when information is required to troubleshoot a problem with SPE modems in the field. Customers are typically asked to send the output for a number of Cisco IOS EXEC commands. The **show tech-support spe** command provides extensive output of many EXEC commands by entering a single command.

The report displayed by the **show tech-support spe** command is the successive output of many commands. The report takes some time to run and, when captured in a buffer, can be over 100 pages in length. The following commands are run by the **show tech-support spe** command. The commands are shown in the order run:

- **show version**
- **show running-config**
- **show spe version**
- **show spe**
- **show spe modem summary**
- **show spe modem csr summary**
- **show spe modem disconnect-reason summary**
- **show spe recovery**
- **show csm call-rate**
- **show nextport mm**
- **show controllers e1 call-counters**
- **show controllers t1 call-counters**
- **show line**
- **show caller**
- **show users all**

The following additional commands are run by the **show tech-support spe detail** command. The commands are shown in the order run:

- **show csm modem**
- **show spe log**
- **show port modem log**

To interpret the modem reports, refer to the descriptions for each command listed in the appropriate command reference manual.

Examples

The following example shows how to display a basic list of modem reports:

```
Router# show tech-support spe
```

The following example shows how to display an extensive list of modem reports:

```
Router# show tech-support spe detail
```

Related Commands

Command	Description
execute-on	Executes a command on a line card to monitor and maintain information on the card (for example, a line card on a dial shelf).

show tgrm

To display information for debugging purposes about defined trunk groups and interfaces that have been assigned to the trunk groups, use the **show tgrm** command in EXEC mode.

show tgrm

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC (>)

Command History

Release	Modification
12.1(3)T	This command was introduced.

Examples

The following is sample output from the **show tgrm** command:

```
Router# show tgrm

      Trunk   Any in  Vce in   Data in
     Group #  Any out Vce out  Data out

        2       65535   65535   65535
                65535   65535   65535
                0 Retries
                Interface Se1/0/1:15    Data = 0, Voice = 0, Free = 30
                Interface Se1/0/8:15    Data = 2, Voice = 0, Free = 28

                Total calls for trunk group:Data = 2, Voice = 0, Free = 58
                Selected Voice Interface :Se1/0/1:15
                Selected Data Interface  :Se1/0/1:15
```

Table 131 describes the significant fields shown in the display.

Table 131 show tgrm Field Descriptions

Field	Description
Trunk Group #	Number of a defined trunk group.
Any in, Vce In, Data In, Any out, Vce out, Data out	Trunk group settings that specify whether incoming and outgoing voice and data traffic is allowed. The nonconfigured number 65535 indicates that **max-calls** values have not been configured in the global **trunk group** command.
Retries	Defined maximum number of retries.
Interface	Specified interface, number of channels currently used for voice and data, and number of free channels.

Table 131 show tgrm Field Descriptions (continued)

Field	Description
Total calls for trunk group	Number of calls to and from the trunk group, number of channels used for voice and data, and number of free channels.
Selected Voice Interface	Interface or trunk to be used next for a voice call.
Selected Data Interface	Interface or trunk to be used next for a data call.

show trunk group

To display information for one or more trunk groups, use the **show trunk group** command in user EXEC or privileged EXEC mode.

show trunk group [*name* [**cic**] [**sort** [**ascending** | **descending**]]

Syntax Description

name	(Optional) Trunk group to display.
cic	(Optional) Displays the Circuit Identification Code (CIC) number.
sort	(Optional) Sorts the output by trunk group number, in ascending or descending order.
ascending	(Optional) Specifies ascending display order for the trunk groups. This is the default.
descending	(Optional) Specifies descending display order for the trunk groups.

Command Default

Trunk groups display in ascending order.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.3(11)T	This command was modified. This command was enhanced to support dial-out trunk groups.
12.4(4)XC	This command was implemented on the Cisco 2600XM series, Cisco 2800 series, Cisco 3700 series, and Cisco 3800 series.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.
15.0(1)XA	This command was modified. The output was enhanced to show the logical partitioning class of restriction (LPCOR) policy for incoming and outgoing calls.
12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The **cic** keyword was added.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

Examples

The following sample output shows that for trunk group 1, preemption is enabled, with a preemption tone timer of 10 seconds, and the preemption level is flash.

```
Router# show trunk group 1

Trunk group: 1
        Description:
        trunk group label: 1

        Translation profile (Incoming):
        Translation profile (Outgoing):
```

```
        LPCOR (Incoming): local_group
        LPCOR (Outgoing): local_group

        Preemption is enabled
        Preemption Tone Timer is 10 seconds
        Preemption Guard Timer is 60 milliseconds

        Hunt Scheme is least-used
        Max Calls (Incoming):   NOT-SET (Any)   NOT-SET (Voice) NOT-SET
(Data)
        Max Calls (Outgoing):   NOT-SET (Any)   NOT-SET (Voice) NOT-SET
(Data)
        Retries: 0

        Trunk Se0/3/0:15        Preference DEFAULT
                Member Timeslots : 1-5
                Total channels available : 5
                Data = 0, Voice = 0, Modem = 0, Pending = 0, Free = 5
        Trunk Se0/3/1:15        Preference DEFAULT
                Member Timeslots : 1-2
                Total channels available : 0
                Data = 0, Voice = 0, Modem = 0, Pending = 0, Free = 0
        Trunk Se1/0/0:15        Preference DEFAULT
                Member Timeslots : 1-31
                Total channels available : 0
                Data = 0, Voice = 0, Modem = 0, Pending = 0, Free = 0
        Trunk Se1/0/1:15        Preference DEFAULT
                Member Timeslots : 1-10
                Total channels available : 0
                Data = 0, Voice = 0, Modem = 0, Pending = 0, Free = 0

        Total calls for trunk group: Data = 0, Voice = 0, Modem = 0
                                     Pend = 0, Free = 5

        Preemption Call Type:   Active  Pending
                Flash-Override  NA      0
                Flash           0       0
                Immediate       0       0
                Priority        0       0
                Routine         0       0

                Total           0       0

        Active preemption call-type shows the number of calls
        of each priority level which can be preempted by
        higher preemption level calls.

        Pending preemption call-type shows the number of calls
        of each priority level which are pending for the completion
        of call preemption.

        advertise_flag 0x00000040, capacity timer 25 sec tripl_config_mask 0x00000000
        AC_curr 5, FD_curr 0, SD_curr 0

        succ_curr 0 tot_curr 1
        succ_report 0 tot_report 1
        changed 1 replacement position 0
```

Table 132 describes the significant fields shown in the output. Fields are listed in alphabetical order.

Table 132 show trunk group Field Descriptions

Field	Description
Description	Description of the trunk group if entered with the **description** (trunk group) command.
trunk group label	Name of the trunk group.
Translation profile (Incoming)	List of incoming translation profiles.
Translation profile (Outgoing)	List of outgoing translation profiles.
LPCOR (Incoming)	Setting of the **lpcor incoming** command.
LPCOR (Outgoing)	Setting of the **lpcor outgoing** command.
Preemption is	Indicates whether preemption is enabled or disabled.
Preemption level	The preemption level for voice calls to be preempted by a DDR call.
Preemption tone timer	The expiry time for the preemption tone for the outgoing calls being preempted by a DDR call.
Hunt Scheme	Name of the idle channel hunt scheme used for this trunk group.
Max calls (incoming)	Maximum number of incoming calls handled by this trunk group.
Max calls (outgoing)	Maximum number of outgoing calls handled by this trunk group.
Retries	Number of times the gateway tries to complete the call on the same trunk group.
Total calls for trunk group	List of the total calls across all trunks in the trunk group.
Preemption Call Type	List of preemption levels for active and pending calls.
Data	Number of currently used data channels on the trunk or total data calls used by the trunk group.
Free	Number of currently available channels on the trunk or total available calls for the trunk group.
Member timeslots	Member timeslots for this trunk.
Pending	Number of pending channels.
Preference	Preference of the trunk in the trunk group. If DEFAULT appears, the trunk does not have a defined preference.
Total channels available	Number of available channels for the trunk.
Trunk group	ID of the trunk group member.
Voice	Number of currently used voice channels on the trunk or total voice calls used by the trunk group.

Related Commands

Command	Description
description (trunk group)	Includes a specific description of the trunk group interface.
hunt-scheme least-idle	Specifies the method for selecting an available incoming or outgoing channel.
trunk group	Initiates a trunk group definition.
trunk group timeslots	Directs an outbound synchronous or asynchronous call initiated by DDR to use specific DS0 channels of an ISDN circuit.

show vtemplate

To display information about all configured virtual templates, use the **show vtemplate** command in privileged EXEC mode.

show vtemplate

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)DC	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(14)T	The show display was modified to display the interface type of the virtual template and to provide counters on a per-interface-type basis for IPsec virtual tunnel interfaces.
12.2(33)SRA	This comand was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This comand was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

The following is sample output from the **show vtemplate** command:

```
Router# show vtemplate

Virtual access subinterface creation is globally enabled

         Active     Active    Subint  Pre-clone Pre-clone Interface
       Interface Subinterface Capable Available   Limit     Type
       --------- ------------ ------- --------- --------- ---------
Vt1            0            0   Yes          --        --   Serial
Vt2            0            0   Yes          --        --   Serial
Vt4            0            0   Yes          --        --   Serial
Vt21           0            0    No          --        --   Tunnel
Vt22           0            0   Yes          --        --   Ether
Vt23           0            0   Yes          --        --   Serial
Vt24           0            0   Yes          --        --   Serial

Usage Summary
                              Interface   Subinterface
                              ---------   ------------
Current Serial  in use                1              0
Current Serial  free                  0              3
Current Ether   in use                0              0
Current Ether   free                  0              0
Current Tunnel  in use                0              0
Current Tunnel  free                  0              0
Total                                 1              3

Cumulative created                    8              4
Cumulative freed                      0              4
```

```
Base virtual access interfaces: 1
Total create or clone requests: 0
Current request queue size: 0
Current free pending: 0

Maximum request duration: 0 msec
Average request duration: 0 msec
Last request duration: 0 msec

Maximum processing duration: 0 msec
Average processing duration: 0 msec
Last processing duration: 0 msec
Last processing duration:0 msec
```

Table 133 describes the significant fields shown in the example.

Table 133 show vtemplate Field Descriptions

Field	Description
Virtual access subinterface creation is globally...	The configured setting of the **virtual-template** command. Virtual access subinterface creation may be enabled or disabled.
Active Interface	The number of virtual access interfaces that are cloned from the specified virtual template.
Active Subinterface	The number of virtual access subinterfaces that are cloned from the specified virtual template.
Subint Capable	Specifies if the configuration of the virtual template is supported on the virtual access subinterface.
Pre-clone Available	The number of precloned virtual access interfaces currently available for use for the particular virtual template.
Pre-clone Limit	The number of precloned virtual access interfaces available for that particular virtual template.
Current in use	The number of virtual access interfaces and subinterfaces that are currently in use.
Current free	The number of virtual access interfaces and subinterfaces that are no longer in use.
Total	The total number of virtual access interfaces and subinterfaces that exist.
Cumulative created	The number of requests for a virtual access interface or subinterface that have been satisfied.
Cumulative freed	The number of times that the application using the virtual access interface or subinterface has been freed.
Base virtual-access interfaces	This field specifies the number of base virtual access interfaces. The base virtual access interface is used to create virtual access subinterfaces. There is one base virtual access interface per application that supports subinterfaces. A base virtual access interface can be identified from the output of the **show interfaces virtual-access** command.
Total create or clone requests	The number of requests that have been made through the asynchronous request API of the virtual template manager.

Table 133 show vtemplate Field Descriptions (continued)

Field	Description
Current request queue size	The number of items in the virtual template manager work queue.
Current free pending	The number of virtual access interfaces whose final freeing is pending. These virtual access interfaces cannot currently be freed because they are still in use.
Maximum request duration	The maximum time that it took from the time that the asynchronous request was made until the application was notified that the request was done.
Average request duration	The average time that it took from the time that the asynchronous request was made until the application was notified that the request was done.
Last request duration	The time that it took from the time that the asynchronous request was made until the application was notified that the request was done for the most recent request.
Maximum processing duration	The maximum time that the virtual template manager spent satisfying the request.
Average processing duration	The average time that the virtual template manager spent satisfying the request.
Last processing duration	The time that the virtual template manager spent satisfying the request for the most recent request.

Related Commands

Command	Description
clear counters	Clears interface counters.
show interfaces virtual-access	Displays status, traffic data, and configuration information about a specified virtual access interface.
virtual-template	Specifies which virtual template will be used to clone virtual access interfaces.

shutdown (port)

To disable a port, use the **shutdown** command in port configuration mode. To change the administrative state of a port from out-of-service to in-service, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

Port is enabled.

Command Modes

Port configuration (config-port)

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5800.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.

Usage Guidelines

The **shutdown** command disables a port.

Note The **shutdown** command is similar to the **modem shutdown** MICA technologies modem command.

Examples

The following example disables ports 1 to 18 and then reenables them:

```
Router(config)# port 1/1 1/18
Router(config-port)# shutdown
Router(config-port)# no shutdown
```

Related Commands

Command	Description
busyout (port)	Disables a port by causing the system to wait for the active services on the port to terminate.
clear port	Resets the NextPort port and clears any active call.
clear spe	Reboots all specified SPEs.

Command	Description
modem shutdown	Abruptly shuts down an active or idle modem installed in an access server or router.
show spe	Displays history statistics of all SPEs, a specified SPE, or the specified range of SPEs.

shutdown (spe)

To take a service processing element (SPE) out of service, use the **shutdown** command in SPE configuration mode. To change the administrative state of this SPE from down to up, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

SPE is in service.

Command Modes

SPE configuration (config-spe)

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5800.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.

Examples

The following example disables SPE ports 1 to 18 and then reenables them:

```
Router(config)# spe 1/1 1/18
Router(config-spe)# shutdown
Router(config-spe)# no shutdown
```

Related Commands

Command	Description
busyout (port)	Disables a port by causing the system to wait for the active services on the port to terminate.
clear spe	Reboots all specified SPEs.
show spe	Displays history statistics of all SPEs, a specified SPE, or the specified range of SPEs.

signaling-class cas

To define a signaling class with a template formed by directives guiding the Call Service Module (CSM) to process the digit sequence, use the **signaling-class cas** command in global configuration mode. To remove the signaling class assignment, use the **no** form of this command.

signaling-class cas *name*

no signaling-class cas *name*

Syntax Description

name	The signaling class name, which specifies the template that processes the ANI/DNIS delimiter.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

The signaling class is referred by the *name* argument.

Examples

The following example enables the **signaling-class cas** command:

```
signaling-class cas test
 profile incoming S<*a<*d<*n
 controller T1 1/0/1
 cas-custom 1
 class test
```

Related Commands

Command	Description
class (controller)	Activates the **signaling-class cas** command.
profile incoming	Defines a template formed by directives guiding the CSM to process the digit sequence for a signaling class.

snapshot client

To configure a client router for snapshot routing, use the **snapshot client** command in interface configuration mode. To disable a client router, use the **no** form of this command.

snapshot client *active-time quiet-time* [**suppress-statechange-updates**] [**dialer**]

no snapshot client *active-time quiet-time* [**suppress-statechange-updates**] [**dialer**]

Syntax Description

active-time	Amount of time, in minutes, that routing updates are regularly exchanged between the client and server routers. This can be an integer ranging from 5 to 100. There is no default value. A typical value is 5 minutes.
quiet-time	Amount of time, in minutes, that routing entries are frozen and remain unchanged between active periods. Routes are not aged during the quiet period, so they remain in the routing table as if they were static entries. This argument can be an integer ranging from 8 to 100000. There is no default value. The minimum quiet time is generally the active time plus 3.
suppress-statechange-updates	(Optional) Disables the exchange of routing updates each time the line protocol goes from "down" to "up" or from "dialer spoofing" to "fully up."
dialer	(Optional) Specifies that the client router dials up the remote router in the absence of regular traffic.

Command Default

Snapshot routing is disabled.

The *active-time* and *quiet-time* arguments have no default values.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The value of the *active-time* argument must be the same for the client and server routers.

To specify that the remote server routers be called by this client router during each active period, use the **dialer map snapshot** command.

Examples

The following example configures a client router for snapshot routing:

```
interface dialer 1
 snapshot client 5 600 suppress-statechange-updates dialer
```

Related Commands

Command	Description
clear resource-pool	Ends the quiet period on a client router within 2 minutes.
dialer map snapshot	Defines a dialer map for the Cisco snapshot routing protocol on a client router connected to a DDR interface.
show snapshot	Displays snapshot routing parameters associated with an interface.
snapshot client	Configures a client router for snapshot routing.
snapshot server	Configures a server router for snapshot routing.

snapshot server

To configure a server router for snapshot routing, use the **snapshot server** command in interface configuration mode. To disable a server router, use the **no** form of this command.

snapshot server *active-time* [**dialer**]

no snapshot server *active-time* [**dialer**]

Syntax Description

active-time	Amount of time, in minutes, that routing updates are regularly exchanged between the client and server routers. This can be an integer ranging from 5 to 100. There is no default value. A typical value is 5 minutes.
dialer	(Optional) Specifies that the client router dials up the remote router in the absence of regular traffic.

Command Default

Snapshot routing is disabled.

The *active-time* argument has no default value.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The value of the *active-time* argument must be the same for the client and server routers.

Examples

The following example configures a server router for snapshot routing:

```
interface dialer 1
 snapshot server 5
```

Related Commands

Command	Description
show snapshot	Displays snapshot routing parameters associated with an interface.
snapshot client	Configures a client router for snapshot routing.

source template

To attach a configured customer profile template to a particular customer profile, use the **source template** command in customer profile configuration mode.

source template *name*

Syntax Description

name	Customer profile template name.

Command Default

No templates are sourced or attached to a customer profile.

Command Modes

Customer profile configuration

Command History

Release	Modification
12.0(6)T	This command was introduced.

Usage Guidelines

All PPP and peer-default commands are allowed for a particular customer profile template under this grouping.

Examples

The following example shows the creation and configuration of a customer profile template named cisco1-direct and its subsequent assignment to the customer profile cisco1:

```
template cisco1-direct
 multilink {max-fragments num | max-links num | min-links num}
 peer match aaa-pools
 peer default ip address pool cisco1-numbers
 ppp ipcp dns 10.1.1.1  10.2.2.2
 ppp multilink
 exit
resource-pool profile customer cisco1
source template cisco1-direct
```

Related Commands

Command	Description
template	Accesses the template configuration mode for configuring a particular customer profile template.

spe

To enter service processing element (SPE) configuration mode and set the range of SPEs, use the **spe** command in global configuration mode.

Cisco AS5350 and Cisco AS5400 with the NextPort Dial Feature Card (DFC)

spe {*slot* | *slot*/*spe*} [*slot* | *slot*/*spe*]

Cisco AS5800 with the Universal Port Card (UPC)

spe {*shelf*/*slot* | *shelf*/*slot*/*spe*} [*shelf*/*slot* | *shelf*/*slot*/*spe*]

Syntax Description

slot	All ports on the specified slot. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7. A range of slots can be specified by entering a second value for the *slot* argument.
slot/*spe*	All ports on the specified slot and SPE. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7. SPE values range from 1 to 17. You must include the slash mark. A range of ports can be specified by entering a second value for the *slot*/*spe* argument.
shelf/*slot*	All ports on the specified shelf and slot. For the Cisco AS5800, shelf values range from 0 to 1 and UPC slot values range from 2 to 11. You must include the slash mark. A range of slots can be specified by entering a second value for the *shelf*/*slot* argument.
shelf/*slot*/*spe*	All ports on the specified SPE. For the Cisco AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and SPE values range from 0 to 53. You must include the slash marks. A range of ports can be specified by entering a second value for the *shelf*/*slot*/*spe* argument.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XI1	This command was introduced.
12.0(5)T	This command was implemented on the Cisco AS5200 and Cisco AS5300 platforms.
12.1(1)XD	This command was implemented on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5800.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.

Usage Guidelines

The **spe** global configuration command enables the SPE configuration mode. Configure your SPE by specifying a slot and an SPE associated with the slot; or, you can configure a range of SPEs by specifying the first and last SPE in the range.

To exit SPE configuration mode, use the **exit** command.

Examples

The following example shows the **spe** command being used from global configuration mode to access the SPE configuration mode for the SPE range from 1/2 to 1/4:

```
Router(config)# spe 5/4 5/6
Router(config-spe)# ?
SPE Configuration Commands:
  busyout   Busyout SPE
  default   Set a command to its defaults
  exit      Exit from SPE Configuration Mode
  firmware  Firmware used for the SPE
  help      Description of the interactive help system
  no        Negate a command or set its defaults
  shutdown  Take the SPE out of Service
```

When the universal gateway is booted, the **spe** global configuration command specifies the location from where the firmware image is downloaded to the SPE. If the **spe** configuration command is used to download the firmware from Flash memory and then subsequently the **no** version of the exact command is entered, then the **spe** command downloads the embedded firmware.

Note Use this command when traffic is low because the **spe** download does not begin until the modems have no active calls.

Caution The **spe** command is a configuration command. Save it using the **write memory** command; otherwise, the configuration is not saved. If the configuration is not saved, the downloading of the specified firmware does not occur after the next reboot.

The following example shows the **spe** command being used from global configuration mode to access the SPE configuration mode for the range of SPEs from 1/2 to 1/4 on the Cisco AS5400:

```
Router(config)# spe 1/2 1/4
```

The following example specifies the range for use of the **shutdown** command:

```
Router(config)# spe 1/1 1/18
Router(config-spe)# shutdown
Router(config-spe)# no shutdown
```

Related Commands

Command	Description
exit	Exits SPE configuration mode.
show spe	Displays SPE status.

spe call-record modem

To generate a modem call record at the end of each call, use the **spe call-record modem** command in global configuration mode. To cancel the request to generate the reports, use the **no** form of the command.

spe call-record modem {**max-userid** *number* | **quiet**}

no spe call-record modem {**max-userid** *number* | **quiet**}

Syntax Description

max-userid *number*	Maximum length of the user ID for the modem call record report in number of bytes. The range is from 0 to 100.
quiet	Disables logging to console and terminal, but not to syslog.

Command Default

An SPE call record is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5800.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.

Usage Guidelines

The **spe modem-call-record** command generates a modem call record at the end of each call.

Note The **spe call-record modem** command is similar to the **modem call-record** command.

Examples

The following example displays an SPE call record:

```
Router# configure terminal
Router(config)# spe call-record modem max-userid 50
Router(config)# end
Router#
00:18:30: %SYS-5-CONFIG_I: Configured from console by console
Router# write memory
Building configuration...
[OK]
```

The following is a partial example of traces generated when a call terminates. The logs from the **show port modem log** command do not change as a result of using the **spe call-record modem** command.

```
.
.
.
%LINK-3-UPDOWN: Interface Async5/105, changed state to down
%MODEMCALLRECORD-6-PM_TERSE_CALL_RECORD: DS0 slot/contr/chan=4/2/15,
shelf/slot/port=5/37, call_id=EE, userid=touraco-e1-4, ip=79.188.24.1,
calling=(n/a), called=35160, std=V.34+, prot=LAP-M, comp=V.42bis,
init-rx/tx b-rate=33600/33600, finl-rx/tx b-rate=33600/33600, rbs=0,
d-pad=None, retr=1, sq=5, snr=10495, rx/tx chars=286/266, bad=0, rx/tx
ec=16/6, bad=0, time=96, finl-state=Steady Retrain,
disc(radius)=(n/a)/(n/a), disc(modem)=1F00 <unknown>/Requested by
host/non-specific host disconnect
%MODEMCALLRECORD-6-PM_TERSE_CALL_RECORD: DS0 slot/contr/chan=4/1/24,
shelf/slot/port=5/38, call_id=FD, userid=touraco-e1-4, ip=79.205.24.1,
calling=(n/a), called=35170, std=V.34+, prot=LAP-M, comp=V.42bis,
init-rx/tx b-rate=33600/33600, finl-rx/tx b-rate=33600/33600, rbs=0,
d-pad=None, retr=1, sq=5, snr=10495, rx/tx chars=289/267, bad=0, rx/tx
ec=17/7, bad=0, time=93, finl-state=Steady Retrain,
disc(radius)=(n/a)/(n/a), disc(modem)=1F00 <unknown>/Requested by
host/non-specific host disconnect
%MODEMCALLRECORD-6-PM_TERSE_CALL_RECORD: DS0 slot/contr/chan=4/3/15,
shelf/slot/port=5/2, call_id=FF, userid=touraco-e1-4, ip=79.200.24.1,
calling=(n/a), called=35170, std=V.34+, prot=LAP-M, comp=V.42bis,
init-rx/tx b-rate=33600/33600, finl-rx/tx b-rate=33600/33600, rbs=0,
d-pad=None, retr=1, sq=5, snr=10495, rx/tx chars=287/270, bad=0, rx/tx
ec=17/7, bad=0, time=92, finl-state=Steady Retrain,
disc(radius)=(n/a)/(n/a), disc(modem)=1F00 <unknown>/Requested by
host/non-specific host disconnect
%MODEMCALLRECORD-6-PM_TERSE_CALL_RECORD: DS0 slot/contr/chan=4/3/10,
shelf/slot/port=5
.
.
.
```

Related Commands

Command	Description
modem call-record	Activates the logging of a summary of modem events upon the termination of a call.

spe country

To specify the country while setting the modem card parameters (including country code and encoding), use the **spe country** command in global configuration mode. To set the country code to the default value, use the **no** form of this command.

spe country {*country-name* | **e1-default** | **t1-default**}

no spe country {*country-name* | **e1-default** | **t1-default**}

Syntax Description

country-name	Name of the country, See Table 134 for a list of supported country name keywords.
e1-default	Use this command when using the E1 interface.
t1-default	Use this command when using the T1 interface.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5800.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.

Usage Guidelines

On the Cisco universal gateway, DS0 companding law selection is configured for the entire system rather than on individual voice ports. Set the **spe country** command to the appropriate country.

If T1 lines are configured, the default is **t1-default**; if E1 lines are configured, the default is **e1-default**.

The Cisco universal gateway must be in an Idle state (no calls are active) for the **spe country** command to function. All sessions on all modules in all slots must be in the Idle state.

Note The **spe country** command is similar to the **modem country mica** and **modem country microcom_hdms** commands.

Table 134 lists the country names and corresponding companding law.

Table 134 Country Names and Corresponding Companding Law

Keyword	Country	Companding Law
australia	Australia	a-law
austria	Austria	a-law
belgium	Belgium	a-law
china	China	a-law
cyprus	Cyprus	a-law
czech-republic	Czech/Slovak Republic	a-law
denmark	Denmark	a-law
e1-default	Default for E1	a-law
finland	Finland	a-law
france	France	a-law
germany	Germany	a-law
hong-kong	Hong Kong	u-law
india	India	a-law
ireland	Ireland	a-law
israel	Israel	a-law
italy	Italy	a-law
japan	Japan	u-law
malaysia	Malaysia	a-law
netherlands	Netherlands	a-law
new-zealand	New Zealand	a-law
norway	Norway	a-law
poland	Poland	a-law
portugal	Portugal	a-law
russia	Russia	a-law
singapore	Singapore	a-law
south-africa	South Africa	a-law
spain	Spain	a-law
sweden	Sweden	a-law
switzerland	Switzerland	a-law
t1-default	Default for T1	u-law
taiwan	Taiwan	u-law
thailand	Thailand	a-law
turkey	Turkey	a-law
united-kingdom	United Kingdom	a-law
usa	United States of America	u-law

Examples

The following example configures the setting of the country code to the default for E1:

```
Router(config)# spe country e1-default
```

The following example configures the setting of the country code to the default for T1:

```
Router(config)# spe country t1-default
```

Related Commands

Command	Reference
modem country mica	Configures the modem country code for a bank of MICA technologies modems.
modem country microcom_hdms	Configures the modem country code for a bank of Microcom modems.
show spe	Displays SPE status.

spe download maintenance

To perform download maintenance on service processing elements (SPEs) that are marked for recovery, use the **spe download maintenance** command in global configuration mode. To disable download maintenance on SPEs, use the **no** form of the command.

spe download maintenance {**time** *hh:mm* | **stop-time** *hh:mm* | **max-spes** *number-of-spes* | **window** *time-period* | **expired-window** {**drop-call** | **reschedule**}}

no spe download maintenance {**time** *hh:mm* | **stop-time** *hh:mm* | **max-spes** *number-of-spes* | **window** *time-period* | **expired-window** {**drop-call** | **reschedule**}}

Syntax Description

time *hh:mm*	Time of the day to start the download maintenance activity. Enter the value in the format of the variable as shown in hours and minutes. Default is 03:00 a.m.
stop-time *hh:mm*	Time of the day to stop the download maintenance activity. Enter the value in the format of the variable as shown in hours and minutes.
max-spes *number-of-spes*	Maximum number of SPEs that can simultaneously be in maintenance. The value ranges from 1 to 10,000. Default is equal to 20 percent of the maximum number of SPEs in each NextPort Dial Feature Card (DFC).
window *time-period*	Time window to perform the maintenance activity. The value ranges from 0 to 360 minutes. Default is 60 minutes.
expired-window	Action to take if SPE maintenance is not completed within the specified window. Default is **reschedule**.
drop-call	Expired window choice that forces download by dropping active calls.
reschedule	Expired window choice that defers recovery to the next maintenance time (default for the **expired-window** keyword).

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5800.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.

Usage Guidelines

The SPE download maintenance activity takes place when SPEs are marked for recovery. The settings are enabled by default. When you want to change the default settings to a desired setting, use the **spe download maintenance** command parameters to perform SPE download maintenance activity with the specific changes.

Enter the **time** *hh:mm* keyword to set a time to start the SPE download maintenance activity. Then enter the **stop-time** *hh:mm* keyword to set a time to stop the download maintenance. Next enter the **max-spes** *number-of-spes* keyword to set the number of SPEs for the download maintenance. Then enter the **window** *time-period* keyword to set a time period to perform the download maintenance. Finally, enter the **expired-window** keyword to set actions in the event the SPE download maintenance is not completed in the set **window** *time-period*.

The download maintenance activity starts at the set start **time** and steps through all the SPEs that need recovery and the SPEs that need a firmware upgrade and starts maintenance on the maximum number of set SPEs for maintenance. The system waits for the **window** delay time for all the ports on the SPE to become inactive before moving the SPE to the Idle state. Immediately after the SPE moves to the Idle state, the system starts to download firmware. If the ports are still in use by the end of **window** delay time, depending upon the **expired-window** setting, connections on the SPE ports are shut down and the firmware is downloaded by choosing the **drop-call** option, or the firmware download is rescheduled to the next download maintenance time by choosing the **reschedule** option. This process continues until the number of SPEs under maintenance is below the **max-spes** value, or until the **stop-time** value (if set), or until all SPEs marked for recovery or upgrade have had their firmware reloaded.

Examples

The following example displays the SPE download maintenance with the different keyword parameters:

```
Router(config)# spe download maintenance time 03:00

Router(config)# spe download maintenance stop-time 04:00

Router(config)# spe download maintenance max-spes 50

Router(config)# spe download maintenance window 30

Router(config)# spe download maintenance expired-window reschedule
```

Related Commands

Command	Description
firmware location	Downloads firmware into Cisco integrated modems.
firmware upgrade	Specifies the method in which the SPE will be downloaded.
show spe version	Displays the firmware version on an SPE.
spe recovery	Sets an SPE port for recovery.

spe log-size

To set the size of the port event log, use the **spe log-size** command in global configuration mode. To restore the default size, use the **no** version of this command.

spe log-size *number*

no spe log-size

Syntax Description

number	The number of recorded events. Valid values for the *number* argument range from 0 to 100. The default value is 50 events.

Command Default

The port event log records 50 events.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T on the Cisco AS5400 and Cisco AS5800.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.

Examples

The following example sets the size of the event log to 70 events:

```
Router(config)# spe log-size 70
```

Related Commands

Command	Description
show port digital log	Displays the digital data event log with the oldest event first.
show port modem log	Displays the modem port history event log or modem test log.

spe recovery

To set a service processing element (SPE) port for recovery, use the **spe recovery** command in global configuration mode. To disable SPE recovery or to restore the default **port-threshold** value, use the **no** form of this command.

spe recovery {**port-action** {**disable** | **recover**} | **port-threshold** *number-failures*}

no spe recovery {**port-action** | **port-threshold**}

Syntax Description

port-action	Action to apply to the port for recovery when the configured **port-threshold** value has been exceeded.
disable	Sets the port to the bad state.
recover	Sets the port for recovery.
port-threshold *number-failures*	Number of consecutive failed attempts made on the port before the **port-action** keyword is applied. The range is from 1 to 10000. The default value is 30.

Command Default

There is no default **port-action** value. SPE recovery is disabled.
The default **port-threshold** value is 30 failed attempts.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)XD	This command was introduced on the Cisco AS5400.
12.1(2.3)T1	This command was implemented on the Cisco AS5800.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco AS5350.

Usage Guidelines

Failure of an SPE port to connect after repeated tries indicates that a problem exists in the SPE or firmware. An SPE port in this state is recovered by downloading firmware.

When an SPE port fails to connect consecutively for a number of times, as specified by the **port-threshold** *number-failures* keyword and argument, the SPE is moved to a state based on the **port-action** configuration.

If the **spe recovery port-action recover** command has been configured, when the **port-threshold** *number-failures* value is exceeded, the port is temporarily marked as disabled (“d” state) to avoid further incoming calls, and it is then marked for recovery (“r” state). Any SPE that has a port marked for recovery will download firmware when the SPE is idle (when none of the ports on the SPE have active calls).

If the **spe recovery port-action disable** command has been configured, when the **port-threshold** *number-failures* value is exceeded, the port is marked as bad ("BAD" state). An SPE with a port that is marked as bad must be explicitly cleared in order for that port to be used again.

If no **port-action** is configured, the port will be marked as not in use ("_" state). An SPE with a port marked as not in use will remain unusable until it is explicitly cleared, and the SPE will not accept incoming calls on any of the ports.

SPE recovery can be disabled by issuing the **no spe recovery port-action** command. If SPE recovery is disabled, the SPE will behave as if no **port-action** has been configured.

Note Beginning with Cisco IOS Release 12.1(2.3)T1, the modem recovery action for MICA technologies modems on the Cisco AS5800 platforms is done using the **spe recovery** command rather than the **modem recovery** command.

Examples

The following example configures the SPE to recover ports that exceed the call failure threshold:

```
Router(config)# spe recovery port-action recover
```

The following example sets a value of 50 for the number of consecutive failed attempts on the port before the **port-action** keyword is applied:

```
Router(config)# spe recovery port-threshold 50
```

Related Commands

Command	Description
clear port	Resets the NextPort port and clears any active call.
clear spe	Reboots all specified SPEs.
firmware upgrade	Specifies an SPE firmware upgrade method.
show spe	Displays history statistics of all SPEs, a specified SPE, or the specified range of SPEs.
show spe version	Displays the firmware version on an SPE and displays the version to firmware file mappings.
spe download maintenance	Performs download maintenance on SPEs that are marked for recovery.

start-character

To set the flow control start character, use the **start-character** command in line configuration mode. To remove the character, use the **no** form of this command.

start-character *ascii-number*

no start-character

Syntax Description

ascii-number	Decimal representation of the start character.

Command Default

Decimal 17

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command defines the character that signals the start of data transmission when software flow control is in effect. Refer to the "ASCII Character Set and Hex Values" appendix in the *Cisco IOS Configuration Fundamentals and Network Management Command Reference* for a list of ASCII characters.

Examples

The following example changes the start character to Ctrl-B, which is decimal 2:

```
line 2
 start-character 2
```

Related Commands

Command	Description
flowcontrol	Sets the method of data flow control between the terminal or other serial device and the router.
stop-character	Sets the flow control stop character.
terminal start-character	Changes the flow control start character for the current session.

start-chat

To specify that a chat script start on a specified line at any point, use the **start-chat** command in privileged EXEC mode. To stop the chat script, use the **no** form of this command.

start-chat *regexp* [[**aux** | **console** | **vty**] *line-number* [*dialer-string*]]

no **start-chat**

Syntax Description

regexp	Name of a regular expression or modem script to be executed. If there is more than one script with a name that matches the argument *regexp*, the first script found will be used.
line-number	(Optional) Line number on which to execute the chat script. If you do not specify a line number, the current line number is chosen. If the specified line is busy, the script is not executed and an error message appears. If the dialer-string argument is specified, line-number must be entered; it is not optional if you specify a dialer string. This command functions only on physical terminal (TTY) lines. It does not function on virtual terminal (VTY) lines.
dialer-string	(Optional) String of characters (often a telephone number) to be sent to a DCE. If you enter a dialer string, you must also specify *line-number*, or the chat script *regexp* will not start.
aux	(Optional) Specifies the auxiliary line.
console	(Optional) Specifies the primary terminal line.
vty	(Optional) Specifies the virtual terminal.

Command Default

If you do not specify a line number, the current line number is chosen. If the specified line is busy, the script is not executed and an error message appears. If the dialer-string argument is specified, line-number must be entered; it is not optional if you specify a dialer string. This command functions only on physical terminal (TTY) lines. It does not function on virtual terminal (VTY) lines.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
15.0(1)M	This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M. The **aux**, **console**, and **vty** keywords were added.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

This command provides modem dialing commands for a chat script that you want to apply immediately to a line. If you do not specify a line, the script runs on the current line. If the specified line is already in use, the script is not activated and an error message appears.

The argument *regexp* is used to specify the name of the modem script that is to be executed. The first script that matches the argument in this command and the **dialer map** command will be used. For more information about regular expressions, refer to the "Regular Expressions" appendix in this publication.

This command functions only on physical terminal (TTY) lines. It does not function on virtual terminal lines.

Examples

The following example shows how to force a dialout on line 8 using the script named "telebit":

```
Router# start-chat telebit 8
```

Related Commands

Command	Description
chat-script	Places calls over a modem and logs in to remote systems.
dialer map	Configures a serial interface or ISDN interface to call one or multiple sites or to receive calls from multiple sites.
script activation	Specifies that a chat script start on a physical terminal line when the line is activated.
script connection	Specifies that a chat script start on a physical terminal line when a remote network connection is made to a line.
script dialer	Specifies a default modem chat script.
script reset	Specifies that a chat script start on a physical terminal line when the specified line is reset.
script startup	Specifies that a chat script start on a physical terminal line when the router is powered up.

stop-character

To set the flow control stop character, use the **stop-character** command in line configuration mode. To remove the character, use the **no** form of this command.

stop-character *ascii-number*

no stop-character

Syntax Description

ascii-number	Decimal representation of the stop character.

Command Default

Decimal 19

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command defines the character that signals the end of data transmission when software flow control is in effect. Refer to the "ASCII Character Set and Hex Values" appendix in the *Cisco IOS Configuration Fundamentals and Network Management Command Reference* for a list of ASCII characters.

Examples

The following example changes the stop character to Ctrl-E, which is decimal 5:

```
line 3
 stop-character 5
```

Related Commands

Command	Description
flowcontrol	Sets the method of data flow control between the terminal or other serial device and the router.
source template	Sets the flow control start character.
stop-character	Sets the flow control stop character.

tdm clock priority

To configure the clock source and priority of the clock source used by the time-division multiplexing (TDM) bus on the Cisco AS5350, AS5400, and AS5850 access servers, use the **tdm clock priority** command in global configuration mode. To return the clock source and priority to the default values, use the **no** form of this command.

tdm clock priority *priority-number* {*slot*/*ds1-port* | *slot*/*ds3-port*:*ds1-port* | **external** | **freerun**}

no tdm clock priority *priority-number* {*slot*/*ds1-port* | *slot*/*ds3-port*:*ds1-port* | **external** | **freerun**}

Syntax Description

priority-number	Priority of the clock source. The priority range is from 1 to 99. A clock set to priority 100 will not drive the TDM bus.
slot/*ds1-port*	Trunk-card slot is a value from 1 to 7. DS1 port number controller is a value between 0 and 7. Specify with a slash separating the numbers; for example, 1/1.
slot/*ds3-port*:*ds1-port*	Trunk-card slot is a value from 1 to 7. DS3 port specifies the T3 port. DS1 port number controller is a value from 1 to 28. Specify with a slash separating the slot and port numbers, and a colon separating the DS1 port number. An example is 1/0:19.
external	Synchronizes the TDM bus with an external clock source that can be used as an additional network reference.
freerun	Selects the free-running clock from the local oscillator when there is no good clocking source from a trunk card or an external clock source.

Command Default

If no clocks are configured, the system uses a default, primary clock. An external clock is never selected by default; it must be explicitly configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The TDM bus can receive an input clock from one of three sources on the gateway:

- CT1, CE1, and CT3 trunk cards
- An external T1/E1 clock source feed directly through the Building Integrated Timing Supply (BITS) interface port on the motherboard
- Free-running clock providing clock from an oscillator

Note BITS is a single building master timing supply. BITS generally supplies DS1- and DS0-level timing throughout an office. BITS is the clocks that provide and distribute timing to a wireline network's lower levels.

Trunk-Card Ports

The TDM bus can be synchronized with any trunk cards. On the CT1/CE1 trunk card, each port receives the clock from the T1/E1 line. The CT3 trunk card uses an M13 multiplexer to receive the DS1 clock. Each port on each trunk-card slot has a default clock priority. Also, clock priority is configurable through the **tdm clock priority** command.

External Clock

The TDM bus can be synchronized with an external clock source that can be used as an additional network reference. If no clocks are configured, the system uses a primary clock through a software-controlled default algorithm. If you want the external T1/E1 clock (from the BITS interface) as the primary clock source, you must configure it using the **external** keyword with the **tdm clock priority** command; the external clock is never selected by default.

The BITS interface requires a T1 line composite clock reference set at 1.544 MHz and an E1 line composite clock reference set at 2.048 MHz.

Free-Running Clock

If there is no good clocking source from a trunk card or an external clock source, then select the free-running clock from the internal oscillator using the **freerun** keyword with the **tdm clock priority** command.

Examples

In the following example, BITS clock is set at priority 1:

```
AS5400(config)# tdm clock priority priority 1 external
```

In the following example, a trunk clock from a CT1 trunk card is set at priority 2 and uses slot 4 and DS1 port (controller) 6:

```
AS5400(config)# tdm clock priority priority 2 4/6
```

In the following example, a trunk clock from a CT3 trunk card is set at priority 2 and uses slot 1, DS3 port 0, and DS1 port 19:

```
AS5400(config)# tdm clock priority priority 2 1/0:19
```

In the following example, free-running clock is set at priority 3:

```
AS5400(config)# tdm clock priority priority 3 freerun
```

Related Commands

Command	Description
dial-tdm-clock	Configures the clock source and priority of the clock source used by the TDM bus on the dial shelf of the Cisco AS5800.
show tdm clocks	Displays default system clocks and clock history.

template

To access the template configuration mode for configuring a particular customer profile template, use the **template** command in global configuration mode. To delete the template of the specified name, use the **no** form of this command.

template *name* [**default | exit | multilink | no | peer | ppp**]

no template *name* [**default | exit | multilink | no | peer | ppp**]

Syntax Description

name	Identifies the template.
default	(Optional) Sets the command to its defaults.
exit	(Optional) Exits from resource-manager configuration mode.
multilink	(Optional) Configures multilink parameters.
no	(Optional) Negates the command or its defaults.
peer	(Optional) Accesses peer parameters for point-to-point interfaces.
ppp	(Optional) Accesses Point-to-Point Protocol.

Command Default

No templates are configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(6)T	This command was introduced.

Usage Guidelines

All PPP and peer-default commands are enabled for a customer profile template under this grouping.

Examples

The following example shows the creation and configuration of a customer profile template named "cisco1-direct" and its subsequent assignment to the customer profile "cisco1":

```
template cisco1-direct
 multilink max-fragments 10
 peer match aaa-pools
 peer default ip address pool cisco1-numbers
 ppp ipcp dns 10.1.1.1  10.2.2.2
 ppp multilink
 exit
resource-pool profile customer cisco1
source template cisco1-direct
```

Related Commands

Command	Description
source template	Attaches a configured customer profile template to a customer profile.

test modem back-to-back

To diagnose an integrated modem that may not be functioning properly, use the **test modem back-to-back** command in EXEC mode.

test modem back-to-back *first-slot/port second-slot/port*

Syntax Description

first-slot/port	Slot and modem number of the first test modem. You must include the slash mark
second-slot/port	Slot and modem number of the second test modem. You must include the slash mark

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use this command to perform back-to-back testing of two modems. You might need to enable this command on several different combinations of modems to determine which one is not functioning properly.

Examples

The following example performs a back-to-back modem test between modem 2/0 and modem 2/1 and removes modem 2/1 (which is associated with TTY line 26) from all dial-in and dial-out services:

```
Router# test modem back-to-back 2/0 2/1

back2back 2/0 2/1
Repetitions (of 10-byte packets) [1]:

Router#

%MODEM-5-B2BCONNECT: Modems (2/0) and (2/1) connected in back-to-back test:
CONNECT9600/REL-MNPM
%MODEM-5-B2BMODEMS: Modems (2/0) and (2/1) completed back-to-back test: success/packets =
2/2
```

Related Commands

Command	Description
modem bad	Removes an integrated modem from service and indicates it as suspected or proven to be inoperable.
test port modem back-to-back	Tests two specified ports back-to-back and transfers a specified amount of data between the ports.

test port modem back-to-back

To test two specified ports back-to-back and transfer a specified amount of data between the ports, use the **test port modem back-to-back** command in EXEC mode.

Cisco AS5350 and Cisco AS5400 with the NextPort Dial Feature Card (DFC)

test port modem back-to-back *slot/port*

Cisco AS5800 with the Universal Port Card (UPC)

test port modem back-to-back *shelf/slot/port*

Syntax Description

slot/port	All ports on the specified slot and SPE. For the Cisco AS5350 slot values range from 1 to 3. For the Cisco AS5400, slot values range from 1 to 7. Port values range from 0 to one less than the number of ports supported by the card. You must include the slash mark.
shelf/slot/port	All ports on the specified SPE. For the Cisco AS5800, shelf values range from 0 to 1, slot values range from 2 to 11, and port values range from 0 to 323. You must include the slash marks.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
11.3	The **test modem back-to-back** form of this command was introduced.
12.1(1)XD	This command was implemented on the Cisco AS5400.
12.1(3)T	This command was implemented on the Cisco AS5800.
12.1(5)XM1	This command was implemented on the Cisco AS5350.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5350.

Usage Guidelines

The **test port modem back-to-back** command should be performed on different combinations to determine a good port.

Note The **test port modem back-to-back** command is similar to the **test modem back-to-back** MICA technologies modem command.

Examples

The following example displays a back-to-back test:

```
Router# test port modem back-to-back 1/1/1

Repetitions (of 10-byte packets) [1]:
*Mar  02 12:13:51.743:%PM_MODEM_MAINT-5-B2BCONNECT:Modems (2/10) and (3/20) connected in
back-to-back test:CONNECT33600/V34/LAP
*Mar  02 12:13:52.783:%PM_MODEM_MAINT-5-B2BMODEMS:Modems (3/20) and (2/10) completed
back-to-back test:success/packets = 2/2
```

Related Commands

Command	Description
port modem autotest	Automatically and periodically performs a modem diagnostic test for modems inside the universal gateway or router.
port modem startup test	Performs diagnostic testing for all modems.
show port modem test	Displays the modem port history event log or modem test log.
test modem back-to-back	Diagnoses an integrated modem that may not be functioning properly.

timeout absolute

To specify a timeout period that controls the duration for which a session can be connected before it is terminated, use the **timeout absolute** command in interface configuration mode. To remove the session timeout period, use the **no** form of this command.

timeout absolute *minutes* [*seconds*]

no timeout absolute

Syntax Description

minutes	Session lifetime, in minutes. The range is 0 to 71582787.
seconds	(Optional) Session lifetime, in seconds. The range is 0 to 59.

Command Default

No timeout absolute parameter is set.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3	This command was introduced.

Examples

The following example shows how to impose a 15-minute (900-second) idle timeout and a 12-hour (720-minute) absolute timeout for session connections:

```
interface Serial0:23
 dialer idle-timeout 900
 timeout absolute 720
!
interface Serial1:23
 dialer idle-timeout 900
 timeout absolute 720
.
.
.
```

Related Commands

Command	Description
ppp idle timeout	Sets the PPP timeout idle parameter.
dialer idle-timeout	Specifies the idle time before the line is disconnected.

timer

To set the Redundant Link Manager (RLM) timer, use the **timer** command in RLM configuration mode. The associated options can overwrite the default setting of timeout values. To disable this function, use the **no** form of this command.

timer {**force-down** | **keepalive** | **minimum-up** | **open-wait** | **recovery** | **retransmit** | **switch-link**} *seconds*

no timer {**force-down** | **keepalive** | **minimum-up** | **open-wait** | **recovery** | **retransmit** | **switch-link**} *seconds*

Syntax Description

force-down	After RLM enters the down state, RLM will stay in the down state for a certain amount of time to make sure that the remote end will also enter the down state. After this occurs, both can be forced to be in sync again. This timer can also prevent RLM links from going up and down rapidly in an unstable network environment.
keepalive	A keepalive packet will be sent out from Network Access Server (NAS) to CSC periodically.
minimum-up	After a link is recovered from the failure state and RLM is in the up state, RLM will wait for a minimum time to make sure the new recovered link is stabilized before doing any operation.
open-wait	To overcome the latency while opening several links at the same time, RLM will use this timer to wait before opening the new links, and then choose the link with the highest weighting to become the active signaling link.
recovery	When the network access server (NAS) loses the active connection to CSC, it will try to reestablish the connection within the interval specified by this command. If it fails to reestablish the connection, RLM will declare that the RLM signaling link is down.
retransmit	Because RLM is operating under UDP, it needs to retransmit the control packet if the packet is not acknowledged within this retransmit interval.
switch-link	The maximum transition period allows RLM to switch from a lower preference link to a higher preference link. If the switching link does not complete successfully before this timer expires, RLM will go into the recovery state.
seconds	Time, in seconds, before executing the designated function. Valid values for the seconds argument range from 1 to 600 seconds.

Defaults

Disabled

Command Modes

RLM configuration

Command History

Release	Modification
11.3(7)	This command was introduced.

Examples

The following example configures a ten second retransmission timer for unacknowledged control packets:

```
timer retransmit 10
```

Related Commands

Command	Description
clear interface virtual-access	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
link (RLM)	Specifies the link preference.
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole rlm-group.
retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
server (RLM)	Defines the IP addresses of the server.
show rlm group statistics	Displays the network latency of the RLM group.
show rlm group status	Displays the status of the RLM group.
show rlm group timer	Displays the current RLM group timer values.
shutdown (RLM)	Shuts down all of the links under the RLM group.

trunk activate port-threshold

To specify the percentage of available port resources required to enable a trunk card transmitter, use the **trunk activate port-threshold** command in global configuration mode. To restore the default value, use the **no** form of this command.

trunk activate port-threshold *resource-percentage*

no trunk activate

Syntax Description

resource-percentage	Decimal integer from 0 through 100 that indicates the percentage of universal port Dial Feature Card (DFC) resources required before a trunk line is enabled.

Command Default

No resource percentage is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the **trunk activate port-threshold** command if you have a CT3 DFC and one or more universal port DFCs on the same platform and calls are dropped at system startup. This command enables the universal port modules to initialize before calls are routed to the platform. If the universal port modules do not initialize, the platform is identified as unavailable and calls are dropped.

Examples

The following example shows how to set the port threshold for the trunk card to 70 percent:

```
Router(config)# trunk activate port-threshold 70
```

trunk group (global)

To define or modify the definition of a trunk group and to enter trunk group configuration mode, use the **trunk group** command in global configuration mode. To delete the trunk group, use the **no** form of this command.

trunk group *name*

no trunk group *name*

Syntax Description

name	Name of the trunk group. Valid names contain a maximum of 63 alphanumeric characters.

Command Default

No trunk group is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

Use the **trunk group** command to assign a number or a name to a set of trunk characteristics. The set of characteristics, or *profile*, is assigned to specific trunks as part of the usual trunk configuration steps.

The **trunk group** command initiates the profile definition and switches from global configuration to trunk group configuration mode. Additional commands are available to construct the characteristics of the profile.

Up to 1000 trunk groups can be configured on the gateway provided that the gateway has sufficient memory to store the profiles. If you see the message "Trunk group name could not be added as the threshold has been reached", enter the **debug tgrm** command and check the number of trunk groups or check for insufficient memory.

To associate a trunk group with an interface, use the **trunk-group** (interface) command. A trunk group that was created using the **trunk group** (global) command can be associated with an interface. However, a trunk group need not be defined globally before being associated with an interface. If a trunk group has not been defined globally, it will be created by issuing the **trunk-group** (interface) command.

Examples

The following example creates trunk group 5 and configures the trunk group profile:

```
Router(config)# trunk group 5
Router(config-trunk-group)# carrier-id allcalls
Router(config-trunk-group)# max-calls voice 500 in
Router(config-trunk-group)# hunt-scheme round-robin even up
Router(config-trunk-group)# translation-profile incoming 3
Router(config-trunk-group)# translation-profile outgoing 2
Router(config-trunk-group)# exit
```

The following example creates a trunk group named “mytrunk” and configures the trunk group profile:

```
Router(config)# trunk group mytrunk
Router(config-trunk-group)# carrier-id local
Router(config-trunk-group)# max-calls voice 500
Router(config-trunk-group)# hunt-scheme least-idle
Router(config-trunk-group)# translation-profile incoming 1
Router(config-trunk-group)# translation-profile outgoing 12
Router(config-trunk-group)# exit
```

Related Commands

Command	Description
carrier-id (trunk group)	Identifies the carrier that owns the trunk group.
description (trunk group)	Permits a description to be associated with a trunk group.
hunt-scheme least-idle	Specifies the least-idle channel search method for incoming and outgoing calls.
hunt-scheme least-used	Specifies the least-used channel search method for incoming and outgoing calls.
hunt-scheme longest-idle	Specifies the longest-idle channel search method for incoming and outgoing calls.
hunt-scheme random	Specifies the random channel search method for incoming and outgoing calls.
hunt-scheme round-robin	Specifies the round-robin channel search method for incoming and outgoing calls.
hunt-scheme sequential	Specifies the sequential channel search method for incoming and outgoing calls.
max-calls	Specifies the number of incoming and outgoing voice and data calls that a trunk group can handle.
show trunk group	Displays the configuration of trunk groups.
translation-profile (trunk group)	Defines call number translation profiles for incoming and outgoing calls.
trunk-group (interface)	Assigns an ISDN PRI or NFAS interface to a trunk group.

trunk-group (timeslots)

To direct an outbound synchronous or asynchronous call initiated by dial-on-demand routing (DDR) to use specific B or digital service 0 (DS0) channels of an ISDN circuit on Cisco AS5800 series access servers, use the **trunk-group** command in CAS custom configuration, controller configuration, or interface configuration mode. To delete DS0s from the trunk group, use the **no** form of this command.

trunk-group *name* [**timeslots** *timeslot-list* [**preference** *preference-number*]]

no trunk-group *name* [**timeslots** *timeslot-list* [**preference** *preference-number*]]

Syntax Description

name	Trunk group name or label.
timeslots *timeslot-list*	(Optional) Selectively adds one or more DS0s from a DS1 to a trunk group. The *timeslot-list* argument accepts DS0s numbered from 1 to 24 for T1 links, and from 1 to 15 and 17 to 31 for E1 links. Successive DS0 numbers can be specified using commas, and ranges of numbers can be specified using a hyphen to separate the numbers. Groups of ranges can also be entered separated by commas. Default is that all DS0s in the signaling circuit are assigned to the trunk group.
preference *preference-number*	(Optional) Assigns a preference for DS0 members in a trunk group. Range is from 1 (highest preference) to 64 (lowest preference). The **preference** keyword appears only when the **timeslots** keyword has been used to configure DS0s.

Command Default

All DS0s in the signaling circuit are assigned to the trunk group.

Command Modes

CAS custom configuration
Controller configuration
Interface configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

Dial-out trunk groups can include individual DS0s from more than one DS1.

Two types of DS0 resources can be pooled: DS0s from common channel signaling circuits (CCS) such as PRI, Non-Facility Associated Signaling (NFAS), Signaling System 7 (SS7), and so on, and DS0s from channel-associated signaling (CAS) circuits.

The large-scale dial-out architecture is an integral part of dial-out trunk groups. The large-scale dial-out architecture is based on dialer rotary groups where physical interfaces are statically bound to dialer interfaces, meaning that the physical interfaces inherit the configuration parameters of the dialer interface. A call placed using a specific dialer interface (dialer rotary) can be done only through a rotary member, and this same rule applies to DDR over DS0 trunk groups.

As an example, a trunk group can have DS0s from three different physical interfaces that are also rotary members of a dialer interface. When an outgoing call is placed through the dialer interface, the Trunk Group Resource Manager (TGRM) provides a DS0 that belongs to a physical interface. The call will fail, however, if the physical interface is *not* a rotary member of a dialer interface. See the "Examples" section for more about the limitations large-scale dial-out places on selecting DS0s from physical interfaces.

The large-scale dial-out framework is used to place outgoing calls over a synchronous or asynchronous line. The framework also enables provisioning of dial-out configurations on an authentication, authorization, and accounting (AAA) server. A trunk group label can be configured as part of a **dialer string** command, or the large-scale dial-out framework can be used to download the trunk group identifier along with the dialer string.

Examples

CAS Configurations

The following examples show how to configure DS0 trunk groups on a CAS:

Example 1

```
Router(config)# controller t1 0
Router(config-controller)# ds0-group 2 timeslots 1-24
Router(config-controller)# cas-custom 2
Router(config-ctrl-cas)# trunk-group label3 timeslots 1-12
```

Example 2

```
Router(config)# controller t1 1
Router(config-controller)# ds0-group 3 timeslots 1-24
Router(config-controller)# cas-custom 3
Router(config-ctrl-cas)# trunk-group label1 timeslots 1-5,17-23 preference 1
Router(config-ctrl-cas)# trunk-group label2 timeslots 6-8,10-12,15 preference 2
```

NFAS Configuration

The following example shows how to configure NFAS/SS7 circuits. With these circuits, signaling can take place over a circuit different than the one over which the data is being transported. The DS0 dial-out trunk group configuration is done in controller configuration mode, because the trunk group is configured under the NFAS primary serial interface, all the NFAS group interface member DS0s are added into the trunk group. The NFAS primary serial interface will *not* have the **timeslots** keyword enabled under its configuration mode. The **timeslots** option is not available in the serial interface configuration mode because a serial interface may represent an NFAS serial interface. Remember that trunk group configurations under the NFAS member controllers and the respective serial interface (D channel) are mutually exclusive.

```
Router(config)# controller T1 0
Router(config-controller)# pri-group timeslots 1-24 nfas_d primary nfas_int 0 nfas_group 0
Router(config-controller)# trunk-group L1 timeslots 1-5 preference 1
Router(config-controller)# trunk-group L2 timeslots 12-14 preference 2
Router(config-controller)# exit
Router(config)# controller T1 1
Router(config-controller)# pri-group timeslots 1-24 nfas_d backup nfas_int 1 nfas_group 0
Router(config-controller)# trunk-group L3 timeslots 1-5
Router(config-controller)# trunk-group L4 timeslots 12-14 preference 4
Router(config-controller)# exit
Router(config)# controller T1 3
Router(config-controller)# pri-group timeslots 1-24 nfas_d none nfas_int 2 nfas_group 0
Router(config-controller)# trunk-group L5 timeslots 7,9,11
Router(config-controller)# trunk-group L6 timeslots 2,4,6,14-16 preference 6
.
.
.
```

Configuring and Associating DS0 Trunk Groups for DDR

The following examples show how to configure the dialer interface and apply a static dial-out trunk configuration on the NAS.

The following example configures a static trunk group dialer association on the NAS:

```
Router(config)# interface dialer 0
Router(config-if)# dialer string 5550112 trunkgroup trunkgroup1
```

The following example configures a static dial-out trunk group on the NAS:

```
Router(config)# controller T1 6/1
Router(config-controller)# framing esf
Router(config-controller)# linecode b8zs
Router(config-controller)# pri-group timeslots 1-24
Router(config-controller)# trunk-group 16 timeslots 1,21-22 preference 1
Router(config-controller)# trunk-group 15 timeslots 18-19
```

The following example configures a dial-out trunk group Cisco AVPair:

```
Cisco-AVPair = "outbound:trunkgroup=number"
```

Dial-Out Trunk Groups in Dialer Rotary Configurations

In the following examples, dial-out trunk groups 15 and 16 have DS0s from PRI interfaces 0:23 and 6:23. These interfaces are also rotary members of dialer interface 0, and are configured correctly for dial-out trunk groups and outbound calling.

The following example configures the AAA server:

```
dialout-out Password="cisco"
    Cisco-AVPair = "outbound:trunkgroup=16"
    Service-Type = Outbound,
    Cisco:AVPair = "outbound:addr*10.121.94.254",
    Cisco:AVPair = "Outbound:dial-number=5551212",

RAS-5400-1 Password="cisco"
    Service-Type = Outbound,
    Framed-Route="10.121.94.254/32 Dialer0 200 name dialout"
    Framed-Route="10.121.94.0/24 10.121.94.254 200"
```

The following example configures a static dial-out trunk group on the NAS:

```
Router(config)# controller t1 0
Router(config-controller)# pri-group timeslots 1-24
Router(config-controller)# trunk-group 16 timeslots 1,21-22 preference 1
Router(config-controller)# trunk-group 15 timeslots 18-19
.
.
.
Router(config)# interface serial 0:23
Router(config-if)# dialer rotary-group 0
Router(config-if)# exit
Router(config)# controller t1 6
Router(config-controller)# pri-group timeslots 1-24
Router(config-controller)# trunk-group 16 timeslots 21-22
Router(config-controller)# trunk-group 15 timeslots 18-19 preference 2
.
.
.
Router(config)# interface serial 6:23
Router(config-if)# dialer rotary-group 0
```

In the following example, trunk group 15 has member DS0s from PRI interfaces 0:23, 6:23, and 7:23. When an outgoing call is placed through interface dialer 0, TGRM could return a DS0 that belongs to physical interfaces serial 6:23 or serial 7:23, which are not part of the same rotary group as serial 0:23. Because these physical serial interfaces are not rotary members of interface dialer 0, the call will fail.

The following example configures the AAA server incorrectly:

```
dialout-out Password="cisco"
    Cisco-AVPair = "outbound:trunkgroup=16"
    Service-Type = Outbound,
    Cisco-AVPair = "outbound:addr*10.121.94.254",
    Cisco-AVPair = "Outbound:dial-number=5551212",

RAS-5400-1 Password="cisco"
    Service-Type = Outbound,
    Framed-Route="10.121.94.254/32 Dialer0 200 name dialout"
    Framed-Route="10.121.94.0/24 10.121.94.254 200"
.
.
.
```

The following example configures the static dial-out trunk group on the NAS incorrectly:

```
Router(config)# controller t1 0
Router(config-controller)# pri-group timeslots 1-24
Router(config-controller)# trunk-group 15 timeslots 1,21-22 preference 1
Router(config-controller)# trunk-group 16 timeslots 18-19
Router(config-controller)# exit
Router(config)# interface serial 0:23
Router(config-if)# dialer rotary-group 0
Router(config-if)# exit
Router(config)# controller t1 6
Router(config-controller)# pri-group timeslots 1-24
Router(config-controller)# trunk-group 15 timeslots 21-22
Router(config-controller)# trunk-group 16 timeslots 18-19 preference 2
Router(config-controller)# exit
Router(config)# interface serial 6:23
Router(config-if)# dialer rotary-group 1
Router(config-if)# exit
Router(config)# controller t1 7
Router(config-controller)# pri-group timeslots 1-24
Router(config-controller)# trunk-group 15 timeslots 18-19
Router(config-controller)# exit
Router(config)# interface serial 7:23
Router(config-if)# dialer rotary-group 1
```

Related Commands

Command	Description
dialer rotary group	Includes a specified interface in a dialer rotary group.
dialer string trunkgroup	Specifies a dial-out telephone number and dial-out trunk group name for a static configuration on an NAS.
pri-group timeslots	Specifies an ISDN PRI group on a channelized T1 or E1 controller, and releases the ISDN PRI signaling time slot.
show trunk group	Displays the configuration of a trunk group.

tunnel

To set up a network layer connection to a router, use the **tunnel** command in EXEC mode.

tunnel *host*

Syntax Description

host	Name or IP address of a specific host on a network that can be reached by the router.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

If you are a mobile user, it is often impractical to dial in to your "home" router from a remote site. The asynchronous mobility feature allows you to dial in to different routers elsewhere on the internetwork while experiencing the same server environment that you would if you were connecting directly to your home router.

This asynchronous host mobility is accomplished by packet tunneling, a technique by which raw data from the dial-in user is encapsulated and transported directly to the host site where your home router performs the actual protocol processing.

You enable asynchronous mobility by entering the **tunnel** command to set up a network layer connection to a specified host. From a router other than a Cisco router, however, you need to use the Telnet protocol.

After a connection is established, you receive an authentication dialog or prompt from your home router and can proceed as if you are connected directly to it. When communications are complete, the network connection can be closed and terminated from either end of the connection.

Examples

The following example establishes a network layer connection with an IBM host named mktg:

```
Router> tunnel mktg
```

virtual-profile aaa

Note Effective with Cisco IOS Release 12.2, the **virtual-profile aaa** command is not available in Cisco IOS software.

To enable virtual profiles by authentication, authorization, and accounting (AAA) configuration, use the **virtual-profile aaa** command in global configuration mode. To disable virtual profiles, use the **no** form of this command.

virtual-profile aaa

no virtual-profile aaa

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2F	This command was introduced.
12.0(7)T	This command was enhanced to allow virtual profiles to be downloaded from an AAA server using the High-Level Data Link Control (HDLC), Link Access Procedure, Balanced-terminal adapter (LAPB-TA), X.25, and Frame Relay encapsulations, in addition to the originally supported PPP encapsulation.
12.2	This command was removed.

Usage Guidelines

The effect of this command for any specific user depends on the router being configured for AAA and the AAA server being configured for that user's specific configuration information.

In releases later than Cisco IOS Release 12.2, the router automatically creates virtual profiles when AAA attributes require a profile.

Examples

The following example configures virtual profiles by AAA configuration only:

```
virtual-profile aaa
```

Related Commands

Command	Description
aaa authentication	Enables AAA authentication to determine if a user can access the privileged command level.
virtual-profile if-needed	Enables virtual profiles by virtual interface template.

virtual-profile if-needed

To specify that a virtual profile be used to create a virtual access interface only if the inbound connection requires a virtual access interface, use the **virtual-profile if-needed** command in global configuration mode. To create virtual access interfaces for every inbound connection, use the **no** form of this command.

virtual-profile if-needed

no virtual-profile if-needed

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

This command is intended to prevent the creating of virtual-access interfaces for inbound calls on physical interfaces that do not require virtual-access interfaces.

This command is compatible with local, RADIUS, and TACACS+ AAA.

Examples

The following example enables selective virtual-access interface creation:

```
virtual-profile if-needed
```

Related Commands

Command	Description
interface virtual-template	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.
virtual-profile aaa	Enables virtual profiles by AAA configuration.
virtual-profile virtual-template	Enables virtual profiles by virtual interface template.

virtual-profile virtual-template

To enable virtual profiles by virtual interface template, use the **virtual-profile virtual-template** command in global configuration mode. To disable this function, use the **no** form of this command.

virtual-profile virtual-template *number*

no virtual-profile virtual-template *number*

Syntax Description

number	Number of the virtual template to apply, ranging from 1 to 30.

Command Default

Disabled. No virtual template is defined, and no default virtual template number is used.

Command Modes

Global configuration

Command History

Release	Modification
11.2F	This command was introduced.

Usage Guidelines

When virtual profiles are configured by virtual templates only, any interface-specific configuration information that is downloaded from the AAA server is ignored in configuring the virtual access interface for a user.

The **interface virtual-template** command defines a virtual template to be used for virtual profiles. Because several virtual templates might be defined for different purposes on the router (such as MLP, PPP over ATM, and virtual profiles), it is important to be clear about the virtual template number to use in each case.

Examples

The following example configures virtual profiles by virtual templates only. The number 2 was chosen because virtual template 1 was previously defined for use by Multilink PPP.

```
virtual-profile virtual-template 2
```

Related Commands

Command	Description
interface virtual-template	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.

vty-async

To configure all virtual terminal lines on a router to support asynchronous protocol features, use the **vty-async** command in global configuration mode. To disable asynchronous protocol features on virtual terminal lines, use the **no** form of this command.

vty-async

no vty-async

Syntax Description

This command has no arguments or keywords.

Command Default

By default, asynchronous protocol features are not enabled on virtual terminal lines.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The **vty-async** command extends asynchronous protocol features from physical asynchronous interfaces to virtual terminal lines. Normally, SLIP and PPP can function only on asynchronous interfaces, not on virtual terminal lines. However, extending asynchronous functionality to virtual terminal lines permits you to run SLIP and PPP on these *virtual asynchronous interfaces*. One practical benefit is the ability to tunnel SLIP and PPP over X.25 PAD, thus extending remote node capability into the X.25 area. You can also tunnel SLIP and PPP over Telnet or LAT on virtual terminal lines. To tunnel SLIP and PPP over X.25, LAT, or Telnet, you use the protocol translation feature in the Cisco IOS software.

To tunnel SLIP or PPP inside X.25, LAT, or Telnet, you can use two-step protocol translation or one-step protocol translation, as follows:

- If you are tunneling SLIP or PPP using the two-step method, you need to first enter the **vty-async** command. Next, you perform two-step translation.
- If you are tunneling SLIP or PPP using the one-step method, you do not need to enter the **vty-async** command. You need to issue only the **translate** command with the SLIP or PPP keywords, because the **translate** command automatically enables asynchronous protocol features on virtual terminal lines.

Examples

The following example enables asynchronous protocol features on virtual terminal lines:

```
vty-async
```

Related Commands

Command	Description
ppp	Starts an asynchronous connection using PPP.
slip	Starts a serial connection to a remote host using SLIP.
translate	Enables asynchronous protocol features on virtual terminal lines.

vty-async dynamic-routing

To enable dynamic routing on all virtual asynchronous interfaces, use the **vty-async dynamic-routing** command in global configuration mode. To disable asynchronous protocol features on virtual terminal lines, and therefore disable routing on virtual terminal lines, use the **no** form of this command.

vty-async dynamic-routing

no vty-async dynamic-routing

Syntax Description

This command has no arguments or keywords.

Command Default

Dynamic routing is not enabled on virtual asynchronous interfaces.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

This feature enables IP routing on virtual asynchronous interfaces. When you issue this command and a user later makes a connection to another host using SLIP or PPP, the user must specify **/routing** on the SLIP or PPP command line.

If you had not previously entered the **vty-async** command, the **vty-async dynamic-routing** command creates virtual asynchronous interfaces, and then enables dynamic routing on them.

Examples

The following example enables dynamic routing on virtual asynchronous interfaces:

```
vty-async dynamic-routing
```

Related Commands

Command	Description
async dynamic routing	Enables manually configured routing on an asynchronous interface.
vty-async	Enables manually configured routing on an asynchronous interface.

vty-async header-compression

To compress the headers of all TCP packets on virtual asynchronous interfaces, use the **vty-async header-compression** command in global configuration mode. To disable virtual asynchronous interfaces and header compression, use the **no** form of this command.

vty-async header-compression [**passive**]

no vty-async header-compression

Syntax Description

passive	(Optional) Outgoing packets are compressed only when TCP incoming packets on the same virtual asynchronous interface are compressed. For SLIP, if you do not specify this option, the Cisco IOS software will compress all traffic. The default is no compression. For PPP, the Cisco IOS software always negotiates header compression.

Defaults

Header compression is not enabled on virtual asynchronous interfaces.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

This feature compresses the headers on TCP/IP packets on virtual asynchronous connections to reduce the size of the packets and to increase performance.This feature only compresses the TCP header, so it has no effect on UDP packets or other protocol headers. The TCP header compression technique, described fully in RFC 1144, is supported on virtual asynchronous interfaces using SLIP or PPP encapsulation. You must enable compression on both ends of a connection.

Examples

The following example compresses outgoing TCP packets on virtual asynchronous interfaces only if incoming TCP packets are compressed:

```
vty-async header-compression passive
```

Related Commands

Command	Description
async dynamic routing	Enables manually configured routing on an asynchronous interface.

vty-async ipx ppp-client loopback

To enable IPX-PPP on virtual terminal lines, use the **vty-async ipx ppp-client loopback** command in global configuration mode. To disable IPX-PPP sessions on virtual terminal lines, use the **no** form of this command.

vty-async ipx ppp-client loopback *number*

no vty-async ipx ppp-client loopback

Syntax Description

number	Number of the loopback interface configured for IPX to which the virtual terminal lines are assigned.

Command Default

IPX over PPP is not enabled on virtual terminal lines.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

This command enables users to log into the router from a device running a virtual terminal protocol, then issue the PPP command at the EXEC prompt to connect to a remote device.

A loopback interface must already have been defined and an IPX network number must have been assigned to the loopback interface before the **vty-async ipx ppp-client loopback** command will permit IPX–PPP on virtual terminal lines.

Examples

The following example enables IPX over PPP on virtual terminal lines:

```
ipx routing
interface loopback0
 ipx network 12345
vty-async ipx ppp-client loopback0
```

Related Commands

Command	Description
interface loopback	Creates a loopback interface.
ipx network	Enables IPX routing on a particular interface and optionally selects the type of encapsulation (framing).

vty-async keepalive

To change the frequency of keepalive packets on all virtual asynchronous interfaces, use the **vty-async keepalive** command in global configuration mode. To disable asynchronous protocol features on virtual terminal lines, use the **no vty-async keepalive** command. To disable keepalive packets on virtual terminal lines, use the **vty-async keepalive 0** command.

vty-async keepalive *seconds*

no vty-async keepalive

vty-async keepalive 0

Syntax Description

seconds	Frequency, in seconds, with which the Cisco IOS software sends keepalive messages to the other end of a virtual asynchronous interface. To disable keepalive packets, use a value of 0. The active keepalive interval range is 1 to 32767 seconds. Keepalive is disabled by default.

Command Default

Keepalive is disabled.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

Use this command to change the frequency of keepalive updates on virtual asynchronous interfaces, or to disable keepalive updates. To determine if keepalive is enabled on an interface, use the **show running-config** command. If the router has not received a keepalive packet after three update intervals have passed, the connection is considered down.

Examples

The following example sets the keepalive interval to 30 seconds:

```
vty-async keepalive 30
```

The following example sets the keepalive interval to 0 (off):

```
vty-async keepalive 0
```

Related Commands

Command	Description
keepalive	Sets the keepalive timer for a specific interface.
show running-config	Displays the contents of the currently running configuration file.

vty-async mtu

To set the maximum transmission unit (MTU) size on virtual asynchronous interfaces, use the **vty-async mtu** command in global configuration mode. To disable asynchronous protocol features on virtual terminal lines, use the **no** form of this command.

vty-async mtu *bytes*

no vty-async

Syntax Description

bytes	MTU size of IP packets that the virtual asynchronous interface can support. The default MTU is 1500 bytes. Valid values for the MTU range from 64 bytes to 1000000 bytes.

Command Default

1500 bytes

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

Use this command to modify the MTU for packets on a virtual asynchronous interfaces. You might want to change to a smaller MTU size for IP packets transmitted on a virtual terminal line configured for asynchronous functions for any of the following reasons:

- The SLIP or PPP application at the other end only supports packets up to a certain size.
- You want to ensure a shorter delay by using smaller packets.
- The host echoing takes longer than 0.2 seconds.

Do not change the MTU size unless the SLIP or PPP implementation running on the host at the other end of the virtual asynchronous interface supports reassembly of IP fragments. Because each fragment occupies a spot in the output queue, it might also be necessary to increase the size of the SLIP or PPP hold queue if your MTU size is such that you might have a high amount of packet fragments in the output queue.

Examples

The following example sets the MTU for IP packets to 256 bytes:

```
vty-async mtu 256
```

Related Commands

Command	Description
mtu	Adjusts the maximum packet size or MTU size.

vty-async ppp authentication

To enable PPP authentication on virtual asynchronous interfaces, use the **vty-async ppp authentication** command in global configuration mode. To disable PPP authentication, use the **no** form of this command.

vty-async ppp authentication {**chap** | **pap**}

no vty-async ppp authentication {**chap** | **pap**}

Syntax Description

chap	Enables CHAP on all virtual asynchronous interfaces.
pap	Enables PAP on all virtual asynchronous interfaces.

Command Default

No CHAP or PAP authentication for PPP.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

This command configures the virtual asynchronous interface to either authenticate CHAP or PAP while running PPP. After you have enabled CHAP or PAP, the local router requires a password from remote devices. If the remote device does not support CHAP or PAP, no traffic will be passed to that device.

Examples

The following example enables CHAP authentication for PPP sessions on virtual asynchronous interfaces:

```
vty-async ppp authentication chap
```

Related Commands

Command	Description
ppp bap call	Sets PPP BACP call parameters.
ppp use-tacacs	Enables TACACS for PPP authentication.
vty-async	Configures all virtual terminal lines on a router to support asynchronous protocol features.
vty-async ppp use-tacacs	Enables TACACS authentication for PPP on virtual asynchronous interfaces.

vty-async ppp use-tacacs

To enable TACACS authentication for PPP on virtual asynchronous interfaces, use the **vty-async ppp use-tacacs** command in global configuration mode. To disable TACACS authentication on virtual asynchronous interfaces, use the **no** form of this command.

vty-async ppp use-tacacs

no vty-async ppp use-tacacs

Syntax Description

This command has no arguments or keywords.

Command Default

TACACS for PPP is disabled.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

This command requires the extended TACACS server.

After you have enabled TACACS, the local router requires a password from remote devices.

This feature is useful when integrating TACACS with other authentication systems that require a clear-text version of a user's password. Such systems include one-time password systems and token card systems.

If the username and password are contained in the CHAP password, the CHAP secret is not used by the router. Because most PPP clients require that a secret be specified, you can use any arbitrary string; Cisco IOS software ignores it.

You cannot enable TACACS authentication for SLIP on asynchronous or virtual asynchronous interfaces.

Examples

The example enables TACACS authentication for PPP sessions:

```
vty-async ppp use-tacacs
```

Related Commands

Command	Description
ppp use-tacacs	Enables TACACS for PPP authentication.
vty-async ppp authentication	Enables PPP authentication on virtual asynchronous interfaces.

vty-async virtual-template

To configure virtual terminal lines to support asynchronous protocol functions based on the definition of a virtual interface template, use the **vty-async virtual-template** command in global configuration mode. To disable virtual interface templates for asynchronous functions on virtual terminal lines, use the **no** form of this command.

vty-async virtual-template *number*

no vty-async virtual-template

Syntax Description

number	Virtual interface number.

Command Default

Asynchronous protocol features are not enabled by default on virtual terminal lines.

Command Modes

Global configuration

Command History

Release	Modification
10.3	The **vty-async** command was introduced.
11.3	The **vty-async virtual-template** command was introduced.

Usage Guidelines

The **vty-async virtual-template** command enables you to support tunneling of SLIP or PPP across X.25, TCP, or LAT networks by using two-step protocol translation.

Before issuing the **vty-async virtual-template** command, create and configure a virtual interface template by using the **interface virtual-template** command. Configure this virtual interface as a regular asynchronous serial interface. That is, assign the virtual interface template the IP address of the Ethernet interface, and configure addressing, just as on an asynchronous interface. You can also enter commands in interface configuration mode that compress TCP headers or configure CHAP authentication for PPP.

After creating a virtual interface template, apply it by issuing the **vty-async virtual-template** command. When a user dials in through a virtual terminal line, the router creates a virtual access interface, which is a temporary interface that supports the asynchronous protocol configuration specified in the virtual interface template. This virtual access interface is created dynamically, and is freed up as soon as the connection drops.

Before virtual templates were implemented, you could use the **vty-async** command to extend asynchronous protocol functions from physical asynchronous interfaces to virtual terminal lines. However, in doing so, you created a virtual asynchronous interface, rather than the virtual access interface. The difference is that the virtual asynchronous interfaces are allocated permanently, whereas the virtual access interfaces are created dynamically when a user calls in and closed down when the connection drops.

You can have up to 25 virtual templates interfaces, but you can apply only one template to vty-async interfaces on a router. There can be up to 300 virtual access interfaces on a router.

Examples

The following example enables asynchronous protocol features on virtual terminal lines:

```
vty-async
vty-async virtual-template 1
vty-async dynamic-routing
vty-async header-compression
!
interface virtual-template1
 ip unnumbered Ethernet0
 encapsulation ppp
 no peer default ip address
 ppp authentication chap
```

Related Commands

Command	Description
interface virtual-template	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.
ppp	Starts an asynchronous connection using PPP.
slip	Starts a serial connection to a remote host using SLIP.
translate lat	Translates a LAT connection request automatically to another outgoing protocol connection.
translate tcp	Translates a TCP connection request automatically to another outgoing protocol connection.
translate x25	Translates an X.25 connection request automatically to another outgoing protocol connection.
vty-async	Configures all virtual terminal lines on a router to support asynchronous protocol features.

x25 aodi

To enable the Always On/Dynamic ISDN (AO/DI) client on an interface, use the **x25 aodi** command in interface configuration mode. To remove AO/DI client functionality, use the **no** form of this command.

x25 aodi

no x25 aodi

Syntax Description

This command has no arguments or keywords.

Command Default

AO/DI client is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.3T	This command was introduced.

Usage Guidelines

Use this command to enable the AO/DI client on an interface.

Examples

The following example enables the AO/DI client on the interface running X.25, using the **x25 aodi** command:

```
interface bri0
 isdn x25 dchannel
 isdn x25 static-tei 8
interface bri0:0
 x25 aodi
 x25 address 12135551234
 x25 htc 4
 x25 win 3
 x25 wout 3
 x25 map ppp 12135556789 interface dialer 1
```

Note Configuring the BRI interface with the **isdn x25 dchannel** command creates a configurable interface (bri 0:0) for other necessary X.25 commands. Refer to the description for this command earlier in this publication for additional information about this command.

Related Commands

Command	Description
isdn x25 dchannel	Creates a configurable interface for X.25 traffic over the ISDN D channel.

x25 map ppp

To enable a PPP session over the X.25 protocol, use the **x25 map ppp** command in interface configuration mode. To remove a prior mapping, use the **no** form of this command.

x25 map ppp *x121-address* **interface** *cloning-interface* [**no-outgoing**]

no x25 map ppp *x121-address* **interface** *cloning-interface* [**no-outgoing**]

Syntax Description

x121-address	X.121 address as follows: • Client side—The calling number. • Server side—The called number.
interface *cloning-interface*	Interface to be used for cloning the configuration.
no-outgoing	(Optional) Ensures that the X.25 map does not originate calls.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.3T	This command was introduced.

Usage Guidelines

Use **x25 map ppp** command to allow a PPP session to run over X.25.

The **interface** keyword refers to the interface that will be used to clone the configuration.

Note For the **x25 map** command used in standard X.25 implementations, refer to the *Cisco IOS Wide-Area Networking Command Reference* publication.

Examples

Client Examples

The following example enables the AO/DI client on the interface and configures the D channel (BRI interface 0:0) with the x25 map statement in order to allow PPP sessions over X.25 encapsulation with the configured AO/DI server:

```
interface BRI0:0
 x25 address 16193368208
 x25 aodi
 x25 htc 4
 x25 win 3
 x25 wout 3
 x25 map ppp 16193368209 interface dialer 1
```

Server Examples

The following example enables the AO/DI server to receive calls from the AO/DI client and configures the D channel (BRI0:0) with the x25 map statement which allows PPP sessions over X.25 encapsulation with the configured AO/DI client. The **no-outgoing** option is used with the x.25 map command since the AO/DI server is receiving, versus initiating, calls.

```
interface BRI0:0
x25 address 16193368209
 x25 htc 4
 x25 win 3
 x25 wout 3
 x25 map ppp 16193368208 interface dialer 1 no-outgoing
```

Note Configuring the BRI interface with the **isdn x25 dchannel** command creates a configurable interface (bri 0:0).

Related Commands

Command	Description
isdn x25 dchannel	Creates a configurable interface for X.25 traffic over the ISDN D channel.