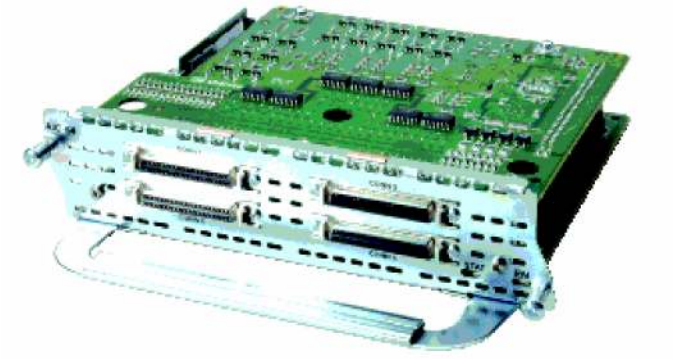
DATA SHEET

ALARM INTERFACE CONTROLLER NETWORK MODULE FOR THE CISCO 2600 AND 3600 SERIES

The Cisco NM-AIC-64 Network Module expands the capabilities of Service Provider and Enterprise networks by providing remote alarm monitoring and control of non-IP devices. By installing this network module into the Cisco Multi-service Access Routers or Integrated Services Routers, network managers have the capability of monitoring and controlling remote, unstaffed sites to provide increased security, reliability, and control of the network. For example, if a flood occurs at a service-provider remote site, the Alarm Interface Controller (AIC) issues an alarm. The network manager can then invoke a command to turn on a sump pump instead of wasting valuable time waiting for somebody to arrive at the facility. In the event of an unauthorized entry into a secure area, the AIC can initiate a visual and audible alarm. Further, if wired to a camera, the AIC can activate it for remote surveillance.

Figure 1. Cisco NM-AIC-64



The Cisco NM-AIC-64 is a network module that greatly expands the network monitoring and control capabilities of the Cisco Multi-service Access Routers or Integrated Services Routers. The AIC functions as an integrated entity, residing within the Cisco 26xx and 36xx routers to provide network alarm monitoring and remote control of network elements through contact closure. The AIC reduces service-provider and enterprise operating expenses by providing a flexible, low-cost integrated solution for migrating existing monitoring equipment onto a highly scalable IP-based solution from Cisco. The AIC facilitates a seamless solution, because it can be housed and configured in a Cisco IOS® Router, greatly simplifying network layout and management, and thereby reducing the high cost of operations, administration, maintenance, and provisioning (OAM&P). The AIC is supported starting with Cisco IOS 12.2 (2) XG & 12.2(8)T

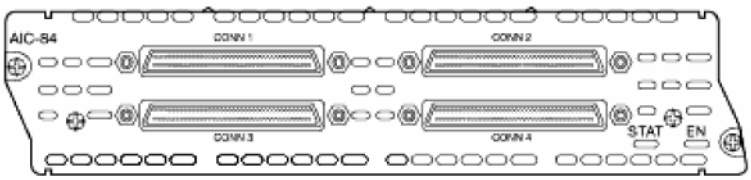
Each AIC can monitor 64 network elements, and remotely control 16 network elements. More than one AIC can be installed per router. For example, a Cisco 366x with its six network-module slots can accommodate up to six AICs, giving the Cisco 366x the ability to monitor up to 384 network elements and remotely control 96 network elements, all in one highly compact chassis

The AIC Network Module supports 64 discrete alarm inputs, of which 8 of the last 64 alarm points are software configurable to accept either analog or discrete inputs. The AIC further supports 16 control relays to facilitate the remote control of network elements. Each of the 64 discrete alarm inputs can be activated via ground or negative battery input. The negative battery range is -36V to -72V. The analog alarm input can be configured to monitor either DC voltage or current. It can measure voltage from -60V to 60V or current from 0 to 20 mA. The control relays can be utilized to remotely control simple network devices. These alarm inputs are configured in Cisco IOS Software. Some reportable events include:

- Network element alarm states
- Building security/intrusion detection (opening and closing of doors and windows)
- Building environmental factors (temperature and humidity)
- Commercial power (A/C) and central-office (CO) (D/C) power readings
- Fire and smoke detection
- Equipment alarm
- Temperature threshold violation
- Voltage fluctuation

The AIC converts relay contact alarm signals to Transaction Language One (TL-1) and Simple Network Management Protocol (SNMP) message formats, providing TL-1 over Transmission Control Protocol/Internet Protocol (TCP/IP) and SNMP protocols. When an event occurs, such as a door alarm or an open gate, the AIC maps the simple discrete and analog alarms to preprogrammed intelligent messages and transports the messages to destinations in the IP network, typically to a Network Operations Center (NOC). Generated either in TL-1 or in SNMP, these messages are used by an Operations Support System (OSS). All the contact closure-related alarms are routed and reported through the existing OSS and the associated OSS networks. The AIC sends the TL-1 or SNMP messages to the OSS autonomously or in response to TL-1 or SNMP commands from the OSS. The option to utilize TL-1 or SNMP is defined by the user, and it is software configurable on the AIC.

Figure 2. Alarm Interface Controller Network Module



CONNECTING THE CISCO NM-AIC-64 NETWORK MODULE TO THE NETWORK

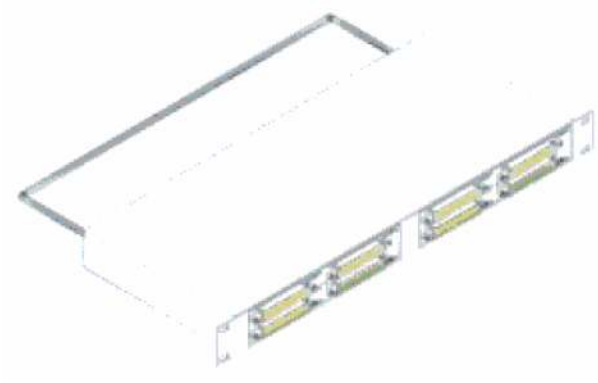
The alarm and remote-control features of the AIC are accessed via four female small computer serial interface (SCSI) II (Micro DB-50) interfaces (see Figure 2). A SCSI II (Micro DB-50) cable with male connectors is required to interface the female SCSI II interfaces on a AIC Network Module to a SCSI II-to-Telco-50 pin patch panel. Two different patch panels are available based on customer requirements (see Table 1). It is highly recommended that a patch panel be used in conjunction with the AIC. Figures 2 and 3 give examples of the two types of patch panels. SCSI cables and the recommended patch panels are not supplied with the network module; they are orderable separately as necessary. The recommended patch panels and cables are available either from Cisco Systems or Components Express (www.networkcable.com). (See Table 1 for part numbers).

Table 1. Accessory Patch Panels and cables for the AIC

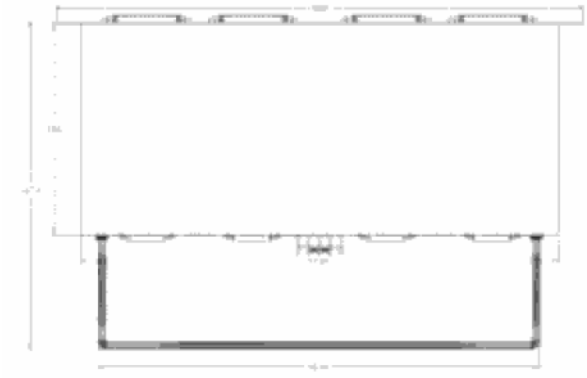
Part Number	Description
AIC-DBL-PNL	Patch panel for terminating up to two AIC or 128 alarm points
AIC-SGL-PNL	Patch panel with power monitoring terminals, for terminating one AIC with eight lugs and fuses for power monitoring
CAB-AIC-008	Set of four eight-foot-long male-to-male SCSI II interface cables

Figure 3. AIC-DBL-PNL: Interfaces up to two (2) Alarm Interface Controllers.

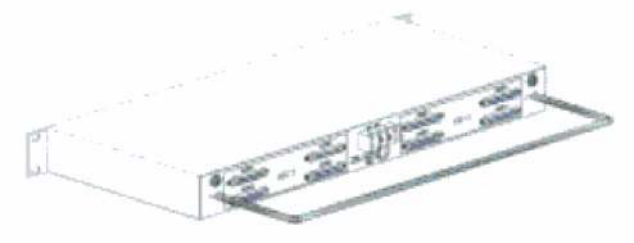
Isometric Front View



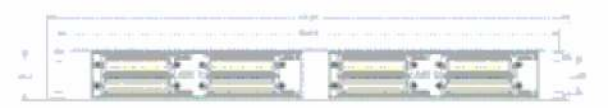
Top View



Isometric Back View



Front View

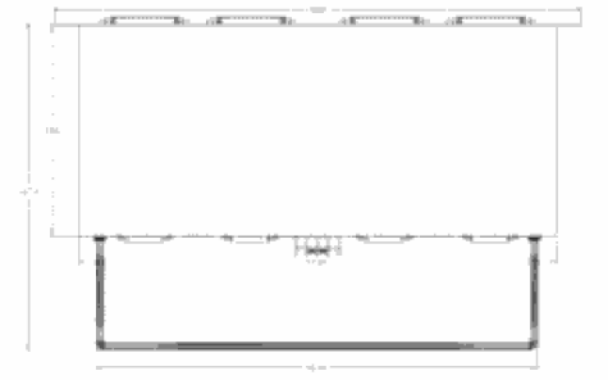


Back View

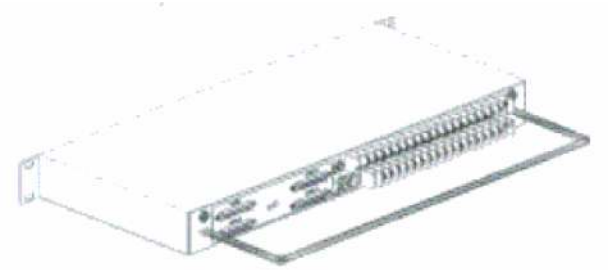
Figure 4. AIC-SGL-PNL: Panel with Voltage Monitoring.

Isometric Front View

Top View



Isometric Back View



Front View

Back View

AIC NETWORK MODULE LIGHT EMITTING DIODES

The AIC follows the convention of other network modules for light emitting diode (LED) operation. There are two LEDs—enable (EN) and status (STAT). Table 2 lists the network-module state indicated by the LEDs, and Figure 5 shows the placement of the LEDs.

Figure 5. AIC Network-Module LEDs

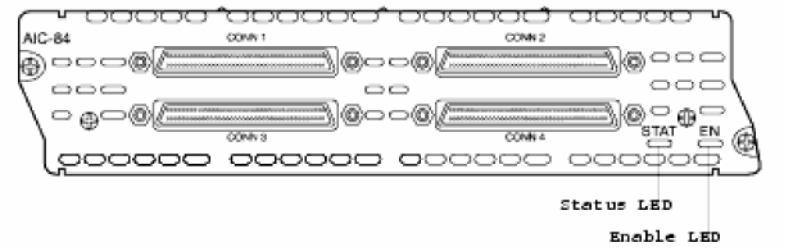


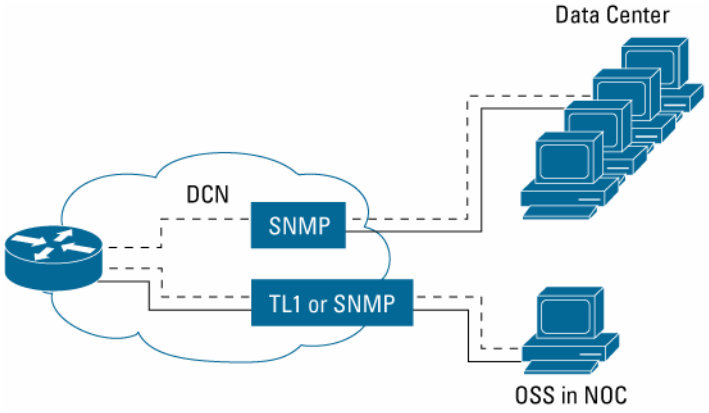
Table 2. AIC LED Description

STAT LED			
EN LED	**Green**	**Orange**	**Description**
Off	Off	Off	Power off to router
On	Off	Off	Software initializing
On	On	Off	Normal operation
On	Off	On	Fault encountered

INTERFACING THE AIC

When the AIC is incorporated into a DCN-Operations Support Network router, all the AIC contact-closure alarms are routed and reported through the same network and systems as the DCN router. This setup facilitates continued use of the existing OSS and its associated networks. A Cisco router with an AIC sends TL-1 or SNMP messages to the OSS autonomously or in response to TL-1 or SNMP commands from the OSS, as shown in Figure 6.

Figure 6. TL-1 and SNMP Message Flow in an Operations Support Network Application



SERIAL COMMUNICATION CHANNELS

The AIC has an embedded operating system that interfaces with the Cisco IOS Software in the router. Communication between the AIC operating system and Cisco IOS Software is accomplished through two serial communications channels, as illustrated in Figure 7:

- Serial data channel
- Asynchronous craft port

Serial Data Channel

The serial data channel supports all TCP/IP traffic to and from the AIC, including communication over IP with NOCs and data centers. The channel consists of one physical interface that provides support for the following applications:

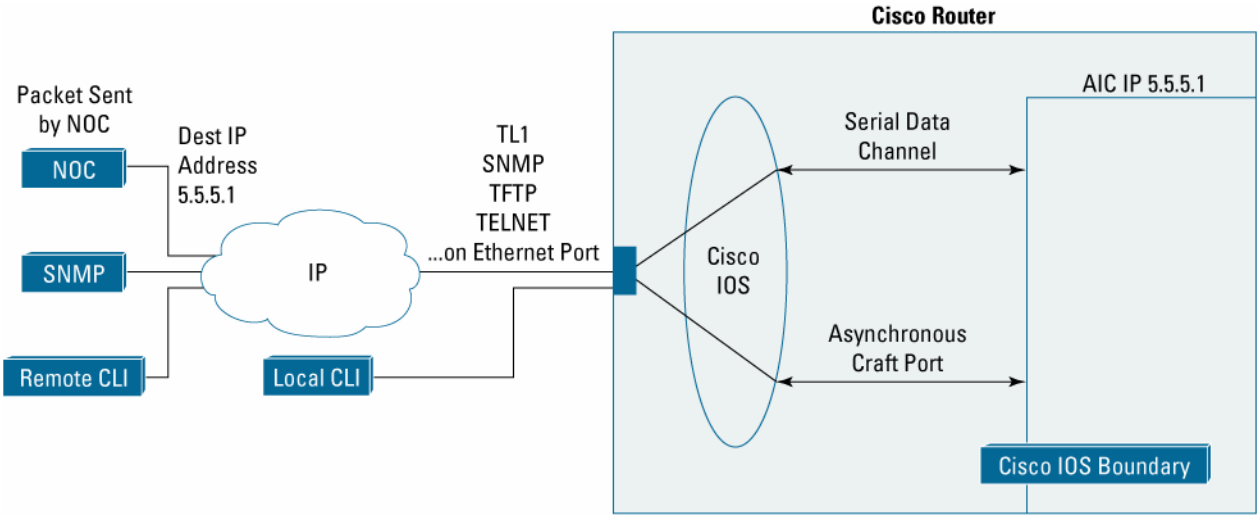
- *Telnet*—Used to communicate directly with the AIC OS and command-line interface (CLI)
- *TL-1*—Used to transport TL-1 messages between the NOC and the AIC
- *Trivial File Transfer Protocol (TFTP)*—Used to download firmware to the AIC
- *SNMP*—Used to transport SNMP traps between the Network Operations Center and the AIC

The Cisco IOS Software assigns an IP address to the AIC for use by the serial data channel. To route traffic, the serial data channel uses IP over synchronous High-Level Data Link Control (HDLC). All IP packets coming to the Cisco router with a destination IP address that matches the AIC IP address are forwarded to the serial data channel using IP over HDLC.

Asynchronous Craft Port

The asynchronous craft port supports Telnet to the AIC port number. This Telnet method, called local CLI, is useful for debugging when remote Telnet to the AIC IP address (remote CLI) is not applicable. The asynchronous craft port also supports an AIC boot sequence, similar to the ROM monitor in Cisco IOS Software, which allows the user to recover from a corrupted software image or configuration.

Figure 7. TOS Boundary into the AIC



SUPPORTED STANDARDS, MIBS, AND RFCS

Standards

The new standard that the AIC adds to the Cisco portfolio of protocols supported is Transaction Language One (TL-1).

MIBs

The AIC introduces a new Management Information Base (MIB) called CISCO-AIC-MIB. To support the AIC, an AIC object type and AIC ID have been added to the following MIBs:

- OLD-CISCO-CHASSIS-MIB
- CISCO-ENTITY-VENDORTYPE-OID-MIB

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB Web site on Cisco.com at: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Configuring Alarms

Alarms are configured using either TL-1 or AIC CLI. Information about TL-1 commands can be found in the Telcordia Technology (formerly Bellcore) document *Network Maintenance: Network Element and Transport Surveillance Messages*, GR-833-CORE, Issue 5, November 1996. For a reference of security-related commands (ACT-USER and CANC-USER), refer to *Telcordia Technology's Operations Applications Messages—Network Element and Network System Security Admin Messages*, TR-NWT-000835, Issue 2, January 1993.

AIC CLI Syntax

The AIC is designed to provide different privilege levels for separation of tasks among various personnel in a central office. Described in Table 3, these modes are designed to mimic the modes available at the Cisco CLI:

Table 3. AIC CLI Privilege Levels

Features	Description
User Mode `(Prompt: name >)`	The interface begins in user mode. This mode is not password protected, by default, although it may be configured to be. In user mode, commands that show information are available. Also available is the command for entering privileged mode.
Privileged Mode `(Prompt: name #)`	In privileged mode, configuration may be viewed and all user-mode commands are available. Also available are the commands for reentering user mode and entering configuration modes. Upon entrance to privileged mode, if one or more users are already using privileged mode (or any configuration mode), the entering user is warned that those other users may be configuring the AIC.
Global Configuration Mode `(Prompt: name (config)#)`	Global configuration mode allows configuration of global options and allows the user to enter the subconfiguration modes. The commands available here are not available in other modes. The prompt in this mode is the AIC name followed by config#.
Subconfiguration Modes `(Prompt: name (config-xxx)#)`	The subconfiguration modes are used for configuring specific parts of the AIC. Commands available in this mode are not available in other modes. Four subconfiguration modes are available: alarm, control, TL-1, and SNMP. The prompts in these modes are the AIC name followed by (config-alarm)#, (config-control)#, (config-tl1)#, and (config-snmp)#.

ORDERABILITY, AVAILABILITY, COMPATIBILITY, MINIMUM SOFTWARE, AND MEMORY REQUIREMENTS

Table 4. Product Specifications/Regulatory Approvals Part Number NM-AIC-64(=

Features	Description
Network Module Density	• 64 discrete alarm points – Up to 8 of the last 64 alarm points can be configured to accept analog or discrete inputs. • 16 relay control points
Cisco IOS Release	Cisco IOS 12.2 (2) XG and higher
Voltage Range Discrete Points	-36V to -72V
Analog Input Modes	Current sense or voltage sense
Voltage Sense Range—Analog Input	-60V to 60V
Current Sense Range	0 to 20 mA
Number of Network Modules Supported	• *Cisco 366x*—Six network modules or 384 contact points, and 96 relay controls • *Cisco 3640*—Three network modules or 192 contact points, and 48 relay controls • *Cisco 3631*—Two network modules or 128 contact points, and 32 relay controls • *Cisco 26xx*—One network module or 64 contact points, and 16 relay controls
Alarm Message Formats/Protocols Supported	*Configurable*—TL-1 (two sessions) or SNMP (four sessions) Alarm messages can be sent autonomous or upon being polled.
Connector Types	Four SCSI II Micro DB-50 female connectors
Recommended Patch Panels and Cables (See Table 1)	AIC-DBL-PNL, AIC-SGL-PNL, CAB-AIC-008
MIB Support	CISCO-AIC-MIB
Online Insertion and Removal (OIR) Support	Yes, on Cisco 366x 3745, and 3845 only
Standards and Compliance Support	Dimensions (H x W x D) 1.55 x 7.10 x 7.2 in.
Weight	1.1 lb maximum
Environmental Conditions	• Operating temperature: +32°to +104°F (0°to +40° C) • Nonoperating temperature: 13°to +158°F (25°to +7 0°C)
Power Requirements	10.7 watts
Maximum Relative Humidity	5 to 95 percent
Mean Time Between Failures (MTBF)	113,772 hours at 25°C ambient conditions
Emissions	• CISPR22:1997 [EN55022:1998] Class A 0.15-30MHz [dBuV/dBuA] Conducted Emissions • CISPR22:1997 [EN55022:1998] Class A 30MHz-1GHz [dBuV/m] Radiated Emissions
Immunity	• EN61000-4-2: 1995 Level 3 6kV Contact,8kV Air ESD • EN61000-4-3: 1997 Level 3 10V/m Radiated RF Susceptibility • EN61000-4-4: 1995 Level 4 2kV Burst/Transients • EN61000-4-4: 1995 Level 4 4kV Burst/Transients • EN61000-4-5: 1995 - 0.5kV/0.5kV Surges • EN61000-4-6: 1996 Level 3 10V Conducted RF Susceptibility • AS/NZS 3548: 1995 incorporating Amendments 1 and 2 • VCCIV-3/ 97.04 • 47 CFR 15 Subpart B: 1998

Features	Description
Additional Conformance	The NM-AIC-64 carries the CE mark for meeting the respective requirements. Additionally, meets AS/NZS 3548: 1995 for Australia.
Glossary AIC	*Alarm Interface Controller*
CAP	*Competitive access provider*
CLEC	*Competitive local exchange carrier*—In the United States, The Telecommunications Act of 1996 allowed CLECs/CAPs) to compete with the regional Bell operating companies (RBOCs) for local traffic. CLECs are frequently aggressive competitors who are trying to grow their networks quickly in order to gain market share. CLECs frequently partner with Tier 2/3 Internet service providers (ISPs). The CLEC provides the access portion of the network and delivers bulk traffic to the ISP. CLECs tend to focus on business customers.
DCN	*Data Communications Network*
IP	*Internet protocol*—IP is the Open System Interconnection (OSI) Layer 3 (the network layer protocol), which contains addressing information and some control information that allows packets to be routed. IP is a connectionless-orientated protocol that offers network services. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security. IP was originally developed by the Department of Defense (DoD) to support interworking of dissimilar computers across a network. This protocol works with TCP and is usually identified as TCP/IP. (See TCP/IP and OSI model; IP is documented in RFC 791.)
Cisco IOS Software	*Cisco Internet Operating System Software*—This software provides common functionality, scalability, and security for all products under the CiscoFusion architecture. Cisco IOS Software allows centralized integrated and automated installation and management of internetworks, while ensuring support for a wide variety of protocols, media, services, and platforms. See CiscoFusion.
NM	*Network module*
NOC	*Network Operating Center*
OSS	*Operation Support Systems*
SNMP	*Simple Network Management Protocol*—This TCP/IP protocol was built to serve as a communications channel for internetwork management operating at the application layer of the IP stack. TL-1 is a widely used management protocol for telecommunications developed by Telcordia Technologies' GRE833-CORE specification.
TCP	*Transmission Control Protocol*—TCP is the common name for the suite of protocols developed by the U.S. DoD in the 1970s to support the internetwork of dissimilar computers across the network and the construction of worldwide internetworks. TCP is a transport protocol that offers a connection-oriented transport service in the Internet suite of protocols. TCP provides transport level connections between hosts. It is designed to provide a reliable connection and handles error detection, lost packets, and packets that arrive out of sequence. It is also called TCP/IP because it uses IP. The entire collection of IP protocols is also frequently referred to as TCP/IP. Telnet uses TCP for its connections. TCP is a Layer 4 protocol that operates under IP to provide the sequencing, reliable transport, and the end-to-end connection of packets. Often, TCP and IP are used in the same context, TCP/IP. Some TCP-based protocols include: • TELNET X-WINDOWS • File Transfer Protocol Hypertext Transfer Protocol (FTP HTTP) • Simple Mail Transfer Protocol (SMTP) TCP is the reliable end-to-end protocol used on the Internet. It is a virtual circuit protocol in that when a connection is established between two endpoints, data flows only between those two endpoints until the connection is closed. TCP is defined in RFC-793. TCP and IP are the two best-known protocols in the suite. See also TCP/IP and IP.

Features	Description
TCP/IP	*The two best-known internet protocols, often erroneously thought of as one protocol*—The Transmission Control Protocol (TCP), which corresponds to Layer 4 (the transport layer) of the Open System Interconnection (OSI) reference model, provides reliable transmission of data. The Internet Protocol (IP) corresponds to Layer 3 (the network layer) of the OSI reference model and provides connectionless datagram service. TCP/IP were the internetworking protocols developed by the U.S. Department of Defense's Advanced Research Project Agency (ARPA) in the 1970s to support the construction of worldwide internetworks. TCP/IP has been widely adopted and supported by computer and software manufacturers as a standard computer networking protocol. It is a transport and interworking protocol that is an accepted networking standard. Commonly used over X.25 and Ethernet cabling, TCP/IP is viewed as one of the few protocols available that is able to offer a true migration path toward OSI. It was originally developed by the U.S. Department of Defense and is able to operate in most environments. TCP/IP operates as Layers 3 and 4 of the OSI model (network and transport, respectively). TCP/IP ensures that packets of data are delivered to their destination in the sequence in which they were transmitted. TCP/IP is also the delivery mechanism for associated services, including Simple Network Management Protocol (SNMP), Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP), and Telnet. TCP/IP protocols are the WAN protocols of choice. They include protocols that address media access, packet transport, session communication, file transfer, electronic mail, and terminal emulation. The main protocols in the suite include the following: • TELNET X-WINDOWS • File Transfer Protocol Hypertext Transfer Protocol (FTP HTTP) • Simple Mail Transfer Protocol (SMTP) TCP is the reliable end-to-end protocol used on the Internet. It is a virtual circuit protocol in that when a connection is established between two endpoints, data flows only between those two endpoints until the connection is closed. TCP is defined in RFC-793. TCP and IP are the two best-known protocols in the suite. See also TCP/IP and IP.
WIC	*Wide-area network (WAN) interface card*—The WIC can be placed in the network-module slot.

RELATED DOCUMENTS

For additional information, see the following documents:

Cisco Network Modules Hardware Installation Guide

NM-AIC-64, Contact Closure Network Module Feature Overview

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

205290.BJ_ETMG_CC_7.05

Printed in the USA