Wired Guest Access: Protect Your Network Against Threats

White Paper

October 2014

3.3.0 SE Release

Contents

What You Will Learn

In enterprise networks, there is typically a need for providing network access to its guests on the campus. The guest access requirements include providing connectivity to the Internet or other selective enterprise resources to both wired and wireless guests in a consistent and manageable way. The same wireless LAN controller can be used to provide access to both types of guests on the campus. For security reasons, a large number of enterprise network administrators segregate guest access to a demilitarized zone (DMZ) controller using tunneling. The guest access solution is also used as a fallback method for guest clients that fail dot1x and MAB authentication methods. Today, solutions exist for providing guest access through wireless and wired networks on the Cisco® AireOS Wireless LAN Controller (WLC).

This document covers deployment of the wired guest access feature on Cisco Catalyst® 3850 Series Switches. The Cisco 5760 Wireless LAN Controller is used as the guest anchor. Depending on the security requirements of the network, the network administrator can choose to implement the wired guest access feature in the following ways, which are described briefly later in this document:

- Open authentication mode
- Web consent mode
- Web authentication mode

Introduction

In modern networks, providing security to safeguard confidential information and assets has become a quintessential part of planning and implementation. The assets need to be secured against a variety of threats, including access to resources through wireless and wired networks. The wired guest access feature provides a high level of security by restricting access to only desired resources and the Internet.

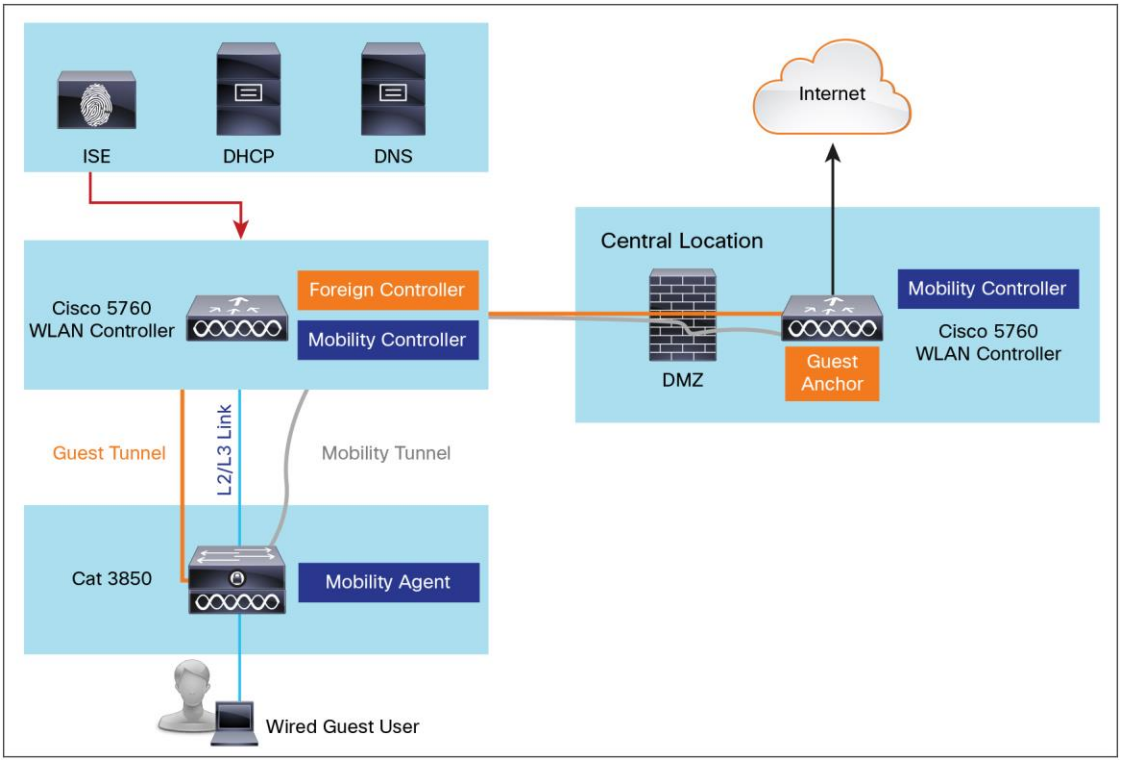
The guest user connects to the designated port for access and optionally might be made to go through web consent or web authentication modes, depending on the security requirements (details in later sections). After guest authentication succeeds, access is provided to the network resources, and the guest controller manages the client traffic. The foreign controller is the primary switch where the client connects for network access. It initiates tunnel requests. The guest anchor is the switch where the client actually gets anchored. Apart from the AireOS-based controllers, the Cisco IOS® Software-based Cisco 5760 WLC can also be used as a guest anchor. Before the guest access feature can be deployed, a mobility tunnel must be established between the foreign controller and guest anchor switches. A typical setup for the guest access feature would be mobility agent -> mobility controller (foreign controller) - mobility controller (guest anchor). The foreign controller switch anchors guest traffic to the guest anchor controller (preferably in a DMZ), and multiple guest anchors can be configured for load balancing. Get more information about mobility controllers and mobility anchors: http://www.cisco.com/c/en/us/td/docs/wireless/controller/5700/software/release/3se/mobility/configuration_guide/b_mobility_3se_5700_cg/b_mobility_32se_5700_cg_chapter_00.html.

For the guest feature, the ports on the foreign controller switch need to be configured in the Layer 2 access mode. The VLAN used on the switchport, depending on implementation, can be a separate VLAN altogether. It is up to the network administrator to have either a data VLAN or some other VLAN specifically for guests. A data VLAN can be used when other authentication methods are configured on the switchport and the guest access feature is used as a fallback method (for example, when other methods such as dot1x and MAB fail). This allows corporate end devices to connect to the same port using dot1x or MAB methods. Noncorporate or guest devices would fail the first two methods and fall back to the guest access method for Internet access. A different use case for using guest VLAN is when the network admin has dedicated few ports for guest access, which in turn warrants the use of guest VLAN on the switchport. The guest VLAN can be made nonroutable so that no traffic flows from it to other VLANs on the corporate network.

Deployment Scenario

This document covers common use cases in which the wired clients connect to access switches for network access. The three modes of access are explained in different examples. In all of the methods, the wired guest access feature can act as a fallback method for authentication. This is typically a use case in which a guest user brings an end device that is unknown to the network. Because the end device is missing an endpoint supplicant, it will fail dot1x authentication. Similarly, MAB authentication would also fail, because the MAC address of the end device would be unknown to the authenticating server. It is worth noting that in such implementations, corporate end devices would successfully get access because they would have either a dot1x supplicant or their MAC addresses in the authenticating server for validation. This allows for flexibility in deployment, because the administrator does not need to restrict and tie up ports specifically for guest access. Figure 1 shows the topology used in the deployment scenario.

Figure 1. Wired Guest Topology



The topology shown in Figure 1 represents a Cisco Catalyst 3850 access switch that is acting as a mobility agent where guest users plug in directly on the access port. The corresponding mobility controller is the Cisco 5760 WLC, local to the site. The local Cisco 5760 WLC connects to another Cisco 5760 WLC at the central location that acts as the guest anchor. The guest tunnels terminate on the guest anchor.

Deployment Modes

Depending on security requirements of the enterprise network, the administrator has the option of providing wired guest access to the Internet using different modes. Among the three methods discussed in this document, one can be implemented. This document assumes the wireless network is in place and the Cisco Catalyst 3850 is already working in a converged access setup. The three modes include open access mode, consent mode, and web authentication mode. This section briefly describes each of those modes.

It is worth noting that the guest LAN security configurations on both foreign controller and guest anchor must match for web consent and web authentication modes; otherwise the tunnel buildup process fails.

The following access modes are available:

- **Open mode:** Open mode allows guest user access to the Internet without requiring any form of consent or authentication.
- **Consent mode:** In consent mode, on connecting, the user is presented with a page to agree/disagree to certain terms of usage.
- **Web authentication mode:** In web authentication access method, the user is presented with a page to enter credentials, which can be provided by the network administrator on a temporary basis.

Configuration Guide

The following sections describe the series of steps that are involved in configuring various access methods on the guest anchor and foreign controller switches for various access modes.

Open, Consent, and WebAuth Mode: Step-by-Step Configuration Guide

In open mode, a guest user connecting to the switchport is given access to guest resources without requiring any form of authentication or consent. As soon as the client MAC address is detected on the port, an access session is started, and a tunnel request is initiated from the foreign controller switch to the guest anchor. After the process is complete, the client is able to access the guest resources. It is typically used when the physical location of the Ethernet ports is in a trustworthy environment and, optionally, the area is secured by other means of physical security.

Consent mode allows access to the network resources only on agreement of terms and conditions by the guest user, as set by the enterprise policy. The tunnel buildup process in consent mode is similar to open mode, but authorization for network access is only provided when the guest user acknowledges the policies of network usage. The user is presented with a splash page that lists the terms of use and might have optional fields for entering the guest email address. Consent mode is usually used as an additional way of making sure that guest users comply with the enterprise network usage policies.

In web authentication mode, a guest user coming on the network needing access to the Internet is required to provide login credentials for authorization. The lobby administrator can provide temporary credentials for the guest user. The tunnel buildup is done in a way similar to that of open mode, but authorization is not provided until the credentials are successfully validated. It allows for additional security because the individual user can be tracked according to the credentials in case of any malicious activity. Web authentication implementation requires an authentication server for validation.

The steps involved in configuring guest controller and foreign controller are detailed in the following sections.

Common Configuration for Open, Consent, and WebAuth Modes

Foreign Controller Configuration	Guest Controller Configuration

Enable IP DHCP relay and snooping information option along with IP DHCP snooping and device tracking. Also VLAN 325 is created, which is used primarily by Cisco for wired guest access:
`ip dhcp relay information trust-all`
`ip dhcp snooping information option allow-untrusted`
`ip dhcp snooping`
`ip device tracking`
`vlan 325`
	Create Wired_client_vlan and SVI along with VLAN 325. A valid and reachable DHCP pool is required; it can be external as well:
	`vlan <Wired_Client_VLAN>`
	`vlan325`
	`interface <Wired_Client_VLAN>`
	`ip address <IP_ADDR> <SUBNET_MASK>`

The switch detects the MAC address of the incoming client on the port configured with “access-session port-control auto” and applies the defined subscriber policy. The policy is created as follows:
`policy-map type control subscriber <Policy_Name>`
`#Name of pre control policy map`
`event session-started match-all`
`#Condition for trigger`
`1 class always do-until-failure`
`2 activate service-template <SERVICE-TEMPLATE_Name>`
`3 authorize`
	Two key features are enabled on the guest anchor controller:
	• IP device tracking
	• IP DHCP snooping on guest VLAN (wired)
	Configuration:
	`ip device tracking`
	`ip dhcp relay information trust-all`
	`ip dhcp snooping vlan <Wired_Client_VLAN>`
	`ip dhcp snooping vlan 325`
	`ip dhcp snooping information option allow-untrusted`
	`ip dhcp snooping`

The policy is referred to sequentially, which in this case points to a service-template:
`service-template <SERVICE-TEMPLATE_Name>`
`#Define Service Template`
`tunnel type capwap name <CAPWAP_Name>`
Configuration on the switchport interface:
`Interface GigabitEthernet<Interface_id>`
`switchport access vlan <vlan_id>`
`switchport mode access`
`access-session port-control auto`
`service-policy type control subscriber <Policy>`	

Additional configuration required for specific modes:

Open Mode Configuration

Foreign Controller Configuration	Guest Controller Configuration

On the foreign controller, the following configuration is needed:
`guest-lan <Guest_LAN_Name> <ID>`
`client vlan <Wired_Client_VLAN> #State the wired client vlan`
`mobility anchor <IP_ADDRESS>`
`no security web-auth`
`no shutdown`
	For open mode, create a guest LAN specifying the client VLAN with the Cisco 5760 WLC itself acting as the mobility anchor. In open mode, the "no security web-auth" command is required.
	`guest-lan < Guest_LAN_Name> <ID>`
	`client vlan <Wired_Client_VLAN> #State the wired client vlan`
	`mobility anchor`
	`no security web-auth`
	`no shutdown`

Consent Mode Configuration

Foreign Controller Configuration	Guest Controller Configuration

Enable HTTP and HTTPS:
`ip http server`
`ip http secure-server`
	Enable HTTP and HTTPS:
	`ip http server`
	`ip http secure-server`

Define the guest LAN configuration:
`guest-lan <GUEST_LAN_NAME> <ID>`
`client vlan <Wired_Client_VLAN>`
`mobility anchor <IP_ADDRESS>`
`security web-auth`
`security web-auth parameter-map <PARAMETER_MAP_NAME>`
`no shutdown`
	For consent mode, create a guest LAN specifying the client VLAN with the Cisco 5760 WLC itself acting as the mobility anchor. Also, security and parameter-map are defined in the following configuration:
	`guest-lan <GUEST_LAN_NAME> <ID>`
	`client vlan <Wired_Client_VLAN>`
	`mobility anchor`
	`security web-auth`
	`security web-auth parameter-map <PARAMETER_MAP_NAME>`
	`no shutdownn`

	For consent mode, create a parameter map type "webauth" for redirecting the user to specific pages for login and on success. The consent page can be stored on flash of the switch as well. In this case, the name of the file is "terms1.txt."
	`parameter-map type webauth <PARAMETER_MAP_NAME>`
	`type consent`
	`consent email`
	`timeout init-state min 5`
	`redirect on-success http://<IP_ADDRESS> # Page to redirect to after success`
	`banner file <LOCATION_OF_FILE> #File containing terms and conditions text`
	`logout-window-disabled`

WebAuth Mode Configuration

Foreign Controller Configuration	Guest Controller Configuration
guest-lan <GUEST_LAN_NAME> <ID> aaa-override client vlan <VLAN_ID> security web-auth #Enable WebAuth mobility anchor <IP_Address> no shutdown	AAA configuration: aaa new-model aaa group server radius <Name> server <Server_IP> ip radius source-interface <Radius_Source_Interface> dot1x system-auth-control aaa authentication login default group radius aaa authentication login <Name_for_Console> none aaa server radius dynamic-author client <Client_IP> server-key <Key> auth-type any radius server <Name> address ipv4 <Auth_Server_IP> auth-port 1812 acct-port 1813 timeout 60 retransmit 3 key <key> line con 0 exec-timeout 0 0 login authentication CON_ACCESS #Disable Authentication on console stopbits 1 speed 115200
	guest-lan <GUEST_LAN_NAME> <ID> aaa-override client vlan <VLAN_ID> security web-auth #Enable WebAuth mobility anchor no shutdown

If VLAN 325 is already in use on the network:

Solution: This solution uses VLAN 325 as the default VLAN for the wired guest access solution. To change it to another custom VLAN, the command “access-session tunnel vlan <VLAN ID>” can be used. This change should be made on both foreign controller and guest controllers.

Troubleshooting

1. Guest LAN tunnel is not initiated on the foreign controller.
   - Make sure that VLAN 325 is configured and is in no shut mode on both foreign controller and guest anchor switches.
   - Check the status of guest LANs. They need to be “no shutdown” manually after the initial configuration.
   - Make sure the guest port is configured for “access-session port-control auto.”
   - Check the service policy “service-policy type control subscriber <policy name>.”

2. Guest LAN tunnel buildup is initiated, but it eventually fails.
   - Check the guest LAN security configuration on both foreign controller and guest anchor using the “show guest-lan <guest-lan_name>” command. Tunnel buildup would fail in case of a mismatch.
3. Clients are in the “Auth” state initially, but cannot get access, web consent, or web authentication login pages.
   - Make sure that the security setting on both foreign controller and guest anchor match. For both web consent and web authentication, security needs to be enabled.
   - Check the configuration for “ip http server” and “ip https-server.”
   - Make sure that parameter-map is configured for web consent mode.
4. Client authentication fails.
   - Check connectivity to the RADIUS server from the foreign controller switch.
   - On the foreign controller switch, use “test aaa group radius <username> <password> new-code” command to check if user id/password are valid.
   - Check if the client exists in the authentication server database.
5. Access-session shows tunnel buildup and IP address assignment, but wcdb database is missing a valid IP address.
   - “ip dhcp snooping” is required for IPDT to update the wireless client database. It should be enabled globally on the foreign controller switch and both globally as well as on the client VLANs (and VLAN 325) on the guest anchor switch.
6. Changes to webconsent parameter configuration are not updated dynamically.
   - It has been observed that when changes are made to the webconsent parameter type, the changes are not applied. A workaround is to remove the entire parameter type and reconfigure with the new configuration.

Caveats

1. Tunnel buildup delay.
   - There can be some delay between the clients connecting to the switchport on the foreign controller switch and tunnel buildup. This is mostly the case when other authentication methods such as dot1x and MAB are used and need to fail before a guest anchor tunnel can be established.
2. Cannot ping clients from the local switch.
   - Because this is a tunnel-based approach, the traffic is sent to a DMZ controller (guest anchor), and clients are not reachable using local switch (foreign controller).
3. Clients cannot access any hosts outside the subnet.
   - The client traffic passes through a tunnel to the DMZ controller. Any routes to and from the client subnet must be defined on the controller (external firewall/routing can be used).
4. Clients cannot get IP address using DHCP and occasionally get stuck in IPLEARN state, causing repeated tunnel teardown and buildup.
   - Workaround is to manually do an ipconfig/release and ipconfig/renew on the client.
5. After SSO, clients need to get reauthenticated.
   - The wired guest access session information is not synced with the standby and member switches. In case of SSO, new sessions need to be established.

6. Wired guest access configuration using WebGUI.
   - Version 03.03.00.SE RELEASE SOFTWARE does not support configuring wired guest access feature using WebGUI.

Appendix

Command Outputs

```
Cat3850#show switch
Switch/Stack Mac Address : 20bb.c0a2.d880 - Local Mac Address
Mac persistency wait time: Indefinite
                                             H/W   Current
Switch#   Role    Mac Address     Priority Version  State
------------------------------------------------------------
*1       Active   20bb.c0a2.d880     15     B0      Ready

Cat3850#show version
Cisco IOS Software, IOS-XE Software, Catalyst L3 Switch Software (CAT3K_CAA-
UNIVERSALK9-M), Version 03.03.00.SE RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 02-Oct-13 21:51 by prod_rel_team

--Output Cut---

Base Ethernet MAC Address          : 20:bb:c0:a2:d8:80
Motherboard Assembly Number        : 73-12241-08
Motherboard Serial Number          : FOC171010AP
Model Revision Number              : B0
Motherboard Revision Number        : C0
Model Number                       : WS-C3850-48P
System Serial Number               : FOC1710V20X


Switch Ports Model              SW Version        SW Image              Mode
------ ----- -----              ----------        ----------            ----
*    1 56    WS-C3850-48P       03.03.00.SE       cat3k_caa-universalk9 BUNDLE


Configuration register is 0x102

Cisco-5760#show switch
Switch/Stack Mac Address : 1ce6.c7b6.2580 - Local Mac Address
Mac persistency wait time: Indefinite
                                             H/W   Current
```

```
Switch#   Role    Mac Address     Priority Version  State
------------------------------------------------------------
*2       Active   1ce6.c7b6.2580     1      PP      Ready
```

Cisco-5760#show version

```
Cisco IOS Software, IOS-XE Software, 5700 Series Wireless LAN Controller Software
(CT5760-IPSERVICESK9-M), Version 03.03.00.SE RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Thu 03-Oct-13 05:20 by prod_rel_team


---Output Cut---

License Level: Ipservices
License Type: Permanent
Next reload license Level: Ipservices

cisco AIR-CT5760 (i686) processor with 10485760K bytes of physical memory.
Processor board ID FOC1704V12C
7 Virtual Ethernet interfaces
6 Ten Gigabit Ethernet interfaces
2048K bytes of non-volatile configuration memory.
10485760K bytes of physical memory.
253992K bytes of Crash Files at crashinfo:.
3531528K bytes of Flash at flash:.
0K bytes of Dummy USB Flash at usbflash0:.
0K bytes of  at webui:.

Base Ethernet MAC Address          : 1c:e6:c7:b6:25:80
Motherboard Assembly Number        : 73-14448-04
Motherboard Serial Number          : FOC170315RJ
Model Revision Number              : PP
Model Number                       : AIR-CT5760
System Serial Number               : FOC1704V12C


Switch Ports Model              SW Version        SW Image              Mode
------ ----- -----              ----------        ----------            ----
*    2 6     AIR-CT5760         03.03.00.SE       ct5760-ipservicesk9   BUNDLE


Configuration register is 0x201 (will be 0x102 at next reload)
```

Table 1 shows software release compatibility for the guest access feature.

Table 1. Software Release Compatibility for Guest Access Feature

Product	First Version Supported
Cisco Catalyst 3650	03.03.00.SE
Cisco Catalyst 3850	03.03.00.SE
Cisco 5760 WLC	03.03.00.SE

Table 2 lists clients used in testing.

Table 2. Clients Used in Testing

Guest Client Brand	Operating System
DELL	Windows 7
Lenovo	Windows 7
MacBook	OSX Version 10.8.5

Show Commands and Troubleshooting

The following show commands are useful in verifying the configuration and troubleshooting most commonly seen issues.

Commands to Check Summary and Details of Guest LAN Profiles

```
Cat3850#show guest-lan summary
Number of Guest LANs                        : 0

GLAN ID   GLAN Profile Name             Status     Interface
-----------------------------------------------------------
1         GUEST_LAN_WEBAUTH             Enabled    33
2         GUEST_LAN_WEBCONSENT          Enabled    33
3         GUEST_LAN_OPENAUTH            Enabled    33

Cisco-5760#show guest-lan summary
Number of Guest LANs                        : 0

GLAN ID   GLAN Profile Name             Status     Interface
-----------------------------------------------------------
1         GUEST_LAN_WEBAUTH             Enabled    33
2         GUEST_LAN_WEBCONSENT          Enabled    33
3         GUEST_LAN_OPENAUTH            Enabled    33


Cat3850#show guest-lan GUEST_LAN_OPENAUTH
Guest LAN Identifier                            : 3
Profile Name                                    : GUEST_LAN_OPENAUTH
Status                                          : Enabled
AAA Policy Override                             : Disabled
```

```
Network Admission Control
  NAC-State                                  :
Number of Active Clients                     : 0
Exclusionlist Timeout                        : Infinity
Session Timeout                              : Infinity
CHD per WLAN                                 : Enabled
Webauth DHCP exclusion                       : Disabled
Interface                                    : 33
Ingress Interface                            : unconfigured
Guest LAN IPv4 ACL                           :
Guest LAN IPv6 ACL                           : none
Accounting list name                         : Disabled
DHCP Server                                  : Default
DHCP Address Assignment Required             : Disabled
Quality of Service                           : Silver (best effort)
Radius Servers
    Authentication                           : Global Servers
    Accounting                               : Global Servers
Security
    Web Based Authentication                 : Disabled
    Conditional Web Redirect                 : Disabled
    Splash-Page Web Redirect                 : Disabled
    Auto Anchor                              : Disabled
    Webauth Parameter Map                    : Disabled

Mobility Anchor List
IP Address
-----------
 164.3.3.2

Cisco-5760#show guest-lan GUEST_LAN_OPENAUTH
Guest LAN Identifier                         : 3
Profile Name                                 : GUEST_LAN_OPENAUTH
Status                                       : Enabled
AAA Policy Override                          : Disabled
Network Admission Control
  NAC-State                                  :
Number of Active Clients                     : 0
Exclusionlist Timeout                        : Infinity
Session Timeout                              : Infinity
CHD per WLAN                                 : Enabled
Webauth DHCP exclusion                       : Disabled
Interface                                    : 33
Ingress Interface                            : unconfigured
Guest LAN IPv4 ACL                           :
```

```
Guest LAN IPv6 ACL                              : none
Accounting list name                            : Disabled
DHCP Server                                     : Default
DHCP Address Assignment Required                : Disabled
Quality of Service                              : Silver (best effort)
Radius Servers
    Authentication                              : Global Servers
    Accounting                                  : Global Servers
Security
    Web Based Authentication                    : Disabled
    Conditional Web Redirect                    : Disabled
    Splash-Page Web Redirect                    : Disabled
    Auto Anchor                                 : Disabled
    Webauth Parameter Map                       : Disabled

Mobility Anchor List
IP Address
-----------
 164.3.3.2
```

Commands to Check Summary and Details About Access Session Profiles

Cat3850#show access-session

```
Interface    MAC Address    Method  Domain  Status Fg Session ID
Gi1/0/11     e89a.8f7a.16a5 N/A     DATA    Auth      0000000000000FCC2532D29E

Session count = 1

Key to Session Events Status Flags:

  A - Applying Policy (multi-line status for details)
  D - Awaiting Deletion
  F - Final Removal in progress
  I - Awaiting IIF ID allocation
  P - Pushed Session (non-transient state)
  R - Removing User Profile (multi-line status for details)
  U - Applying User Profile (multi-line status for details)
  X - Unknown Blocker
```

More details about the access-session can be seen:

```
Cat3850#show access-session mac e89a.8f7a.16a5 details
            Interface:  GigabitEthernet1/0/11
```

```
                IIF-ID:  0x1087580000000B6
           MAC Address:  e89a.8f7a.16a5
          IPv6 Address:  Unknown
          IPv4 Address:  Unknown
                Status:  Authorized
                Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  0000000000000FCC2532D29E
      Acct Session ID:  0x00000FD8
                Handle:  0xDD00002B
       Current Policy:  OPENAUTH

Local Policies:
        Template: SERV-TEMP3-OPENAUTH (priority 150)
  Tunnel Profile Name:  GUEST_LAN_OPENAUTH
         Tunnel State:  2

Method status list: empty


Cat3850#show wireless client summary
Number of Local Clients : 1


MAC Address    AP Name                          WLAN State              Protocol
-------------------------------------------------------------------------------
e89a.8f7a.16a5 N/A                              3    UP                 Ethernet
```

Open Mode Outputs

Tunnel request is initiated from the foreign controller to the guest anchor for the client, and a “tunnel add success” indicated that the tunnel buildup process completed:

```
*Nov  4 15:49:22.511: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/11, changed
state to up
*Nov  4 15:49:23.512: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet1/0/11, changed state to up
*Nov  4 15:49:35.802: epm_spi_client_tunnel_add:server
*Nov  4 15:49:35.802: Sending tunnel add request to WCM for server_handle
DF000044, server_rh AD000053, mac e89a.8f7a.16a5, audit_ses_id
0000000000000FCC2532D29E, profile name GUEST_LAN_OPENAUTH, src intf
0x108B90000000021, client iif id 0x1087580000000B6, client hdl 20000016
*Nov  4 15:49:35.824: spi_epm_wired_tunnel_wcm_epm_response_handler
*Nov  4 15:49:35.824: tunnel add success
```

1. The client is moved to virtual LAN 325 from access VLAN on the port:

```
Cat3850#show vlan id 325

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
325  VLAN0325                         active    Gi1/0/11, Te1/1/1, Ca1, Ca0, Ca3,
   Ca4


Cat3850#show vlan id 19

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
19   VLAN0019                         active    Gi1/0/9, Gi1/0/10, Te1/1/1,  Ca1,
   Ca0, Ca3, Ca4
```

2. The access session created for the particular client can be seen using the CLI:

```
Cat3850#show access-session

Interface    MAC Address    Method  Domain  Status Fg Session ID
Gi1/0/11     e89a.8f7a.16a5 N/A     DATA    Auth      0000000000000FCC2532D29E

   Session count = 1


More details about the access-session can be seen:

Cat3850#show access-session mac e89a.8f7a.16a5 details
            Interface:  GigabitEthernet1/0/11
               IIF-ID:  0x1087580000000B6
          MAC Address:  e89a.8f7a.16a5
         IPv6 Address:  Unknown
         IPv4 Address:  Unknown
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  0000000000000FCC2532D29E
      Acct Session ID:  0x00000FD8
               Handle:  0xDD00002B
```

```
       Current Policy:  OPENAUTH

Local Policies:
        Template: SERV-TEMP3-OPENAUTH (priority 150)
  Tunnel Profile Name:  GUEST_LAN_OPENAUTH
         Tunnel State:  2

Method status list: empty
```

```
Cat3850#show wireless client summary
Number of Local Clients : 1

MAC Address    AP Name                           WLAN State              Protocol
-------------------------------------------------------------------------------
e89a.8f7a.16a5 N/A                               3    UP                 Ethernet
```

```
Cat3850#show wcdb da all
        Total Number of Wireless Clients = 1
                Clients Waiting to Join   = 0
                Local Clients             = 0
                Anchor Clients            = 0
                Foreign Clients           = 1
                MTE Clients               = 0

Mac Address    VlanId IP Address      Src If             Auth     Mob
-------------- ------ --------------- ------------------ -------- -------
e89a.8f7a.16a5     33 33.1.1.4        0x0108B90000000021 RUN      FOREIGN
```

```
Cisco-5760#show wireless client summary
Number of Local Clients : 1

MAC Address    AP Name                           WLAN State              Protocol
-------------------------------------------------------------------------------
e89a.8f7a.16a5 N/A                               3    UP                 Ethernet
```

```
Cisco-5760#show wcdb da all
        Total Number of Wireless Clients = 1
                Clients Waiting to Join   = 0
                Local Clients             = 0
                Anchor Clients            = 1
```

```
                Foreign Clients           = 0
                MTE Clients               = 0

Mac Address    VlanId IP Address      Src If             Auth     Mob
-------------- ------ --------------- ------------------ -------- -------
e89a.8f7a.16a5     33 33.1.1.4        0x0067770000000008 RUN      ANCHOR

Cisco-5760#show wcdb database e89a.8f7a.16a5
mac:             e89a.8f7a.16a5
ssid:            GUEST_LAN_OPENAUTH
client_type:     Export Anchor
client_id:       0x00635B4000000021
client_index:    20
user_id:
src_interface:   0x0067770000000008
dst_interface:   0x0000000000000000
bssid:           0000.0000.0000
radio_id:        0
wgbid:           0000.0000.0000
wlan_id:         0
global_wlan_id:  516
assoc_id:        0
vlan_id:         33
mcast_vlan_id:   33
mobility_state:  ANCHOR
auth_state:      RUN
auth_state_wcm:  RUN

dhcp_req_rx:     0
ipv4_source:     DHCP
ipsg_flag:       0
num_v4_addrs:    1
ipv4addr[0]:     33.1.1.4
ipv4addr[1]:     0.0.0.0
ipv4addr[2]:     0.0.0.0
ipv4addr[3]:     0.0.0.0

num_v6_addrs:    0

dhcp_server_ip:  0.0.0.0
dhcp_class_name: Test
dhcp_action_flags: 0
option 82:
option_82 length: 0
dhcp_notify_preference_flag: 0
```

```
dhcp_notify_interested_options: 0
options_length: 0
options TLV is:

p2p_state:        P2P_BLOCKING_DISABLE
bssid_iifid:     0x0000000000000000
radio_iifid:     0x0000000000000000
num_protocol_values:  0
ip_learnt:     0x1
flags:         0x2
switch_num:      2
asic_num:        0

state_change_history:
    Vlan Auth     Mob    Flags IPv4Src IPv4Address(s)      time
 2. 33   LEARN_IP ANCHOR  0x2  IP SNOO [1]33.1.1.4         11-04-2013
15:55:55.490307
 1. 33   L2_AUTH_ ANCHOR  0x2  UNKNOWN [0]                 11-04-2013
15:55:25.98624
 0. 33   ASSOCIAT ANCHOR  0x0  UNKNOWN [0]                 11-04-2013
15:55:25.97002

    IPLearnt IPv6Address(s)
 2. 0x1      [0]
 1. 0x0      [0]
 0. 0x0      [0]
```

Consent Mode Outputs

1. Tunnel request is initiated by the foreign controller to the guest anchor for the client, and a “tunnel add success” indicated that the tunnel buildup process completed:

```
Cat3850#
   *Nov  5 14:52:52.990: epm_spi_client_tunnel_add:server
   *Nov  5 14:52:52.990: Sending tunnel add request to WCM for server_handle
   DF000044, server_rh AD000053, mac 5cf9.dd52.0778, audit_ses_id
   0000000000000FD62A25426E, profile name GUEST_LAN_WEBCONSENT, src intf
   0x1008FC00000001F, client iif id 0x1000300000000BB, client hdl 4000001B
   *Nov  5 14:52:53.012: spi_epm_wired_tunnel_wcm_epm_response_handler
   *Nov  5 14:52:53.012: tunnel add success
```

2. The client is moved onto virtual LAN 325 instead of the access VLAN on the port similar to the OPENAUTH mode.

3. The access session created for the particular client can be seen using the CLI:

Cat3850#show access-session

```
Interface    MAC Address    Method  Domain  Status Fg Session ID
Gi1/0/10     5cf9.dd52.0778 N/A     DATA    Auth   0000000000000FD62A25426E

Session count = 1

Key to Session Events Status Flags:

A - Applying Policy (multi-line status for details)
D - Awaiting Deletion
F - Final Removal in progress
I - Awaiting IIF ID allocation
P - Pushed Session (non-transient state)
R - Removing User Profile (multi-line status for details)
U - Applying User Profile (multi-line status for details)
X - Unknown Blocker
```

Cat3850#show access-session mac 5cf9.dd52.0778 details

```
            Interface:  GigabitEthernet1/0/10
               IIF-ID:  0x1000300000000BB
          MAC Address:  5cf9.dd52.0778
         IPv6 Address:  Unknown
         IPv4 Address:  Unknown
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  0000000000000FD62A25426E
      Acct Session ID:  0x00000FE6
               Handle:  0xFC000034
       Current Policy:  WEBCONSENT

Local Policies:
        Template: SERV-TEMP2-WEBCONSENT (priority 150)
  Tunnel Profile Name:  GUEST_LAN_WEBCONSENT
         Tunnel State:  2

Method status list: empty
```

4. Client is also visible in the switch wcdb database:

```
Cat3850#show wcdb da all
        Total Number of Wireless Clients = 1
                Clients Waiting to Join   = 0
                Local Clients             = 0
                Anchor Clients            = 0
                Foreign Clients           = 1
                MTE Clients               = 0

Mac Address    VlanId IP Address      Src If             Auth     Mob
-------------- ------ --------------- ------------------ -------- -------
5cf9.dd52.0778     33 33.1.1.5        0x01008FC00000001F RUN      FOREIGN

Cat3850#show wcdb da 5cf9.dd52.0778
mac:             5cf9.dd52.0778
ssid:            GUEST_LAN_WEBCONSENT
client_type:     Wired Guest
client_id:       0x01000300000000BB
client_index:    27
user_id:
src_interface:   0x01008FC00000001F
dst_interface:   0x00CA7B0000000006
bssid:           0000.0000.0000
radio_id:        0
wgbid:           0000.0000.0000
wlan_id:         0
global_wlan_id:  67
assoc_id:        0
vlan_id:         33
mcast_vlan_id:   33
mobility_state:  FOREIGN
auth_state:      RUN
auth_state_wcm:  RUN

dhcp_req_rx:     0
ipv4_source:     DHCP
ipsg_flag:       0
num_v4_addrs:    1
ipv4addr[0]:     33.1.1.5
ipv4addr[1]:     0.0.0.0
ipv4addr[2]:     0.0.0.0
ipv4addr[3]:     0.0.0.0

num_v6_addrs:    0
```

```
dhcp_server_ip:  0.0.0.0
dhcp_class_name: Test
dhcp_action_flags: 0
option 82:
option_82 length: 0
dhcp_notify_preference_flag: 0
dhcp_notify_interested_options: 0
options_length: 0
options TLV is:


p2p_state:         P2P_BLOCKING_DISABLE
bssid_iifid:      0x0000000000000000
radio_iifid:      0x0000000000000000
num_protocol_values:  0
ip_learnt:      0x1
flags:          0x0
switch_num:       0
asic_num:         0

state_change_history:
    Vlan Auth      Mob     Flags IPv4Src IPv4Address(s)       time
 2. 33   RUN       FOREIGN 0x0   UNKNOWN [0]                  11-05-2013
14:52:53.11170
 1. 33   L2_AUTH_ INIT     0x0   UNKNOWN [0]                  11-05-2013
14:52:53.10939
 0. 33   ASSOCIAT INIT     0x0   UNKNOWN [0]                  11-05-2013
14:52:52.990985

    IPLearnt IPv6Address(s)
 2. 0x0      [0]
 1. 0x0      [0]
 0. 0x0      [0]
```

5. At this stage, the guest anchor controller (Cisco 5760 WLC) indicates that the client is in the L3_AUTH state, because the user needs to agree to certain terms of use:

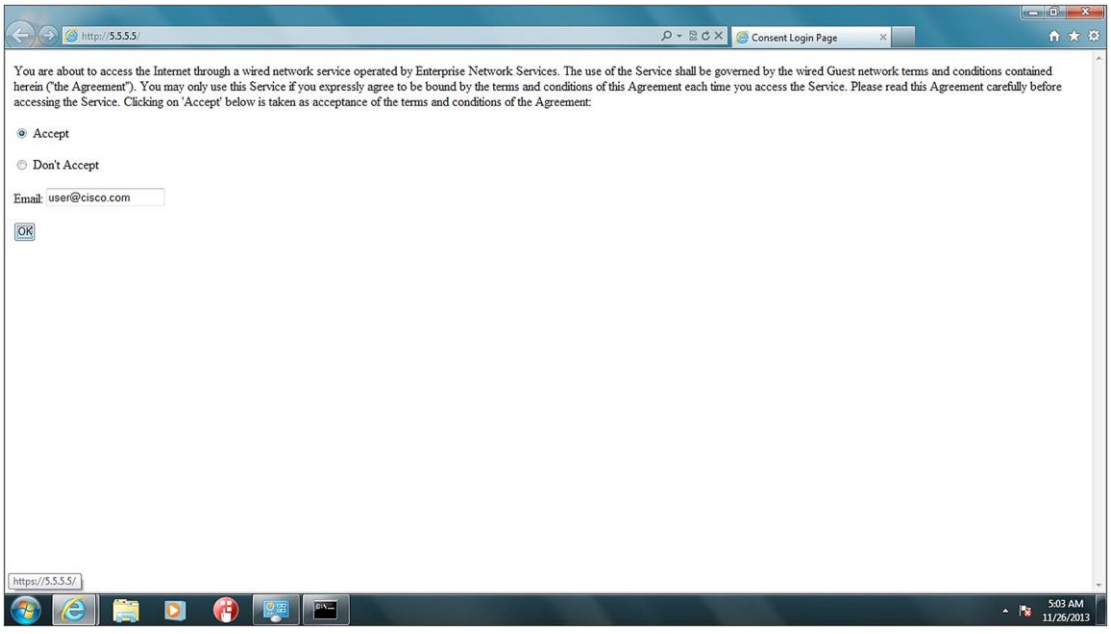
```
Cisco-5760#show wcdb da all
       Total Number of Wireless Clients = 1
        Clients Waiting to Join   = 0
             Local Clients             = 0
             Anchor Clients            = 1
             Foreign Clients           = 0
             MTE Clients               = 0
```

```
Mac Address    VlanId IP Address      Src If             Auth     Mob
-------------- ------ --------------- ------------------ -------- -------
5cf9.dd52.0778     33 33.1.1.5        0x0067770000000008 L3_AUTH  ANCHOR


Cisco-5760#show wcdb da 5cf9.dd52.0778
mac:             5cf9.dd52.0778
ssid:            GUEST_LAN_WEBCONSENT
client_type:     Export Anchor
client_id:       0x0044060000000025
client_index:    24
user_id:
src_interface:   0x0067770000000008
dst_interface:   0x0000000000000000
bssid:           0000.0000.0000
radio_id:        0
wgbid:           0000.0000.0000
wlan_id:         0
global_wlan_id:  515
assoc_id:        0
vlan_id:         33
mcast_vlan_id:   33
mobility_state:  ANCHOR
auth_state:      L3_AUTH
auth_state_wcm:  L3_AUTH

dhcp_req_rx:     0
ipv4_source:     DHCP
ipsg_flag:       0
num_v4_addrs:    1
ipv4addr[0]:     33.1.1.5
ipv4addr[1]:     0.0.0.0
ipv4addr[2]:     0.0.0.0
ipv4addr[3]:     0.0.0.0

num_v6_addrs:    0

dhcp_server_ip:  0.0.0.0
dhcp_class_name: Test
dhcp_action_flags: 0
option 82:
option_82 length: 0
dhcp_notify_preference_flag: 0
dhcp_notify_interested_options: 0
```

```
options_length: 0
options TLV is:

p2p_state:         P2P_BLOCKING_DISABLE
bssid_iifid:      0x0000000000000000
radio_iifid:      0x0000000000000000
num_protocol_values:  0
ip_learnt:      0x1
flags:          0x2
switch_num:       2
asic_num:         0

state_change_history:
    Vlan Auth      Mob     Flags IPv4Src IPv4Address(s)       time
 2. 33   LEARN_IP ANCHOR  0x2   DHCP    [1]33.1.1.5          11-05-2013
15:00:08.31845
 1. 33   L2_AUTH_ ANCHOR  0x2   UNKNOWN [0]                   11-05-2013
14:58:47.151266
 0. 33   ASSOCIAT ANCHOR  0x0   UNKNOWN [0]                   11-05-2013
14:58:47.147955

    IPLearnt IPv6Address(s)
 2. 0x1      [0]
 1. 0x0      [0]
 0. 0x0      [0]
```

6. The user is presented with the screen shown in Figure 2, containing the terms of use.

Figure 2. User Consent Form and Acceptance Webpage



7. In the last state, after the guest agrees to the terms, the state is changed to RUN, and the following log message is seen on the screen:

```
Cisco-5760# *Nov  5 15:03:23.215: *%PEM-6-GUESTIN: 2 wcm:  Guest user logged in
with user account (ecsg-solutions@cisco.com) MAC address  5cf9.dd52.0778
AuditSessionID: 0000000000000FD62A25426E, IP address 33.1.1.5


Client state on 5750 Guest Anchor is changed to RUN:

Cisco-5760#show wcdb da all
        Total Number of Wireless Clients = 1
                Clients Waiting to Join   = 0
                Local Clients             = 0
                Anchor Clients            = 1
                Foreign Clients           = 0
                MTE Clients               = 0

Mac Address    VlanId IP Address      Src If             Auth     Mob
-------------- ------ --------------- ------------------ -------- -------
5cf9.dd52.0778     33 33.1.1.5        0x0067770000000008 RUN      ANCHOR

Cisco-5760#show wcdb da 5cf9.dd52.0778
mac:             5cf9.dd52.0778
ssid:            GUEST_LAN_WEBCONSENT
client_type:     Export Anchor
client_id:       0x0044060000000025
client_index:    24
user_id:         ecsg-solutions@cisco.com
src_interface:   0x0067770000000008
dst_interface:   0x0000000000000000
bssid:           0000.0000.0000
radio_id:        0
wgbid:           0000.0000.0000
wlan_id:         0
global_wlan_id:  515
assoc_id:        0
vlan_id:         33
mcast_vlan_id:   33
mobility_state:  ANCHOR
auth_state:      RUN
auth_state_wcm:  RUN

dhcp_req_rx:     0
ipv4_source:     DHCP
```

```
ipsg_flag:       0
num_v4_addrs:    1
ipv4addr[0]:     33.1.1.5
ipv4addr[1]:     0.0.0.0
ipv4addr[2]:     0.0.0.0
ipv4addr[3]:     0.0.0.0

num_v6_addrs:    0

dhcp_server_ip:  0.0.0.0
dhcp_class_name: Test
dhcp_action_flags: 0
option 82:
option_82 length: 0
dhcp_notify_preference_flag: 0
dhcp_notify_interested_options: 0
options_length: 0
options TLV is:

p2p_state:        P2P_BLOCKING_DISABLE
bssid_iifid:     0x0000000000000000
radio_iifid:     0x0000000000000000
num_protocol_values:  0
ip_learnt:     0x1
flags:         0x2
switch_num:      2
asic_num:        0

state_change_history:
    Vlan Auth     Mob    Flags IPv4Src IPv4Address(s)      time
 3. 33   L3_AUTH  ANCHOR  0x2  DHCP    [1]33.1.1.5         11-05-2013
15:03:23.215764
 2. 33   LEARN_IP ANCHOR  0x2  DHCP    [1]33.1.1.5         11-05-2013
15:00:08.31845
 1. 33   L2_AUTH_ ANCHOR  0x2  UNKNOWN [0]                 11-05-2013
14:58:47.151266
 0. 33   ASSOCIAT ANCHOR  0x0  UNKNOWN [0]                 11-05-2013
14:58:47.147955

    IPLearnt IPv6Address(s)
 3. 0x1      [0]
 2. 0x1      [0]
 1. 0x0      [0]
 0. 0x0      [0]
```

Webauth Mode Outputs

1. The access session created for the particular client can be seen using the CLI:

```
Cat3850#show access-session

Interface    MAC Address    Method  Domain  Status Fg Session ID
Gi1/0/9      5cf9.dd52.0778 N/A     DATA    Auth    0000000000000FDC2A55EA40

Session count = 1

Key to Session Events Status Flags:

  A - Applying Policy (multi-line status for details)
  D - Awaiting Deletion
  F - Final Removal in progress
  I - Awaiting IIF ID allocation
  P - Pushed Session (non-transient state)
  R - Removing User Profile (multi-line status for details)
  U - Applying User Profile (multi-line status for details)
  X - Unknown Blocker

Cat3850#show access-session mac 5cf9.dd52.0778 details
            Interface:  GigabitEthernet1/0/9
               IIF-ID:  0x1055C00000000C0
          MAC Address:  5cf9.dd52.0778
         IPv6 Address:  Unknown
         IPv4 Address:  Unknown
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  0000000000000FDC2A55EA40
      Acct Session ID:  0x00000FF1
               Handle:  0x0800003E
       Current Policy:  WEBAUTH

Local Policies:
        Template: SERV-TEMP1-WEBAUTH (priority 150)
  Tunnel Profile Name:  GUEST_LAN_WEBAUTH
        Tunnel State:  2
```

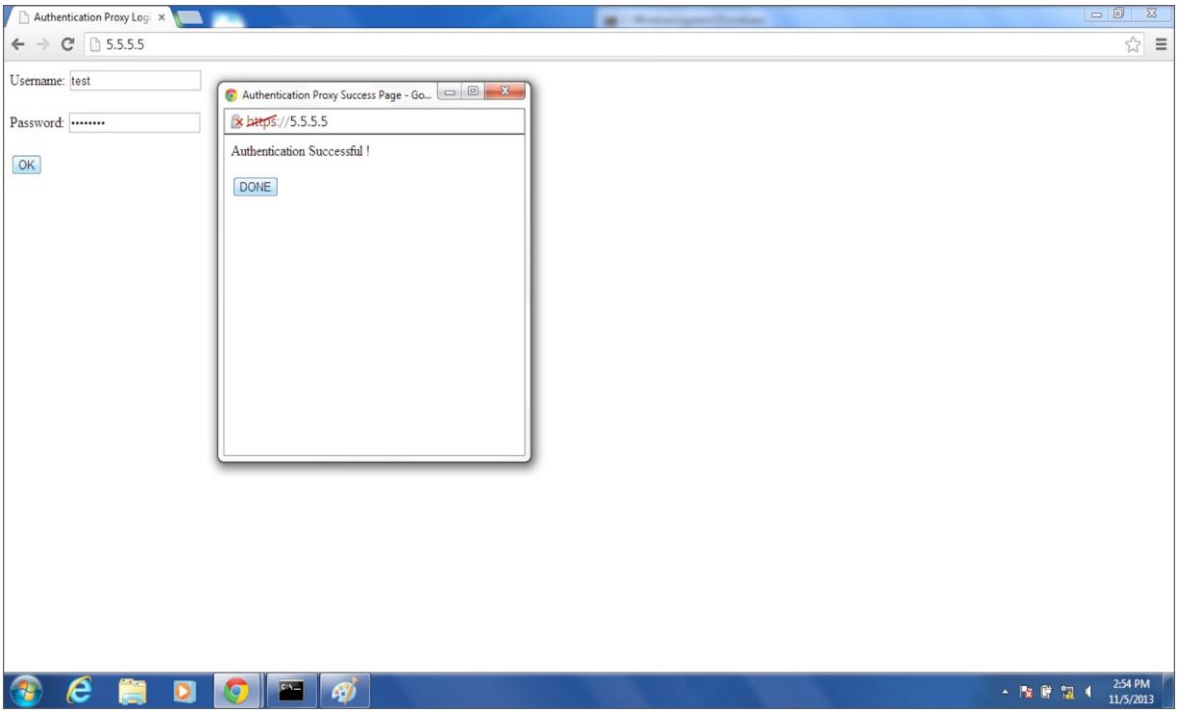
2. Because the client is not authorized to access the network at this point, it is seen in the “L3_AUTH” state on the guest anchor switch (Cisco 5760 WLC):

```
Cisco-5760#show wcdb da all
        Total Number of Wireless Clients = 1
                Clients Waiting to Join   = 0
                Local Clients             = 0
                Anchor Clients            = 1
                Foreign Clients           = 0
                MTE Clients               = 0

Mac Address    VlanId IP Address      Src If             Auth     Mob
-------------- ------ --------------- ------------------ -------- -------
5cf9.dd52.0778     33 33.1.1.7        0x0067770000000008 L3_AUTH  ANCHOR

Cisco-5760#show wcdb da 5cf9.dd52.0778
mac:             5cf9.dd52.0778
ssid:            GUEST_LAN_WEBAUTH
client_type:     Export Anchor
client_id:       0x0042A7800000002A
client_index:    29
user_id:
src_interface:   0x0067770000000008
dst_interface:   0x0000000000000000
bssid:           0000.0000.0000
radio_id:        0
wgbid:           0000.0000.0000
wlan_id:         0
global_wlan_id:  514
assoc_id:        0
vlan_id:         33
mcast_vlan_id:   33
mobility_state:  ANCHOR
auth_state:      L3_AUTH
auth_state_wcm:  L3_AUTH

dhcp_req_rx:     0
ipv4_source:     DHCP
ipsg_flag:       0
num_v4_addrs:    1
ipv4addr[0]:     33.1.1.7
ipv4addr[1]:     0.0.0.0
ipv4addr[2]:     0.0.0.0
ipv4addr[3]:     0.0.0.0
```

```
num_v6_addrs:    0

dhcp_server_ip:  0.0.0.0
dhcp_class_name: Test
dhcp_action_flags: 0
option 82:
option_82 length: 0
dhcp_notify_preference_flag: 0
dhcp_notify_interested_options: 0
options_length: 0
options TLV is:

p2p_state:        P2P_BLOCKING_DISABLE
bssid_iifid:     0x0000000000000000
radio_iifid:     0x0000000000000000
num_protocol_values:  0
ip_learnt:     0x1
flags:         0x2
switch_num:      2
asic_num:        0

state_change_history:
    Vlan Auth     Mob    Flags IPv4Src IPv4Address(s)      time
 2. 33   LEARN_IP ANCHOR  0x2  DHCP    [1]33.1.1.7         11-05-2013
15:52:47.86363
 1. 33   L2_AUTH_ ANCHOR  0x2  UNKNOWN [0]                 11-05-2013
15:51:56.22121
 0. 33   ASSOCIAT ANCHOR  0x0  UNKNOWN [0]                 11-05-2013
15:51:56.19161

    IPLearnt IPv6Address(s)
 2. 0x1      [0]
 1. 0x0      [0]
 0. 0x0      [0]
```

3. After the client opens the web browser and tries to access a webpage, it is redirected to the authentication page where the guest enters the credentials, shown in Figure 3.

Figure 3. User Authentication Success Webpage



4. In the last state, after the user credentials are verified using a RADIUS server, the state is changed to RUN, and the following log message is seen on the screen:

```
Cisco-5760#
*Nov  5 15:54:39.329: *%PEM-6-GUESTIN: 2 wcm:  Guest user logged in with user
account (test) MAC address  5cf9.dd52.0778  AuditSessionID:
0000000000000FDC2A55EA40, IP address 33.1.1.7.
Cisco-5760#


Client state on 5750 Guest Anchor is changed to RUN:


Cisco-5760#show wcdb da all
Total Number of Wireless Clients = 1
                Clients Waiting to Join   = 0
                Local Clients             = 0
                Anchor Clients            = 1
                Foreign Clients           = 0
                MTE Clients               = 0

Mac Address    VlanId IP Address      Src If             Auth     Mob
-------------- ------ --------------- ------------------ -------- -------
5cf9.dd52.0778     33 33.1.1.7        0x0067770000000008 RUN      ANCHOR
```

```
Cisco-5760#show wcdb da 5cf9.dd52.0778
mac:              5cf9.dd52.0778
ssid:             GUEST_LAN_WEBAUTH
client_type:      Export Anchor
client_id:        0x004799000000002B
client_index:     30
user_id:          test
src_interface:    0x0067770000000008
dst_interface:    0x0000000000000000
bssid:            0000.0000.0000
radio_id:         0
wgbid:            0000.0000.0000
wlan_id:          0
global_wlan_id:   514
assoc_id:         0
vlan_id:          33
mcast_vlan_id:    33
mobility_state:   ANCHOR
auth_state:       RUN
auth_state_wcm:   RUN

dhcp_req_rx:      0
ipv4_source:      DHCP
ipsg_flag:        0
num_v4_addrs:     1
ipv4addr[0]:      33.1.1.7
ipv4addr[1]:      0.0.0.0
ipv4addr[2]:      0.0.0.0
ipv4addr[3]:      0.0.0.0

num_v6_addrs:     0

dhcp_server_ip:   0.0.0.0
dhcp_class_name: Test
dhcp_action_flags: 0
option 82:
option_82 length: 0
dhcp_notify_preference_flag: 0
dhcp_notify_interested_options: 0
options_length: 0
options TLV is:

p2p_state:         P2P_BLOCKING_DISABLE
bssid_iifid:      0x0000000000000000
radio_iifid:      0x0000000000000000
```

```
num_protocol_values:  0
ip_learnt:     0x1
flags:         0x2
switch_num:      2
asic_num:        0

state_change_history:
    Vlan Auth     Mob    Flags IPv4Src IPv4Address(s)      time
 3. 33   L3_AUTH  ANCHOR  0x2  DHCP    [1]33.1.1.7         11-05-2013
16:02:04.475985
 2. 33   LEARN_IP ANCHOR  0x2  DHCP    [1]33.1.1.7         11-05-2013
16:01:24.283908
 1. 33   L2_AUTH_ ANCHOR  0x2  UNKNOWN [0]                 11-05-2013
16:00:51.793540
 0. 33   ASSOCIAT ANCHOR  0x0  UNKNOWN [0]                 11-05-2013
16:00:51.791676

    IPLearnt IPv6Address(s)
 3. 0x1      [0]
 2. 0x1      [0]
 1. 0x0      [0]
 0. 0x0      [0]

Cisco-5760#
```


Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-732935-00 11/14