



Examples and Technotes, Cisco IOS XE Release Denali 16.1.1

First Published: November 30, 2015

Last Modified:

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© November, 2015 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Auto Anchor SSID between Wireless LAN Controllers acting as MC 1

- Configuring WLAN on Foreign Cisco Catalyst 3850 Series Switches 1
- Configuring WLAN on Anchor Cisco 5500 Series Wireless Controller 2
- Global AAA Configuration 2
- Global Parameter-map Configuration 2
- Mobility Summary for Foreign Cisco Catalyst 3850 Series Switches 3
- Mobility Summary for Anchor Cisco 5500 Series Wireless Controller 3

CHAPTER 2

Enabling Central Web Authentication on ISE 5

- Enabling CWA on ISE through Global Configuration Commands 5
- Enabling External Policy Server using Dynamic Authorization Commands 6
 - Related Commands 6
- Configuring WLAN Commands 7
- Authentication Flow on ISE 7

CHAPTER 3

Configuring Auto Anchor and Mobility Groups on Wireless Services 11

- Supported Platforms and Releases 11
- Configuring Mobility Groups on Cisco Catalyst 3850 Series Switch 12
- Configuring Foreign SSID 12
- Configuring Auto Mobility Groups on Cisco 5500 Series Wireless Controller GUI 13
- Configuring Anchor SSID on Cisco 5500 Series GUI 13
- Testing Client Connectivity on Wireless Services 14
- Configuring Auto Anchor SSID on Cisco Catalyst 3850 Series Switch 14
- Configuring Foreign SSID on Cisco 5500 Series Wireless Controller 14
- Verifying Auto Anchor and Mobility Groups Configuration 14
 - Verifying Client Connectivity Status 15
 - Verifying Mobility Group Status between Wireless Services 15

CHAPTER 4**Configuring Wireless Multicast on Wireless LAN Controllers 17**

Prerequisites 17

Supported Platforms and Releases 17

Configuring Multicast on Converged Access Platforms 18

Configuring Multicast Flow on Converged Access 18

Verifying the Wireless Multicast Configuration on Wireless LAN Controller 19

Troubleshooting Wireless Multicast Configuration on Wireless LAN Controller Issues 21

CHAPTER 5**Converged Access Consolidated Quick Reference Templates for Wireless LAN 25**

Prerequisites 25

Supported Platforms and Releases 25

Configuration Templates for Layer 2 Security 26

Open WLAN No Security Template 26

Static Wired Equivalent Privacy Template 26

MAC Filter - Local Database Template 26

MAC Filter - External RADIUS Template 26

Wireless Protected Access 2 Pre-Shared Key Template 27

802.1x Local Extensible Authentication Protocol Authentication Template 27

802.1x on External RADIUS Template 27

Configuration Templates for Layer 3 Security 28

Web Passthrough Template 28

Local Authentication Template 28

Web Authentication with External RADIUS Authentication Template 29

External Web Authentication Template 29

Customized Local Web Authentication Template 30

Auto Anchor Web Authentication Template 30

CHAPTER 6**Converged Access Controller AP Join Issue Troubleshoot with Traces 33**

Prerequisites 33

Supported Platforms and Releases 33

Associated Products 34

AP Join Sequence and Troubleshoot 35

AP Join Sequence 35

Troubleshoot 36

Basic Steps	36
Traces from Controller	36
Discovery-Request / Response	38
DTLS-Handshake	38
Join Request-Response	41
Configuration Status Request-Response/Update Request-Response	43
Common Reasons for AP Join Failure	46
General Technical Tips on Trace Commands	49

CHAPTER 7**Converged Access Controllers MAC Address Entry for Network Mobility Service Protocol 51**

Prerequisites	51
Adding the MAC Address and the SSC on Converged Access WLCs	51

CHAPTER 8**Configuration Example: Converged Access Management through Prime Infrastructure with**

SNMP v2 and v3	53
Prerequisites	53
Supported Platforms and Releases	53
Configuring Converged Access Management	54
Configuring SNMP v2 on a Switch using CLI	54
Configuring SNMP v2 on a Switch using GUI	55
Configuring SNMP v3 on a Switch using CLI	57
Configuring on Prime Infrastructure	57
Verifying Converged Access Management Configuration	61
Verifying SNMP v2 Configuration on a Switch	61
Verifying SNMP v3 Configuration on a Switch	61
Verifying Configuration on Prime Infrastructure	62
Troubleshooting Converged Access Management Configuration Issues	62

CHAPTER 9**Converged Access Path Maximum Transmission Unit Discovery 63**

Supported Platforms and Releases	63
Network Diagram	63
Setting Maximum Transmission Unit	63
Dynamic Path Maximum Transmission Unit Discovery	64
ICMP Error over MPLS Example	64
Verifying Dynamic Path Maximum Transmission	64

Troubleshooting Dynamic Path Maximum Transmission Unit 64

CHAPTER 10**Third-Party Certificate Installation on Converged Access Wireless LAN Controllers 65**

Installing Third Party Certificates 65

Example for Installing Third Party Certificates 67

CHAPTER 11**Configuration Example: Converged Access for WLC EAP-FAST with Internal RADIUS**

Server 71

Prerequisites 71

Supported Platform and Releases 71

Configuring Converged Access WLC as RADIUS Server 73

Network Diagram for Converged Access 73

Configuring Converged Access 73

Configuring WLC with CLI 73

Configuring the WLC with the GUI 74

Verifying Configuration for Converged Access 79

Troubleshooting the Configuration for Converged Access 79

CHAPTER 12**Converged Access and WLC Local EAP Authentication Configuration Example 83**

Prerequisites 83

Supported Platforms and Releases 84

WLC Local EAP Authentication 84

Configuring Local EAP authentication 85

Network Diagram of LAP and WLC 85

Configuring Local EAP Authentication 85

Verifying the Local EAP Authentication Configuration 87

Troubleshooting the Local EAP Authentication configuring issues 89

Enable Traces for Wireless Client Issues 89

Debugs for dot1x and EAP 89

CHAPTER 13**Configuration Example: Custom Web Authentication with Local Authentication 109**

Prerequisites 109

Supported Platforms and Releases 109

Configuring Custom Web Authentication 110

Network Diagram 110

Configuring Authentication, Authorization, and Accounting	111
Configuring Virtual IP address and Setting Parameter-Map	111
Configuring WLAN	111
Configuring Globally	111
Creating Local Users	112
Configuring FTP for File Transfer	112
Uploading to Flash	112
Configuring WLAN using GUI	112
Sample Webauth_login HTML	112
Verifying the Custom Web Authentication with Local Authentication Configuration	113
Troubleshooting the Custom Web Authentication with Local Authentication Configuration Issues	114

CHAPTER 14**Dynamic VLAN Assignment with Converged Access and ACS 5.2 Configuration Example 129**

Prerequisites	129
Supported Platforms and Releases	129
Dynamic VLAN Assignment	130
Configuring Dynamic VLAN Assignment	130
Network Diagram of Dynamic VLAN Assignment	131
Configuring WLC (CLI)	132
Configuring WLAN (GUI)	133
Configuring RADIUS Server on WLC (GUI)	136
Configuring RADIUS Server	138
Verifying the Dynamic VLAN Assignment with Converged Access Configuration	140
Troubleshooting the Dynamic VLAN Assignment Configuration Issues	142

CHAPTER 15**Configuration Example: External RADIUS Server EAP Authentication 145**

Prerequisites	145
Supported Platforms and Releases	146
Configuring External RADIUS Server EAP Authentication	146
Network Diagram	147
Configuring WLAN for the Client VLAN using CLI	147
Configuring WLAN for the Client VLAN using GUI	148
Configuring ACS 5.2 (RADIUS Server)	154
Verifying External RADIUS Server EAP Authentication Configuration	157

Troubleshooting External RADIUS Server EAP Authentication Configuration Issues 158

CHAPTER 16**External Web Authentication on Converged Access 179**

Example: Configuring WLAN Commands 180

Configuring External Web Authentication with Custom Guest Portal page on ISE 180

Example: External Web Authentication Page 185

Example: Configuring External Web Authentication on Converged Access 186

CHAPTER 17**Installing Wireless Services 191**

Supported Platforms and Releases 191

About Unified Access Cisco 3850 Series Switch 191

Cisco Catalyst 3850 Series Switch: Initial Configuration 192

Joining Access Points 195

Verifying Access Points 198

Troubleshooting Access Point Issues 198

CHAPTER 18**Local Web Authentication with External RADIUS Authentication 199**

List of Global Configuration Commands 199

WLAN Configuration Commands 200

CHAPTER 19**Local Web Authentication on Converged Access 201**

List of Global Configuration Commands 201

Information about Parameter Maps 202

Global Parameter Maps 202

User Defined Parameter Maps 203

Additional Information on Parameter Maps 204

WLAN Configuration Commands 204

Troubleshooting the Configuration 204

CHAPTER 20**PEAP Authentication with Microsoft NPS Configuration 205**

Prerequisites for WLC PEAP Authentication with Microsoft NPS Configuration 205

Supported Platforms and Releases 206

Background Information on PEAP 206

TLS-Encrypted Channel 206

EAP-Authenticated Communication 206

Configuring PEAP with MS-CHAP v2	207
Network Diagram of PEAP with MS-CHAP v2 authentication	208
Configuring Converged Access WLCs (CLI)	209
Configuring Converged Access WLCs (GUI)	209
Configuring the Microsoft Windows Version 2008 Server	211
Configuring the Microsoft Windows 2008 Server as a Domain Controller	211
Installing and configuring the Microsoft server as a CA server	215
Installing the NPS on the Microsoft Windows Version 2008 Server	216
Installing a Certificate on NPS Server	217
Configuring the NPS for PEAP-MS-CHAP v2 Authentication	219
Adding Users to the Active Directory	222
Verifying the PEAP Authentication with Microsoft NPS Configuration	222
Troubleshooting WLC PEAP Authentication with Microsoft NPS Configuration Issues	223

CHAPTER 21
QoS on Converged Access Controllers and Lightweight Access Points 227

Prerequisites	227
Supported Platforms and Releases	227
Information about QoS	228
Configuring Wireless Network for QoS with MQC	229
Default Hardcoded Policies for QoS	230
Platinum	231
Gold	231
Silver	232
Bronze	232
Configuring QoS Manually	234
Identifying and Marking of Voice Traffic	235
Bandwidth and Priority Management at Port Level	237
Bandwidth and Priority Management at SSID Level	239
Call Limitation with CAC	241
Verifying Configuration for QoS	242
show class-map	243
show policy-map	243
show wlan	244
show policy-map interface	244
show platform qos policies	247

show wireless client mac-address <mac> service-policy 248
 Troubleshooting QoS Configuration Issues 248

CHAPTER 22
Configuration Example: TACACS Administrator Access to Converged Access Wireless LAN
Controllers 249

Network Diagram for TACACS Administrator Access 250
 Configuring TACACS Administrator Access to the Converged Access WLCs 250
 Configuring TACACS Administrator Access to Converged Access WLCs 251
 Verifying TACACS Administrator Access to the Converged Access WLC 256
 Troubleshooting TACACS Administrator Access to the Converged Access WLC 256

CHAPTER 23
Configuration Example: Unified Access WLC Guest Anchor with Converged Access 259
Prerequisites 259

Supported Platforms and Releases 260

Unified Access WLC Guest Anchor with Converged Access 261

Network Diagram 262

Part 1: Configuring on the Cisco 5500 Series Anchor Wireless Controller 262

Part 2: Configuring Converged Access Mobility between the Cisco 5500 Series Wireless
 Controller and Cisco Catalyst 3850 Series Switch 264

Part 3 - Configuring on the Foreign Catalyst 3850 Series Switch 266

Verifying the Unified WLC Guest Anchor with Converged Access Configuration 268

Client-side Packet Capture 268

Troubleshooting Unified WLC Guest Anchor with Converged Access Configuration
 Issues 268

CHAPTER 24
VideoStream Troubleshooting 275
Prerequisites 275

Supported Platforms and Releases 275

Overview of the VideoStream flow through WLC 275

VideoStream Limitations 276

VideoStream Flow Through the WLC 276

Troubleshooting the Videostream Issues 277

Verify that Multicast Direct is Enabled 277

Enable Debugging on the WLC 278

Example Debug Command Outputs 278

- Verify the MGID Entries on the WLC 281
- Troubleshooting of Video Quality on the AP 282
- Flow Denied by the WLC 282

CHAPTER 25**Custom Web Authentication Locally Hosted on WLC or an External Server 285**

- Configuring Custom Web Authentication Locally Hosted on WLC 285
- Configuring the Custom HTML pages 286
 - Web Authentication for Login Page 286
 - Web Authentication for Success Page 286
 - Web Authentication for Failure page 287

CHAPTER 26**Wireless Converged Access Chromecast Configuration Example 289**

- Prerequisites 289
 - Supported Platforms and Releases 289
- Configuring Chromecast Support 290
 - Configuring Wireless Multicast Globally 290
 - Configuring WLAN 291

CHAPTER 27**Web Passthrough Configuration Example 293**

- Prerequisites 293
 - Supported Platforms and Releases 293
- Web Passthrough on WLC 294
- Configuring Web Passthrough on Wireless LAN Controller 294
 - Configuring Web Passthrough on Wireless LAN Controller using CLI 295
 - Configuring Web Passthrough on Wireless LAN Controller (GUI) 296
 - Client-side Capture 300
- Verifying the Web Passthrough Configuration 301
- Troubleshooting Web Passthrough Configuration Issues 301

CHAPTER 28**Configuration Examples: WPA2-PSK and Open Authentication 311**

- Prerequisites 311
 - Supported Platforms and Releases 311
- WPA2 PSK and Open Authentication 312
 - Configuring WPA2-PSK Configuration using CLI 312
 - Configuring WPA2-PSK Configuration using GUI 313

Configuring Open Authentication using CLI **315**
Configuring Open Authentication using GUI **316**
Verifying WPA2-PSK and Open Authentication Configuration **316**
Troubleshooting WPA2-PSK and Open Authentication Configuration Issues **318**



CHAPTER

1

Auto Anchor SSID between Wireless LAN Controllers acting as MC

This document describes configuring the web authentication converged access on Cisco Catalyst 3850 Series Switches and Cisco 5500 Series Wireless Controller acting as mobility controller.

- [Configuring WLAN on Foreign Cisco Catalyst 3850 Series Switches, page 1](#)
- [Configuring WLAN on Anchor Cisco 5500 Series Wireless Controller, page 2](#)
- [Global AAA Configuration, page 2](#)
- [Global Parameter-map Configuration, page 2](#)
- [Mobility Summary for Foreign Cisco Catalyst 3850 Series Switches, page 3](#)
- [Mobility Summary for Anchor Cisco 5500 Series Wireless Controller, page 3](#)

Configuring WLAN on Foreign Cisco Catalyst 3850 Series Switches

To configure WLAN on the foreign Cisco Catalyst 3850 Series Switches, use the following commands:

```
wlan converged_access_guest 3 converged_access_guest
client vlan 254
mobility anchor 192.0.2.1 -----> Anchor 3850

no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list wcm_local
security web-auth parameter-map test_web
no shutdown
```

Configuring WLAN on Anchor Cisco 5500 Series Wireless Controller

To configure WLAN on the anchor Cisco 5500 Series Wireless Controller, use the following commands:

```
wlan converged_access_guest 3 converged_access_guest
  client vlan 254
  mobility anchor 192.0.2.1
  no security wpa
  no security wpa akm dot1x
  no security wpa wpa2
  no security wpa wpa2 ciphers aes
  security web-auth
  security web-auth authentication-list rad_ise
  security web-auth parameter-map test_web
  no shutdown
```

Global AAA Configuration

The following are the global AAA configuration commands:

Command or Action	Description or Purpose or Example
aaa authentication login rad_ise group ise	Defines the login authentication method to call under WLAN.
radius server ise address ipv4 192.0.2.1 auth-port 1812 acct-port 1813 key ww-wireless	Configures the RADIUS server. The RADIUS server name is: ise
aaa group server radius ise server name ise	Configures the RADIUS group. The radius group name is: ise

Global Parameter-map Configuration

The following are the global parameter-map configuration commands:

Command or Action	Description or Purpose or Example
parameter-map type webauth global virtual-ip ipv4 1.1.1.1	Defines the virtual IP address.
parameter-map type webauth test_web type webauth banner	The parameter map is called under the WLAN.

Mobility Summary for Foreign Cisco Catalyst 3850 Series Switches

The following displays the mobility controller summary for Cisco Catalyst 3850 Series Switches:

```

Mobility Role                : Mobility Controller
Mobility Protocol Port       : 16666
Mobility Group Name          : 3850
Mobility Oracle               : Disabled
Mobility Oracle IP Address   : 0.0.0.0
DTLS Mode                     : Enabled
Mobility Domain ID for 802.11r : 0xfa71
Mobility Keepalive Interval  : 10
Mobility Keepalive Count     : 3
Mobility Control Message DSCP Value : 0
Mobility Domain Member Count : 4
  
```

Link Status is Control Link Status : Data Link Status

Controllers configured in the Mobility Domain:

IP	Public IP	Group Name	Multicast IP	Link Status
198.51.100.1	-	3850	0.0.0.0	UP : UP
198.51.100.10	198.51.100.10	wlab		UP : UP
198.51.100.15	198.51.100.15	wlab		UP : UP
198.51.100.20	198.51.100.20	converged access		UP : UP

Mobility Summary for Anchor Cisco 5500 Series Wireless Controller

The following displays the mobility controller summary for Cisco 5500 Series Wireless Controller:

```

Mobility Role                : Mobility Controller
Mobility Protocol Port       : 16666
Mobility Group Name          : convergedaccess
Mobility Oracle               : Disabled
Mobility Oracle IP Address   : 0.0.0.0
DTLS Mode                     : Enabled
Mobility Domain ID for 802.11r : 0x81c
Mobility Keepalive Interval  : 10
Mobility Keepalive Count     : 3
Mobility Control Message DSCP Value : 0
Mobility Domain Member Count : 2
  
```

Link Status is Control Link Status : Data Link Status

Controllers configured in the Mobility Domain:

IP	Public IP	Group Name	Multicast IP	Link Status
198.51.100.15	-	converged access	0.0.0.0	UP : UP
198.51.100.20	198.51.100.20	5500		UP : UP



CHAPTER 2

Enabling Central Web Authentication on ISE

The document describes the procedure to enable Central Web Authentication (CWA) on Identity Services Engine (ISE).

- [Enabling CWA on ISE through Global Configuration Commands, page 5](#)
- [Enabling External Policy Server using Dynamic Authorization Commands, page 6](#)
- [Configuring WLAN Commands, page 7](#)
- [Authentication Flow on ISE, page 7](#)

Enabling CWA on ISE through Global Configuration Commands

Use the following commands to enable CWA on ISE to work with Converged Access controllers:

Command or Action	Description/Purpose/Example
show run aaa	Displays the Authorization, Authentication, and Accounting (AAA) related configurations.
aaa authentication login <i>ext_ise</i> group <i>rad_ise</i>	Defines the 'exe ise' login method list which points to the ISE server 'rad_ise'.
aaa authorization network <i>cwa_mac</i> group <i>rad_ise</i>	The authorization method 'cwa_mac' is the mac filter list name which is called under the WLAN configuration. It points to the ISE server 'rad_ise' for authorization.
radius server <i>ise</i> address ipv4 192.0.2.1 auth-port 1812 acct-port 1813 key <i>Cisco123</i>	Displays the RADIUS server definition for the 'ise' server.
aaa group server radius <i>rad_ise</i> server name <i>ise</i>	The 'rad_ise' AAA group server points to the server 'ise'.

<pre>aaa server radius dynamic-author client 192.0.2.1 server-key Cisco123 auth-type any</pre>	Required for Change of Authorization (CoA). For more information on CoA, refer to Dynamic Authorization Commands.
--	---

Enabling External Policy Server using Dynamic Authorization Commands

Use the following dynamic authorization commands to enable an external policy server to dynamically send updates to a device:

Command or Action	Description/Purpose/Example
<pre>radius-server attribute 31 send nas -port-detail mac-only</pre> <p>Or,</p> <pre>radius-server attribute 31 send nas-port-detail</pre>	<p>Sends the calling station ID for MAC.</p> <p>Sends calling station ID for all operating systems other than MAC.</p>
<pre>ip access-list extended ACL-REDIRECT</pre>	<p>This is a url-redirect-acl. To redirect the guest portal, the Identity Services Engine (ISE) returns an AAA override and the redirect URL. The url-redirect-acl is a punt ACL which is a reverse ACL that is used for unified architecture. You need to block access to DHCP, DHCP Server, DNS, DNS server, and ISE server and allow www, 443 port, or the 8443 port as required. The ISE guest portal uses port 8443 and the redirection works with the following ACL:</p> <pre>10 deny udp any eq bootps any 20 deny udp any any eq bootpc 30 deny udp any eq bootpc any 40 deny ip any host 192.0.2.1 50 deny ip any host 192.0.2.2 60 permit tcp any any eq www</pre>
<pre>mac access-list extended cwa_mac permit any any</pre>	<p>The access list is defined based on the MAC Authentication Bypass (MAB) rule.</p>

Related Commands

The following table displays the commands that are associated with dynamic authorization:

Command or Action	Description/Purpose/Example
auth-type (ISO)	Specifies the server authorization type.
Client	Specifies a RADIUS client from which a device accepts CoA and disconnects requests.
Default	Sets the RADIUS application command to default domain and then specifies the username domain options.
Ignore	Overrides a behavior to ignore the parameters that are specified.
Port	Specifies a port on which local RADIUS server listens to.
server-key	Specifies the encryption key shared with the RADIUS clients.

Configuring WLAN Commands

The following example describes the WLAN configuration:

```
wlan cwa_guest 11 cwa_guest
aaa-override
client vlan 263
mac-filtering cwa_mac ----> mac filter pointing to authorization on ISE server
nac
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
no shutdown
```

Authentication Flow on ISE

The ISE logs shown in the following figure displays the authentication flow on the ISE:

The following figure displays the authentication Flow based on the ISE logs:

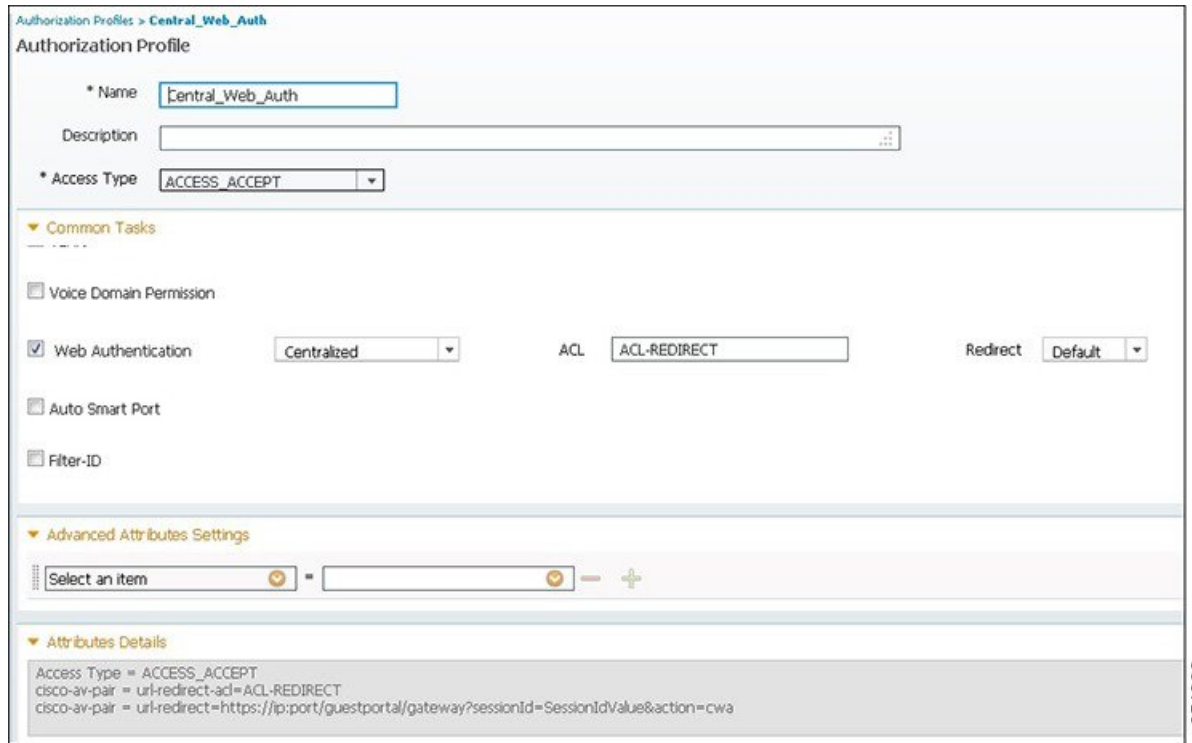
Figure 1: Authentication Flow

Time	Status	Details	Identity	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Event	Failure
Apr 11, 13 01:05:26.796 PM	✓	🔍	viten	38-48-4C-ED-C6-62		3850	2	PermitAccess	Any,Profiled/Workst..	NotApplicable		
Apr 11, 13 01:05:20.116 PM	✓	🔍				3850					Dynamic Authorization succ..	
Apr 11, 13 01:05:20.101 PM	✓	🔍	viten	38-48-4C-ED-C6-62					Any		Guest Authentication Passed	
Apr 11, 13 01:04:11.435 PM	✓	🔍	38-48-4C-ED-C6-62	38-48-4C-ED-C6-62		3850	0	Central_Web_Auth	Profiled/Workstation	Pending	Authentication succeeded	

354302

The following figure displays the authorization profile details for CWA:

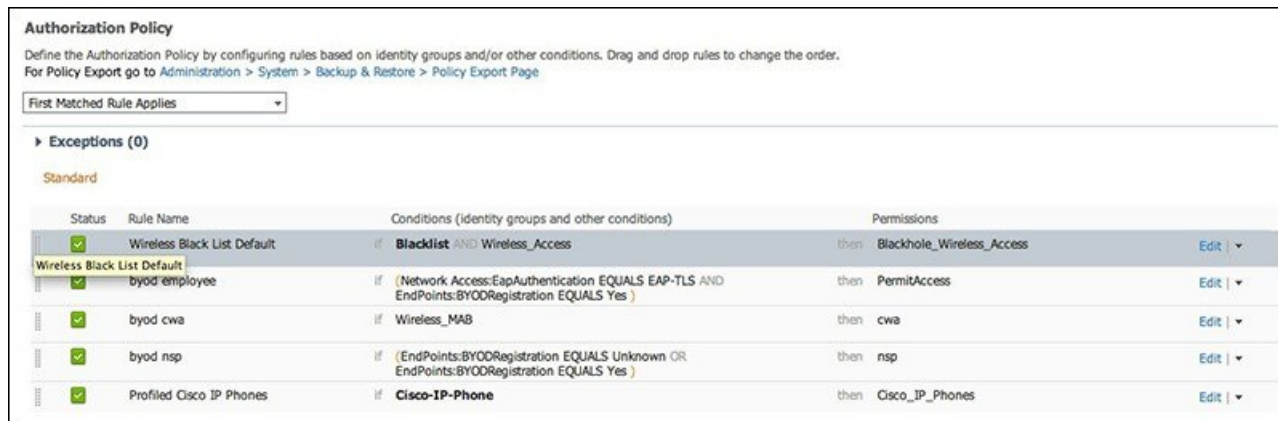
Figure 2: Authorization Profile



354303

The following illustration displays the authorization policy on ISE to redirect Mobile Devices to CWA:

Figure 3: Authorization Policy



**Note**

-
- To integrate ISE into the design, the foreign controller is the only Network Access Device (NAD) that interacts with the ISE.

The foreign controller that is configured for Layer 2 MAC filtering, where the guests access the Wireless MAB, continue the authentication rule on ISE.

- In a static anchor setup that uses controllers and Access Control Server (ACS), if AAA override is enabled to dynamically assign VLAN and QoS, the foreign controller updates the anchor controller with the right VLAN after a Layer 2 authentication (802.1x).

For Layer 3 RADIUS authentication, the RADIUS requests for authentication are sent by the anchor controller.

For more information, refer to the 'Information About Mobility' chapter in the Cisco Wireless LAN Controller Configuration Guide, Release 7.4.



Configuring Auto Anchor and Mobility Groups on Wireless Services

This document describes the procedure to configure an auto anchor between Cisco 5500 Series Wireless Controller and Cisco Catalyst 3850 Series Switches. It also includes the procedure to configure mobility groups on Cisco Catalyst 3850 Series Switches and the procedure to configure a Pre Shared Key (PSK) Service Set Identifier (SSID).

This article considers Cisco Catalyst 3850 Series Switch as both foreign and anchor Wireless LAN Controller (WLC).

- [Supported Platforms and Releases, page 11](#)
- [Configuring Mobility Groups on Cisco Catalyst 3850 Series Switch, page 12](#)
- [Configuring Foreign SSID, page 12](#)
- [Configuring Auto Mobility Groups on Cisco 5500 Series Wireless Controller GUI, page 13](#)
- [Configuring Anchor SSID on Cisco 5500 Series GUI, page 13](#)
- [Testing Client Connectivity on Wireless Services, page 14](#)
- [Configuring Auto Anchor SSID on Cisco Catalyst 3850 Series Switch, page 14](#)
- [Configuring Foreign SSID on Cisco 5500 Series Wireless Controller, page 14](#)
- [Verifying Auto Anchor and Mobility Groups Configuration, page 14](#)

Supported Platforms and Releases

- Cisco Catalyst 3850 Series Switch
- Cisco 5500 Series Wireless Controller

Configuring Mobility Groups on Cisco Catalyst 3850 Series Switch

To configure the Cisco Catalyst 3850 Series Switch for mobility groups, the Cisco Catalyst 3850 Series Switch needs to be in the Mobility Controller (MC) mode.

Device# **configure terminal**

Device(config)# **wireless mobility controller**

To configure the mobility groups on Cisco Catalyst 3850 Series Switch, reset the switch and then configure the mobility groups on the Cisco Catalyst 3850 Series Switch. The following table displays the details that are used to create a sample mobility group for Cisco Catalyst 3850 Series Switch and Cisco 5500 Series Wireless Controller:

Model	IP address	MAC Address	Group Name
5508	192.0.2.1	00:24:97:69:63:c0	mcast_mob
3850	192.0.2.2	20:37:06:cf:5f:f9	Converged Access



Note

- To document the Cisco Catalyst 3850 Series Switch MAC address, use the following command:
show interface vlan 262
- To configure Mobility Controller with the Cisco 5500 Series Wireless Controller information and form a mobility group, use the following command:
wireless mobility group member ip 192.0.2.1 group mcast_mob
- To configure the Cisco Catalyst 3850 Series Switch to be in the Converged Access mobility group, use the following command:
wireless mobility group name Converged Access

The following is the output that is displayed after you perform the above configurations on Cisco Catalyst 3850 Series Switches:

```
Device# do show run | section wireless
qos wireless-default-untrust
wireless mobility controller
wireless mobility group member ip 192.0.2.1 public-ip 192.168.75.44 group mcast_mob
wireless mobility group name Converged Access
wireless management interface Vlan262
```

Configuring Foreign SSID

To create a PSK SSID, the SSID is configured as a foreign SSID and the clients are pushed to Cisco 5500 Series Wireless Controller.

- To create the SSID on Cisco Catalyst 3850 Series Switch, use the following commands:

```
wlan anchor-profile 1 anchor-ssid
no security wpa akm dot1x
security wpa wpa1 ciphers tkip
security wpa akm psk set-key ascii 0 Testlab1
```

- To enable the Service Set Identifier (SSID) to push the clients to the Cisco anchor 5500 WLC, use the following commands:

```
mobility anchor 192.0.2.1
no shutdown
```

Configuring Auto Mobility Groups on Cisco 5500 Series Wireless Controller GUI

To form a mobility group between Cisco Catalyst 3850 Series Switches and Cisco 5500 Series Wireless Controller, perform the following steps:

- 1 To enable New Mobility, navigate to **Controller > Mobility Management > Mobility Configuration**.



Note

- After you enable New Mobility, the Wireless LAN Controller restarts.
- Cisco Catalyst 3850 Series Switch and Cisco 5500 Series Wireless Controller can form a mobility group only if New Mobility is enabled.

- 2 Confirm that Cisco 5500 Series Wireless Controller's Management IP address is listed in the Mobility Controller's public IP address. The WLC is configured to support the new mobility architecture.



Note

You can also enable the Mobility Oracle. However, this is optional.

- 3 Add the Cisco Catalyst 3850 Series Switches in the mobility group. The mobility group is configured. However, approximately a minute is taken for the control path to form as compared to the flat mobility group architecture.



Note

The procedure is similar to configuring any other WLC.

Configuring Anchor SSID on Cisco 5500 Series GUI

To configure an anchor SSID on Cisco 5500 Series GUI, perform the following tasks:

- 1 Configure Cisco 5500 Series Wireless Controller with WPA1 TKIP or WPA2 AES PSK SSID that is pointed to the management interface of the WLC.
- 2 Configure the SSID to be an anchor SSID on the Cisco 5500 Wireless Controller.

Testing Client Connectivity on Wireless Services

To test the connectivity between the client and Cisco Catalyst 3850 Series Switches and Cisco 5500 Series Wireless Controller, perform the following:

- To verify that the client connects to Cisco Catalyst 3850 Series Switch, use the following command:

```
Device# show wireless client summary  
show wireless client mac-address <MAC ADDR> detail
```

The following output displays the connectivity status of the client on Cisco Catalyst 3850 Series Switch:

```
Wireless LAN Id : 1  
Wireless LAN Name: anchor-profile  
Policy Manager State : RUN
```

- To confirm that the client successfully connects to Cisco 5500 Series Wireless Controller, use the following commands:

```
Device# show client summary  
show client detail <mac addr> or use the GUI
```

Configuring Auto Anchor SSID on Cisco Catalyst 3850 Series Switch

To configure the anchor SSID on Cisco Catalyst 3850 Series Switch, perform the following tasks:

- 1 To remove the previous mobility command from the SSID, use the following commands:

```
wlan anchor-profile 1 anchor-ssid  
no mobility anchor 192.0.2.1
```
- 2 To define Cisco Catalyst 3850 Series Switch as the anchor of the SSID, use the following command:

```
mobility anchor 192.0.2.2
```
- 3 To configure SSID to map a client to a particular client VLAN, use the following command:

```
Client vlan 21
```

Configuring Foreign SSID on Cisco 5500 Series Wireless Controller

To configure the Cisco 5500 Series Wireless Controller so that the clients are navigated to Cisco Catalyst 3850 Series Switch, change the mobility anchor settings so that the mobility anchor sends the clients to Cisco Catalyst 3850 Series switch.

Verifying Auto Anchor and Mobility Groups Configuration

The new mobility architecture uses three User Datagram Protocol (UDP) ports to transfer information between WLCs in the mobility group. The three UDPs must be open in both directions for communication to work. The three UDPs to transfer information between WLCs in the mobility group are the following:

UDP Port	Function
16666	Mobility Control Path
16667	Mobility Data Path
16668	Mobility Oracle Path

To display the status of the mobility group, use the following command:

```
Device# show wireless mobility summary
```

The following output displays the summary of the mobility controller:

```
Mobility Role                : Mobility Controller
Mobility Protocol Port       : 16666
Mobility Group Name          : CONVERGEDACCESS
Mobility Oracle IP Address   : 0.0.0.0
DTLS Mode                    : Enabled
Mobility Domain ID for 802.11r : 0x8ff4
Mobility Keepalive Interval  : 10
Mobility Keepalive Count     : 3
Mobility Control Message DSCP Value : 0
Mobility Domain Member Count : 2
```

Link Status is Control Link Status: Data Link Status

The following displays the controllers that are configured in the mobility domain:

IP	Public IP	Group Name	Multicast IP	Link Status
198.51.100.1	-	CONVERGED ACCESS	0.0.0.0	UP : UP
203.0.113.1	192.0.2.254	mcast_mob		UP : UP

Verifying Client Connectivity Status

To verify the status of client connectivity, use the following commands:

```
Device# show wireless mobility controller client summary
```

```
Device# show wireless client summary
```

Verifying Mobility Group Status between Wireless Services

The mobility group between Cisco 5500 Series Wireless Controller and Cisco Catalyst 3850 Series Switch is enabled when the following is displayed on the terminal:

```
Device#
*Apr 17 05:47:59.230: %IOSXE-6-PLATFORM: 1 process wcm: *capwapPingSocketTask:
%MM-6-MEMBER_UP:
Data path to mobility member 198.51.100.1 is UP.
3850#
*Apr 17 05:48:29.228: %IOSXE-6-PLATFORM: 1 process wcm: *mcListen: %MM-6-MEMBER_UP:
Control path to mobility member 203.0.113.1 is UP.
```




Configuring Wireless Multicast on Wireless LAN Controllers

This document describes how to configure wireless multicast, which supports multicast with unicast delivery mechanism, on Cisco Catalyst 3850 Series Switches with WLCs.

- [Prerequisites, page 17](#)
- [Configuring Multicast on Converged Access Platforms, page 18](#)
- [Configuring Multicast Flow on Converged Access, page 18](#)
- [Verifying the Wireless Multicast Configuration on Wireless LAN Controller, page 19](#)
- [Troubleshooting Wireless Multicast Configuration on Wireless LAN Controller Issues, page 21](#)

Prerequisites

We recommend that you have a basic knowledge of the multicast implementation on Cisco Catalyst 3850 Series Switches with WLC.

Supported Platforms and Releases

The information in this document is based on the following software and hardware versions:

- Cisco Catalyst 3850 Series Switch with WLC
- Cisco 3602 Access Point (AP)



Note

The information in this document refers to devices in a specific lab environment. Descriptions of the devices is provided with default configuration values. If you are on a live network, you must understand the potential impact of all the commands.

Configuring Multicast on Converged Access Platforms

To enable multicast on the Converged Access platforms, perform the following tasks:

Step 1 To enable multicast on Cisco Catalyst 3850 Series Switches with WLC, use the **wireless multicast** command in global configuration mode.

```
Device(config)# wireless multicast
```

Note By default, this command enables the multicast with unicast delivery mechanism.

Step 2 To enable Internet Group Management Protocol (IGMP) snooping on Cisco WLC (enabled by default), use the **ip igmp snooping** command in global configuration mode:

```
Device(config)# ip igmp snooping
Device(config)# ip igmp snooping querier
```

Note The **ip igmp snooping querier** command configures Cisco WLC to periodically monitor whether a client still interacts with multicast traffic.

Configuring Multicast Flow on Converged Access

The following steps outline the multicast traffic flow on the Converged Access. Refer to the Configuring Multicast on Converged Access Platforms section for configuration details.

-
- Step 1** Cisco WLC intercepts the IGMP packets sent by wireless clients.
If there is an existing entry for the multicast group-vlan-source combination client, Cisco WLC updates the IGMP timers.
If this is a new entry, Cisco WLC creates a Multicast Group Identifier (MGID) based on the tuple (source, group, and VLAN) with a multiple range, either between 1 and 4,095 for Layer 2 (L2) or between 4,160 and 8,191 for Layer 3 (L3).
- Step 2** The IGMP packet is forwarded as an upstream.
- Step 3** The MGID entry is sent to an AP along with the associated client information, to receive the multicast traffic on a client.
- Step 4** Cisco WLC forwards the traffic to the AP appropriately, if the delivery mechanism is multicast with unicast .
Note If the delivery mechanism is multicast, Datagram Transport Layer Security (DTLS) encryption and Quality of Service (QoS) marking are not applicable.
- Step 5** The AP then forwards the traffic to each client, as per the requirement.
-

Verifying the Wireless Multicast Configuration on Wireless LAN Controller

To verify the configuration, perform the following steps:

Step 1 To verify whether multicast is enabled properly, use the **show wireless multicast** command in EXEC mode:

```
Device# show wireless multicast
Multicast: Enabled
AP Capwap Multicast: Multicast
AP Capwap Multicast group Address: 239.255.255.249
AP Capwap Multicast QoS Policy Name: unknown
AP Capwap Multicast QoS Policy State: None
Wireless Broadcast: Disabled
Wireless Multicast non-ip-mcast: Disabled
```

```
Vlan Non-ip-mcast Broadcast MGID
-----
1          Enabled Enabled Disabled
10         Enabled Enabled Enabled
24         Enabled Enabled Enabled
25         Enabled Enabled Enabled
26         Enabled Enabled Enabled
32         Enabled Enabled Enabled
```

Step 2 To verify whether an MGID entry is created for the multicast group the client attempts to join (239.255.255.250 is used as an example), use the **show wireless multicast group summary** command in EXEC mode:

```
Device# show wireless multicast group summary
IPv4 groups
-----
MGID   Source   Group           Vlan
-----
4160   0.0.0.0   239.255.255.250 32
```

Step 3 To verify whether the required client is added to the MGID table, use the **show wireless multicast group** command in EXEC mode:

```
Device# show wireless multicast group 239.255.255.250 vlan 32
Source : 0.0.0.0
Group  : 239.255.255.250
Vlan   : 32
MGID   : 4160

Number of Active Clients : 1
Client List
-----
```

```

Client MAC      Client IP      Status
-----
1410.9fef.272c  192.168.24.50  MC_ONLY

```

Step 4 To verify whether the required MGID entry is added to the AP for this client, use the **show capwap mcast mgid** command in EXEC mode:

```
Device# show capwap mcast mgid id 4160
```

```

L3 MGID = 4160 WLAN bitmap = 0x0001
Slot map/tx-cnt: R0:0x0000/0 R1:0x0001/1499
Clients per Wlan
Wlan: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

```

!! This shows the number of clients per slot, per Service Set Identification (SSID) on the AP.

```

Normal Mcast Clients R0: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Normal Mcast Clients R1: 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
rx pkts = 1499 drp pkts = 0
tx packets:
wlan : 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
slots0 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
slots1 : 1499 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

```

```

Normal Mcast Clients:
Client: 1410.9fef.272c --- Qos User Priority: 0

```

Note Consider the counters on the received and transmitted packets. This information is useful to determine whether the AP properly forwards the packets to the client.

Step 5 To view all the client-multicast group mappings, use the **show ip igmp snooping igmpv2-tracking** command in EXEC mode. This command provides an overview of the connected clients and the joined groups.

```
Device# show ip igmp snooping igmpv2-tracking
```

```

Client to SGV mappings
-----

```

```

Client: 192.168.24.50 Port: Ca1
Group: 239.255.255.250 Vlan: 32 Source: 0.0.0.0 blacklisted: no

```

!! If the client has joined more than one multicast group, all the group entries will be shown here one after the other.

```

SGV to Client mappings
-----

```

```

Group: 239.255.255.250 Source: 0.0.0.0 Vlan: 32
Client: 192.168.24.50 Port: Ca1 Blacklisted: no

```

!! If there is more than one client entry, these will be shown here.

Step 6 To verify the MGID from Cisco WLC, use the **show ip igmp snoop wireless mgid** command in EXEC mode:

```
Device# show ip igmp snoop wireless mgid
```



```
Total number of L2-MGIDs = 33
```

```
Total number of MCAST MGIDs = 0
```

```
Wireless multicast is Enabled in the system
```

```
Vlan bcast nonip-mcast mcast mDNS-br mgid StdbY Flags
```

```
1 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
100 Enabled Disabled Enabled Enabled Disabled 0:1:1:0
115 Enabled Disabled Enabled Enabled Disabled 0:1:1:0
517 Enabled Disabled Enabled Enabled Disabled 0:1:1:0
518 Enabled Disabled Enabled Enabled Disabled 0:1:1:0
519 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
520 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
521 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
522 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
523 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
524 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
525 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
526 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
527 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
528 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
529 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
530 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
531 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
1002 Enabled Enabled Enabled Enabled Disabled 0:0:1:0
1003 Enabled Enabled Enabled Enabled Disabled 0:0:1:0
1004 Enabled Enabled Enabled Enabled Disabled 0:0:1:0
1005 Enabled Enabled Enabled Enabled Disabled 0:0:1:0
```

```
Index MGID (S, G, V)
```

```
-----
```

Troubleshooting Wireless Multicast Configuration on Wireless LAN Controller Issues

To troubleshoot the configuration issues from Cisco WLC, use the following commands:

```
debug igmp ipmp snooping
debug ip igmp snooping 239.255.255.250
debug ip igmp snooping querier
debug ip igmp snoop wireless ios client-tracking
debug ip igmp snoop wireless ios events
debug ip igmp snoop wireless ios error
debug ip igmp snoop wireless ap detail
debug ip igmp snoop wireless ap error
```

debug ip igmp snoop wireless ap event

debug ip igmp snoop wireless ap message

debug platform l2m-igmp

debug l2mcast wireless ios error

debug l2mcast wireless ios mgid

debug l2mcast wireless ios spi

debug l2mcast wireless ios ipc

debug l2mcast wireless ios broadcast



Note

To avoid performance issues, ensure that you use the relevant multicast debug commands.

The following is an output for the **show debug** command:

```
Device# show debug

NG3K Wireless:
  NG3K WIRELESS Error DEBUG debugging is on
L3 Multicast platform:
  NGWC L3 Multicast Platform debugs debugging is on
L2M IGMP platform debug:
  NGWC L2M IGMP Platform debugs debugging is on
  NGWC L2M IGMP SPI debugs debugging is on
  NGWC L2M IGMP Error debugs debugging is on
IP multicast:
  IGMP debugging is on for 239.10.10.11
IGMP tracking:
  igmpv2 tracking debugging is on
L2MC Wireless:
  L2MC WIRELESS SPI EVENTS debugging is on
  L2MC WIRELESS REDUNDANCY EVENTS debugging is on
  L2MC WIRELESS ERROR debugging is on
IGMP Wireless:
  IGMP SNOOP wireless IOS Errors debugging is on
  IGMP SNOOP wireless IOS Events debugging is on

igmp/snooping/wireless/ap/event debugging is on
multicast/event debugging is on
igmp/snooping/wireless/ap/message/rx debugging is on
igmp/snooping/wireless/ap/message/tx debugging is on
wireless/log debugging is on
l2multicast/error debugging is on
igmp/snooping/wireless/ap/error debugging is on
multicast/error debugging is on
multicast debugging is on
l2multicast/event debugging is on
wireless/platform debugging is on
igmp/snooping/wireless/ap/detail debugging is on
```

The following sample output displays MGID creation on the Cisco WLC:

```
*Sep 7 00:12:11.029: IGMP SN: Received IGMPv2 Report for group 239.255.255.250 received
on Vlan 32, port Cal
*Sep 7 00:12:11.029: IGMP SN: group: Received IGMPv2 report for group 239.255.255.250
from Client 192.168.24.50 received on Vlan 32, port Cal
*Sep 7 00:12:11.029: (l2mcast_tracking_is_client_blacklisted) Client: 192.168.24.50
Group: 239.255.255.250 Source: 0.0.0.0 Vlan: 32 Port: Cal
*Sep 7 00:12:11.029: (l2mcsn_process_report) Allocating MGID for Vlan: 32 (S,G):
:239.255.255.250
*Sep 7 00:12:11.029: (l2mcast_wireless_alloc_mcast_mgid) Vlan: 32 Source: 0.0.0.0
Group: 239.255.255.250
*Sep 7 00:12:11.030: (l2mcast_wireless_alloc_mcast_mgid) Hash entry added!
*Sep 7 00:12:11.030: (l2mcast_wireless_track_and_inform_client) Protocol: IGMP SN
```

```

Client-address: 192.168.24.50 (S,G,V): 0.0.0.0 239.255.255.250 32 Port: Cal, MGID:
4160 Add: Add
*Sep 7 00:12:11.030: (l2mcast_get_client_params) Client Addr: 192.168.24.50 Client-id:
40512055681220617 Mcast-vlan: 32(l2mcast_wireless_inform_client) Protocol: IGMP SN
Client-address: 192.168.24.50 (S,G,V): 0.0.0.0 239.255.255.250 32 Port: Cal, iifid =
0x9667c000000004 MGID: 4160 Add: Add
*Sep 7 00:12:11.030: (l2mcast_wireless_inform_client) Sent INFORM CLIENT SPI
*Sep 7 00:12:11.030: (l2mcast_wireless_track_and_inform_client)
l2mcast_wireless_inform_client passed
*Sep 7 00:12:11.032: %IOSXE-7-PLATFORM: 1 process wcm: IGMP has sent the
WCM_INFORM_CLIENT with ^I client_id = 40512055681220617/8fed8000000009 ^I capwap id =
42335320837980164 ^I mac_addr = 1410.9fef.272c ^I num_entry = 1

```

The entry created on the Cisco IOS is passed to the Wireless Control Module (WCM) process. The WCM process verifies and adds the entry.

```

*Sep 7 00:12:11.032: %IOSXE-7-PLATFORM: 1 process wcm: i = 0, source = 0.0.0.0 group =
239.255.255.250 client_ip = 192.168.24.50 vlan = 32, mgid = 4160 add = 1
*Sep 7 00:12:11.032: %IOSXE-7-PLATFORM: 1 process wcm: in igmp wcm_client_join_callback
source = 0.0.0.0 group = 239.255.255.250 client_ip = 192.168.24.50 vlan = 32
client_mac = 1410.9fef.272c mgid = 4160
*Sep 7 00:12:11.032: %IOSXE-7-PLATFORM: 1 process wcm: apfMswtp_iifid = 9667c000000004
capwap_if_id = 9667c000000004
*Sep 7 00:12:11.032: %IOSXE-7-PLATFORM: 1 process wcm: rrc_manual_mode = 0
rrc_status = 2
*Sep 7 00:12:11.032: %IOSXE-7-PLATFORM: 1 process wcm: locking mgid Tree in file
bcast_process.c line 491
*Sep 7 00:12:11.033: %IOSXE-7-PLATFORM: 1 process wcm: allocateL3mgid: mgid entry AVL
search key dump:
*Sep 7 00:12:11.033: %IOSXE-7-PLATFORM: 1 process wcm: 00000000: 00 00 00 00 ef 01 01
01 00 08 ff ff ff ff ff ff .....^M 00000010: ff ff ff ff ff ff ff ff ff ff
ff ff ff ff ff ff .....^M 00000020: ff ff ..^M
*Sep 7 00:12:11.033: %IOSXE-7-PLATFORM: 1 process wcm: mcast_group_client_lookup:
Lookup failed for client with mac 1410.9fef.272c
*Sep 7 00:12:11.033: %IOSXE-7-PLATFORM: 1 process wcm: unlocking mgid Tree in file
bcast_process.c line 624
*Sep 7 00:12:11.033: %IOSXE-7-PLATFORM: 1 process wcm: spamLradSendMgidInfo: ap =
0c85.25c7.9ad0 slotId = 1, apVapId = 1, numOfMgid = 1 join = 1 isL2Mgid = 0,
mc2ucflag = 0, qos = 0
*Sep 7 00:12:11.033: %IOSXE-7-PLATFORM: 1 process wcm: mscbApMac = 0c85.25c7.9ad0
client_mac_addr = 1410.9fef.272c slotId = 1 vapId = 1 mgid = 4160 numOfSGs = 2,
rrc_status = 2

```

To troubleshoot configuration issues from the AP, use the following commands:

debug capwap mcast fwd

debug capwap mcast query

The following is a sample output of the **debug** commands:

```

*Sep 7 06:00:38.099: CAPWAP MCAST: capwapDecodeMgidPayload: mgidTypeStr L3 IGMP MGID
ADD,mgidType 53,mgid=4160,mgid operation=1
*Sep 7 06:00:38.099: CAPWAP MCAST: capwapAddMgidEntry: slotId= 1, client_mac=
1410.9fef.272c, mgid= 4160, wlanid= 0, mc2ucflag= 0, priority= 0, downpriority= 0
L3 mgid flag = L3 IGMP MGID .
*Sep 7 06:00:38.099: CAPWAP MCAST: allocateMgidEntry: mgid = 4160, isL3Mgid=1
*Sep 7 06:00:38.099: CAPWAP MCAST: capwap_bss_mgid_enable:MGID 4160 enable -
Slot=1 WLAN=1
*Sep 7 06:00:38.099: CAPWAP MCAST: L3 IGMP MGID ADD MGID = 4160 SUCCESSFUL!!

```



Note

- When an MGID entry is added, the VLAN ID displayed in the output is 0.
- The output displays the correct VLAN mapping even after the MGID entry is deleted.

Use the following commands for further analysis from Cisco WLC:

show wireless client summary

show wcdb database all

show wireless multicast group summary

show wireless multicast group <ip> vlan <id>

show wireless multicast source <ip> group <ip> vlan <id>

show ip igmp snooping wireless mgid

show ip igmp snooping igmpv2-tracking

Use the following commands for further analysis from the AP:

show capwap mcast mgid all

show capwap mcast mgid id <id>



Note

- The number of multicast groups to which each client can be associated is limited to 16. When the client sends a join request for a possible 17th group, the group is created on the Cisco IOS. But, on the WCM, a deny message is sent to Cisco IOS. The Cisco IOS then deletes that group.
- Currently, only IGMP V2 is supported. If a client uses IGMP V3, MGID is not created on the on the Cisco WLC. For this reason, the source address in the source, group, and VLAN is always 0.0.0.0.
- The number of L3 MGIDs supported on the Converged Access range from 4,160 to 8,191. Because an MGID entry is a combination of the multicast address and VLAN, there can only be 4,000 such combinations. This can be a limitation in large environments.
- The Bonjour feature is not supported across VLANs. This is because of the IP address 224.0.0.251, which is a link-local multicast address. Cisco Catalyst 3850 Series Switches with WLCs do not snoop link-local addresses like other Catalyst switches. Therefore, you will see the following error message:

```
IGMPSN: group: Received IGMPv2 report for group 224.0.0.251 from Client 192.168.24.94
received on Vlan 32, port Ca93 with invalid group address.
```



Converged Access Consolidated Quick Reference Templates for Wireless LAN

This document describes the CLI configuration templates for basic and known Layer 2 and Layer 3 WLANs configurations. The configuration templates are used for the lab recreations and customer initial installations of Cisco Catalyst 3850 Series Switches.

- [Prerequisites, page 25](#)
- [Configuration Templates for Layer 2 Security, page 26](#)
- [Configuration Templates for Layer 3 Security, page 28](#)

Prerequisites

- We recommend that you have a basic knowledge and understanding of Converged Access Release 3.3 or later.
- Switch Virtual Interfaces (SVIs) and DHCP pools or snooping must be configured.

Supported Platforms and Releases

This document is not restricted to specific software and hardware versions.



Note

The information in this document refers to devices in a specific lab environment. Descriptions of the devices is provided with default configuration values. If you are on a live network, you must understand the potential impact of all the commands.

Configuration Templates for Layer 2 Security

Open WLAN No Security Template

The following is the template for Open WLAN No Security:

```
wlan 1 name testwlan ssid testwlan
client vlan 20
no security wpa
no shutdown
```

Static Wired Equivalent Privacy Template

The following is the template for Static Wired Equivalent Privacy (WEP):

```
wlan staticWEP 6 staticWEP
client vlan 79
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security static-wep-key encryption 40 ascii 0 Cisco 1
session-timeout 1800
no shutdown
```

MAC Filter - Local Database Template

The following is the template for MAC Filter - Local Database:

```
username 24770319eB75 mac

aaa new-model
aaa authorization network test_mac local

wlan macfiltering 6 macfiltering
client vlan Vlan7
mac-filtering test_mac
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
no shutdown
```

MAC Filter - External RADIUS Template

The following is the template for MAC Filter - External RADIUS:

```
aaa new-model
aaa group server radius wcm_rad

server name RAD_EXT
subscriber mac-filtering security-mode mac
mac-delimiter colon

radius server RAD_EXT
address ipv4 x.x.x.x auth-port 1812 acct-port 1813
key cisco
```

```

aaa authorization network wcm_macfilter group wcm_rad

wlan macfiltering 1 macfiltering
client vlan Vlan7
mac-filtering wcm_macfilter
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
no shutdown

```

Wireless Protected Access 2 Pre-Shared Key Template

The following is a template for Wireless Protected Access 2 (WPA2) Pre-Shared Key (PSK):

```

wlan wpa2psk 1 wpa2psk
client vlan 20
no security wpa akm dot1x
security wpa akm psk set-key ascii 0 Cisco123
no shutdown

```

802.1x Local Extensible Authentication Protocol Authentication Template

The following is the template for 802.1x Local Extensible Authentication Protocol (EAP):

```

user-name test
privilege 15

password 0 cisco
type network-user description pass=cisco
aaa new-model
aaa authentication dot1x default local
aaa authorization credential-download author_list local
aaa authentication dot1x authen_list local
aaa local authentication authen_list authorization author_list
dot1x system-auth-control
eap profile PEAPProfile
method ?
    fast          EAP-FAST method allowed
    gtc           EAP-GTC method allowed
    leap         EAP-LEAP method allowed
    md5          EAP-MD5 method allowed
    mschapv2     EAP-MSCHAPV2 method allowed
    peap         EAP-PEAP method allowed
    tls          EAP-TLS method allowed

method peap
method mschapv2
wlan TestCONVERGEDACCESS 1 TestCONVERGEDACCESS
client vlan VLAN0080
ip dhcp server 192.0.2.14
local-auth PEAPProfile

```

802.1x on External RADIUS Template

The following is the template for 802.1x on External RADIUS:

```

aaa new-model
!
!
aaa group server radius ACS
server name ACS
!
aaa authentication dot1x ACS group ACS

```

```

radius server ACS
  address ipv4 203.0.113.50 auth-port 1645 acct-port 1646
  key Cisco123

dot1x system-auth-control

wlan EAPFAST 4 EAPFAST
  client vlan VLAN0020
  security dot1x authentication-list ACS
  session-timeout 1800
  no shutdown

```

Configuration Templates for Layer 3 Security

Web Passthrough Template

The following is the template for Web Passthrough:

```

parameter-map type webauth global
  type consent
  virtual-ip ipv4 192.0.2.1
  !
  !
parameter-map type webauth web
  type consent

wlan Webauth 9 Webauth
  client vlan VLAN0020
  no security wpa
  no security wpa akm dot1x
  no security wpa wpa2
  no security wpa wpa2 ciphers aes
  security web-auth
  security web-auth parameter-map web
  session-timeout 1800

```

Local Authentication Template

The following is the template for Local Web Authentication:

```

aaa new-model
aaa authentication login wcm_local local
aaa authorization network default local
aaa authorization credential-download default local
username test password 0 test12345
parameter-map type webauth global
  virtual-ip ipv4 1.1.1.1
parameter-map type webauth test_web
  type webauth
  banner c test webauth c
ip http server
ip http authentication local
ip http secure-server

wlan local_webauth 11 local_webauth
  client vlan 263
  no security wpa
  no security wpa akm dot1x
  no security wpa wpa2
  no security wpa wpa2 ciphers aes
  security web-auth
  security web-auth authentication-list wcm_local
  security web-auth parameter-map test_web

```


Web Authentication with External RADIUS Authentication Template

The following is the template for Web Authentication and External RADIUS Authentication:

```
radius server ise
    address ipv4 192.0.2.119 auth-port 1812 acct-port 1813
    key Cisco123
aaa group server radius rad_ise
server name ise

aaa authentication login ext_ise group rad_ise
parameter-map type webauth global
    virtual-ip ipv4 1.1.1.1
parameter-map type webauth test_web
    type webauth
    banner c test webauth c
wlan local_webauth 11 local_webauth
client vlan 263
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list ext_ise
security web-auth parameter-map test_web
no shutdown
```

External Web Authentication Template

The following is the template for External Web Authentication:

```
//Parameter Map //
parameter-map type webauth test_web
type webauth
redirect for-login https: //192.0.2.119:8443 /guestportal
/portals/external_webauth/portal.jsp

redirect portal ipv4 192.0.2.119

    redirect on-success <url> //Optional//
    redirect on-failure <url> //Optional//

banner

//Pre auth ACL//
ip access-lists extended preauth_ise
    10 permit udp any eq bootps any
    20 permit udp any any eq bootpc
    30 permit udp any eq bootpc any
    40 permit udp any any eq domain
    50 permit udp any eq domain any
    60 permit ip any host 192.0.2.119
    70 permit ip host 192.0.2.119 any
wlan external_webauth 11 external_webauth
client vlan 263
ip access-group web preauth_ise
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list ext_ise
security web-auth parameter-map test_web
no shutdown
```

Customized Local Web Authentication Template

The following is the template for Customized Web Authentication with Local Authentication:

```

ip http server
ip device tracking

aaa new-model
aaa authentication login local_webauth local
aaa authorization network default local
aaa authorization credential-download default local

username <username> password 0 <password>

FTP Configuration for file transfer:
ip ftp username <username>
ip ftp password <password>

Upload custom html files to flash: with command:
Device# copy ftp: //x.x.x.x /webauth_login.html flash:

Example of flash content:
Device# dir flash:

Directory of flash:/
64649  -rw-      1164   Oct 7 2013 04:36:23 +00:00  webauth_failure.html
64654  -rw-      2047   Oct 7 2013 13:32:38 +00:00  webauth_login.html
64655  -rw-      1208   Oct 7 2013 04:34:12 +00:00  webauth_success.html
64656  -rw-       900   Oct 7 2013 04:35:00 +00:00  webauth_expired.html
64657  -rw-     96894   Oct 7 2013 05:05:09 +00:00  web_auth_logo.png
64658  -rw-     23037   Oct 7 2013 13:17:58 +00:00  web_auth_cisco.png
64660  -rw-      2586   Oct 7 2013 13:31:27 +00:00  web_auth_aup.html

parameter-map type webauth global
virtual-ip ipv4 1.1.1.1

parameter-map type webauth custom
type webauth
redirect on-success http://www.cisco.com
banner text ^C CC global ip for redirect ^C
  custom-page login device flash:webauth_login.html
  custom-page success device flash:webauth_success.html
  custom-page failure device flash:webauth_failure.html
  custom-page login expired device flash:webauth_expired.html

wlan cisco 1 cisco
client vlan Vlanx
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list local_webauth
security web-auth parameter-map custom
session-timeout 1800
no shutdown

```

Auto Anchor Web Authentication Template

The following is the template for Auto Anchor Web Authentication:

```

//Verify//
show wireless mobility summary
<snip>

```

IP	Public IP	Group Name	Multicast IP	Link Status
-----	-----	-----	-----	-----

```
192.168.100.8 - CONVERGEDACCESS 0.0.0.0 UP : UP
192.168.100.15 192.168.100.15 5760 UP : UP
```

```
radius server ise
    address ipv4 192.0.2.119 auth-port 1812 acct-port 1813
    key Cisco123
aaa group server radius rad_ise
server name ise

aaa authentication login ext_ise group rad_ise
parameter-map webauth global
    virtual-ip ipv4 1.1.1.1
parameter-map type webauth test_web
    type webauth
    banner
```

WLAN configs on the Foreign 5760

```
wlan convergedaccess_guest 3 convergedaccess_guest
client vlan 254
mobility anchor 192.0.2.8 //Anchor
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list wcm_local
security web-auth parameter-map test_web
no shutdown
```

WLAN configs on the Anchor 5760

```
wlan convergedaccess_guest 3 convergedaccess_guest
client vlan 254
mobility anchor 192.0.2.8 //Local
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list rad_ise
security web-auth parameter-map test_web
no shutdown
```




Converged Access Controller AP Join Issue Troubleshoot with Traces

This document describes about trace commands that are used to troubleshoot Access Point (AP) join issues on converged access controllers and some of the common reasons for AP join failure.

- [Prerequisites, page 33](#)
- [AP Join Sequence and Troubleshoot, page 35](#)
- [Common Reasons for AP Join Failure, page 46](#)
- [General Technical Tips on Trace Commands , page 49](#)

Prerequisites

You should have basic knowledge on following topics:

Supported Platforms and Releases

The information in this document is based on a Cisco Catalyst 3850 Series Switch that runs software Version 3.3.0 SE.

- Lightweight Access Point Protocol (LWAPP) / Control and Provisioning of Wireless Access Points (CAPWAP).
- Lightweight Access Point (LAP) and Wireless LAN Controller (WLC) configurations for basic operation.

**Note**

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Associated Products

The following listed products are applicable to all converged access controllers:

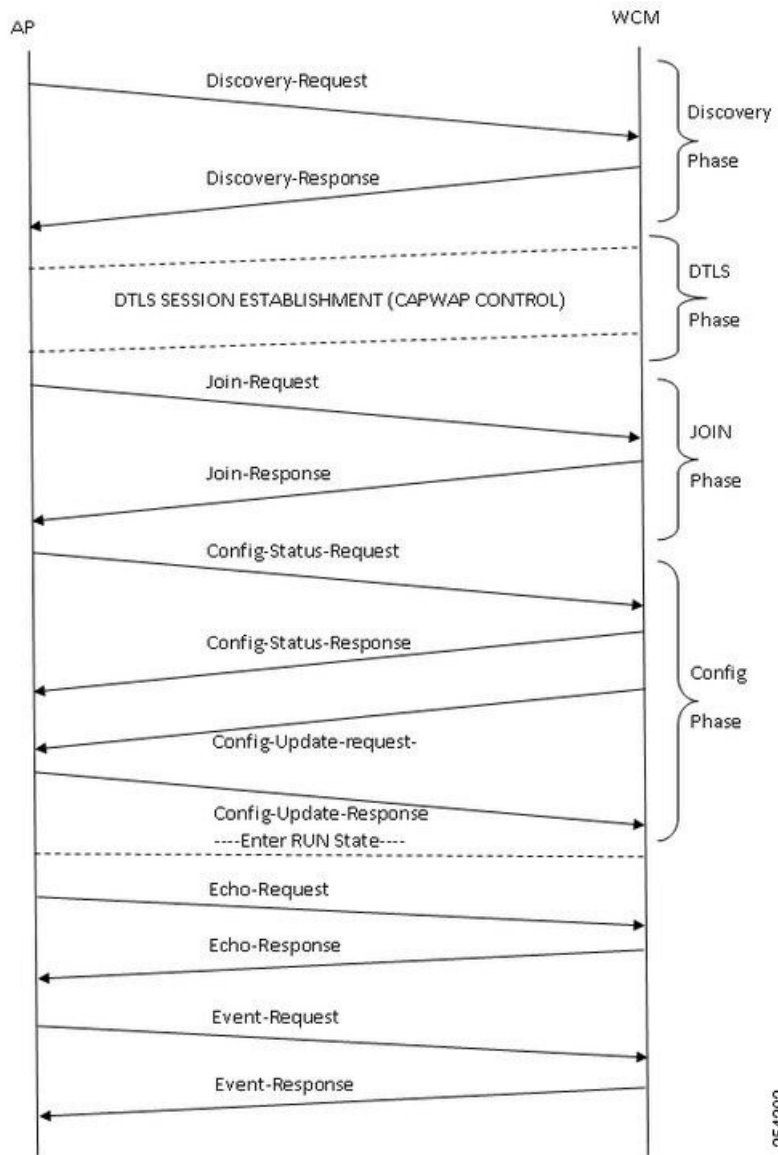
- Cisco Catalyst 3560 Series Switches
- Cisco Catalyst 3850 Series Switches

AP Join Sequence and Troubleshoot

AP Join Sequence

The following figure depicts the join sequences between an Access Point and Wireless Control Module (WCM).

Figure 4: Join sequences between an Access Point and Wireless Control Module (WCM).



Troubleshoot

Basic Steps

Perform the following task to troubleshoot the AP join issues on converged access controllers:

- 1 First, confirm that the AP is able to pull an IP address.
- 2 From the switch where the AP is plugged in, enter the following command: **# show cdp neighbor <port_id> detail**



Note

The AP should be connected to the Cisco Catalyst 3850 Series Switch and the switchport must be configured as:

```
Interface gig <>
Switchport mode access
Switchport access vlan x
```

(Where x is the wireless management interface and vlan x configured on the Cisco Catalyst 3850 Series Switch)

- 3 Make sure that the WLC can ping the IP address and vice versa.
- 4 To verify that a wireless mobility controller (MC) is configured on the network, enter the following command: **#show wireless mobility summary**



Note

If you logged into a Mobility Agent, ensure that the tunnel mobility controller is active.

- 5 Confirm the AP license is enabled on the MC: **#show license right-to-use summary**
- 6 Authorize the correct country code is enabled: **#show wireless country configured**

Traces from Controller

If AP fails even after configuration is successful, use the following trace commands on the controller in order to troubleshoot CAPWAP and AP join:

- **#Set trace capwap**
- **#Set trace capwap ap**
- **#Set trace group-ap**

Based on the review of trace outputs, the group-ap traces provides more significant output to troubleshoot the AP join. Hence this trace (unfiltered) is discussed in detail.

Refer to the General Technical Tips on Trace Commands section for more information about filtering options and limitations on this trace.



Note Sample output (filtered and unfiltered) for **capwap** and **capwap ap** is included for reference.

Default settings of the group-ap

To view the default settings of the **group-ap** trace, enter the following command:

```
#show trace settings group-ap
```

```
Buffer Properties:
Feature Name                               Size           Level
-----
capwap/ap/event                           0              warning
dtls/ap/event                              0              warning
iosd-wireless/capwap                       0              warning

Feature-Name: capwap/ap/event
Filters: None
Feature-Name: dtls/ap/event
Filters: None
Feature-Name: iosd-wireless/capwap
Filters: None
```



Note By default, there are no filters set on any of the traces.

Clearing the group-ap

To clear the trace buffer that corresponds to the **group-ap** trace, enter the following command:

```
#set trace control group-ap clear
```

Setting the trace level group-ap

Enter the following command to set the trace level for the **group-ap**:

```
#set trace group-ap level ?
debug    Debug-level messages (7)
default  Unset Trace Level Value
err      Error conditions (3)
info     Informational (6)
warning  Warning conditions (4)
```



Note Use the **#set trace group-ap level debug** to debug while you troubleshoot the issues.

Verifying the tracing level

To verify the tracing level, enter the following command:

```
#show trace settings group-ap
```

```
Buffer Properties:
Feature-Name                               Size           Level
-----
capwap/ap/event                           0              debug
dtls/ap/event                              0              debug
iosd-wireless/capwap                       0              debug

Feature-Name: capwap/ap/event
```

```

Filters: None
Feature-Name: dtls/ap/event
Filters: None
Feature-Name: iosd-wireless/capwap
Filters: None

```

Viewing trace output of group-ap

To view the trace output of **group-ap**, enter the following command:

```
# show trace messages group-ap
```

Discovery-Request / Response

```

[11/14/13 14:50:17.484 UTC 702f4a 8528] f84f.57ca.3860 Discovery Request from
10.201.234.24:18759

[11/14/13 14:50:17.484 UTC 702f4b 8528] f84f.57ca.3860 Discovery apType = 0,
apModel = AIR-CAP2602I-A-K9, Discovery supportedRadios = 0, incomingRadJoinPriority
= 1, Discovery versionNum = 167863296

[11/14/13 14:50:17.484 UTC 702f4c 8528] f84f.57ca.3860 Join Priority Processing
status =0, Incoming Ap's Priority 1, MaxLrads = 50, joined Aps =0

[11/14/13 14:50:17.484 UTC 702f4d 8528] f84f.57ca.3860 Validated Discovery request
with dest ip : 255.255.255.255 from AP 10.201.234.24. Response to be sent using
ip : 10.201.234.4

[11/14/13 14:50:17.484 UTC 702f4e 8528] Encode static AP manager 10.201.234.4,
AP count 0

[11/14/13 14:50:17.484 UTC 702f4f 8528] acEncodeMwarTypePayload encode mwarType = 0
in capwapMwarTypePayload.

[11/14/13 14:50:17.484 UTC 702f50 8528] f84f.57ca.3860 Discovery Response sent to
10.201.234.24:18759

[11/14/13 14:50:27.484 UTC 57 8528] Connection not found in hash table - Table empty.

```

DTLS-Handshake

```

[11/14/13 14:50:27.484 UTC 702f51 8528] DTLS connection not found, creating new
connection for 10:201:234:24 (18759) 10:201:234:4 (5246)

[11/14/13 14:50:27.484 UTC 702f52 8528] acDtlsCallback: entering...

[11/14/13 14:50:27.484 UTC 702f53 8528] acDtlsCallback: cb->code 10

[11/14/13 14:50:27.484 UTC 58 8528] Certificate installed for PKI based
authentication.

[11/14/13 14:50:27.484 UTC 59 8528] Incremented concurrent handshaking count 1

[11/14/13 14:50:27.484 UTC 5a 8528] f84f.57ca.3860 record=Handshake epoch=0
seq=0

[11/14/13 14:50:27.484 UTC 5b 8528] f84f.57ca.3860 msg=ClientHello len=44 seq=0
frag_off=0 frag_len=44

[11/14/13 14:50:27.485 UTC 5c 8528] f84f.57ca.3860 Handshake in progress...

[11/14/13 14:50:27.489 UTC 5d 8528] f84f.57ca.3860 record=Handshake epoch=0 seq=1

[11/14/13 14:50:27.489 UTC 5e 8528] f84f.57ca.3860 msg=ClientHello len=76
seq=1 frag_off=0 frag_len=76 (with cookie)

[11/14/13 14:50:27.490 UTC 5f 8528] f84f.57ca.3860 Handshake in progress...

[11/14/13 14:50:27.670 UTC 60 8528] f84f.57ca.3860 record=Handshake epoch=0 seq=2

```

```
[11/14/13 14:50:27.670 UTC 61 8528] f84f.57ca.3860 msg=Certificate len=1146
seq=2 frag_off=0 frag_len=519
[11/14/13 14:50:27.670 UTC 62 8528] f84f.57ca.3860 Handshake in progress...
[11/14/13 14:50:27.670 UTC 63 8528] f84f.57ca.3860 record=Handshake epoch=0 seq=3
[11/14/13 14:50:27.670 UTC 64 8528] f84f.57ca.3860 msg=Certificate len=1146
seq=2 frag_off=519 frag_len=519
[11/14/13 14:50:27.670 UTC 65 8528] f84f.57ca.3860 Handshake in progress...
[11/14/13 14:50:27.670 UTC 66 8528] f84f.57ca.3860 record=Handshake epoch=0 seq=4
[11/14/13 14:50:27.670 UTC 67 8528] f84f.57ca.3860 msg=Certificate len=1146
seq=2 frag_off=1038 frag_len=108
[11/14/13 14:50:27.671 UTC 702f54 8528] acDtlsCallback: entering...
[11/14/13 14:50:27.671 UTC 702f55 8528] acDtlsCallback: cb->code 3
[11/14/13 14:50:27.672 UTC 68 8528] Verify X.509 certificate from wtp
7c69.f604.9460
[11/14/13 14:50:27.673 UTC 702f56 8528] acDtlsCallback Cert validation PENDING
[11/14/13 14:50:27.673 UTC 69 8528] f84f.57ca.3860 Certificate verification -
pending...
[11/14/13 14:50:27.673 UTC 6a 8528] f84f.57ca.3860 Handshake in process..
awaiting certificate verification result..
[11/14/13 14:50:27.673 UTC 6b 8528] f84f.57ca.3860 record=Handshake epoch=0 seq=5
[11/14/13 14:50:27.673 UTC 6c 8528] f84f.57ca.3860 msg=ClientKeyExchange
len=130 seq=3 frag_off=0 frag_len=130
[11/14/13 14:50:27.673 UTC 702f57 8528] acDtlsCallback: entering...
[11/14/13 14:50:27.673 UTC 702f58 8528] acDtlsCallback: cb->code 3
[11/14/13 14:50:27.674 UTC 6d 8528] Verify X.509 certificate from wtp
7c69.f604.9460
[11/14/13 14:50:27.675 UTC 702f59 8528] acDtlsCallback Cert validation PENDING
[11/14/13 14:50:27.675 UTC 6e 8528] f84f.57ca.3860 Certificate verification -
pending...
[11/14/13 14:50:27.675 UTC 6f 8528] f84f.57ca.3860 Handshake in process..
awaiting certificate verification result..
[11/14/13 14:50:27.675 UTC 70 8528] f84f.57ca.3860 record=Handshake epoch=0 seq=6
[11/14/13 14:50:27.675 UTC 71 8528] f84f.57ca.3860 msg=CertificateVerify
len=258 seq=4 frag_off=0 frag_len=258
[11/14/13 14:50:27.675 UTC 702f5a 8528] acDtlsCallback: entering...
[11/14/13 14:50:27.675 UTC 702f5b 8528] acDtlsCallback: cb->code 3
[11/14/13 14:50:27.676 UTC 72 8528] Verify X.509 certificate from wtp 7c69.f604.9460
[11/14/13 14:50:27.676 UTC 702f5c 8528] acDtlsCallback Cert validation PENDING
[11/14/13 14:50:27.676 UTC 73 8528] f84f.57ca.3860 Certificate verification -
pending...
[11/14/13 14:50:27.676 UTC 74 8528] f84f.57ca.3860 Handshake in process..
awaiting certificate verification result..
[11/14/13 14:50:27.677 UTC 75 8528] f84f.57ca.3860 record=ChangeCipherSpec
```

```

epoch=0 seq=7
[11/14/13 14:50:27.677 UTC 702f5d 8528] acDtlsCallback: entering...
[11/14/13 14:50:27.677 UTC 702f5e 8528] acDtlsCallback: cb->code 3
[11/14/13 14:50:27.677 UTC 76 8528] Verify X.509 certificate from wtp 7c69.f604.9460
[11/14/13 14:50:27.678 UTC 702f5f 8528] acDtlsCallback Cert validation PENDING
[11/14/13 14:50:27.678 UTC 77 8528] f84f.57ca.3860 Certificate verification -
pending...
[11/14/13 14:50:27.678 UTC 78 8528] f84f.57ca.3860 Handshake in process..
awaiting certificate verification result..
[11/14/13 14:50:27.678 UTC 79 8528] f84f.57ca.3860 record=Handshake epoch=1 seq=0
[11/14/13 14:50:27.678 UTC 7a 8528] f84f.57ca.3860 msg=Unknown or Encrypted
[11/14/13 14:50:27.679 UTC 702f60 8528] acDtlsCallback: entering...
[11/14/13 14:50:27.679 UTC 702f61 8528] acDtlsCallback: cb->code 3
[11/14/13 14:50:27.679 UTC 7b 8528] Verify X.509 certificate from wtp 7c69.f604.9460
[11/14/13 14:50:27.680 UTC 702f62 8528] acDtlsCallback Cert validation PENDING
[11/14/13 14:50:27.680 UTC 7c 8528] f84f.57ca.3860 Certificate verification -
pending...
[11/14/13 14:50:27.680 UTC 7d 8528] f84f.57ca.3860 Handshake in process..
awaiting certificate verification result..
[11/14/13 14:50:27.681 UTC 7e 8528] Tickling the connection: 10.201.234.4:5246
<-> 10.201.234.24:18759.
[11/14/13 14:50:27.681 UTC 702f63 8528] acDtlsCallback: entering...
[11/14/13 14:50:27.681 UTC 702f64 8528] acDtlsCallback: cb->code 3
[11/14/13 14:50:27.682 UTC 7f 8528] Verify X.509 certificate from wtp
7c69.f604.9460 >> AP Ethernet mac
[11/14/13 14:50:27.683 UTC 702f65 8528] acDtlsCallback Cert validation SUCCESS.
[11/14/13 14:50:27.683 UTC 80 8528] f84f.57ca.3860 Certificate verification -
passed!
[11/14/13 14:50:27.706 UTC 81 8528] f84f.57ca.3860 Connection established!
[11/14/13 14:50:27.706 UTC 702f66 8528] acDtlsCallback: entering...
[11/14/13 14:50:27.706 UTC 702f67 8528] acDtlsCallback: cb->code 0
[11/14/13 14:50:27.706 UTC 82 8528] f84f.57ca.3860 DTLS Connection 0x5789a5e0
established on local port 5246
[11/14/13 14:50:27.706 UTC 83 8528] f84f.57ca.3860 Setting DTLS MTU for link to
peer 10.201.234.24:18759
[11/14/13 14:50:27.706 UTC 84 8528] Load Balancer: Platform Not supported,
Exiting from ctrl_tunnel_lb
[11/14/13 14:50:27.706 UTC 85 8528] Capwap Control DTLS key plumbing: Get SA
resources from LB for AP IP 10.201.234.24, rc = 4
[11/14/13 14:50:27.706 UTC 86 8528] Plumbing DTLS keys for local 10.201.234.4:5246
and peer 10.201.234.24:18759, anc_sw_id 0, anc_asic_id 0, res_sw_id 0, res_asic_id 0
[11/14/13 14:50:27.706 UTC 87 8528] Created CAPWAP control DTLS engine session
10.201.234.4:5246 <-> 10.201.234.24:18759.

```

```
[11/14/13 14:50:27.706 UTC 88 8528] f84f.57ca.3860 Sending Finished using epoch 1
[11/14/13 14:50:27.706 UTC 702f68 8528] DTLS Session established server
(10.201.234.4:5246), client (10.201.234.24:18759)
[11/14/13 14:50:27.706 UTC 702f69 8528] Starting wait join timer for AP:
10.201.234.24:18759
[11/14/13 14:50:27.707 UTC 30e2 267] %DTLS: entering dtls_add_dtls_session_db_entry
[11/14/13 14:50:27.707 UTC 30e3 267] %DTLS: sip = 0xac9ea04 dip = 0xac9ea18
sport =5246 dport=18759
[11/14/13 14:50:27.707 UTC 30e4 267] %DTLS: dtls_add_dtls_session_db_entry:
anchor_port iifd : 1088ec00000003b : capwap_iifd : 0 : session type : 0 :
sw_num : 0 : asic : 0
[11/14/13 14:50:27.707 UTC 30e5 267] %DTLS: bk_sw_num : 0 bk_asic : 0
[11/14/13 14:50:27.710 UTC 89 8528] Received DTLS engine action feedback for
CAPWAP connection
[11/14/13 14:50:27.711 UTC 8a 8528] DTLS Engine Add Success received for
connection 10.201.234.4:5246 / 10.201.234.24:18759
[11/14/13 14:50:27.711 UTC 8b 8528] Key plumb succeeded
[11/14/13 14:50:27.711 UTC 8c 8528] Decrement concurrent handshaking count 0
[11/14/13 14:50:27.711 UTC 8d 8528] Updating state for wtp f84f.57ca.3860 ip
10.201.234.24
[11/14/13 14:50:27.711 UTC 8e 8528] CAPWAP WTP entry not yet created.
[11/14/13 14:50:27.712 UTC 702f6a 8528] Unable to find the First RCB index.
Return Value: 2
```



Note The above output is from the AP point of view, therefore only messages sent by AP are seen.

Join Request-Response

```
[11/14/13 14:50:27.712 UTC 702f6b 8528] f84f.57ca.3860 Join Request from
10.201.234.24:18759
[11/14/13 14:50:27.712 UTC 702f6c 8528] f84f.57ca.3860 For phy port iif id
0x01088ec00000003b, control session - anc sw id 0, anc asic id 0, res sw id 0,
res asic id 0 in RCB for AP 10.201.234.24
[11/14/13 14:50:27.712 UTC 8f 8528] Creating WTP 0x3823a0f0 for AP f84f.57ca.3860
with hardware encryption flag = TRUE
[11/14/13 14:50:27.712 UTC 702f6d 8528] f84f.57ca.3860 Deleting AP entry
10.201.234.24:18759 from temporary database.
[11/14/13 14:50:27.712 UTC 702f6e 8528] CAPWAP Interface-Name CAPWAP WCM Client
f84f57ca3860 used for IIF ID allocation
[11/14/13 14:50:27.712 UTC 702f6f 8528] CAPWAP IIF ID Allocation Successful!
ID:0x00d2a98000000796 for AP 10.201.234.24, AP hash 1 [This indicates generation
of a capwapx interface seen in show ip interface brief]
[11/14/13 14:50:27.712 UTC 702f70 8528] Adding Node to AVL Tree with IIF
Id:0xd2a98000000796
[11/14/13 14:50:27.712 UTC 702f71 8528] WTP IIF ID Type: 0
[11/14/13 14:50:27.712 UTC 702f72 8528] Timer created successfully for WTP
IIF ID: 0xd2a98000000796
```

```

[11/14/13 14:50:27.712 UTC 702f73 8528] Added IIF ID to AVL Tree Database
Oxd2a98000000796

[11/14/13 14:50:27.712 UTC 702f74 8528] f84f.57ca.3860 Join Version: =
167863296

[11/14/13 14:50:27.712 UTC 702f75 8528] Encode static AP manager 10.201.234.4,
AP count 0

[11/14/13 14:50:27.712 UTC 702f76 8528] f84f.57ca.3860 Join resp: CAPWAP Maximum
Msg element len = 87

[11/14/13 14:50:27.712 UTC 702f77 8528] f84f.57ca.3860 Join Response sent to
10.201.234.24:18759

[11/14/13 14:50:27.712 UTC 702f78 8528] f84f.57ca.3860 CAPWAP State: Join

[11/14/13 14:50:27.712 UTC 702f79 8528] f84f.57ca.3860 capwap_ac_platform.c:767 -
Operation State 0 ==> 4

[11/14/13 14:50:27.713 UTC 702f7a 8528] f84f.57ca.3860 Register LWAPP event for AP
f84f.57ca.3860 slot 0

[11/14/13 14:50:27.713 UTC 702f7b 8528] capwap_iif_client_action_func: myid = 1,
myid_len=1

[11/14/13 14:50:27.713 UTC 702f7c 8528] CAPWAP Interface ID Acked
Id=0x00d2a98000000796 by IIF - IIF status = 0x1001, for AP 10.201.234.24,
rcb->ap_registered = 1

[11/14/13 14:50:27.713 UTC 702f7d 8528] f84f.57ca.3860 Not ready to send
Config Status Response to AP 10.201.234.24 as SPI ACK is not received

[11/14/13 14:50:27.713 UTC 702f7e 8528] Unable to find entry for PhyIifId:
0x1088ec00000003b from AVL Tree

[11/14/13 14:50:27.713 UTC 702f7f 8528] Adding Node to Physical Iif Id AVL Tree
with PhyIifId:0x1088ec00000003b

[11/14/13 14:50:27.713 UTC 702f80 8528] Unable to find entry for PhyIifId:
0x1088ec00000003b from AVL Tree

[11/14/13 14:50:27.713 UTC 702f81 8528] f84f.57ca.3860 Register LWAPP event for
AP f84f.57ca.3860 slot 1

[11/14/13 14:50:27.713 UTC 702f82 8528] Added PhyIifId: 0x1088ec00000003b to AVL
Tree Database

[11/14/13 14:50:27.714 UTC 702f83 8528] Get the Interface name from the
Phy-Port-IIF-ID:0x1088ec00000003b

[11/14/13 14:50:27.714 UTC 702f84 8528]

---Phy-IIF-ID = 0x1088ec00000003b-----

[11/14/13 14:50:27.714 UTC 702f85 8528] f84f.57ca.3860 Not ready to send Config
Status Response to AP 10.201.234.24 as SPI ACK is not received

[11/14/13 14:50:27.714 UTC 702f86 8528] CSM-SPAM:Input monitor name after copying
from vapcb to vap data is wireless-avc-basic

[11/14/13 14:50:27.714 UTC 702f87 8528] CSM-SPAM:Output monitor name after copying
from vapcb to vapdata is wireless-avc-basic

[11/14/13 14:50:27.714 UTC 702f88 8528] CSM-SPAM:Input monitor name after copying
from vapcb to vap data is wireless-avc-basic

[11/14/13 14:50:27.714 UTC 702f89 8528] CSM-SPAM:Output monitor name after copying
from vapcb to vapdata is wireless-avc-basic

[11/14/13 14:50:27.714 UTC 702f8a 8528] RSN Capabilities: (26)

```

```
[11/14/13 14:50:27.714 UTC 702f8b 8528] [0000] 30 18 01 00 00 0f ac 02 02
00 00 0f ac 02 00 0f

[11/14/13 14:50:27.714 UTC 702f8c 8528] [0016] ac 04 01 00 00 0f ac 02 28 00

[11/14/13 14:50:27.714 UTC 702f8d 8528] WARP IEs: (12)

[11/14/13 14:50:27.714 UTC 702f8e 8528] [0000] dd 0a 00 c0 b9 01 00 00
00 08 01 01

[11/14/13 14:50:27.714 UTC 702f8f 8528] f84f.57ca.3860 Not ready to send Config
Status Response to AP 10.201.234.24 as SPI ACK is not received

[11/14/13 14:50:27.715 UTC 702f90 8528] Physical interface Info: IIF-ID =
0x1088ec00000003b, Message Code = 0x802, Interface Name ->gigabitethernet1/0/24,
Interface Type = 0x92, Client N<truncated>

[11/14/13 14:50:27.715 UTC 702f91 8528] Updated AVL entry for phyIifid:
0x1088ec00000003b macAddr:f84f.57ca.3860, phyIfName: gigabitethernet1/0/24 Number
of APs on this Phy <truncated>

[11/14/13 14:50:27.725 UTC 702f92 8528] capwap opaque data f84f.57ca.3860
length = 0

[11/14/13 14:50:27.725 UTC 702f93 8528] No update; will insert f84f.57ca.3860
```

Configuration Status Request-Response/Update Request-Response

```
[11/14/13 14:50:27.869 UTC 702f94 8528] f84f.57ca.3860 Configuration Status
from 10.201.234.24:18759

[11/14/13 14:50:27.870 UTC 702f95 8528] f84f.57ca.3860 CAPWAP State: Configure

[11/14/13 14:50:27.870 UTC 702f96 8528] f84f.57ca.3860 New unsupported Payload
254 in message from AP f84f.57ca.3860, Return SUCCESS

[11/14/13 14:50:27.870 UTC 702f97 8528] f84f.57ca.3860 Decoding new unsupported
Payload 254 in message from AP f84f.57ca.3860, Return SUCCESS

[11/14/13 14:50:27.870 UTC 702f98 8528] Invalid channel 11 spacificied for the AP
AP2602I-1, slotId = 0

[11/14/13 14:50:27.870 UTC 702f99 8528] Invalid channel 56 spacificied for the AP
AP2602I-1, slotId = 1

[11/14/13 14:50:27.870 UTC 702f9a 8528] f84f.57ca.3860 Updating IP info for AP
f84f.57ca.3860 -- static 0, 10.201.234.24/255.255.255.224, gw 10.201.234.2

[11/14/13 14:50:27.870 UTC 702f9b 8528] f84f.57ca.3860 Updating IP
10.201.234.24 ==> 10.201.234.24 for AP f84f.57ca.3860

|

[11/14/13 14:50:27.870 UTC 702fab 8528] f84f.57ca.3860 LWAPP message validation
failed for SPAM Vendor Specific Payload(104) in message of len=7 from AP
f84f.57ca.3860

[11/14/13 14:50:27.870 UTC 702fac 8528] f84f.57ca.3860 Failed to validate vendor
specific message element

[11/14/13 14:50:27.871 UTC 702fad 8528] f84f.57ca.3860 Setting MTU to 1485

[11/14/13 14:50:27.871 UTC 702fae 8528] f84f.57ca.3860 Platform not Supported,
exiting Load Balancer function

[11/14/13 14:50:27.871 UTC 702faf 8528] load balancer rc=4 for AP 10.201.234.24,
IIF ID:0x00d2a98000000796

[11/14/13 14:50:27.871 UTC 702fb0 8528] opaque data size 0 with capwap interface
create f84f.57ca.3860

[11/14/13 14:50:27.871 UTC 702fb1 8528] spiCapwapParams->
```

```

data_tunnel.opaque_data.opaque_data_len: 0

[11/14/13 14:50:27.871 UTC 702fb2 8528] f84f.57ca.3860 Data Tunnel Create timer
started for 240 seconds timeout

[11/14/13 14:50:27.871 UTC 702fb3 8528] f84f.57ca.3860 Data Tunnel created -
tunnel type NON_CRYPTO, load balancer support Not supported, tunnel mtu 1449,

    anc_sw_id 0, anc_asic_id 0, res_sw_id 0, res_asic_id 0

    anc_wp_iif_id 0x0000000000000000, res_wp_iif_id 0x0000000000000000

[11/14/13 14:50:27.871 UTC 702fb4 8528] f84f.57ca.3860 Not ready to send Config
Status Response to AP 10.201.234.24 as SPI ACK is not received

[11/14/13 14:50:27.871 UTC 702fb5 8528] f84f.57ca.3860 AP f84f.57ca.3860
associated. Last AP failure was due to Configuration changes,reason:
controller reboot command

[11/14/13 14:50:27.871 UTC 30e6 260] [CAPWAP]: CAPWAP data tunnel create message.
[11/14/13 14:50:27.871 UTC 30e7 260] [CAPWAP]: capwap_data_tunnel_create called
[11/14/13 14:50:27.871 UTC 30e8 260] [CAPWAP]: Data tunnel id = 0xd2a98000000796
[11/14/13 14:50:27.871 UTC 30e9 260] [CAPWAP]: Tunnel Entry not found for AP
(10.201.234.24, 18759)

[11/14/13 14:50:27.873 UTC 30ea 260] [CAPWAP]: CAPWAP IDB init complete

[11/14/13 14:50:27.882 UTC 30eb 260] [CAPWAP]: capwap_interface_status_update:
tunnel 0xd2a98000000796 status 0

[11/14/13 14:50:27.882 UTC 30ec 260] [CAPWAP]: csb pd flag 0 opaque_data_len 0
attr opaque_data 0x00000000

[11/14/13 14:50:27.882 UTC 30ed 260] [CAPWAP]: Send capwap_data_tunnel_status_update
0 Slot-Unit 1 Unit 1 for iif_id 0xd2a98000000796 to WCM.

[11/14/13 14:50:27.882 UTC 30ee 260] [CAPWAP]: (capwap_process_fed_results) CAPWAP
FED result (0) for IIF ID: 0xd2a98000000796

[11/14/13 14:50:27.882 UTC 702fb6 8528

Received CAPWAP Tunnel SPI update opaque size 0

[11/14/13 14:50:27.882 UTC 702fb7 8528] opaque data len 0 with capwap server update

[11/14/13 14:50:27.883 UTC 702fb8 8528] f84f.57ca.3860 SPI ACK : Capwap Data
Tunnel create successful for iifid:0x00d2a98000000796 AP:10.201.234.24

[11/14/13 14:50:27.883 UTC 702fb9 8528]

Received CAPWAP interface update opaque len 0

[11/14/13 14:50:27.883 UTC 702fba 8528] SPI IifId ACK: Capwap Data Tunnel Created
Successfully for IifId: 0x00d2a98000000796 AP: 10.201.234.24

[11/14/13 14:50:27.883 UTC 702fbb 8528] f84f.57ca.3860 OK to send Config Status
Response to AP 10.201.234.24

[11/14/13 14:50:27.888 UTC 30ef 260] [CAPWAP]: Notify PM (done).

[11/14/13 14:50:27.888 UTC 30f0 260] [CAPWAP]: SNMP Register: Cal HWIDB 32f44570

[11/14/13 14:50:27.888 UTC 30f1 260] [CAPWAP]: capwap_port_hashitem added: slot 1
slotunit 24 vlan 1104

[11/14/13 14:50:27.888 UTC 30f2 260] [CAPWAP]: 7c69.f604.9460 is AP's mac addr

[11/14/13 14:50:27.932 UTC 702fbc 8528] Sending multicast payload to ap AP2602I-1,
mcast_mode 0, mcast group 0.0.0.0

```



```
[11/14/13 14:50:27.933 UTC 702fbd 8528] f84f.57ca.3860 Config status response sent
to 10.201.234.24:18759

[11/14/13 14:50:27.933 UTC 702fbe 8528] f84f.57ca.3860 Configuration Status
Response sent to 10:201:234:24

[11/14/13 14:50:27.933 UTC 702fbf 8528] f84f.57ca.3860 Configuration update
request for Band Select Cfg sent to 10.201.234.24:18759

[11/14/13 14:50:27.933 UTC 702fc0 8528] f84f.57ca.3860 Configuration update
request for HaConfig message sent to 10.201.234.24:18759

[11/14/13 14:50:27.934 UTC 702fc1 8528] f84f.57ca.3860 Configuration update
request for AP NGWC Qos sent to 10.201.234.24:18759

[11/14/13 14:50:28.121 UTC 702fc2 8528] f84f.57ca.3860 Change State Event
Request from 10.201.234.24:18759

[11/14/13 14:50:28.122 UTC 702fc3 8528] f84f.57ca.3860 Received LWAPP Up event
for AP f84f.57ca.3860 slot 0!

[11/14/13 14:50:28.122 UTC 702fc4 8528] f84f.57ca.3860 Radio state change for
slot: 0 state: 2 cause: 0 detail cause: 0

[11/14/13 14:50:28.122 UTC 702fc5 8528] f84f.57ca.3860 Change State Event
Response sent to 10.201.234.24:18759

[11/14/13 14:50:28.122 UTC 702fc6 8528] f84f.57ca.3860 CAPWAP State: Run

[11/14/13 14:50:28.122 UTC 702fc7 8528] f84f.57ca.3860 Sending the remaining
config to AP 10.201.234.24:18759

[11/14/13 14:50:28.122 UTC 702fc8 8528] f84f.57ca.3860 AP Going to RUN
10.201.234.24: ConcurrentJoins: 0

[11/14/13 14:50:28.122 UTC 702fc9 8528] f84f.57ca.3860 Configuration update
request for Init VAP-DATA for slot 1 sent to 10.201.234.24:18759

[11/14/13 14:50:28.122 UTC 702fca 8528] f84f.57ca.3860 Configuration update
request for configuring association limit params sent to 10.201.234.24:18759

[11/14/13 14:50:28.122 UTC 702fcb 8528] f84f.57ca.3860 Configuration update
request for Band Select Cfg sent to 10.201.234.24:18759

[11/14/13 14:50:28.122 UTC 702fcc 8528] f84f.57ca.3860 Configuration update
request for HaConfig message sent to 10.201.234.24:18759

[11/14/13 14:50:28.123 UTC 702fcd 8528] CAPWAP: No update, will insert
f84f.57ca.3860

[11/14/13 14:50:28.123 UTC 702fce 8528] capwap opaque data f84f.57ca.3860
length = 0

[11/14/13 14:50:28.124 UTC 702fcf 8528] CAPWAP HA insert f84f.57ca.3860

[11/14/13 14:50:28.124 UTC 702fd0 8528] CAPWAP HA insert f84f.57ca.3860

[11/14/13 14:50:28.124 UTC 702fd1 8528] f84f.57ca.3860 Configuration update
request for PHY payload sent to 10:201:234:24

[11/14/13 14:50:28.126 UTC 702fd2 8528] f84f.57ca.3860 Configuration Update
Response from 10.201.234.24:18759

[11/14/13 14:50:28.126 UTC 702fd3 8528] f84f.57ca.3860 Configuration update
request for RrmInterferenceCtrl payload sent to 10:201:234:24

[11/14/13 14:50:28.126 UTC 702fd4 8528] f84f.57ca.3860 Configuration update
request for RrmNeighbourCtrl payload sent to 10.201.234.24

[11/14/13 14:50:28.126 UTC 702fd5 8528] f84f.57ca.3860 Configuration update
request for RrmReceiveCtrl payload sent to 10:201:234:24

[11/14/13 14:50:28.126 UTC 702fd6 8528] f84f.57ca.3860 Configuration update
```

```

request for CcxRmMeas payload sent to 10.201.234.24

[11/14/13 14:50:28.132 UTC 702fd7 8528] f84f.57ca.3860 Change State Event
Request from 10.201.234.24:18759

[11/14/13 14:50:28.132 UTC 702fd8 8528] f84f.57ca.3860 Radio state change
for slot: 1 state: 2 cause: 0 detail cause: 0

[11/14/13 14:50:28.132 UTC 702fd9 8528] f84f.57ca.3860 Change State Event
Response sent to 10.201.234.24:18759

[11/14/13 14:50:28.132 UTC 702fda 8528] f84f.57ca.3860 CAPWAP State: Run

[11/14/13 14:50:28.132 UTC 702fdb 8528] f84f.57ca.3860 Sending the remaining
config to AP 10.201.234.24:18759

[11/14/13 14:50:28.133 UTC 702fdc 8528] f84f.57ca.3860 Configuration update
request for qos pm payload payload sent to 10.201.234.24:18759

[11/14/13 14:50:28.133 UTC 702fdd 8528] f84f.57ca.3860 Received LWAPP Up
event for AP f84f.57ca.3860 slot 1!

[11/14/13 14:50:28.133 UTC 702fde 8528] f84f.57ca.3860 Configuration update
request for PHY payload sent to 10:201:234:24

[11/14/13 14:50:28.133 UTC 702fdf 8528] f84f.57ca.3860 Configuration update
request for RrmInterferenceCtrl payload sent to 10:201:234:24

[11/14/13 14:50:28.133 UTC 702fe0 8528] f84f.57ca.3860 Configuration update
request for RrmNeighbourCtrl payload sent to 10.201.234.24

[11/14/13 14:50:28.134 UTC 702fe1 8528] f84f.57ca.3860 Configuration update
request for RrmReceiveCtrl payload sent to 10:201:234:24

[11/14/13 14:50:28.134 UTC 702fe2 8528] f84f.57ca.3860 Configuration update
request for CcxRmMeas payload sent to 10.201.234.24

[11/14/13 14:50:28.188 UTC 702fe3 8528] f84f.57ca.3860 Configuration Update
Response from 10.201.234.24:18759

[11/14/13 14:50:28.188 UTC 702fe4 8528] f84f.57ca.3860 Change State Event
Request from 10.201.234.24:18759

[11/14/13 14:50:28.188 UTC 702fe5 8528] f84f.57ca.3860 Change State Event
Response sent to 10.201.234.24:18759

[11/14/13 14:50:28.188 UTC 702fe6 8528] f84f.57ca.3860 CAPWAP State: Run

[11/14/13 14:50:28.188 UTC 702fe7 8528] f84f.57ca.3860 Sending the remaining
config to AP 10.201.234.24:18759

[11/14/13 14:50:28.194 UTC 702fe8 8528] f84f.57ca.3860 Configuration Update
Response from 10.201.234.24:18759

[11/14/13 14:50:28.194 UTC 702fe9 8528] f84f.57ca.3860 WTP Event Request
from 10.201.234.24:18759

[11/14/13 14:50:28.194 UTC 702fea 8528] f84f.57ca.3860 WTP Event Response
sent to 10.201.234.24:18759

```

Common Reasons for AP Join Failure

This section describes about common causes of AP join failures.

Problem 1: The AP on the Cisco Catalyst 3850 Series Switch is not in the wireless management VLAN

```
#show run interface GigabitEthernet 1/0/22
```

```
interface GigabitEthernet 1/0/22
description AP
```

```
switchport access vlan 25
switchport mode access
```

#show run | inc wireless

```
wireless mobility controller
wireless management interface Vlan1104
```

#show log

```
*%CAPWAP-3-DISC_WIRELESS_INTERFACE_ERR: 1 wcm: Unable to process discovery
request from AP 0019.0737.f630 , VLAN (25) scrIp (10.10.25.13) dstIp
(255.255.255.255), could not get wireless interface belonging to this network
```

The AP is in VLAN 25, and there is no wireless management interface configuration for VLAN 25.

Problem 2: The AP model is unsupported

Following portion of command shows test of AP1131.

#show log

```
*%CAPWAP-3-JOIN_UNSUPP_AP: 1 wcm: Received a join request from an unsupported AP
0019.0737.f630 AP8-1131AG-eb:66 (model AIR-AP1131AG-A-K9)
```

Problem 3: The AP count license is not enabled on the controller

#show license right-to-use summ

License Name	Type	Count	Period left
ipservices	permanent	N/A	Lifetime
apcount	base	0	Lifetime
apcount	adder	0	Lifetime

```
License Level In Use: ipservices
License Level on Reboot: ipservices
Evaluation AP-Count: Disabled
Total AP Count Licenses: 0
AP Count Licenses In-use: 0
AP Count Licenses Remaining: 0
```

#show log

```
*%LWAPP-3-AP_LICENSE_REQUEST_ERR: 1 wcm: License request failed for AP
0c:68:03:eb:9b:20 - Check for Controller Licenses
*%CAPWAP-3-AP_DB_ALLOC: 1 wcm: Unable to alloc AP entry in database for
10.201.234.xx:29817
```

Problem 4: The regulatory domain is mismatched

#show wireless country configured

```
Configured Country.....: BE - Belgium
```

Configured Country Codes

BE - Belgium : 802.11a Indoor,Outdoor/ 802.11b / 802.11g

#show log

```
*%LWAPP-3-RD_ERR8: 1 wcm: Country code (US ) not configured for AP 0c:68:03:eb:9b:20
*%LWAPP-3-RD_ERR4: 1 wcm: Invalid regulatory domain 802.11bg:-E
802.11a:-E for AP 0c:68:03:eb:9b:20
```

Problem 5: The wireless mobility controller is not defined

#show wireless mobility summary

```
Mobility Agent Summary:
Mobility Role                : Mobility Agent
Mobility Protocol Port       : 16666
Mobility Switch Peer Group Name :
Multicast IP Address         : 0.0.0.0
DTLS Mode                    : Enabled
Mobility Domain ID for 802.11r : 0xac34
Mobility Keepalive Interval  : 10
Mobility Keepalive Count     : 3
Mobility Control Message DSCP Value : 0
Switch Peer Group Members Configured : 0
```

Link Status is Control Link Status : Data Link Status

The status of Mobility Controller:

IP	Public IP	Link Status
0.0.0.0	0.0.0.0	- : -

#show log

```
*%LWAPP-3-AP_LICENSE_REQUEST_ERR: 1 wcm: License request failed for AP
0c:68:03:eb:9b:20 - AP License Request timedout, ensure MC link is up, Resetting AP
```

Problem 6: The AP has mesh code on it

The following message does not indicate any current issue but it is quite generic. Examine the AP console log for further diagnosis until additional logging is added.

```
*%CAPWAP-3-SPI_TUNNEL_CREATE_ACK_NOT_REC: 1 wcm: Dropping discovery request from AP
0c68.03eb.9b20 - SPI Tunnel Create Ack not received[...It occurred 3 times/sec!..]
```

Problem 7: The AP3700 is connected to a Cisco Catalyst 3850 Series Switch that runs 3.3.0SE

#show log

```
*%CAPWAP-3-DISC_UNSUPPORTED_AP: 1 wcm: Rejecting discovery request from unsupported AP
08cc.68b4.4780 [...It occurred 2 times/sec!..]
```

Problem 8: The controller time is outside the AP certificate validity interval

#show clock

```
*00:14:59.459 GMT0:0 Thu Jan 1 1970
```

#show log

```
*Jan 1 00:05:51.338: %PKI-3-CERTIFICATE_INVALID_NOT_YET_VALID: Certificate chain
validation has failed. The certificate (SN: 17978AAD00000036823E) is not yet valid
Validity period starts on 04:25:46 GMT0:0 Jun 8 2013
```

```
*Jan 1 00:05:51.344: *%DTLS-4-BAD_CERT: 1 wcm: Certificate verification failed.
Peer IP: 10.201.234.21
```

```
*Jan 1 00:05:51.344: *%DTLS-3-HANDSHAKE_FAILURE: 1 wcm: Failed to complete DTLS handshake
with peer 10.201.234.21 Reason: no certificate returned
```

Problem 9: The AP authorization list is enabled on the WLC; the AP is not in the authorization list

#show ap auth-list

```
Authorize MIC APs against AAA                : Enabled
Authorize LSC APs against Auth-List          : Disabled
```

APs Allowed to Join:

```
AP with Manufacturing Installed Certificate : Enabled
AP with Self-Signed Certificate            : Disabled
AP with Locally Significant Certificate     : Disabled
```

#show log

```
*%LWAPP-3-RADIUS_ERR: 1 wcm: Could not send join reply, AP authorization failed;
AP:0c:68:03:eb:9b:20
```

```
*%CAPWAP-3-DATA_TUNNEL_DELETE_ERR2: 1 wcm: Failed to delete CAPWAP data tunnel
with interface id: 0x0 from internal database. Reason: AVL database entry not found
```

Problem 10: The MIC AP Policy is disabled

#show ap auth-list

```
Authorize MIC APs against AAA                : Disabled
Authorize LSC APs against Auth-List          : Disabled
```

APs Allowed to Join:

```
AP with Manufacturing Installed Certificate : Disabled
AP with Self-Signed Certificate            : Disabled
AP with Locally Significant Certificate     : Disabled
```

#show log

```
*%LOG-3-Q_IND: 1 wcm: Validation of SPAM Vendor Specific Payload failed - AP
f8:4f:57:3b:8c:d0
```

```
*%CAPWAP-3-ALREADY_IN_JOIN: 1 wcm: Dropping join request from AP f84f.573b.8cd0 -
AP is already in joined state
```

```
*%CAPWAP-3-DATA_TUNNEL_DELETE_ERR2: 1 wcm: Failed to delete CAPWAP data tunnel
with interface id: 0x0 from internal database. Reason: AVL database entry not found
```

#show trace messages group-ap

```
|
MIC AP is not allowed to join by config
|
```

General Technical Tips on Trace Commands

This section provides some helpful tips on filtering options and limitations on trace commands.

- Before you begin with troubleshoot procedure, clear all previously collected traces for the specific feature. In this case, capwap, group-ap, and all filtered traces.
 - **# Set trace control capwap**
 - **# Set trace control group-ap**
 - **# Set trace control sys-filtered-trace** (this command clears the filtered traces and cannot be run on a per-feature basis)

- AP join on converged access controllers makes use of the radio MAC address of the AP. So, when you set a filter for the trace, make use of the radio or base MAC address of the AP.

Enter the **show ap join stats summary** command to find the radio MAC address of the AP.

- Issues with certificates are handled by IOSd and require the use of debugs, not traces. For further diagnosis use the following debugs:
 - **#debug crypto pki API**
 - **#debug crypto pki callbacks**
 - **#debug crypto pki server**
 - **#debug crypto pki transactions**
 - **#debug crypto pki messages**



Converged Access Controllers MAC Address Entry for Network Mobility Service Protocol

This document describes the procedure to add the Location Based Service - Self Signed Certificate (LBS-SSC) and the MAC address of the Mobility Services Engine (MSE) on Cisco Catalyst 3850 Series, and Cisco Catalyst 3650 Series Switches.

- [Prerequisites, page 51](#)
- [Adding the MAC Address and the SSC on Converged Access WLCs, page 51](#)

Prerequisites

The information in this document is based on the following:

- Cisco Catalyst 3850 Series Switches
- Cisco Catalyst 3650 Series Switches

Adding the MAC Address and the SSC on Converged Access WLCs

Perform the following tasks to add the MAC Address and the SSC on Converged Access WLCs:

- 1 To enter the CMD prompt on the MSE, use the **cmdshell** command in the MSE CLI. To obtain the SSC hash and the MAC address which needs to be added to the WLCs, use the **show server-auth-info** command

```
[root@device ~]# cmdshell
cmd> show server-auth-info

invoke command: com.aes.server.cli.CmdGetServerAuthInfo
AesLog queue high mark: 50000
AesLog queue low mark: 500

-----Server Auth Info-----
MAC Address: 5c:f3:fc:e8:06:943:04
```

```
Key Hash: 29FADAE1392AE51C90942E813139DF53D5EAE1EF  
Certificate Type: SSC>
```

- 2 Copy the MAC address and key hash. To apply the copied MAC address and key hash to Converged Access WLCs, use the following commands:

```
username 5cf3fce80694  
username 5cf3fce80694 aaa attribute list NMSP  
aaa attribute list NMSP  
attribute type password 29FADAE1392AE51C90942E813139DF53D5EAE1EF
```




Configuration Example: Converged Access Management through Prime Infrastructure with SNMP v2 and v3

The Converged Access Management through Prime Infrastructure with SNMP v2 and v3 document describes how to add Converged Access (Cisco Catalyst 3850 Series and Cisco Catalyst 3650 Series Switches) to Prime Infrastructure with Simple Network Management Protocol (SNMP) v2 and v3.



Note

For more information on the commands used in this section, refer to [Command Lookup Tool](#) (Registered customers only).

- [Prerequisites](#), page 53
- [Configuring Converged Access Management](#), page 54
- [Verifying Converged Access Management Configuration](#), page 61
- [Troubleshooting Converged Access Management Configuration Issues](#), page 62

Prerequisites

We recommend that you have knowledge on the following topics:

- Converged Access Cisco IOS Version 3.3.2 or later.
- Prime Infrastructure Version 2.0 or later.

Supported Platforms and Releases

- Cisco Catalyst 3850 Series Switch
- Cisco Catalyst 3650 Series Switch

**Note**

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuring Converged Access Management

Configuring SNMP v2 on a Switch using CLI

To configure SNMP v2, use the following commands:

```
Device# configure terminal
```

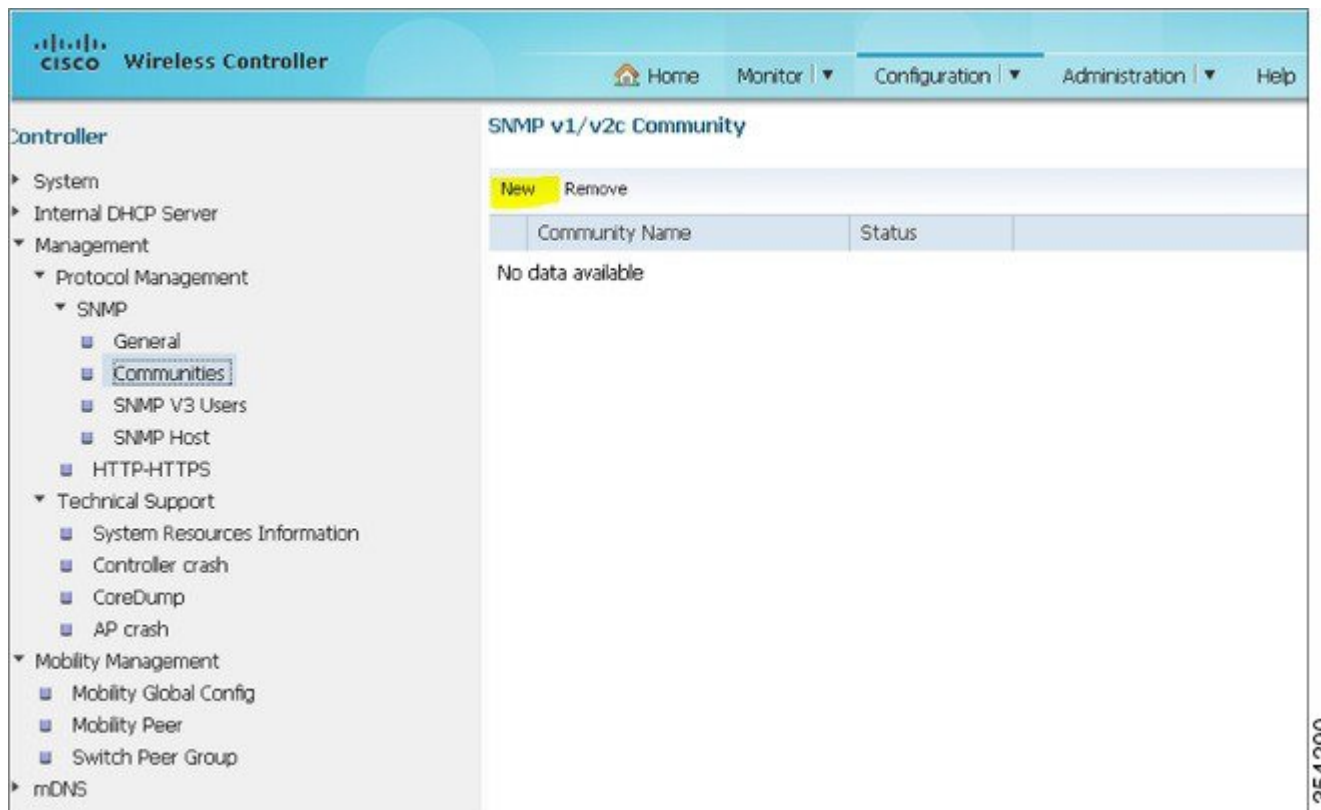
```
Device(config)# snmp-server community V2Community RW
```

Configuring SNMP v2 on a Switch using GUI

Perform the following steps to configure SNMP v2:

Step 1 From the GUI, navigate to **Configuration > Controller > Management > SNMP > Communities > New**

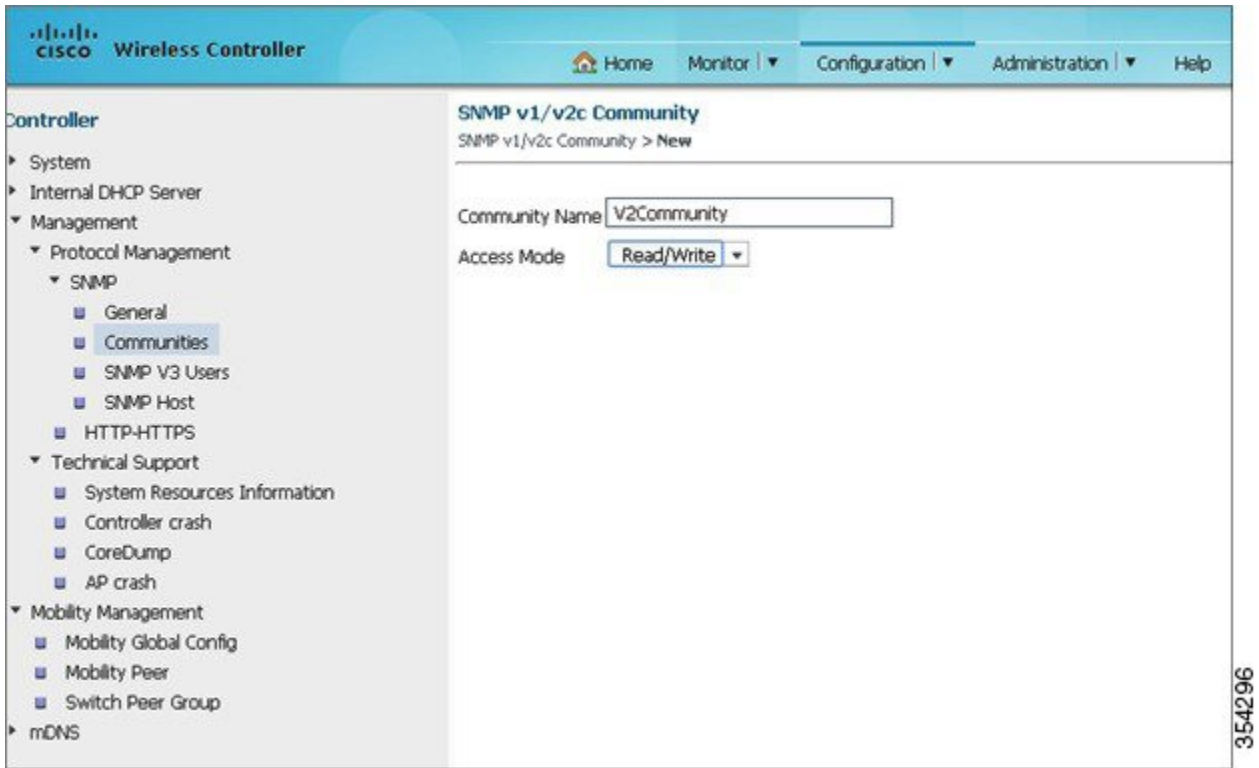
Figure 5: Configuring SNMP V2



354290

Step 2 Enter the details as shown in the following figure.

Figure 6: Configuring SNMP V2



Configuring SNMP v3 on a Switch using CLI

To configure SNMP v3, use the following commands:

```
Device# configure terminal
Device(config)# snmp-server group V3Group v3 auth read V3Read write V3Write
Device(config)# snmp-server user V3User V3Group v3 auth sha Password1 priv aes 128 Password1
Device(config)# snmp-server view V3Read iso included
Device(config)# snmp-server view V3Write iso included
Device(config)# snmp-server host 198.51.100.170 version 3 auth V3User
Device(config)# snmp-server enable traps
```

Configuring on Prime Infrastructure

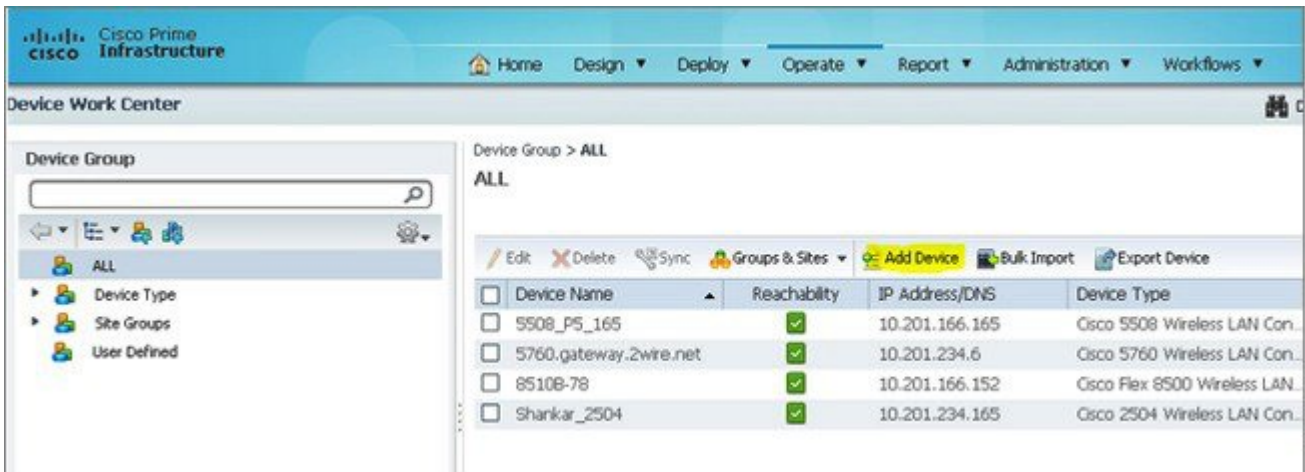
Perform the following tasks to configure SNMP v2 and SNMP v3 on Prime Infrastructure:



Note Use the Lifecycle view.

Step 1 Navigate to **Operate > Device Work Center > Add Device**.

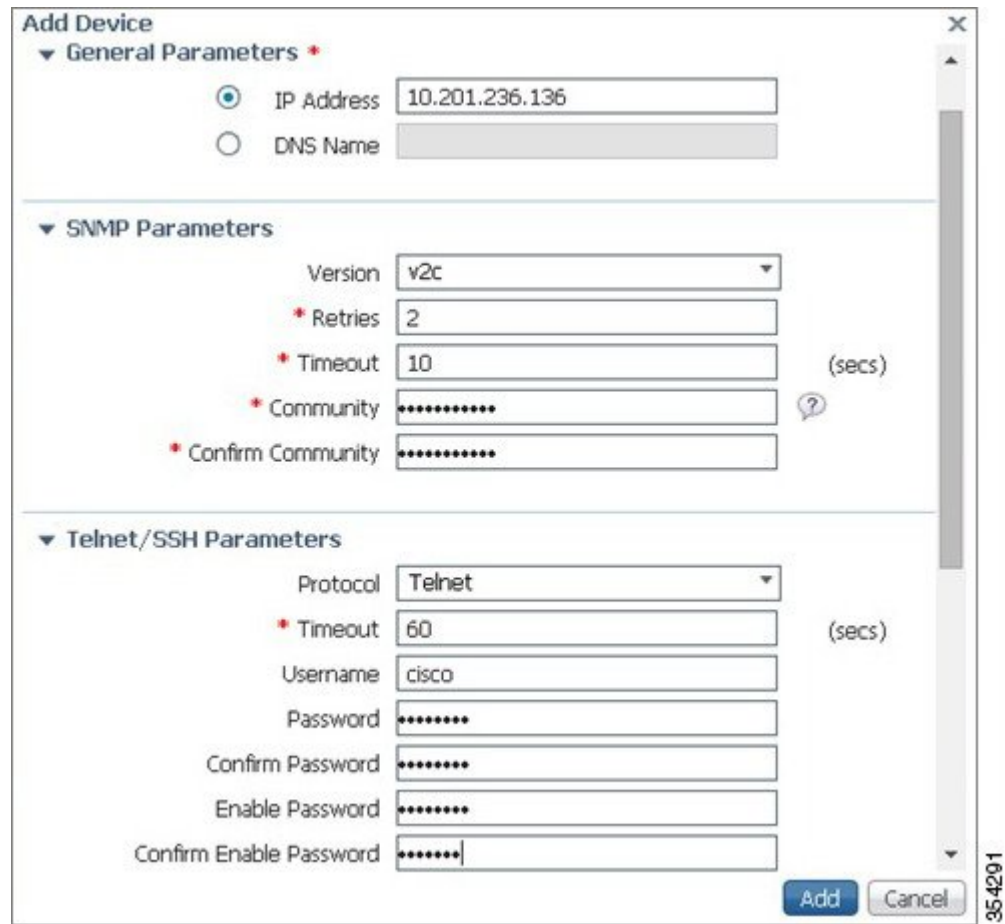
Figure 7: Add Device



354292

Step 2 Add the SNMP V2 configuration details as shown in the following figure:

Figure 8: SNMP V2 Configuration Details



The screenshot shows the 'Add Device' configuration window with the following settings:

- General Parameters:**
 - IP Address: 10.201.236.136
 - DNS Name: (empty)
- SNMP Parameters:**
 - Version: v2c
 - * Retries: 2
 - * Timeout: 10 (secs)
 - * Community: (masked)
 - * Confirm Community: (masked)
- Telnet/SSH Parameters:**
 - Protocol: Telnet
 - * Timeout: 60 (secs)
 - Username: cisco
 - Password: (masked)
 - Confirm Password: (masked)
 - Enable Password: (masked)
 - Confirm Enable Password: (masked)

Buttons: Add, Cancel

354201

Step 3 Enter the SNMP v3 details as shown in the following figure:

Figure 9: SNMP V3 Configuration Details

The screenshot shows the 'Add Device' configuration window with the following settings:

- General Parameters ***
 - IP Address: 10.201.236.136
 - DNS Name: (empty)
- SNMP Parameters**
 - Version: v3
 - * Retries: 2
 - * Timeout: 10 (secs)
 - Username: V3User
 - Auth. Type: HMAC-SHA
 - Auth. Password: (masked with dots)
 - Privacy Type: CFB-AES-128
 - Privacy Password: (masked with dots)
- Telnet/SSH Parameters**
 - Protocol: Telnet
 - * Timeout: 60 (secs)
 - Username: cisco
 - Password: (masked with dots)

Buttons: Add, Cancel. A vertical scrollbar on the right shows the value 354295.

Note If Telnet or Secure Shell parameters are not entered, Prime Infrastructure will not collect inventory from the switch.

Verifying Converged Access Management Configuration

Verifying SNMP v2 Configuration on a Switch

To verify SNMP v2 configuration on the switch, use the following commands:

```
Device# show snmp community

Community name: V2Community
Community Index: V2Community
Community SecurityName: V2Community
storage-type: nonvolatile active
```

Verifying SNMP v3 Configuration on a Switch

To verify SNMP v3 configuration on a switch, use the following commands:

```
Device# show snmp user

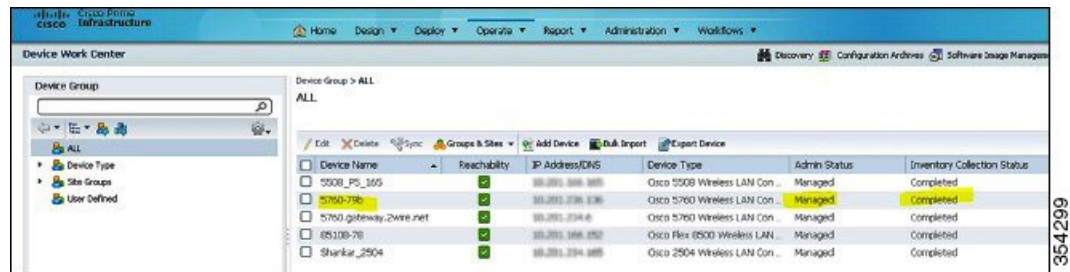
User name: V3User
Engine ID: 80000009030068BC0C5A8F80
storage-type: nonvolatile          active
Authentication Protocol: SHA
Privacy Protocol: AES128
Group-name: V3Group

Device# show snmp group
groupname: V3Group                security model:v3 auth
contextname: <no context specified> storage-type: nonvolatile
readview : V3Read                 writeview: V3Write
notifyview: <no notifyview specified>
row status: active
```

Verifying Configuration on Prime Infrastructure

The following figure verifies the configuration on Prime Infrastructure:

Figure 10: Verifying Prime Infrastructure Configuration



Device Name	Reachability	IP Address/DNS	Device Type	Admin Status	Inventory Collection Status
5508_IP_305	✓	10.255.1.100	Osco 5508 Wireless LAN Con ..	Managed	Completed
5760-750	✓	10.255.1.101	Osco 5760 Wireless LAN Con ..	Managed	Completed
5760.gateway_2Wire.net	✓	10.255.1.102	Osco 5760 Wireless LAN Con ..	Managed	Completed
85108-78	✓	10.255.1.103	Osco Flex (8500) Wireless LAN ..	Managed	Completed
Shankar_2504	✓	10.255.1.104	Osco 2504 Wireless LAN Con ..	Managed	Completed

Troubleshooting Converged Access Management Configuration Issues

There is currently no specific troubleshooting information available for this configuration.



Converged Access Path Maximum Transmission Unit Discovery

This document describes the Path Maximum Transmission Unit (MTU) Discovery algorithm for Wireless LAN Controller (WLC) (version 6.0 and above) and Converged Access.

- [Supported Platforms and Releases](#), page 63
- [Network Diagram](#), page 63
- [Setting Maximum Transmission Unit](#), page 63
- [Verifying Dynamic Path Maximum Transmission](#) , page 64
- [Troubleshooting Dynamic Path Maximum Transmission Unit](#), page 64

Supported Platforms and Releases

The information in this document is based on Cisco 5700 Series Wireless LAN Controller.

Network Diagram

Sender (Access Point) > (Multiprotocol Label Switching [MPLS] or Router) > Receiver (WLC or Converged Access)

Setting Maximum Transmission Unit

The sender detects the default MTU and sends a discovery request (Access Point [AP] to WLC). The request is for 1500 bytes with a Don't Fragment (DF) bit set. If the receiver receives the request, then it replies with a 1500 bytes packet. When the sender receives the reply from the receiver, the MTU path is set at 1500 MTU.

In cases, where the receiver does not receive the discovery request (or the sender does not receive the response from the receiver), the MTU is set to 576 and the dynamic discovery process starts.

Dynamic Path Maximum Transmission Unit Discovery

The sender or receiver if allowed, sets the MTU information available in the Internet Control Message Protocol (ICMP) as the next value for MTU.

If no information available, the sender or receiver receives an ICMP error. The initial MTU size is then set at 576 and dynamic discovery is in progress. Every 30 seconds, the sender attempts to increase the MTU to check for improvements in the path.

The sender can set the MTU values as 576, 1006, 1492, and 1500. Based on the router configuration, the customer can see the ICMP errors every 30 seconds for every AP.

ICMP Error over MPLS Example

The following example describes ICMP Error over MPLS:

```
MPLS: ICMP: dst (10.10.10.10) frag. needed and DF set unreachable sent to 192.0.2.5
```

Verifying Dynamic Path Maximum Transmission

To verify the Dynamic Path Maximum Transmission (PMTU), use the **show ap config general** command in EXEC mode.

```
Device(config)# show ap config general | b <APname>
.
CAPWAP Path MTU                               : 1500

Device> show ap config general <APname>
.
CAPWAP Path MTU..... 1500
```

Troubleshooting Dynamic Path Maximum Transmission Unit

To troubleshoot Dynamic PMTU issues, perform a packet capture on the AP switch port.



Third-Party Certificate Installation on Converged Access Wireless LAN Controllers

This document describes installing a certificate on Cisco Catalyst 3850 Series Switch. Also, it explains the process to install certificates on Converged Access and to use the certificate for authentication.



Note

- For more information on the commands used in this section, refer to [Command Lookup Tool](#) (for Registered Users only).
- To view an analysis of show command output, refer to the [Output Interpreter](#).
- After you receive a user certificate from a vendor, you receive the following entities in the Privacy Enhanced Mail (PEM) format:
 - User certificate
 - Rivest-Shamir-Adleman (RSA) key
 - Root certificate
- The installation process for the Cisco Catalyst 3850 Series Switch is different from the installation process for Cisco 5500 Series Wireless Controller.

- [Installing Third Party Certificates, page 65](#)

Installing Third Party Certificates

Perform the following steps to install a third-party certificate:

Step 1

To install the trustpoint, use the following commands:

```
configure terminal
crypto pki trustpoint trustp1 <--- trustp1 is a word string any word can be used here.
```

```
(ca-trustpoint)#enrollment terminal pem
(ca-trustpoint)#exit
```

Step 2 To authenticate the trustpoint, perform the following:

1 Enter the **crypto pki authenticate** command.

```
(config)#crypto pki authenticate trustp1
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
```

2 Copy and paste the user certificate. Ensure that the Begin Certificate and End Certificate lines are included.

3 Press **Enter** and then type *quit*.

```
Trustpoint 'trustp1' is a subordinate CA and holds a non self signed
cert
Trustpoint 'trustp1' is a subordinate CA.
but certificate is not a CA certificate.
Manual verification required
Certificate has the following attributes:
```

```
Fingerprint MD5: EF9EE16F 535D51D4 0E5E9809 F48CF6EE
Fingerprint SHA1: FB166D5D 5F301F93 3CA2015A F5745C52 46030D9E
```

```
% Do you accept this certificate? [yes/no]:
```

4 Type *Yes*, when prompted.

Note To view the certificate, enter **show crypto pki trustpoint** command.

Step 3 To import the root certificate, perform the following:

1 Enter the following **crypto pki import** command:

```
(config)#crypto pki import trustroot pem terminal passphrase
% Enter PEM-formatted CA certificate.
% End with a blank line or "quit" on a line by itself
```

2 Copy and paste the root certificate.

3 Press **Enter**, and type *quit*.

```
% Enter PEM-formatted encrypted private General Purpose key.
% End with "quit" on a line by itself
```

4 Copy and paste the RSA key, press **Enter**, and then type *quit*.

```
% Enter PEM-formatted General Purpose certificate.
% End with a blank line or "quit" on a line by itself
```

5 Copy and paste the user certificate and press **Enter**.

6 The certificate import is successfully completed.

The certificate can also be retrieved, converted to .p12 format, and imported with the **crypto pki import** command on the controller. To import the certificate, use the following command:

```
crypto pki import name pkcs12 tftp: // url password
```

Example for Installing Third Party Certificates

The following is an example to install a certificate:

```
(config)#crypto pki trustpoint verisign.com ?
<cr>

(config)#crypto pki trustpoint verisign.com
(ca-trustpoint)#enrollment terminal pem
(ca-trustpoint)#exit

(config)#crypto pki authenticate verisign.com <--- This is the USER CERTIFICATE
```

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE-----
```

```
MIIFCzCCBFugAwIBAgIQOrtXHG8Y534dY6EkS6gHiDANBgkqhkiG9w0BAQUFADCB
tTELMAkGA1UEBhMCVVMxZmFzAVBgNVBAoTD1ZlcmlTaWduLCBjb2R1bWVudDQwZDQw
ExZWZlbnBiUcnVzdCB0ZXR3b3JrMTswOQYDVQQLZSJuZmVudDQwZDQwZDQwZDQw
YXQGaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSAoY29tL3JwYSAoY29tL3Jw
VmVyaVNPZ24gQ2xhc3MgMyBTZWNLcmUgU2VydmlVYIENBIC0gRzZmMwHhcnMTIwNzIz
MDAwMDAwWhcnMTQwODE5MjM1OTU5WjCBpTELMAkGA1UEBhMCVVMxZmFzAVBgNVBAoT
CE1hcnlsYW5kMkRlEAYDVQQLFAlCYWw0aW1vcmluZS4uY29tL3JwYSAoY29tL3Jw
UHJpY2UgQXNjb2NpYXRlc3RjaGVjaGVjaGVjaGVjaGVjaGVjaGVjaGVjaGVjaGVja
bm9sb2dpZXMxZmFzAVBgNVBAMUG3dsZ3Vlc3RjaGVjaGVjaGVjaGVjaGVjaGVjaGVja
AS1wDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBBAJvJpXZRzliY8d11vCZcChi2c
5uIn0TnUhr8QQrW0kstroJtTmsJpaOVtWOb0HoLgC81H2VRAIxxvXdi49AqpYoY5
z8Uxeh29XqKiYR399K7/L9W9caYwWSjn4eLq1lk0GLmGMtE7T4T2bhssAgfV2+k
kpS4RymNUdSgCWzDrm575xyzVCCiOGUPjTxB5U7sWPASqpEvgoX88fPPpTtztJ1
XE1nleRlcbElz1/wpRxlFH4XMpTL79F8FQTWZ0MvMzyLEriR+dHXxtbBUkCPvgFY
7Nruz4Rj5Uk4S33G1EVVExfMF/wa+rtFU4RwLV4DEsbrhSFhLeEruFfpzOWHmJ0C
AwEAAoCAYSwggGHMCYGA1UdEQQfMB2CG3dsZ3Vlc3RjaGVjaGVjaGVjaGVjaGVjaGV
LmNvbTAJBGNVHRMEAJAAMA4GA1UdDwEB/wQEAwIFoDBFBGNVHR8EPjA8MDggOKA2
hjRodHRWoi8vU1ZSU2VjdXJ1LUCzLWNybc52ZXJpc2lmbi5jb20vU1ZSU2VjdXJ1
RzMuY3JsmEMGA1UdIAQ8MDowOAYKIYIZIAyb4RQEHNjAqMCGCCsGAQUFBwIBFhxo
dHRwczovL3d3dy52ZXJpc2lmbi5jb20vY3BzMB0GA1UdJQQQWMBQGCCsGAQUFBwMB
BggrBgEFBQcDAjAfbgNVHSMEGDAwQBQRNRFWU0TBgn4dIKs19AFj2L55pTB2Bggr
BgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGGGH0dHA6Ly9vY3NwLnZlcmlzaWduLmNv
bTBABBggrBgEFBQcAwOY0aHR0cDovL1NWU1NlY3VyZS1HMy1haWEudmVyaXNpZ24u
Y29tL1NWU1NlY3VyZUczLmNlcjANBgkqhkiG9w0BAQUFAAOCAQEARyq+92lCiDX
8hG4FyABsvcllDEhGUvY0URn8U7nYF7kN4NZdUKHFx86izPYjIC0yB6SsbMtZ68t
r8OwPFUOzRvPfhzivtn/mL1TcEPjWiItOKmM6vpYayDMv8bbgIf+LL981qS2XV5L
Sk3eylzVvVCqavw2BsvPacKlqvx7stSjQHTAoXeL9WBCfPLI5w/Fd6OP5J6XVBF
CHgAauqR5hONWge9M4xh6jDC0kLcrRcFXLbcDtS0DXHVbFBfDipoM2yRDdaVOWfZ
CrTL3cZA9HLzI3QtPkzLC7RrRP8r3bBkIYMNyGO465fe9IMV3MgTFey8G26mn+R5
iG3ddRLhhA==
```

```
-----END CERTIFICATE-----
```

```
Trustpoint 'verisign.com' is a subordinate CA and holds a non self signed cert
Trustpoint 'verisign.com' is a subordinate CA.
but certificate is not a CA certificate.
Manual verification required
Certificate has the following attributes:
```

```
Fingerprint MD5: EF9EE16F 535D51D4 0E5E9809 F48CF6EE
Fingerprint SHA1: FB166D5D 5F301F93 3CA2015A F5745C52 46030D9E
```

```
% Do you accept this certificate? [yes/no]:
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

```
(config)#s
% Incomplete command.

# show crypto pki trustpoints

Trustpoint verisign.com:
Subject Name:
```

Example for Installing Third Party Certificates

```

cn=ciscouser
ou=ciscotech
o=ciscoj
l=Bangalore
c=IN
Serial Number (hex): 411B571C6F18E77E1D63A1244BA80788
Certificate configured.

(config)# crypto pki import VeriG3 pem terminal password
% Enter PEM-formatted CA certificate.           <--- This is the ROOT CERTIFICATE
% End with a blank line or "quit" on a line by itself.

-----BEGIN CERTIFICATE-----
MIIF7DCCBNsgAwIBAgIQbsx6pacDIAm4zrz06VLuKtANBgkqhkiG9w0BAQUFADCB
yJELMAkGALUEBhMCVVMxZmVzAVBgnVBAoTDI1ZmlmLTAWduLjEjY3MjMjAwMjE3MjYy
EXZlbnB1bnB1bnB1bnB1bnB1bnB1bnB1bnB1bnB1bnB1bnB1bnB1bnB1bnB1bnB1bn
ZlbnB1bnB1bnB1bnB1bnB1bnB1bnB1bnB1bnB1bnB1bnB1bnB1bnB1bnB1bnB1bn
ZXJpU2lnbiBDbGFzcyAzIFB1YmxyYyBQcm1tYXJ5IEUENlcnRyZm1lYXRpb24gQXV0
aG9yaXR5IC0qRzUwHhcnMTAwMjE3MjYyZmVzAVBgnVBAoTDI1ZmlmLTAWduLjEjY3
MAkGALUEBhMCVVMxZmVzAVBgnVBAoTDI1ZmlmLTAWduLjEjY3MjMjAwMjE3MjYy
ZXJpU2lnbiB1bnB1bnB1bnB1bnB1bnB1bnB1bnB1bnB1bnB1bnB1bnB1bnB1bnB1bn
aHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSAoYykxMDEvMCOGA1UEAxMmVmVjYy
aVnpZ24gQ2xhc3MgMyBTZW51bnB1bnB1bnB1bnB1bnB1bnB1bnB1bnB1bnB1bnB1bn
DQEBAAQAA4IBDWAaggEKAoIBAQCxh4QfwgXF9byrJZenraI+nLr2wTm4i8rCrFbG
5bt1jKRPTc5v7QlK1K90EJxoiy6Ve4mbE8riNDBT81vzSxtig0iBdNGIEGwCU/m8
f0MmV1gzgzsChew0E6RJk2GfWQS3HRKNKedCuqWHQsV/KNLO85jIND4LQyUhhDK
tP9yus3nABINyYpUHjoRWPNGUFp9ZXse5jUxHGzUL4os4+guVoc9cosI6n9FAbo
GLSa6Dxugf3kzTU2s1HTAewSulZub5tXxYsU5w7Hn01KVGrJTcW/EbGuHGeBy0RV
M51/JJs/UoV/hhrzPPptf4H1uErT9YU3HLWm0AnkGHs4TvoPAGMBAAGjggHfMIIIB
2za0BggrBgEFBQcBAQQoMCIYwJAyIKwYBBQUHMAAGGGGh0dHA6Ly9vY3NwLnZlcm1z
aWduLmNvbTASBgNVHRMBAf8ECDAGAQH/AgEAMHAGALUdIARpMGcwZQYLYIZIAyB4
RQEHFMwVjAoBggrBgEFBQcCARYcaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nw
czAqBggrBgEFBQcCAjAeGhxodHRwczovL3d3dy52ZXJpc2lnbi5jb20vcnBhMDQg
A1UdHwQtMCswKaAnoCWI2h0dHA6Ly9jcmwudmVyaXNpZ24uY29tL3BjYTMtZzUu
Y3JsMA4GA1UdDwEB/wQEAWiBBjBTBGRggrBgEFBQcBDBARhMF+hXaBbMfkwVzBVfGlP
bWfNzS9naWYwITAFAmAGBSsOawIaBBSF5dMahqyNjmvDz4Bq1EgYLHSZLjAlFiNo
dHRwO18vbG9nby52ZXJpc2lnbi5jb20vdmNsb2dvdmlmZmZjAoBgNVHREITAFpB0W
GzEZMBcGA1UEAxMQVmVyaVnpZ25NUEtJLTItNjAdBgNVHQ4EFgQUQDURcFlnEWYj+
HScRjFQB91+eaUwHwYDVR0jBBGwFoAUF9Nlp8Ld7LvWManzQzn6Aq8zMTMwDQYJ
KozIHvNAQEFBQADggEBAAyDJO/dwzZWJz+NrbriobL0aP3nfPMU++CnqOh5pfB
WJ1lb0AdG0z60cEtBcDqbrIicFXZIDNAMwfcZYp6j0M3m+oOmmxw7vacgDvZn/R6
bezQGH1JSSqZxxkooR7YdyT3hSaGybYcFQEfn0Sc67dxIHSLNCwuLvPSxe/20majp
dirhGi2HbnTtIn0eIsbfFrYrghqK1FzyU0yvvz9iNw2tZdMGQVPtAhtTtVg0oazg
W+yzf5VK+wPIrSbb5mZ4EkrZn0L74ZjmQoObj49nJOhhGbxXdzULJgW0w27EyHW4
Rs/iGAZeqa6ogZpHft4MKGwLj7net4RYxh84HqTEy2Y=
-----END CERTIFICATE-----

% Enter PEM-formatted encrypted private General Purpose key.
% End with "quit" on a line by itself.

-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: DES-EDE3-CBC, 1E71580604A10032
xz3n4/odG8PFwe/FL6lhNmkXUgg09A82kupYuA1jWy4Pmz0gAk7fMTNBnrilk/Uq
c2Wrm34tdURukNfyv3IbvkGa6QsTQu5sYZ+83Igsdsh0xOw/xJNvs6aaOnF0frNN
wiRYOS5QGF9+A98kEw0g66ye04C9XjR39+peSgmAchI4smAF486bK2xDRz1p2Ewi
bL+pqS5y61/fYMDQwASRzJkkCi4sG4kQo5c5j3HpAwz3nVoQcj/R3AU7zcywMuVz0
qYiU4dcCq0Za6HXQS8vJ0yct10FjoXADzmgYtj7LbX1c+mJhTPDaPyKC56X3LOBg
KAQ0xwIC/ucyBoR02NhlSDoXGvX76W0J6J/jdaam/vcWdO212SEq68FkRNsr8y/
DS7/aU4rhw3pI994essfAgkeloqSx200zRb4Sxy5pfR/yVrlszwDmqQadFYogQxS
UR7KruVaXqZBFNhesUnxs5EmIMWsbTe+qbavSJYUYUqS0FTezNWSaLkTTSQaCE2
AkhSajND2HwzBrGvMBwObIFgk0000wcwras216uBp3mEGtjqdpmYhY7C5JXzkYUI
Ct8ZY+dJHMF0Uips/JvmglJ7Vr+ixCKa3ZmAf7J9sbJfChRkDvKXvzVZXkf3W12
AAGVNlbTf8xHyfSRA/b/BXJjuJAKSgzbDdHU19GJNh/CjRlGpJyvcRfVX+dirC50
r1EsIBP+supl1fQphVTEwHol1nYPg7sMLfV/vr8tHllzrJAxtde/LsXQDHd2XFwuo
VMexTY9t9EhtM4tHOOLEDOzv/nIUocDqKorAd8/arJ4iSQKttjnlIUFC1TS1Lqg
U2icCL4/9NL0Ulnuy2DxL1j7u6gNiXGLTuDWGaKR90UwEqLuw2he73pUS2eAIbW6
AP7YgRhoQMLa5M1JYHNz6uWdqtBLLbNL1TopVcK4EWemTSZtRD94ucNsBmH7GBJ
juUYPh8mFrvBRDOBe70vche0vzN3ouW3CvdtT6VAuVzns3LfPgxSbBUyoAV6SD7
7xHahcoCXAacgf2eXmTWNwocm2sf19Hv4tPrWzftYKd1tHcg+GxPqAOg5NsGw4D
H/61+6tO3lZt73/NI2tj+osdgqs+MarqWpOfjfwVlbW2/4cjin39qa4jB33QUebuJu
zXJdWwK9jfcMzJM7lQVcnGT8xqsC/+mcVY72rYf5QwQDagUcpOirHc+6/ULvYMy7
LWPjKLaOzDt1fqnIlkYg+cQkbPBbrbBARZ1XhqjKBmUm2oaCU5Bh6ppRIrBB/+I1

```



```

Dat43W3/MB0vu9LBC+oPB8MXVeumYU96Uky1l3hh7YX0iP7Wn9wuwr+jx/Nl1St0
dNST+pSRIPDgdph2ebRA7zNmruu9/U0+zQH+hJ8KdpGWVe3r4R6aR+FHRyT17rXz
Jbn1gT/yfIU4QnMTFislbnJNbJNzGRWKC55A7kDPshUJ/gB5OiytB4covXFtEel7g
odqkmlAc3Pgb6YQnVvHC4kCNtbgSvtPdidQRxMT2nVFrpn7qI5x9pFp+IW015gk
-----END RSA PRIVATE KEY-----
quit
% Enter PEM-formatted General Purpose certificate.
% End with a blank line or "quit" on a line by itself.

-----BEGIN CERTIFICATE-----
<--- This is the USER CERTIFICATE
MIIFCzCCBFugAwIBAgIQQRtXHG8Y534dY6EkS6gHiDANBgkqhkiG9w0BAQUFADCB
tTElMAkGAlUEBhMCMVVMxZzAVBgNVBAAoTD1Zlcm1TaWduLCBmMuMR8wHQYDVQQL
ExZWZlXJpU2lnb1BUCnVzdCBOZXR3b3JrMTswOQYDVQQLZzJuZXJtcyBvZiB1c2Ug
YXQgHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSAoYyYkxMDEvMCA1UEAxMm
VmVyaVNPZ24gQ2xhc3MgMyBTZW51cmUgU2VydmluYyIENBIC0gRzRmHhcnMTwNzIz
MDAwMDAwWhcnMTQwODE5MjM1OTU5WjCBPTelMAkGAlUEBhMCMVVMxETAPBgNVBAGT
CElhcmlsYw5kMRIwEAYDVQQHFA1CYWx0aW1vcmluZS41bG93bG93bG93bG93bG93
UHJpY2UgQXNzb2NpYXRlc3MgSW5jLjEgMB4GA1UECmQXSW5jZ293bG93bG93bG93
bm95b2dpZXNjb2NpYXRlc3MgSW5jLjEgMB4GA1UECmQXSW5jZ293bG93bG93bG93
AS1wDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBBAJvJpXRzliY8d11vCZcChi2c
5uIn0TnUhr8QQrw0kstroJtmsJpaOVtWob0HoLgC81H2VRAIxxvXdi49AqpYoY5
z8UxeH29XqKIYR399K7/L9W9caYwSjn4eLq1lk0GLmGmTE7T4T2bhssAgfV2+k
kpS4RymNudSgCWzDrm575xyzVCCiOGUPjTxpB5U7sWPASqpEvgoX88fPPpTtzTJl
XEInleRlcbE1z1/wpRxlFH4XMptL79F8FQTWZOMvMzyLErIR+dHXxtbBUKCPvgFY
7Nruz4Rj5Uk4S33G1EVVExFMF/wa+rtFU4Rwlv4DESbrhSFhLeEruFfpzOWhMj0C
AwEAAoCAYSwggGHCYGA1UEEQQfMB2CG3dsZ3Vlc3RjaGVjaGVjaGVjaGVjaGVjaGV
LmNvbTAJBgNVHRMEAjaAMA4GAlUdDwEB/wQEAWIFoDBFBGnVHR8EPJA8MDqgOKA2
hjRodHRwO18vU1ZSU2VjdXJlLWUzLWUzLWUzLWUzLWUzLWUzLWUzLWUzLWUzLWUz
RzMuY3JSMEMGAlUdIAQ8MDowOAYKIZIAYb4RQEHnJAqMcGCCsGAQUFBwIBFhxo
dHRwczovL3d3dy52ZzJpc2lnb15jb20vY3BzMB0GAlUdJQqWMBQGCCsGAQUFBwMB
BggrBgEFBQcDAjAfbG93bG93bG93bG93bG93bG93bG93bG93bG93bG93bG93bG93
BgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGGGH0dHA6Ly9vY3NwLnZlcm1zaWduLmNv
bTBABGgrBgEFBQcwoA0AHR0cDovL1NWU1N1Y3VzS1HMylhaWEudmVyaXNpZ24u
Y29tL1NWU1N1Y3VzUzUzUzUzUzUzUzUzUzUzUzUzUzUzUzUzUzUzUzUzUzUzUzUz
8hG4FyABsvcllDEhGUVy0URn8U7nYF7kN4NZdUKHFX86izPYJiC0yB6SsbMtZ68t
r8OwPFUozRvPfzhivtn/mL1TcepJWiItOKmM6vpYayDMv8bbgIf+LL981qS2XV5L
Sk3ey1zYVVVCqavw2BsvPAcklqv7stSjQhtAoXeL9WBCfPLI5w/Fd60P5J6XVBF
CHgAauqR5hONWge9M4xh6jDC0kLcrRcFXLbcdtS0DXHVbfbfDipoM2yRDdaVOwfZ
CrTL3cZA9HLzI3QtPzkzLC7RrRP8r3bBkLYMNYGO465fe9IMV3MgTFey8G26mn+R5
iG3ddRLhHA==
-----END CERTIFICATE-----

% PEM files import succeeded.
(config)#
#sh crypto pki trustpoints
Trustpoint TP-self-signed-0:

Trustpoint CISCO_IDEVID_SUDI:
  Subject Name:
  cn=Cisco Manufacturing CA
  o=Cisco Systems
  Serial Number (hex): 6A6967B3000000000003
  Certificate configured.

Trustpoint CISCO_IDEVID_SUDI0:
  Subject Name:
  cn=Cisco Root CA 2048
  o=Cisco Systems
  Serial Number (hex): 5FF87B282B54DC8D42A315B568C9ADFF
  Certificate configured.

Trustpoint HTTPS_SS_CERT_KEYPAIR:
  Subject Name:
  serialNumber=FOC1618V3T0+hostname=
  cn=
  Serial Number (hex): 01

Trustpoint verisign.com:
  Subject Name:
  cn=ciscouser
  ou=ciscotech
  o=ciscoj
  l=Bangalore

```

```
c=IN
  Serial Number (hex): 411B571C6F18E77E1D63A1244BA80788
Certificate configured.
```

```
Trustpoint VeriG3:   Subject Name:   cn=VeriSign Class 3 Secure Server CA - G3
```

```
ou=Terms of use at <url>
ou=VeriSign Trust Network
o=VeriSign\
  Inc.
c=US
  Serial Number (hex): 6ECC7AA5A7032009B8CEBCF4E952D491
Certificate configured
```



Configuration Example: Converged Access for WLC EAP-FAST with Internal RADIUS Server

This document describes how to configure the Cisco Converged Access Wireless LAN Controllers (WLCs), Cisco Catalyst 3850 Series, and Cisco Catalyst 3650 Series Switches to act as RADIUS servers that perform Cisco Extensible Authentication Protocol-Flexible Authentication via Secure Protocol (EAP-FAST, in this example) for client authentication.

An external RADIUS server is usually used to authenticate users, which in some cases is not a feasible solution. In situations where the RADIUS server is not a feasible solution to authenticate users, a Converged Access WLC can act as a RADIUS server, where users are authenticated against the local database that is configured in the WLC. The previously explained feature is called a Local RADIUS Server feature.

- [Prerequisites, page 71](#)
- [Configuring Converged Access WLC as RADIUS Server, page 73](#)
- [Verifying Configuration for Converged Access, page 79](#)
- [Troubleshooting the Configuration for Converged Access, page 79](#)

Prerequisites

We recommend that you have knowledge of the following topics before starting the configuration:

- Cisco IOS GUI or CLI with the Converged Access 3850 Series Switches WLCs, Cisco Catalyst 3850 Series, and Cisco Catalyst 3650 Series Switches.
- Extensible Authentication Protocol (EAP) concepts
- Service Set Identifier (SSID) configuration.
- RADIUS

Supported Platform and Releases

- Cisco Catalyst 3650 Series Switches

- Cisco Catalyst 3850 Series Switches

The information in this document is based on the following software and hardware versions:

- Cisco 3602 Series Lightweight Access Point (AP)
- Microsoft Windows XP with Intel PROset Supplicant
- Cisco Catalyst 3560 Series Switches



Note

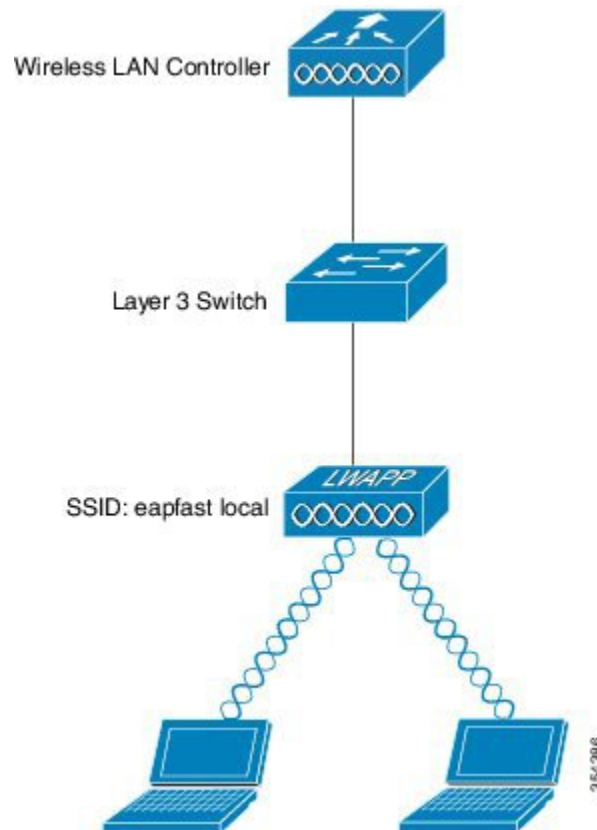
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a specific (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuring Converged Access WLC as RADIUS Server

Network Diagram for Converged Access

The following figure describes the network diagram of converged access:

Figure 11: Network Diagram



Configuring Converged Access

Configuring Converged Access WLC as RADIUS Server is based on the following steps:

- Configure the WLC for the local EAP method and the related authentication and authorization profiles with the CLI or GUI.
- Configure the WLAN and map the method list that has the authentication and authorization profiles.

Configuring WLC with CLI

Perform the following tasks to configure the WLC with the CLI:

- 1 To enable the AAA model on the WLC, use the following commands:

```
aaa new-model
```

- 2 To define authentication and authorization, use the following commands:

```
aaa local authentication eapfast authorization eapfast
aaa authentication dot1x eapfast local
aaa authorization credential-download eapfast local
aaa authentication dot1x default local
```

- 3 To configure the local EAP profile and the method, use the following commands (EAP-FAST is used in the following example):

```
eap profile eapfast
  method fast
!
```

- 4 To configure advanced EAP-FAST parameters, use the following commands:

```
eap method fast profile eapfast
  description test
  authority-id identity 1
  authority-id information 1
  local-key 0 cisco123
```

- 5 To configure WLAN and to map the local authorization profile to the WLAN, use the following commands:

```
wlan eapfastlocal 13 eapfastlocal
  client vlan VLAN0020
  local-auth eapfast
  session-timeout 1800
  no shutdown
```

- 6 To configure infrastructure to support the client connectivity, use the following commands:

```
ip dhcp snooping vlan 12,20,30,40,50
ip dhcp snooping
!
ip dhcp pool vlan20
  network 203.0.113.0 255.255.255.0
  default-router 203.0.113.251
  dns-server 203.0.113.251

interface TenGigabitEthernet1/0/1
  switchport trunk native vlan 12
  switchport mode trunk
  ip dhcp relay information trusted
  ip dhcp snooping trust
```

Configuring the WLC with the GUI

Perform the following tasks to configure the WLC with the GUI:

- 1 To configure the method list of Authentication, perform the following:
 - Configure the eapfast Type as **Dot1x**.

- Configure the eapfast Group Type as **Local**.

Figure 12: Authentication

Name	Type	Group Type	Group1	Group2	Group3	Group4
<input type="checkbox"/> Local_webauth	login	local	N/A	N/A	N/A	N/A
<input checked="" type="checkbox"/> default	dot1x	local	N/A	N/A	N/A	N/A
<input type="checkbox"/> ACS	dot1x	group	ACS	N/A	N/A	N/A
<input type="checkbox"/> TEF	dot1x	group	TEF	N/A	N/A	N/A
<input checked="" type="checkbox"/> eapfast	dot1x	local	N/A	N/A	N/A	N/A
<input type="checkbox"/> Webauth	dot1x	group	ACS	N/A	N/A	N/A

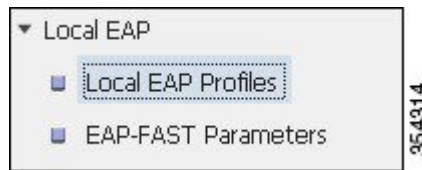
- 2 To configure the method list for Authorization, perform the following:
 - Configure the eapfast Type as **Credential-Download**.
 - Configure the eapfast Group Type as **Local**.

Figure 13: Authorization

Name	Type	Group Type	Group1	Group2	Group3	Group4
<input type="checkbox"/> default	network	local	N/A	N/A	N/A	N/A
<input type="checkbox"/> Webauth	network	group	ACS	N/A	N/A	N/A
<input type="checkbox"/> default	credential-download	local	N/A	N/A	N/A	N/A
<input checked="" type="checkbox"/> eapfast	credential-download	local	N/A	N/A	N/A	N/A

- 3 Configure the Local EAP profile.

Figure 14: EAP Profile



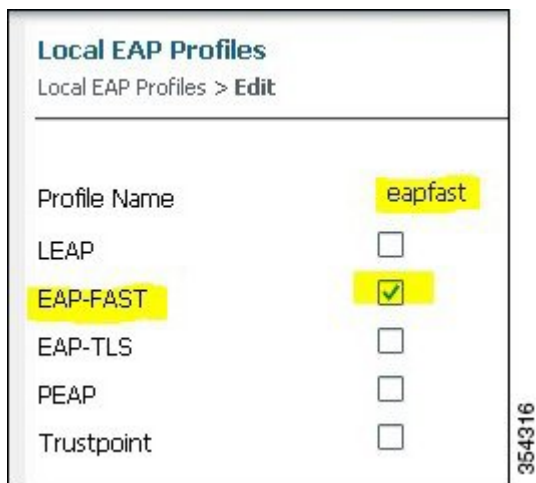
- 4 Create a new profile and choose the EAP type.

Figure 15: Local EAP Profiles

Profile Name	LEAP	EAP-FAST	EAP-TLS	PEAP
<input type="checkbox"/> eapfast	Disabled	Enabled	Disabled	Disabled

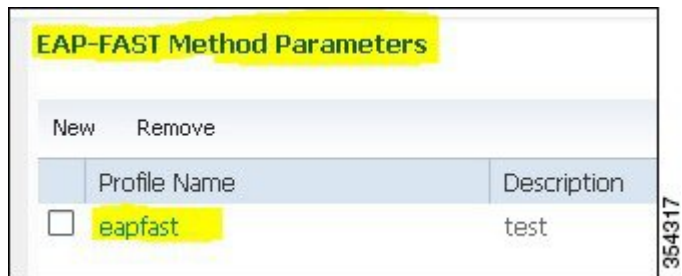
The Profile Name is **eapfast** and the chosen EAP type is **EAP-FAST** as shown in the following figure:

Figure 16: Local EAP Profiles



5 Configure the EAP-FAST Method Parameters:

Figure 17: EAP-FAST Method Parameters



The Server Key is configured as **Cisco123**.

Figure 18: EAP-FAST Method Profile

EAP-FAST Method Profile	
EAP-FAST Method Profile > Edit	
Profile Name	eapfast
Server Key	••••••••
Confirm Server Key	••••••••
Time to live (secs)	86400
Authority ID	1
Authority ID Information	1
Description	test

354318

- 6 Check the **Dot1x System Auth** Control check box and choose **eapfast** for the Method Lists. Selecting Dot1x System Auth control and eapfast Method Lists helps you to perform the local EAP authentication.

Figure 19: Security

Security	
General	
Dot1x System Auth Control	<input checked="" type="checkbox"/>
Local Authentication	Method List
Authentication Method List	eapfast
Local Authorization	Method List
Authorization Method List	eapfast

354319

- 7 Configure the WLAN for WPA2 AES encryption.

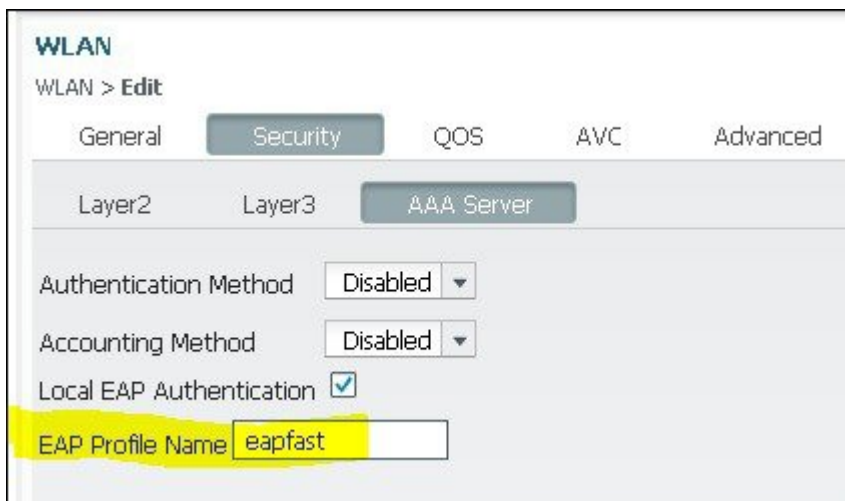
Figure 20: WLAN



354320

- 8 On the AAA Server tab, map the EAP Profile Name eapfast to the WLAN:

Figure 21: WLAN



354321

Verifying Configuration for Converged Access

Perform the following steps to verify the configuration:

- 1 Connect the client to the WLAN as shown in the following figure:

Figure 22:



- 2 Verify that the Protected Access Credentials (PAC) popup appears. Accept the PAC popup to authenticate successfully.

Figure 23:



Troubleshooting the Configuration for Converged Access

We recommend that you use traces to troubleshoot wireless issues. Traces are saved in the circular buffer and are not processor intensive.

To enable the traces to obtain the Layer 2 (L2) auth logs, use the following commands:

- **set trace group-wireless-secure level debug**
- **set trace group-wireless-secure filter mac0021.6a89.51ca**

To enable these traces to obtain the DHCP events logs, use the following commands:

- set trace dhcp events level debug
- set trace dhcp events filter mac 0021.6a89.51ca

The following output is an example of a successful trace:

```
[04/10/14 18:49:50.719 IST 3 8116] 0021.6a89.51ca Association received from
mobile on AP c8f9.f983.4260

[04/10/14 18:49:50.719 IST 4 8116] 0021.6a89.51ca qos upstream policy is
unknown and downstream policy is unknown
[04/10/14 18:49:50.719 IST 5 8116] 0021.6a89.51ca apChanged 1 wlanChanged 0
mscb ipAddr 20.20.20.6, apf RadiusOverride 0x0, numIPv6Addr=0
[04/10/14 18:49:50.719 IST 6 8116] 0021.6a89.51ca Applying WLAN policy on MSCB.
[04/10/14 18:49:50.719 IST 7 8116] 0021.6a89.51ca Applying WLAN ACL policies
to client

[04/10/14 18:49:50.719 IST 9 8116] 0021.6a89.51ca Applying site-specific IPv6
override for station 0021.6a89.51ca - vapId 13, site 'default-group',
interface 'VLAN0020'
[04/10/14 18:49:50.719 IST a 8116] 0021.6a89.51ca Applying local bridging
Interface Policy for station 0021.6a89.51ca - vlan 20, interface 'VLAN0020'
[04/10/14 18:49:50.719 IST b 8116] 0021.6a89.51ca STA - rates (8):
140 18 152 36 176 72 96 108 48 72 96 108 0 0 0 0

[04/10/14 18:49:50.727 IST 2f 8116] 0021.6a89.51ca Session Manager Call Client
57ca4000000048, uid 42, capwap id 50b94000000012, Flag 4, Audit-Session ID
0a6987b253468efb00000002a, method list

[04/10/14 18:49:50.727 IST 30 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
[0021.6a89.51ca, Ca3] Session update from Client[1] for 0021.6a89.51ca,
ID list 0x00000000
[04/10/14 18:49:50.727 IST 31 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
[0021.6a89.51ca, Ca3] (UPD): method: Dot1X, method list: none, aaa id:
0x00000002A
[04/10/14 18:49:50.727 IST 32 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
[0021.6a89.51ca, Ca3] (UPD): eap profile: eapfast

[04/10/14 18:49:50.728 IST 4b 278] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3]
Posting AUTH_START for 0xF700000A
[04/10/14 18:49:50.728 IST 4c 278] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3]
0xF700000A:entering request state
[04/10/14 18:49:50.728 IST 4d 278] ACCESS-METHOD-DOT1X-NOTF:[0021.6a89.51ca,Ca3]
Sending EAPOL packet
[04/10/14 18:49:50.728 IST 4e 278] ACCESS-METHOD-DOT1X-INFO:[0021.6a89.51ca,Ca3]
Platform changed src mac of EAPOL packet
[04/10/14 18:49:50.728 IST 4f 278] ACCESS-METHOD-DOT1X-INFO:[0021.6a89.51ca,Ca3]
EAPOL packet sent to client 0xF700000A
[04/10/14 18:49:50.728 IST 50 278] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3]
0xF700000A:idle request action
[04/10/14 18:49:50.761 IST 51 8116] 0021.6a89.51ca 1XA: Received 802.11 EAPOL
message (len 5) from mobile
[04/10/14 18:49:50.761 IST 52 8116] 0021.6a89.51ca 1XA: Received EAPOL-Start
from mobile
[04/10/14 18:49:50.761 IST 53 8116] 0021.6a89.51ca 1XA: EAPOL-Start -
EAPOL start message from mobile as mobile is in Authenticating state, restart
authenticating

[04/10/14 18:49:50.816 IST 95 278] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3]
0xF700000A:entering response state
[04/10/14 18:49:50.816 IST 96 278] ACCESS-METHOD-DOT1X-NOTF:[0021.6a89.51ca,Ca3]
Response sent to the server from 0xF700000A
[04/10/14 18:49:50.816 IST 97 278] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3]
0xF700000A:ignore response action
[04/10/14 18:49:50.816 IST 98 203] Parsed CLID MAC Address = 0:33:106:137:81:202
[04/10/14 18:49:50.816 IST 99 203] AAA SRV(00000000): process authen req
[04/10/14 18:49:50.816 IST 9a 203] AAA SRV(00000000): Authen method=LOCAL

[04/10/14 18:49:50.846 IST 11d 181] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
[0021.6a89.51ca, Ca3] Session authz status notification sent to Client[1] for
0021.6a89.51ca with handle FE000052, list 630007B2
[04/10/14 18:49:50.846 IST 11e 181]ACCESS-METHOD-DOT1X-NOTF:[0021.6a89.51ca,Ca3]
```

```
Received Authz Success for the client 0xF700000A (0021.6a89.51ca)
[04/10/14 18:49:50.846 IST 11f 271] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3]
Posting AUTHZ SUCCESS on Client 0xF700000A
[04/10/14 18:49:50.846 IST 120 271] ACCESS-METHOD-DOT1X-DEB:[0021.6a89.51ca,Ca3]
0xF700000A:entering authenticated state
[04/10/14 18:49:50.846 IST 121 271]ACCESS-METHOD-DOT1X-NOTF:[0021.6a89.51ca,Ca3]
EAPOL success packet was sent earlier.

[04/10/14 18:49:50.846 IST 149 8116] 0021.6a89.51ca 1XA:authentication succeeded
[04/10/14 18:49:50.846 IST 14a 8116] 0021.6a89.51ca 1XK: Looking for BSSID
c8f9.f983.4263 in PMKID cache
[04/10/14 18:49:50.846 IST 14b 8116] 0021.6a89.51ca 1XK: Looking for BSSID
c8f9.f983.4263 in PMKID cache
[04/10/14 18:49:50.846 IST 14c 8116] 0021.6a89.51ca Starting key exchange with
mobile - data forwarding is disabled
[04/10/14 18:49:50.846 IST 14d 8116] 0021.6a89.51ca 1XA: Sending EAPOL message
to mobile, WLAN=13 AP WLAN=13
[04/10/14 18:49:50.858 IST 14e 8116] 0021.6a89.51ca 1XA: Received 802.11 EAPOL
message (len 123) from mobile
[04/10/14 18:49:50.858 IST 14f 8116] 0021.6a89.51ca 1XA: Received EAPOL-Key from
mobile
[04/10/14 18:49:50.858 IST 150 8116] 0021.6a89.51ca 1XK: Received EAPOL-key in
PTK_START state (msg 2) from mobile
[04/10/14 18:49:50.858 IST 151 8116] 0021.6a89.51ca 1XK: Stopping retransmission
timer
[04/10/14 18:49:50.859 IST 152 8116] 0021.6a89.51ca 1XA: Sending EAPOL message
to mobile, WLAN=13 AP WLAN=13
[04/10/14 18:49:50.862 IST 153 8116] 0021.6a89.51ca 1XA: Received 802.11 EAPOL
message (len 99) from mobile
[04/10/14 18:49:50.862 IST 154 8116] 0021.6a89.51ca 1XA: Received EAPOL-Key from
mobile
[04/10/14 18:49:50.862 IST 155 8116] 0021.6a89.51ca 1XK: Received EAPOL-key in
PTKINITNEGOTIATING state (msg 4) from mobile

[04/10/14 18:49:50.863 IST 172 338] [WCDB] wcdb_ffcp_cb: client (0021.6a89.51ca)
client (0x57ca4000000048): FFCP operation (UPDATE) return code (0)
[04/10/14 18:49:50.914 IST 173 273] dhcp pkt processing routine is called for pak
with SMAC = 0021.6a89.51ca and SRC_ADDR = 0.0.0.0
[04/10/14 18:49:50.914 IST 174 219] sending dhcp packet outafter processing with
SMAC = 0021.6a89.51ca and SRC_ADDR = 0.0.0.0
[04/10/14 18:49:50.914 IST 175 256] DHCPD: address 20.20.20.6 mask 203.0.113.1
[04/10/14 18:49:54.279 IST 176 273] dhcp pkt processing routine is called for pak
with SMAC = 0021.6a89.51ca and SRC_ADDR = 20.20.20.6
[04/10/14 18:49:54.279 IST 177 219] sending dhcp packet outafter processing with
SMAC = 0021.6a89.51ca and SRC_ADDR = 20.20.20.6
```




Converged Access and WLC Local EAP Authentication Configuration Example

This document describes how to configure the Cisco Catalyst 3850 Series Switch for Local Extensible Authentication Protocol (EAP) to authenticate the wireless network users. The authentication method used in this document is **PEAP-MSChapv2**, which is one of the most-common method available in the supplicants.

- [Prerequisites, page 83](#)
- [WLC Local EAP Authentication, page 84](#)
- [Configuring Local EAP authentication, page 85](#)
- [Verifying the Local EAP Authentication Configuration, page 87](#)
- [Troubleshooting the Local EAP Authentication configuring issues, page 89](#)
- [Debugs for dot1x and EAP, page 89](#)

Prerequisites

We recommend that you have basic and functional knowledge on the following topics:

- WLC and Lightweight Access Points (LAPs).
- Authentication, Authorization, and Accounting (AAA) server.
- Wireless networks and wireless security issues.



Note

The information in this document is written by assuming, wireless access points have already joined the Cisco Catalyst 3850 Series Switch and supplicant is properly configured for the authentication methods that are used.

Supported Platforms and Releases

The information in this document is based on the following:

- Code used for GUI Cisco Catalyst 3850 Series Switch is 03.02.02.SE.150-1.EX2 (This is valid on June 25, 2013).
- Access Point (AP) used is AP1142N.
- Supplicant used is Microsoft (MS) Windows 7 Enterprise with a wireless card TP-Link n600 Dual Band USB Adapter and Cisco Anyconnect Version 3.1.

**Note**

The information in this document is created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

WLC Local EAP Authentication

Local EAP is an authentication method that allows user and wireless client authentication locally on the controller. When you enable local EAP, the controller serves as the authentication server and the local user database, hence it removes dependence on an external authentication server. Local EAP retrieves user credentials from the local user database.

To view the methods that local EAP supports for authentication between the controller and wireless client, enter the following command:

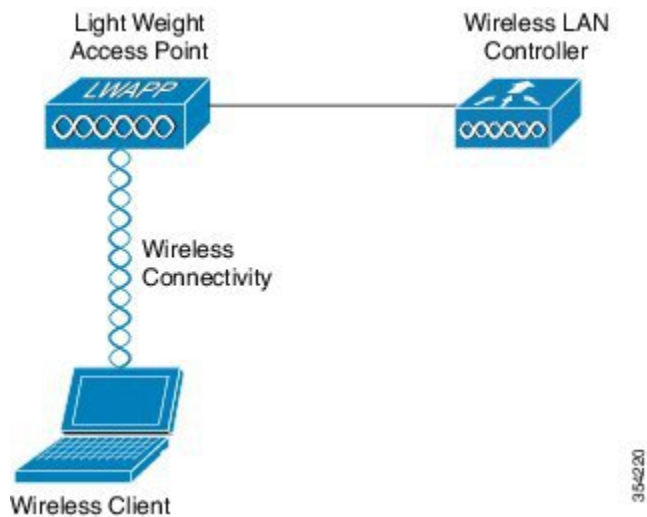
```
Device(config-eap-profile)# method ?
fast      EAP-FAST method allowed
gtc       EAP-GTC method allowed
leap      EAP-LEAP method allowed
md5       EAP-MD5 method allowed
mschapv2  EAP-MSCHAPV2 method allowed
peap      EAP-PEAP method allowed
tls       EAP-TLS method allowed
```


Configuring Local EAP authentication

Network Diagram of LAP and WLC

The following figure represents the network diagram of LAP and WLC connected to a wireless client.

Figure 24: Network diagram of LAP and WLC connected to a wireless client



3154220

Configuring Local EAP Authentication

Perform the following tasks in order to configure local EAP authentication:

- 1 Create a test user, by entering following command:

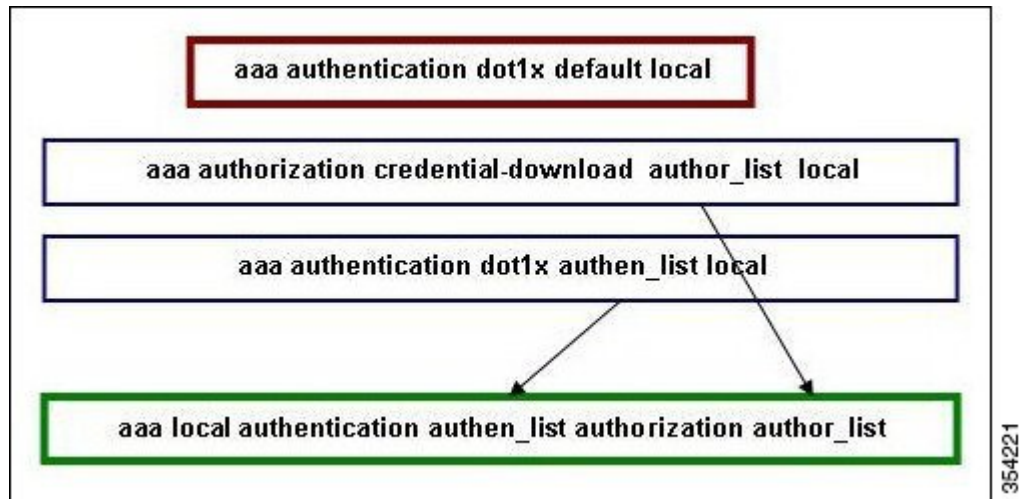
```
user-name test
privilege 15
password 0 cisco
type network-user description pass=cisco
```

- 2 To enable the authentication, authorization, and accounting (AAA) access control model, enter the following command:

```
aaa new-model
```

- 3 Define the authentication and authorization for AAA as shown in the following figure:

Figure 25: Flow of authentication and authorization for AAA



- a** To terminate EAP sessions locally, enter the following command;
`aaa authentication dot1x default local`
- b** To prepare a method list for the credential download, enter the following command;
`aaa authorization credential-download author_list local`



Note In this example, the local is configured in the method list `author_list`. This method list is one of the parameters for the `aaa local authentication authen_list authorization author_list` CLI command.

- c** Enter the following CLI command in order to define an authentication method list, which is used by the local EAP for verification of the credentials when the EAP requests local EAP with the `EAP_VERIFY_PASSWORD_EVENT` event:
`aaa authentication dot1x authen_list local`



Note This method list name is the parameter for the `aaa local authentication authen_list authorization author_list` CLI command.

- d** Specify where the local EAP must be downloaded or verify the credentials:
`aaa local authentication authen_list authorization author_list`



Note Define the `authen_list` and `author_list` before downloading local EAP; refer to steps a and b for more information on how to prepare and define the method list.

- 4 Begin the dot1x process by entering following command:
`dot1x system-auth-control`

- 5 To define the supported authentication methods, create the EAP profile (For example, PEAP-MSchapv2).

```
eap profile PEAPProfile
method peap
method mschapv2
```

- 6 Use the EAP profile to configure the Service Set Identifier (SSID).

```
wlan TiagoNGWC 1 TiagoNGWC

client vlan VLAN0080
ip dhcp server 192.168.80.14
local-auth PEAPProfile
```

- 7 Set up the DHCP pool and the Switch Virtual Interface (SVI) for the client VLAN. In the following example set up is completed on Converged Access with use of VLAN80:

```
ip dhcp excluded-address 192.168.80.1 192.168.80.99
!
ip dhcp pool VLAN80
network 192.168.80.0 255.255.255.0
default-router 192.168.80.14

interface Vlan80
ip address 192.168.80.14 255.255.255.0
```

Verifying the Local EAP Authentication Configuration

Perform the following task in order to verify your configuration:

Device# **show wlan name TiagoNGWC**

```
WLAN Profile Name      : TiagoNGWC
=====
Identifier              : 1
Network Name (SSID)    : TiagoNGWC
Status                  : Enabled
Broadcast SSID         : Enabled
Maximum number of Associated Clients : 0
AAA Policy Override    : Disabled
Network Admission Control
  NAC-State             : Disabled
Number of Active Clients : 1
Exclusionlist Timeout  : 60
Session Timeout       : 1800 seconds
CHD per WLAN          : Enabled
Webauth DHCP exclusion : Disabled
Interface              : VLAN0080
Interface Status      : Up
Multicast Interface    : Unconfigured
WLAN IPv4 ACL          : unconfigured
WLAN IPv6 ACL          : unconfigured
DHCP Server            : 192.168.80.14
DHCP Address Assignment Required : Disabled
DHCP Option 82        : Disabled
DHCP Option 82 Format  : ap-mac
DHCP Option 82 Ascii Mode : Disabled
DHCP Option 82 Rid Mode : Disabled
QoS Service Policy - Input
  Policy Name          : unknown
  Policy State         : None
QoS Service Policy - Output
  Policy Name          : unknown
  Policy State         : None
QoS Client Service Policy
  Input Policy Name    : unknown
  Output Policy Name   : unknown
WMM                    : Allowed
```

Verifying the Local EAP Authentication Configuration

```

Channel Scan Defer Priority:
  Priority (default)           : 4
  Priority (default)           : 5
  Priority (default)           : 6
Scan Defer Time (msecs)      : 100
Media Stream Multicast-direct : Disabled
CCX - AironetIe Support      : Enabled
CCX - Gratuitous ProbeResponse (GPR) : Disabled
CCX - Diagnostics Channel Capability : Disabled
Dot11-Phone Mode (7920)     : Invalid
Wired Protocol               : None
Peer-to-Peer Blocking Action : Disabled
Radio Policy                  : All
DTIM period for 802.11a radio : 1
DTIM period for 802.11b radio : 1
Local EAP Authentication     : PEAPProfile
Mac Filter Authorization list name : Disabled
Accounting list name         : Disabled
802.1x authentication list name : Disabled
Security
  802.11 Authentication      : Open System
  Static WEP Keys            : Disabled
  802.1X
    Wi-Fi Protected Access (WPA/WPA2) : Enabled
      WPA (SSN IE)           : Disabled
      WPA2 (RSN IE)         : Enabled
      TKIP Cipher            : Disabled
      AES Cipher             : Enabled
    Auth Key Management
      802.1x                  : Enabled
      PSK                     : Disabled
      CCKM                    : Disabled
  CKIP                       : Disabled
  IP Security                 : Disabled
  IP Security Passthru       : Disabled
  L2TP                       : Disabled
  Web Based Authentication   : Disabled
  Conditional Web Redirect   : Disabled
  Splash-Page Web Redirect   : Disabled
  Auto Anchor                 : Disabled
  Sticky Anchoring           : Enabled
  Cranite Passthru           : Disabled
  Fortress Passthru          : Disabled
  PPTP                       : Disabled
  Infrastructure MFP protection : Enabled
  Client MFP                  : Optional
  Webauth On-mac-filter Failure : Disabled
  Webauth Authentication List Name : Disabled
  Webauth Parameter Map      : Disabled
  Tkip MIC Countermeasure Hold-down Timer : 60
Call Snooping                : Disabled
Passive Client                : Disabled
Non Cisco WGB                 : Disabled
Band Select                   : Disabled
Load Balancing                : Disabled
IP Source Guard               : Disabled

```

Device# **show wireless client mac-address 6470.0227.0a89 detail**

```

Client MAC Address : 6470.0227.0a89
Client Username   : tiago
AP MAC Address    : 64d8.146f.e5a0
AP Name: APd48c.b52f.4a1e
Client State      : Associated
Wireless LAN Id   : 1
Wireless LAN Name: TiagoNGWC
BSSID : 64d8.146f.e5a0
Connected For    : 323 secs
Protocol : 802.11n - 2.4 GHz
Channel : 6
IPv4 Address    : 192.168.80.100
IPv6 Address    : Unknown
Association Id   : 1

```

```
Authentication Algorithm : Open System
...
Policy Manager State : RUN
Policy Manager Rule Created : Yes
NPU Fast Fast Notified : Yes
Last Policy Manager State : RUN
Client Entry Create Time : 153207 seconds
Policy Type : WPA2
Authentication Key Management : 802.1x
Encryption Cipher : CCMP (AES)
Management Frame Protection : No
EAP Type : PEAP
Interface : VLAN0080
VLAN : 80
Quarantine VLAN : 0
Access VLAN : 80
...
```

Troubleshooting the Local EAP Authentication configuring issues

This section provides troubleshooting information on Local EAP Authentication configuring issues.

Enable Traces for Wireless Client Issues

- To trace the wireless client issues enter the following command:

```
set trace group-wireless-client level debug
debug client mac <MAC>
```

- To filter on a specific MAC address, enter:

```
set trace group-wireless-client filter mac <MAC>
```

- To view unfiltered output, enter:

```
show trace messages group-wireless-client
```

- To view filtered output, enter:

```
show trace sys-filtered-traces
```

- To view the settings, enter:

```
show trace all-buffer settings
```

- Enable **debug ip device tracking**, suppose if you come across issues while retrieving IP addresses.

**Note**

Depending on issues encountered, you may need to view other traces.

Debugs for dot1x and EAP

Following are the debug commands used for **dot1x** and **EAP** configurations.

Debug command outputs are as follows;

```
Device#
*Sep 19 07:00:21.423: 6470.0227.0A89 Association received from mobile on AP
```

```

64D8.146F.E5A0 1 wcm: cct Msg Sent at 1379573926 se
*Sep 19 07:00:21.423: 6470.0227.0A89 qos upstream policy is unknown and
downstreampolicy is unknown 1 wcm: Sent at 1379573926 se
*Sep 19 07:00:21.423: 6470.0227.0A89 apChanged 0 wlanChanged 0 mscb ipAddr
192.168.80.100, apf RadiusOverride 0x0, numIPv6Addr=0 1 wcm: = 0^M
*Sep 19 07:00:21.423: 6470.0227.0A89 Applying WLAN policy on MSCB. 1 wcm:
ipAddr 192.168.80.100, apf RadiusOverride 0x0, numIPv6Addr=0
*Sep 19 07:00:21.424: 6470.0227.0A89 Applying WLAN ACL policies to client 1
wcm: 192.168.80.100, apf RadiusOverride 0x0, numIPv6Addr=0
*Sep 19 07:00:21.424: 6470.0227.0A89 No Interface ACL used for Wireless
client in WCM(NGWC) 1 wcm: pf RadiusOverride 0x0, numIPv6Addr=0
*Sep 19 07:00:21.424: 6470.0227.0A89 Applying site-specific IPv6 override for
station 6470.0227.0A89 - vapId 1, site 'default-group', interface
'VLAN0080' 1 wcm:
*Sep 19 07:00:21.424: 6470.0227.0A89 Applying local bridging Interface Policy
for station 6470.0227.0A89 - vlan 80, interface 'VLAN0080' 1 wcm: erface
'VLAN0080'
*Sep 19 07:00:21.424: 6470.0227.0A89 STA - rates (8): 1 wcm:
130 132 139 12 18 150 24 36 48 72 96 108 0 0 0 0
*Sep 19 07:00:21.424: 6470.0227.0A89 STA - rates (12): 1 wcm:
130 132 139 12 18 150 24 36 48 72 96 108 0 0 0 0
*Sep 19 07:00:21.424: 6470.0227.0A89 new capwap_wtp_iif_id d7844000000004,sm
capwap_wtp_iif_id d7844000000004 1 wcm: an 80, interface 'VLAN0080'
*Sep 19 07:00:21.424: 6470.0227.0A89 In >= L2AUTH_COMPLETE for station
6470.0227.0A89 1 wcm: iif_id d7844000000004
*Sep 19 07:00:21.424: 6470.0227.0A89 192.168.80.100 RUN (20) Change state
to START (0) last state RUN (20)
1 wcm:
*Sep 19 07:00:21.424: 6470.0227.0A89 WCDB_CHANGE: 1 wcm: Client 1 m_vlan 80
Radio iif id 0xdf0f4000000005 bssid iif Id 0xcd248000000015, bssid
64D8.146F.E5A0
*Sep 19 07:00:21.424: 6470.0227.0A89 WCDB_AUTH: 1 wcm: Adding opt82 len 0
*Sep 19 07:00:21.425: 6470.0227.0A89 WCDB_LLM: 1 wcm: NoRun Prev Mob 1, Curr
Mob 1 llmReq 5, return True
*Sep 19 07:00:21.425: 6470.0227.0A89 auth state 0 mob state 1 setWme 0 wme 1
roam_sent 0
1 wcm: rn True
*Sep 19 07:00:21.425: 6470.0227.0A89 WCDB_CHANGE: 1 wcm: auth=ASSOCIATION(0)
vlan 80 radio 0 client_id 0xde51c000000021 mobility=Local(1) src_int
0xd7844000000004 dst_int 0x0 ackflag 2 reassoc_client 0 llm_notif 1 ip
192.168.80.100 ip_learn_type ARP
*Sep 19 07:00:21.425: 6470.0227.0A89 192.168.80.100 START (0) Initializing
policy 1 wcm: 0 client_id 0xde51c000000021 mobility=Local(1) src_int
0xd7844000000004 dst_int 0x0 ackflag 2 reassoc_client 0 llm_notif 1 ip
192.168.80.100 ip_learn_type ARP
*Sep 19 07:00:21.425: PEM recv processing msg Del SCB(4) 1 wcm: T (0)
Initializing policy
*Sep 19 07:00:21.425: 6470.0227.0A89 192.168.80.100 START (0) Change state
to AUTHCHECK (2) last state RUN (20)
1 wcm: bility=Local(1) src_int 0xd7844000000004 dst_int 0x0 ackflag 2
reassoc_client 0 llm_notif 1 ip 192.168.80.100 ip_learn_type ARP
*Sep 19 07:00:21.425: 6470.0227.0A89 192.168.80.100 AUTHCHECK (2) Change
state to 8021X_REQD (3) last state RUN (20)
1 wcm: y=Local(1) src_int 0xd7844000000004 dst_int 0x0 ackflag 2
reassoc_client 0 llm_notif 1 ip 192.168.80.100 ip_learn_type ARP
*Sep 19 07:00:21.425: 6470.0227.0A89 192.168.80.100 8021X_REQD (3) DHCP
required on AP 64D8.146F.E5A0 vapId 1 apVapId 1 for this client 1 wcm:
0xd7844000000004 dst_int 0x0 ackflag 2 reassoc_client 0 llm_notif 1 ip
192.168.80.100 ip_learn type ARP
*Sep 19 07:00:21.425: 6470.0227.0A89 Not Using WMM Compliance code qosCap 00
1 wcm: uired on AP 64D8.146F.E5A0 vapId 1 apVapId 1 for this client
*Sep 19 07:00:21.425: 6470.0227.0A89 192.168.80.100 8021X_REQD (3) Plumbed
mobile LWAPP rule on AP 64D8.146F.E5A0 vapId 1 apVapId 1 1 wcm: nt
*Sep 19 07:00:21.425: 6470.0227.0A89 apfPemAddUser2 (apf_policy.c: 1 wcm:161)
Changing state for mobile 6470.0227.0A89 on AP 64D8.146F.E5A0 from
Associated to Associated
*Sep 19 07:00:21.426: 6470.0227.0A89 Stopping deletion of Mobile Station: 1
wcm: (callerId: 48)
*Sep 19 07:00:21.426: 6470.0227.0A89 Ms Timeout = 0, Session Timeout = 1800
1 wcm: llerId: 48)
*Sep 19 07:00:21.426: 6470.0227.0A89 Sending Assoc Response to station on
BSSID 64D8.146F.E5A0 (status 0) ApVapId 1 Slot 0 1 wcm: .146F.E5A0 from
Associated to Associated

```

```

*Sep 19 07:00:21.426: 6470.0227.0A89 apfProcessAssocReq (apf_80211.c: 1 wcm:
5260) Changing state for mobile 6470.0227.0A89 on AP 64D8.146F.E5A0 from
Associated to Associated
*Sep 19 07:00:21.426: 6470.0227.0A89 192.168.80.100 8021X_REQD (3) Handling
pemDelScb Event skipping delete 1 wcm: 7.0A89 on AP 64D8.146F.E5A0 from
Associated to Associated
*Sep 19 07:00:21.435: dot1x-sm:[6470.0227.0a89, Ca0] Posting RESTART on
Client 0x60000009
*Sep 19 07:00:21.435: dot1x_auth Ca0: during state auth_authenticated,
got event 13(restart)
*Sep 19 07:00:21.435: @@@ dot1x_auth Ca0: auth_authenticated -> auth_restart
*Sep 19 07:00:21.435: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:exiting
authenticated state
*Sep 19 07:00:21.435: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:
entering restart
*Sep 19 07:00:21.435: dot1x-ev:[6470.0227.0a89, Ca0] Override cfg -
MAC 6470.0227.0a89 - profile PEAPProfile
*Sep 19 07:00:21.435: dot1x-ev:[6470.0227.0a89, Ca0] Override cfg -
SuppTimeout 30s, ReAuthMax 2, MaxReq 2, TxPeriod 30s
*Sep 19 07:00:21.435: dot1x-ev:[6470.0227.0a89, Ca0] Sending create new
context event to EAP for 0x60000009 (6470.0227.0a89)
*Sep 19 07:00:21.435: EAP-EVENT: Received context create from LL
(Dot1x-Authenticator) (0x60000009)
*Sep 19 07:00:21.436: EAP-AUTH-EVENT: Received AAA ID 0x0000001F from LL
*Sep 19 07:00:21.436: EAP-AUTH-AAA-EVENT: Assigning AAA ID 0x0000001F
*Sep 19 07:00:21.436: EAP-AUTH-EVENT: Received Session ID
"00a82104523aa0a30000001f" from LL
*Sep 19 07:00:21.436: EAP-AUTH-EVENT: Setting authentication mode:
Passthrough
*Sep 19 07:00:21.436: EAP-EVENT: Using EAP profile "PEAPProfile"
(handle 0x26000052)
*Sep 19 07:00:21.436: eap_authen : initial state eap_auth_initialize
has enter
*Sep 19 07:00:21.436: EAP-EVENT: Allocated new EAP context
(handle = 0x26000052)
*Sep 19 07:00:21.436: dot1x-sm:[6470.0227.0a89, Ca0] Posting
!EAP_RESTART on Client 0x60000009
*Sep 19 07:00:21.436: dot1x_auth Ca0: during state auth_restart, got
event 6(no_eapRestart)
*Sep 19 07:00:21.436: @@@ dot1x_auth Ca0: auth_restart -> auth_connecting
*Sep 19 07:00:21.436: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:enter
connecting state
*Sep 19 07:00:21.436: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009: restart
connecting
*Sep 19 07:00:21.436: EAP-EVENT: Received EAP event
'EAP_AUTHENTICATOR_START' on handle 0x26000052
*Sep 19 07:00:21.436: eap_authen : during state eap_auth_initialize,
got event 25(eapStartTmo)
*Sep 19 07:00:21.436: @@@ eap_authen : eap_auth_initialize ->
eap_auth_select_action
*Sep 19 07:00:21.436: eap_authen : during state eap_auth_select_action,
got event 20(eapDecisionPropose)
*Sep 19 07:00:21.436: @@@ eap_authen : eap_auth_select_action ->
eap_auth_propose_method
*Sep 19 07:00:21.436: eap_authen : idle during state
eap_auth_propose_method
*Sep 19 07:00:21.436: @@@ eap_authen : eap_auth_propose_method ->
eap_auth_method_request
*Sep 19 07:00:21.436: eap_authen : idle during state
eap_auth_method_request
*Sep 19 07:00:21.436: @@@ eap_authen : eap_auth_method_request ->
eap_auth_tx_packet
*Sep 19 07:00:21.436: EAP-AUTH-EVENT: Current method = Identity
*Sep 19 07:00:21.436: EAP-EVENT: Sending LL (Dot1x-Authenticator) event
'EAP_CUSTOMIZE_ID_REQUEST' on handle 0x26000052
*Sep 19 07:00:21.436: eap_authen : idle during state eap_auth_tx_packet
*Sep 19 07:00:21.437: @@@ eap_authen : eap_auth_tx_packet -> eap_auth_idle
*Sep 19 07:00:21.437: EAP-AUTH-TX-PAK: Code:REQUEST ID:0xA Length:0x0047
Type:IDENTITY
Payload: 006E6574776F726B69643D546961676F ...
*Sep 19 07:00:21.437: EAP-EVENT: Started 'Authenticator ReqId Retransmit'
timer (30s) for EAP sesion handle 0x26000052
*Sep 19 07:00:21.437: EAP-EVENT: Started EAP tick timer

```

```

*Sep 19 07:00:21.437: EAP-EVENT: Sending LL (Dot1x-Authenticator) event
'EAP_TX_PACKET' on handle 0x26000052
*Sep 19 07:00:21.437: dot1x-sm:[6470.0227.0a89, Ca0] Posting RX_REQ on Client
0x60000009
*Sep 19 07:00:21.437: dot1x_auth Ca0: during state auth_connecting, got
event 10(eapReq_no_reAuthMax)
*Sep 19 07:00:21.437: @@@ dot1x_auth Ca0: auth_connecting ->
auth_authenticating
*Sep 19 07:00:21.437: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:
authenticating state entered
*Sep 19 07:00:21.437: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:connecting
authenticating action
*Sep 19 07:00:21.437: dot1x-sm:[6470.0227.0a89, Ca0] Posting AUTH_START for
0x60000009
*Sep 19 07:00:21.437: dot1x_auth_bend Ca0: during state auth_bend_idle,
got event 4(eapReq_authStart)
*Sep 19 07:00:21.437: @@@ dot1x_auth_bend Ca0: auth_bend_idle ->
auth_bend_request
*Sep 19 07:00:21.437: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:entering
request state
*Sep 19 07:00:21.437: dot1x-ev:[6470.0227.0a89, Ca0] Sending EAPOL packet
*Sep 19 07:00:21.437: dot1x-packet:[6470.0227.0a89, Ca0] Platform changed
src mac of EAPOL packet
*Sep 19 07:00:21.438: dot1x-registry:registry:dot1x_ether_macaddr called
*Sep 19 07:00:21.438: dot1x-packet:EAPOL pak Tx - Ver: 0x3 type: 0x0
*Sep 19 07:00:21.438: dot1x-packet: length: 0x0047
*Sep 19 07:00:21.438: dot1x-packet:EAP code: 0x1 id: 0xA length: 0x0047
*Sep 19 07:00:21.438: dot1x-packet: type: 0x1
*Sep 19 07:00:21.438: dot1x-packet:[6470.0227.0a89, Ca0] EAPOL packet sent
to client 0x60000009
*Sep 19 07:00:21.438: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:idle request
action
*Sep 19 07:00:22.149: dot1x-packet:[6470.0227.0a89, Ca0] Queuing an EAPOL
pkt on Authenticator Q
*Sep 19 07:00:22.149: dot1x-packet:EAPOL pak rx - Ver: 0x3 type: 0x0
*Sep 19 07:00:22.149: dot1x-packet: length: 0x000A
*Sep 19 07:00:22.149: dot1x-ev:[Ca0] Dequeued pkt: Int Ca0 CODE= 2,TYPE= 1,
LEN= 10

*Sep 19 07:00:22.149: dot1x-ev:[Ca0] Received pkt saddr =6470.0227.0a89,
daddr = 64d8.146f.e5a0, pae-ether-type = 888e.0300.000a
*Sep 19 07:00:22.149: dot1x-packet:EAPOL pak rx - Ver: 0x3 type: 0x0
*Sep 19 07:00:22.150: dot1x-packet: length: 0x000A
*Sep 19 07:00:22.150: dot1x-sm:[6470.0227.0a89, Ca0] Posting EAPOL_EAP for
0x60000009
*Sep 19 07:00:22.150: dot1x_auth_bend Ca0: during state
auth_bend_request, got event 6(eapolEap)
*Sep 19 07:00:22.150: @@@ dot1x_auth_bend Ca0: auth_bend_request ->
auth_bend_response
*Sep 19 07:00:22.150: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:entering
response state
*Sep 19 07:00:22.150: dot1x-ev:[6470.0227.0a89, Ca0] Response sent to the
server from 0x60000009
*Sep 19 07:00:22.150: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:request
response action
*Sep 19 07:00:22.150: EAP-EVENT: Received LL (Dot1x-Authenticator) event
'EAP_RX_PACKET' on handle 0x26000052
*Sep 19 07:00:22.150: EAP-AUTH-RX-PAK: Code:RESPONSE ID:0xA Length:0x000A
Type:IDENTITY
*Sep 19 07:00:22.150: Payload: 746961676F
*Sep 19 07:00:22.150: eap_authen : during state eap_auth_idle, got
event 1(eapRxPacket)
*Sep 19 07:00:22.150: @@@ eap_authen : eap_auth_idle -> eap_auth_received
*Sep 19 07:00:22.150: EAP-AUTH-EVENT: EAP Response received by context
0x26000052
*Sep 19 07:00:22.150: EAP-AUTH-EVENT: EAP Response type = Identity
*Sep 19 07:00:22.150: EAP-EVENT: Stopping 'Authenticator ReqId Retransmit'
timer for EAP session handle 0x26000052
*Sep 19 07:00:22.150: eap_authen : during state eap_auth_received, got
event 10(eapMethodData)
*Sep 19 07:00:22.150: @@@ eap_authen : eap_auth_received ->
eap_auth_method_response
*Sep 19 07:00:22.151: EAP-AUTH-EVENT: Received peer identity: tiago

```



```

*Sep 19 07:00:22.151: EAP-EVENT: Sending LL (Dot1x-Authenticator) event
'EAP_IDENTITY' on handle 0x26000052
*Sep 19 07:00:22.151: eap_authen : during state
eap_auth_method_response, got event 13(eapMethodEnd)
*Sep 19 07:00:22.151: @@@ eap_authen : eap_auth_method_response ->
eap_auth_select_action
*Sep 19 07:00:22.151: eap_authen : during state eap_auth_select_action,
got event 19(eapDecisionPass)
*Sep 19 07:00:22.151: @@@ eap_authen : eap_auth_select_action ->
eap_auth_passthru_init
*Sep 19 07:00:22.151: eap_authen : during state eap_auth_passthru_init,
got event 22(eapPthruIdentity)
*Sep 19 07:00:22.151: @@@ eap_authen : eap_auth_passthru_init ->
eap_auth_aaa_req
*Sep 19 07:00:22.151: EAP-EVENT: Sending LL (Dot1x-Authenticator) event
'EAP_GET_PEER_MAC_ADDRESS' on handle 0x26000052
*Sep 19 07:00:22.151: EAP-AUTH-AAA-EVENT: Adding Audit-Session-ID
"0ca82104523aa0a30000001f" to RADIUS Req
*Sep 19 07:00:22.151: EAP-AUTH-AAA-EVENT: Added Audit-Session-ID
*Sep 19 07:00:22.151: EAP-AUTH-AAA-EVENT: Adding IDB "0x38167B5C" to
RADIUS Req
*Sep 19 07:00:22.151: EAP-AUTH-AAA-EVENT: Added IDB
*Sep 19 07:00:22.151: EAP-AUTH-AAA-EVENT: Adding EAP profile name
"PEAPProfile" to RADIUS Req
*Sep 19 07:00:22.151: EAP-AUTH-AAA-EVENT: Added EAP profile name to request
*Sep 19 07:00:22.151: EAP-EVENT: Sending LL (Dot1x-Authenticator) event
'EAP_CUSTOMIZE AAA REQUEST' on handle 0x26000052
*Sep 19 07:00:22.151: EAP-AUTH-AAA-EVENT: eap_auth_aaa_authen_request_shim
aaa_service 19, eap aaa list handle 0, mlist handle 0
*Sep 19 07:00:22.151: EAP-AUTH-AAA-EVENT: Request sent successfully
*Sep 19 07:00:22.151: eap_authen : during state eap_auth_aaa_req, got
event 24(eapAAAReqOk)
*Sep 19 07:00:22.151: @@@ eap_authen : eap_auth_aaa_req ->
eap_auth_aaa_idle
*Sep 19 07:00:22.152: EAP-EVENT: Received context create from LL
(AAA_LOCAL EAP) (0x00000019)
*Sep 19 07:00:22.152: EAP-AUTH-EVENT: Setting authentication mode: Local
*Sep 19 07:00:22.152: EAP-EVENT: Using EAP profile "PEAPProfile"
(handle 0xCE000053)
*Sep 19 07:00:22.152: eap_authen : initial state eap_auth_initialize
has enter
*Sep 19 07:00:22.152: eap_authen : during state eap_auth_initialize,
got event 25(eapStartTmo)
*Sep 19 07:00:22.152: @@@ eap_authen : eap_auth_initialize ->
eap_auth_select_action
*Sep 19 07:00:22.152: eap_authen : during state eap_auth_select_action,
got event 20(eapDecisionPropose)
*Sep 19 07:00:22.152: @@@ eap_authen : eap_auth_select_action ->
eap_auth_propose_method
*Sep 19 07:00:22.152: eap_authen : idle during state
eap_auth_propose_method
*Sep 19 07:00:22.152: @@@ eap_authen : eap_auth_propose_method ->
eap_auth_method_request
*Sep 19 07:00:22.152: eap_authen : during state eap_auth_method_request,
got event 21(eapDecisionWait)
*Sep 19 07:00:22.152: @@@ eap_authen : eap_auth_method_request ->
eap_auth_idle
*Sep 19 07:00:22.152: EAP-EVENT: Allocated new EAP context
(handle = 0xCE000053)
*Sep 19 07:00:22.152: EAP-EVENT: Received LL (AAA_LOCAL EAP) event
'EAP_RX_PACKET' on handle 0xCE000053
*Sep 19 07:00:22.152: EAP-AUTH-RX-PAK: Code:RESPONSE ID:0xA Length:0x000A
Type:IDENTITY
*Sep 19 07:00:22.152: Payload: 746961676F
*Sep 19 07:00:22.152: eap_authen : during state eap_auth_idle, got event
1(eapRxPacket)
*Sep 19 07:00:22.152: @@@ eap_authen : eap_auth_idle -> eap_auth_received
*Sep 19 07:00:22.152: EAP-AUTH-EVENT: EAP Response received by context
0xCE000053
*Sep 19 07:00:22.152: EAP-AUTH-EVENT: EAP Response type = Identity
*Sep 19 07:00:22.152: eap_authen : during state eap_auth_received, got
event 10(eapMethodData)
*Sep 19 07:00:22.152: @@@ eap_authen : eap_auth_received ->

```

```

eap_auth method response
*Sep 19 07:00:22.152: EAP-AUTH-EVENT: Received peer identity: tiago
*Sep 19 07:00:22.153: eap_authen : during state eap_auth_method_response
got event 13(eapMethodEnd)
*Sep 19 07:00:22.153: @@@ eap_authen : eap_auth_method_response ->
eap_auth_select_action
*Sep 19 07:00:22.153: EAP-AUTH-EVENT: Using authentication mode: Local
*Sep 19 07:00:22.153: EAP-EVENT: Local methods by EAP type: [025 026]
*Sep 19 07:00:22.153: eap_authen : during state eap_auth_select_action,
got event 20(eapDecisionPropose)
*Sep 19 07:00:22.153: @@@ eap_authen : eap_auth_select_action ->
eap_auth_propose_method
*Sep 19 07:00:22.153: eap_authen : idle during state
eap_auth_propose_method
*Sep 19 07:00:22.153: @@@ eap_authen : eap_auth_propose_method ->
eap_auth_method_request
*Sep 19 07:00:22.153: EAP-AUTH-EVENT: Maximum EAP packet size: 1456
*Sep 19 07:00:22.153: EAP-EVENT: Sending method (PEAP) event 'New Context'
on handle 0xCE000053
*Sep 19 07:00:22.153: EAP-EVENT: Sending method (PEAP) event 'Receive Packet'
on handle 0xCE000053
*Sep 19 07:00:22.153: EAP-AUTH-EVENT: Waiting for asynchronous reply from
method (PEAP)
*Sep 19 07:00:22.153: eap_authen : during state eap_auth_method_request,
got event 15(eapMethodWaitReply)
*Sep 19 07:00:22.153: @@@ eap_authen : eap_auth_method_request ->
eap_auth_idle
*Sep 19 07:00:22.154: EAP-EVENT: Received Method (PEAP) event
'EAP_METHOD_REPLY' on handle 0xCE000053
*Sep 19 07:00:22.154: eap_authen : during state eap_auth_idle, got event
4(eapMethodReply)
*Sep 19 07:00:22.154: @@@ eap_authen : eap_auth_idle ->
eap_auth_method_response
*Sep 19 07:00:22.154: EAP-AUTH-EVENT: Handling asynchronous method response
for context 0xCE000053
*Sep 19 07:00:22.154: EAP-AUTH-EVENT: EAP method state: Continue
*Sep 19 07:00:22.154: EAP-AUTH-EVENT: EAP method decision: Unknown
*Sep 19 07:00:22.154: eap_authen : during state eap_auth_method_response,
got event 14(eapMethodContinue)
*Sep 19 07:00:22.154: @@@ eap_authen : eap_auth_method_response ->
eap_auth_method_request
*Sep 19 07:00:22.154: eap_authen : idle during state
eap_auth_method_request
*Sep 19 07:00:22.154: @@@ eap_authen : eap_auth_method_request ->
eap_auth_tx_packet
*Sep 19 07:00:22.154: EAP-AUTH-EVENT: Current method = 25
*Sep 19 07:00:22.154: eap_authen : idle during state eap_auth_tx_packet
*Sep 19 07:00:22.154: @@@ eap_authen : eap_auth_tx_packet -> eap_auth_idle
*Sep 19 07:00:22.154: EAP-AUTH-TX-PAK: Code:REQUEST ID:0xB Length:0x0006
Type:PEAP
*Sep 19 07:00:22.154: Payload: 21
*Sep 19 07:00:22.154: EAP-EVENT: Sending LL (AAA_LOCAL_EAP) event
'EAP_TX_PACKET' on handle 0xCE000053
*Sep 19 07:00:22.154: EAP-EVENT: eap_aaa_reply
*Sep 19 07:00:22.154: EAP-AUTH-AAA-EVENT: Reply received session_label
BB000020
*Sep 19 07:00:22.154: EAP-AUTH-AAA-EVENT: Response contains EAP Message,
code: 1
*Sep 19 07:00:22.155: EAP-EVENT: Received AAA event 'EAP_AAA_RX_PACKET' on
handle 0x26000052
*Sep 19 07:00:22.155: EAP-AUTH-RX-AAA-PAK: Code:REQUEST ID:0xB Length:0x0006
Type:PEAP
*Sep 19 07:00:22.155: Payload: 21
*Sep 19 07:00:22.155: eap_authen : during state eap_auth_aaa_idle, got
event 5(eapAAARxPacket)
*Sep 19 07:00:22.155: @@@ eap_authen : eap_auth_aaa_idle ->
eap_auth_aaa_resp
*Sep 19 07:00:22.155: eap_authen : idle during state eap_auth_aaa_resp
*Sep 19 07:00:22.155: @@@ eap_authen : eap_auth_aaa_resp ->
eap_auth_tx_packet2
*Sep 19 07:00:22.155: EAP-AUTH-EVENT: Current method = 25
*Sep 19 07:00:22.155: eap_authen : idle during state eap_auth_tx_packet2
*Sep 19 07:00:22.155: @@@ eap_authen : eap_auth_tx_packet2 -> eap_auth_idle2

```

```

*Sep 19 07:00:22.155: EAP-AUTH-TX-PAK: Code:REQUEST ID:0xB Length:0x0006
Type:PEAP
*Sep 19 07:00:22.155: Payload: 21
*Sep 19 07:00:22.155: EAP-EVENT: Started 'Authenticator Retransmit' timer
(30s) for EAP sesion handle 0x26000052
*Sep 19 07:00:22.155: EAP-EVENT: Started EAP tick timer
*Sep 19 07:00:22.155: EAP-EVENT: Sending LL (Dot1x-Authenticator) event
'EAP_TX_PACKET' on handle 0x26000052
*Sep 19 07:00:22.155: dot1x-sm:[6470.0227.0a89, Ca0] Posting EAP_REQ for
0x60000009
*Sep 19 07:00:22.155: dot1x_auth_bend Ca0: during state
auth_bend_response, got event 7(eapReq)
*Sep 19 07:00:22.155: @@@ dot1x_auth_bend Ca0: auth_bend_response ->
auth_bend_request
*Sep 19 07:00:22.155: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:exiting
response state
*Sep 19 07:00:22.155: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:entering
request state
*Sep 19 07:00:22.155: dot1x-ev:[6470.0227.0a89, Ca0] Sending EAPOL packet
*Sep 19 07:00:22.155: dot1x-packet:[6470.0227.0a89, Ca0] Platform changed
src mac of EAPOL packet
*Sep 19 07:00:22.155: dot1x-registry:registry:dot1x_ether_macaddr called
*Sep 19 07:00:22.155: dot1x-packet:EAPOL pak Tx - Ver: 0x3 type: 0x0
*Sep 19 07:00:22.155: dot1x-packet: length: 0x0006
*Sep 19 07:00:22.155: dot1x-packet:EAP code: 0x1 id: 0xB length: 0x0006
*Sep 19 07:00:22.155: dot1x-packet: type: 0x19
*Sep 19 07:00:22.156: dot1x-packet:[6470.0227.0a89, Ca0] EAPOL packet sent
to client 0x60000009
*Sep 19 07:00:22.156: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:response
request action
*Sep 19 07:00:22.395: dot1x-packet:[6470.0227.0a89, Ca0] Queuing an EAPOL
pkt on Authenticator Q
*Sep 19 07:00:22.395: dot1x-packet:EAPOL pak rx - Ver: 0x3 type: 0x0
*Sep 19 07:00:22.395: dot1x-packet: length: 0x0098
*Sep 19 07:00:22.395: dot1x-ev:[Ca0] Dequeued pkt: Int Ca0 CODE= 2,TYPE= 25,
LEN= 152

*Sep 19 07:00:22.396: dot1x-ev:[Ca0] Received pkt saddr =6470.0227.0a89 ,
daddr = 64d8.146f.e5a0, pae-ether-type = 888e.0300.0098
*Sep 19 07:00:22.396: dot1x-packet:EAPOL pak rx - Ver: 0x3 type: 0x0
*Sep 19 07:00:22.396: dot1x-packet: length: 0x0098
*Sep 19 07:00:22.396: dot1x-sm:[6470.0227.0a89, Ca0] Posting EAPOL_EAP for
0x60000009
*Sep 19 07:00:22.396: dot1x_auth_bend Ca0: during state
auth_bend_request, got event 6(eapOlEap)
*Sep 19 07:00:22.396: @@@ dot1x_auth_bend Ca0: auth_bend_request ->
auth_bend_response
*Sep 19 07:00:22.396: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:entering
response state
*Sep 19 07:00:22.396: dot1x-ev:[6470.0227.0a89, Ca0] Response sent to the
server from 0x60000009
*Sep 19 07:00:22.396: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:request
response action
*Sep 19 07:00:22.396: EAP-EVENT: Received LL (Dot1x-Authenticator) event
'EAP_RX_PACKET' on handle 0x26000052
*Sep 19 07:00:22.396: EAP-AUTH-RX-PAK: Code:RESPONSE ID:0xB Length:0x0098
Type:PEAP
*Sep 19 07:00:22.396: Payload: 810000008E1603010089010000850301 ...
*Sep 19 07:00:22.396: eap_authen : during state eap_auth_idle2, got
event 1(eapRxPacket)
*Sep 19 07:00:22.396: @@@ eap_authen : eap_auth_idle2 -> eap_auth_received2
*Sep 19 07:00:22.396: EAP-AUTH-EVENT: EAP Response received by context
0x26000052
*Sep 19 07:00:22.396: EAP-AUTH-EVENT: EAP Response type = Method (25)
*Sep 19 07:00:22.396: EAP-EVENT: Stopping 'Authenticator Retransmit' timer
for EAP sesion handle 0x26000052
*Sep 19 07:00:22.396: eap_authen : during state eap_auth_received2, got
event 10(eapMethodData)
*Sep 19 07:00:22.397: @@@ eap_authen : eap_auth_received2->eap_auth_aaa_req
*Sep 19 07:00:22.397: EAP-AUTH-AAA-EVENT: Adding Audit-Session-ID
"c0a82104523aa0a30000001f" to RADIUS Req
*Sep 19 07:00:22.397: EAP-AUTH-AAA-EVENT: Added Audit-Session-ID
*Sep 19 07:00:22.397: EAP-AUTH-AAA-EVENT: Adding IDB "0x38167B5C" to

```

```

RADIUS Req
*Sep 19 07:00:22.397: EAP-AUTH-AAA-EVENT: Added IDB
*Sep 19 07:00:22.397: EAP-AUTH-AAA-EVENT: Adding EAP profile name
"PEAPProfile" to RADIUS Req
*Sep 19 07:00:22.397: EAP-AUTH-AAA-EVENT: Added EAP profile name to request
*Sep 19 07:00:22.397: EAP-EVENT: Sending LL (Dot1x-Authenticator) event
'EAP_CUSTOMIZE AAA REQUEST' on handle 0x26000052
*Sep 19 07:00:22.397: EAP-AUTH-AAA-EVENT: eap_auth_aaa_authen_request_shim
aaa_service 19, eap_aaa_list handle 0, mlist_handle 0
*Sep 19 07:00:22.397: EAP-AUTH-AAA-EVENT: Request sent successfully
*Sep 19 07:00:22.397: eap_authen : during state eap_auth_aaa_req, got
event 24(eapAAAREqOk)
*Sep 19 07:00:22.397: @@@ eap_authen : eap_auth_aaa_req -> eap_auth_aaa_idle
*Sep 19 07:00:22.397: EAP-EVENT: Received LL (AAA_LOCAL_EAP) event
'EAP_RX_PACKET' on handle 0xCE000053
*Sep 19 07:00:22.398: EAP-AUTH-RX-PAK: Code:RESPONSE ID:0xB Length:0x0098
Type:PEAP
*Sep 19 07:00:22.398: Payload: 810000008E1603010089010000850301 ...
*Sep 19 07:00:22.398: eap_authen : during state eap_auth_idle, got event
1(eapRxPacket)
*Sep 19 07:00:22.398: @@@ eap_authen : eap_auth_idle -> eap_auth_received
*Sep 19 07:00:22.398: EAP-AUTH-EVENT: EAP Response received by context
0xCE000053
*Sep 19 07:00:22.398: EAP-AUTH-EVENT: EAP Response type = Method (25)
*Sep 19 07:00:22.398: eap_authen : during state eap_auth_received, got
event 10(eapMethodData)
*Sep 19 07:00:22.398: @@@ eap_authen : eap_auth_received ->
eap_auth_method_response
*Sep 19 07:00:22.398: EAP-EVENT: Sending method (PEAP) event 'Receive Packet'
on handle 0xCE000053
*Sep 19 07:00:22.398: EAP-AUTH-EVENT: Waiting for asynchronous reply from
method (PEAP)
*Sep 19 07:00:22.398: eap_authen : during state eap_auth_method_response,
got event 15(eapMethodWaitReply)
*Sep 19 07:00:22.398: @@@ eap_authen : eap_auth_method_response ->
eap_auth_idle
*Sep 19 07:00:22.399: EAP-EVENT: Received Method (PEAP) event
'EAP_METHOD_REPLY' on handle 0xCE000053
*Sep 19 07:00:22.399: eap_authen : during state eap_auth_idle, got event
4(eapMethodReply)
*Sep 19 07:00:22.399: @@@ eap_authen : eap_auth_idle ->
eap_auth_method_response
*Sep 19 07:00:22.399: EAP-AUTH-EVENT: Handling asynchronous method response
for context 0xCE000053
*Sep 19 07:00:22.399: EAP-AUTH-EVENT: EAP method state: Continue
*Sep 19 07:00:22.399: EAP-AUTH-EVENT: EAP method decision: Unknown
*Sep 19 07:00:22.399: eap_authen : during state eap_auth_method_response,
got event 14(eapMethodContinue)
*Sep 19 07:00:22.399: @@@ eap_authen : eap_auth_method_response ->
eap_auth_method_request
*Sep 19 07:00:22.399: eap_authen : idle during state
eap_auth_method_request
*Sep 19 07:00:22.399: @@@ eap_authen : eap_auth_method_request ->
eap_auth_tx_packet
*Sep 19 07:00:22.399: EAP-AUTH-EVENT: Current method = 25
*Sep 19 07:00:22.399: eap_authen : idle during state eap_auth_tx_packet
*Sep 19 07:00:22.399: @@@ eap_authen : eap_auth_tx_packet -> eap_auth_idle
*Sep 19 07:00:22.399: EAP-AUTH-TX-PAK: Code:REQUEST ID:0xC Length:0x02B1
Type:PEAP
*Sep 19 07:00:22.399: Payload: 81000002A7160301004A020000460301 ...
*Sep 19 07:00:22.399: EAP-EVENT: Sending LL (AAA_LOCAL_EAP) event
'EAP_TX_PACKET' on handle 0xCE000053
*Sep 19 07:00:22.399: EAP-EVENT: eap_aaa_reply
*Sep 19 07:00:22.400: EAP-AUTH-AAA-EVENT: Reply received session_label
BB000020
*Sep 19 07:00:22.400: EAP-AUTH-AAA-EVENT: Response contains EAP Message,
code: 1
*Sep 19 07:00:22.400: EAP-EVENT: Received AAA event 'EAP_AAA_RX_PACKET' on
handle 0x26000052
*Sep 19 07:00:22.400: EAP-AUTH-RX-AAA-PAK: Code:REQUEST ID:0xC Length:0x02B1
Type:PEAP
*Sep 19 07:00:22.400: Payload: 81000002A7160301004A020000460301 ...
*Sep 19 07:00:22.400: eap_authen : during state eap_auth_aaa_idle, got

```

```

event 5(eapAAARxPacket)
*Sep 19 07:00:22.400: @@@ eap_authen : eap_auth_aaa_idle ->
  eap_auth_aaa_resp
*Sep 19 07:00:22.400: eap_authen : idle during state eap_auth_aaa_resp
*Sep 19 07:00:22.400: @@@ eap_authen : eap_auth_aaa_resp ->
  eap_auth_tx_packet2
*Sep 19 07:00:22.400: EAP-AUTH-EVENT: Current method = 25
*Sep 19 07:00:22.400: eap_authen : idle during state eap_auth_tx_packet2
*Sep 19 07:00:22.400: @@@ eap_authen : eap_auth_tx_packet2 -> eap_auth_idle2
*Sep 19 07:00:22.400: EAP-AUTH-TX-PAK: Code:REQUEST ID:0xC Length:0x02B1
  Type:PEAP
*Sep 19 07:00:22.400: Payload: 81000002A7160301004A020000460301 ...
*Sep 19 07:00:22.400: EAP-EVENT: Started 'Authenticator Retransmit' timer
  (30s) for EAP sesion handle 0x26000052
*Sep 19 07:00:22.400: EAP-EVENT: Started EAP tick timer
*Sep 19 07:00:22.400: EAP-EVENT: Sending LL (Dot1x-Authenticator) event
  'EAP_TX_PACKET' on handle 0x26000052
*Sep 19 07:00:22.400: dot1x-sm:[6470.0227.0a89, Ca0] Posting EAP_REQ for
  0x60000009
*Sep 19 07:00:22.400: dot1x_auth_bend Ca0: during state
  auth_bend_response, got event 7(eapReq)
*Sep 19 07:00:22.400: @@@ dot1x_auth_bend Ca0: auth_bend_response ->
  auth_bend_request
*Sep 19 07:00:22.400: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:exiting
  response state
*Sep 19 07:00:22.400: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:entering
  request state
*Sep 19 07:00:22.400: dot1x-ev:[6470.0227.0a89, Ca0] Sending EAPOL packet
*Sep 19 07:00:22.401: dot1x-packet:[6470.0227.0a89, Ca0] Platform changed
  src mac of EAPOL packet
*Sep 19 07:00:22.401: dot1x-registry:registry:dot1x_ether_macaddr called
*Sep 19 07:00:22.401: dot1x-packet:EAPOL pak Tx - Ver: 0x3 type: 0x0
*Sep 19 07:00:22.401: dot1x-packet: length: 0x02B1
*Sep 19 07:00:22.401: dot1x-packet:EAP code: 0x1 id: 0xC length: 0x02B1
*Sep 19 07:00:22.401: dot1x-packet: type: 0x19
*Sep 19 07:00:22.401: dot1x-packet:[6470.0227.0a89, Ca0] EAPOL packet sent
  to client 0x60000009
*Sep 19 07:00:22.401: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:response
  request action
*Sep 19 07:00:22.646: dot1x-packet:[6470.0227.0a89, Ca0] Queuing an EAPOL
  pkt on Authenticator Q
*Sep 19 07:00:22.646: dot1x-packet:EAPOL pak rx - Ver: 0x3 type: 0x0
*Sep 19 07:00:22.646: dot1x-packet: length: 0x00C8
*Sep 19 07:00:22.646: dot1x-ev:[Ca0] Dequeued pkt: Int Ca0 CODE= 2,TYPE= 25,
  LEN= 200
*Sep 19 07:00:22.646: dot1x-ev:[Ca0] Received pkt saddr =6470.0227.0a89 ,
  daddr = 64d8.146f.e5a0, pae-ether-type = 888e.0300.00c8
*Sep 19 07:00:22.646: dot1x-packet:EAPOL pak rx - Ver: 0x3 type: 0x0
*Sep 19 07:00:22.646: dot1x-packet: length: 0x00C8
*Sep 19 07:00:22.647: dot1x-sm:[6470.0227.0a89, Ca0] Posting EAPOL_EAP for
  0x60000009
*Sep 19 07:00:22.647: dot1x_auth_bend Ca0: during state
  auth_bend_request, got event 6(eapolEap)
*Sep 19 07:00:22.647: @@@ dot1x_auth_bend Ca0: auth_bend_request ->
  auth_bend_response
*Sep 19 07:00:22.647: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:entering
  response state
*Sep 19 07:00:22.647: dot1x-ev:[6470.0227.0a89, Ca0] Response sent to the
  server from 0x60000009
*Sep 19 07:00:22.647: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:request
  response action
*Sep 19 07:00:22.647: EAP-EVENT: Received LL (Dot1x-Authenticator) event
  'EAP_RX_PACKET' on handle 0x26000052
*Sep 19 07:00:22.647: EAP-AUTH-RX-PAK: Code:RESPONSE ID:0xC Length:0x00C8
  Type:PEAP
*Sep 19 07:00:22.647: Payload: 81000000BE1603010086100000820080 ...
*Sep 19 07:00:22.647: eap_authen : during state eap_auth_idle2, got
  event 1(eapRxPacket)
*Sep 19 07:00:22.647: @@@ eap_authen : eap_auth_idle2 -> eap_auth_received2
*Sep 19 07:00:22.647: EAP-AUTH-EVENT: EAP Response received by context
  0x26000052
*Sep 19 07:00:22.647: EAP-AUTH-EVENT: EAP Response type = Method (25)

```

```

*Sep 19 07:00:22.647: EAP-EVENT: Stopping 'Authenticator Retransmit' timer
for EAP sesion handle 0x26000052
*Sep 19 07:00:22.647: eap_authen : during state eap_auth_received2, got
event 10(eapMethodData)
*Sep 19 07:00:22.647: @@@ eap_authen : eap_auth_received2 ->
eap_auth_aaa_req
*Sep 19 07:00:22.647: EAP-AUTH-AAA-EVENT: Adding Audit-Session-ID
"c0a82104523aa0a30000001f" to RADIUS Req
*Sep 19 07:00:22.647: EAP-AUTH-AAA-EVENT: Added Audit-Session-ID
*Sep 19 07:00:22.647: EAP-AUTH-AAA-EVENT: Adding IDB "0x38167B5C" to
RADIUS Req
*Sep 19 07:00:22.647: EAP-AUTH-AAA-EVENT: Added IDB
*Sep 19 07:00:22.648:
EAP-AUTH-AAA-EVENT: Adding EAP profile name "PEAPProfile" to RADIUS Req
*Sep 19 07:00:22.648: EAP-AUTH-AAA-EVENT: Added EAP profile name to request
*Sep 19 07:00:22.648: EAP-EVENT: Sending LL (Dot1x-Authenticator) event
'EAP_CUSTOMIZE AAA REQUEST' on handle 0x26000052
*Sep 19 07:00:22.648: EAP-AUTH-AAA-EVENT: eap_auth_aaa_authen_request_shim
aaa_service 19, eap aaa_list handle 0, mlist_handle 0
*Sep 19 07:00:22.648: EAP-AUTH-AAA-EVENT: Request sent successfully
*Sep 19 07:00:22.648: eap_authen : during state eap_auth_aaa_req, got
event 24(eapAAAReqOk)
*Sep 19 07:00:22.648: @@@ eap_authen : eap_auth_aaa_req -> eap_auth_aaa_idle
*Sep 19 07:00:22.648: EAP-EVENT: Received LL (AAA_LOCAL_EAP) event
'EAP_RX_PACKET' on handle 0xCE000053
*Sep 19 07:00:22.648: EAP-AUTH-RX-PAK: Code:RESPONSE ID:0xC Length:0x00C8
Type:PEAP
*Sep 19 07:00:22.648: Payload: 81000000BE1603010086100000820080 ...
*Sep 19 07:00:22.648: eap_authen : during state eap_auth_idle, got event
1(eapRxPacket)
*Sep 19 07:00:22.648: @@@ eap_authen : eap_auth_idle -> eap_auth_received
*Sep 19 07:00:22.648: EAP-AUTH-EVENT: EAP Response received by context
0xCE000053
*Sep 19 07:00:22.648: EAP-AUTH-EVENT: EAP Response type = Method (25)
*Sep 19 07:00:22.649: eap_authen : during state eap_auth_received, got
event 10(eapMethodData)
*Sep 19 07:00:22.649: @@@ eap_authen : eap_auth_received ->
eap_auth_method_response
*Sep 19 07:00:22.649: EAP-EVENT: Sending method (PEAP) event 'Receive Packet'
on handle 0xCE000053
*Sep 19 07:00:22.649: EAP-AUTH-EVENT: Waiting for asynchronous reply from
method (PEAP)
*Sep 19 07:00:22.649: eap_authen : during state eap_auth_method_response,
got event 15(eapMethodWaitReply)
*Sep 19 07:00:22.649: @@@ eap_authen : eap_auth_method_response ->
eap_auth_idle
*Sep 19 07:00:22.675: EAP-EVENT: Received Method (PEAP) event
'EAP_METHOD_REPLY' on handle 0xCE000053
*Sep 19 07:00:22.675: eap_authen : during state eap_auth_idle, got
event 4(eapMethodReply)
*Sep 19 07:00:22.675: @@@ eap_authen : eap_auth_idle ->
eap_auth_method_response
*Sep 19 07:00:22.675: EAP-AUTH-EVENT: Handling asynchronous method response
for context 0xCE000053
*Sep 19 07:00:22.675: EAP-AUTH-EVENT: EAP method state: Continue
*Sep 19 07:00:22.675: EAP-AUTH-EVENT: EAP method decision: Unknown
*Sep 19 07:00:22.675: eap_authen : during state eap_auth_method_response,
got event 14(eapMethodContinue)
*Sep 19 07:00:22.675: @@@ eap_authen : eap_auth_method_response ->
eap_auth_method_request
*Sep 19 07:00:22.675: eap_authen : idle during state
eap_auth_method_request
*Sep 19 07:00:22.675: @@@ eap_authen : eap_auth_method_request ->
eap_auth_tx_packet
*Sep 19 07:00:22.675: EAP-AUTH-EVENT: Current method = 25
*Sep 19 07:00:22.675: eap_authen : idle during state eap_auth_tx_packet
*Sep 19 07:00:22.675: @@@ eap_authen : eap_auth_tx_packet -> eap_auth_idle
*Sep 19 07:00:22.675: EAP-AUTH-TX-PAK: Code:REQUEST ID:0xD Length:0x003D
Type:PEAP
*Sep 19 07:00:22.676: Payload: 81000000331403010001011603010028 ...
*Sep 19 07:00:22.676: EAP-EVENT: Sending LL (AAA_LOCAL_EAP) event
'EAP_TX_PACKET' on handle 0xCE000053
*Sep 19 07:00:22.676: EAP-EVENT: eap_aaa_reply

```

```

*Sep 19 07:00:22.676: EAP-AUTH-AAA-EVENT: Reply received session_label
BB000020
*Sep 19 07:00:22.676: EAP-AUTH-AAA-EVENT: Response contains EAP Message,
code: 1
*Sep 19 07:00:22.676: EAP-EVENT: Received AAA event 'EAP_AAA_RX_PACKET' on
handle 0x26000052
*Sep 19 07:00:22.676: EAP-AUTH-RX-AAA-PAK: Code:REQUEST ID:0xD Length:0x003D
Type:PEAP
*Sep 19 07:00:22.676: Payload: 81000000331403010001011603010028 ...
*Sep 19 07:00:22.676: eap_authen : during state eap_auth_aaa_idle, got
event 5(eapAAARxPacket)
*Sep 19 07:00:22.676: @@@ eap_authen : eap_auth_aaa_idle ->
eap_auth_aaa_resp
*Sep 19 07:00:22.676: eap_authen : idle during state eap_auth_aaa_resp
*Sep 19 07:00:22.676: @@@ eap_authen : eap_auth_aaa_resp ->
eap_auth_tx_packet2
*Sep 19 07:00:22.676: EAP-AUTH-EVENT: Current method = 25
*Sep 19 07:00:22.676: eap_authen : idle during state eap_auth_tx_packet2
*Sep 19 07:00:22.676: @@@ eap_authen : eap_auth_tx_packet2 -> eap_auth_idle2
*Sep 19 07:00:22.676: EAP-AUTH-TX-PAK: Code:REQUEST ID:0xD Length:0x003D
Type:PEAP
*Sep 19 07:00:22.676: Payload: 81000000331403010001011603010028 ...
*Sep 19 07:00:22.676: EAP-EVENT: Started 'Authenticator Retransmit' timer
(30s) for EAP sesion handle 0x26000052
*Sep 19 07:00:22.676: EAP-EVENT: Started EAP tick timer
*Sep 19 07:00:22.676: EAP-EVENT: Sending LL (Dot1x-Authenticator) event
'EAP_TX_PACKET' on handle 0x26000052
*Sep 19 07:00:22.677: dot1x-sm:[6470.0227.0a89, Ca0] Posting EAP_REQ for
0x60000009
*Sep 19 07:00:22.677: dot1x_auth_bend Ca0: during state
auth_bend_response, got event 7(eapReq)
*Sep 19 07:00:22.677: @@@ dot1x_auth_bend Ca0: auth_bend_response ->
auth_bend_request
*Sep 19 07:00:22.677: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:exiting
response state
*Sep 19 07:00:22.677: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:entering
request state
*Sep 19 07:00:22.677: dot1x-ev:[6470.0227.0a89, Ca0] Sending EAPOL packet
*Sep 19 07:00:22.677: dot1x-packet:[6470.0227.0a89, Ca0] Platform changed src
mac of EAPOL packet
*Sep 19 07:00:22.677: dot1x-registry:registry:dot1x_ether_macaddr called
*Sep 19 07:00:22.677: dot1x-packet:EAPOL pak Tx - Ver: 0x3 type: 0x0
*Sep 19 07:00:22.677: dot1x-packet: length: 0x003D
*Sep 19 07:00:22.677: dot1x-packet:EAP code: 0x1 id: 0xD length: 0x003D
*Sep 19 07:00:22.677: dot1x-packet: type: 0x19
*Sep 19 07:00:22.677: dot1x-packet:[6470.0227.0a89, Ca0] EAPOL packet sent to
client 0x60000009
*Sep 19 07:00:22.677: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:response
request action
*Sep 19 07:00:22.902: dot1x-packet:[6470.0227.0a89, Ca0] Queuing an EAPOL
pkt on Authenticator Q
*Sep 19 07:00:22.903: dot1x-packet:EAPOL pak rx - Ver: 0x3 type: 0x0
*Sep 19 07:00:22.903: dot1x-packet: length: 0x0006
*Sep 19 07:00:22.903: dot1x-ev:[Ca0] Dequeued pkt: Int Ca0 CODE= 2,TYPE= 25,
LEN= 6
*Sep 19 07:00:22.903: dot1x-ev:[Ca0] Received pkt saddr =6470.0227.0a89 ,
daddr = 64d8.146f.e5a0, pae-ether-type = 888e.0300.0006
*Sep 19 07:00:22.903: dot1x-packet:EAPOL pak rx - Ver: 0x3 type: 0x0
*Sep 19 07:00:22.903: dot1x-packet: length: 0x0006
*Sep 19 07:00:22.903: dot1x-sm:[6470.0227.0a89, Ca0] Posting EAPOL_EAP for
0x60000009
*Sep 19 07:00:22.903: dot1x_auth_bend Ca0: during state
auth_bend_request, got event 6(eapolEap)
*Sep 19 07:00:22.903: @@@ dot1x_auth_bend Ca0: auth_bend_request ->
auth_bend_response
*Sep 19 07:00:22.903: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:entering
response state
*Sep 19 07:00:22.903: dot1x-ev:[6470.0227.0a89, Ca0] Response sent to the
server from 0x60000009
*Sep 19 07:00:22.903: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:request
response action
*Sep 19 07:00:22.904: EAP-EVENT: Received LL (Dot1x-Authenticator) event

```

```

'EAP_RX_PACKET' on handle 0x26000052
*Sep 19 07:00:22.904: EAP-AUTH-RX-PAK: Code:RESPONSE ID:0xD Length:0x0006
Type:PEAP
*Sep 19 07:00:22.904: Payload: 01
*Sep 19 07:00:22.904: eap_authen : during state eap_auth_idle2, got event
1(eapRxPacket)
*Sep 19 07:00:22.904: @@@ eap_authen : eap_auth_idle2 -> eap_auth_received2
*Sep 19 07:00:22.904: EAP-AUTH-EVENT: EAP Response received by context
0x26000052
*Sep 19 07:00:22.904: EAP-AUTH-EVENT: EAP Response type = Method (25)
*Sep 19 07:00:22.904: EAP-EVENT: Stopping 'Authenticator Retransmit' timer
for EAP session handle 0x26000052
*Sep 19 07:00:22.904: eap_authen : during state eap_auth_received2, got
event 10(eapMethodData)
*Sep 19 07:00:22.904: @@@ eap_authen : eap_auth_received2 -> eap_auth_aaa_req
*Sep 19 07:00:22.904: EAP-AUTH-AAA-EVENT: Adding Audit-Session-ID
"c0a82104523aa0a30000001f" to RADIUS Req
*Sep 19 07:00:22.904: EAP-AUTH-AAA-EVENT: Added Audit-Session-ID
*Sep 19 07:00:22.904: EAP-AUTH-AAA-EVENT: Adding IDB "0x38167B5C" to
RADIUS Req
*Sep 19 07:00:22.904: EAP-AUTH-AAA-EVENT: Added IDB
*Sep 19 07:00:22.904: EAP-AUTH-AAA-EVENT: Adding EAP profile name
"PEAPProfile" to RADIUS Req
*Sep 19 07:00:22.904: EAP-AUTH-AAA-EVENT: Added EAP profile name to request
*Sep 19 07:00:22.904: EAP-EVENT: Sending LL (Dot1x-Authenticator) event
'EAP_CUSTOMIZE_AAA_REQUEST' on handle 0x26000052
*Sep 19 07:00:22.904: EAP-AUTH-AAA-EVENT: eap_auth_aaa_authen_request_shim
aaa_service 19, eap_aaa_list handle 0, mlist_handle 0
*Sep 19 07:00:22.905: EAP-AUTH-AAA-EVENT: Request sent successfully
*Sep 19 07:00:22.905: eap_authen : during state eap_auth_aaa_req, got
event 24(eapAAReqOk)
*Sep 19 07:00:22.905: @@@ eap_authen : eap_auth_aaa_req -> eap_auth_aaa_idle
*Sep 19 07:00:22.905: EAP-EVENT: Received LL (AAA_LOCAL_EAP) event
'EAP_RX_PACKET' on handle 0xCE000053
*Sep 19 07:00:22.905: EAP-AUTH-RX-PAK: Code:RESPONSE ID:0xD Length:0x0006
Type:PEAP
*Sep 19 07:00:22.905: Payload: 01
*Sep 19 07:00:22.905: eap_authen : during state eap_auth_idle, got event
1(eapRxPacket)
*Sep 19 07:00:22.905: @@@ eap_authen : eap_auth_idle -> eap_auth_received
*Sep 19 07:00:22.905: EAP-AUTH-EVENT: EAP Response received by context
0xCE000053
*Sep 19 07:00:22.905: EAP-AUTH-EVENT: EAP Response type = Method (25)
*Sep 19 07:00:22.905: eap_authen : during state eap_auth_received, got
event 10(eapMethodData)
*Sep 19 07:00:22.905: @@@ eap_authen : eap_auth_received ->
eap_auth_method_response
*Sep 19 07:00:22.905: EAP-EVENT: Sending method (PEAP) event 'Receive Packet'
on handle 0xCE000053
*Sep 19 07:00:22.905: EAP-EVENT: Received context create from LL (PEAP)
(0x69000006)
*Sep 19 07:00:22.905: EAP-AUTH-EVENT: Setting authentication mode: Local
*Sep 19 07:00:22.905: EAP-EVENT: Using EAP profile "PEAP Inner Method EAP
Profile" (handle 0x99000054)
*Sep 19 07:00:22.905: eap_authen : initial state eap_auth_initialize has
enter
*Sep 19 07:00:22.905: EAP-EVENT: Allocated new EAP context
(handle = 0x99000054)
*Sep 19 07:00:22.906: EAP-AUTH-EVENT: Waiting for asynchronous reply from
method (PEAP)
*Sep 19 07:00:22.906: eap_authen : during state eap_auth_method_response,
got event 15(eapMethodWaitReply)
*Sep 19 07:00:22.906: @@@ eap_authen : eap_auth_method_response ->
eap_auth_idle
*Sep 19 07:00:22.906: EAP-EVENT: Received EAP event 'EAP_AUTHENTICATOR_START'
on handle 0x99000054
*Sep 19 07:00:22.906: eap_authen : during state eap_auth_initialize, got
event 25(eapStartTmo)
*Sep 19 07:00:22.906: @@@ eap_authen : eap_auth_initialize ->
eap_auth_select_action
*Sep 19 07:00:22.906: eap_authen : during state eap_auth_select_action,
got event 20(eapDecisionPropose)
*Sep 19 07:00:22.906: @@@ eap_authen : eap_auth_select_action ->

```



```

eap_auth_propose_method
*Sep 19 07:00:22.906: eap_authen : idle during state
eap_auth_propose_method
*Sep 19 07:00:22.906: @@@ eap_authen : eap_auth_propose_method ->
eap_auth_method_request
*Sep 19 07:00:22.908: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:response
request action
*Sep 19 07:00:23.148: dot1x-packet:[6470.0227.0a89, Ca0] Queuing an EAPOL pkt
on Authenticator Q
*Sep 19 07:00:23.148: dot1x-packet:EAPOL pak rx - Ver: 0x3 type: 0x0
*Sep 19 07:00:23.148: dot1x-packet: length: 0x0048
*Sep 19 07:00:23.148: dot1x-ev:[Ca0] Dequeued pkt: Int Ca0 CODE= 2,TYPE= 25,
LEN= 72
*Sep 19 07:00:23.148: dot1x-ev:[Ca0] Received pkt saddr =6470.0227.0a89 ,
daddr = 64d8.146f.e5a0, pae-ether-type = 888e.0300.0048
*Sep 19 07:00:23.148: dot1x-packet:EAPOL pak rx - Ver: 0x3 type: 0x0
*Sep 19 07:00:23.148: dot1x-packet: length: 0x0048
*Sep 19 07:00:23.148: dot1x-sm:[6470.0227.0a89, Ca0] Posting EAPOL_EAP for
0x60000009
*Sep 19 07:00:23.148: dot1x_auth_bend Ca0: during state
auth_bend_request, got event 6(eapolEap)
*Sep 19 07:00:23.148: @@@ dot1x_auth_bend Ca0: auth_bend_request ->
auth_bend_response
*Sep 19 07:00:23.148: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:entering
response state
*Sep 19 07:00:23.148: dot1x-ev:[6470.0227.0a89, Ca0] Response sent to the
server from 0x60000009
*Sep 19 07:00:23.148: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:request
response action
*Sep 19 07:00:23.149: EAP-EVENT: Received LL (Dot1x-Authenticator) event
'EAP_RX_PACKET' on handle 0x26000052
*Sep 19 07:00:23.149: EAP-AUTH-RX-PAK: Code:RESPONSE ID:0xE Length:0x0048
Type:PEAP
*Sep 19 07:00:23.149: Payload: 011703010018E5BC67F95BDE2D2BF45C ...
*Sep 19 07:00:23.149: eap_authen : during state eap_auth_idle2, got event
1(eapRxPacket)
*Sep 19 07:00:23.149: @@@ eap_authen : eap_auth_idle2 -> eap_auth_received2
*Sep 19 07:00:23.149: EAP-AUTH-EVENT: EAP Response received by context
0x26000052
*Sep 19 07:00:23.149: EAP-AUTH-EVENT: EAP Response type = Method (25)
*Sep 19 07:00:23.149: EAP-EVENT: Stopping 'Authenticator Retransmit' timer
for EAP sesion handle 0x26000052
*Sep 19 07:00:23.149: eap_authen : during state eap_auth_received2, got
event 10(eapMethodData)
*Sep 19 07:00:23.149: @@@ eap_authen : eap_auth_received2 -> eap_auth_aaa_req
*Sep 19 07:00:23.149: EAP-AUTH-AAA-EVENT: Adding Audit-Session-ID
"c0a82104523aa0a30000001f" to RADIUS Req
*Sep 19 07:00:23.149: EAP-AUTH-AAA-EVENT: Added Audit-Session-ID
*Sep 19 07:00:23.149: EAP-AUTH-AAA-EVENT: Adding IDB "0x38167B5C" to RADIUS
Req
*Sep 19 07:00:23.149: EAP-AUTH-AAA-EVENT: Added IDB
*Sep 19 07:00:23.149: EAP-AUTH-AAA-EVENT: Adding EAP profile name
"PEAPPprofile" to RADIUS Req
*Sep 19 07:00:23.149: EAP-AUTH-AAA-EVENT: Added EAP profile name to request
*Sep 19 07:00:23.149: EAP-EVENT: Sending LL (Dot1x-Authenticator) event
'EAP_CUSTOMIZE_AAA_REQUEST' on handle 0x26000052
*Sep 19 07:00:23.149: EAP-AUTH-AAA-EVENT: eap_auth_aaa_authen_request_shim
aaa_service 19, eap aaa_list handle 0, mlist handle 0
*Sep 19 07:00:23.150: EAP-AUTH-AAA-EVENT: Request sent successfully
*Sep 19 07:00:23.150: eap_authen : during state eap_auth_aaa_req, got
event 24(eapAAAReqOk)
*Sep 19 07:00:23.150: @@@ eap_authen : eap_auth_aaa_req -> eap_auth_aaa_idle
*Sep 19 07:00:23.150: EAP-EVENT: Received LL (AAA_LOCAL_EAP) event
'EAP_RX_PACKET' on handle 0xCE000053
*Sep 19 07:00:23.150: EAP-AUTH-RX-PAK: Code:RESPONSE ID:0xE Length:0x0048
Type:PEAP
*Sep 19 07:00:23.150: Payload: 011703010018E5BC67F95BDE2D2BF45C ...
*Sep 19 07:00:23.150: eap_authen : during state eap_auth_idle, got event
1(eapRxPacket)
*Sep 19 07:00:23.150: @@@ eap_authen : eap_auth_idle -> eap_auth_received
*Sep 19 07:00:23.150: EAP-AUTH-EVENT: EAP Response received by context
0xCE000053

```

```

*Sep 19 07:00:23.150: EAP-AUTH-EVENT: EAP Response type = Method (25)
*Sep 19 07:00:23.150: eap_authen : during state eap_auth_received, got
event 10(eapMethodData)
*Sep 19 07:00:23.150: @@@ eap_authen : eap_auth_received ->
eap_auth_method_response
*Sep 19 07:00:23.150: EAP-EVENT: Sending method (PEAP) event 'Receive Packet'
on handle 0xCE000053
*Sep 19 07:00:23.150: EAP-AUTH-EVENT: Waiting for asynchronous reply from
method (PEAP)
*Sep 19 07:00:23.150: eap_authen : during state eap_auth_method_response,
got event 15(eapMethodWaitReply)
*Sep 19 07:00:23.150: @@@ eap_authen : eap_auth_method_response ->
eap_auth_idle
*Sep 19 07:00:23.151: EAP-EVENT: Received LL (PEAP) event 'EAP_RX_PACKET' on
handle 0x99000054
*Sep 19 07:00:23.151: EAP-AUTH-RX-PAK: Code:RESPONSE ID:0xE Length:0x000A
Type:IDENTITY
*Sep 19 07:00:23.151: Payload: 746961676F
*Sep 19 07:00:23.151: eap_authen : during state eap_auth_idle, got event
1(eapRxPacket)
*Sep 19 07:00:23.151: @@@ eap_authen : eap_auth_idle -> eap_auth_received
*Sep 19 07:00:23.151: EAP-AUTH-EVENT: EAP Response received by context
0x99000054
*Sep 19 07:00:23.151: EAP-AUTH-EVENT: EAP Response type = Identity
*Sep 19 07:00:23.151: eap_authen : during state eap_auth_received, got
event 10(eapMethodData)
*Sep 19 07:00:23.151: @@@ eap_authen : eap_auth_received ->
eap_auth_method_response
*Sep 19 07:00:23.151: EAP-AUTH-EVENT: Received peer identity: tiago
*Sep 19 07:00:23.151: eap_authen : during state eap_auth_method_response,
got event 13(eapMethodEnd)
*Sep 19 07:00:23.151: @@@ eap_authen : eap_auth_method_response ->
eap_auth_select_action
*Sep 19 07:00:23.151: EAP-AUTH-EVENT: Using authentication mode: Local
*Sep 19 07:00:23.151: EAP-EVENT: Sending LL (PEAP) event
'EAP_GET_CREDENTIAL_PROFILE_FROM_USERNAME' on handle 0x99000054
*Sep 19 07:00:23.151: EAP-EVENT: Sending LL (AAA_LOCAL_EAP) event
'EAP_GET_CREDENTIAL_PROFILE_FROM_USERNAME' on handle 0xCE000053
*Sep 19 07:00:23.151: EAP-AUTH-EVENT: Waiting for asynchronous reply from LL
(AAA_LOCAL_EAP)
*Sep 19 07:00:23.151: EAP-AUTH-EVENT: Waiting for asynchronous reply from LL
(PEAP)
*Sep 19 07:00:23.152: EAP-EVENT: Local methods by EAP type: [006 026]
*Sep 19 07:00:23.152: eap_authen : during state eap_auth_select_action,
got event 21(eapDecisionWait)
*Sep 19 07:00:23.152: @@@ eap_authen : eap_auth_select_action ->
eap_auth_idle
*Sep 19 07:00:23.152: EAP-EVENT: Received LL (AAA_LOCAL_EAP) event
'EAP_LL_REPLY' on handle 0xCE000053
*Sep 19 07:00:23.152: EAP-AUTH-EVENT: Relaying LL response for context
0xCE000053
*Sep 19 07:00:23.152: EAP-AUTH-EVENT: Using credential profile name: tiago
(0xCE000053)
*Sep 19 07:00:23.152: EAP-EVENT: Sending method (PEAP) event 'LL Response'
on handle 0xCE000053
*Sep 19 07:00:23.152: EAP-EVENT: Received LL (PEAP) event 'EAP_LL_REPLY' on
handle 0x99000054
*Sep 19 07:00:23.152: eap_authen : during state eap_auth_idle, got event
2(eapLLReply)
*Sep 19 07:00:23.152: @@@ eap_authen : eap_auth_idle ->
eap_auth_select_action
*Sep 19 07:00:23.152: EAP-AUTH-EVENT: Using credential profile name: tiago
(0x99000054)
*Sep 19 07:00:23.152: eap_authen : during state eap_auth_select_action,
got event 20(eapDecisionPropose)
*Sep 19 07:00:23.152: @@@ eap_authen : eap_auth_select_action ->
eap_auth_propose_method
*Sep 19 07:00:23.152: eap_authen : idle during state
eap_auth_propose_method
*Sep 19 07:00:23.152: @@@ eap_authen : eap_auth_propose_method ->
eap_auth_method_request
*Sep 19 07:00:23.152: EAP-AUTH-EVENT: Maximum EAP packet size: 1464
*Sep 19 07:00:23.152: EAP-EVENT: Sending method (GTC) event 'New Context' on

```

```

handle 0x99000054
*Sep 19 07:00:23.153: EAP-EVENT: Sending method (GTC) event 'Receive Packet'
on handle 0x99000054
*Sep 19 07:00:23.153: EAP-AUTH-EVENT: Method (GTC) state: Continue
*Sep 19 07:00:23.153: EAP-AUTH-EVENT: Method (GTC) decision: Unknown
*Sep 19 07:00:23.153:     eap_authen : idle during state
eap_auth_method_request
*Sep 19 07:00:23.153: @@@ eap_authen : eap_auth_method_request ->
eap_auth_tx_packet
*Sep 19 07:00:23.153: EAP-AUTH-EVENT: Current method = 6
*Sep 19 07:00:23.153:     eap_authen : idle during state
eap_auth_tx_packet
*Sep 19 07:00:23.153: @@@ eap_authen : eap_auth_tx_packet -> eap_auth_idle
*Sep 19 07:00:23.153: EAP-AUTH-TX-PAK: Code:REQUEST ID:0xF Length:0x0005
Type:GTC
*Sep 19 07:00:23.153: EAP-EVENT: Sending LL (PEAP) event 'EAP_TX_PACKET' on
handle 0x99000054
*Sep 19 07:00:23.153: EAP-EVENT: Received Method (PEAP) event
'EAP_METHOD_REPLY' on handle 0xCE000053
*Sep 19 07:00:23.153:     eap_authen : during state eap_auth_idle, got event
4(eapMethodReply)
*Sep 19 07:00:23.153: @@@ eap_authen : eap_auth_idle ->
eap_auth_method_response
*Sep 19 07:00:23.153: EAP-AUTH-EVENT: Handling asynchronous method response
for context 0xCE000053
*Sep 19 07:00:23.153: EAP-AUTH-EVENT: EAP method state: Continue
*Sep 19 07:00:23.153: EAP-AUTH-EVENT: EAP method decision: Unknown
*Sep 19 07:00:23.153:     eap_authen : during state eap_auth_method_response,
got event 14(eapMethodContinue)
*Sep 19 07:00:23.153: @@@ eap_authen : eap_auth_method_response ->
eap_auth_method_request
*Sep 19 07:00:23.153:     eap_authen : idle during state
eap_auth_method_request
*Sep 19 07:00:23.153: @@@ eap_authen : eap_auth_method_request ->
eap_auth_tx_packet
*Sep 19 07:00:23.153: EAP-AUTH-EVENT: Current method = 25
*Sep 19 07:00:23.153:     eap_authen : idle during state eap_auth_tx_packet
*Sep 19 07:00:23.153: @@@ eap_authen : eap_auth_tx_packet -> eap_auth_idle
*Sep 19 07:00:23.153: EAP-AUTH-TX-PAK: Code:REQUEST ID:0xF Length:0x002B
Type:PEAP
*Sep 19 07:00:23.153:     Payload: 011703010020377AEA34B95C78A82976 ...
*Sep 19 07:00:23.153: EAP-EVENT: Sending LL (AAA_LOCAL_EAP) event
'EAP_TX_PACKET' on handle 0xCE000053
*Sep 19 07:00:23.154: EAP-EVENT: eap_aaa_reply
*Sep 19 07:00:23.154: EAP-AUTH-AAA-EVENT: Reply received session_label
BB000020
*Sep 19 07:00:23.154: EAP-AUTH-AAA-EVENT: Response contains EAP Message,
code: 1
*Sep 19 07:00:23.154: EAP-EVENT: Received AAA event 'EAP_AAA_RX_PACKET' on
handle 0x26000052
*Sep 19 07:00:23.154: EAP-AUTH-RX-AAA-PAK: Code:REQUEST ID:0xF Length:0x002B
Type:PEAP
*Sep 19 07:00:23.154:     Payload: 011703010020377AEA34B95C78A82976 ...
*Sep 19 07:00:23.154:     eap_authen : during state eap_auth_aaa_idle, got
event 5(eapAAARxPacket)
*Sep 19 07:00:23.154: @@@ eap_authen : eap_auth_aaa_idle -> eap_auth_aaa_resp
*Sep 19 07:00:23.154:     eap_authen : idle during state eap_auth_aaa_resp
*Sep 19 07:00:23.154: @@@ eap_authen : eap_auth_aaa_resp ->
eap_auth_tx_packet2
*Sep 19 07:00:23.154: EAP-AUTH-EVENT: Current method = 25
*Sep 19 07:00:23.154:     eap_authen : idle during state eap_auth_tx_packet2
*Sep 19 07:00:23.154: @@@ eap_authen : eap_auth_tx_packet2 -> eap_auth_idle2
*Sep 19 07:00:23.154: EAP-AUTH-TX-PAK: Code:REQUEST ID:0xF Length:0x002B
Type:PEAP
*Sep 19 07:00:23.154:     Payload: 011703010020377AEA34B95C78A82976 ...
*Sep 19 07:00:23.154: EAP-EVENT: Started 'Authenticator Retransmit' timer
(30s) for EAP sesion handle 0x26000052
*Sep 19 07:00:23.154: EAP-EVENT: Started EAP tick timer
*Sep 19 07:00:23.154: EAP-EVENT: Sending LL (Dot1x-Authenticator) event
'EAP_TX_PACKET' on handle 0x26000052
*Sep 19 07:00:23.154: dot1x-sm:[6470.0227.0a89, Ca0] Posting EAP_REQ for
0x60000009
*Sep 19 07:00:23.154: dot1x_auth_bend Ca0: during state auth_bend_response,

```

```

got event 7(eapReq)
*Sep 19 07:00:23.154: @@@ dot1x_auth_bend Ca0: auth_bend_response ->
auth_bend_request
*Sep 19 07:00:23.154: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:exiting
response state
*Sep 19 07:00:23.871: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:response
request action
*Sep 19 07:00:24.114: dot1x-packet:[6470.0227.0a89, Ca0] Queuing an EAPOL pkt
on Authenticator Q
*Sep 19 07:00:24.115: dot1x-packet:EAPOL pak rx - Ver: 0x3 type: 0x0
*Sep 19 07:00:24.114: dot1x-packet: length: 0x0048
*Sep 19 07:00:24.114: dot1x-ev:[Ca0] Dequeued pkt: Int Ca0 CODE= 2,TYPE= 25,
LEN= 72

*Sep 19 07:00:24.114: dot1x-ev:[Ca0] Received pkt saddr =6470.0227.0a89 ,
daddr = 64d8.146f.e5a0, pae-ether-type = 888e.0300.0048
*Sep 19 07:00:24.115: dot1x-packet:EAPOL pak rx - Ver: 0x3 type: 0x0
*Sep 19 07:00:24.115: dot1x-packet: length: 0x0048
*Sep 19 07:00:24.115: dot1x-sm:[6470.0227.0a89, Ca0] Posting EAPOL_EAP for
0x60000009
*Sep 19 07:00:24.115: dot1x_auth_bend Ca0: during state auth_bend_request,
got event 6(eapolEap)
*Sep 19 07:00:24.115: @@@ dot1x_auth_bend Ca0: auth_bend_request ->
auth_bend_response
*Sep 19 07:00:24.115: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:entering
response state
*Sep 19 07:00:24.115: dot1x-ev:[6470.0227.0a89, Ca0] Response sent to the
server from 0x60000009
*Sep 19 07:00:24.115: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:request
response action
*Sep 19 07:00:24.115: EAP-EVENT: Received LL (Dot1x-Authenticator) event
'EAP_RX_PACKET' on handle 0x26000052
*Sep 19 07:00:24.115: EAP-AUTH-RX-PAK: Code:RESPONSE ID:0x12 Length:0x0048
Type:PEAP
*Sep 19 07:00:24.115: Payload: 0117030100186DEF131BC85E44CBDD50 ...
*Sep 19 07:00:24.115: eap_authen : during state eap_auth_idle2, got
event 1(eapRxPacket)
*Sep 19 07:00:24.115: @@@ eap_authen : eap_auth_idle2 -> eap_auth_received2
*Sep 19 07:00:24.115: EAP-AUTH-EVENT: EAP Response received by context
0x26000052
*Sep 19 07:00:24.115: EAP-AUTH-EVENT: EAP Response type = Method (25)
*Sep 19 07:00:24.115: EAP-EVENT: Stopping 'Authenticator Retransmit' timer
for EAP sesion handle 0x26000052
*Sep 19 07:00:24.115: eap_authen : during state eap_auth_received2, got
event 10(eapMethodData)
*Sep 19 07:00:24.115: @@@ eap_authen : eap_auth_received2 -> eap_auth_aaa_req
*Sep 19 07:00:24.116: EAP-AUTH-AAA-EVENT: Adding Audit-Session-ID
"c0a82104523aa0a30000001f" to RADIUS Req
*Sep 19 07:00:24.116: EAP-AUTH-AAA-EVENT: Added Audit-Session-ID
*Sep 19 07:00:24.116: EAP-AUTH-AAA-EVENT: Adding IDB "0x38167B5C" to
RADIUS Req
*Sep 19 07:00:24.116: EAP-AUTH-AAA-EVENT: Added IDB
*Sep 19 07:00:24.116: EAP-AUTH-AAA-EVENT: Adding EAP profile name
"PEAPProfile" to RADIUS Req
*Sep 19 07:00:24.116: EAP-AUTH-AAA-EVENT: Added EAP profile name to request
*Sep 19 07:00:24.116: EAP-EVENT: Sending LL (Dot1x-Authenticator) event
'EAP_CUSTOMIZE_AAA_REQUEST' on handle 0x26000052
*Sep 19 07:00:24.116: EAP-AUTH-AAA-EVENT: eap_auth_aaa_authen_request_shim
aaa_service 19, eap aaa_list handle 0, mlist handle 0
*Sep 19 07:00:24.116: EAP-AUTH-AAA-EVENT: Request sent successfully
*Sep 19 07:00:24.116: eap_authen : during state eap_auth_aaa_req, got
event 24(eapAAReqOk)
*Sep 19 07:00:24.116: @@@ eap_authen : eap_auth_aaa_req -> eap_auth_aaa_idle
*Sep 19 07:00:24.116: EAP-EVENT: Received LL (AAA_LOCAL_EAP) event
'EAP_RX_PACKET' on handle 0xCE000053
*Sep 19 07:00:24.116: EAP-AUTH-RX-PAK: Code:RESPONSE ID:0x12 Length:0x0048
Type:PEAP
*Sep 19 07:00:24.117: Payload: 0117030100186DEF131BC85E44CBDD50 ...
*Sep 19 07:00:24.117: eap_authen : during state eap_auth_idle, got event
1(eapRxPacket)
*Sep 19 07:00:24.117: @@@ eap_authen : eap_auth_idle -> eap_auth_received
*Sep 19 07:00:24.117: EAP-AUTH-EVENT: EAP Response received by context
0xCE000053

```

```

*Sep 19 07:00:24.117: EAP-AUTH-EVENT: EAP Response type = Method (25)
*Sep 19 07:00:24.117: eap_authen : during state eap_auth_received, got
event 10(eapMethodData)
*Sep 19 07:00:24.117: @@@ eap_authen : eap_auth_received ->
eap_auth_method_response
*Sep 19 07:00:24.117: EAP-EVENT: Sending method (PEAP) event 'Receive Packet'
on handle 0xCE000053
*Sep 19 07:00:24.117: EAP-AUTH-EVENT: Waiting for asynchronous reply from
method (PEAP)
*Sep 19 07:00:24.117: eap_authen : during state eap_auth_method_response,
got event 15(eapMethodWaitReply)
*Sep 19 07:00:24.117: @@@ eap_authen : eap_auth_method_response ->
eap_auth_idle
*Sep 19 07:00:24.118: EAP-EVENT: Received Method (PEAP) event
'EAP_METHOD_REPLY' on handle 0xCE000053
*Sep 19 07:00:24.118: eap_authen : during state eap_auth_idle, got event
4(eapMethodReply)
*Sep 19 07:00:24.118: @@@ eap_authen : eap_auth_idle ->
eap_auth_method_response
*Sep 19 07:00:24.118: EAP-AUTH-EVENT: Handling asynchronous method response
for context 0xCE000053
*Sep 19 07:00:24.118: EAP-EVENT: Sending LL (AAA_LOCAL_EAP) event
'EAP_KEY_AVAILABLE' on handle 0xCE000053
*Sep 19 07:00:24.118: EAP-AUTH-EVENT: EAP method state: Done
*Sep 19 07:00:24.118: EAP-AUTH-EVENT: EAP method decision: Unconditional
Success
*Sep 19 07:00:24.118: eap_authen : during state eap_auth_method_response,
got event 13(eapMethodEnd)
*Sep 19 07:00:24.118: @@@ eap_authen : eap_auth_method_response ->
eap_auth_select_action
*Sep 19 07:00:24.118: eap_authen : during state eap_auth_select_action,
got event 18(eapDecisionSuccess)
*Sep 19 07:00:24.118: @@@ eap_authen : eap_auth_select_action ->
eap_auth_success
*Sep 19 07:00:24.118: EAP-EVENT: Received get canned status from lower layer
(0xCE000053)
*Sep 19 07:00:24.118: EAP-AUTH-TX-PAK: Code:SUCCESS ID:0x12 Length:0x0004
*Sep 19 07:00:24.118: EAP-EVENT: Sending method (PEAP) event 'Free Context'
on handle 0xCE000053
*Sep 19 07:00:24.119: EAP-EVENT: Sending LL (AAA_LOCAL_EAP) event
'EAP_SUCCESS' on handle 0xCE000053
*Sep 19 07:00:24.119: EAP-EVENT: Received free context (0xCE000053) from LL
(AAA_LOCAL_EAP)
*Sep 19 07:00:24.119: EAP-EVENT: eap_aaa_reply
*Sep 19 07:00:24.119: EAP-AUTH-AAA-EVENT: Reply received session_label
BB000020
*Sep 19 07:00:24.119: EAP-AUTH-AAA-EVENT: Response contains EAP Message,
code: 3
*Sep 19 07:00:24.119: EAP-AUTH-AAA-EVENT: Response contains MS MPPE Send Key,
length:139
*Sep 19 07:00:24.119: EAP-AUTH-AAA-EVENT: Response contains MS MPPE Recv Key,
length:97
*Sep 19 07:00:24.119: EAP-EVENT: Sending LL (Dot1x-Authenticator) event
'EAP_KEY_AVAILABLE' on handle 0x26000052
*Sep 19 07:00:24.119: EAP-AUTH-AAA-EVENT: Authorization not required for
this context
*Sep 19 07:00:24.119: EAP-EVENT: Received LL (AAA_LOCAL_EAP) event
'EAP_DELETE' on handle 0xCE000053
*Sep 19 07:00:24.119: EAP-AUTH-AAA-ERROR: Failed to delete aaa coord
transaction for 0xCE000053
*Sep 19 07:00:24.119: EAP-AUTH-EVENT: Freed EAP auth context
*Sep 19 07:00:24.119: EAP-EVENT: Freed EAP context
*Sep 19 07:00:24.120: EAP-EVENT: Received AAA event 'EAP_AAA_SUCCESS' on
handle 0x26000052
*Sep 19 07:00:24.120: eap_authen : during state eap_auth_aaa_idle, got
event 7(eapAAASuccess)
*Sep 19 07:00:24.120: @@@ eap_authen : eap_auth_aaa_idle -> eap_auth_success
*Sep 19 07:00:24.120: EAP-AUTH-TX-PAK: Code:SUCCESS ID:0x12 Length:0x0004
*Sep 19 07:00:24.120: EAP-AUTH-EVENT: SUCCESS for EAP method ID: 25, name:
PEAP, on handle 0x26000052
*Sep 19 07:00:24.120: EAP-EVENT: Sending LL (Dot1x-Authenticator) event
'EAP_SUCCESS' on handle 0x26000052
*Sep 19 07:00:24.120: dot1x-packet:[6470.0227.0a89, Ca0] Received an EAP

```

```

Success
*Sep 19 07:00:24.120: dot1x-sm:[6470.0227.0a89, Ca0] Posting EAP_SUCCESS for
0x60000009
*Sep 19 07:00:24.120: dot1x_auth_bend Ca0: during state
auth_bend_response, got event 11(eapSuccess)
*Sep 19 07:00:24.120: @@@ dot1x_auth_bend Ca0: auth_bend_response ->
auth_bend_success
*Sep 19 07:00:24.120: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:exiting
response state
*Sep 19 07:00:24.120: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:entering
success state
*Sep 19 07:00:24.120: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:response
success action
*Sep 19 07:00:24.120: dot1x_auth_bend Ca0: idle during state
auth_bend_success
*Sep 19 07:00:24.121: @@@ dot1x_auth_bend Ca0: auth_bend_success ->
auth_bend_idle
*Sep 19 07:00:24.121: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:entering
idle state
*Sep 19 07:00:24.121: dot1x-sm:[6470.0227.0a89, Ca0] Posting AUTH_SUCCESS on
Client 0x60000009
*Sep 19 07:00:24.121: dot1x_auth Ca0: during state auth_authenticating,
got event 12(authSuccess_portValid)
*Sep 19 07:00:24.121: @@@ dot1x_auth Ca0: auth_authenticating ->
auth_authc_result
*Sep 19 07:00:24.121: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:exiting
authenticating state
*Sep 19 07:00:24.121: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:entering
authc_result state
*Sep 19 07:00:24.121: dot1x-ev:[6470.0227.0a89, Ca0] Sending EAPOL success
immediately
*Sep 19 07:00:24.121: dot1x-ev:[6470.0227.0a89, Ca0] Sending EAPOL packet
*Sep 19 07:00:24.121: dot1x-packet:[6470.0227.0a89, Ca0] Platform changed
src mac of EAPOL packet
*Sep 19 07:00:24.121: dot1x-registry:registry:dot1x_ether_macaddr called
*Sep 19 07:00:24.121: dot1x-packet:EAPOL pak Tx - Ver: 0x3 type: 0x0
*Sep 19 07:00:24.121: dot1x-packet: length: 0x0004
*Sep 19 07:00:24.121: dot1x-packet:EAP code: 0x3 id: 0x12 length: 0x0004
*Sep 19 07:00:24.121: dot1x-packet:[6470.0227.0a89, Ca0] EAPOL packet sent
to client 0x60000009
*Sep 19 07:00:24.122: dot1x-ev:[6470.0227.0a89, Ca0] Received Authz Success
for the client 0x60000009 (6470.0227.0a89)
*Sep 19 07:00:24.122: dot1x-sm:[6470.0227.0a89, Ca0] Posting AUTHZ_SUCCESS
on Client 0x60000009
*Sep 19 07:00:24.122: dot1x_auth Ca0: during state auth_authc_result,
got event 23(authzSuccess)
*Sep 19 07:00:24.122: @@@ dot1x_auth Ca0: auth_authc_result ->
auth_authenticated
*Sep 19 07:00:24.122: dot1x-sm:[6470.0227.0a89, Ca0] 0x60000009:entering
authenticated state
*Sep 19 07:00:24.122: dot1x-ev:[6470.0227.0a89, Ca0] EAPOL success packet
was sent earlier.
*Sep 19 07:00:24.122: EAP-EVENT: Received free context (0x26000052) from LL
(Dot1x-Authenticator)
*Sep 19 07:00:24.122: EAP-EVENT: Received LL (Dot1x-Authenticator) event
'EAP_DELETE' on handle 0x26000052
*Sep 19 07:00:24.123: EAP-AUTH-AAA-ERROR: Failed to delete aaa coord
transaction for 0x26000052
*Sep 19 07:00:24.123: EAP-AUTH-EVENT: Freed EAP auth context
*Sep 19 07:00:24.123: EAP-EVENT: Freed EAP context
*Sep 19 07:00:24.122: 6470.0227.0A89
client incoming attribute size are 304 1 wcm: pemDelScb Event skipping
delete
*Sep 19 07:00:24.636: 6470.0227.0A89 192.168.80.100 8021X_REQD (3) Change
state to L2AUTHCOMPLETE (4) last state RUN (20)
1 wcm: ^K4D8.146F.E5A
*Sep 19 07:00:24.636: 6470.0227.0A89 WCDB_CHANGE: 1 wcm: Client 1 m_vlan 80
Radio iif id 0xdf0f4000000005 bssid iif id 0xcd248000000015,
bssid 64D8.146F.E5A0
*Sep 19 07:00:24.636: 6470.0227.0A89 WCDB_AUTH: 1 wcm: Adding opt82 len 0
*Sep 19 07:00:24.636: 6470.0227.0A89 WCDB_CHANGE: 1 wcm: Suppressing SPI
(L2 Auth for reassoc) pemstate 4 state L2_AUTH(1) vlan 80 client_id
0xde51c000000021 mob 1 ackflag 2 dropd 0

```

```
*Sep 19 07:00:24.636: 6470.0227.0A89 192.168.80.100 L2AUTHCOMPLETE (4)
  pemAdvanceState2: 1 wcm: MOBILITY-COMPLETE with state 4.
*Sep 19 07:00:24.636: 6470.0227.0A89 Send request to EPM 1 wcm: UTHCOMPLETE
(4) pemAdvanceState2: MOBILITY-COMPLETE with state 4.
*Sep 19 07:00:24.649: 6470.0227.0A89 Received _EPM_SPI_STATUS_SUCCESS for
  request sent for client 1 wcm: for client
*Sep 19 07:00:24.649: 6470.0227.0A89 Post-auth policy ACK recvd from EPM,
  unset flag on MSCB 1 wcm: ient
*Sep 19 07:00:24.907: EAP-EVENT: Stopped EAP tick timer
```




Configuration Example: Custom Web Authentication with Local Authentication

The Custom Web Authentication with Local Authentication document describes how to configure a custom Web Authentication (WebAuth) with local authentication on a Wireless LAN Controller (WLC).

- [Prerequisites, page 109](#)
- [Configuring Custom Web Authentication, page 110](#)
- [Verifying the Custom Web Authentication with Local Authentication Configuration, page 113](#)
- [Troubleshooting the Custom Web Authentication with Local Authentication Configuration Issues, page 114](#)

Prerequisites

Before you configure and customize WebAuth, ensure your workstation:

- Has an IP address on an Open Service Set Identifier (SSID).
- Can ping and communicate with the default gateway.
- Can identify and locate the e-Domain Name Server (DNS) (**ipconfig all**)
- Can resolve names (with **nslookup**)
- Can access the internet.

Supported Platforms and Releases

The information in this document is based on the following software and hardware versions:

- Cisco Catalyst 3850 Series Switch
- Cisco Aironet 3600 Series Lightweight Access Point
- Microsoft Windows 7 Native Wireless Supplicant

**Note**

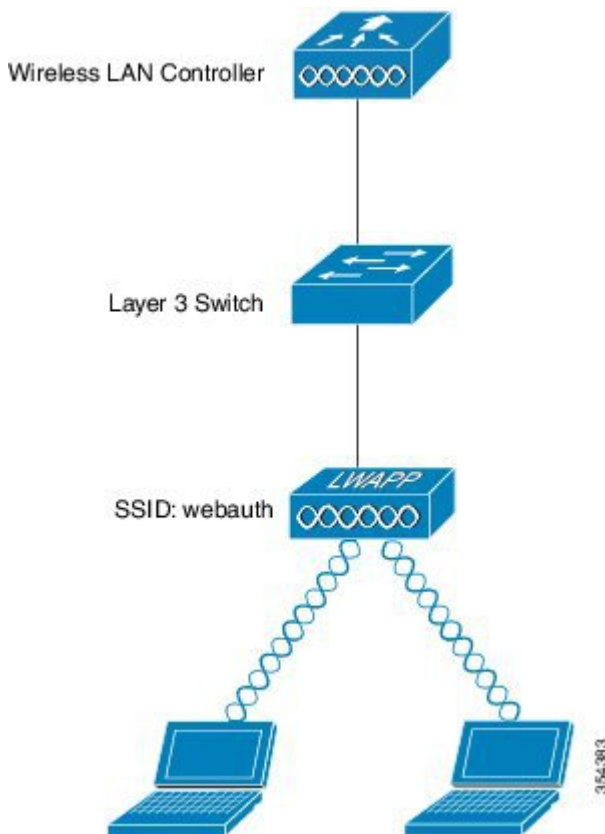
The information in this document refers to the devices in a specific lab environment. The devices have default configuration. If you are on a live network, you must understand the potential impact of all the commands

Configuring Custom Web Authentication

Network Diagram

The following figure describes the network diagram of the configuration:

Figure 26: Network Diagram



Configuring Authentication, Authorization, and Accounting

To configure Authentication, Authorization, and Accounting (AAA), use the following commands. The following commands configure the authentication and the authorization profiles such that the clients who connect are authenticated to the local WLC database:

```
aaa new-model
aaa authentication login local_webauth local
aaa authorization network default local
aaa authorization credential-download default local
```

Configuring Virtual IP address and Setting Parameter-Map

To configure the Virtual IP address on the WLC and to set the parameter type, which helps to specify the redirect URL, Login Page, Logout page, and Failure page, use the following commands:



Note Ensure that the files mentioned are available on Flash.

```
parameter-map type webauth custom
 type webauth
 timeout init-state sec 400
 custom-page login device flash:login.html
 custom-page failure device flash:failed.html
```

Configuring WLAN

To configure WLAN for Layer 3 security, use the following commands. The WLAN configuration maps the authentication list to Local_webauth and ensures that the authentication is handled by the local net users. The local authentication calls the AAA configuration configured in AAA.

```
wlan webauth 4 webauth
 client vlan 74
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security web-auth
 security web-auth authentication-list default
 security web-auth parameter-map custom
 no shutdown
```

Configuring Globally

To configure global, use the following commands:

Ensure that HTTP or HTTPS and IP device tracking are enabled. If HTTP or HTTPS is not enabled, then you cannot access the web page

```
ip http server
ip device tracking
```

Creating Local Users

To create local users, use the following command:

```
username <username> password 0 <password>
```

Configuring FTP for File Transfer

To configure FTP for file transfer, use the following commands:

```
ip ftp username <username>
ip ftp password <password>
```

Uploading to Flash

To upload custom HTML files to Flash, use the following command:

```
Device# copy ftp: //x.x.x.x /webauth_login.html flash:
The following example describes Flash content:
```

```
Device(config)# dir flash:
Directory of flash:/
64649  -rw-      1164    Oct 7 2013 04:36:23 +00:00  webauth_failure.html
64654  -rw-      2047    Oct 7 2013 13:32:38 +00:00  webauth_login.html
64655  -rw-      1208    Oct 7 2013 04:34:12 +00:00  webauth_success.html
64656  -rw-       900    Oct 7 2013 04:35:00 +00:00  webauth_expired.html
64657  -rw-     96894    Oct 7 2013 05:05:09 +00:00  web_auth_logo.png
64658  -rw-     23037    Oct 7 2013 13:17:58 +00:00  web_auth_cisco.png
64660  -rw-      2586    Oct 7 2013 13:31:27 +00:00  web_auth_aup.html
```

Configuring WLAN using GUI

Perform the following steps to configure WLAN using GUI:

-
- Step 1** Open a browser to connect to WLAN. You will be redirected to the login page.
 - Step 2** Enter the username and password.
 - Step 3** After successful authentication, retry the original URL when prompted.
-

Sample Webauth_login HTML

The following HTML code describes the Webauth_login:



Note

For any modification or customization of the following code, contact a HTML developer. Cisco Technical Assistance Center will not help in modifying or customizing the code.

```
<HTML><HEAD>
<TITLE>Authentication Proxy Login Page</TITLE>
```

```

<script type="text/javascript">
var pxypromptwindow1;
var pxysubmitted = false;
function submitreload() {
  if (pxysubmitted == false) {
    pxypromptwindow1=window.open('', 'pxywindow1',
' resizable=no,width=350,height=350,scrollbars=yes');
    pxysubmitted = true;
    return true;
  } else {
    alert("This page cannot be submitted twice.");
    return false;
  }
}
</script>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<style type="text/css">
body {
  background-color: #ffffff;
}
</style>
</HEAD>
<BODY>
<H1></H1>
<center>
<H2> Wireless Guest Access Web Authentication</H2>
<center>
<iframe src="http: //192.168.2.91 /flash:web_auth_aup.html" width="950" height="250"
scrolling="auto"></iframe><BR><BR>

<FORM method=post action="/" target="pxywindow1">
  Username: <input type=text name=uname><BR><BR>
  Password: <input type=password name=pwd><BR><BR>
  <input type=submit name=ok value=OK   onClick="return submitreload();">
</FORM><noscript>
<BR>
<UL>
  <H2><FONT COLOR="red">Warning!</FONT></H2>
  <p>JavaScript should be enabled in your Web browser
    for secure authentication</p>
  <LI>Follow the instructions of your Web browser to enable
    JavaScript if you would like to have JavaScript enabled
    for secure authentication</LI>
  <BR><OR><BR><BR>
  <LI> Follow these steps if you want to keep JavaScript
    disabled or if your browser does not support JavaScript
  <OL><BR>
    <LI> Close this Web browser window</LI>
    <LI> Click on Reload button of the original browser window</LI>
  </OL></LI>
</UL>
</noscript>
<center>
<p>&nbsp;</p>

</center>
</BODY></HTML>

```

Verifying the Custom Web Authentication with Local Authentication Configuration

Currently, there is no verification procedure available for Custom Web Authentication configuration.

Troubleshooting the Custom Web Authentication with Local Authentication Configuration Issues

Use the following example to troubleshoot configuration issues:

```
debug platform condition mac xx.yy.zz
debug platform condition start
show platform condition
```

```
request platform software trace filter-binary wireless
```

```
11/25 10:18:36.065 [ft]: [21669]: UUID: 8c000000001e4, ra: 7 (info): Processing assoc-req
station: 48f8.b38a.flb0 AP: 5087.89be.7420 -01 thread:0xffed2f7130
11/25 10:18:36.065 [rf-profile]: [21669]: UUID: 8c000000001e4, ra: 7 (info): RF profile
is NULL for default-group
11/25 10:18:36.065 [apf-mobile]: [21669]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
Client entry not found in the TRANS List.
11/25 10:18:36.065 [avc]: [21669]: UUID: 8c000000001e4, ra: 7 (info): 0000.0000.0000
4045:apfCreateMobileStationEntry: Set isAvcEnabled to FALSE, New Client
11/25 10:18:36.065 [apf-mobile-state]: [21669]: UUID: 8c000000001e4, ra: 7 (debug):
48f8.b38a.flb0 Changing state for mobile 48f8.b38a.flb0 on AP 5087.89be.7420 from Idle
to Idle, Reason:IDLE CREATE

11/25 10:18:36.065 [pem-state]: [21669]: UUID: 8c000000001e4, ra: 7 (debug): 48f8.b38a.flb0
Change state to START (0) last state START (0)

11/25 10:18:36.065 [avc]: [21669]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
4396:apfCreateMobileStationEntry: create MSCB ctxOwnerApIp = 9.5.74.101, ApIp = 9.5.74.101
11/25 10:18:36.065 [avc]: [21669]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
4405:apfCreateMobileStationEntry: create MSCB ctxOwnerApMac = 5087.89be.7420, AP Mac =
5087.89be.7420
11/25 10:18:36.065 [avc]: [21669]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
4415:apfCreateMobileStationEntry: create MSCB ctxOwnerMwarIp = 9.5.74.10, MwarIp = 9.5.74.10
ctxOwnerApSlotId = 1
11/25 10:18:36.065 [apf-mobile]: [21669]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
Adding mobile on LWAPP AP 5087.89be.7420 (1)
11/25 10:18:36.066 [apf-mobile]: [21669]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
Association received from mobile on radio 1 AP 5087.89be.7420
11/25 10:18:36.066 [rf-profile]: [21669]: UUID: 8c000000001e4, ra: 7 (info): RF Profile
data read: Profile count: 0 (empty)
11/25 10:18:36.066 [rf-profile]: [21669]: UUID: 8c000000001e4, ra: 7 (info): Profile Entry
Doesn't exist for
11/25 10:18:36.066 [apf-mobile]: [21669]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
Global 200 Clients are allowed to AP radio

11/25 10:18:36.066 [rf-profile]: [21669]: UUID: 8c000000001e4, ra: 7 (info): RF Profile
data read: Profile count: 0 (empty)
11/25 10:18:36.066 [rf-profile]: [21669]: UUID: 8c000000001e4, ra: 7 (info): Profile Entry
Doesn't exist for
11/25 10:18:36.066 [apf-mobile]: [21669]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
Rf profile 800 Clients are allowed to AP wlan

11/25 10:18:36.066 [apf-mobile]: [21669]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
apChanged 0 wlanChanged 0 mscb ipAddr 0.0.0.0, apf RadiusOverride 0x(nil), numIPv6Addr=0
11/25 10:18:36.066 [apf-mobile]: [21669]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
Applying WLAN policy on MSCB.
11/25 10:18:36.066 [pem]: [21669]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
Applying WLAN ACL policies to client
11/25 10:18:36.066 [pem]: [21669]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0 No
Interface ACL used for Wireless client in WCM(NGWC)
11/25 10:18:36.066 [ap-grp]: [21669]: UUID: 8c000000001e4, ra: 7 (debug): The name of the
interface is VLAN0074

11/25 10:18:36.066 [apf-mobile]: [21669]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
Applying site-specific IPv6 override for station 48f8.b38a.flb0 - vapId 4, site
'default-group', interface 'VLAN0074'
11/25 10:18:36.066 [apf-mobile]: [21669]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
```

```

Applying local bridging Interface Policy for station 48f8.b38a.flb0 - vlan 74, interface
'VLAN0074'
11/25 10:18:36.066 [ap-grp]: [21669]: UUID: 8c000000001e4, ra: 7 (debug): default-group
configured: no override needed

11/25 10:18:36.066 [rf-profile]: [21669]: UUID: 8c000000001e4, ra: 7 (info): RF profile
is NULL for default-group
11/25 10:18:36.066 [apf-mobile]: [21669]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
STA - rates (8): 140 18 152 36 176 72 96 108 0 0 0 0 0 0 0
11/25 10:18:36.066 [wps-mfp-client]: [21669]: UUID: 8c000000001e4, ra: 7 (debug):
48f8.b38a.flb0 apfProcessAssocReq MFP=0 CCX=0 vapEncr=0 status=0

11/25 10:18:36.066 [avc]: [21669]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0 AVC
NOT enabled on Wlan
11/25 10:18:36.066 [avc]: [21669]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0 AVC
not supported: Disable client AVC support
11/25 10:18:36.066 [capwap]: [21669]: UUID: 8c000000001e4, ra: 7 (debug): Platform capability
Virtual-port is FALSE
11/25 10:18:36.066 [apf-mobile]: [21669]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
new capwap_wtp_iif_id 0x800000004
11/25 10:18:36.066 [ifid_mgr]: [21669]: UUID: 8c000000001e4, ra: 7 (info): ifid alloc:
idx:[0x00000000] wcmObjId:[0x030048f8b38af1b0] mac:[48f8.b38a.flb0] major:[3] minor:[0]
reclaim:[FALSE]
11/25 10:18:36.066 [tdllib]: [21669]: UUID: 8c000000001e4, ra: 7 (info): TDL handle
0xaabd670ab0 set affinity to thread 0xff5e0ae780, pre-lock
11/25 10:18:36.066 [tdllib]: [21669]: UUID: 8c000000001e4, ra: 7 (info): TDL handle
0xaabd670ab0 set affinity to thread 0xff5e0ae780, post-lock
11/25 10:18:36.066 [tdllib]: [21669]: UUID: 8c000000001e4, ra: 7 (info): TDL handle
0xaabd670ab0 set affinity to thread 0xff5e0ae780
11/25 10:18:36.066 [ifid_mgr]: [21669]: UUID: 8c000000001e4, ra: 7 (debug): ifid alloc
0x030048f8b38af1b0 DELETE_PENDING/REUSE record found, id 0x80000012
11/25 10:18:36.067 [tdllib]: [21669]: UUID: 8c000000001e4, ra: 7 (info): Empty read cursor
list and no AOM handle. Destroying record.
11/25 10:18:36.067 [tdllib]: [21669]: UUID: 8c000000001e4, ra: 7 (info): ReplDB destroy
record: Found valid previous record intemporal list
11/25 10:18:36.067 [tdllib]: [21669]: UUID: 8c000000001e4, ra: 7 (info): ReplDB destroy
record: Destroyed a record in table (name: ifidmgr_reuse/86944351259f13d4e7132ff6c31de6fa,
id: 0, and LUID: 86944351259f13d4e7132ff6c31de6fa)
11/25 10:18:36.067 [(null)]: [21669]: UUID: 8c000000001e4, ra: 7 (info): Record was modified.
Done resetting modified bit.
11/25 10:18:36.067 [(null)]: [21669]: UUID: 8c000000001e4, ra: 7 (info): Record was modified.
Done resetting modified bit.
11/25 10:18:36.067 [tdllib]: [21669]: UUID: 8c000000001e4, ra: 7 (info): ReplDB internal
write cursor move: Assigning GC cursor to point to record
11/25 10:18:36.067 [ifid_mgr]: [21669]: UUID: 8c000000001e4, ra: 7 (debug): ifid alloc
0x030048f8b38af1b0 added active record 0x80000012
11/25 10:18:36.067 [tdllib]: [21669]: UUID: 8c000000001e4, ra: 7 (info): TDL handle
0xaabd670ab0 unset affinity to thread 0xff5e0ae780
11/25 10:18:36.067 [apf-mobile]: [21669]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
WLCLIENT: Client IIF Id alloc SUCCESS w/ client 0x80000012
11/25 10:18:36.067 [capwap]: [21669]: UUID: 8c000000001e4, ra: 7 (debug): Platform capability
Virtual-port is FALSE
11/25 10:18:36.067 [pem]: [21669]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0 In
>= L2AUTH COMPLETE for station 48f8.b38a.flb0
11/25 10:18:36.067 [pem]: [21669]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
0.0.0.0 START (0) Initializing policy
11/25 10:18:36.067 [pem-state]: [21669]: UUID: 8c000000001e4, ra: 7 (debug): 48f8.b38a.flb0
Change state to AUTHCHECK (2) last state START (0)

11/25 10:18:36.067 [pem-state]: [21669]: UUID: 8c000000001e4, ra: 7 (debug): 48f8.b38a.flb0
Change state to L2AUTHCOMPLETE (4) last state AUTHCHECK (2)

11/25 10:18:36.067 [pem]: [21669]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
0.0.0.0 L2AUTHCOMPLETE (4) DHCP Not required on AP 5087.89be.7420 vapId 4 apVapId 4for
this client
11/25 10:18:36.067 [pem]: [21669]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0 Not
Using WMM Compliance code qosCap 00
11/25 10:18:36.067 [bcast-igmp]: [21669]: UUID: 8c000000001e4, ra: 7 (debug): spamAddMobile:
num of mgid = 0

11/25 10:18:36.067 [avc]: [21669]: UUID: 8c000000001e4, ra: 7 (info): 5087.89be.7420
13725:spamAddMobile: ctxOwnerMwarIp: 9.5.74.10. ApIp: 9.5.74.101 ApEthMac: 5087.8991.e4d4
11/25 10:18:36.067 [pem]: [21669]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0

```

```

0.0.0.0 L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 5087.89be.7420 vapId 4 apVapId
4
11/25 10:18:36.067 [pem-state]: [21669]: UUID: 8c00000001e4, ra: 7 (debug): 48f8.b38a.flb0
Change state to DHCP_REQD (7) last state L2AUTHCOMPLETE (4)

11/25 10:18:36.067 [pem]: [21669]: UUID: 8c00000001e4, ra: 7 (info): 48f8.b38a.flb0
Incrementing the Reassociation Count 1 for client (of interface VLAN0074)
11/25 10:18:36.067 [dot1x]: [21669]: UUID: 8c00000001e4, ra: 7 (info): 48f8.b38a.flb0
apfMsAssoStateInc
11/25 10:18:36.067 [apf-mobile-state]: [21669]: UUID: 8c00000001e4, ra: 7 (debug):
48f8.b38a.flb0 Changing state for mobile 48f8.b38a.flb0 on AP 5087.89be.7420 from Idle
to Associated, Reason:ASSOC PEM ADD

11/25 10:18:36.067 [apf-lb]: [21669]: UUID: 8c00000001e4, ra: 7 (info): 48f8.b38a.flb0
New client (policy)
11/25 10:18:36.068 [apf-mobile]: [21669]: UUID: 8c00000001e4, ra: 7 (info): 48f8.b38a.flb0
Reason code 0, Preset 4, AAA cause 1
11/25 10:18:36.068 [apf-mobile]: [21669]: UUID: 8c00000001e4, ra: 7 (info): 48f8.b38a.flb0
Scheduling deletion of Mobile Station: (callerId: 49) in 1800 seconds
11/25 10:18:36.068 [location-client]: [21668]: UUID: 8c00000001e4, ra: 7 (debug):
48f8.b38a.flb0 Client associated - stopping probe timer if running

11/25 10:18:36.068 [apf-mobile]: [21669]: UUID: 8c00000001e4, ra: 7 (info): 48f8.b38a.flb0
Ms Timeout = 1800, Session Timeout = 1800

11/25 10:18:36.068 [wips]: [21669]: UUID: 8c00000001e4, ra: 7 (info): WIPS Auto-Immune
Get returned 0
11/25 10:18:36.068 [ft]: [21669]: UUID: 8c00000001e4, ra: 7 (info): Sending assoc-resp
station: 48f8.b38a.flb0 AP: 5087.89be.7420 -01 thread:0xffed2f7130
11/25 10:18:36.068 [rf-profile]: [21669]: UUID: 8c00000001e4, ra: 7 (info): RF profile
is NULL for default-group
11/25 10:18:36.068 [rf-profile]: [21669]: UUID: 8c00000001e4, ra: 7 (info): From global
config: Applying Rate:[12] index: 0 State: 2 Configs On Slot: 1On AP: 50:87:89:be:74:20
11/25 10:18:36.068 [rf-profile]: [21669]: UUID: 8c00000001e4, ra: 7 (info): From global
config: Applying Rate:[18] index: 1 State: 1 Configs On Slot: 1On AP: 50:87:89:be:74:20
11/25 10:18:36.068 [rf-profile]: [21669]: UUID: 8c00000001e4, ra: 7 (info): From global
config: Applying Rate:[24] index: 2 State: 2 Configs On Slot: 1On AP: 50:87:89:be:74:20
11/25 10:18:36.068 [rf-profile]: [21669]: UUID: 8c00000001e4, ra: 7 (info): From global
config: Applying Rate:[36] index: 3 State: 1 Configs On Slot: 1On AP: 50:87:89:be:74:20
11/25 10:18:36.068 [rf-profile]: [21669]: UUID: 8c00000001e4, ra: 7 (info): From global
config: Applying Rate:[48] index: 4 State: 2 Configs On Slot: 1On AP: 50:87:89:be:74:20
11/25 10:18:36.068 [rf-profile]: [21669]: UUID: 8c00000001e4, ra: 7 (info): From global
config: Applying Rate:[72] index: 5 State: 1 Configs On Slot: 1On AP: 50:87:89:be:74:20
11/25 10:18:36.068 [rf-profile]: [21669]: UUID: 8c00000001e4, ra: 7 (info): From global
config: Applying Rate:[96] index: 6 State: 1 Configs On Slot: 1On AP: 50:87:89:be:74:20
11/25 10:18:36.068 [rf-profile]: [21669]: UUID: 8c00000001e4, ra: 7 (info): From global
config: Applying Rate:[108] index: 7 State: 1 Configs On Slot: 1On AP: 50:87:89:be:74:20
11/25 10:18:36.068 [dtls]: [21669]: UUID: 8c00000001e4, ra: 7 (debug):
openssl_dtls_connection_find_using_link_info: DTLS connection find with Local 9.5.74.10:5247
Peer 9.5.74.101:7759

11/25 10:18:36.068 [dtls]: [21669]: UUID: 8c00000001e4, ra: 7 (info): Cannot find DTLS
connection handle 9.5.74.101:7759 from hash

11/25 10:18:36.068 [capwap]: [21669]: UUID: 8c00000001e4, ra: 7 (debug): DTLS Connection
not found for 9.5.74.101:7759

11/25 10:18:36.068 [apf-mobile]: [21669]: UUID: 8c00000001e4, ra: 7 (info): 48f8.b38a.flb0
Sending Assoc Response to station on BSSID 5087.89be.7420 (status 0) ApVapId 4 Slot 1
11/25 10:18:36.068 [apf-mobile-state]: [21669]: UUID: 8c00000001e4, ra: 7 (debug):
48f8.b38a.flb0 Changing state for mobile 48f8.b38a.flb0 on AP 5087.89be.7420 from
Associated to Associated, Reason:ASSOC TIME

11/25 10:18:36.068 [location-client]: [21669]: UUID: 8c00000001e4, ra: 7 (debug):
48f8.b38a.flb0 802 new client 48f8.b38a.flb0

11/25 10:18:36.068 [mob-handoff]: [21669]: UUID: 8c00000001e4, ra: 7 (debug): 48f8.b38a.flb0
Mobility query: PEM State: DHCP_REQD, apfMmState=apfMsMmInitial apfMmRole=Unassoc
11/25 10:18:36.068 [location-client]: [21668]: UUID: 8c00000001e4, ra: 7 (debug):
48f8.b38a.flb0 Client associated - stopping probe timer if running

11/25 10:18:36.068 [pem]: [21669]: UUID: 8c00000001e4, ra: 7 (info): 48f8.b38a.flb0
0.0.0.0 DHCP_REQD (7) MOBILITY-INCOMPLETE with state 7.

```



```
11/25 10:18:36.068 [mob-handoff]: [21669]: UUID: 8c000000001e4, ra: 7 (debug): 48f8.b38a.flb0
mmMaRxAssocReq:6696 MA FSM event MM_MAFSM_EV_FULLL_AUTH: state Init ->
Init_Wait_Announce_Response
11/25 10:18:36.068 [pem]: [21669]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
0.0.0.0 DHCP_REQD (7) MOBILITY-INCOMPLETE with state 7.

11/25 10:18:36.069 [sim-cs]: [21669]: UUID: 8c000000001e4, ra: 7 (info): System IP addr :
9.5.74.10

11/25 10:18:36.069 [sim-cs]: [21669]: UUID: 8c000000001e4, ra: 7 (info): System IP addr :
9.5.74.10

11/25 10:18:36.069 [mob-handoff]: [21669]: UUID: 8c000000001e4, ra: 7 (debug): 48f8.b38a.flb0
[1691: Mobile Announce MA->MC] to 9.5.74.10:16666
11/25 10:18:36.069 [snmp-trap]: [21669]: UUID: 8c000000001e4, ra: 7 (debug):
80211ClientAssociationTrap called
11/25 10:18:36.069 [mob-handoff]: [22238]: UUID: 8c000000001e4, ra: 7 (debug): 48f8.b38a.flb0
[1691: Mobile Announce MA->MC] from 9.5.74.10:16666
11/25 10:18:36.069 [cond_debug]: [22238]: UUID: 8c000000001e4, ra: 7 (info): Search
condition: ft_id 43, cond: type 16, fmt 2, id: 0x48f8b38a, name: H□□□□
11/25 10:18:36.069 [cond_debug]: [22238]: UUID: 8c000000001e4, ra: 7 (info): Condition
found
11/25 10:18:36.069 [qos]: [21632]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0 [QOS]
%: Skipped Add Mobile QoS Thinbind Payld for STA
11/25 10:18:36.069 [wcm]: [22238]: UUID: 8c000000001e5, ra: 7 (appctx): mac
48:f8:b3:8a:f1:b0
11/25 10:18:36.069 [mob-handoff]: [22238]: UUID: 8c000000001e5, ra: 7 (debug): 48f8.b38a.flb0
Mobile announce received, sender IP addr 9.5.74.10

11/25 10:18:36.069 [dtls]: [21632]: UUID: 8c000000001e4, ra: 7 (debug):
openssl_dtls_connection_find_using_link_info: DTLS connection find with Local 9.5.74.10:5246
Peer 9.5.74.101:7759

11/25 10:18:36.069 [sim-cs]: [22238]: UUID: 8c000000001e5, ra: 7 (info): System IP addr :
9.5.74.10

11/25 10:18:36.069 [dtls]: [21632]: UUID: 8c000000001e4, ra: 7 (debug): 5087.89be.7420
DTLS connection found! Acquiring lock for 0xffed6f8378
11/25 10:18:36.069 [sim-cs]: [22238]: UUID: 8c000000001e5, ra: 7 (info): System IP addr :
9.5.74.10

11/25 10:18:36.069 [mob-handoff]: [22238]: UUID: 8c000000001e5, ra: 7 (debug): 48f8.b38a.flb0
[1691: Mobile Announce MC->MC] to 9.5.79.10:16666
11/25 10:18:36.069 [sim-cs]: [22238]: UUID: 8c000000001e5, ra: 7 (info): System IP addr :
9.5.74.10

11/25 10:18:36.069 [dtls]: [21632]: UUID: 8c000000001e4, ra: 7 (debug): 5087.89be.7420
Releasing lock for 0xffed6f8378
11/25 10:18:36.069 [sim-cs]: [22238]: UUID: 8c000000001e5, ra: 7 (info): System IP addr :
9.5.74.10

11/25 10:18:36.069 [mob-dtls]: [22238]: UUID: 8c000000001e5, ra: 7 (info):
mmEncryptAndSendFragMsg:254 hdrLen 8 dataLen 200
11/25 10:18:36.069 [spam]: [21632]: UUID: 8c000000001e4, ra: 7 (info): 5087.89be.7420
Successful transmission of LWAPP Add-Mobile to AP 5087.89be.7420
11/25 10:18:36.069 [sim-cs]: [22238]: UUID: 8c000000001e5, ra: 7 (info): System IP addr :
9.5.74.10

11/25 10:18:36.069 [cac]: [21632]: UUID: 8c000000001e4, ra: 7 (info): In ADD_MOBILE snooping
spam_status callSnoop = 0 vapid 4
11/25 10:18:36.069 [mob-dtls]: [22238]: UUID: 8c000000001e5, ra: 7 (info):
mm_dtls2_process_snd_msg:933 hdrLen 8, DataLen 200
11/25 10:18:36.069 [mob-dtls]: [22238]: UUID: 8c000000001e5, ra: 7 (info):
dtls2_encrypt_and_send:1731 keys plumbed, forwarding to the DTLS engine, hdrLen 8 len 200
flags 0x3
11/25 10:18:36.069 [mob-dtls]: [22238]: UUID: 8c000000001e5, ra: 7 (info):
mm_dtls2_send_callback:141 hdrLen 8 length 200 flag 3
11/25 10:18:36.069 [mob-dtls]: [22238]: UUID: 8c000000001e5, ra: 7 (info):
mmUdpSendMsgFromDtls:226 is not Encrypted enabled hdrLen 8 dataLen 200
11/25 10:18:36.069 [sim-cs]: [22238]: UUID: 8c000000001e5, ra: 7 (info): System IP addr :
9.5.74.10, VLAN ID: 74
```

```

11/25 10:18:36.069 [sim-cs]: [22238]: UUID: 8c00000001e5, ra: 7 (info): System IP addr :
9.5.74.10, IIF ID: 0x2a

11/25 10:18:36.069 [mob-ka]: [22238]: UUID: 8c00000001e5, ra: 7 (debug): MM packet to
9.5.79.10 :16666 with VLAN: 74, src if id: 0x2a
11/25 10:18:36.070 [mob-handoff]: [22238]: UUID: 8c00000001e5, ra: 7 (debug): Mobile
announce from MA and Client entry not found, groupcasted to peer MC's

11/25 10:18:36.071 [wcm]: [22238]: UUID: 8c00000001e6, ra: 7 (appctx): mac
48:f8:b3:8a:f1:b0
11/25 10:18:36.950 [mob-handoff]: [21621]: UUID: 8c00000001e4, ra: 7 (debug): 48f8.b38a.flb0
[1691: Mobile Announce MA->MC] to 9.5.74.10:16666
11/25 10:18:36.950 [mob-handoff]: [21621]: UUID: 8c00000001e4, ra: 7 (debug): 48f8.b38a.flb0
Mobile Announce retry1 to IP: 9.5.74.10 Peer IP: 0.0.0.0, Anchor IP: 0.0.0.0
11/25 10:18:36.950 [mob-handoff]: [22238]: UUID: 8c00000001e4, ra: 7 (debug): 48f8.b38a.flb0
[1691: Mobile Announce MA->MC] from 9.5.74.10:16666
11/25 10:18:36.950 [cond_debug]: [22238]: UUID: 8c00000001e4, ra: 7 (info): Search
condition: ft_id 43, cond: type 16, fmt 2, id: 0x48f8b38a, name: H□□□□
11/25 10:18:36.950 [cond_debug]: [22238]: UUID: 8c00000001e4, ra: 7 (info): Condition
found
11/25 10:18:36.950 [wcm]: [22238]: UUID: 8c00000001e7, ra: 7 (appctx): mac
48:f8:b3:8a:f1:b0
11/25 10:18:36.950 [mob-handoff]: [22238]: UUID: 8c00000001e7, ra: 7 (debug): 48f8.b38a.flb0
Mobile announce received, sender IP addr 9.5.74.10

11/25 10:18:36.951 [sim-cs]: [22238]: UUID: 8c00000001e7, ra: 7 (info): System IP addr :
9.5.74.10

11/25 10:18:36.951 [sim-cs]: [22238]: UUID: 8c00000001e7, ra: 7 (info): System IP addr :
9.5.74.10

11/25 10:18:36.951 [mob-handoff]: [22238]: UUID: 8c00000001e7, ra: 7 (debug): 48f8.b38a.flb0
[1691: Mobile Announce MC->MC] to 9.5.79.10:16666
11/25 10:18:36.951 [sim-cs]: [22238]: UUID: 8c00000001e7, ra: 7 (info): System IP addr :
9.5.74.10

11/25 10:18:36.951 [sim-cs]: [22238]: UUID: 8c00000001e7, ra: 7 (info): System IP addr :
9.5.74.10

11/25 10:18:36.951 [mob-dtls]: [22238]: UUID: 8c00000001e7, ra: 7 (info):
mmEncryptAndSendFragMsg:254 hdrLen 8 dataLen 200
11/25 10:18:36.951 [sim-cs]: [22238]: UUID: 8c00000001e7, ra: 7 (info): System IP addr :
9.5.74.10

11/25 10:18:36.951 [mob-dtls]: [22238]: UUID: 8c00000001e7, ra: 7 (info):
mm_dtls2_process_snd_msg:933 hdrLen 8, DataLen 200
11/25 10:18:36.951 [mob-dtls]: [22238]: UUID: 8c00000001e7, ra: 7 (info):
dtls2_encrypt_and_send:1731 keys plumbed, forwarding to the DTLS engine, hdrLen 8 len 200
flags 0x3
11/25 10:18:36.951 [mob-dtls]: [22238]: UUID: 8c00000001e7, ra: 7 (info):
mm_dtls2_send_callback:141 hdrLen 8 length 200 flag 3
11/25 10:18:36.951 [mob-dtls]: [22238]: UUID: 8c00000001e7, ra: 7 (info):
mmUdpSendMsgFromDtls:226 is not Encrypted enabled hdrLen 8 dataLen 200
11/25 10:18:36.951 [sim-cs]: [22238]: UUID: 8c00000001e7, ra: 7 (info): System IP addr :
9.5.74.10, VLAN ID: 74

11/25 10:18:36.951 [sim-cs]: [22238]: UUID: 8c00000001e7, ra: 7 (info): System IP addr :
9.5.74.10, IIF ID: 0x2a

11/25 10:18:36.951 [mob-ka]: [22238]: UUID: 8c00000001e7, ra: 7 (debug): MM packet to
9.5.79.10 :16666 with VLAN: 74, src if id: 0x2a
11/25 10:18:36.951 [mob-handoff]: [22238]: UUID: 8c00000001e7, ra: 7 (debug): Mobile
announce from MA and Client entry not found, groupcasted to peer MC's

11/25 10:18:36.952 [wcm]: [22238]: UUID: 8c00000001e8, ra: 7 (appctx): mac
48:f8:b3:8a:f1:b0
11/25 10:18:37.942 [mob-handoff]: [21621]: UUID: 8c00000001e4, ra: 7 (debug): 48f8.b38a.flb0
[1691: Mobile Announce MA->MC] to 9.5.74.10:16666
11/25 10:18:37.942 [mob-handoff]: [21621]: UUID: 8c00000001e4, ra: 7 (debug): 48f8.b38a.flb0
Mobile Announce retry2 to IP: 9.5.74.10 Peer IP: 0.0.0.0, Anchor IP: 0.0.0.0
11/25 10:18:37.942 [mob-handoff]: [22238]: UUID: 8c00000001e4, ra: 7 (debug): 48f8.b38a.flb0
[1691: Mobile Announce MA->MC] from 9.5.74.10:16666
11/25 10:18:37.942 [cond_debug]: [22238]: UUID: 8c00000001e4, ra: 7 (info): Search

```

```
condition: ft id 43, cond: type 16, fmt 2, id: 0x48f8b38a, name: H□□□□
11/25 10:18:37.942 [cond_debug]: [22238]: UUID: 8c000000001e4, ra: 7 (info): Condition
found
11/25 10:18:37.942 [wcm]: [22238]: UUID: 8c000000001e9, ra: 7 (appctx): mac
48:f8:b3:8a:f1:b0
11/25 10:18:37.942 [mob-handoff]: [22238]: UUID: 8c000000001e9, ra: 7 (debug): 48f8.b38a.flb0
Mobile announce received, sender IP addr 9.5.74.10

11/25 10:18:37.942 [sim-cs]: [22238]: UUID: 8c000000001e9, ra: 7 (info): System IP addr :
9.5.74.10

11/25 10:18:37.942 [sim-cs]: [22238]: UUID: 8c000000001e9, ra: 7 (info): System IP addr :
9.5.74.10

11/25 10:18:37.942 [mob-handoff]: [22238]: UUID: 8c000000001e9, ra: 7 (debug): 48f8.b38a.flb0
[1691: Mobile Announce MC->MC] to 9.5.79.10:16666
11/25 10:18:37.942 [sim-cs]: [22238]: UUID: 8c000000001e9, ra: 7 (info): System IP addr :
9.5.74.10

11/25 10:18:37.942 [sim-cs]: [22238]: UUID: 8c000000001e9, ra: 7 (info): System IP addr :
9.5.74.10

11/25 10:18:37.943 [mob-dtls]: [22238]: UUID: 8c000000001e9, ra: 7 (info):
mmEncryptAndSendFragMsg:254 hdrLen 8 dataLen 200
11/25 10:18:37.943 [sim-cs]: [22238]: UUID: 8c000000001e9, ra: 7 (info): System IP addr :
9.5.74.10

11/25 10:18:37.943 [mob-dtls]: [22238]: UUID: 8c000000001e9, ra: 7 (info):
mm dtls2_process_snd_msg:933 hdrLen 8, DataLen 200
11/25 10:18:37.943 [mob-dtls]: [22238]: UUID: 8c000000001e9, ra: 7 (info):
dtls2_encrypt_and_send:1731 keys plumbed, forwarding to the DTLS engine, hdrLen 8 len 200
flags 0x3
11/25 10:18:37.943 [mob-dtls]: [22238]: UUID: 8c000000001e9, ra: 7 (info):
mm dtls2_send callback:141 hdrLen 8 length 200 flag 3
11/25 10:18:37.943 [mob-dtls]: [22238]: UUID: 8c000000001e9, ra: 7 (info):
mmUdpSendMsgFromDtls:226 is not Encrypted enabled hdrLen 8 dataLen 200
11/25 10:18:37.943 [sim-cs]: [22238]: UUID: 8c000000001e9, ra: 7 (info): System IP addr :
9.5.74.10, VLAN ID: 74

11/25 10:18:37.943 [sim-cs]: [22238]: UUID: 8c000000001e9, ra: 7 (info): System IP addr :
9.5.74.10, IIF ID: 0x2a

11/25 10:18:37.943 [mob-ka]: [22238]: UUID: 8c000000001e9, ra: 7 (debug): MM packet to
9.5.79.10 :16666 with VLAN: 74, src if id: 0x2a
11/25 10:18:37.943 [mob-handoff]: [22238]: UUID: 8c000000001e9, ra: 7 (debug): Mobile
announce from MA and Client entry not found, groupcasted to peer MC's

11/25 10:18:37.944 [wcm]: [22238]: UUID: 8c000000001ea, ra: 7 (appctx): mac
48:f8:b3:8a:f1:b0
11/25 10:18:38.207 [mgmt_infra]: [17333]: UUID: 0, ra: 0 (ERR): Failed to get values
11/25 10:18:38.934 [mob-handoff]: [21621]: UUID: 8c000000001e4, ra: 7 (debug): 48f8.b38a.flb0
ma_process_mc_announce_nak:749 MA FSM event MM_MAFSM_EV_MA_NAK_FROM_MC_OR_MAX_RETX_TIMEOUT:
state Init Wait Announce Response -> Local
11/25 10:18:38.934 [sim-cs]: [21621]: UUID: 8c000000001e4, ra: 7 (info): System IP addr :
9.5.74.10

11/25 10:18:38.934 [sim-cs]: [21621]: UUID: 8c000000001e4, ra: 7 (info): System IP addr :
9.5.74.10

11/25 10:18:38.934 [mob-handoff]: [21621]: UUID: 8c000000001e4, ra: 7 (debug):
48f8.b38a.flb0 0.0.0.0 DHCP_REQD (7) mobility role update request from Unassociated to
Local
Peer = 0.0.0.0, Old Anchor = 0.0.0.0, New Anchor = 9.5.74.10
11/25 10:18:38.934 [ipv6]: [21621]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
pemUpdateIpv6FwdTbl: vlan = 74, STA mac = 48f8.b38a.flb0 role=Local, oldRole=Unassociated
11/25 10:18:38.934 [ipv6]: [21621]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
pemUpdateIpv6FwdTbl: Add the client to the IPv6 MGID table, vlan=74, bridgeDomain=0 role=Local
11/25 10:18:38.934 [mob-handoff]: [21621]: UUID: 8c000000001e4, ra: 7 (debug): 48f8.b38a.flb0
Client did an initial full auth

11/25 10:18:38.934 [pem]: [21621]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
0.0.0.0 DHCP_REQD (7) pemAdvanceState2: MOBILITY-COMPLETE with state 7.
```

```

11/25 10:18:38.934 [ipv6]: [21695]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.f1b0
Receive IPV6_MSG_MGID_CLIENT_ADD event, vlanId = 74, bridgeDomain 0
11/25 10:18:38.934 [ipv6]: [21695]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.f1b0 IPv6:
client is not found in the RA table
11/25 10:18:38.934 [apf-mobile-state]: [21621]: UUID: 8c000000001e4, ra: 7 (debug):
48f8.b38a.f1b0 Changing state for mobile 48f8.b38a.f1b0 on AP 5087.89be.7420 from
Associated to Associated, Reason:Mobility Complete

11/25 10:18:38.934 [ipv6]: [21695]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.f1b0
ipv6AddClientMgidTbl: send IPv6 mgid-join message to AP=5087.89be.7420, mgid=16383, slotid=1,
vapId=4
11/25 10:18:38.934 [pem]: [21621]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.f1b0
0.0.0.0 DHCP_REQD (7) State Update from Mobility-Incomplete to Mobility-Complete, mobility
role=Local, client state=APF_MS_STATE_ASSOCIATED
11/25 10:18:38.934 [ipv6]: [21695]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.f1b0
sendMgidInfoMsgToSpam: numofmgid=1, mgid=16383
11/25 10:18:38.934 [wcm]: [21621]: UUID: 8c000000001e4, ra: 7 (debug): AAA-Proxy attr list
alloc: Created attribute list = (450000B7)
11/25 10:18:38.934 [ipv6]: [21695]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.f1b0
ipv6AddClientMgidTbl: Add the client in the MGID table, vlan=74, BridgeDomain=0
11/25 10:18:38.934 [smrcl]: [21621]: UUID: 8c000000001e4, ra: 7 (debug): EEDGE-RCL: Session
start event
11/25 10:18:38.934 [bcast-igmp]: [21631]: UUID: 8c000000001e4, ra: 7 (debug):
spamLradSendMgidInfo: ap = 5087.89be.7420 slotId = 1, apVapId = 4, numOfMgid = 1 mc2ucflag
= 1, qos = 3

11/25 10:18:38.935 [dtls]: [21631]: UUID: 8c000000001e4, ra: 7 (debug):
openssl_dtls_connection_find_using_link_info: DTLS connection find with Local 9.5.74.10:5246
Peer 9.5.74.101:7759

11/25 10:18:38.935 [dtls]: [21631]: UUID: 8c000000001e4, ra: 7 (debug): 5087.89be.7420
DTLS connection found! Acquiring lock for 0xffed6f8378
11/25 10:18:38.935 [tdllib]: [21621]: UUID: 8c000000001e4, ra: 7 (debug): marshal: set
uuid 8c000000001e4, ra 7
11/25 10:18:38.935 [wcm]: [21621]: UUID: 8c000000001e4, ra: 7 (debug): AAA-Proxy attr list
free: Freed attribute list = (450000B7).
11/25 10:18:38.935 [pem]: [21621]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.f1b0 SANET
session start initiated with trusted flag: 0
11/25 10:18:38.935 [pem]: [21621]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.f1b0
WEBAUTH: Session with SMD successfully created
11/25 10:18:38.935 [mob-handoff]: [21621]: UUID: 8c000000001e4, ra: 7 (debug): 48f8.b38a.f1b0
Mobility Response: IP 0.0.0.0 code MA Handoff (7), reason Unknown (7), PEM State DHCP_REQD,
Role Local(1)
11/25 10:18:38.935 [sim-cs]: [21621]: UUID: 8c000000001e4, ra: 7 (info): System IP addr :
9.5.74.10

11/25 10:18:38.935 [sim-cs]: [21621]: UUID: 8c000000001e4, ra: 7 (info): System IP addr :
9.5.74.10

11/25 10:18:38.935 [dtls]: [21631]: UUID: 8c000000001e4, ra: 7 (debug): 5087.89be.7420
Releasing lock for 0xffed6f8378
11/25 10:18:38.935 [cond_debug]: [22238]: UUID: 8c000000001e4, ra: 7 (info): Condition
found
11/25 10:18:38.935 [wcm]: [22238]: UUID: 8c000000001eb, ra: 7 (appctx): mac
48:f8:b3:8a:f1:b0
11/25 10:18:38.935 [sim-cs]: [22238]: UUID: 8c000000001eb, ra: 7 (info): System IP addr :
9.5.74.10

11/25 10:18:38.935 [mob-handoff]: [22238]: UUID: 8c000000001eb, ra: 7 (debug): 48f8.b38a.f1b0
Handoff Complete msg for Client(Ip: 0.0.0.0 roam-type: None)Sender(Ip: 9.5.74.10 Type: 1)
Anchor(Ip: 0.0.0.0 MC : 0.0.0.0)Foreign(Ip : 0.0.0.0 MC : 0.0.0.0)
11/25 10:18:38.935 [mob-handoff]: [22238]: UUID: 8c000000001eb, ra: 7 (debug): 48f8.b38a.f1b0
MC MA client: 0.0.0.0 Added
11/25 10:18:38.936 [sim-cs]: [22238]: UUID: 8c000000001eb, ra: 7 (info): System IP addr :
9.5.74.10

11/25 10:18:38.936 [mob-handoff]: [22238]: UUID: 8c000000001eb, ra: 7 (debug): 48f8.b38a.f1b0
[1692: Handoff Complete Ack MC->MA] to 9.5.74.10:16666
11/25 10:18:38.936 [sim-cs]: [22238]: UUID: 8c000000001eb, ra: 7 (info): System IP addr :
9.5.74.10

11/25 10:18:38.936 [mob-handoff]: [22238]: UUID: 8c000000001eb, ra: 7 (debug): 48f8.b38a.f1b0
Handoff Complete Ack sent to IP: 9.5.74.10

```

```

11/25 10:18:38.936 [ipv6]: [22238]: UUID: 8c000000001eb, ra: 7 (info): 48f8.b38a.flb0
mCMobileHandoffCmplRcv: IPv6: set client vlanId = 74, bridgeDomain Id =0
11/25 10:18:38.936 [mob-handoff]: [21656]: UUID: 8c000000001eb, ra: 7 (debug): 48f8.b38a.flb0
[1692: Handoff Complete Ack MC->MA] from 9.5.74.10:16666
11/25 10:18:38.936 [sim-cs]: [21656]: UUID: 8c000000001eb, ra: 7 (info): System IP addr :
9.5.74.10

11/25 10:18:38.936 [mob-directory]: [22238]: UUID: 8c000000001eb, ra: 7 (debug):
48f8.b38a.flb0 HANDOFF MA: 9.5.74.10 : Local Wireless client ip: 0.0.0.0 learn:0 ssid:webauth
vap_sec:[ Webauth ] PEM:DHCP_REQD, vlan:74/74 AP:5087.89be.7420 radio:1 ch:36 state:3
mobile_status:0 reason:4
11/25 10:18:38.936 [cond_debug]: [21656]: UUID: 8c000000001eb, ra: 7 (info): Search
condition: ft_id 43, cond: type 16, fmt 2, id: 0x1010074, name:
11/25 10:18:38.936 [sim-cs]: [22238]: UUID: 8c000000001eb, ra: 7 (info): System IP addr :
9.5.74.10

11/25 10:18:38.936 [cond_debug]: [21656]: UUID: 8c000000001eb, ra: 7 (info): Condition not
found
11/25 10:18:38.936 [wcm]: [21656]: UUID: 8c000000001ec, ra: 7 (appctx): mac
48:f8:b3:8a:fl:b0
11/25 10:18:38.936 [mob-handoff]: [22238]: UUID: 8c000000001eb, ra: 7 (debug): 48f8.b38a.flb0
MC: Changing client state from 0 to 1
11/25 10:18:38.936 [mob-handoff]: [21656]: UUID: 8c000000001ec, ra: 7 (debug): 48f8.b38a.flb0
mmProcessInMsg:1377 MA FSM event MM_MAFSM_EV_HDOFF_COMPL ACK: state Local -> Local
11/25 10:18:38.943 [tdllib]: [17333]: UUID: 8c000000001e4, ra: 7 (debug): unmarshal: got
uuid 8c000000001e4, ra 7
11/25 10:18:38.943 [smrcl]: [17333]: UUID: 8c000000001e4, ra: 7 (debug): EEDGE-RCL: Rx -
[eEdge --> IOS] OUT Callback Notify type 4 for rcl_conn_hdl = 101
11/25 10:18:38.943 [wcm]: [17333]: UUID: 8c000000001e4, ra: 7 (debug): AAA-Proxy attr list
alloc: Created attribute list = (D20000B8)
11/25 10:18:38.943 [aaa]: [17333]: UUID: 8c000000001e4, ra: 7 (debug): 48f8.b38a.flb0 Start
response cb rcvd, label: 838860839, ASID: 09054A0A000000313CF8CE5F
11/25 10:18:38.944 [aaa]: [17333]: UUID: 8c000000001e4, ra: 7 (debug): 48f8.b38a.flb0 Start
response cb from SANET successfully enqueued
11/25 10:18:38.944 [wcm]: [17333]: UUID: 8c000000001e4, ra: 7 (debug): AAA-Proxy attr list
free: Freed attribute list = (D20000B8).
11/25 10:18:38.944 [apf-mobile]: [21661]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
Start response callback from SANET successfully processed
11/25 10:18:38.944 [smrcl]: [17333]: UUID: 8c000000001e4, ra: 7 (debug):
ipc(mqipc/wcm/smd-wcm):End of MQIPC queue with 2 messages in 0 ms
11/25 10:18:38.979 [dtls]: [21631]: UUID: 8c000000001e4, ra: 7 (debug):
openssl_dtls_connection_find_using_link_info: DTLS connection find with Local 9.5.74.10:5246
Peer 9.5.74.101:7759

11/25 10:18:38.979 [dtls]: [21631]: UUID: 8c000000001e4, ra: 7 (debug): 5087.89be.7420
DTLS connection found! Acquiring lock for 0xffed6f8378
11/25 10:18:38.980 [dtls]: [21631]: UUID: 8c000000001e4, ra: 7 (debug): 5087.89be.7420
Releasing lock for 0xffed6f8378
11/25 10:18:38.980 [aaa]: [21631]: UUID: 8c000000001e4, ra: 7 (debug): 48f8.b38a.flb0
FQDN-REPORT: Register success in sending URL msg snooping = 1 to AP 5087.89be.7420, slot =
1
11/25 10:18:38.980 [smrcl]: [17333]: UUID: 8c000000001e4, ra: 7 (debug):
ipc(mqipc/wcm/smd-wcm):Get a MQIPC message (len 252)
11/25 10:18:38.980 [tdllib]: [17333]: UUID: 8c000000001e4, ra: 7 (debug): unmarshal: got
uuid 8c000000001e4, ra 7
11/25 10:18:38.980 [aaa]: [17333]: UUID: 8c000000001e4, ra: 7 (debug): 48f8.b38a.flb0
Policy Source received in Bind Call: policy_src[0]: NONE
11/25 10:18:38.980 [aaa]: [17333]: UUID: 8c000000001e4, ra: 7 (debug): 48f8.b38a.flb0
Policy Source received in Bind Call: policy_src[1]: NONE
11/25 10:18:38.980 [aaa]: [17333]: UUID: 8c000000001e4, ra: 7 (debug): 48f8.b38a.flb0
Policy Source received in Bind Call: policy_src[2]: NONE
11/25 10:18:38.980 [aaa]: [17333]: UUID: 8c000000001e4, ra: 7 (debug): 48f8.b38a.flb0
Policy Source received in Bind Call: policy_src[3]: CLI
11/25 10:18:38.980 [aaa]: [17333]: UUID: 8c000000001e4, ra: 7 (debug): 48f8.b38a.flb0 Bind
policy msg from SANET successfully enqueued
11/25 10:18:38.980 [aaa]: [21661]: UUID: 8c000000001e4, ra: 7 (debug): 48f8.b38a.flb0
***----- Bind policies from EPM -----***
11/25 10:18:38.980 [smrcl]: [17333]: UUID: 8c000000001e4, ra: 7 (debug):
ipc(mqipc/wcm/smd-wcm):End of MQIPC queue with 3 messages in 13 ms
11/25 10:18:38.980 [aaa]: [21661]: UUID: 8c000000001e4, ra: 7 (debug): 48f8.b38a.flb0 Vlan:
74, Vlan Name: , Vlan Source: CLI
11/25 10:18:38.980 [aaa]: [21661]: UUID: 8c000000001e4, ra: 7 (debug): 48f8.b38a.flb0

```

```

Session Timeout: 1800
11/25 10:18:38.980 [aaa]: [21661]: UUID: 8c000000001e4, ra: 7 (debug): 48f8.b38a.flb0
IF NUM: 0x80000004
11/25 10:18:38.980 [aaa]: [21661]: UUID: 8c000000001e4, ra: 7 (debug): 48f8.b38a.flb0
Template name:
implicit_deny_v6:implicit_deny:preauth_v6:preauth_v4:IP-Adm-V6-Int-ACL-gldbal:IP-Adm-V4-Int-ACL-gldbal:implicit_deny:l409364070,
URL Present: 1
11/25 10:18:38.980 [aaa]: [21661]: UUID: 8c000000001e4, ra: 7 (debug): 48f8.b38a.flb0 Qos
Level: 5, Qos Level Src: NONE, Qos Input Name: , Qos Input Src: NONE, Qos Output Name: ,
Qos Output Src: NONE
11/25 10:18:38.980 [aaa]: [21661]: UUID: 8c000000001e4, ra: 7 (debug): 48f8.b38a.flb0
*****
11/25 10:18:38.980 [apf-mobile]: [21661]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
Processing the policy bind call from SANET
11/25 10:18:38.981 [apf-mobile]: [21661]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
Device Classification:Applying Session Timeout. State DHCP_REQD
Current SessionTimeout 1800 Updated Timeout 1800

11/25 10:18:38.981 [apf-mobile]: [21661]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
Device Classification: Setting Session Timeout to 1800

11/25 10:18:38.981 [pem]: [21661]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0 Setting
session timeout 1800 on mobile 48f8.b38a.flb0
11/25 10:18:38.981 [apf-mobile-state]: [21661]: UUID: 8c000000001e4, ra: 7 (debug):
48f8.b38a.flb0 Session Timeout is 1800 - starting session timer for the mobile
11/25 10:18:38.981 [pem]: [21661]: UUID: 8c000000001e4, ra: 7 (info): Not applying bind
vlan policy: Policy Vlan 74, Access Vlan 74, MmRole 1

11/25 10:18:38.981 [qos]: [21661]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0 [QOS]
%: Sending native profile info to QoS task
11/25 10:18:38.981 [pem]: [21661]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
0.0.0.0 DHCP_REQD (7) BIND-COMplete with state 7.

11/25 10:18:38.981 [pem]: [21661]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
0.0.0.0 DHCP_REQD (7) State Update from BIND-Incomplete to BIND-Complete, mobility role=Local,
client state=APF_MS_STATE ASSOCIATED
11/25 10:18:38.981 [pem]: [21661]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
0.0.0.0 DHCP_REQD (7) pemAdvanceState2 3944, Adding TMP rule
11/25 10:18:38.981 [pem]: [21661]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
0.0.0.0 DHCP_REQD (7) Adding Fast Path rule
on AP 5087.89be.7420 , slot 1 802.1P = 0

11/25 10:18:38.981 [pem]: [21661]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
0.0.0.0 DHCP_REQD (7) Successfully plumbed mobile rule
11/25 10:18:38.981 [apf-mobile]: [21661]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
Successfully processed the policy bind call from SANET
11/25 10:18:38.981 [pem]: [21652]: UUID: 8c000000001e4, ra: 7 (info): PEM rcv processing
msg Add SCB(3)
11/25 10:18:38.981 [pem]: [21652]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
0.0.0.0, auth_state 7 mmRole Local !!!
11/25 10:18:38.981 [pem]: [21652]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0
***WLCLIENT IIF 0x80000012: adding to FMAN and WDB
11/25 10:18:38.981 [capwap]: [21652]: UUID: 8c000000001e4, ra: 7 (debug): Platform capability
Asic-level-load-balancing is FALSE
11/25 10:18:38.981 [apf-lb]: [21652]: UUID: 8c000000001e4, ra: 7 (info): Platform not
supported
11/25 10:18:38.981 [client]: [21652]: UUID: 8c000000001e4, ra: 7 (debug): IPC_ADD: WLCLIENT:
IIF 0x80000012 send station ADD to FMAN and IOSD
11/25 10:18:38.981 [tdllib]: [21652]: UUID: 8c000000001e4, ra: 7 (debug): marshal: set
uuid 8c000000001e4, ra 7
11/25 10:18:38.982 [client]: [21652]: UUID: 8c000000001e4, ra: 7 (debug): IPC_ADD: WLCLIENT:
IIF 0x80000012 Sending station ADD to FMAN
11/25 10:18:38.982 [client]: [21652]: UUID: 8c000000001e4, ra: 7 (debug): Client bitmap
is 010000000000000010
11/25 10:18:38.982 [client]: [21652]: UUID: 8c000000001e4, ra: 7 (debug): MOBILITY_STATE
set
11/25 10:18:38.982 [client]: [21652]: UUID: 8c000000001e4, ra: 7 (debug):
DYNAMIC POLICY TEMPLATE set
11/25 10:18:38.982 [apf-mobile]: [21652]: UUID: 8c000000001e4, ra: 7 (info): wcm_wdb create:
ipv4_addr = 0.0.0.0
11/25 10:18:38.982 [apf-mobile]: [21652]: UUID: 8c000000001e4, ra: 7 (info): wcm_wdb create:
numv6 address = 0
11/25 10:18:38.982 [apf-mobile]: [21652]: UUID: 8c000000001e4, ra: 7 (info): Setting WCDB

```

```
VLAN to 74
11/25 10:18:38.982 [tdllib]: [21652]: UUID: 8c000000001e4, ra: 7 (debug): marshal: set
uuid 8c000000001e4, ra 7
11/25 10:18:38.982 [apf-mobile]: [21652]: UUID: 8c000000001e4, ra: 7 (info): WLCLIENT:
wcm_wdb client creation message was sent successfully
11/25 10:18:38.982 [client]: [21652]: UUID: 8c000000001e4, ra: 7 (debug): IPC_UPDATE:
IIF 0x800000012 Sending station ADD to IOSD
11/25 10:18:38.982 [pem]: [21652]: UUID: 8c000000001e4, ra: 7 (info): 48f8.b38a.flb0 Tclas
Plumb needed: 0
11/25 10:18:38.982 [qos-ipc]: [21623]: UUID: 8c000000001e4, ra: 7 (info): [QOS-IPC] %:
QOS_HANDLE_NATIVE_PROFILE_CLIENT_POLICY_POST_RUN: 20 Recvd.
11/25 10:18:38.982 [qos-ipc]: [21623]: UUID: 8c000000001e4, ra: 7 (info): [QOS-IPC] %:
Regular QoS requests can be processed...
11/25 10:18:39.133 [tdllib]: [21661]: UUID: 8c000000001ed, ra: 7 (debug): unmarshal: got
uuid 8c000000001ed, ra 7
11/25 10:18:39.133 [cond_debug]: [21661]: UUID: 8c000000001ed, ra: 7 (info): Search
condition: ft id 43, cond: type 16, fmt 2, id: 0x48f8b38a, name: H□□□□
11/25 10:18:39.133 [cond_debug]: [21661]: UUID: 8c000000001ed, ra: 7 (info): Condition
found
11/25 10:18:39.133 [wcm]: [21661]: UUID: 8c000000001ee, ra: 7 (appctx): mac
48:f8:b3:8a:fl:b0
11/25 10:18:39.133 [apf-mobile]: [21661]: UUID: 8c000000001ee, ra: 7 (info): 48f8.b38a.flb0
wcm_wdb received ip binding message: client mac 48f8.b38a.flb0, ip learn type 2, v4/v6 0,
ipv6 address 9.5.74.106 , ipv6 address 0000:0000:0000:0000:0000:0000:0000:0000, add/delete
1, options length 0, subnet vlan 74
11/25 10:18:39.133 [apf-mobile]: [21661]: UUID: 8c000000001ee, ra: 7 (info): 48f8.b38a.flb0
wcm_wdb ip binding message was processed
11/25 10:18:39.133 [apf-mobile]: [21661]: UUID: 8c000000001ee, ra: 7 (info): 48f8.b38a.flb0
WcdbClientUpdate: IP Binding from WCDB ip learn type 2, add_or_delete 1
11/25 10:18:39.133 [apf-mobile]: [21661]: UUID: 8c000000001ee, ra: 7 (info): 48f8.b38a.flb0
IPv4 Addr: 9:5:74:106

11/25 10:18:39.133 [pem]: [21661]: UUID: 8c000000001ee, ra: 7 (info): 48f8.b38a.flb0 MS
got the IP, resetting the Reassociation Count 0 for client
11/25 10:18:39.133 [apf-lb]: [21661]: UUID: 8c000000001ee, ra: 7 (info): 48f8.b38a.flb0
fap IP change from 0 to 9054a6a for client 48f8.b38a.flb0
11/25 10:18:39.133 [apf-mobile]: [21661]: UUID: 8c000000001ee, ra: 7 (info): In
apfHaIpChangeAfterRunChkpt: ssoClientHaFlag 0x0, IP 0x9054a6a 48f8.b38a.flb0
11/25 10:18:39.133 [apf-mobile]: [21661]: UUID: 8c000000001ee, ra: 7 (info): 48f8.b38a.flb0
***WLCLIENT IIF 0x800000012: IP address updated. Set flag for IPADDR_INFO
11/25 10:18:39.133 [pem-state]: [21661]: UUID: 8c000000001ee, ra: 7 (debug): 48f8.b38a.flb0
Moving to webauth state, URL Flag is set
11/25 10:18:39.133 [pem-state]: [21661]: UUID: 8c000000001ee, ra: 7 (debug): 48f8.b38a.flb0
Change state to WEBAUTH_REQD (8) last state DHCP_REQD (7)

11/25 10:18:39.133 [capwap]: [21661]: UUID: 8c000000001ee, ra: 7 (debug): Platform capability
Asic-level-load-balancing is FALSE
11/25 10:18:39.133 [apf-lb]: [21661]: UUID: 8c000000001ee, ra: 7 (info): Platform not
supported
11/25 10:18:39.133 [client]: [21661]: UUID: 8c000000001ee, ra: 7 (debug): IPC_UPDATE:
WLCLIENT: IIF 0x800000012 send station UPDATE to FMAN and IOSD
11/25 10:18:39.134 [tdllib]: [21661]: UUID: 8c000000001ee, ra: 7 (debug): marshal: set
uuid 8c000000001ee, ra 7
11/25 10:18:39.134 [client]: [21661]: UUID: 8c000000001ee, ra: 7 (debug): IPC_UPDATE:
WLCLIENT: IIF 0x800000012 Sending station UPDATE to FMAN
11/25 10:18:39.134 [client]: [21661]: UUID: 8c000000001ee, ra: 7 (debug): Client bitmap
is 00100000010000010
11/25 10:18:39.134 [client]: [21661]: UUID: 8c000000001ee, ra: 7 (debug): AUTH STATE set
11/25 10:18:39.134 [client]: [21661]: UUID: 8c000000001ee, ra: 7 (debug): IPADDR_INFO set
11/25 10:18:39.134 [client]: [21661]: UUID: 8c000000001ee, ra: 7 (debug):
DYNAMIC POLICY TEMPLATE set
11/25 10:18:39.134 [client]: [21661]: UUID: 8c000000001ee, ra: 7 (debug): Not sending IP
address in WDB update for local/anchor case
11/25 10:18:39.134 [apf-mobile]: [21661]: UUID: 8c000000001ee, ra: 7 (info): wcm_wdb create:
ipv4_addr = 0.0.0.0
11/25 10:18:39.134 [apf-mobile]: [21661]: UUID: 8c000000001ee, ra: 7 (info): wcm_wdb update:
numv6 address = 0
11/25 10:18:39.134 [tdllib]: [21661]: UUID: 8c000000001ee, ra: 7 (debug): marshal: set
uuid 8c000000001ee, ra 7
11/25 10:18:39.134 [apf-mobile]: [21661]: UUID: 8c000000001ee, ra: 7 (info): WLCLIENT:
wcm_wdb client update message was sent successfully
11/25 10:18:39.134 [client]: [21661]: UUID: 8c000000001ee, ra: 7 (debug): IPC_UPDATE:
WLCLIENT: IIF 0x800000012 Sending station UPDATE to IOSD
```

```

11/25 10:18:39.134 [apf-mobile]: [21661]: UUID: 8c000000001ee, ra: 7 (info): 48f8.b38a.flb0
  Sending IPv4 update to Controller 9.5.74.10
11/25 10:18:39.134 [sim-cs]: [21661]: UUID: 8c000000001ee, ra: 7 (info): System IP addr :
  9.5.74.10
11/25 10:18:39.134 [sim-cs]: [21661]: UUID: 8c000000001ee, ra: 7 (info): System IP addr :
  9.5.74.10
11/25 10:18:39.134 [mob-handoff]: [21661]: UUID: 8c000000001ee, ra: 7 (debug): 48f8.b38a.flb0
  mmBuildSendClientUpdate: destIp:9.5.74.10, destType:2 callType:1
11/25 10:18:39.134 [mob-handoff]: [21661]: UUID: 8c000000001ee, ra: 7 (debug): 48f8.b38a.flb0
  mmBuildMsgUpdateIpPayload:3938 Sending msg with new client IP 9.5.74.106
11/25 10:18:39.134 [mob-handoff]: [21661]: UUID: 8c000000001ee, ra: 7 (debug): 48f8.b38a.flb0
  [1693: Client Update MA->MC] to 9.5.74.10:16666
11/25 10:18:39.135 [apf-mobile]: [21661]: UUID: 8c000000001ee, ra: 7 (info): 48f8.b38a.flb0
  Assigning Address 9.5.74.106 to mobile
11/25 10:18:39.135 [mob-handoff]: [22238]: UUID: 8c000000001ee, ra: 7 (debug): 48f8.b38a.flb0
  [1693: Client Update MA->MC] from 9.5.74.10:16666
11/25 10:18:39.135 [cond_debug]: [22238]: UUID: 8c000000001ee, ra: 7 (info): Search
  condition: ft_id 43, cond: type 16, fmt 2, id: 0x48f8b38a, name: H□□□□
11/25 10:18:39.135 [cond_debug]: [22238]: UUID: 8c000000001ee, ra: 7 (info): Condition
  found
11/25 10:18:39.135 [wcm]: [22238]: UUID: 8c000000001ef, ra: 7 (appctx): mac
  48:f8:b3:8a:f1:b0
11/25 10:18:39.135 [mob-handoff]: [22238]: UUID: 8c000000001ef, ra: 7 (debug): 48f8.b38a.flb0
  Updating client IPv4 address: 9.5.74.106 . Client learn type: 2.
11/25 10:18:40.637 [mgmt infra]: [17333]: UUID: 0, ra: 0 (ERR): Failed to get values
11/25 10:19:09.814 [dtls]: [21631]: UUID: 8c0000000020d, ra: 7 (debug):
  openssl_dtls_connection_find_using_link_info: DTLS connection find with Local 9.5.74.10:5246
  Peer 9.5.74.101:7759
11/25 10:19:09.814 [dtls]: [21631]: UUID: 8c0000000020d, ra: 7 (debug): 5087.89be.7420
  DTLS connection found! Acquiring lock for 0xffed6f8378
11/25 10:19:09.814 [smrcl]: [17333]: UUID: 8c0000000020d, ra: 7 (debug):
  ipc(mqipc/wcm/smd-wcm):End of MQIPC queue with 2 messages in 2 ms
11/25 10:19:09.814 [dtls]: [21631]: UUID: 8c0000000020d, ra: 7 (debug): 5087.89be.7420
  Releasing lock for 0xffed6f8378
11/25 10:19:09.815 [aaa]: [21631]: UUID: 8c0000000020d, ra: 7 (debug): 48f8.b38a.flb0
  FQDN-REPORT: Unregister success in sending URL msg snooping = 0 to AP 5087.89be.7420, slot
  = 1
11/25 10:19:09.824 [tdllib]: [17333]: UUID: 8c0000000020d, ra: 7 (debug): unmarshal: got
  uuid 8c0000000020d, ra 7
11/25 10:19:09.824 [wcm]: [17333]: UUID: 8c0000000020d, ra: 7 (debug): AAA-Proxy attr list
  alloc: Created attribute list = (090000B9)
11/25 10:19:09.824 [smrcl]: [17333]: UUID: 8c0000000020d, ra: 7 (debug): EEDGE-RCL:
  policy_src[0] in rcl_sm_handler is : [0]
11/25 10:19:09.824 [smrcl]: [17333]: UUID: 8c0000000020d, ra: 7 (debug): EEDGE-RCL:
  policy_src[1] in rcl_sm_handler is : [0]
11/25 10:19:09.824 [smrcl]: [17333]: UUID: 8c0000000020d, ra: 7 (debug): EEDGE-RCL:
  policy_src[2] in rcl_sm_handler is : [0]
11/25 10:19:09.824 [smrcl]: [17333]: UUID: 8c0000000020d, ra: 7 (debug): EEDGE-RCL:
  policy_src[3] in rcl_sm_handler is : [4]
11/25 10:19:09.824 [aaa]: [17333]: UUID: 8c0000000020d, ra: 7 (debug): AUTHC Callback rcvd
  from SANET, label: 838860839, auth_result:0 bind result:0 eap_type: 0
11/25 10:19:09.824 [aaa]: [17333]: UUID: 8c0000000020d, ra: 7 (debug): SMD policy src[0]:
  0
11/25 10:19:09.824 [aaa]: [17333]: UUID: 8c0000000020d, ra: 7 (debug): Qos source received
  from SMD: 0 ->NONE
11/25 10:19:09.824 [aaa]: [17333]: UUID: 8c0000000020d, ra: 7 (debug): SMD policy src[1]:
  0
11/25 10:19:09.824 [aaa]: [17333]: UUID: 8c0000000020d, ra: 7 (debug): Qos source received
  from SMD: 1 ->NONE
11/25 10:19:09.825 [aaa]: [17333]: UUID: 8c0000000020d, ra: 7 (debug): SMD policy src[2]:
  0
11/25 10:19:09.825 [aaa]: [17333]: UUID: 8c0000000020d, ra: 7 (debug): Qos source received
  from SMD: 2 ->NONE
11/25 10:19:09.825 [aaa]: [17333]: UUID: 8c0000000020d, ra: 7 (debug): SMD policy src[3]:
  4
11/25 10:19:09.825 [aaa]: [17333]: UUID: 8c0000000020d, ra: 7 (debug): Qos source received
  from SMD: 3 ->CLI
11/25 10:19:09.825 [aaa]: [17333]: UUID: 8c0000000020d, ra: 7 (debug): 48f8.b38a.flb0

```



```

***----- Bind policies from EPM -----***
11/25 10:19:09.825 [aaa]: [17333]: UUID: 8c000000020d, ra: 7 (debug): 48f8.b38a.flb0 Vlan:
 74, Vlan Name: VLAN0074, Vlan Source: CLI
11/25 10:19:09.825 [aaa]: [17333]: UUID: 8c000000020d, ra: 7 (debug): 48f8.b38a.flb0
Session Timeout: 1800
11/25 10:19:09.825 [aaa]: [17333]: UUID: 8c000000020d, ra: 7 (debug): 48f8.b38a.flb0
IF_NUM: 0x80000004
11/25 10:19:09.825 [aaa]: [17333]: UUID: 8c000000020d, ra: 7 (debug): 48f8.b38a.flb0
Template name: IP-Adm-V4-LOGOUT-ACL:, URL Present: 0
11/25 10:19:09.825 [aaa]: [17333]: UUID: 8c000000020d, ra: 7 (debug): 48f8.b38a.flb0 Qos
Level: 5, Qos Level Src: NONE, Qos Input Name: , Qos Input Src: NONE, Qos Output Name: ,
Qos Ouput Src: NONE
11/25 10:19:09.825 [aaa]: [17333]: UUID: 8c000000020d, ra: 7 (debug): 48f8.b38a.flb0
***-----***
11/25 10:19:09.825 [aaa]: [17333]: UUID: 8c000000020d, ra: 7 (debug): AVP type=757 len=4
: 0x00000001 (1)
11/25 10:19:09.825 [aaa]: [17333]: UUID: 8c000000020d, ra: 7 (debug): Session Label:
838860839client mac 48f8.b38a.flb0
Auth Results 0

11/25 10:19:09.825 [pem]: [17333]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0
WEBAUTH: received authentication response, status=0
11/25 10:19:09.825 [smrcl]: [17333]: UUID: 8c000000020d, ra: 7 (debug):
ipc(mqipc/wcm/smd-wcm):End of MQIPC queue with 2 messages in 1 ms
11/25 10:19:09.825 [pem]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0
WEBAUTH: Received message from webauth queue: 1
11/25 10:19:09.825 [pem]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0
WEBAUTH: SANET Auth Event - Authentication Success!
11/25 10:19:09.825 [pem]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0 Policy
Source: QOS IN NONE QOS OUT: NONE, VLAN:CLI
11/25 10:19:09.825 [aaa]: [21653]: UUID: 8c000000020d, ra: 7 (debug): 48f8.b38a.flb0
Applying new AAA override for station 48f8.b38a.flb0 AllowOverride 1
11/25 10:19:09.825 [aaa]: [21653]: UUID: 8c000000020d, ra: 7 (debug): 48f8.b38a.flb0
Override Values: source: 48, valid_bits: 0x0101, qosLevel: -1 dscp: 0xffffffff, dot1pTag:
0xffffffff, sessionTimeout: 1800
11/25 10:19:09.825 [aaa]: [21653]: UUID: 8c000000020d, ra: 7 (debug): 48f8.b38a.flb0
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1 rTimeBurstC: -1, vlanIfName: , aclName:
11/25 10:19:09.825 [qos]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0 QoS
policies from SMD: dot1pTag: 0xffffffff, qosLevel: -1, qos-policy-In: , qos-in-src:NONE
qos-policy-out: , qos-out-src:NONE sub-qos-policy-in: sub-qos-policy-out: , sub-policy-in:
sub-policy-out:
11/25 10:19:09.825 [apf-mobile]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0
Clearing Dhcp state for station ---
11/25 10:19:09.825 [pem]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0
Applying WLAN ACL policies to client
11/25 10:19:09.825 [pem]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0 No
Interface ACL used for Wireless client in WCM(NGWC)
11/25 10:19:09.825 [ap-grp]: [21653]: UUID: 8c000000020d, ra: 7 (debug): no location
defined

11/25 10:19:09.825 [apf-mobile]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0
Inserting AAA Override struct for mobile
MAC: 48f8.b38a.flb0 , source 48

11/25 10:19:09.825 [aaa]: [21653]: UUID: 8c000000020d, ra: 7 (debug): 48f8.b38a.flb0
Inserting new RADIUS override into chain for station 48f8.b38a.flb0
11/25 10:19:09.825 [aaa]: [21653]: UUID: 8c000000020d, ra: 7 (debug): 48f8.b38a.flb0
Override Values: source: 48, valid_bits: 0x0101, qosLevel: -1 dscp: 0xffffffff, dot1pTag:
0xffffffff, sessionTimeout: 1800
11/25 10:19:09.825 [aaa]: [21653]: UUID: 8c000000020d, ra: 7 (debug): 48f8.b38a.flb0
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1 rTimeBurstC: -1, vlanIfName: , aclName:
11/25 10:19:09.826 [qos]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0 QoS
policies from SMD: dot1pTag: 0xffffffff, qosLevel: -1, qos-policy-In: , qos-in-src:NONE
qos-policy-out: , qos-out-src:NONE sub-qos-policy-in: sub-qos-policy-out: , sub-policy-in:
sub-policy-out:
11/25 10:19:09.826 [aaa]: [21653]: UUID: 8c000000020d, ra: 7 (debug): 48f8.b38a.flb0
Applying override policy from source Override Summation:

11/25 10:19:09.826 [aaa]: [21653]: UUID: 8c000000020d, ra: 7 (debug): 48f8.b38a.flb0
Override Values: source: 256, valid_bits: 0x0101, qosLevel: -1 dscp: 0xffffffff, dot1pTag:
0xffffffff, sessionTimeout: 1800
11/25 10:19:09.826 [aaa]: [21653]: UUID: 8c000000020d, ra: 7 (debug): 48f8.b38a.flb0
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1 rTimeBurstC: -1, vlanIfName: , aclName:

```

```

11/25 10:19:09.826 [qos]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0 QoS
policies from SMD: dot1pTag: 0xffffffff, qosLevel: -1, qos-policy-In: , qos-in-src:NONE
qos-policy-out: , qos-out-src:NONE sub-qos-policy-in: sub-qos-policy-out: , sub-policy-in:
sub-policy-out:
11/25 10:19:09.826 [pem]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0 Setting
session timeout 1800 on mobile 48f8.b38a.flb0
11/25 10:19:09.826 [apf-mobile-state]: [21653]: UUID: 8c000000020d, ra: 7 (debug):
48f8.b38a.flb0 Session Timeout is 1800 - starting session timer for the mobile
11/25 10:19:09.826 [pem]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0
client incoming attribute size are 675
11/25 10:19:09.826 [pem]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0
WEBAUTH: received RADIUS attr type 450
11/25 10:19:09.826 [aaa]: [21653]: UUID: 8c000000020d, ra: 7 (debug): AVP type=450 len=5
: admin
11/25 10:19:09.826 [apf-mobile]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0
Username entry (admin) created for mobile
11/25 10:19:09.826 [pem]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0
WEBAUTH: received RADIUS attr type 958
11/25 10:19:09.826 [pem]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0
WEBAUTH: received RADIUS attr type 960
11/25 10:19:09.826 [pem]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0
WEBAUTH: received RADIUS attr type 42
11/25 10:19:09.826 [pem]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0
WEBAUTH: received RADIUS attr type 8
11/25 10:19:09.826 [pem]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0
WEBAUTH: received RADIUS attr type 1208
11/25 10:19:09.826 [pem]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0
WEBAUTH: received RADIUS attr type 819
11/25 10:19:09.826 [pem]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0
WEBAUTH: received RADIUS attr type 220
11/25 10:19:09.826 [pem]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0
WEBAUTH: received RADIUS attr type 952
11/25 10:19:09.826 [pem]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0
WEBAUTH: received RADIUS attr type 600
11/25 10:19:09.826 [pem]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0
WEBAUTH: received RADIUS attr type 685
11/25 10:19:09.826 [pem]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0
WEBAUTH: received RADIUS attr type 221
11/25 10:19:09.826 [pem]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0
WEBAUTH: received RADIUS attr type 225
11/25 10:19:09.826 [pem]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0
WEBAUTH: received RADIUS attr type 876
11/25 10:19:09.826 [pem]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0
WEBAUTH: received RADIUS attr type 82
11/25 10:19:09.826 [pem]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0
WEBAUTH: received RADIUS attr type 939
11/25 10:19:09.826 [pem]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0
WEBAUTH: received RADIUS attr type 1193
11/25 10:19:09.826 [pem]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0
WEBAUTH: received RADIUS attr type 335
11/25 10:19:09.826 [pem]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0
WEBAUTH: received RADIUS attr type 757
11/25 10:19:09.826 [pem]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0
WEBAUTH: received RADIUS attr type 42
11/25 10:19:09.826 [pem]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0
WEBAUTH: received RADIUS attr type 1265
11/25 10:19:09.826 [dot1x]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0
apfMsRunStateInc
11/25 10:19:09.826 [pem-state]: [21653]: UUID: 8c000000020d, ra: 7 (debug): 48f8.b38a.flb0
***WLCLIENT IIF 0x80000012: Client is going to RUN state.Set flag for AUTH_STATE update.
11/25 10:19:09.827 [pem-state]: [21653]: UUID: 8c000000020d, ra: 7 (debug): 48f8.b38a.flb0
Change state to RUN (20) last state WEBAUTH_REQD (8)

11/25 10:19:09.827 [snmp-trap]: [21653]: UUID: 8c000000020d, ra: 7 (debug):
80211ClientMovedToRunStateTrap called
11/25 10:19:09.827 [apf-rogue-client]: [21653]: UUID: 8c000000020d, ra: 7 (info):
48f8.b38a.flb0 APF notify RogueTask about client association: 48f8.b38a.flb0

11/25 10:19:09.827 [apf-mobile]: [21653]: UUID: 8c000000020d, ra: 7 (info): 48f8.b38a.flb0
Stopping deletion of Mobile Station: (callerId: 74)
11/25 10:19:09.827 [apf-rogue]: [22288]: UUID: 8c000000020d, ra: 7 (info): rogueTask:
Processing apfMsgTypeNotifyClientAssoc
11/25 10:19:09.827 [apf-mobile-state]: [21653]: UUID: 8c000000020d, ra: 7 (debug):

```

```
48f8.b38a.flb0 Session Timeout is 1800 - starting session timer for the mobile
11/25 10:19:09.827 [pem]: [21653]: UUID: 8c0000000020d, ra: 7 (info): 48f8.b38a.flb0
9.5.74.106 RUN (20) Reached PLUMBFASPATH: from line 4487
11/25 10:19:09.827 [pem]: [21653]: UUID: 8c0000000020d, ra: 7 (info): 48f8.b38a.flb0
9.5.74.106 RUN (20) Replacing Fast Path rule
    on AP 5087.89be.7420 , slot 1 802.1P = 0

11/25 10:19:09.827 [aaa]: [21653]: UUID: 8c0000000020d, ra: 7 (debug): 48f8.b38a.flb0 AAAS:
  acct method list NOT configured for WLAN 4, accounting skipped
11/25 10:19:09.827 [pem]: [21653]: UUID: 8c0000000020d, ra: 7 (info): 48f8.b38a.flb0
9.5.74.106 RUN (20) Successfully plumbed mobile rule
11/25 10:19:09.827 [pem]: [21652]: UUID: 8c0000000020d, ra: 7 (info): PEM rcv processing
msg Add SCB(3)
11/25 10:19:09.827 [capwap]: [21653]: UUID: 8c0000000020d, ra: 7 (debug): Platform capability
  Asic-level-load-balancing is FALSE
11/25 10:19:09.827 [apf-lb]: [21653]: UUID: 8c0000000020d, ra: 7 (info): Platform not
supported
11/25 10:19:09.827 [client]: [21653]: UUID: 8c0000000020d, ra: 7 (debug): IPC_UPDATE:
WLCLIENT: IIF 0x80000012 send station UPDATE to FMAN and IOSD
11/25 10:19:09.827 [tdllib]: [21653]: UUID: 8c0000000020d, ra: 7 (debug): marshal: set
  uuid 8c0000000020d, ra 7
11/25 10:19:09.827 [client]: [21653]: UUID: 8c0000000020d, ra: 7 (debug): IPC_UPDATE:
WLCLIENT: IIF 0x80000012 Sending station UPDATE to FMAN
11/25 10:19:09.827 [client]: [21653]: UUID: 8c0000000020d, ra: 7 (debug): Client bitmap
  is 001000000000000010
11/25 10:19:09.827 [client]: [21653]: UUID: 8c0000000020d, ra: 7 (debug): AUTH_STATE set
11/25 10:19:09.827 [client]: [21653]: UUID: 8c0000000020d, ra: 7 (debug):
DYNAMIC_POLICY_TEMPLATE set
11/25 10:19:09.827 [client]: [21653]: UUID: 8c0000000020d, ra: 7 (debug): Not sending IP
  address in WDB update for local/anchor case
11/25 10:19:09.827 [apf-mobile]: [21653]: UUID: 8c0000000020d, ra: 7 (info): wcm_wdb create:
  ipv4_addr = 0.0.0.0
11/25 10:19:09.827 [apf-mobile]: [21653]: UUID: 8c0000000020d, ra: 7 (info): wcm_wdb update:
  numv6 address = 0
11/25 10:19:09.828 [tdllib]: [21653]: UUID: 8c0000000020d, ra: 7 (debug): marshal: set
  uuid 8c0000000020d, ra 7
11/25 10:19:09.828 [apf-mobile]: [21653]: UUID: 8c0000000020d, ra: 7 (info): WLCLIENT:
  wcm_wdb client update message was sent successfully
11/25 10:19:09.828 [client]: [21653]: UUID: 8c0000000020d, ra: 7 (debug): IPC_UPDATE:
WLCLIENT: IIF 0x80000012 Sending station UPDATE to IOSD
11/25 10:19:09.828 [qos]: [21653]: UUID: 8c0000000020d, ra: 7 (info): [QOS] %: IPC_UPDATE:
  client is in RUN state, check for QoS trigger
11/25 10:19:09.828 [qos]: [21653]: UUID: 8c0000000020d, ra: 7 (info): 48f8.b38a.flb0 [QOS]
  %: Client becomes present, install QoS policy
11/25 10:19:09.828 [qos]: [21653]: UUID: 8c0000000020d, ra: 7 (info): 48f8.b38a.flb0 [QOS]
  %: Send QOS_CLIENT_JOIN_MSG to QoS Task, len 6
11/25 10:19:09.828 [pem]: [21653]: UUID: 8c0000000020d, ra: 7 (info): 48f8.b38a.flb0
WEBAUTH: callback status - AuthC successfully processed
11/25 10:19:09.828 [qos-ipc]: [21623]: UUID: 8c0000000020d, ra: 7 (info): [QOS-IPC] %:
  QoS_CLIENT_JOIN Msg: 13 Recvd.
```




Dynamic VLAN Assignment with Converged Access and ACS 5.2 Configuration Example

This document describes the concept of dynamic VLAN assignment and how to configure wireless LAN controller (WLC) and a RADIUS server to assign a wireless LAN (WLAN) clients to a specific VLAN dynamically. In this document, the RADIUS server is an Access Control Server (ACS) that runs Cisco Secure Access Control System Version 5.2.roduction

- [Prerequisites, page 129](#)
- [Dynamic VLAN Assignment , page 130](#)
- [Configuring Dynamic VLAN Assignment, page 130](#)
- [Verifying the Dynamic VLAN Assignment with Converged Access Configuration, page 140](#)
- [Troubleshooting the Dynamic VLAN Assignment Configuration Issues, page 142](#)

Prerequisites

We recommend that you have basic and functional knowledge on following topics:

- WLC and Lightweight Access Points (LAPs)
- Authentication, Authorization and Accounting (AAA) server
- Wireless networks and wireless security issues

Supported Platforms and Releases

The information in this document is based on the following:

- Cisco Catalyst 3850 series Switches Wireless LAN Controller with Cisco IOS[®] XE Software Release 3.2.2
- Cisco Aironet 3600 Series Lightweight Access Point
- Microsoft Windows XP with Intel Proset Supplicant

- Cisco Secure Access Control System Version 5.2
- Cisco Catalyst 3500 Series Switches

**Note**

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Dynamic VLAN Assignment

In most WLAN systems, each WLAN has a static policy that applies to all clients associated with a Service Set Identifier (SSID), or WLAN in the controller terminology. Although this static policy is powerful, it has some limitations since it requires clients to associate with different SSIDs in order to inherit different QoS and security policies.

Cisco WLAN solution supports identity networking that allows the network to advertise a single SSID, only for specific users to inherit different QoS, VLAN attributes, and/or security policies based on the user credentials.

Dynamic VLAN assignment is one such feature that places a wireless user into a specific VLAN, based on the credentials supplied by the user. This task of user assignment to a specific VLAN is handled by a RADIUS authentication server, i.e. a Cisco Secure ACS. This feature can be used, for example, in order to allow the wireless host to remain on the same VLAN as it moves within a campus network.

As a result, when a client attempts to associate to a LAP registered with a controller, the LAP passes the credentials of the user to the RADIUS server for validation. Once the authentication is successful, the RADIUS server passes certain Internet Engineering Task Force (IETF) attributes to the user. These RADIUS attributes decide the VLAN ID that should be assigned to the wireless client. The SSID of the client (the WLAN, in terms of the WLC) does not matter because the user is always assigned to this predetermined VLAN ID.

The RADIUS user attributes used for the VLAN ID assignment are:

- IETF 64 (Tunnel Type) - Set to VLAN.
- IETF 65 (Tunnel Medium Type) - Set to 802.
- IETF 81 (Tunnel-Private-Group-ID) - Set to the VLAN ID.
- The VLAN ID is 12 bits and takes a value between 1 and 4094 (inclusive of both 1 and 4094). The Tunnel-Private-Group-ID is of type string for use with IEEE 802.1X. Therefore, the VLAN ID integer value is encoded as a string. When these tunnel attributes are sent, it is necessary to fill in the Tag field.

As noted in RFC2868, section 3.1—The Tag field is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same tunnel.

Valid values for the Tag field are 0x01 through 0x1F, inclusive. If the Tag field is unused, it must be zero (0x00). Refer to RFC 2868 for more information on all RADIUS attributes.

Configuring Dynamic VLAN Assignment

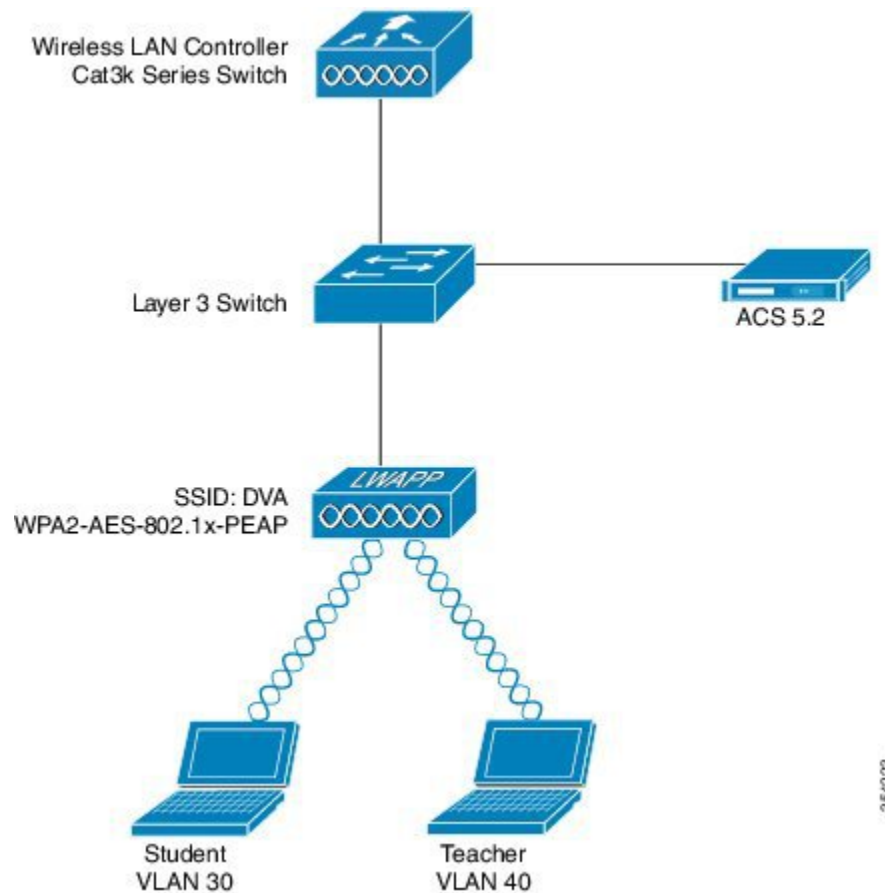
Configuring dynamic VLAN assignment is a two-step process which includes:

- Configuring WLC with the Command-Line Interface (CLI) or with the Graphical User Interface (GUI).
- Configuring RADIUS server.

Network Diagram of Dynamic VLAN Assignment

The following figure shows the network setup of Dynamic VLAN Assignment with Converged Access and ACS 5.2

Figure 27: Network setup of Dynamic VLAN Assignment with Converged Access



Security mechanism used in this document is 802.1X with Protected Extensible Authentication Protocol (PEAP).

Make sure the following tasks are completed before you start with configuration:

- Switches are configured for all Layer 3 (L3) VLANs.
- The DHCP server is assigned a DHCP scope.
- L3 connectivity exists between all devices in the network.
- The LAP is already joined to the WLC.

- Each VLAN has a /24 mask.
- ACS 5.2 has a self-signed certificate installed.

Configuring WLC (CLI)

This section shows configuring WLAN, RADIUS Server and DHCP Pool for Client VLAN.

Configuring WLAN

The following example shows how WLAN is configured with the SSID of DVA:

```
wlan DVA 3 DVA
aaa-override
client vlan VLAN0020
security dot1x authentication-list ACS
session-timeout 1800
no shutdown
```

Configuring RADIUS Server on WLC

Configuring the RADIUS server on WLC is shown in the below example:

```
aaa new-model
!
!
aaa group server radius ACS
server name ACS
!
aaa authentication dot1x ACS group ACS

radius server ACS
address ipv4 10.106.102.50 auth-port 1645 acct-port 1646
key Cisco123

dot1x system-auth-control
```

Configuring DHCP Pool for Client VLAN

This is an example to configure DHCP pool for the client VLAN 30 and VLAN 40:

```
interface Vlan30
ip address 30.30.30.1 255.255.255.0
!
interface Vlan40
ip address 40.40.40.1 255.255.255.0

ip dhcp pool vla30
network 30.30.30.0 255.255.255.0
default-router 30.30.30.1
!
ip dhcp pool vlan40
network 40.40.40.0 255.255.255.0
default-router 40.40.40.1

ip dhcp snooping vlan 30,40
ip dhcp snooping
```


Configuring WLAN (GUI)

Perform the following tasks to configure WLAN.

Step 1 Navigate to **Configuration > Wireless > WLAN > NEW**.

Figure 28: Configuring WLAN window



- Step 2** Click the **General** tab to verify that the WLAN is configured for WPA2-802.1X, and Interface / Interface Group (G) is mapping to *VLAN 20 (VLAN0020)*.

Figure 29: Verifying the WLAN configuration

WLAN
WLAN > Edit

General Security QOS Advanced

Profile Name DVA

Type WLAN

SSID DVA

Status

Security Policies [WPA2][Auth(802.1x)]
(Modifications done under security tab will appear after applying the changes.)

Radio Policy All

Interface/Interface Group(G) VLAN0020

Broadcast SSID

Multicast VLAN Feature

354225

- Step 3** To enable the AAA Override, click the **Advanced** tab and check **Allow AAA Override** check box.

Figure 30: Enabling the AAA Override

WLAN
WLAN > Edit

General Security QOS Advanced

Allow AAA Override

Coverage Hole Detection

Session Timeout (secs) 1800

354226

- Step 4** Click the **Layer2** tab under the **Security** tab, and check **AES** check box as WPA2 Encryption.
- Step 5** Choose **802.1x** as **Auth Key Mgmt** from drop-down list.

Figure 31: Selecting the Auth Key Management

The screenshot shows the WLAN configuration interface. At the top, there are tabs for General, Security, QOS, and Advanced. Under the Security tab, there are sub-tabs for Layer2, Layer3, and AAA Server. The Layer2 sub-tab is selected. Below the sub-tabs, there are fields for Layer 2 Security (set to WPA + WPA2) and MAC Filtering. The WPA+WPA2 Parameters section includes checkboxes for WPA Policy (unchecked), WPA2 Policy (checked), and WPA2 Encryption (checked). The WPA2 Encryption options are AES (checked) and TKIP (unchecked). The Auth Key Mgmt dropdown menu is set to 802.1x. A vertical ID number 354227 is visible on the right side of the screenshot.

Configuring RADIUS Server on WLC (GUI)

The following section describes how to configure RADIUS server on WLC.

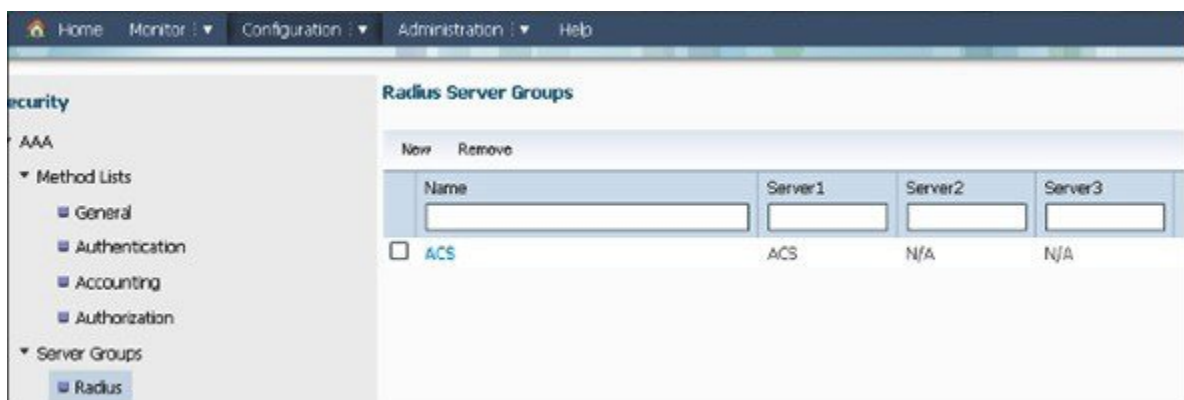
Step 1 Navigate to **Configuration > Security**.

Figure 32: Configuring Radius Server on WLC



Step 2 To create the Radius Server Groups, navigate to **AAA > Server Groups > Radius** (In this example, the Radius Server Group is named as ACS).

Figure 33: Creating radius server group



Step 3 Edit the Radius Server entry to add the Server IP Address and the Shared Secret.

Figure 34: Editing radius server

The screenshot shows the Cisco Wireless Controller GUI. The navigation menu includes Home, Monitor, Configuration, Administration, and Help. The left sidebar shows the Security menu with options for AAA, Method Lists, Server Groups, and RADIUS. The main content area is titled 'Radius Servers' and shows the configuration for a server named 'ACS'. The fields are as follows:

Server Name	ACS
Server IP Address	10.106.102.50
Shared Secret
Confirm Shared Secret
Acct Port (0-65535)	1646
Auth Port (0-65535)	1645
Server Timeout (0-1000) secs	
Retry Count (0-100)	

354229

Note The Shared Secret entered must be same as Shared Secret on the WLC and the RADIUS server.

Step 4 The following figure shows, example of a complete configuration of Radius Server on WLC.

Figure 35: Radius server example

The screenshot shows the 'Radius Servers' configuration page with a table of servers. The table has columns for Server Name, Address, Auth Port, and Acct Port. There are 'New' and 'Remove' buttons at the top. The table contains one entry for 'ACS'.

Server Name	Address	Auth Port	Acct Port
<input type="checkbox"/> ACS	10.106.102.50	1645	1646

354230

Configuring RADIUS Server

Perform the following tasks to configure the RADIUS server.

- Step 1** On the RADIUS server, navigate to **Users and Identity Stores > Internal Identity Stores > Users**.
- Step 2** Create the appropriate User Names and Identity Groups. In this example, student and teacher are created as Usernames and similarly All Groups:Students, and AllGroups:Teachers are created as Identity Groups.

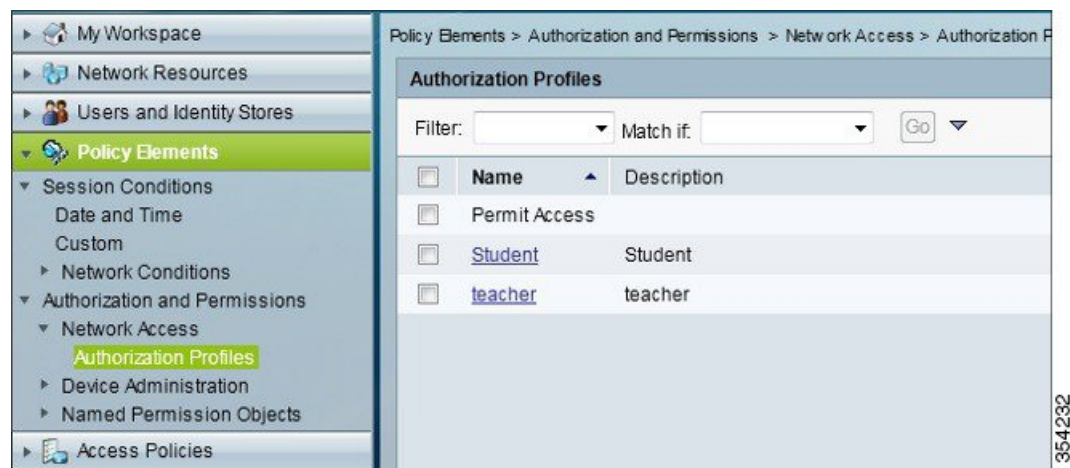
Figure 36: Creating user names and identity groups



354231

- Step 3** Create the Authorization Profiles for AAA override by navigating to **Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles**.

Figure 37: Creating the auth profile



354232

Step 4 Edit the Authorization Profile for Student.

Figure 38: Editing the auth profile

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "Student"

General Common Tasks RADIUS Attributes

Name: Student

Description: Student

= Required fields

354233

Step 5 Set the VLAN ID/Name as **Static** using drop-down list and a Value of 30 (VLAN 30) for student.

Figure 39: Setting the VLAN

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "Student"

General Common Tasks RADIUS Attributes

ACLS

Downloadable ACL Name: Not in Use

Filter-ID ACL: Not in Use

Proxy ACL: Not in Use

Voice VLAN

Permission to Join: Not in Use

VLAN

VLAN ID/Name: Static Value 30

Reauthentication

Reauthentication Timer: Not in Use

Maintain Connectivity during Reauthentication:

QOS

Input Policy Map: Not in Use

Output Policy Map: Not in Use

802.1X-REV

LinkSec Security Policy: Not in Use

URL Redirect

When a URL is defined for Redirect an ACL must also be defined

URL for Redirect: Not in Use

URL Redirect ACL: Not in Use

= Required fields

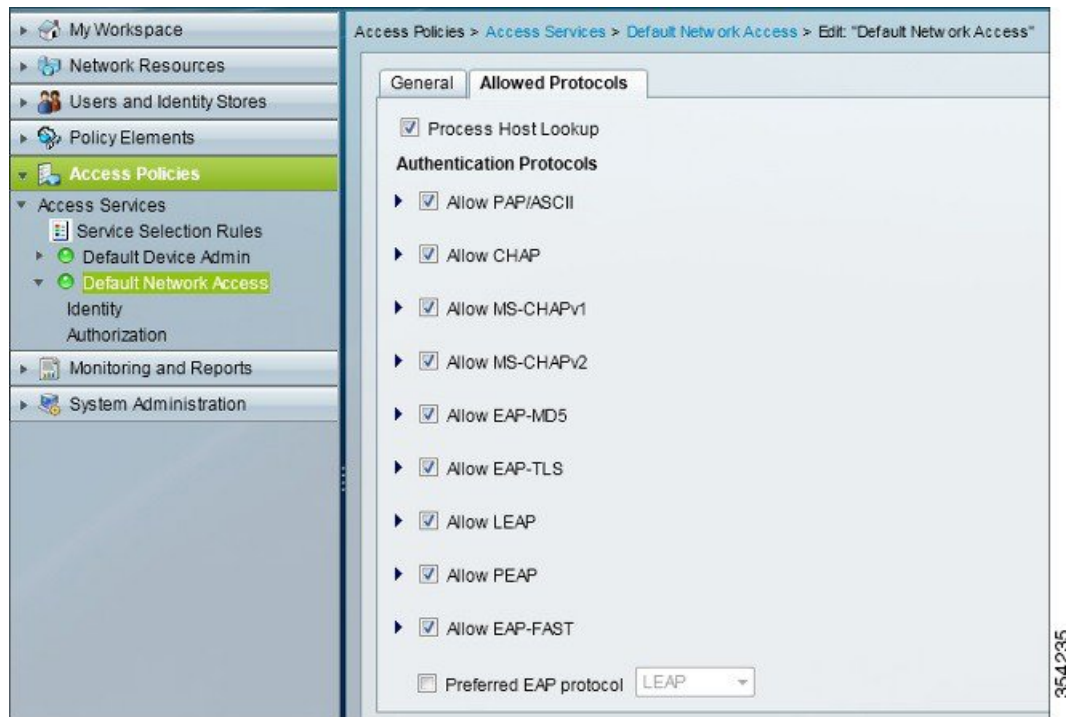
354234

Step 6 Similarly, edit the Authorization Profile for Teacher.

Step 7 Set the VLAN ID / Name as **Static** from drop-down list and a Value of 40 (VLAN 40) for teacher.

- Step 8** Navigate to **Access Policies > Access Services > Default Network Access**, and click the **Allowed Protocols**. Check the **Allow PEAP** checkbox.

Figure 40: Selecting allowed protocols



- Step 9** Define the rules in order to allow PEAP users by navigating to **Identity**.
- Step 10** Map Student and Teacher to the Authorization Policy by navigating to **Authorization**. In this configuration we mapped Student for VLAN30 and Teacher for VLAN 40.

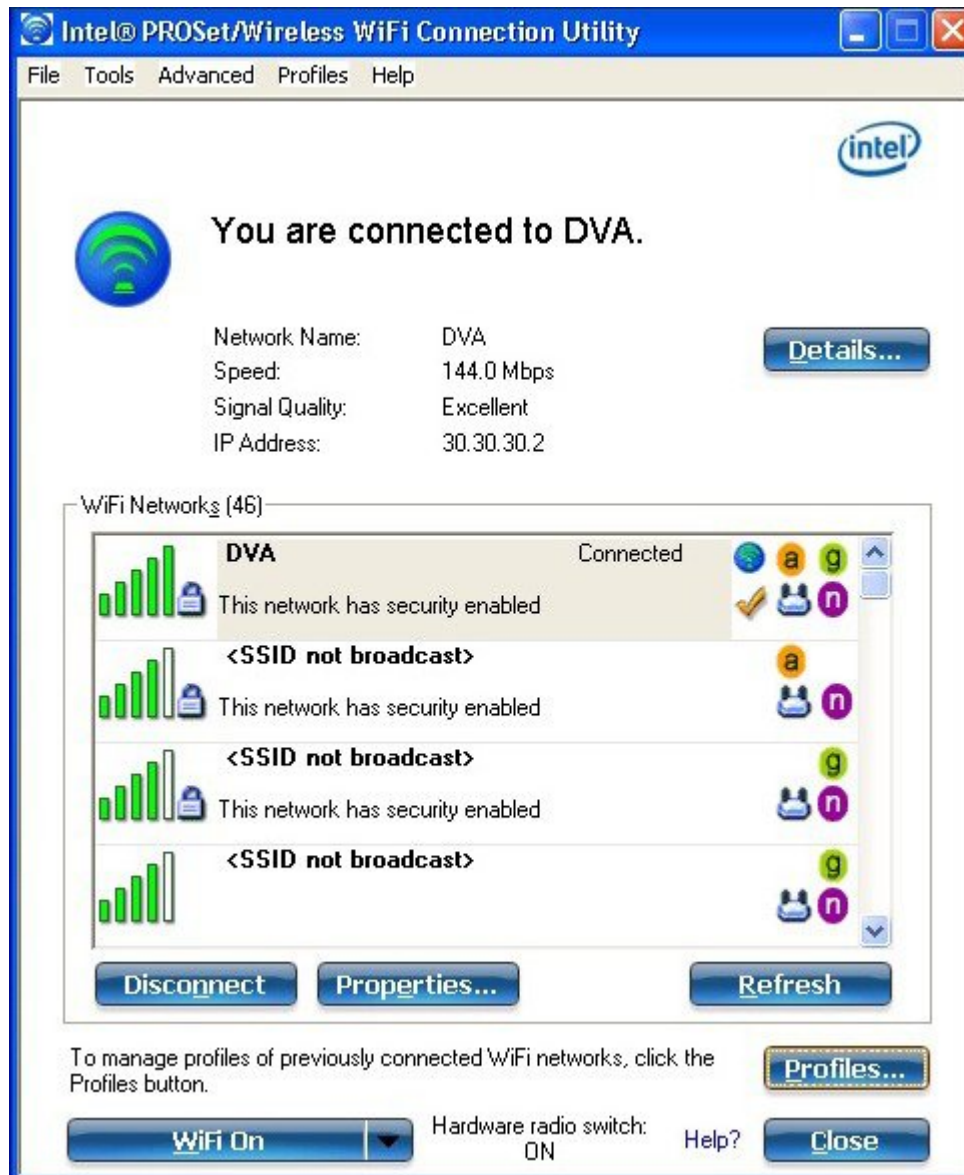
Verifying the Dynamic VLAN Assignment with Converged Access Configuration

Perform the following task in order to verify Dynamic VLAN assignment with Converged Access configuration.

- Step 1** Monitor the page on the ACS that shows which clients are authenticated.

Step 2 Connect to the DVA WLAN with Student Group, and review the client WiFi Connection Utility.

Figure 41: Connecting to the DVA WLAN



Step 3 Similarly, connect to the DVA WLAN with the Teacher Group, and review the client WiFi Connection Utility.

Troubleshooting the Dynamic VLAN Assignment Configuration Issues

This section provides troubleshoot information of Dynamic VLAN Assignment with Converged Access configuration.



Note

Refer to [Important Information on Debug Commands](#) before you use debug commands.

Useful debugs include **debug client mac-address mac**, as well as the following Converged Access trace commands:

- **set trace group-wireless-client level debug**
- **set trace group-wireless-client filter mac** XXXX.XXXX.XXXX
- **show trace sys-filtered-traces**

The Converged Access trace does not include dot1x/AAA, so use this entire list of combined traces for dot1x/AAA:

- **set trace group-wireless-client level debug**
- **set trace wcm-dot1x event level debug**
- **set trace wcm-dot1x aaa level debug**
- **set trace aaa wireless events level debug**
- **set trace access-session core sm level debug**
- **set trace access-session method dot1x level debug**
- **set trace group-wireless-client filter mac** XXXX.XXXX.XXXX
- **set trace wcm-dot1x event filter mac** XXXX.XXXX.XXXX
- **set trace wcm-dot1x aaa filter mac** XXXX.XXXX.XXXX
- **set trace aaa wireless events filter mac** XXXX.XXXX.XXXX
- **set trace access-session core sm filter mac** XXXX.XXXX.XXXX
- **set trace access-session method dot1x filter mac** XXXX.XXXX.XXXX
- **show trace sys-filtered-traces**

When dynamic VLAN assignment is working correctly, you should see following type of output from the debugs as follows:

```
09/01/13 12:13:28.598 IST 1ccc 5933] 0021.5C8C.C761 1XA: Received Medium tag (0)
Tunnel medium type (6) and Tunnel-Type tag (0) and Tunnel-type (13)
Tunnel-Private-Id (30)
[09/01/13 12:13:28.598 IST 1ccd 5933] 0021.5C8C.C761 Tunnel-Group-Id is 30
[09/01/13 12:13:28.598 IST 1cce 5933] 0021.5C8C.C761 Checking Interface
Change - Current VlanId: 40 Current Intf: VLAN0040 New Intf: VLAN0030 New
GroupIntf: intfChanged: 1
[09/01/13 12:13:28.598 IST 1ccf 5933] 0021.5C8C.C761 Incrementing the
Reassociation Count 1 for client (of interface VLAN0040)
```

```

--More--          [09/01/13 12:13:28.598 IST 1cd0 5933] 0021.5C8C.C761
Clearing Address 40.40.40.2 on mobile
[09/01/13 12:13:28.598 IST 1cd1 5933] 0021.5C8C.C761 Applying new AAA override
for station 0021.5C8C.C761
[09/01/13 12:13:28.598 IST 1cd2 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
vlanIfName: 'VLAN0030', aclName: ''

[09/01/13 12:13:28.598 IST 1cd3 5933] 0021.5C8C.C761 Clearing Dhcp state for
station ---
[09/01/13 12:13:28.598 IST 1cd4 5933] 0021.5C8C.C761 Applying WLAN ACL policies
to client
[09/01/13 12:13:28.598 IST 1cd5 5933] 0021.5C8C.C761 No Interface ACL used for
Wireless client in WCM(NGWC)
[09/01/13 12:13:28.598 IST 1cd6 5933] 0021.5C8C.C761 Inserting AAA Override
struct for mobile
MAC: 0021.5C8C.C761 , source 4

[09/01/13 12:13:28.598 IST 1cd7 5933] 0021.5C8C.C761 Inserting new RADIUS
override into chain for station 0021.5C8C.C761
[09/01/13 12:13:28.598 IST 1cd8 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
vlanIfName: 'VLAN0030', aclName: ''

--More--          [09/01/13 12:13:28.598 IST 1cd9 5933] 0021.5C8C.C761
Applying override policy from source Override Summation:

[09/01/13 12:13:28.598 IST 1cda 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
vlanIfName: 'VLAN0030', aclName: ''

[09/01/13 12:13:28.598 IST 1cdb 5933] 0021.5C8C.C761 Applying local bridging
Interface Policy for station 0021.5C8C.C761 - vlan 30, interface 'VLAN0030'
[09/01/13 12:13:28.598 IST 1cdc 5933] 0021.5C8C.C761 1XA: Setting reauth timeout
to 1800 seconds from WLAN config
[09/01/13 12:13:28.598 IST 1cdd 5933] 0021.5C8C.C761 1XA: Setting reauth timeout
to 1800 seconds
[09/01/13 12:13:28.598 IST 1cde 5933] 0021.5C8C.C761 1XK: Creating a PKC PMKID
Cache entry (RSN 1)
[09/01/13 12:13:28.598 IST 1cdf 5933] 0021.5C8C.C761 1XK: Set Link Secure: 0

[09/01/13 12:08:59.553 IST 1ae1 5933] 0021.5C8C.C761 1XA: Received Medium tag (0)
Tunnel medium type (6) and Tunnel-Type tag (0) and Tunnel-type (13)
Tunnel-Private-Id (40)
[09/01/13 12:08:59.553 IST 1ae2 5933] 0021.5C8C.C761 Tunnel-Group-Id is 40
--More--          [09/01/13 12:08:59.553 IST 1ae3 5933] 0021.5C8C.C761
Checking Interface Change - Current VlanId: 20 Current Intf: VLAN0020 New Intf:
VLAN0040 New GroupIntf: intfChanged: 1
[09/01/13 12:08:59.553 IST 1ae4 5933] 0021.5C8C.C761 Applying new AAA override for
station 0021.5C8C.C761
[09/01/13 12:08:59.553 IST 1ae5 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
vlanIfName: 'VLAN0040', aclName: ''

[09/01/13 12:08:59.553 IST 1ae6 5933] 0021.5C8C.C761 Clearing Dhcp state for
station ---
[09/01/13 12:08:59.553 IST 1ae7 5933] 0021.5C8C.C761 Applying WLAN ACL policies
to client
[09/01/13 12:08:59.553 IST 1ae8 5933] 0021.5C8C.C761 No Interface ACL used for
Wireless client in WCM(NGWC)
[09/01/13 12:08:59.553 IST 1ae9 5933] 0021.5C8C.C761 Inserting AAA Override struct
for mobile
MAC: 0021.5C8C.C761 , source 4

[09/01/13 12:08:59.553 IST 1aea 5933] 0021.5C8C.C761 Inserting new RADIUS override
into chain for station 0021.5C8C.C761
[09/01/13 12:08:59.553 IST 1aeb 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
vlanIfName: 'VLAN0040', aclName: ''
--More--
[09/01/13 12:08:59.553 IST 1aec 5933] 0021.5C8C.C761 Applying override policy
from source Override Summation:

```

```
[09/01/13 12:08:59.553 IST laed 5933] 0021.5C8C.C761 Override values (cont..)
  dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
  vlanIfName: 'VLAN0040', aclName: ''

[09/01/13 12:08:59.553 IST laee 5933] 0021.5C8C.C761 Applying local bridging
  Interface Policy for station 0021.5C8C.C761 - vlan 40, interface 'VLAN0040'
[09/01/13 12:08:59.553 IST laef 5933] 0021.5C8C.C761 1XA: Setting reauth timeout
  to 1800 seconds from WLAN config
[09/01/13 12:08:59.553 IST laf0 5933] 0021.5C8C.C761 1XA: Setting reauth timeout
  to 1800 seconds
[09/01/13 12:08:59.553 IST laf1 5933] 0021.5C8C.C761 1XK: Creating a PKC PMKID
  Cache entry (RSN 1)
```



Configuration Example: External RADIUS Server EAP Authentication

The External RADIUS Server EAP Authentication document explains how to configure a wireless LAN controller (WLC) for Extensible Authentication Protocol (EAP) - Flexible Authentication via Secure Tunneling (FAST) authentication using an external RADIUS server. The External RADIUS Server EAP Authentication configuration uses Cisco Secure Access Control Server (ACS) as the external RADIUS server to authenticate the wireless client.

- [Prerequisites, page 145](#)
- [Configuring External RADIUS Server EAP Authentication, page 146](#)
- [Verifying External RADIUS Server EAP Authentication Configuration, page 157](#)
- [Troubleshooting External RADIUS Server EAP Authentication Configuration Issues, page 158](#)

Prerequisites

We recommend that you have knowledge about the following topics:

- Configuring lightweight access points (LAPs) and Cisco Catalyst 3850 Series Switch
- Lightweight Access Point Protocol (LWAPP)
- Configuring an external RADIUS server, such as the Cisco Secure ACS 5.2



Note The configuration example described in this document uses EAP-FAST.

- General EAP framework
- Security protocols, such as Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2) and EAP-Generic Token Card (EAP-GTC)
- Digital certificates

Supported Platforms and Releases

The information in this document is based on the following software and hardware versions:

- Cisco Catalyst 3850 Series Switch
- Cisco 3602 Series Lightweight Access Point
- Microsoft Windows XP with Intel PROset Supplicant
- Cisco Secure Access Control Server Release 5.2
- Cisco Catalyst 3560 Series Switch



Note

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuring External RADIUS Server EAP Authentication

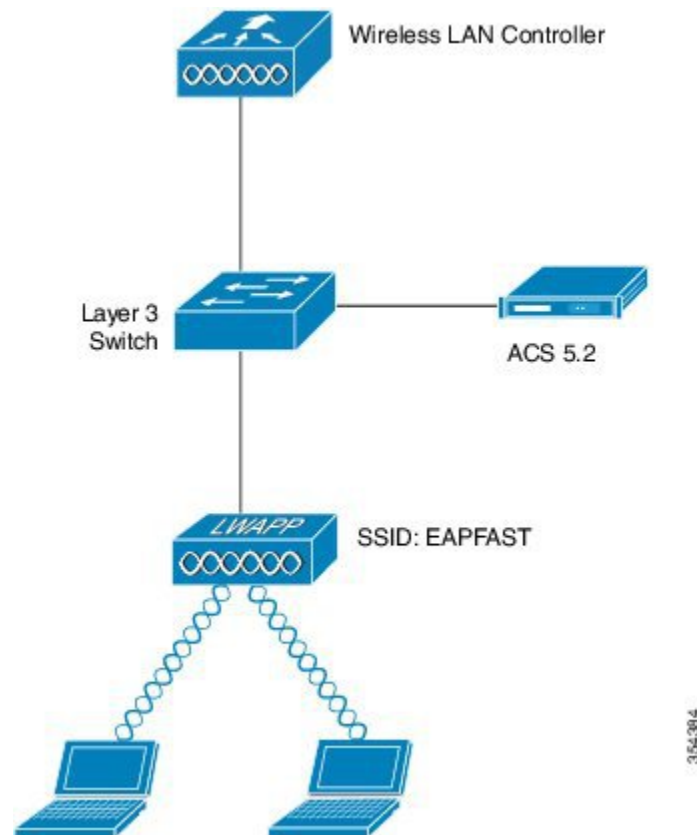


Note

For more information on the commands used in this section, refer to the [Command Lookup Tool](#) (for Registered Users only).

The following figure is an example of a network diagram:

Figure 42: Network Diagram



Network Diagram

Configuring External RADIUS Server EAP Authentication includes the following:

- Configuring Cisco Catalyst 3850 Series Switch using CLI or GUI.
- Configuring ACS 5.2 (RADIUS server).

Configuring WLAN for the Client VLAN using CLI

To configure the WLAN for the required client VLAN and map it to the authentication method list, use the following commands:

```
wlan EAPFAST 4 EAPFAST
  client vlan VLAN0020
  security dot1x authentication-list ACS
  session-timeout 1800
  no shutdown

aaa new-model
!
```

```

!
aaa group server radius ACS
 server name ACS
!
aaa authentication dot1x ACS group ACS

radius server ACS
 address ipv4 203. 0.113.50 auth-port 1645 acct-port 1646
 key Cisco123

dot1x system-auth-contro

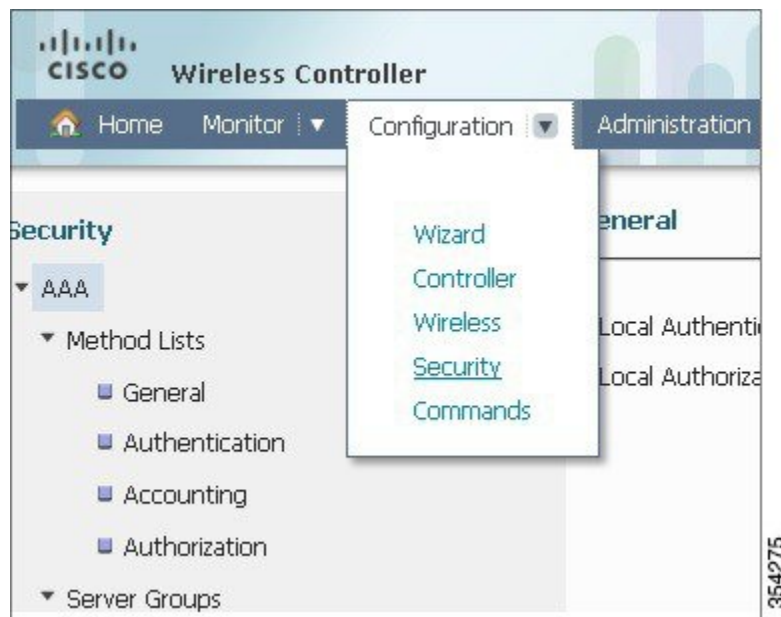
```

Configuring WLAN for the Client VLAN using GUI

Perform the following steps to configure the WLAN for the client VLAN:

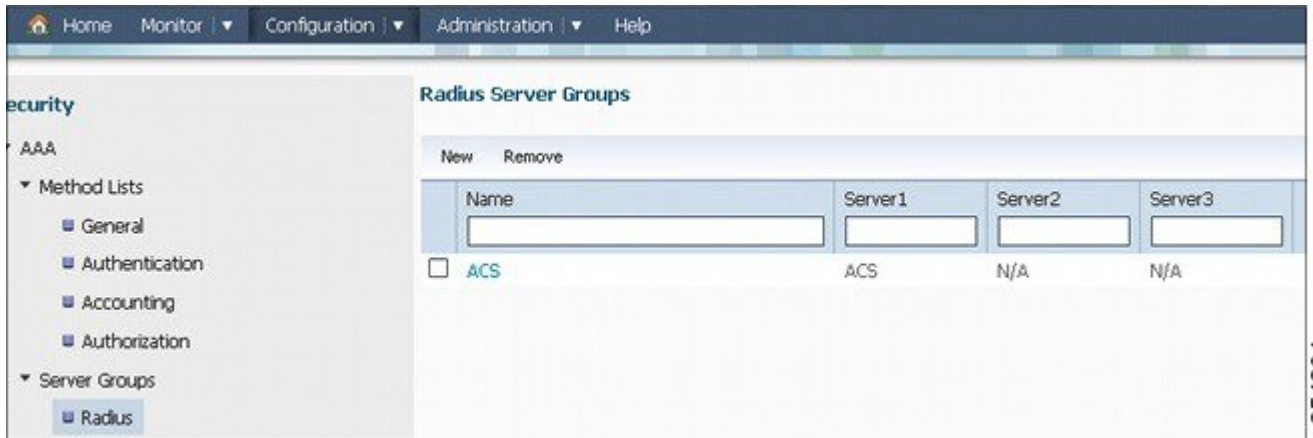
Step 1 To add the RADIUS server, navigate to **Configuration > Security > AAA**.

Figure 43: Adding RADIUS server



Step 2 To create a RADIUS Server group with the name ACS, navigate to **Server Groups > RADIUS**.

Figure 44: Creating RADIUS server group



354284

Step 3 To configure ACS RADIUS Server, navigate to **RADIUS > Services**.

Figure 45: Configuring ACS RADIUS server



354250

The following figure shows a complete configuration:

Figure 46: Complete Configuration

Radius Servers				
New Remove				
Server Name	Address	Auth Port	Acct Port	
<input type="checkbox"/> ACS	198.51.100.50	1645	1646	

Step 4 To enable Dot1x System Auth Control (802.1X System Auth Control), navigate to **Method Lists > General**. If Dot1x System Auth Control is not enabled, authentication might fail.

Figure 47: Enabling Dot1x

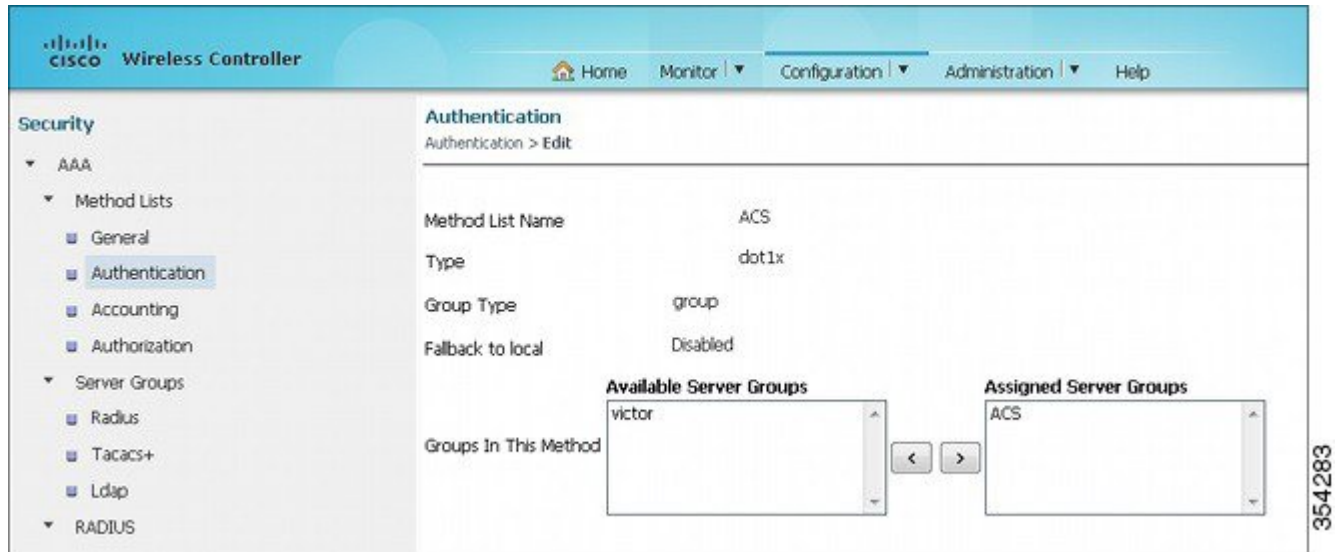
Cisco Wireless Controller
 Home Monitor Configuration

Security
 AAA
 Method Lists
 General
 Authentication
 Accounting

General
 Dot1x System Auth Control
 Local Authentication None
 Local Authorization None

Step 5 To map the configured ACS RADIUS Server to the method list, which in turn is mapped to the WLAN under the Authentication, Authorization, and Accounting (AAA) server, navigate to **Method Lists > Authentication**.

Figure 48: Mapping ACS RADIUS server



The following figure shows ACL on the Method List:

Figure 49: ACL on list method



- Step 6** To configure the WLAN and map the ACS, open the GUI access on the WLC and navigate to **Configuration > Wireless > WLAN > WLANs**.

Figure 50: Configuring WLAN and mapping ACS



- Step 7** To create a WLAN with 802.1X and map the RADIUS Server, on the WLAN page, click **NEW** and navigate to the **General** tab.

Figure 51: Creating WLAN with 802.1x and mapping RADIUS server

 A screenshot of the 'WLAN > Edit' configuration page in the Cisco Wireless Controller GUI. The 'General' tab is selected. The configuration fields are as follows:

Profile Name	EAPFAST
Type	WLAN
SSID	EAPFAST
Status	<input checked="" type="checkbox"/>
Security Policies	[WPA2][Auth(802.1x)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	VLAN0020
Broadcast SSID	<input checked="" type="checkbox"/>
Multicast VLAN Feature	<input type="checkbox"/>

 A vertical ID '354279' is visible on the right edge.

Step 8 To check if WPA or WPA2 with 802.1X enabled is available, navigate to the **Security > Layer 2** tab.

Figure 52: WPA or WPA2 with 802.1x



Step 9 To map the Authentication Method list for the ACS WLAN, navigate to the **AAA Server** tab.

Figure 53: Mapping Authentication Method List



Configuring ACS 5.2 (RADIUS Server)

Perform the following steps to configure the RADIUS Server:



Note

Ensure that the Cisco Catalyst 3850 Series Switch are already added on the ACS under AAA clients.

Step 1 To configure the users and user database on the ACS, navigate to **Users and Identity Stores > Internal Identity Stores > Users**.

Figure 54: Users and user database configuration

Users and Identity Stores > Internal Identity Stores > Users

Internal Users

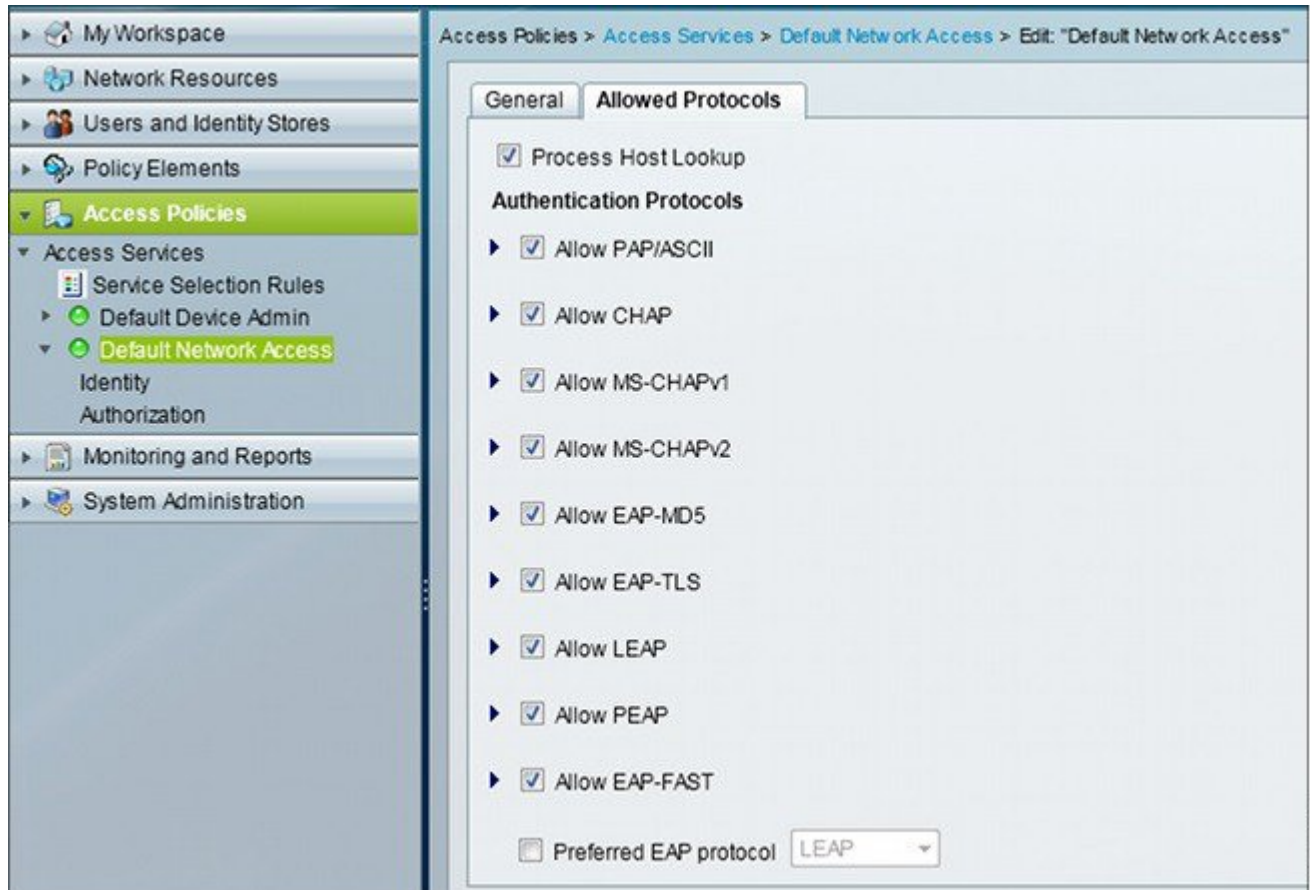
Filter: Match if:

<input type="checkbox"/>	Status	User Name	Identity Group	Description
<input type="checkbox"/>	●	student	All Groups:Students	
<input type="checkbox"/>	●	teacher	All Groups:Teachers	
<input type="checkbox"/>	●	user	All Groups	user

354277

Step 2 To enable required authentication protocols and EAP-FAST, navigate to **Access Policies > Access Services > Default Network Access**.

Figure 55: Enabling Authentication Protocols



Step 3 To configure the Identity Sequence rules for EAP-FAST, navigate to **Default Network Access > Identity**.

Figure 56: Identity sequence rules configuration

	Status	Name	Conditions		Results	Hit Count
			Eap Authentication Method	Eap Tunnel Building Method	Identity Source	
1	<input checked="" type="checkbox"/>	Peap	-ANY-	match PEAP	Internal Users	32
2	<input checked="" type="checkbox"/>	Leap	match LEAP	-ANY-	Internal Users	0
3	<input checked="" type="checkbox"/>	Eapfast	-ANY-	match EAP-FAST	Internal Users	3

354281

Step 4 To view the authorization rules that grant access to EAP client after successful navigation, navigate to **Default Network Access > Authorization**.

Figure 57: View authorization rules

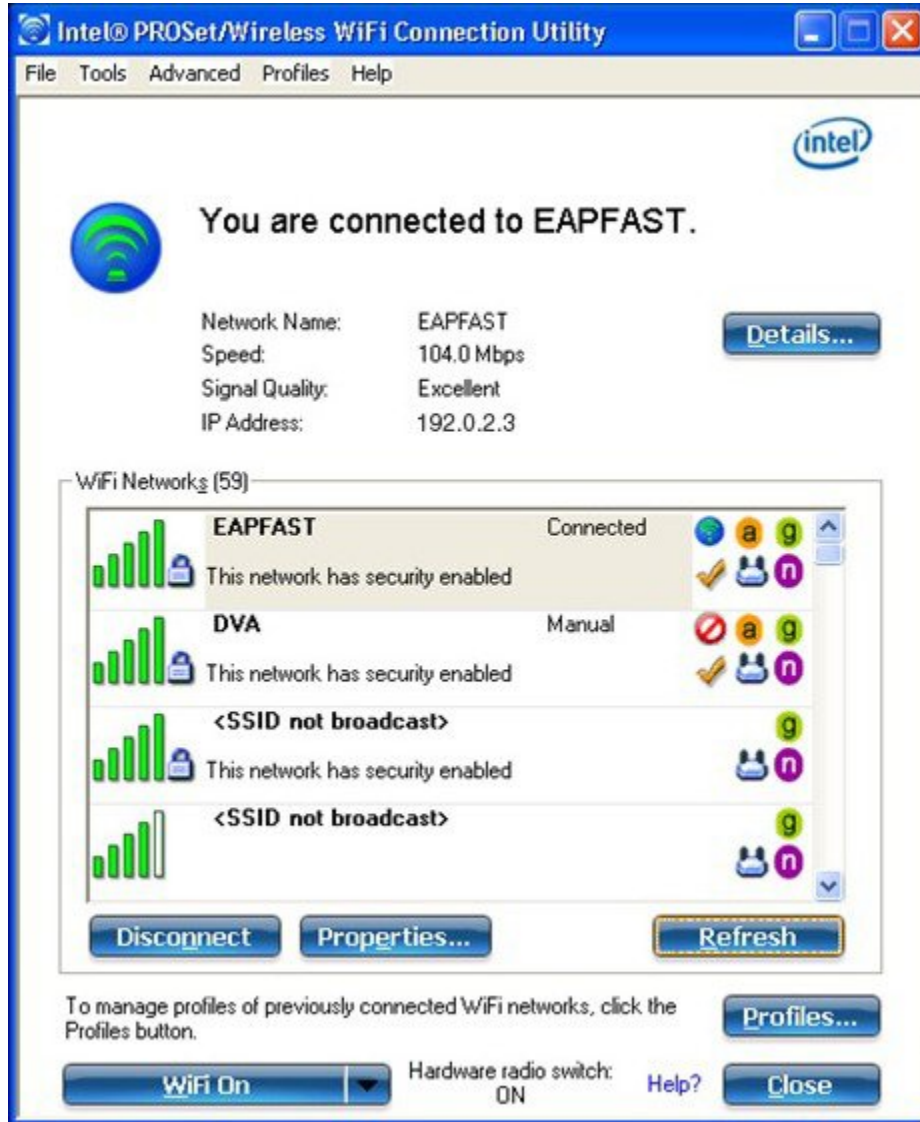
	Status	Name	Eap Authentication Method	Eap Tunnel Building Method	Compound Condition	Protocol	Identity Group	Results	Hit Count
1	<input checked="" type="checkbox"/>	Student	-ANY-	match PEAP	-ANY-	match Radius	In All Groups Students	Student	11
2	<input checked="" type="checkbox"/>	Teacher	-ANY-	match PEAP	-ANY-	match Radius	In All Groups Teachers	teacher	4
3	<input checked="" type="checkbox"/>	EAP-FAST	-ANY-	match EAP-FAST	-ANY-	match Radius	-ANY-	Permit Access	3

354285

Verifying External RADIUS Server EAP Authentication Configuration

To verify that your configuration works properly, connect to the EAP-FAST WLAN as shown in the following figure:

Figure 58: Verifying configuration



Troubleshooting External RADIUS Server EAP Authentication Configuration Issues

To troubleshoot any issues with your configuration, use the **debug** commands.

Device# **show debugging**

```

dot11/state debugging is on
pem/events debugging is on
client/mac-addr debugging is on
dot11/detail debugging is on
mac/ filters[string 0021.5c8c.c761] debugging is on
dot11/error debugging is on
dot11/mobile debugging is on
pem/state debugging is on

set trace group-wireless-client filter mac 0021.5c8c.c761
set trace wcm-dot1x event filter mac 0021.5c8c.c761
set trace wcm-dot1x aaa filter mac 0021.5c8c.c761
set trace aaa wireless events filter mac 0021.5c8c.c761
set trace access-session core sm filter mac 0021.5c8c.c761
set trace access-session method dot1x filter 0021.5c8c.c761

Device#
*Sep 1 06:00:18.282: 0021.5C8C.C761 Association received from mobile on AP
C8F9.F983.4260 1 wcm: .D^Iw for client 0:21:5c:t! w\2105HnJ^Iwy_status
0 attr len^G$8\227v^K
*Sep 1 06:00:18.282: 0021.5C8C.C761 qos upstream policy is unknown and
downstream policy is unknown 1 wcm: r client 0:21:5c:t! w\2105HnJ^Iwy_status
0 attr len^G$8\227v^K
*Sep 1 06:00:18.282: 0021.5C8C.C761 apChanged 0 wlanChanged 1 mscb ipAddr
20.20.20.3, apf RadiusOverride 0x0, numIPv6Addr=0 1 wcm: nJ^Iwy_status 0 attr
len^G$8\227v^K
*Sep 1 06:00:18.282: 0021.5C8C.C761 Applying WLAN policy on MSCB. 1 wcm:
ipAddr 20.20.20.3, apf RadiusOverride 0x0, numIPv6Addr=0
*Sep 1 06:00:18.282: 0021.5C8C.C761 Scheduling deletion of Mobile Station:
1 wcm: (callerId: 50) in 1 seconds
*Sep 1 06:00:18.282: 0021.5C8C.C761 Disconnecting client due to switch of WLANs
from 1(wpa2psk) to 4(EAPFAST) 1 wcm: numIPv6Addr=0
*Sep 1 06:00:19.174: 0021.5C8C.C761 apfMsExpireCallback (apf_ms.c: 1 wcm: 664)
Expiring Mobile!
*Sep 1 06:00:19.174: 0021.5C8C.C761 apfMsExpireMobileStation (apf_ms.c: 1 wcm:
6953) Changing state for mobile 0021.5C8C.C761 on AP C8F9.F983.4260 from
Associated to Disassociated
*Sep 1 06:00:19.174: 0021.5C8C.C761 Sent Deauthenticate to mobile on BSSID
C8F9.F983.4260 slot 1(caller apf_ms.c: 1 wcm: 7036)
*Sep 1 06:00:19.174: 0021.5C8C.C761 apfMsExpireMobileStation (apf_ms.c: 1 wcm:
7092) Changing state for mobile 0021.5C8C.C761 on AP C8F9.F983.4260 from
Disassociated to Idle
*Sep 1 06:00:19.174: 0021.5C8C.C761 20.20.20.3 RUN (20) Deleted mobile LWAPP
rule on AP [ C8F9.F983.4260 ] 1 wcm: 5C8C.C761 on AP C8F9.F983.4260 from
Disassociated to Idle
*Sep 1 06:00:19.174: PEM recv processing msg Del SCB(4) 1 wcm: Deleted mobile
*Sep 1 06:00:19.174: 0021.5C8C.C761 20.20.20.3 RUN (20) FastSSID for the client
[ C8F9.F983.4260 ] NOTENABLED 1 wcm: C.C761 on AP C8F9.F983.4260 from
Disassociated to Idle
*Sep 1 06:00:19.174: 0021.5C8C.C761 Incrementing the Reassociation Count 1 for
client (of interface VLAN0020) 1 wcm: D
*Sep 1 06:00:19.174: 0021.5C8C.C761 Clearing Address 20.20.20.3 on mobile 1 wcm:
for client (of interface VLAN0020)
*Sep 1 06:00:19.174: 0021.5C8C.C761 20.20.20.3 RUN (20) Skipping TMP rule add 1
wcm: lient (of interface VLAN0020)
*Sep 1 06:00:19.174: 0021.5C8C.C761 20.20.20.3 RUN (20) Change state to
DHCP REQD (7) last state RUN (20) 1 wcm:
*Sep 1 06:00:19.174: 0021.5C8C.C761 WCDB_CHANGE: 1 wcm: Client 1 m_vlan 20 Radio
iif id 0xbfc0c000000003a bssid iif id 0x8a3a80000000043, bssid C8F9.F983.4260
*Sep 1 06:00:19.174: 0021.5C8C.C761 WCDB_AUTH: 1 wcm: Adding opt82 len 0

```

```

*Sep 1 06:00:19.174: 0021.5C8C.C761 WCDB CHANGE: 1 wcm: Suppressing SPI (client
pending deletion) pemstate 7 state LEARN_IP(2) vlan 20 client_id 0x8006400000004e
mob=Local(1) ackflag 2 dropd 0, delete 1
*Sep 1 06:00:19.174: 0021.5C8C.C761 Sending SPI spi_epm_epm_terminate_session
successfull 1 wcm: pemstate 7 state LEARN_IP(2) vlan 20 client_id
0x8006400000004e mob=Local(1) ackflag 2 dropd 0, delete 1
*Sep 1 06:00:19.175: 0021.5C8C.C761 Sending SPI spi_epm_epm_terminate_session
successfull 1 wcm: pemstate 7 state LEARN_IP(2) vlan 20 client_id
0x8006400000004e mob=Local(1) ackflag 2 dropd 0, delete 1
*Sep 1 06:00:19.175: 0021.5C8C.C761 Deleting wireless client; Reason code 0,
Preset 1, AAA cause 1 1 wcm: 7 state LEARN_IP(2) vlan 20 client_id
0x8006400000004e mob=Local(1) ackflag 2 dropd 0, delete 1
*Sep 1 06:00:19.175: 0021.5C8C.C761 WCDB_DEL: 1 wcm: Successfully sent
*Sep 1 06:00:19.175: 0021.5C8C.C761 Expiring mobile state delete 1 wcm: on code
0, Preset 1, AAA cause 1
*Sep 1 06:00:19.175: 0021.5C8C.C761 0.0.0.0 DHCP_REQD (7) Handling pemDelScb
Event skipping delete 1 wcm: state LEARN_IP(2) vlan 20 client_id 0x8006400000004e
mob=Local(1) ackflag 2 dropd 0, delete 1
*Sep 1 06:00:19.178: 0021.5C8C.C761 WCDB SPI response msg handler client code 1
mob state 1 1 wcm: g delete
*Sep 1 06:00:19.178: 0021.5C8C.C761 apfProcessWcdbClientDelete: 1 wcm: Delete
ACK from WCDB.
*Sep 1 06:00:19.178: 0021.5C8C.C761 WCDB_DELACK: 1 wcm: wcdbAckRecvdFlag updated
*Sep 1 06:00:19.178: 0021.5C8C.C761 WCDB_DELACK: 1 wcm: Client IIF Id dealloc
SUCCESS w/ 0x8006400000004e.
*Sep 1 06:00:19.178: 0021.5C8C.C761 Invoked platform delete and cleared handle 1
wcm: w/ 0x8006400000004e.
*Sep 1 06:00:19.178: 0021.5C8C.C761 Deleting mobile on AP C8F9.F983.4260 (1) 1
wcm: w/ 0x8006400000004e.
*Sep 1 06:00:19.178: 0021.5C8C.C761 Unlinked and freed mscb 1 wcm: 8F9.F983.4260
(1)
*Sep 1 06:00:19.178: WCDB IIF: 1 wcm: Ack Message ID: 0x8006400000004e code 1003
*Sep 1 06:00:19.361: 0021.5C8C.C761 Adding mobile on LWAPP AP C8F9.F983.4260 (1)
1 wcm: x800640000.D^Iwe.
*Sep 1 06:00:19.361: 0021.5C8C.C761 Creating WL station entry for client - rc
0 1 wcm:
*Sep 1 06:00:19.361: 0021.5C8C.C761 Association received from mobile on AP
C8F9.F983.4260 1 wcm: 0.D^Iwe.
*Sep 1 06:00:19.361: 0021.5C8C.C761 qos upstream policy is unknown and downstream
policy is unknown 1 wcm:
*Sep 1 06:00:19.361: 0021.5C8C.C761 apChanged 0 wlanChanged 0 mscb ipAddr
0.0.0.0, apf RadiusOverride 0x0, numIPv6Addr=0 1 wcm:
\2105HnJ^Iwlient_id 0x80064000^G$8\227v^K
*Sep 1 06:00:19.361: 0021.5C8C.C761 Applying WLAN policy on MSCB. 1 wcm: ipAddr
0.0.0.0, apf RadiusOverride 0x0, numIPv6Addr=0
*Sep 1 06:00:19.361: 0021.5C8C.C761 Applying WLAN ACL policies to client 1 wcm:
0.0.0.0, apf RadiusOverride 0x0, numIPv6Addr=0
*Sep 1 06:00:19.361: 0021.5C8C.C761 No Interface ACL used for Wireless client in
WCM(CONVERGEDACCESS) 1 wcm: usOverride 0x0, numIPv6Addr=0
*Sep 1 06:00:19.361: 0021.5C8C.C761 Applying site-specific IPv6 override for
station 0021.5C8C.C761 - vapId 4, site 'default-group', interface 'VLAN0020'
1 wcm:
*Sep 1 06:00:19.361: 0021.5C8C.C761 Applying local bridging Interface Policy for
station 0021.5C8C.C761 - vlan 20, interface 'VLAN0020' 1 wcm: erface 'VLAN0020'
*Sep 1 06:00:19.361: 0021.5C8C.C761 STA - rates (8): 1 wcm: 140 18 152 36 176 72
96 108 0 0 0 0 0 0
*Sep 1 06:00:19.361: 0021.5C8C.C761 new capwap_wtp_iif_id b6818000000038, sm
capwap_wtp_iif_id 0 1 wcm: 8C.C761 - vlan 20, interface 'VLAN0020'
*Sep 1 06:00:19.361: 0021.5C8C.C761 WCDB_ADD: 1 wcm: Radio IIFID
0xbfc0000000003a, BSSID IIF Id 0x81fac0000000041, COS 4
*Sep 1 06:00:19.361: Load Balancer: 1 wcm: Success, Resource allocated are:
Active Switch number: 1, Active Asic number : 0, Reserve Switch number 0 Reserve
Asic number 0. AP Asic num 0
*Sep 1 06:00:19.361: 0021.5C8C.C761 WCDB_ADD: 1 wcm: Anchor Sw 1, Doppler 0
*Sep 1 06:00:19.361: 0021.5C8C.C761 WCDB_ALLOCATE: 1 wcm: Client IIF Id alloc
SUCCESS w/ client 84fd0000000050 (state 0).
*Sep 1 06:00:19.361: 0021.5C8C.C761 iifid Clearing Ack flag 1 wcm: F Id alloc
SUCCESS w/ client 84fd0000000050 (state 0).
*Sep 1 06:00:19.361: 0021.5C8C.C761 WCDB_ADD: 1 wcm: Adding opt82 len 0
*Sep 1 06:00:19.361: 0021.5C8C.C761 WCDB_ADD: 1 wcm: Clearing Ack flag
*Sep 1 06:00:19.361: 0021.5C8C.C761 WCDB_ADD: 1 wcm: ssid EAPFAST bssid
C8F9.F983.4260 vlan 20 auth=ASSOCIATION(0) wlan(ap-group/global) 4/4 client 0
assoc 3 mob=Unassoc(0) radio 1 m_vlan 20 ip 0.0.0.0 src 0xb6818000000038 dst 0x0

```

```

cid 0x84fd0000000050 glob rsc id 16dhcpsrv 0.0.0.0
*Sep 1 06:00:19.361: 0021.5C8C.C761 WCDB_ADD: 1 wcm: mscb iifid 0x84fd0000000050
msinfo iifid 0x0
*Sep 1 06:00:19.361: 0021.5C8C.C761 0.0.0.0 START (0) Initializing policy 1
wcm: info iifid 0x0
*Sep 1 06:00:19.361: 0021.5C8C.C761 0.0.0.0 START (0) Change state to AUTHCHECK
(2) last state AUTHCHECK (2) 1 wcm: (ap-group/global) 4/4 client 0 assoc 3
mob=Unassoc(0) radio 1 m_vlan 20 ip 0.0.0.0 src 0xb6818000000038 dst 0x0 cid
0x84fd0000000050 glob rsc id 16dhcpsrv 0.0.0.0
*Sep 1 06:00:19.361: 0021.5C8C.C761 0.0.0.0 AUTHCHECK (2) Change state to
8021X_REQD (3) last state 8021X_REQD (3) 1 wcm: oup/global) 4/4 client 0 assoc 3
mob=Unassoc(0) radio 1 m_vlan 20 ip 0.0.0.0 src 0xb6818000000038 dst 0x0 cid
0x84fd0000000050 glob rsc id 16dhcpsrv 0.0.0.0
*Sep 1 06:00:19.361: 0021.5C8C.C761 0.0.0.0 8021X_REQD (3) DHCP Not required on
AP C8F9.F983.4260 vapId 4 apVapId 4for this client 1 wcm: lient 0 assoc 3
mob=Unassoc(0) radio 1 m_vlan 20 ip 0.0.0.0 src 0xb6818000000038 dst 0x0 cid
0x84fd0000000050 glob rsc id 16dhcpsrv 0.0.0.0
*Sep 1 06:00:19.361: 0021.5C8C.C761 Not Using WMM Compliance code qosCap 00 1
wcm: ed on AP C8F9.F983.4260 vapId 4 apVapId 4for this client
*Sep 1 06:00:19.361: 0021.5C8C.C761 0.0.0.0 8021X_REQD (3) Plumbed mobile LWAPP
rule on AP C8F9.F983.4260 vapId 4 apVapId 4 1 wcm: client
*Sep 1 06:00:19.361: 0021.5C8C.C761 apfPemAddUser2 (apf_policy.c: 1 wcm: 161)
Changing state for mobile 0021.5C8C.C761 on AP C8F9.F983.4260 from Idle to
Associated
*Sep 1 06:00:19.361: 0021.5C8C.C761 Stopping deletion of Mobile Station: 1 wcm:
(callerId: 48)
*Sep 1 06:00:19.361: 0021.5C8C.C761 Ms Timeout = 0, Session Timeout = 1800 1 wcm:
llerId: 48)
*Sep 1 06:00:19.361: 0021.5C8C.C761 Sending Assoc Response to station on BSSID
C8F9.F983.4260 (status 0) ApVapId 4 Slot 1 1 wcm: .F983.4260 from Idle to
Associated
*Sep 1 06:00:19.362: 0021.5C8C.C761 apfProcessAssocReq (apf 80211.c: 1 wcm: 5260)
Changing state for mobile 0021.5C8C.C761 on AP C8F9.F983.4260 from Associated
to Associated
*Sep 1 06:00:19.362: WCDB_IIF: 1 wcm: Ack Message ID: 0x84fd0000000050 code 1001
*Sep 1 06:00:21.239: 0021.5C8C.C761 client incoming attribute size are 485 1 wcm:
anging state for .D^Iwle 0021.5C8C.C761 t! w\2105HnJ^IwF983.4260 from
Ass^G$8\227v^K
*Sep 1 06:00:21.258: 0021.5C8C.C761 0.0.0.0 8021X_REQD (3) Change state to
L2AUTHCOMPLETE (4) last state L2AUTHCOMPLETE (4) 1 wcm: ^IwF983.4260 from
Ass^G$8\227v^K
*Sep 1 06:00:21.258: 0021.5C8C.C761 WCDB_CHANGE: 1 wcm: Client 1 m_vlan 20 Radio
iif id 0xbfcfdc00000003a bssid iif id 0x81fac000000041, bssid C8F9.F983.4260
*Sep 1 06:00:21.258: 0021.5C8C.C761 WCDB_AUTH: 1 wcm: Adding opt82 len 0
*Sep 1 06:00:21.258: 0021.5C8C.C761 WCDB_LLM: 1 wcm: NoRun Prev Mob 0, Curr Mob
0 llmReq 1, return False
*Sep 1 06:00:21.258: 0021.5C8C.C761 auth state 1 mob state 0 setWme 0 wme 1
roam_sent 0 1 wcm: rn False
*Sep 1 06:00:21.258: 0021.5C8C.C761 WCDB_CHANGE: 1 wcm: auth=L2_AUTH(1) vlan 20
radio 1 client_id 0x84fd0000000050 mobility=Unassoc(0) src_int_0xb6818000000038
dst_int 0x0 ackflag 0 reassoc_client 0 llm_notif 0 ip 0.0.0.0 ip_learn_type
UNKNOWN
*Sep 1 06:00:21.258: 0021.5C8C.C761 WCDB_CHANGE: 1 wcm: In L2 auth but l2ack
waiting lflag not set,so set
*Sep 1 06:00:21.258: 0021.5C8C.C761 0.0.0.0 L2AUTHCOMPLETE (4)
pemAdvanceState2: 1 wcm: MOBILITY-INCOMPLETE with state 4.
*Sep 1 06:00:21.258: 0021.5C8C.C761 0.0.0.0 L2AUTHCOMPLETE (4)
pemAdvanceState2: 1 wcm: MOBILITY-INCOMPLETE with state 4.
*Sep 1 06:00:21.258: 0021.5C8C.C761 0.0.0.0 L2AUTHCOMPLETE (4) DHCP Not
required on AP C8F9.F983.4260 vapId 4 apVapId 4for this client 1 wcm:
68180000000038 dst_int 0x0 ackflag 0 reassoc_client 0 llm_notif 0 ip 0.0.0.0
ip_learn_type UNKNOWN
*Sep 1 06:00:21.258: 0021.5C8C.C761 Not Using WMM Compliance code qosCap 00 1
wcm: quired on AP C8F9.F983.4260 vapId 4 apVapId 4for this client
*Sep 1 06:00:21.258: 0021.5C8C.C761 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed mobile
LWAPP rule on AP C8F9.F983.4260 vapId 4 apVapId 4 1 wcm: client
*Sep 1 06:00:21.258: 0021.5C8C.C761 0.0.0.0 L2AUTHCOMPLETE (4) Change state to
DHCP_REQD (7) last state DHCP_REQD (7) 1 wcm: apVapId 4
*Sep 1 06:00:21.258: 0021.5C8C.C761 WCDB_CHANGE: 1 wcm: Client 1 m_vlan 20 Radio
iif id 0xbfcfdc00000003a bssid iif id 0x81fac000000041, bssid C8F9.F983.4260
*Sep 1 06:00:21.258: 0021.5C8C.C761 WCDB_AUTH: 1 wcm: Adding opt82 len 0
*Sep 1 06:00:21.258: 0021.5C8C.C761 WCDB_CHANGE: 1 wcm: Suppressing SPI
(Mobility state not known) pemstate 7 state LEARN_IP(2) vlan 20 client_id

```

```

0x84fd0000000050 mob=Unassoc(0) ackflag 1 dropd 0
*Sep 1 06:00:21.258: 0021.5C8C.C761 0.0.0.0 DHCP_REQD (7) pemAdvanceState2
4001, Adding TMP rule 1 wcm: e 7 state LEARN_IP(2) vlan 20 client_id
0x84fd0000000050 mob=Unassoc(0) ackflag 1 dropd 0
*Sep 1 06:00:21.258: 0021.5C8C.C761 0.0.0.0 DHCP_REQD (7) Adding Fast Path rule
on AP C8F9.F983.4260 , slot 1 802.1P = 0 1 wcm: client_id 0x84fd0000000050
mob=Unassoc(0) ackflag 1 dropd 0
*Sep 1 06:00:21.258: 0021.5C8C.C761 0.0.0.0 DHCP_REQD (7) Successfully plumbed
mobile rule 1 wcm: F9.F983.4260 , slot 1 802.1P = 0^M
*Sep 1 06:00:21.258: PEM rcv processing msg Add SCB(3) 1 wcm: 7) Successfully
plumbed mobile rule
*Sep 1 06:00:21.258: 0021.5C8C.C761 Incrementing the Reassociation Count 1 for
client (of interface VLAN0020) 1 wcm: lot 1 802.1P = 0^M
*Sep 1 06:00:21.258: 0021.5C8C.C761 0.0.0.0, auth_state 7 mmRole Unassoc !!! 1
wcm: r client (of interface VLAN0020)
*Sep 1 06:00:21.258: 0021.5C8C.C761 0.0.0.0, auth_state 7 mmRole Unassoc,
updating wcdb not needed 1 wcm: VLAN0020)
*Sep 1 06:00:21.258: 0021.5C8C.C761 Tclas Plumb needed: 1 wcm: 0
*Sep 1 06:00:21.258: 0021.5C8C.C761 0.0.0.0 DHCP_REQD (7) pemAdvanceState2: 1
wcm: MOBILITY-COMLETE with state 7.
*Sep 1 06:00:21.258: 0021.5C8C.C761 0.0.0.0 DHCP_REQD (7) State Update from
Mobility-Incomplete to Mobility-Complete, mobility role=Local, client
state=APF_MS_STATE_ASSOCIATED 1 wcm: 1 dropd 0
*Sep 1 06:00:21.258: 0021.5C8C.C761 0.0.0.0 DHCP_REQD (7) pemAdvanceState2
3611, Adding TMP rule 1 wcm: o Mobility-Complete, mobility role=Local, client
state=APF_MS_STATE_ASSOCIATED
*Sep 1 06:00:21.258: 0021.5C8C.C761 0.0.0.0 DHCP_REQD (7) Replacing Fast Path
rule on AP C8F9.F983.4260 , slot 1 802.1P = 0 1 wcm: e=Local, client
state=APF_MS_STATE_ASSOCIATED
*Sep 1 06:00:21.258: 0021.5C8C.C761 0.0.0.0 DHCP_REQD (7) Successfully plumbed
mobile rule 1 wcm: C8F9.F983.4260 , slot 1 802.1P = 0^M
*Sep 1 06:00:21.258: 0021.5C8C.C761 WCDB CHANGE: 1 wcm: Client 1 m vlan 20 Radio
iif id 0xbfcfdc00000003a bssid iif id 0x81fac000000041, bssid C8F9.F983.4260
*Sep 1 06:00:21.258: 0021.5C8C.C761 WCDB_AUTH: 1 wcm: Adding opt82 len 0
*Sep 1 06:00:21.258: 0021.5C8C.C761 WCDB_LLM: 1 wcm: NoRun Prev Mob 0, Curr
Mob 1 llmReq 1, return False
*Sep 1 06:00:21.258: 0021.5C8C.C761 WCDB CHANGE: 1 wcm: Suppressing SPI (ACK
message not recvd) pemstate 7 state LEARN_IP(2) vlan 20 client_id 0x84fd0000000050
mob=Local(1) ackflag 1 dropd 1
*Sep 1 06:00:21.258: 0021.5C8C.C761 Error updating wcdb on mobility complete 1
wcm: not recvd) pemstate 7 state LEARN_IP(2) vlan 20 client_id 0x84fd0000000050
mob=Local(1) ackflag 1 dropd 1
*Sep 1 06:00:21.258: PEM rcv processing msg Epm spi response(12) 1 wcm:
complete
*Sep 1 06:00:21.258: 0021.5C8C.C761 aaa attribute list length is 79 1 wcm:
complete
*Sep 1 06:00:21.258: 0021.5C8C.C761 Sending SPI spi_epm_epm_session_create
successfull 1 wcm: ) pemstate 7 state LEARN_IP(2) vlan 20 client_id
0x84fd0000000050 mob=Local(1) ackflag 1 dropd 1
*Sep 1 06:00:21.258: PEM rcv processing msg Add SCB(3) 1 wcm: pm_session_create
successfull
*Sep 1 06:00:21.259: 0021.5C8C.C761 0.0.0.0, auth_state 7 mmRole Local !!! 1 wcm:
successfull
*Sep 1 06:00:21.259: 0021.5C8C.C761 0.0.0.0, auth_state 7 mmRole Local, updating
wcdb not needed 1 wcm: 7 state LEARN_IP(2) vlan 20 client_id 0x84fd0000000050
mob=Local(1) ackflag 1 dropd 1
*Sep 1 06:00:21.259: 0021.5C8C.C761 Tclas Plumb needed: 1 wcm: 0
*Sep 1 06:00:21.260: EPM: 1 wcm: Session create resp - client handle
84fd0000000050 session f2000027
*Sep 1 06:00:21.260: EPM: 1 wcm: Netflow session create resp - client handle
84fd0000000050 sess f2000027
*Sep 1 06:00:21.260: PEM rcv processing msg Epm spi response(12) 1 wcm: le
84fd0000000050 sess f2000027
*Sep 1 06:00:21.261: 0021.5C8C.C761 Received session_create_response for client
handle 37432873367634000 1 wcm: LEARN_IP(2) vlan 20 client_id 0x84fd0000000050
mob=Local(1) ackflag 1 dropd 1
*Sep 1 06:00:21.261: 0021.5C8C.C761 Received session_create_response with EPM
session handle 4060086311 1 wcm:
*Sep 1 06:00:21.261: 0021.5C8C.C761 Send request to EPM 1 wcm: ate_response with
EPM session handle 4060086311
*Sep 1 06:00:21.261: 0021.5C8C.C761 aaa attribute list length is 485 1 wcm: with
EPM session handle 4060086311
*Sep 1 06:00:21.261: 0021.5C8C.C761 Sending Activate request for session handle

```

```

4060086311 successful 1 wcm: 1
*Sep 1 06:00:21.261: 0021.5C8C.C761 Post-auth policy request sent! Now wait for
post-auth policy ACK from EPM 1 wcm: N_IP(2) vlan 20 client_id 0x84fd0000000050
mob=Local(1) ackflag 1 dropd 1
*Sep 1 06:00:21.261: EPM: 1 wcm: Init feature, client handle 84fd0000000050
session f2000027 authz 8f000011
*Sep 1 06:00:21.261: EPM: 1 wcm: Activate feature client handle 84fd0000000050
sess f2000027 authz 8f000011
*Sep 1 06:00:21.261: PEM rcv processing msg Epm spi response(12) 1 wcm: 0050
sess f2000027 authz 8f000011
*Sep 1 06:00:21.261: 0021.5C8C.C761 Received activate_features_resp for client
handle 37432873367634000 1 wcm: m EPM
*Sep 1 06:00:21.261: 0021.5C8C.C761 Received activate_features_resp for EPM
session handle 4060086311 1 wcm: 0
*Sep 1 06:00:21.261: EPM: 1 wcm: Policy enforcement - client handle
84fd0000000050 session a8000011 authz 8f000011
*Sep 1 06:00:21.261: EPM: 1 wcm: Netflow policy enforcement - client handle
84fd0000000050 sess a8000011 authz 8f000011 msg_type 0 policy_status 0 attr len 0
*Sep 1 06:00:21.262: PEM rcv processing msg Epm spi response(12) 1 wcm: e
84fd0000000050 sess a8000011 authz 8f000011 msg_type 0 policy_status 0 attr len 0
*Sep 1 06:00:21.262: 0021.5C8C.C761 Received policy_enforcement_response for
client handle 37432873367634000 1 wcm: 011 msg_type 0 policy_status 0 attr len 0
*Sep 1 06:00:21.262: 0021.5C8C.C761 Received policy_enforcement_response for EPM
session handle 2818572305 1 wcm: 0
*Sep 1 06:00:21.262: 0021.5C8C.C761 Received response for
_EPM_SPI_ACTIVATE_FEATURES request sent for client 1 wcm: 011 msg_type 0
policy_status 0 attr len 0
*Sep 1 06:00:21.262: 0021.5C8C.C761 Received _EPM_SPI_STATUS_SUCCESS for request
sent for client 1 wcm: for client
*Sep 1 06:00:21.262: 0021.5C8C.C761 Post-auth policy ACK recvd from EPM, unset
flag on MSCB 1 wcm: ient
*Sep 1 06:00:21.262: 0021.5C8C.C761 WCDB SPI response msg handler client code 0
mob state 0 1 wcm: ient
*Sep 1 06:00:21.262: 0021.5C8C.C761 WcdbClientUpdate: 1 wcm: L2 Auth ACK from
WCDB
*Sep 1 06:00:21.262: 0021.5C8C.C761 WCDB_L2ACK: 1 wcm: wcdbAckRecvdFlag updated
*Sep 1 06:00:21.262: 0021.5C8C.C761 WCDB_CHANGE: 1 wcm: Client 1 m_vlan 20 Radio
iif id 0xbfdcd00000003a bssid iif id 0x81fac000000041, bssid C8F9.F983.4260
*Sep 1 06:00:21.262: 0021.5C8C.C761 WCDB_AUTH: 1 wcm: Adding opt82 len 0
*Sep 1 06:00:21.262: 0021.5C8C.C761 WCDB_LLM: 1 wcm: NoRun Prev Mob 0, Curr
Mob 1 llmReq 1, return False
*Sep 1 06:00:21.263: 0021.5C8C.C761 auth state 2 mob state 1 setWme 0 wme 1
roam sent 0 1 wcm: rn False
*Sep 1 06:00:21.263: 0021.5C8C.C761 WCDB_CHANGE: 1 wcm: auth=LEARN_IP(2) vlan 20
radio 1 client_id 0x84fd0000000050 mobility=Local(1) src_int 0xb6818000000038
dst_int 0x0 ackflag 2 reassoc_client 0 llm_notif 0 ip 0.0.0.0 ip_learn_type
UNKNOWN
*Sep 1 06:00:24.425: 0021.5C8C.C761 WCDB_IP_BIND: 1 wcm: w/ IPv4 20.20.20.3
ip_learn_type DHCP add delete 1,options_length 0
*Sep 1 06:00:24.425: 0021.5C8C.C761 WcdbClientUpdate: 1 wcm: IP Binding from
WCDB ip_learn_type 1, add_or delete 1
*Sep 1 06:00:24.425: 0021.5C8C.C761 IPv4 Addr: 1 wcm: 20:20:20:3
*Sep 1 06:00:24.425: 0021.5C8C.C761 MS got the IP, resetting the Reassociation
Count 0 for client 1 wcm: delete 1
*Sep 1 06:00:24.425: 0021.5C8C.C761 20.20.20.3 DHCP_REQD (7) Session Update not
required for Initial authenticated dot1x client 1 wcm: nt 0xb68180000000^G$8\227v^K
*Sep 1 06:00:24.426: 0021.5C8C.C761 20.20.20.3 DHCP_REQD (7) Change state to
RUN (20) last state RUN (20) 1 wcm: ticated dot1x client
*Sep 1 06:00:24.426: 0021.5C8C.C761 WCDB_CHANGE: 1 wcm: Client 1 m_vlan 20 Radio
iif id 0xbfdcd00000003a bssid iif id 0x81fac000000041, bssid C8F9.F983.4260
*Sep 1 06:00:24.426: 0021.5C8C.C761 WCDB_AUTH: 1 wcm: Adding opt82 len 0
*Sep 1 06:00:24.426: 0021.5C8C.C761 WCDB_LLM: 1 wcm: prev Mob state 1 curr Mob
State 1 llReq flag 0
*Sep 1 06:00:24.426: 0021.5C8C.C761 auth state 4 mob state 1 setWme 0 wme 1
roam sent 0 1 wcm: g 0
*Sep 1 06:00:24.426: 0021.5C8C.C761 WCDB_CHANGE: 1 wcm: auth=RUN(4) vlan 20
radio 1 client_id 0x84fd0000000050 mobility=Local(1) src_int 0xb6818000000038
dst_int 0x0 ackflag 2 reassoc_client 0 llm_notif 0 ip 20.20.20.3 ip_learn_type
DHCP
*Sep 1 06:00:24.426: 0021.5C8C.C761 20.20.20.3 RUN (20) Reached PLUMBFASPATH:
1 wcm: from line 4430
*Sep 1 06:00:24.426: 0021.5C8C.C761 20.20.20.3 RUN (20) Replacing Fast Path
rule on AP C8F9.F983.4260 , slot 1 802.1P = 0 1 wcm: 0xb6818000000038 dst_int

```

```

0x0
ackflag 2 reassoc_client 0 llm_notif 0 ip 20.$=6v0.3
ip_lt^ Dv^\7HnP6v^D6H15Ht^ Dv$6H8^ r^D6H>&5v8^ r^D6H>&5v^D6Ht^M^Lw^\7H8^ r
*Sep 1 06:00:24.426: 0021.5C8C.C761 20.20.20.3 RUN (20) Successfully plumbed
mobile rule 1 wcm: C8F9.F983.4260 , slot 1 802.1P = 0^M
*Sep 1 06:00:24.426: 0021.5C8C.C761 Sending IPv4 update to Controller
10.105.135.176 1 wcm: e
*Sep 1 06:00:24.426: 0021.5C8C.C761 Assigning Address 20.20.20.3 to mobile 1
wcm: 05.135.176
*Sep 1 06:00:24.426: PEM rcv processing msg Add SCB(3) 1 wcm: 20.20.3 to mobile
*Sep 1 06:00:24.426: 0021.5C8C.C761 20.20.20.3, auth_state 20 mmRole Local !!! 1
wcm: 135.176
*Sep 1 06:00:24.426: 0021.5C8C.C761 20.20.20.3, auth_state 20 mmRole Local,
updating wcdb not needed 1 wcm: 3.4260 , slot 1 802.1P = 0^M
*Sep 1 06:00:24.426: 0021.5C8C.C761 Tclas Plumb needed: 1 wcm: 0
*Sep 1 06:00:34.666: PEM rcv processing msg Del SCB(4) 1 wcm:
*Sep 1 06:00:34.864: PEM rcv processing msg Add SCB(3) 1 wcm:
*Sep 1 06:00:34.865: EPM: 1 wcm: Init feature, client handle a028c00000004c
session a600001f authz 5e00000d
*Sep 1 06:00:34.865: EPM: 1 wcm: Activate feature client handle a028c00000004c
sess a600001f authz 5e00000d
*Sep 1 06:00:34.865: PEM rcv processing msg Epm spi response(12) 1 wcm: 004c
sess a600001f authz 5e00000d
*Sep 1 06:00:34.865: EPM: 1 wcm: Policy enforcement - client handle
a028c00000004c session ca00000d authz 5e00000d
*Sep 1 06:00:34.865: EPM: 1 wcm: Netflow policy enforcement - client handle
a028c00000004c sess ca00000d authz 5e00000d msg_type 0 policy_status 0 attr len 0
*Sep 1 06:00:34.865: PEM rcv processing msg Epm spi response(12) 1 wcm: e
a028c00000004c sess ca00000d authz 5e00000d msg_type 0 policy_status 0 attr len 0
*Sep 1 06:00:52.802: PEM rcv processing msg Del SCB(4) 1 wcm: nse(12)
*Sep 1 06:00:53.015: PEM rcv processing msg Add SCB(3) 1 wcm:
*Sep 1 06:00:53.015: EPM: 1 wcm: Init feature, client handle a028c00000004c
session a600001f authz 5e00000d
*Sep 1 06:00:53.015: EPM: 1 wcm: Activate feature client handle a028c00000004c
sess a600001f authz 5e00000d
*Sep 1 06:00:53.015: PEM rcv processing msg Epm spi response(12) 1 wcm: 004c
sess a600001f authz 5e00000d
*Sep 1 06:00:53.016: EPM: 1 wcm: Policy enforcement - client handle
a028c00000004c session ca00000d authz 5e00000d
*Sep 1 06:00:53.016: EPM: 1 wcm: Netflow policy enforcement - client handle
a028c00000004c sess ca00000d authz 5e00000d msg_type 0 policy_status 0 attr len 0
*Sep 1 06:00:53.016: PEM rcv processing msg Epm spi response(12) 1 wcm: e
a028c00000004c sess ca00000d authz 5e00000d msg_type 0 policy_status 0 attr len 0
*Sep 1 06:01:18.829: PEM rcv processing msg Del SCB(4) 1 wcm: nse(12)
*Sep 1 06:01:19.037: PEM rcv processing msg Add SCB(3) 1 wcm:
*Sep 1 06:01:19.037: EPM: 1 wcm: Init feature, client handle a028c00000004c
session a600001f authz 5e00000d
*Sep 1 06:01:19.037: EPM: 1 wcm: Activate feature client handle a028c00000004c
sess a600001f authz 5e00000d
*Sep 1 06:01:19.037: PEM rcv processing msg Epm spi response(12) 1 wcm: 004c
sess a600001f authz 5e00000d
*Sep 1 06:01:19.037: EPM: 1 wcm: Policy enforcement - client handle
a028c00000004c session ca00000d authz 5e00000d
*Sep 1 06:01:19.037: EPM: 1 wcm: Netflow policy enforcement - client handle
a028c00000004c sess ca00000d authz 5e00000d msg_type 0 policy_status 0 attr len 0
*Sep 1 06:01:19.037: PEM rcv processing msg Epm spi response(12) 1 wcm: e
a028c00000004c sess ca00000d authz 5e00000d msg_type 0 policy_status 0 attr len 0
*Sep 1 06:01:20.108: 0021.5C8C.C761
Client stats update: 1 wcm: Time now in sec 1378015280, Last Acct Msg Sent at
1378015224 sec

[09/01/13 11:59:18.282 IST 1572 5933] 0021.5C8C.C761 Scheduling deletion of Mobile
Station: (callerId: 50) in 1 seconds
--More-- [09/01/13 11:59:18.282 IST 1573 5933] 0021.5C8C.C761
Disconnecting client due to switch of WLANs from 1(wpa2psk) to 4(EAPFAST)
[09/01/13 11:59:19.174 IST 1574 5933] 0021.5C8C.C761 apfMsExpireCallback
(apf.ms.c:664) Expiring Mobile!
[09/01/13 11:59:19.174 IST 1575 5933] 0021.5C8C.C761 apfMsExpireMobileStation
(apf.ms.c:6953) Changing state for mobile 0021.5C8C.C761 on AP C8F9.F983.4260
from Associated to Disassociated
[09/01/13 11:59:19.174 IST 1576 5933] 0021.5C8C.C761 1XA: Cleaning up dot1x
[09/01/13 11:59:19.174 IST 1577 5933] 0021.5C8C.C761 1XA: Session Manager Call to

```

```

cleanup session for Client capwap iif id b6818000000038
[09/01/13 11:59:19.174 IST 1578 5933] 0021.5C8C.C761 Sent Deauthenticate to mobile
on BSSID C8F9.F983.4260 slot 1 (caller apf.ms.c:7036)
[09/01/13 11:59:19.174 IST 1579 5933] 0021.5C8C.C761 AAAS: acct method list NOT
configured for WLAN 1, accounting skipped
[09/01/13 11:59:19.174 IST 157a 5933] 0021.5C8C.C761 AAAS: freeing AAA accounting
session
[09/01/13 11:59:19.174 IST 157b 5933] 0021.5C8C.C761 apfMsAssoStateDec
[09/01/13 11:59:19.174 IST 157c 5933] 0021.5C8C.C761 apfMsExpireMobileStation
(apf_ms.c:7092) Changing state for mobile 0021.5C8C.C761 on AP C8F9.F983.4260
from Disassociated to Idle
[09/01/13 11:59:19.174 IST 157d 33] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
[0021.5c8c.c761, Cal] Session stop request received for Client[1] MAC
[0021.5c8c.c761] SID [] Disc
cause [(default)/0]
--More-- [09/01/13 11:59:19.174 IST 157e 173] ACCESS-CORE-SM-NOTF:
[0021.5c8c.c761, Cal] Received session event 'SESSION_STOP' from client
[09/01/13 11:59:19.174 IST 157f 5933] 0021.5C8C.C761 Incrementing the
Reassociation Count 1 for client (of interface VLAN0020)
[09/01/13 11:59:19.174 IST 1580 5933] 0021.5C8C.C761 Clearing Address 20.20.20.3
on mobile
[09/01/13 11:59:19.174 IST 1581 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Session stop for 0021.5c8c.c761 - Audit ID (none), reason (default)/0
[09/01/13 11:59:19.174 IST 1582 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Unlocking 0xF3000023 for deletion
[09/01/13 11:59:19.174 IST 1583 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Processing SM CB request for 0xF3000023: Event: Pre-Disconnect notification t
[09/01/13 11:59:19.174 IST 1584 5933] 0021.5C8C.C761 apfMsRunStateDec
[09/01/13 11:59:19.174 IST 1585 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Predisconnect notification - teardown complete for 0xF3000023(0021.5c8c.c761)
[09/01/13 11:59:19.174 IST 1586 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Session teardown completing, deleting context
[09/01/13 11:59:19.174 IST 1587 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Signalling "pre" delete for client 0021.5c8c.c761 / 0xF3000023
[09/01/13 11:59:19.174 IST 1588 5933] 0021.5C8C.C761 WCDB_AUTH: Adding opt82 len 0
[09/01/13 11:59:19.174 IST 1589 5933] 0021.5C8C.C761 WCDB_CHANGE: Suppressing SPI
(client pending deletion) pemstate 7 state LEARN_IP(2) vlan 20 client_id
0x8006400000004e mob=Local(1) ackflag 2 dropd 0, delete 1
--More-- [09/01/13 11:59:19.174 IST 158a 173] ACCESS-CORE-SM-NOTF:
[0021.5c8c.c761, Cal] Deleted record - hdl 0xF3000023. 2 session(s) remain on IDB.
[09/01/13 11:59:19.174 IST 158b 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Processing SM CB request for 0xF3000023: Event: Client disconnect notificatio
[09/01/13 11:59:19.174 IST 158c 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
AAA-ID 0x0000001C for 0021.5c8c.c761 not freed, as externally generated
[09/01/13 11:59:19.174 IST 158d 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Removed policy (tgt 0x00000000) from session (hdl 0xF3000023)
[09/01/13 11:59:19.174 IST 158e 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Unblock events for 0021.5c8c.c761.
[09/01/13 11:59:19.174 IST 158f 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
AAA-ID 0x0000001C for 0021.5c8c.c761 not freed, as externally generated
[09/01/13 11:59:19.174 IST 1590 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Freed Auth Manager context 0xF3000023
[09/01/13 11:59:19.174 IST 1591 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Signalling "post" delete for client in domain DATA
[09/01/13 11:59:19.174 IST 1592 5933] 0021.5C8C.C761 Sending SPI
spi epm epm terminate_session successfull
[09/01/13 11:59:19.175 IST 1593 5933] 0021.5C8C.C761 Sending SPI
spi epm epm terminate_session successfull
[09/01/13 11:59:19.175 IST 1594 5933] 0021.5C8C.C761 Deleting wireless client;
Reason code 0, Preset 1, AAA cause 1
[09/01/13 11:59:19.175 IST 1595 5933] 0021.5C8C.C761 WCDB_DEL: Successfully sent
[09/01/13 11:59:19.175 IST 1596 5933] 0021.5C8C.C761 Expiring mobile state delete
--More-- [09/01/13 11:59:19.175 IST 1597 190] [WCDB] ==Delete event for
Wireless client (0021.5c8c.c761) client id (0x8006400000004e) vlan 20 auth_state
RUN mob_state LOCAL flags 2
[09/01/13 11:59:19.175 IST 1598 190] [WCDB] wcdb_client_mcast_update_notify: add =
0, port update = 0, delete = 1
[09/01/13 11:59:19.175 IST 1599 190] ACCESS-CORE-SM-FEATURE-WIRED_TUNNEL-NOT:
[0021.5c8c.c761] Client 0021.5c8c.c761 is not tunnel client..Return
[09/01/13 11:59:19.176 IST 159a 190] [WCDB] wcdb_ffcp_wcdb_client_delete_notify:
client (0021.5c8c.c761) id 0x8006400000004e ffcp delete
[09/01/13 11:59:19.178 IST 159b 33] [WCDB] wcdb_ffcp_cb: client (0021.5c8c.c761)
client (0x8006400000004e): FFCP operation (DELETE) return code (0)

```



```

[09/01/13 11:59:19.178 IST 159c 33] [WCDB] wcdb_send delete_notify_callback_event:
Delete ACK sent to WCM after confirming clientLe is deleted for mac 0021.5c8c.c761
[09/01/13 11:59:19.178 IST 159d 33] [WCDB] wcdb_client_delete_actual: WCDB DB
client 0021.5c8c.c761 is being deleted
[09/01/13 11:59:19.178 IST 159e 33] [WCDB] wcdb_client_delete_actual Client delete
notification is sent to DHCP snooping: host mac: 0021.5c8c.c761, IP: 20.20.20.3
[09/01/13 11:59:19.178 IST 159f 33] [WCDB] wcdb_client_delete_actual: Exit: WCDB
DB client 0021.5c8c.c761 is being deleted
[09/01/13 11:59:19.178 IST 15a0 186] ACCESS-CORE-SM-CLIENT-IPDT-ERR:
[0021.5c8c.c761, Cal] No session for MAC 0021.5c8c.c761
[09/01/13 11:59:19.178 IST 15a1 5933] 0021.5C8C.C761 WCDB SPI response msg handler
client code 1 mob state 1
--More-- [09/01/13 11:59:19.178 IST 15a2 5933] 0021.5C8C.C761
apfProcessWcdbClientDelete: Delete ACK from WCDB.
[09/01/13 11:59:19.178 IST 15a3 5933] 0021.5C8C.C761 WCDB_DELACK: wcdbAckRecvdFlag
updated
[09/01/13 11:59:19.178 IST 15a4 5933] 0021.5C8C.C761 Invoked platform delete and
cleared handle
[09/01/13 11:59:19.178 IST 15a5 5933] 0021.5C8C.C761 apfMslxStateDec
[09/01/13 11:59:19.178 IST 15a6 5933] 0021.5C8C.C761 Deleting mobile on AP
C8F9.F983.4260 (1)
[09/01/13 11:59:19.178 IST 15a7 5933] 0021.5C8C.C761 1XA: Cleaning up dot1x
[09/01/13 11:59:19.178 IST 15a8 5933] 0021.5C8C.C761 Unlinked and freed mscb
[09/01/13 11:59:19.361 IST 15a9 5933] 0021.5C8C.C761 Adding mobile on LWAPP AP
C8F9.F983.4260 (1)
[09/01/13 11:59:19.361 IST 15aa 5933] 0021.5C8C.C761 Association received from
mobile on AP C8F9.F983.4260
[09/01/13 11:59:19.361 IST 15ab 5933] 0021.5C8C.C761 qos upstream policy is
unknown and downstream policy is unknown
[09/01/13 11:59:19.361 IST 15ac 5933] 0021.5C8C.C761 apChanged 0 wlanChanged 0
mscb ipAddr 0.0.0.0, apf RadiusOverride 0x0, numIPv6Addr=0
[09/01/13 11:59:19.361 IST 15ad 5933] 0021.5C8C.C761 Applying WLAN policy on MSCB.
[09/01/13 11:59:19.361 IST 15ae 5933] 0021.5C8C.C761 Applying WLAN ACL policies to
client
[09/01/13 11:59:19.361 IST 15af 5933] 0021.5C8C.C761 No Interface ACL used for
Wireless client in WCM(CONVERGEDACCESS)
--More-- [09/01/13 11:59:19.361 IST 15b0 5933] 0021.5C8C.C761 Applying
site-specific IPv6 override for station 0021.5C8C.C761 - vapId 4, site
'default-group', interface 'VLAN0020'
[09/01/13 11:59:19.361 IST 15b1 5933] 0021.5C8C.C761 Applying local bridging
Interface Policy for station 0021.5C8C.C761 - vlan 20, interface 'VLAN0020'
[09/01/13 11:59:19.361 IST 15b2 5933] 0021.5C8C.C761 STA - rates (8):
140 18 152 36 176 72 96 108 0 0 0 0 0 0
[09/01/13 11:59:19.361 IST 15b3 5933] 0021.5C8C.C761 Processing RSN IE type 48,
length 22 for mobile 0021.5C8C.C761
[09/01/13 11:59:19.361 IST 15b4 5933] 0021.5C8C.C761 Received RSN IE with 0 PMKIDs
from mobile 0021.5C8C.C761
[09/01/13 11:59:19.361 IST 15b5 5933] 0021.5C8C.C761 1XK: Looking for BSSID
C8F9.F983.426C in PMKID cache
[09/01/13 11:59:19.361 IST 15b6 5933] 0021.5C8C.C761 1XK: Set Link Secure: 0
[09/01/13 11:59:19.361 IST 15b7 5933] 0021.5C8C.C761 new
capwap_wtp_iif_id b6818000000038, sm capwap_wtp_iif_id 0
[09/01/13 11:59:19.361 IST 15b8 5933] 0021.5C8C.C761 WCDB ADD: Adding opt82 len 0
[09/01/13 11:59:19.361 IST 15b9 5933] 0021.5C8C.C761 WCDB ADD: ssid EAPFAST bssid
C8F9.F983.4260 vlan 20 auth=ASSOCIATION(0) wlan(ap-group/global) 4/4 client 0
assoc 3 mob=Unassoc(0) radio 1 m_vlan 20 ip 0.0.0.0 src 0xb6818000000038 dst 0x0
cid 0x84fd0000000050 glob rsc id 16dhcpsrv 0.0.0.0
[09/01/13 11:59:19.361 IST 15ba 5933] 0021.5C8C.C761 Not Using WMM Compliance code
qosCap 00
--More-- [09/01/13 11:59:19.361 IST 15bb 5933] 0021.5C8C.C761
apfMsAssoStateInc
[09/01/13 11:59:19.361 IST 15bc 5933] 0021.5C8C.C761 apfPemAddUser2
(apf_policy.c:161) Changing state for mobile 0021.5C8C.C761 on AP
C8F9.F983.4260 from Idle to Associated
[09/01/13 11:59:19.361 IST 15bd 5933] 0021.5C8C.C761 Stopping deletion of Mobile
Station: (callerId: 48)
[09/01/13 11:59:19.361 IST 15be 5933] 0021.5C8C.C761 Ms Timeout = 0, Session
Timeout = 1800
[09/01/13 11:59:19.361 IST 15bf 5933] 0021.5C8C.C761 Sending Assoc Response to
station on BSSID C8F9.F983.4260 (status 0) ApVapId 4 Slot 1
[09/01/13 11:59:19.362 IST 15c0 5933] 0021.5C8C.C761 apfProcessAssocReq
(apf_80211.c:5260) Changing state for mobile 0021.5C8C.C761 on AP
C8F9.F983.4260 from Associated to Associated

```

```

[09/01/13 11:59:19.363 IST 15c1 190] [WCDB] ==Add event: type Regular Wireless
client (0021.5c8c.c761) client id (0x84fd0000000050) client index (16) vlan (20)
auth state (ASSOCIATION) mob_state (INIT)
[09/01/13 11:59:19.363 IST 15c2 190] [WCDB] ===intf src/dst (0xb6818000000038)/
(0x0) radio_id (1) p2p_state (P2P_BLOCKING_DISABLE) switch/asic (1/0)
[09/01/13 11:59:19.367 IST 15c3 5933] 0021.5C8C.C761 1XA: Initiating
authentication
[09/01/13 11:59:19.368 IST 15c4 5933] 0021.5C8C.C761 1XA: Setting reauth timeout
to 1800 seconds
--More--
*Sep 1 06:01:59.543: PEM rcv processing msg Del SCB(4) 1 wcm: Time now in sec
1378015280, Last Ac.D^Iwsg Sent at 137801522t! w\2105HnJ^Iw_status 0 attr len
^G$8\227v^K
*Sep 1 06:01:59.547: WCDB_IIF: 1 wcm: Ack Message ID: 0x973c000000004f code 1003
*Sep 1 06:02:50.119: 0021.5C8C.C761
Client stats update: 1 wcm: Time now in sec 1378015370, Last Acct Msg Sent at
1378015224 sec
*Sep 1 06:02:50.119: 0021.5C8C.C761 Requested to send acct interim update request
msg to APF task for client 0: 1 wcm: 21:5c:8c:c7:61 [09/01/13 11:59:19.368
IST 15c5 5933] 0021.5C8C.C761 1XK: Set Link Secure: 0
--More-- [09/01/13 11:59:19.368 IST 15c6 5933] 0021.5C8C.C761 1XA:
Allocated uid 30
[09/01/13 11:59:19.368 IST 15c7 5933] 0021.5C8C.C761 1XA: Calling Auth Mgr to
authenticate client 84fd0000000050 uid 30
--More-- [09/01/13 11:59:19.368 IST 15c8 5933] 0021.5C8C.C761 1XA:
Session Start from wireless client
--More--

[09/01/13 11:59:19.368 IST 15c9 5933] 0021.5C8C.C761 Session Manager Call Client
84fd0000000050, uid 30, capwap id b6818000000038,Flag 0, Audit-Session ID
0a6987b05222d7f30000001e, method list ACS
[09/01/13 11:59:19.368 IST 15ca 33] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
[0021.5c8c.c761, Cal] Session start request from Client[1] for 0021.5c8c.c761
(method: Dot1X, method
list: ACS, aaa id: 0x0000001E)
[09/01/13 11:59:19.368 IST 15cb 33] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
[0021.5c8c.c761, Cal] - client iif_id: 84FD0000000050, session ID:
0a6987b05222d7f30000001e for
0021.5c8c.c761
[09/01/13 11:59:19.368 IST 15cc 33] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
[0021.5c8c.c761, Cal] - eap profile: none
[09/01/13 11:59:19.368 IST 15cd 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Received session event 'SESSION_START' from client
[09/01/13 11:59:19.368 IST 15ce 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Session start for 0021.5c8c.c761
[09/01/13 11:59:19.368 IST 15cf 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Found 2 sessions on this port, checking host limit
[09/01/13 11:59:19.368 IST 15d0 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Using stored AAA ID 0x0000001E
[09/01/13 11:59:19.368 IST 15d1 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Retrieved Client IIF ID 84FD0000000050
[09/01/13 11:59:19.368 IST 15d2 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Allocated new Auth Manager context (handle 0x32000026)
--More-- [09/01/13 11:59:19.368 IST 15d3 173] ACCESS-CORE-SM-DEB:
[0021.5c8c.c761, Cal] Client 0021.5c8c.c761, Initialising Method state to
'Not run'
[09/01/13 11:59:19.368 IST 15d4 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal]
Adding method Session Mgr IPDT Shim to runnable list for session 0x32000026
[09/01/13 11:59:19.368 IST 15d5 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal]
Client 0021.5c8c.c761, Initialising Method SVM state to 'Not run'
[09/01/13 11:59:19.368 IST 15d6 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal]
Adding method SVM to runnable list for session 0x32000026
[09/01/13 11:59:19.368 IST 15d7 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal]
Client 0021.5c8c.c761, Initialising Method state to 'Not run'
[09/01/13 11:59:19.368 IST 15d8 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal]
Adding method Switch PI to runnable list for session 0x32000026
[09/01/13 11:59:19.368 IST 15d9 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal]
Client 0021.5c8c.c761, Initialising Method state to 'Not run'
[09/01/13 11:59:19.368 IST 15da 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal]
Adding method Session Mgr SIFS Shim to runnable list for session 0x32000026
[09/01/13 11:59:19.368 IST 15db 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal]
Client 0021.5c8c.c761, Initialising Method iaf state to 'Not run'
[09/01/13 11:59:19.368 IST 15dc 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal]

```

```

Adding method iaf to runnable list for session 0x32000026
[09/01/13 11:59:19.368 IST 15dd 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal]
Client 0021.5c8c.c761, Initialising Method Tag state to 'Not run'
[09/01/13 11:59:19.368 IST 15de 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal]
Adding method Tag to runnable list for session 0x32000026
--More-- [09/01/13 11:59:19.368 IST 15df 173] ACCESS-CORE-SM-DEB:
[0021.5c8c.c761, Cal] Client 0021.5c8c.c761, Initialising Method dct state to
'Not run'
[09/01/13 11:59:19.368 IST 15e0 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal]
Adding method dct to runnable list for session 0x32000026
[09/01/13 11:59:19.368 IST 15e1 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal]
Client 0021.5c8c.c761, Initialising Method SM Reauth Plugin state to 'Not run'
[09/01/13 11:59:19.368 IST 15e2 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal]
Adding method SM Reauth Plugin to runnable list for session 0x32000026
[09/01/13 11:59:19.368 IST 15e3 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal]
Client 0021.5c8c.c761, Initialising Method SM Accounting Feature state to 'Not run'
[09/01/13 11:59:19.368 IST 15e4 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal]
Adding method SM Accounting Feature to runnable list for session 0x32000026
[09/01/13 11:59:19.368 IST 15e5 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal]
Client 0021.5c8c.c761, Initialising Method state to 'Not run'
[09/01/13 11:59:19.368 IST 15e6 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal]
Adding method Session Mgr FFCP Shim to runnable list for session 0x32000026
[09/01/13 11:59:19.368 IST 15e7 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal]
Client 0021.5c8c.c761, Initialising Method state to 'Not run'
[09/01/13 11:59:19.368 IST 15e8 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal]
Adding method AIM to runnable list for session 0x32000026
[09/01/13 11:59:19.368 IST 15e9 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal]
Client 0021.5c8c.c761, Initialising Method dot1x state to 'Not run'
[09/01/13 11:59:19.368 IST 15ea 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal]
Adding method dot1x to runnable list for session 0x32000026
--More-- [09/01/13 11:59:19.368 IST 15eb 173] ACCESS-CORE-SM-DEB:
[0021.5c8c.c761, Cal] Client 0021.5c8c.c761, Initialising Method mab state to
'Not run'
[09/01/13 11:59:19.368 IST 15ec 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal]
Adding method mab to runnable list for session 0x32000026
[09/01/13 11:59:19.368 IST 15ed 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal]
Client 0021.5c8c.c761, Initialising Method webauth state to 'Not run'
[09/01/13 11:59:19.368 IST 15ee 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal]
Adding method webauth to runnable list for session 0x32000026
[09/01/13 11:59:19.368 IST 15ef 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Processing SM CB request for 0x32000026: Event: New client notification (201)
[09/01/13 11:59:19.368 IST 15f0 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal]
Create attr list, session 0x32000026:
[09/01/13 11:59:19.368 IST 15f1 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal] -
adding MAC 0021.5c8c.c761
[09/01/13 11:59:19.368 IST 15f2 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal] -
adding Swidb 0x99E27F00
[09/01/13 11:59:19.368 IST 15f3 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal] -
adding AAA ID=1E
[09/01/13 11:59:19.368 IST 15f4 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal] -
adding Audit_sid=0a6987b05222d7f30000001e
[09/01/13 11:59:19.368 IST 15f5 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal] -
adding IIF ID=0x84FD0000000050
[09/01/13 11:59:19.368 IST 15f6 173] ACCESS-CORE-SM-CLIENT-IPDT-NOTF:
[0021.5c8c.c761, Cal] NewClient: No entry for 0021.5c8c.c761. session 0x32000026
--More-- [09/01/13 11:59:19.368 IST 15f7 173] ACCESS-CORE-SM-NOTF:
[0021.5c8c.c761, Cal] New client 0021.5c8c.c761 - client handle 0x00000001 for SVM
[09/01/13 11:59:19.368 IST 15f8 173] ACCESS-CORE-SM-CLIENT-SISF-NOTF:
[0021.5c8c.c761, Cal] No IPv6 binding found for 0021.5c8c.c761(0x32000026)
[09/01/13 11:59:19.368 IST 15f9 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Added record to DB - hdl 0x32000026 / 0021.5c8c.c761. 3 session(s) on IDB
[09/01/13 11:59:19.368 IST 15fa 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal]
Add record - adding MAC 0021.5c8c.c761
[09/01/13 11:59:19.368 IST 15fb 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal]
Add record - adding SWIDB Capwap1
[09/01/13 11:59:19.368 IST 15fc 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal]
Add record - adding AAA-ID 1E
[09/01/13 11:59:19.368 IST 15fd 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal]
Add record - adding AUDIT-ID 0a6987b05222d7f30000001e
[09/01/13 11:59:19.368 IST 15fe 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal] Add
record - adding IIF-ID 0x84FD0000000050
[09/01/13 11:59:19.368 IST 15ff 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal] Add
record - adding TARGET_SCOPE (Client)

```

```

[09/01/13 11:59:19.368 IST 1600 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal] No
policy handle to bind session
[09/01/13 11:59:19.368 IST 1601 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal]
Create attr list, session 0x32000026:
[09/01/13 11:59:19.368 IST 1602 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal] -
adding MAC 0021.5c8c.c761
--More--      [09/01/13 11:59:19.368 IST 1603 173] ACCESS-CORE-SM-DEB:
[0021.5c8c.c761, Cal] - adding Swidb 0x99E27F00
[09/01/13 11:59:19.368 IST 1604 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal] -
adding AAA_ID=1E
[09/01/13 11:59:19.368 IST 1605 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal] -
adding Audit_sid=0a6987b05222d7f30000001e
[09/01/13 11:59:19.368 IST 1606 173] ACCESS-CORE-SM-DEB: [0021.5c8c.c761, Cal] -
adding IIF_ID=0x84FD0000000050
[09/01/13 11:59:19.368 IST 1607 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Processing SM CB request for 0x32000026: Event: Start a method (200)
[09/01/13 11:59:19.368 IST 1608 173] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761,
Cal] 0xA100000F: initialising
[09/01/13 11:59:19.368 IST 1609 173] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761,
Cal] 0xA100000F: disconnected
[09/01/13 11:59:19.368 IST 160a 173] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761,
Cal] 0xA100000F: entering restart
[09/01/13 11:59:19.368 IST 160b 173] ACCESS-METHOD-DOT1X-NOTF: [0021.5c8c.c761,
Cal] Override cfg - MAC 0021.5c8c.c761 - profile (none)
[09/01/13 11:59:19.368 IST 160c 173] ACCESS-METHOD-DOT1X-NOTF: [0021.5c8c.c761,
Cal] Override cfg - SuppTimeout 30s, ReAuthMax 2, MaxReq 2, TxPeriod 30s
[09/01/13 11:59:19.368 IST 160d 173] ACCESS-METHOD-DOT1X-NOTF: [0021.5c8c.c761,
Cal] Sending create new context event to EAP for 0xA100000F (0021.5c8c.c761)
[09/01/13 11:59:19.368 IST 160e 173] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761,
Cal] 0xA100000F: entering init state
--More--      [09/01/13 11:59:19.368 IST 160f 173] ACCESS-METHOD-DOT1X-DEB:
[0021.5c8c.c761, Cal] 0xA100000F:entering idle state
[09/01/13 11:59:19.368 IST 1610 173] ACCESS-METHOD-DOT1X-NOTF: [0021.5c8c.c761,
Cal] Created a client entry (0xA100000F)
[09/01/13 11:59:19.368 IST 1611 173] ACCESS-METHOD-DOT1X-NOTF: [0021.5c8c.c761,
Cal] Dot1x authentication started for 0xA100000F (0021.5c8c.c761)
[09/01/13 11:59:19.368 IST 1612 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Client 0021.5c8c.c761, Context changing state from 'Idle' to 'Running'
[09/01/13 11:59:19.368 IST 1613 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Client 0021.5c8c.c761, Method dot1x changing state from 'Not run' to 'Running'
[09/01/13 11:59:19.368 IST 1614 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
SM will not apply policy for SESSION STARTED on 0x32000026 / 0021.5c8c.c761
[09/01/13 11:59:19.368 IST 1615 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Processing default action(s) for event SESSION STARTED for session 0x32000026.
[09/01/13 11:59:19.368 IST 1616 179] ACCESS-CORE-SM-CLIENT-DOT11-NOTF:
[0021.5c8c.c761, Cal] DB alloc for 0021.5c8c.c761
[09/01/13 11:59:19.368 IST 1617 179] ACCESS-CORE-SM-CLIENT-DOT11-NOTF:
[0021.5c8c.c761, Cal] Dot11 params, bssid: c8f9.f983.4260, radio id: 1, wlan id: 4,
assoc id: 3, ssid: EAPFAST
[09/01/13 11:59:19.368 IST 1618 179] ACCESS-CORE-SM-CLIENT-DOT11-NOTF:
[0021.5c8c.c761, Cal] Dot11 params, wlan bssid set to: c8f9.f983.426c
[09/01/13 11:59:19.368 IST 1619 262] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
Posting !EAP RESTART on Client 0xA100000F
[09/01/13 11:59:19.368 IST 161a 262] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
0xA100000F:enter connecting state
--More--      [09/01/13 11:59:19.368 IST 161b 262] ACCESS-METHOD-DOT1X-DEB:
[0021.5c8c.c761, Cal] 0xA100000F: restart connecting
[09/01/13 11:59:19.368 IST 161c 262] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
Posting RX_REQ on Client 0xA100000F
[09/01/13 11:59:19.368 IST 161d 262] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
0xA100000F: authenticating state entered
[09/01/13 11:59:19.368 IST 161e 262] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
0xA100000F:connecting authenticating action
[09/01/13 11:59:19.368 IST 161f 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
Posting AUTH_START for 0xA100000F
[09/01/13 11:59:19.368 IST 1620 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
0xA100000F:entering request state
[09/01/13 11:59:19.368 IST 1621 270] ACCESS-METHOD-DOT1X-NOTF: [0021.5c8c.c761, Cal]
Sending EAPOL packet
[09/01/13 11:59:19.368 IST 1622 270] ACCESS-METHOD-DOT1X-INFO: [0021.5c8c.c761, Cal]
Platform changed src mac of EAPOL packet
[09/01/13 11:59:19.368 IST 1623 270] ACCESS-METHOD-DOT1X-INFO: [0021.5c8c.c761, Cal]
EAPOL packet sent to client 0xA100000F

```

```
[09/01/13 11:59:19.368 IST 1624 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
  0xA100000F:idle request action
[09/01/13 11:59:19.500 IST 1625 176] ACCESS-METHOD-DOT1X-INFO: [0021.5c8c.c761, Cal]
  Queuing an EAPOL pkt on Authenticator Q
[09/01/13 11:59:19.500 IST 1626 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal] SM
  will not apply policy for RX_METHOD_AGENT_FOUND on 0x32000026 / 0021.5c8c.c761
--More-- [09/01/13 11:59:19.500 IST 1627 173] ACCESS-CORE-SM-NOTF:
  [0021.5c8c.c761, Cal] Processing default action(s) for event RX_METHOD_AGENT_FOUND
  for session 0x32000026.
[09/01/13 11:59:19.500 IST 1628 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761,
  Cal]
  Posting EAPOL_EAP for 0xA100000F
[09/01/13 11:59:19.500 IST 1629 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
  0xA100000F:entering response state
[09/01/13 11:59:19.500 IST 162a 270] ACCESS-METHOD-DOT1X-NOTF: [0021.5c8c.c761, Cal]
  Response sent to the server from 0xA100000F
[09/01/13 11:59:19.500 IST 162b 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
  0xA100000F:request response action
[09/01/13 11:59:19.503 IST 162c 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
  Posting EAP_REQ for 0xA100000F
[09/01/13 11:59:19.503 IST 162d 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
  0xA100000F:exiting response state
[09/01/13 11:59:19.503 IST 162e 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
  0xA100000F:entering request state
[09/01/13 11:59:19.503 IST 162f 270] ACCESS-METHOD-DOT1X-NOTF: [0021.5c8c.c761, Cal]
  Sending EAPOL packet
[09/01/13 11:59:19.503 IST 1630 270] ACCESS-METHOD-DOT1X-INFO: [0021.5c8c.c761, Cal]
  Platform changed src mac of EAPOL packet
[09/01/13 11:59:19.503 IST 1631 270] ACCESS-METHOD-DOT1X-INFO: [0021.5c8c.c761, Cal]
  EAPOL packet sent to client 0xA100000F
[09/01/13 11:59:19.503 IST 1632 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
  0xA100000F:response request action
--More-- [09/01/13 11:59:19.525 IST 1633 176] ACCESS-METHOD-DOT1X-INFO:
  [0021.5c8c.c761, Cal] Queuing an EAPOL pkt on Authenticator Q
[09/01/13 11:59:19.525 IST 1634 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
  Posting EAPOL_EAP for 0xA100000F
[09/01/13 11:59:19.525 IST 1635 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
  0xA100000F:entering response state
[09/01/13 11:59:19.525 IST 1636 270] ACCESS-METHOD-DOT1X-NOTF: [0021.5c8c.c761, Cal]
  Response sent to the server from 0xA100000F
[09/01/13 11:59:19.525 IST 1637 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
  0xA100000F:request response action
[09/01/13 11:59:19.529 IST 1638 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
  Posting EAP_REQ for 0xA100000F
[09/01/13 11:59:19.529 IST 1639 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
  0xA100000F:exiting response state
[09/01/13 11:59:19.529 IST 163a 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
  0xA100000F:entering request state
[09/01/13 11:59:19.529 IST 163b 270] ACCESS-METHOD-DOT1X-NOTF: [0021.5c8c.c761, Cal]
  Sending EAPOL packet
[09/01/13 11:59:19.529 IST 163c 270] ACCESS-METHOD-DOT1X-INFO: [0021.5c8c.c761, Cal]
  Platform changed src mac of EAPOL packet
[09/01/13 11:59:19.529 IST 163d 270] ACCESS-METHOD-DOT1X-INFO: [0021.5c8c.c761, Cal]
  EAPOL packet sent to client 0xA100000F
[09/01/13 11:59:19.529 IST 163e 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
  0xA100000F:response request action
--More-- [09/01/13 11:59:21.191 IST 163f 176] ACCESS-METHOD-DOT1X-INFO:
  [0021.5c8c.c761, Cal] Queuing an EAPOL pkt on Authenticator Q
[09/01/13 11:59:21.191 IST 1640 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
  Posting EAPOL_EAP for 0xA100000F
[09/01/13 11:59:21.191 IST 1641 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
  0xA100000F:entering response state
[09/01/13 11:59:21.191 IST 1642 270] ACCESS-METHOD-DOT1X-NOTF: [0021.5c8c.c761, Cal]
  Response sent to the server from 0xA100000F
[09/01/13 11:59:21.191 IST 1643 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
  0xA100000F:request response action
[09/01/13 11:59:21.194 IST 1644 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
  Posting EAP_REQ for 0xA100000F
[09/01/13 11:59:21.194 IST 1645 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
  0xA100000F:exiting response state
[09/01/13 11:59:21.194 IST 1646 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
  0xA100000F:entering request state
[09/01/13 11:59:21.194 IST 1647 270] ACCESS-METHOD-DOT1X-NOTF: [0021.5c8c.c761, Cal]
```

```

Sending EAPOL packet
[09/01/13 11:59:21.194 IST 1648 270] ACCESS-METHOD-DOT1X-INFO: [0021.5c8c.c761, Ca1]
Platform changed src mac of EAPOL packet
[09/01/13 11:59:21.194 IST 1649 270] ACCESS-METHOD-DOT1X-INFO: [0021.5c8c.c761, Ca1]
EAPOL packet sent to client 0xA100000F
[09/01/13 11:59:21.194 IST 164a 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Ca1]
0xA100000F:response request action
--More--      [09/01/13 11:59:21.201 IST 164b 176] ACCESS-METHOD-DOT1X-INFO:
[0021.5c8c.c761, Ca1] Queuing an EAPOL pkt on Authenticator Q
[09/01/13 11:59:21.201 IST 164c 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Ca1]
Posting EAPOL EAP for 0xA100000F
[09/01/13 11:59:21.201 IST 164d 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Ca1]
0xA100000F:entering response state
[09/01/13 11:59:21.201 IST 164e 270] ACCESS-METHOD-DOT1X-NOTF: [0021.5c8c.c761, Ca1]
Response sent to the server from 0xA100000F
[09/01/13 11:59:21.201 IST 164f 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Ca1]
0xA100000F:request response action
[09/01/13 11:59:21.203 IST 1650 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Ca1]
Posting EAP_REQ for 0xA100000F
[09/01/13 11:59:21.203 IST 1651 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Ca1]
0xA100000F:exiting response state
[09/01/13 11:59:21.203 IST 1652 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Ca1]
0xA100000F:entering request state
[09/01/13 11:59:21.203 IST 1653 270] ACCESS-METHOD-DOT1X-NOTF: [0021.5c8c.c761, Ca1]
Sending EAPOL packet
[09/01/13 11:59:21.203 IST 1654 270] ACCESS-METHOD-DOT1X-INFO: [0021.5c8c.c761, Ca1]
Platform changed src mac of EAPOL packet
[09/01/13 11:59:21.203 IST 1655 270] ACCESS-METHOD-DOT1X-INFO: [0021.5c8c.c761, Ca1]
EAPOL packet sent to client 0xA100000F
[09/01/13 11:59:21.203 IST 1656 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Ca1]
0xA100000F:response request action
--More--      [09/01/13 11:59:21.213 IST 1657 176] ACCESS-METHOD-DOT1X-INFO:
[0021.5c8c.c761, Ca1] Queuing an EAPOL pkt on Authenticator Q
[09/01/13 11:59:21.213 IST 1658 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Ca1]
Posting EAPOL EAP for 0xA100000F
[09/01/13 11:59:21.213 IST 1659 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Ca1]
0xA100000F:entering response state
[09/01/13 11:59:21.213 IST 165a 270] ACCESS-METHOD-DOT1X-NOTF: [0021.5c8c.c761, Ca1]
Response sent to the server from 0xA100000F
[09/01/13 11:59:21.213 IST 165b 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Ca1]
0xA100000F:request response action
[09/01/13 11:59:21.220 IST 165c 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Ca1]
Posting EAP_REQ for 0xA100000F
[09/01/13 11:59:21.220 IST 165d 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Ca1]
0xA100000F:exiting response state
[09/01/13 11:59:21.220 IST 165e 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Ca1]
0xA100000F:entering request state
[09/01/13 11:59:21.220 IST 165f 270] ACCESS-METHOD-DOT1X-NOTF: [0021.5c8c.c761, Ca1]
Sending EAPOL packet
[09/01/13 11:59:21.220 IST 1660 270] ACCESS-METHOD-DOT1X-INFO: [0021.5c8c.c761, Ca1]
Platform changed src mac of EAPOL packet
[09/01/13 11:59:21.220 IST 1661 270] ACCESS-METHOD-DOT1X-INFO: [0021.5c8c.c761, Ca1]
EAPOL packet sent to client 0xA100000F
[09/01/13 11:59:21.220 IST 1662 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Ca1]
0xA100000F:response request action
--More--      [09/01/13 11:59:21.224 IST 1663 176] ACCESS-METHOD-DOT1X-INFO:
[0021.5c8c.c761, Ca1] Queuing an EAPOL pkt on Authenticator Q
[09/01/13 11:59:21.224 IST 1664 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Ca1]
Posting EAPOL EAP for 0xA100000F
[09/01/13 11:59:21.224 IST 1665 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Ca1]
0xA100000F:entering response state
[09/01/13 11:59:21.224 IST 1666 270] ACCESS-METHOD-DOT1X-NOTF: [0021.5c8c.c761, Ca1]
Response sent to the server from 0xA100000F
[09/01/13 11:59:21.224 IST 1667 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Ca1]
0xA100000F:request response action
[09/01/13 11:59:21.227 IST 1668 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Ca1]
Posting EAP_REQ for 0xA100000F
[09/01/13 11:59:21.227 IST 1669 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Ca1]
0xA100000F:exiting response state
[09/01/13 11:59:21.227 IST 166a 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Ca1]
0xA100000F:entering request state
[09/01/13 11:59:21.227 IST 166b 270] ACCESS-METHOD-DOT1X-NOTF: [0021.5c8c.c761, Ca1]
Sending EAPOL packet

```

```

[09/01/13 11:59:21.227 IST 166c 270] ACCESS-METHOD-DOT1X-INFO: [0021.5c8c.c761, Cal]
Platform changed src mac of EAPOL packet
[09/01/13 11:59:21.227 IST 166d 270] ACCESS-METHOD-DOT1X-INFO: [0021.5c8c.c761, Cal]
EAPOL packet sent to client 0xA100000F
[09/01/13 11:59:21.227 IST 166e 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
0xA100000F:response request action
--More-- [09/01/13 11:59:21.235 IST 166f 176] ACCESS-METHOD-DOT1X-INFO:
[0021.5c8c.c761, Cal] Queuing an EAPOL pkt on Authenticator Q
[09/01/13 11:59:21.235 IST 1670 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
Posting EAPOL EAP for 0xA100000F
[09/01/13 11:59:21.235 IST 1671 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
0xA100000F:entering response state
[09/01/13 11:59:21.235 IST 1672 270] ACCESS-METHOD-DOT1X-NOTF: [0021.5c8c.c761, Cal]
Response sent to the server from 0xA100000F
[09/01/13 11:59:21.235 IST 1673 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
0xA100000F:request response action
[09/01/13 11:59:21.238 IST 1674 179] ACCESS-METHOD-DOT1X-INFO: [0021.5c8c.c761, Cal]
Received an EAP Success
[09/01/13 11:59:21.238 IST 1675 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
Posting EAP SUCCESS for 0xA100000F
[09/01/13 11:59:21.238 IST 1676 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
0xA100000F:exiting response state
[09/01/13 11:59:21.238 IST 1677 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
0xA100000F:entering success state
[09/01/13 11:59:21.238 IST 1678 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
0xA100000F:response success action
[09/01/13 11:59:21.238 IST 1679 270] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
00xA100000F:entering idle state
[09/01/13 11:59:21.238 IST 167a 262] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
Posting AUTH_SUCCESS on Client 0xA100000F
--More-- [09/01/13 11:59:21.238 IST 167b 262] ACCESS-METHOD-DOT1X-DEB:
[0021.5c8c.c761, Cal] 0xA100000F:exiting authenticating state
[09/01/13 11:59:21.238 IST 167c 262] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Cal]
0xA100000F:entering authc result state
[09/01/13 11:59:21.238 IST 167d 262] ACCESS-METHOD-DOT1X-NOTF: [0021.5c8c.c761, Cal]
Sending EAPOL success immediately
[09/01/13 11:59:21.238 IST 167e 262] ACCESS-METHOD-DOT1X-NOTF: [0021.5c8c.c761, Cal]
Sending EAPOL packet
[09/01/13 11:59:21.238 IST 167f 262] ACCESS-METHOD-DOT1X-INFO: [0021.5c8c.c761, Cal]
Platform changed src mac of EAPOL packet
[09/01/13 11:59:21.239 IST 1680 262] ACCESS-METHOD-DOT1X-INFO: [0021.5c8c.c761, Cal]
EAPOL packet sent to client 0xA100000F
[09/01/13 11:59:21.239 IST 1681 262] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Authc success from Dot1X (1), status OK (0) / event success (0)
[09/01/13 11:59:21.239 IST 1682 262] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Highest prio method: INVALID, Authz method: INVALID, Conn hdl: dot1x
[09/01/13 11:59:21.239 IST 1683 262] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Queued AUTHC SUCCESS from Dot1X for session 0x32000026 (0021.5c8c.c761)
[09/01/13 11:59:21.239 IST 1684 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Received internal event APPLY_USER_PROFILE (handle 0x32000026)
[09/01/13 11:59:21.239 IST 1685 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Clearing AAA data for: 0021.5c8c.c761
[09/01/13 11:59:21.239 IST 1686 173] ACCESS-CORE-SM-SYNC-NOTF: [0021.5c8c.c761, Cal]
Delay add/update sync of username for 0021.5c8c.c761 / 0x32000026
--More-- [09/01/13 11:59:21.239 IST 1687 173] ACCESS-CORE-SM-NOTF:
[0021.5c8c.c761, Cal] Received User-Name user for client 0021.5c8c.c761
[09/01/13 11:59:21.239 IST 1688 173] ACCESS-CORE-SM-SYNC-NOTF: [0021.5c8c.c761, Cal]
Delay add/update sync of auth-domain for 0021.5c8c.c761 / 0x32000026
[09/01/13 11:59:21.239 IST 1689 173] ACCESS-CORE-SM-SYNC-NOTF: [0021.5c8c.c761, Cal]
Delay add/update sync of target-scope for 0021.5c8c.c761 / 0x32000026
[09/01/13 11:59:21.239 IST 168a 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Existing AAA ID: 0x0000001E
[09/01/13 11:59:21.239 IST 168b 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Client 0021.5c8c.c761, Method dot1x changing state from 'Running' to 'Authc Success'
[09/01/13 11:59:21.239 IST 168c 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Client 0021.5c8c.c761, Context changing state from 'Running' to 'Authc Success'
[09/01/13 11:59:21.239 IST 168d 173] ACCESS-CORE-SM-CLIENT-DOT11-NOTF:
[0021.5c8c.c761, Cal] Applying authz attrs - 0x1D0003FF
[09/01/13 11:59:21.239 IST 168e 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Cal]
Non-SM policy applied for 0x32000026. Authz attrs not freed
[09/01/13 11:59:21.239 IST 168f 173] ACCESS-CORE-SM-SYNC-NOTF: [0021.5c8c.c761, Cal]
Delay add/update sync of method for 0021.5c8c.c761 / 0x32000026
[09/01/13 11:59:21.239 IST 1690 173] ACCESS-CORE-SM-CLIENT-DOT11-NOTF:

```

```

[0021.5c8c.c761, Ca1] Dot11: authz success signalled for 0021.5c8c.c761
[09/01/13 11:59:21.239 IST 1691 173] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
[0021.5c8c.c761, Ca1] Session authz status notification sent to Client[1] for
0021.5c8c.c761 with handle CE38188, list 1D0003FF
--More-- [09/01/13 11:59:21.239 IST 1692 173] ACCESS-CORE-SM-NOTF:
[0021.5c8c.c761, Ca1] SM will not apply policy for RX_METHOD_AUTHC_SUCCESS on
0x32000026 / 0021.5c8c.c761
[09/01/13 11:59:21.239 IST 1693 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Ca1]
Processing default action(s) for event RX_METHOD_AUTHC_SUCCESS for session
0x32000026.
[09/01/13 11:59:21.239 IST 1694 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Ca1]
Executing default action handler for AUTHC SUCCESS (0x32000026)
[09/01/13 11:59:21.239 IST 1695 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Ca1]
AUTHC_SUCCESS - authorize by default
[09/01/13 11:59:21.239 IST 1696 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Ca1]
Signalling Authz success for client 0021.5c8c.c761
[09/01/13 11:59:21.239 IST 1697 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Ca1]
Client 0021.5c8c.c761, Context changing state from 'Authc Success' to 'Authz
Success'
[09/01/13 11:59:21.239 IST 1698 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Ca1]
Processing SM CB request for 0x32000026: Event: Authorize request (216)
[09/01/13 11:59:21.239 IST 1699 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Ca1]
Authz complete (SUCCESS) for client 0021.5c8c.c761/0x32000026 reported
[09/01/13 11:59:21.239 IST 169a 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Ca1]
Received internal event AUTHZ SUCCESS (handle 0x32000026)
[09/01/13 11:59:21.239 IST 169b 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Ca1]
Processing AUTHZ CB RESULT (success) for 0x32000026
[09/01/13 11:59:21.239 IST 169c 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Ca1]
Processing SM CB request for 0x32000026: Event: Authz result processed (215)
--More-- [09/01/13 11:59:21.239 IST 169d 173] ACCESS-CORE-SM-NOTF:
[0021.5c8c.c761, Ca1] Authz result processed, result: 0
[09/01/13 11:59:21.239 IST 169e 173] ACCESS-METHOD-DOT1X-NOTF: [0021.5c8c.c761, Ca1]
Received Authz Success for the client 0xA100000F (0021.5c8c.c761)
[09/01/13 11:59:21.239 IST 169f 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Ca1] SM
Reauth Plugin: Client authz change, result=Success
[09/01/13 11:59:21.239 IST 16a0 173] ACCESS-CORE-SM-NOTF: [0021.5c8c.c761, Ca1]
Signalling Authz complete (success) for client 0x32000026
[09/01/13 11:59:21.239 IST 16a1 262] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Ca1]
Posting AUTHZ SUCCESS on Client 0xA100000F
[09/01/13 11:59:21.239 IST 16a2 262] ACCESS-METHOD-DOT1X-DEB: [0021.5c8c.c761, Ca1]
0xA100000F:entering authenticated state
[09/01/13 11:59:21.239 IST 16a3 262] ACCESS-METHOD-DOT1X-NOTF: [0021.5c8c.c761, Ca1]
EAPOL success packet was sent earlier.
[09/01/13 11:59:21.239 IST 16a4 5933] 0021.5C8C.C761 1XA: received authentication
response, status=0 AAA ID=0 protocol=0
[09/01/13 11:59:21.239 IST 16a5 5933] 0021.5C8C.C761 1XA: Handling status
notification request from dot1x, uid=30/0
[09/01/13 11:59:21.239 IST 16a6 5933] 0021.5C8C.C761
client incoming attribute size are 485
[09/01/13 11:59:21.239 IST 16a7 5933] 0021.5C8C.C761 1XA: received RADIUS attr
type 450
[09/01/13 11:59:21.239 IST 16a8 5933] 0021.5C8C.C761 1XA: received RADIUS attr
type 450
--More-- [09/01/13 11:59:21.239 IST 16a9 5933] 0021.5C8C.C761 1XA:
received RADIUS attr type 383
[09/01/13 11:59:21.239 IST 16aa 5933] 0021.5C8C.C761 1XA: received RADIUS attr
type 383
[09/01/13 11:59:21.239 IST 16ab 5933] 0021.5C8C.C761 1XA: received RADIUS attr
type 87
[09/01/13 11:59:21.239 IST 16ac 5933] 0021.5C8C.C761 1XA: received RADIUS attr
type 87
[09/01/13 11:59:21.239 IST 16ad 5933] 0021.5C8C.C761 1XA: received RADIUS attr
type 274
[09/01/13 11:59:21.239 IST 16ae 5933] 0021.5C8C.C761 1XA: received RADIUS attr
type 274
[09/01/13 11:59:21.239 IST 16af 5933] 0021.5C8C.C761 1XA: received RADIUS attr
type 88
[09/01/13 11:59:21.239 IST 16b0 5933] 0021.5C8C.C761 1XA: received RADIUS attr
type 88
[09/01/13 11:59:21.239 IST 16b1 5933] 0021.5C8C.C761 1XA: received RADIUS attr
type 661
[09/01/13 11:59:21.239 IST 16b2 5933] 0021.5C8C.C761 1XA: received RADIUS attr
type 661

```



```

[09/01/13 11:59:21.239 IST 16b3 5933] 0021.5C8C.C761 1XA: received RADIUS attr
type 662
[09/01/13 11:59:21.239 IST 16b4 5933] 0021.5C8C.C761 1XA: received RADIUS attr
type 662
--More--          [09/01/13 11:59:21.239 IST 16b5 5933] 0021.5C8C.C761 1XA:
received RADIUS attr type 82
[09/01/13 11:59:21.239 IST 16b6 5933] 0021.5C8C.C761 1XA: received RADIUS attr
type 82
[09/01/13 11:59:21.239 IST 16b7 5933] 0021.5C8C.C761 1XA: received RADIUS attr
type 37
[09/01/13 11:59:21.239 IST 16b8 5933] 0021.5C8C.C761 1XA: received RADIUS attr
type 37
[09/01/13 11:59:21.239 IST 16b9 5933] 0021.5C8C.C761 1XA: received RADIUS attr
type 819
[09/01/13 11:59:21.239 IST 16ba 5933] 0021.5C8C.C761 1XA: received RADIUS attr
type 819
[09/01/13 11:59:21.239 IST 16bb 5933] 0021.5C8C.C761 Applying new AAA override for
station 0021.5C8C.C761
[09/01/13 11:59:21.239 IST 16bc 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1  vlanIfName: '',
aclName: ''
[09/01/13 11:59:21.239 IST 16bd 5933] 0021.5C8C.C761 Not applying override policy -
allow override is FALSE
[09/01/13 11:59:21.239 IST 16be 5933] 0021.5C8C.C761 1XA: Setting reauth timeout to
1800 seconds from WLAN config
[09/01/13 11:59:21.239 IST 16bf 5933] 0021.5C8C.C761 1XA: Setting reauth timeout to
1800 seconds
--More--          [09/01/13 11:59:21.239 IST 16c0 5933] 0021.5C8C.C761 1XK: Creating
a PKC PMKID Cache entry (RSN 1)
[09/01/13 11:59:21.239 IST 16c1 5933] 0021.5C8C.C761 1XK: Set Link Secure: 0
[09/01/13 11:59:21.239 IST 16c2 5933] 0021.5C8C.C761 1XK: Set Link Secure: 0
[09/01/13 11:59:21.239 IST 16c3 5933] 0021.5C8C.C761 1XK: Looking for BSSID
C8F9.F983.426C in PMKID cache
[09/01/13 11:59:21.239 IST 16c4 5933] 0021.5C8C.C761 1XK: Adding BSSID
C8F9.F983.426C to PMKID cache
[09/01/13 11:59:21.239 IST 16c5 5933] 0021.5C8C.C761 1XA: Disabling reauth - using
PMK lifetime instead
[09/01/13 11:59:21.239 IST 16c6 5933] 0021.5C8C.C761 Radius overrides disabled,
ignoring source 4
[09/01/13 11:59:21.239 IST 16c7 5933] 0021.5C8C.C761 Radius overrides disabled,
ignoring source 4
[09/01/13 11:59:21.239 IST 16c8 5933] 0021.5C8C.C761 Radius overrides disabled,
ignoring source 4
[09/01/13 11:59:21.239 IST 16c9 5933] 0021.5C8C.C761 PMK sent to mobility group
[09/01/13 11:59:21.239 IST 16ca 5933] 0021.5C8C.C761 1XA: authentication succeeded
[09/01/13 11:59:21.239 IST 16cb 5933] 0021.5C8C.C761 1XK: Looking for BSSID
C8F9.F983.426C in PMKID cache
[09/01/13 11:59:21.239 IST 16cc 5933] 0021.5C8C.C761 1XK: Looking for BSSID
C8F9.F983.426C in PMKID cache
--More--          [09/01/13 11:59:21.239 IST 16cd 5933] 0021.5C8C.C761 Starting key
exchange with mobile - data forwarding is disabled
[09/01/13 11:59:21.239 IST 16ce 5933] 0021.5C8C.C761 1XA: Sending EAPOL message to
mobile, WLAN=4 AP WLAN=4
[09/01/13 11:59:21.246 IST 16cf 5933] 0021.5C8C.C761 1XA: Received 802.11 EAPOL
message (len 123) from mobile
[09/01/13 11:59:21.246 IST 16d0 5933] 0021.5C8C.C761 1XA: Received EAPOL-Key from
mobile
[09/01/13 11:59:21.246 IST 16d1 5933] 0021.5C8C.C761 1XK: Received EAPOL-key in
PTK START state (msg 2) from mobile
[09/01/13 11:59:21.246 IST 16d2 5933] 0021.5C8C.C761 1XK: Stopping retransmission
timer
[09/01/13 11:59:21.246 IST 16d3 5933] 0021.5C8C.C761 1XA: Sending EAPOL message to
mobile, WLAN=4 AP WLAN=4
[09/01/13 11:59:21.258 IST 16d4 5933] 0021.5C8C.C761 1XA: Received 802.11 EAPOL
message (len 99) from mobile
[09/01/13 11:59:21.258 IST 16d5 5933] 0021.5C8C.C761 1XA: Received EAPOL-Key from
mobile
[09/01/13 11:59:21.258 IST 16d6 5933] 0021.5C8C.C761 1XK: Received EAPOL-key in
PTKINITNEGOTIATING state (msg 4) from mobile
[09/01/13 11:59:21.258 IST 16d7 5933] 0021.5C8C.C761 1XK: Set Link Secure: 1
[09/01/13 11:59:21.258 IST 16d8 5933] 0021.5C8C.C761 1XK: Key exchange complete -
updating PEM
--More--          [09/01/13 11:59:21.258 IST 16d9 5933] 0021.5C8C.C761

```

```

apfMslxStateInc
[09/01/13 11:59:21.258 IST 16da 5933] 0021.5C8C.C761 WCDB_AUTH: Adding opt82 len 0
[09/01/13 11:59:21.258 IST 16db 5933] 0021.5C8C.C761 WCDB_LLM: NoRun Prev Mob 0,
  Curr Mob 0 llmReq 1, return False
[09/01/13 11:59:21.258 IST 16dc 5933] 0021.5C8C.C761 WCDB_CHANGE: auth=L2_AUTH(1)
  vlan 20 radio 1 client_id 0x84fd0000000050 mobility=Unassoc(0) src_int
  0xb68180000000038 dst_int 0x0 ackflag 0 reassoc_client 0 llm_notif 0 ip 0.0.0.0
  ip learn type UNKNOWN
[09/01/13 11:59:21.258 IST 16dd 5933] 0021.5C8C.C761 WCDB_CHANGE: In L2 auth but
  l2ack waiting lfag not set,so set
[09/01/13 11:59:21.258 IST 16de 5933] 0021.5C8C.C761 Not Using WMM Compliance code
  qosCap 00
[09/01/13 11:59:21.258 IST 16df 5933] 0021.5C8C.C761 WCDB_AUTH: Adding opt82 len 0
[09/01/13 11:59:21.258 IST 16e0 5933] 0021.5C8C.C761 WCDB_CHANGE: Suppressing SPI
  (Mobility state not known) pemstate 7 state LEARN_IP(2) vlan 20 client_id
  0x84fd00000000050 mob=Unassoc(0) ackflag 1 dropd 0
[09/01/13 11:59:21.258 IST 16e1 5933] 0021.5C8C.C761 Incrementing the Reassociation
  Count 1 for client (of interface VLAN0020)
[09/01/13 11:59:21.258 IST 16e2 5933] 0021.5C8C.C761 1XK: Stopping retransmission
  timer
[09/01/13 11:59:21.258 IST 16e3 5933] 0021.5C8C.C761 0.0.0.0, auth_state 7 mmRole
  Unassoc !!!
--More--      [09/01/13 11:59:21.258 IST 16e4 5933] 0021.5C8C.C761 0.0.0.0,
  auth_state 7 mmRole Unassoc, updating wcdb not needed
[09/01/13 11:59:21.258 IST 16e5 5933] 0021.5C8C.C761 Tclas Plumb needed: 0
[09/01/13 11:59:21.258 IST 16e6 5933] 0021.5C8C.C761 WCDB_AUTH: Adding opt82 len 0
[09/01/13 11:59:21.258 IST 16e7 5933] 0021.5C8C.C761 WCDB_LLM: NoRun Prev Mob 0,
  Curr Mob 1 llmReq 1, return False
[09/01/13 11:59:21.258 IST 16e8 5933] 0021.5C8C.C761 WCDB_CHANGE: Suppressing SPI
  (ACK message not recvd) pemstate 7 state LEARN_IP(2) vlan 20
  client_id 0x84fd00000000050 mob=Local(1) ackflag 1 dropd 1
[09/01/13 11:59:21.258 IST 16e9 5933] 0021.5C8C.C761 Error updating wcdb on mobility
  complete
[09/01/13 11:59:21.258 IST 16ea 5933] 0021.5C8C.C761 aaa attribute list length is 79
[09/01/13 11:59:21.258 IST 16eb 5933] 0021.5C8C.C761 Sending SPI
  spi epm epm session_create successfull
[09/01/13 11:59:21.259 IST 16ec 5933] 0021.5C8C.C761 0.0.0.0, auth_state 7 mmRole
  Local !!!
[09/01/13 11:59:21.259 IST 16ed 5933] 0021.5C8C.C761 0.0.0.0, auth_state 7 mmRole
  Local, updating wcdb not needed
[09/01/13 11:59:21.259 IST 16ee 5933] 0021.5C8C.C761 Tclas Plumb needed: 0
[09/01/13 11:59:21.260 IST 16ef 190] [WCDB] ==Update event: client (0021.5c8c.c761)
  client id:(0x84fd00000000050) vlan (20->20) global_wlan (4->4) auth_state
  (ASSOCIATION->L2 AUTH DONE) mob_state (INIT->INIT)
--More--      [09/01/13 11:59:21.260 IST 16f0 190] [WCDB] ===intf src/dst
  (0xb68180000000038->0xb68180000000038)/(0x0->0x0) radio/bssid
  (1->1)/(c8f9.f983.4260->c8f9.f983.4260) llm_notify (false) addr v4/v6 (0)/(0)
[09/01/13 11:59:21.260 IST 16f1 190] [WCDB] wcdb_client_mcast_update_notify: No
  mcast action reqd
[09/01/13 11:59:21.260 IST 16f2 190] [WCDB] Allocating Client LE and waiting for
  ACK
[09/01/13 11:59:21.260 IST 16f3 190] [WCDB] wcdb_ffcp_wcdb_client_add_notify:
  client (0021.5c8c.c761) id 0x84fd00000000050 ffcp create flags=0x0 iifid
  bssid/radio = 0x81fac0000000041/0xbfc0c000000003a, src intf = 0xb68180000000038
[09/01/13 11:59:21.261 IST 16f4 5933] 0021.5C8C.C761 Received
  session_create_response for client handle 37432873367634000
[09/01/13 11:59:21.261 IST 16f5 5933] 0021.5C8C.C761 Received
  session_create_response with EPM session handle 4060086311
[09/01/13 11:59:21.261 IST 16f6 5933] 0021.5C8C.C761 Send request to EPM
[09/01/13 11:59:21.261 IST 16f7 5933] 0021.5C8C.C761 aaa attribute list length is
  485
[09/01/13 11:59:21.261 IST 16f8 5933] 0021.5C8C.C761 Sending Activate request for
  session handle 4060086311 successful
[09/01/13 11:59:21.261 IST 16f9 5933] 0021.5C8C.C761 Post-auth policy request sent!
  Now wait for post-auth policy ACK from EPM
[09/01/13 11:59:21.261 IST 16fa 5933] 0021.5C8C.C761 Received
  activate_features_resp for client handle 37432873367634000
[09/01/13 11:59:21.261 IST 16fb 5933] 0021.5C8C.C761 Received
  activate_features_resp for EPM session handle 4060086311
--More--      [09/01/13 11:59:21.262 IST 16fc 5933] 0021.5C8C.C761 Received
  policy_enforcement_response for client handle 37432873367634000
[09/01/13 11:59:21.262 IST 16fd 5933] 0021.5C8C.C761 Received
  policy_enforcement_response for EPM session handle 2818572305

```

```

[09/01/13 11:59:21.262 IST 16fe 5933] 0021.5C8C.C761 Received response
for _EPM_SPI_ACTIVATE_FEATURES request sent for client
[09/01/13 11:59:21.262 IST 16ff 5933] 0021.5C8C.C761
Received _EPM_SPI_STATUS_SUCCESS for request sent for client
[09/01/13 11:59:21.262 IST 1700 5933] 0021.5C8C.C761 Post-auth policy ACK recvd
from EPM, unset flag on MSCB
[09/01/13 11:59:21.262 IST 1701 33] [WCDB] wcdb_ffcp_add_cb: client (0021.5c8c.c761)
client (0x84fd0000000050): FFCP operation (CREATE) return code (0)
[09/01/13 11:59:21.262 IST 1702 33] [WCDB] wcdb_send_add_notify_callback_event:
Notifying other features about client add
[09/01/13 11:59:21.262 IST 1703 33] ACCESS-CORE-SM-FEATURE-WIRED_TUNNEL-NOT:
[0021.5c8c.c761] Client 0021.5c8c.c761 is not tunnel client..Return
[09/01/13 11:59:21.262 IST 1704 33] [WCDB] wcdb_sisf_client_add_notify: Notifying
SISF of DEASSOC to DOWN any old entry for 0021.5c8c.c761
[09/01/13 11:59:21.262 IST 1705 33] [WCDB] wcdb_sisf_client_add_notify: Notifying
SISF of new Association for 0021.5c8c.c761
[09/01/13 11:59:21.262 IST 1706 5933] 0021.5C8C.C761 WCDB SPI response msg handler
client code 0 mob state 0
[09/01/13 11:59:21.262 IST 1707 5933] 0021.5C8C.C761 WcdbClientUpdate: L2 Auth ACK
from WCDB
--More-- [09/01/13 11:59:21.262 IST 1708 5933] 0021.5C8C.C761 WCDB_L2ACK:
wcdbAckRecvdFlag updated
[09/01/13 11:59:21.262 IST 1709 5933] 0021.5C8C.C761 WCDB_AUTH: Adding opt82 len 0
[09/01/13 11:59:21.262 IST 170a 5933] 0021.5C8C.C761 WCDB_LLM: NoRun Prev Mob 0,
Curr Mob 1 llmReq 1, return False
[09/01/13 11:59:21.263 IST 170b 5933] 0021.5C8C.C761 WCDB_CHANGE: auth=LEARN_IP(2)
vlan 20 radio 1 client_id 0x84fd0000000050 mobility=Local(1) src int
0xb6818000000038 dst_int 0x0 ackflag 2 reassoc_client 0 llm_notify 0 ip 0.0.0.0
ip_learn_type UNKNOWN
[09/01/13 11:59:21.263 IST 170c 190] [WCDB] ==Update event: client (0021.5c8c.c761)
client id:(0x84fd0000000050) vlan (20->20) global_vlan (4->4) auth_state
(L2 AUTH DONE->LEARN_IP) mob_state (INIT->LOCAL)
[09/01/13 11:59:21.263 IST 170d 190] [WCDB] ===intf src/dst
(0xb6818000000038->0xb6818000000038)/(0x0->0x0)
radio/bssid (1->1)/(c8f9.f983.4260->c8f9.f983.4260) llm_notify (false) addr v4/v6
(0)/(0)
[09/01/13 11:59:21.263 IST 170e 190] [WCDB] wcdb_client_mcast_update_notify: No
mcast action reqd
[09/01/13 11:59:21.263 IST 170f 190] [WCDB] wcdb_ffcp_wcdb_client_update_notify
client (0021.5c8c.c761) id 0x84fd0000000050 ffcp update with flags=0x18
[09/01/13 11:59:21.263 IST 1710 190] [WCDB] wcdb_client_state_change_notify:
update flags = 0x3
[09/01/13 11:59:21.263 IST 1711 190] ACCESS-CORE-SM-CLIENT-DOT11-NOTF:
[0021.5c8c.c761] WCDB notification (LEARN_IP) for 0021.5c8c.c761
--More-- [09/01/13 11:59:21.263 IST 1712 190] [WCDB]
wcdb_sisf_client_update_notify: Notifying SISF
[09/01/13 11:59:21.263 IST 1713 329] [WCDB] wcdb_ffcp_cb: client (0021.5c8c.c761)
client (0x84fd0000000050): FFCP operation (UPDATE) return code (0)
[09/01/13 11:59:24.417 IST 1714 264] dhcp pkt processing routine is called for pak
with SMAC = 0021.5c8c.c761 and SRC_ADDR = 0.0.0.0
[09/01/13 11:59:24.417 IST 1715 210] sending dhcp packet outafter processing with
SMAC = 0021.5c8c.c761 and SRC_ADDR = 0.0.0.0
[09/01/13 11:59:24.417 IST 1716 144] DHCPD: Sending notification of DISCOVER:
[09/01/13 11:59:24.417 IST 1717 144] DHCPD: Sending notification of DISCOVER:
[09/01/13 11:59:24.417 IST 1718 144] DHCPD: DHCPPOFFER notify setup address
20.20.20.3 mask 255.255.255.0
[09/01/13 11:59:24.425 IST 1719 264] dhcp pkt processing routine is called for pak
with SMAC = 0021.5c8c.c761 and SRC_ADDR = 0.0.0.0
[09/01/13 11:59:24.425 IST 171a 210] sending dhcp packet outafter processing with
SMAC = 0021.5c8c.c761 and SRC_ADDR = 0.0.0.0
[09/01/13 11:59:24.425 IST 171b 144] DHCPD: address 20.20.20.3 mask 255.255.255.0
[09/01/13 11:59:24.425 IST 171c 186] ACCESS-CORE-SM-CLIENT-IPDT-NOTF:
[0021.5c8c.c761, Cal] IP update for MAC 0021.5c8c.c761. New IP 20.20.20.3
[09/01/13 11:59:24.425 IST 171d 186] ACCESS-CORE-SM-CLIENT-IPDT-NOTF:
[0021.5c8c.c761, Cal] IPv4 ID update notify success for label 0x32000026, MAC
0021.5c8c.c761
[09/01/13 11:59:24.425 IST 171e 186] [WCDB] wcdb_ffcp_wcdb_client_update_notify
client (0021.5c8c.c761) id 0x84fd0000000050 ffcp update with flags=0x18
--More-- [09/01/13 11:59:24.425 IST 171f 173] ACCESS-CORE-SM-NOTF:
[0021.5c8c.c761, Cal] Received internal event SINGLE_ID_UPDATE (handle 0x32000026)
[09/01/13 11:59:24.425 IST 1720 173] ACCESS-CORE-SM-SYNC-NOTF: [0021.5c8c.c761, Cal]
Delay add/update sync of addr for 0021.5c8c.c761 / 0x32000026
[09/01/13 11:59:24.425 IST 1721 5933] 0021.5C8C.C761 WCDB_IP_BIND: w/ IPv4

```

```

20.20.20.3 ip learn_type DHCP add delete 1,options_length 0
[09/01/13 11:59:24.425 IST 1722 5933] 0021.5C8C.C761 wcdbClientUpdate: IP Binding
from Wcdb ip learn type 1, add or delete 1
[09/01/13 11:59:24.425 IST 1723 5933] 0021.5C8C.C761 IPv4 Addr: 20:20:20:3
[09/01/13 11:59:24.425 IST 1724 5933] 0021.5C8C.C761 MS got the IP, resetting the
Reassociation Count 0 for client
[09/01/13 11:59:24.425 IST 1725 5933] 0021.5C8C.C761 apfMsRunStateInc
[09/01/13 11:59:24.426 IST 1726 5933] 0021.5C8C.C761 Wcdb_AUTH: Adding opt82 len 0
[09/01/13 11:59:24.426 IST 1727 5933] 0021.5C8C.C761 Wcdb_LLM: prev Mob state 1
curr Mob State 1 llReq flag 0
[09/01/13 11:59:24.426 IST 1728 5933] 0021.5C8C.C761 Wcdb_CHANGE: auth=RUN(4) vlan
20 radio 1 client_id 0x84fd0000000050 mobility=Local(1) src_int 0xb6818000000038
dst_int 0x0 ackflag 2 reassoc_client 0 llm_notif 0 ip 20.20.20.3 ip_learn_type DHCP
[09/01/13 11:59:24.426 IST 1729 329] [Wcdb] wcdb_ffcp_cb: client (0021.5c8c.c761)
client (0x84fd0000000050): FFCP operation (UPDATE) return code (0)
[09/01/13 11:59:24.426 IST 172a 5933] 0021.5C8C.C761 AAAS: acct method list NOT
configured for WLAN 4, accounting skipped
--More-- [09/01/13 11:59:24.426 IST 172b 5933] 0021.5C8C.C761
Sending IPv4 update to Controller 10.105.135.176
[09/01/13 11:59:24.426 IST 172c 5933] 0021.5C8C.C761 Assigning Address 20.20.20.3
to mobile
[09/01/13 11:59:24.426 IST 172d 5933] 0021.5C8C.C761 20.20.20.3, auth_state 20
mmRole Local !!!
[09/01/13 11:59:24.426 IST 172e 5933] 0021.5C8C.C761 20.20.20.3, auth_state 20
mmRole Local, updating wcdb not needed
[09/01/13 11:59:24.426 IST 172f 5933] 0021.5C8C.C761 Tclas Plumb needed: 0
[09/01/13 11:59:24.427 IST 1730 190] [Wcdb] ==Update event: client (0021.5c8c.c761)
client id:(0x84fd0000000050) vlan (20->20) global_wlan (4->4) auth_state
(LEARN IP->RUN) mob state (LOCAL->LOCAL)
[09/01/13 11:59:24.427 IST 1731 190] [Wcdb] ===intf src/dst
(0xb6818000000038->0xb6818000000038)/(0x0->0x0) radio/bssid
(1->1)/(c8f9.f983.4260->c8f9.f983.4260) llm_notify (false) addr v4/v6 (0)/(0)
[09/01/13 11:59:24.427 IST 1732 190] [Wcdb] wcdb_client_mcast_update_notify: No
mcast action reqd
[09/01/13 11:59:24.427 IST 1733 190] [Wcdb] wcdb_ffcp_wcdb_client_update_notify
client (0021.5c8c.c761) id 0x84fd0000000050 ffcp update with flags=0x18
[09/01/13 11:59:24.427 IST 1734 190] [Wcdb] wcdb_client_state_change_notify:
update flags = 0x2
[09/01/13 11:59:24.427 IST 1735 190] ACCESS-CORE-SM-CLIENT-DOT11-NOTF:
[0021.5c8c.c761] Ignore Wcdb run notification for 0021.5c8c.c761 as authz complete.
--More-- [09/01/13 11:59:24.427 IST 1736 190] [Wcdb]
wcdb_sisf_client_update_notify: Notifying SISF
[09/01/13 11:59:24.427 IST 1737 329] [Wcdb] wcdb_ffcp_cb: client (0021.5c8c.c761)
client (0x84fd0000000050): FFCP operation (UPDATE) return code (0)
[09/01/13 11:59:34.667 IST 1738 190] [Wcdb] ==Update event: client (60fa.cd4c.597b)
client id:(0xa028c00000004c) vlan (20->20) global_wlan (2->2) auth_state
(RUN->ASSOCIATION) mob state (LOCAL->LOCAL)
[09/01/13 11:59:34.667 IST 1739 190] [Wcdb] ===intf src/dst
(0xb6818000000038->0xb6818000000038)/(0x0->0x0) radio/bssid (0->0)/
(c8f9.f983.4260->c8f9.f983.4260) llm_notify (true) addr v4/v6 (0)/(0)
[09/01/13 11:59:34.667 IST 173a 190] [Wcdb] wcdb_client_mcast_update_notify:
No mcast action reqd
[09/01/13 11:59:34.667 IST 173b 190] [Wcdb] Ignoring auth state transition
(4 -> 0)
[09/01/13 11:59:34.667 IST 173c 190] [Wcdb] wcdb_ffcp_wcdb_client_update_notify
client (60fa.cd4c.597b) id 0xa028c00000004c ffcp update with flags=0x18
[09/01/13 11:59:34.667 IST 173d 190] [Wcdb] wcdb_client_state_change_notify:
update flags = 0x2
[09/01/13 11:59:34.667 IST 173e 190] [Wcdb] wcdb_sisf_client_update_notify:
Notifying SISF
[09/01/13 11:59:34.667 IST 173f 329] [Wcdb] wcdb_ffcp_cb: client (60fa.cd4c.597b)
client (0xa028c00000004c): FFCP operation (UPDATE) return code (0)
[09/01/13 11:59:34.865 IST 1740 190] [Wcdb] ==Update event: client (60fa.cd4c.597b)
client id:(0xa028c00000004c) vlan (20->20) global_wlan (2->2) auth_state (RUN->RUN)
mob state (LOCAL->LOCAL)
--More-- [09/01/13 11:59:34.865 IST 1741 190] [Wcdb] ===intf src/dst
(0xb6818000000038->0xb6818000000038)/(0x0->0x0)
radio/bssid (0->0)/(c8f9.f983.4260->c8f9.f983.4260) llm_notify (false) addr v4/v6
(0)/(0)
[09/01/13 11:59:34.865 IST 1742 190] [Wcdb] wcdb_client_mcast_update_notify: No
mcast action reqd
[09/01/13 11:59:34.865 IST 1743 190] [Wcdb] wcdb_ffcp_wcdb_client_update_notify
client (60fa.cd4c.597b) id 0xa028c00000004c ffcp update with flags=0x18

```

```

[09/01/13 11:59:34.865 IST 1744 190] [WCDB] wcdb_client_state_change_notify:
update flags = 0x2
[09/01/13 11:59:34.865 IST 1745 190] [WCDB] wcdb_sisf_client_update_notify:
Notifying SISF
[09/01/13 11:59:34.865 IST 1746 329] [WCDB] wcdb_ffcp_cb: client (60fa.cd4c.597b)
client (0xa028c00000004c): FFCP operation (UPDATE) return code (0)
[09/01/13 11:59:36.010 IST 1747 264] dhcp pkt processing routine is called for pak
with SMAC = 60fa.cd4c.597b and SRC_ADDR = 0.0.0.0
[09/01/13 11:59:36.010 IST 1748 210] sending dhcp packet outafter processing with
SMAC = 60fa.cd4c.597b and SRC_ADDR = 0.0.0.0
[09/01/13 11:59:36.010 IST 1749 144] DHCPD: address 20.20.20.2 mask 255.255.255.0
[09/01/13 11:59:52.802 IST 174a 190] [WCDB] ==Update event: client (60fa.cd4c.597b)
client id:(0xa028c00000004c) vlan (20->20) global_wlan (2->2) auth_state
(RUN->ASSOCIATION) mob_state (LOCAL->LOCAL)
[09/01/13 11:59:52.802 IST 174b 190] [WCDB] ===intf src/dst
(0xb6818000000038->0xb6818000000038)/(0x0->0x0)
radio/bssid (0->0)/(c8f9.f983.4260->c8f9.f983.4260) llm_notify (true) addr v4/v6
(0)/(0)
--More-- [09/01/13 11:59:52.802 IST 174c 190] [WCDB]
wcdb_client_mcast_update_notify: No mcast action reqd
[09/01/13 11:59:52.802 IST 174d 190] [WCDB] Ignoring auth state transition (4 -> 0)
[09/01/13 11:59:52.802 IST 174e 190] [WCDB] wcdb_ffcp_wcdb_client_update_notify
client (60fa.cd4c.597b) id 0xa028c00000004c ffcpc update with flags=0x18
[09/01/13 11:59:52.802 IST 174f 190] [WCDB] wcdb_client_state_change_notify:
update flags = 0x2
[09/01/13 11:59:52.802 IST 1750 190] [WCDB] wcdb_sisf_client_update_notify:
Notifying SISF
[09/01/13 11:59:52.803 IST 1751 329] [WCDB] wcdb_ffcp_cb: client (60fa.cd4c.597b)
client (0xa028c00000004c): FFCP operation (UPDATE) return code (0)
[09/01/13 11:59:53.015 IST 1752 190] [WCDB] ==Update event: client (60fa.cd4c.597b)
client id:(0xa028c00000004c) vlan (20->20) global_wlan (2->2) auth_state (RUN->RUN)
mob_state (LOCAL->LOCAL)
[09/01/13 11:59:53.015 IST 1753 190] [WCDB] ===intf src/dst
(0xb6818000000038->0xb6818000000038)/(0x0->0x0)
radio/bssid (0->0)/(c8f9.f983.4260->c8f9.f983.4260) llm_notify (false) addr v4/v6
(0)/(0)
[09/01/13 11:59:53.015 IST 1754 190] [WCDB] wcdb_client_mcast_update_notify: No
mcast action reqd
[09/01/13 11:59:53.015 IST 1755 190] [WCDB] wcdb_ffcp_wcdb_client_update_notify
client (60fa.cd4c.597b) id 0xa028c00000004c ffcpc update with flags=0x18
[09/01/13 11:59:53.015 IST 1756 190] [WCDB] wcdb_client_state_change_notify: update
flags = 0x2
--More-- [09/01/13 11:59:53.015 IST 1757 190] [WCDB]
wcdb_sisf_client_update_notify: Notifying SISF
[09/01/13 11:59:53.016 IST 1758 329] [WCDB] wcdb_ffcp_cb: client (60fa.cd4c.597b)
client (0xa028c00000004c): FFCP operation (UPDATE) return code (0)
[09/01/13 11:59:54.045 IST 1759 264] dhcp pkt processing routine is called for pak
with SMAC = 60fa.cd4c.597b and SRC_ADDR = 0.0.0.0
[09/01/13 11:59:54.045 IST 175a 210] sending dhcp packet outafter processing with
SMAC = 60fa.cd4c.597b and SRC_ADDR = 0.0.0.0
[09/01/13 11:59:54.045 IST 175b 144] DHCPD: address 20.20.20.2 mask 255.255.255.0
[09/01/13 12:00:18.830 IST 175c 190] [WCDB] ==Update event: client (60fa.cd4c.597b)
client id:(0xa028c00000004c) vlan (20->20) global_wlan (2->2) auth_state
(RUN->ASSOCIATION) mob_state (LOCAL->LOCAL)
[09/01/13 12:00:18.830 IST 175d 190] [WCDB] ===intf src/dst
(0xb6818000000038->0xb6818000000038)/(0x0->0x0)
radio/bssid (0->0)/(c8f9.f983.4260->c8f9.f983.4260) llm_notify (true) addr v4/v6
(0)/(0)
[09/01/13 12:00:18.830 IST 175e 190] [WCDB] wcdb_client_mcast_update_notify: No
mcast action reqd
[09/01/13 12:00:18.830 IST 175f 190] [WCDB] Ignoring auth state transition
(4 -> 0)
[09/01/13 12:00:18.830 IST 1760 190] [WCDB] wcdb_ffcp_wcdb_client_update_notify
client (60fa.cd4c.597b) id 0xa028c00000004c ffcpc update with flags=0x18
[09/01/13 12:00:18.830 IST 1761 190] [WCDB] wcdb_client_state_change_notify:
update flags = 0x2
--More-- [09/01/13 12:00:18.830 IST 1762 190] [WCDB]
wcdb_sisf_client_update_notify: Notifying SISF
[09/01/13 12:00:18.830 IST 1763 329] [WCDB] wcdb_ffcp_cb: client (60fa.cd4c.597b)
client (0xa028c00000004c): FFCP operation (UPDATE) return code (0)
[09/01/13 12:00:19.038 IST 1764 190] [WCDB] ==Update event: client (60fa.cd4c.597b)
client id:(0xa028c00000004c) vlan (20->20) global_wlan (2->2) auth_state (RUN->RUN)
mob_state (LOCAL->LOCAL)

```

```
[09/01/13 12:00:19.038 IST 1765 190] [WCDB] ===intf src/dst
(0xb6818000000038->0xb6818000000038)/(0x0->0x0)
radio/bssid (0->0)/(c8f9.f983.4260->c8f9.f983.4260) llm_notify (false) addr v4/v6
(0)/(0)
[09/01/13 12:00:19.038 IST 1766 190] [WCDB] wcdb_client_mcast_update_notify:
No mcast action reqd
[09/01/13 12:00:19.038 IST 1767 190] [WCDB] wcdb_ffcp_wcdb_client_update_notify
client (60fa.cd4c.597b) id 0xa028c00000004c ffcp update with flags=0x18
[09/01/13 12:00:19.038 IST 1768 190] [WCDB] wcdb_client_state_change_notify:
update flags = 0x2
[09/01/13 12:00:19.038 IST 1769 190] [WCDB] wcdb_sisf_client_update_notify:
Notifying SISF
[09/01/13 12:00:19.038 IST 176a 329] [WCDB] wcdb_ffcp_cb: client (60fa.cd4c.597b)
client (0xa028c00000004c): FFCP operation (UPDATE) return code (0)
[09/01/13 12:00:20.108 IST 176b 5933] 0021.5C8C.C761
Client stats update: Time now in sec 1378015280, Last Acct Msg Sent at 1378015224
sec
[09/01/13 12:00:20.590 IST 176c 264] dhcp pkt processing routine is called for pak
with SMAC = 60fa.cd4c.597b and SRC_ADDR = 0.0.0.0
--More-- [09/01/13 12:00:20.590 IST 176d 210] sending dhcp packet outafter
processing with SMAC = 60fa.cd4c.597b and SRC_ADDR = 0.0.0.0
[09/01/13 12:00:20.590 IST 176e 144] DHCPD: address 20.20.20.2 mask 255.255.255.0
```

Device#

```
*Sep 1 06:04:20.121: 0021.5C8C.C761
Client stats update: 1 wcm: Time now in sec 1378015460, Last Acct Msg Sent at
1378015370 sec
*Sep 1 06:04:20.121: 0021.5C8C.C761 Requested to send acct interim update request
msg to APF task for client 0: 1 wcm: 21:5c:8c:c7:61
*Sep 1 06:04:21.326: Load Balancer: 1 wcm: Success, Resource allocated are:
Active Switch number: 1, Active Asic number : 2, Reserve Switch number 0 Reserve
Asic number 0. AP Asic num 0
*Sep 1 06:04:21.326: WCDB_IIF: 1 wcm: Ack Message ID: 0x85780000000052 code 1001
*Sep 1 06:04:21.326: PEM rcv processing msg Epm spi response(12) 1 wcm: e 1001
*Sep 1 06:04:21.326: PEM rcv processing msg Add SCB(3) 1 wcm: onse(12)
*Sep 1 06:04:21.327: EPM: 1 wcm: Session create resp - client handle
85780000000052 session 32000028
*Sep 1 06:04:21.327: EPM: 1 wcm: Netflow session create resp - client handle
85780000000052 sess 32000028
*Sep 1 06:04:21.328: PEM rcv processing msg Epm spi response(12) 1 wcm: le
85780000000052 sess 32000028
*Sep 1 06:04:21.328: EPM: 1 wcm: Init feature, client handle 85780000000052
session 32000028 authz 5000012
*Sep 1 06:04:21.328: EPM: 1 wcm: Activate feature client handle 85780000000052
sess 32000028 authz 5000012
*Sep 1 06:04:21.328: PEM rcv processing msg Epm spi response(12) 1 wcm: 0052
sess 32000028 authz 5000012
*Sep 1 06:04:21.328: EPM: 1 wcm: Policy enforcement - client handle
85780000000052 session c8000012 authz 5000012
*Sep 1 06:04:21.328: EPM: 1 wcm: Netflow policy enforcement - client handle
85780000000052 sess c8000012 authz 5000012 msg_type 0 policy_status 0 attr len 0
*Sep 1 06:04:21.328: PEM rcv processing msg Epm spi response(12) 1 wcm: e
85780000000052 sess c8000012 authz 5000012 msg_type 0 policy_status 0 attr len 0
*Sep 1 06:04:28.456: PEM rcv processing msg Add SCB(3) 1 wcm: onse(12)
```



External Web Authentication on Converged Access

The configuration procedure for the External Web Authentication on Converged Access is similar to the configuration procedure of Local Web Authentication with External RADIUS Authentication. However, to configure an External Web Authentication, in addition to configuring Local Web Authentication, you need to do the following:

- Add pre-authentication Access Control Lists (ACL)
- Change the Web Authentication parameter map



Note

For information on Local Web Authentication with External RADIUS Authentication, refer to Local Web Authentication with External RADIUS Authentication.

The following example describes the parameter maps in global configuration mode:

```
parameter-map type webauth test_web
  type webauth
  redirect for-login https://192.168.154.119 : 8443
/guestportal/portals/external_webauth/portal.jsp -> ISE customguest portal
  redirect portal ipv4 192.168.154.119 -> Redirect
  to ISE banner
```



Note

You can specify the redirect pages for success and failure scenario using the following commands:

- redirect on-success url
- redirect on-failure url

The following example describes the pre-authentication ACL in global configuration mode:



Note

Preauth_ise is an optional configuration for external web authentication.

```
ip access-lists extended preauth_ise
10 permit udp any eq bootps any -> allow DHCP
20 permit udp any any eq bootpc -> allow DHCP
```

```

30 permit udp any eq bootpc any -> allow DHCP
40 permit udp any any eq domain -> allow DNS
50 permit udp any eq domain any -> allow DNS
60 permit ip any host 192.0.2.1 -> allow access to ISE
70 permit ip host 192.0.2.1 any -> allow ISE to talk back

```

**Note**

On Converged Access, the traffic for Web Authentication, Service Set Identifier (SSID), DHCP, and Domain Name System (DNS) is not allowed, by default. You need to enable DHCP, DNS, and access to the external server.

- [Example: Configuring WLAN Commands, page 180](#)
- [Configuring External Web Authentication with Custom Guest Portal page on ISE, page 180](#)
- [Example: External Web Authentication Page , page 185](#)
- [Example: Configuring External Web Authentication on Converged Access, page 186](#)

Example: Configuring WLAN Commands

The following example describes how to configure WLAN commands:

```

wlan external_webauth 11 external_webauth
client vlan 263
ip access-group web_preauth_ise          ----> applying preauth ACL
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list ext_ise
security web-auth parameter-map test_web
no shutdown

```

Configuring External Web Authentication with Custom Guest Portal page on ISE

Perform the following steps to configure the External Web Authentication with a custom guest portal page on Identity Services Engine (ISE):



Note In the figure, the custom default portal is 'external webauth'.

Step 1 To add a custom default portal, click **Add**.

Figure 59: Multi Portal Configurations

The screenshot shows the Cisco ISE Administration console interface. The top navigation bar includes Home, Operations, Policy, and Administration. Below this, there are tabs for System, Identity Management, Network Resources, and Web Portal Management. The main content area is titled 'Settings' and contains a tree view on the left with categories like General, Sponsor, My Devices, and Guest. The 'Multi-Portal Configurations' section is selected and highlighted. On the right, there is a table with columns for Multi-Portal Name, Portal Type, and Description. The table contains three entries: DefaultGuestPortal (Default), DevicePortal (DeviceWebAuth), and external_webauth (CustomDefault). Above the table, there are buttons for Edit, Add, and Delete. A blue arrow points to the 'Add' button.

Multi-Portal Name	Portal Type	Description
DefaultGuestPortal	Default	default portal
DevicePortal	DeviceWebAuth	
external_webauth	CustomDefault	

354305

Step 2 To upload files, choose **Custom Default Portal (upload files)**.

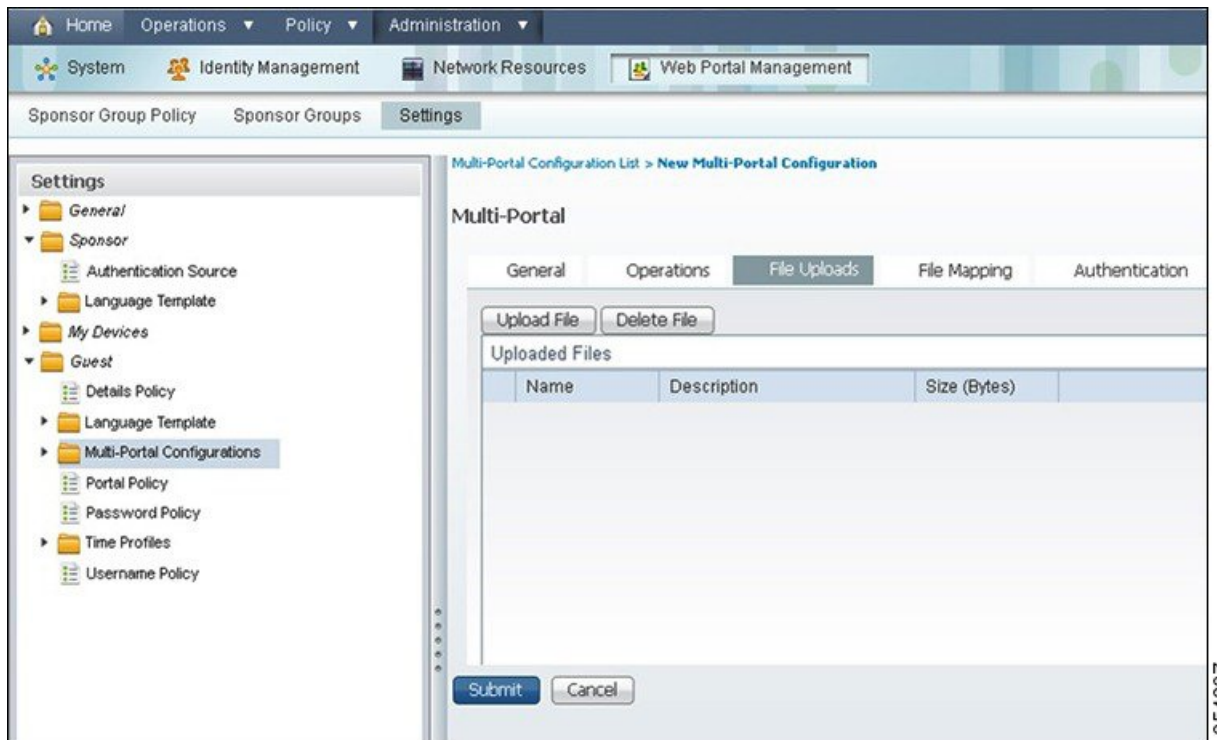
Figure 60: Custom Default Portal

The screenshot displays the Cisco ISE configuration interface for Multi-Portal Configurations. The left-hand navigation pane shows the 'Settings' menu with 'Multi-Portal Configurations' highlighted. The main content area is titled 'Multi-Portal Configuration List > New Multi-Portal Configuration'. It features a 'Multi-Portal' section with tabs for 'General', 'Operations', 'File Uploads', 'File Mapping', and 'Authentication'. The 'General' tab is active, showing input fields for '* Name' and 'Description'. Below these fields, a section titled 'Please select a portal type' contains four radio button options: 'Default Portal (Choose customization template and theme)', 'Device Web Authorization Portal (Choose customization template and theme)', 'Custom Default Portal (Upload files)' (which is selected), and 'Custom Device Web Authorization Portal (Upload files)'. At the bottom of the form are 'Submit' and 'Cancel' buttons. A vertical ID number '354306' is visible on the right edge of the screenshot.

Step 3 Navigate to **File Uploads**. In the **File Uploads** area, click **Upload File** and select the relevant page.

Note You can upload the login, success, and failure pages.

Figure 61: File Uploads



The screenshot displays the Cisco ISE Administration console interface. The top navigation bar includes Home, Operations, Policy, and Administration. Below this, there are tabs for System, Identity Management, Network Resources, and Web Portal Management. The main content area is divided into two sections: a left-hand navigation pane and a right-hand main workspace.

The left-hand navigation pane is titled "Settings" and contains a tree view of configuration categories:

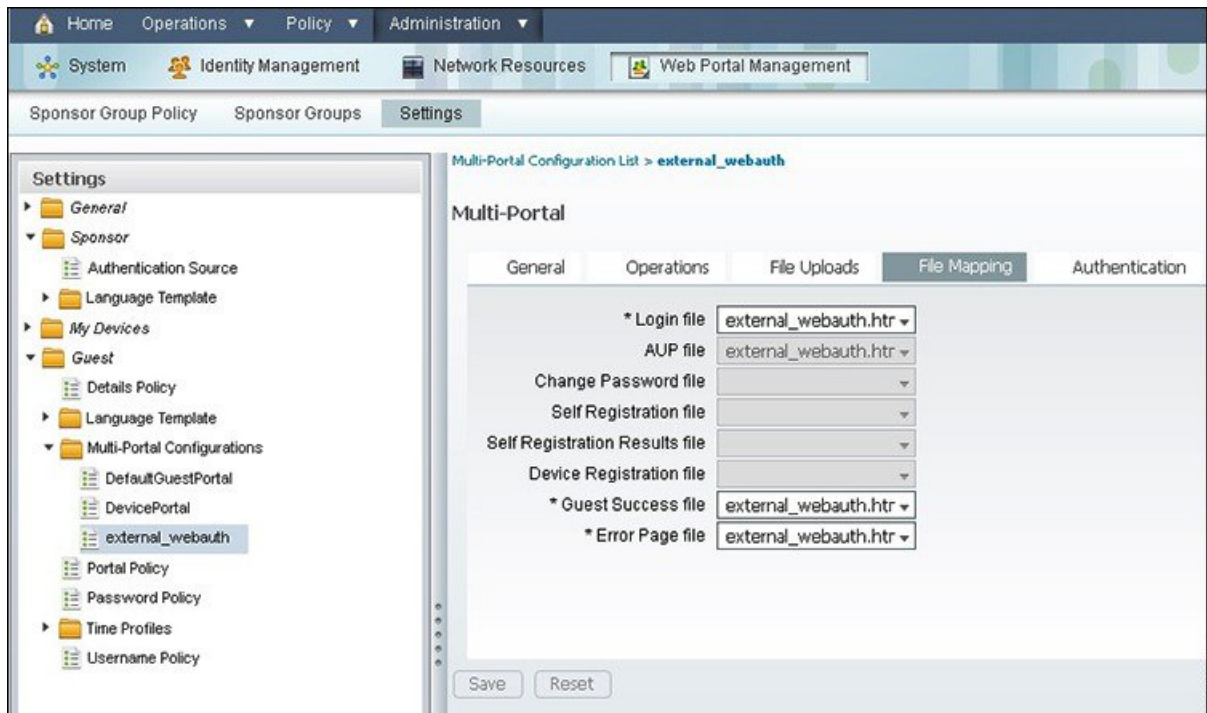
- General
- Sponsor
 - Authentication Source
 - Language Template
- My Devices
- Guest
 - Details Policy
 - Language Template
 - Multi-Portal Configurations (highlighted)
 - Portal Policy
 - Password Policy
 - Time Profiles
 - Username Policy

The right-hand main workspace is titled "Multi-Portal Configuration List > New Multi-Portal Configuration". It features a tabbed interface with the following tabs: General, Operations, File Uploads (active), File Mapping, and Authentication. The "File Uploads" tab contains an "Upload File" button and a "Delete File" button. Below these buttons is a table titled "Uploaded Files" with the following columns: Name, Description, and Size (Bytes). The table is currently empty. At the bottom of the workspace, there are "Submit" and "Cancel" buttons.

354307

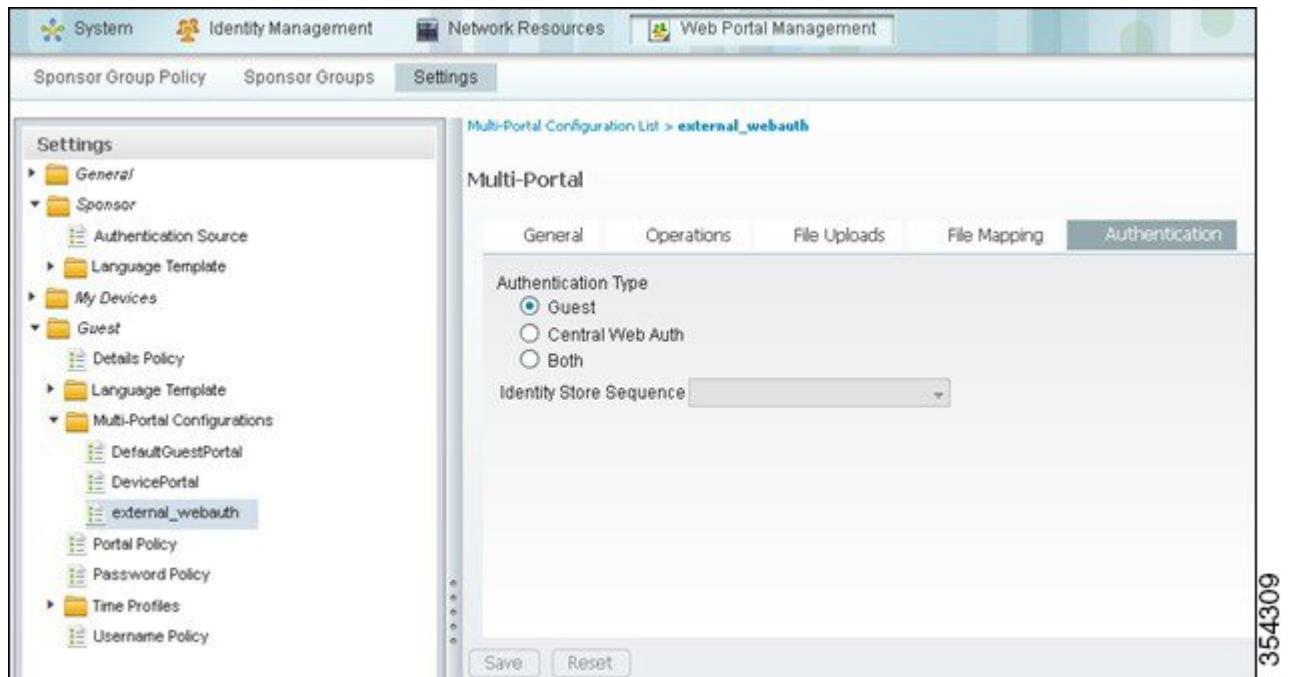
Step 4 To enter the file mapping details, navigate to **File Mapping** and enter the details, as required.

Figure 62: File Mapping



Step 5 To enter authentication details, navigate to **Authentication** and enter the details, as required.

Figure 63: Authentication



Step 6 The ISE Authentication success log is displayed. The authorization policy returns an access-accept.

Example: External Web Authentication Page

The following code describes an external web authentication page:

```
<HTML><HEAD><TITLE>Authentication Proxy Login Page</TITLE>
<script type="text/javascript">
var pxypromptwindow1;
var pxysubmitted = false;
function submitreload() {
    if (pxysubmitted == false) {
        pxypromptwindow1=window.open('', 'pxywindow1',
'resizable=no,width=350,height=350,scrollbars=yes');
        pxysubmitted = true;
        return true;
    } else {
        alert("This page can not be submitted twice.");
        return false;
    }
}
</script>
</HEAD>
<!--
// The form "action" url must be set to the webauth virtual-ip address
//
```

```

-->
<BODY>
<H1>Cisco Systems</H1><H2>Web Authentication</H2>
<FORM method=post action="http://1.1.1.1/" target="pxywindow1">
  Username: <input type=text name=uname><BR><BR>
  Password: <input type=password name=pwd><BR><BR>
  <input type=submit name=ok value=OK   onClick="return submitreload();">
</FORM><noscript>
<BR>
<UL>
  <H2><FONT COLOR="red">Warning!</FONT></H2>
  <p>JavaScript should be enabled in your Web browser
    for secure authentication</p>
  <LI>Follow the instructions of your Web browser to enable
    JavaScript if you would like to have JavaScript enabled
    for secure authentication</LI>
  <BR>OR<BR><BR>
  <LI> Follow these steps if you want to keep JavaScript
    disabled or if your browser does not support JavaScript
    <OL><BR>
      <LI> Close this Web browser window</LI>
      <LI> Click on Reload button of the original browser window</LI>
    </OL></LI>
</UL>
</noscript></BODY></HTML>

```

Example: Configuring External Web Authentication on Converged Access

The following code describes the configuration of an external web authentication on converged access using **show run** command on Cisco Catalyst 3850 Series Switch:

```

Device# Device# show run
Building configuration...
Current configuration : 7946 bytes
!
! Last configuration change at 07:29:52 UTC Tue Apr 9 2013
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname Switch
!
boot-start-marker
boot system switch 1 flash:packages.conf
boot system switch 1 flash:cat3k_caa-universalk9.SSA.03.09.55.RDP.150-9.55.RDP.bin
boot-end-marker
!
!
vrf definition Mgmt-vrf
!
  address-family ipv4
  exit-address-family
!
  address-family ipv6
  exit-address-family
!
enable secret 4 EqmAkK0J3mSG00ZICurjr4sQh0jNaaNBjAFiEDDLi1s
!
username admin privilege 15 password 0 ww-wireless
username 3850 password 0 3850
aaa new-model

```

```

!
!
aaa group server radius rad_ise
  server name ise
!
aaa authentication login wcm_local local
aaa authentication login ext_ise group rad_ise
aaa authorization network default local
!
!
!
!
!
aaa session-id common
switch 1 provision ws-c3850-24p
access-session mac-move deny
!
ip device tracking
ip dhcp snooping
!
!
qos wireless-default-untrust
vtp mode transparent
!
crypto pki trustpoint TP-self-signed-0
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-0
  revocation-check none
  rsakeypair TP-self-signed-0
!
!
crypto pki certificate chain TP-self-signed-0
certificate self-signed 01
  3082022C 30820195 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  28312630 24060355 0403131D 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 30301E17 0D313330 34303930 34343531 325A170D 32303031
  30313030 30303030 5A302831 26302406 03550403 131D494F 532D5365 6C662D53
  69676E65 642D4365 72746966 69636174 652D3030 819F300D 06092A86 4886F70D
  01010105 0003818D 00308189 02818100 A80E6C19 126053DC AF217458 7A9F5E74
  7E4FF6CB F0DA23BB 36603DC4 4418FA85 655F670C 38CDB836 497A3BCD 2ABF4A5C
  15F46CAB C503BD09 61AC0D7F C2F25DC0 670E30AD 926368BF 24BD0834 87750901
  5C2EA184 689700FE 10379C58 A9A778EA 88A05B32 AC2D7F6F BE90F6D1 C73625BA
  35F89D4F 633AC666 92B88255 094BF927 02030100 01A36630 64300F06 03551D13
  0101FF04 05300301 01FF3011 0603551D 11040A30 08820653 77697463 68301F06
  03551D23 04183016 801438DB 46071ACE AA940D18 EB943367 D62E08D7 93E1301D
  0603551D 0E041604 1438DB46 071ACEAA 940D18EB 943367D6 2E08D793 E1300D06
  092A8648 86F70D01 01040500 03818100 6039B3A8 BD78C3D3 3631D01D 44EE79FC
  5EE37CCD AC1244EF 97DC8B36 0D937D9F 6F965DCB 908ABBDC 8BBB7D10 3D7C1DE2
  0EC93557 2C162A8D 1EFB319D EFOE944D CEF2CC8E 5741ACD5 7C7E0B75 34C51700
  11ACDA36 A8968447 A86D6685 52277348 1EF6E60D BA7DD0B5 CB5A7264 B0CB7D1F
  E1AB1040 D580C937 CD227437 8695049A
  quit
dot1x system-auth-control
!
!
!
!
!
diagnostic bootup level minimal
service-template webauth-global-inactive
  inactivity-timer 3600
spanning-tree mode pvst
spanning-tree extend system-id
!
redundancy
  mode sso
!
!
parameter-map type webauth global
  virtual-ip ipv4 1.1.1.1
parameter-map type webauth test_web
  type webauth
  redirect for-login https://192.0.2.1:8443/guestportal/portals/external_webauth/portal.jsp

```

Example: Configuring External Web Authentication on Converged Access

```

    redirect portal ipv4 192.0.2.1
    banner
parameter-map type webauth webconsent
  type webauth
  banner
  custom-page login device flash:custom_login.html
  custom-page success device flash:custom_success.html
  custom-page failure device flash:custom_fail.html
  custom-page login expired device flash:custom_fail.html
parameter-map type webauth localweb
  type webauth
  banner text ^C test webauth ^C
!
!
vlan 254,263
!
!
class-map match-any non-client-nrt-class
  match non-client-nrt
!
policy-map port_child_policy
  class non-client-nrt-class
    bandwidth remaining ratio 10
!
!
!
!
!
interface GigabitEthernet0/0
  vrf forwarding Mgmt-vrf
  no ip address
  no ip route-cache
  negotiation auto
!
interface GigabitEthernet1/0/1
  switchport access vlan 263
  switchport mode access
!
interface GigabitEthernet1/0/2
!
interface GigabitEthernet1/0/3
  switchport access vlan 263
  switchport mode access
!
interface GigabitEthernet1/0/4
!
interface GigabitEthernet1/0/5
  switchport mode trunk
  ip dhcp snooping trust
!
interface GigabitEthernet1/0/6
!
interface GigabitEthernet1/0/7
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!

```



```
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface TenGigabitEthernet1/1/1
!
interface TenGigabitEthernet1/1/2
!
interface TenGigabitEthernet1/1/3
!
interface TenGigabitEthernet1/1/4
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan263
 ip dhcp relay information trusted
 ip address 192.0.2.2 192.0.2.254
 ip helper-address 192.0.2.25
 no ip route-cache
!
ip default-gateway 192.0.2.1
ip http server
ip http authentication local
ip http secure-server
!
!
ip access-list extended ACL-REDIRECT
 deny  udp any eq bootps any
 deny  udp any any eq bootpc
 deny  udp any eq bootpc any
 deny  ip any host 192.0.2.5
 deny  ip any host 192.0.2.6
 deny  ip any host 192.0.2.6
 permit tcp any any eq www
ip access-list extended ACL_Provisioning
 permit udp any eq bootpc any eq bootps
 permit udp any host 192.0.2.25 eq domain
 permit udp any host 192.0.2.119 eq domain
 permit ip any host 192.0.2.14
ip access-list extended ACL_Provisioning_Web
 permit ip any host 192.0.2.250
 permit udp any eq bootpc any eq bootps
 permit udp any host 192.0.2.25 eq domain
 permit tcp any host 192.0.2.119 eq 443
 permit tcp any host 192.0.2.119 eq 8443
 permit tcp any host 192.0.2.119 eq www
ip access-list extended ACL_Redirect
 deny  ip any 198.51.100.1 198.51.100.2
 deny  ip any 198.51.100.5 198.51.100.9
 deny  ip any 198.51.100.15 198.51.100.20
```

Example: Configuring External Web Authentication on Converged Access

```

deny ip any 198.51.100.30 198.51.100.40
deny ip any 198.51.100.50 198.51.100.60
deny ip any 198.51.100.70 198.51.100.80
deny ip any 198.51.100.80 198.51.100.90
deny ip any host 198.51.100.95
permit tcp any any eq www
permit tcp any any eq 443
permit tcp any any eq 8443
ip access-list extended preauth_ise
permit udp any eq bootps any
permit udp any any eq bootpc
permit udp any eq bootpc any
permit ip any host 192.0.2.251
permit ip host 192.0.2.250 any
permit ip any host 192.0.2.249
permit ip host 192.0.2.245 any
!
ip radius source-interface Vlan263
!
!
!
radius server ise
address ipv4 192.0.2.240 auth-port 1812 acct-port 1813
key Cisco123
!
!
!
banner motd ^Citen login
^C
!
line con 0
login authentication console
stopbits 1
line aux 0
stopbits 1
line vty 5 15
!
wireless mobility controller
wireless management interface Vlan263
wireless security dot1x radius call-station-id ap-macaddress-ssid
wlan ua-webl 11 ua-webl
client vlan 263
ip access-group web preauth_ise
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list ext_ise
security web-auth parameter-map test_web
no shutdown
ap dot11 24ghz rrm channel dca 1
ap dot11 24ghz rrm channel dca 6
ap dot11 24ghz rrm channel dca 11
ap dot11 5ghz rrm channel dca 36
ap dot11 5ghz rrm channel dca 40
ap dot11 5ghz rrm channel dca 44
ap dot11 5ghz rrm channel dca 48
ap dot11 5ghz rrm channel dca 52
ap dot11 5ghz rrm channel dca 56
ap dot11 5ghz rrm channel dca 60
ap dot11 5ghz rrm channel dca 64
ap dot11 5ghz rrm channel dca 149
ap dot11 5ghz rrm channel dca 153
ap dot11 5ghz rrm channel dca 157
ap dot11 5ghz rrm channel dca 161
ap group default-group
end

```



Installing Wireless Services

Installing Wireless Services document describes the steps to install and prepare wireless services on the Cisco Catalyst 3850 Series Switches. This document also describes the initial configuration and the procedure to join the Access Points (AP) for Cisco Catalyst 3850 Series Switches.

- [Supported Platforms and Releases, page 191](#)
- [About Unified Access Cisco 3850 Series Switch, page 191](#)
- [Cisco Catalyst 3850 Series Switch: Initial Configuration, page 192](#)

Supported Platforms and Releases

The information in this document is based on Cisco Catalyst 3850 Series Switch.



Note

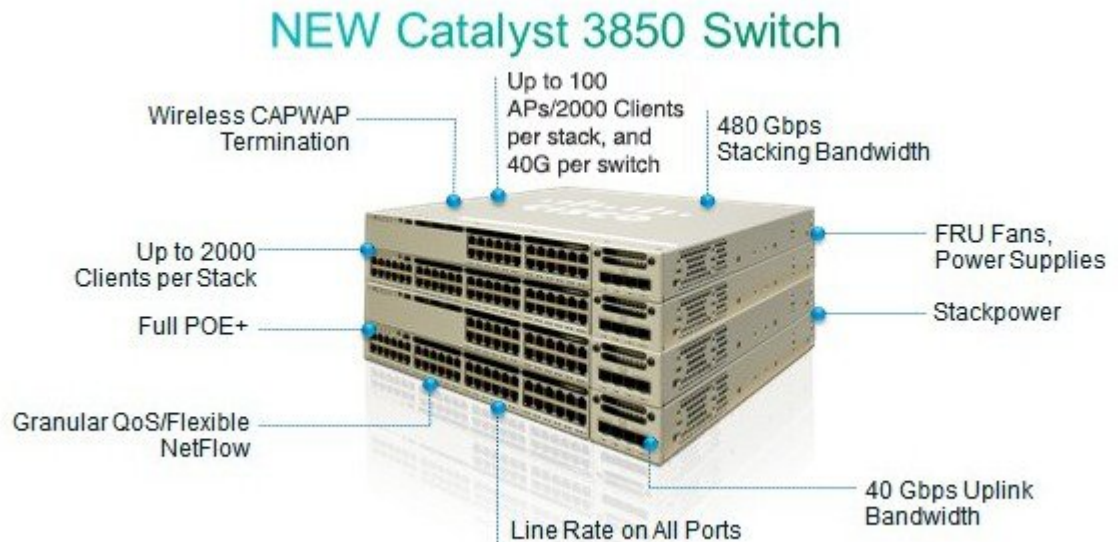
The information in this document is based on the devices in a specific lab environment. The devices used in this document started with a default configuration. If your network is live, make sure that you understand the potential impact of the commands.

About Unified Access Cisco 3850 Series Switch

The Cisco Catalyst 3850 Series Switch is an enterprise class stackable access layer switch that provides full convergence between wired and wireless networks on a single platform. Powered by IOS-XE software, wireless service is supported through the Control and Provisioning of Wireless Access Points (CAPWAP) protocol. Cisco's new Unified Access Data Plane (UADP) ASIC powers the switch and enables uniform wired and wireless policy enforcement, application visibility, flexibility, and application optimization. This convergence is built on the resilience of the Cisco StackWise-480. The Cisco Catalyst 3850 Series switch supports full IEEE 802.3at Power over Ethernet Plus (PoE+), modular and field-replaceable network modules, redundant fan, and power supplies.

The following figure displays the components of Cisco Catalyst 3850 Series Switch:

Figure 64: Components of Cisco Catalyst 3850 Series Switch



350244

Cisco Catalyst 3850 Series Switch: Initial Configuration

Use the following setup script to configure Cisco Catalyst 3850 Series Switch:

```
--- System Configuration Dialog ---

Enable secret warning
-----
In order to access the device manager, an enable secret is required
If you enter the initial configuration dialog, you will be prompted
for the enable secret
If you choose not to enter the initial configuration dialog, or if you
exit setup without setting the enable secret,
please set an enable secret using the following CLI in configuration mode-
enable secret 0 <cleartext password>
-----
Would you like to enter the initial configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

Enter host name [Switch]: sw-3850-1

The enable secret is a password used to protect access to
privileged EXEC and configuration modes. This password, after
entered, becomes encrypted in the configuration.
```

```
Enter enable secret: Cisco123
```

```
The enable password is used when you do not specify an
enable secret password, with some older software versions, and
some boot images.
```

```
Enter enable password: Cisco123
```

```
The virtual terminal password is used to protect
access to the router over a network interface.
```

```
Enter virtual terminal password: Cisco123
```

```
Do you want to configure country code? [no]: yes
```

```
Enter the country code[US]:US
```

Note : Enter the country code in which you are installing this 3850 Switch and the AP(s). If your country code is not recognized, enter one that is compliant with the regulatory domain of your own country

```
Setup account for accessing HTTP server? [yes]: yes
```

```
Username [admin]: admin
```

```
Password [cisco]: cisco
```

```
Password is UNENCRYPTED.
```

```
Configure SNMP Network Management? [no]: no
```

```
Current interface summary
```

```
Any interface listed with OK? value "NO" does not have a valid configuration
```

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	unassigned	NO	unset	up	down
GigabitEthernet0/0	unassigned	YES	unset	up	up
GigabitEthernet2/0/1	unassigned	YES	unset	down	down
GigabitEthernet2/0/2	unassigned	YES	unset	down	down
GigabitEthernet2/0/3	unassigned	YES	unset	down	down
...					
...					
...					
GigabitEthernet2/0/46	unassigned	YES	unset	down	down
GigabitEthernet2/0/47	unassigned	YES	unset	down	down
GigabitEthernet2/0/48	unassigned	YES	unset	up	up
GigabitEthernet2/1/1	unassigned	YES	unset	down	down
GigabitEthernet2/1/2	unassigned	YES	unset	down	down
GigabitEthernet2/1/3	unassigned	YES	unset	down	down
GigabitEthernet2/1/4	unassigned	YES	unset	down	down
Te2/1/1	unassigned	YES	unset	down	down
Te2/1/2	unassigned	YES	unset	down	down
Te2/1/3	unassigned	YES	unset	down	down
Te2/1/4	unassigned	YES	unset	down	down

```
Enter interface name used to connect to the
management network from the above interface summary: vlan1
```

```
Configuring interface Vlan1:
```

```
Configure IP on this interface? [yes]: yes
```

```
IP address for this interface: 192.0.2.2
```

```
Subnet mask for this interface [255.255.255.0] : 255.255.255.0
```

```
Class C network is 192.0.2.5, 24 subnet bits; mask is /24
```

The following configuration command script is created:

```
hostname sw-3850-1
enable secret 4 vwcGVdcUZcRMcyxaH2U9Y/PTujsnQWPSbt.LFG8lhTw
enable password Cisco123
line vty 0 15
password Cisco123
  ap dot11 24ghz shutdown
  ap dot11 5ghz shutdown
  ap country US
  no ap dot11 24ghz shutdown
```

```

no ap dot11 5ghz shutdown

username admin privilege 15 password 0 cisco
no snmp-server
!
no ip routing

!
interface Vlan1
no shutdown
ip address 192.0.2.1 255.255.255.0
!
interface GigabitEthernet0/0
shutdown
no ip address
!
interface GigabitEthernet2/0/1
!
interface GigabitEthernet2/0/2
!
interface GigabitEthernet2/0/3
...
...
...
interface GigabitEthernet2/0/46
!
interface GigabitEthernet2/0/47
!
interface GigabitEthernet2/0/48
!
interface GigabitEthernet2/1/1
!
interface GigabitEthernet2/1/2
!
interface GigabitEthernet2/1/3
!
interface GigabitEthernet2/1/4
!
interface TenGigabitEthernet2/1/1
!
interface TenGigabitEthernet2/1/2
!
interface TenGigabitEthernet2/1/3
!
interface TenGigabitEthernet2/1/4
!
end

```

[0] Go to the IOS command prompt without saving this config.
 [1] Return back to the setup without saving this config.
 [2] Save this configuration to nvram and exit.

```

Enter your selection [2]: 2
The enable password you have chosen is the same as your enable secret.
This is not recommended. Re-enter the enable password.
Changing country code could reset channel and RRM grouping configuration.
If running in RRM One-Time mode, reassign channels after this command.
Check customized APs for valid channel values after this command.
Are you sure you want to continue? (y/n) [y]: y
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

```

```

Building configuration...
Compressed configuration from 4414 bytes to 2038 bytes[OK]
Use the enabled mode 'configure' command to modify this configuration.

```

Press RETURN to get started

Joining Access Points

To enable wireless services, run `ipservices` or an `ibase` license.


Note

Use the **`boot system switch all flash:packages.conf`** command to boot the switch from internal flash memory.

Connect the Access Points to access mode switch ports in the same VLAN.

Perform the following steps to join the access points on Cisco Catalyst 3850 Series Switch:

- 1 To enable wireless on the switch, use the following commands.

```
sw-3850-1(config)# wireless management interface vlan <1-4095>
```

- 2 Define the Mobility Controller

- To define Cisco Catalyst 3850 Series Switch as the mobility controller, use the following command:

```
sw-3850-1(config)# wireless mobility controller
```


Note

This configuration change requires reboot.

- If Cisco Catalyst 3850 is the Mobility Agent, do the following:

- 1 To the Mobility Controller IP address with the following command:

```
sw-3850-1(config)# wireless mobility controller ip a.b.c.d
```

- 2 Enter the following commands on the Mobility Controller:

```
3850MC(config)# wireless mobility controller peer-group <SPG1>
```

```
3850MC(config)# wireless mobility controller peer-group <SPG1> member ip w.x.y.z
```

- 3 Ensure license availability.

To ensure that the active Access Point Licenses are available on the Mobility Controller, use the following commands. The Mobility Agent uses the licenses that are activated on the Mobility Controller.


Note

- To enable wireless services, run `ipservices` or an `ibase` license.
- Access Point count licenses are applied on the Mobility Controller, and are automatically provisioned and applied on the Mobility Agent.
- The Cisco Catalyst 3850 Series Switches, which act as Mobility Controller can support up to 100 APs.

```
sw-3850-1# show license right-to-use summary
```

License Name	Type	Count	Period left
ipservices	permanent	N/A	Lifetime
apcount	base	0	Lifetime

```
apcount      adder      100      Lifetime
-----
```

```
License Level In Use: ipservices
License Level on Reboot: ipservices
Evaluation AP-Count: Disabled
Total AP Count Licenses: 100
AP Count Licenses In-use: 3
AP Count Licenses Remaining: 97
```

- 4 To activate the Access Point count license on the Cisco Catalyst 3850 Series Switch, enter the following command with the required Access Point count on the Mobility Controller:

```
sw-3850-1# license right-to-use activate apcount <count> slot <#> acceptEULA
```

- 5 Configure the Access Point discovery process.

To enable the Access Points to join the controller, the switch port must be set as an access port in the wireless management VLAN. Use the following command if VLAN100 is used for the wireless management interface:

```
sw-3850-1(config)# interface gigabitEthernet1/0/10
sw-3850-1(config-if)# switchport mode access
sw-3850-1(config-if)# switchport access vlan 100
```

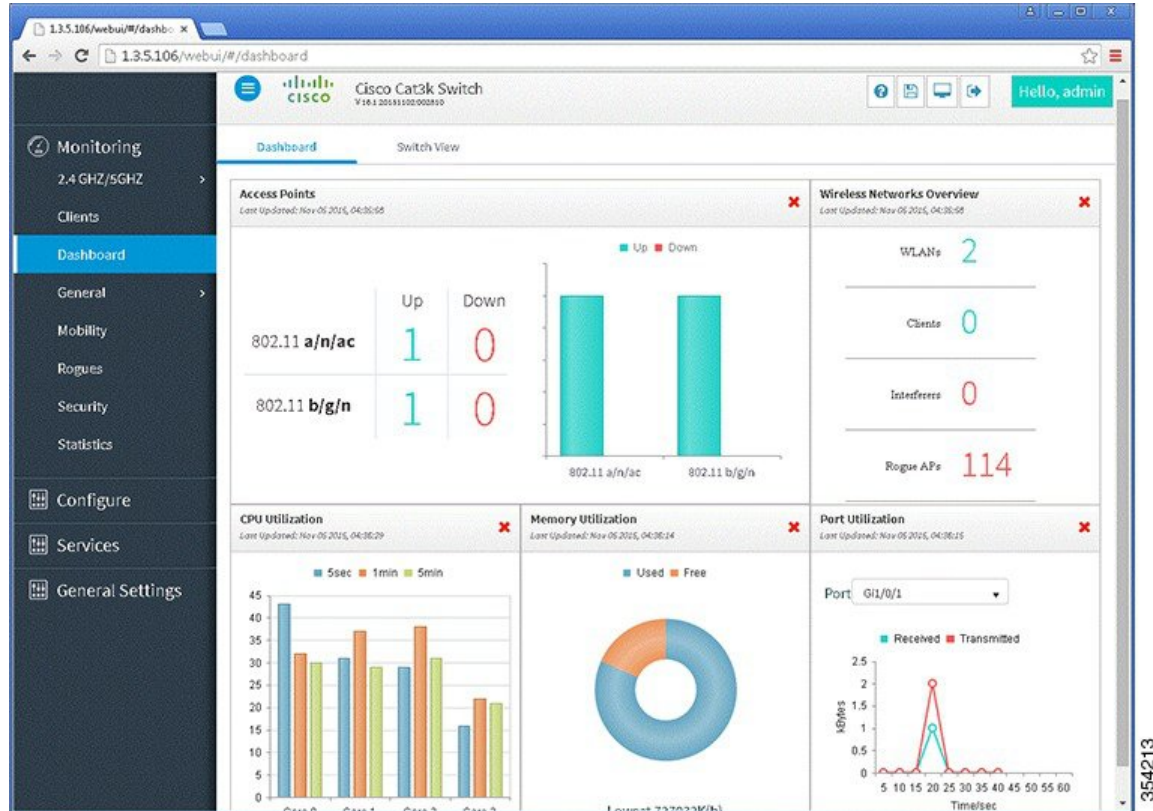
- 6 To configure web access, use the following command.

```
sw-3850-1(config)# username admin privilege 15 password 0 admin
sw-3850-1(config)# ip http server
```

- To access the GUI, log on to `http:// mgmt_ip/ webui/`

- Define the login credentials in the initial configuration dialog box. After successful authentication, the Wireless Controller Home page displays, as shown in the following figure.

Figure 65: Wireless Controller Home Page



- 7 To ensure that the proper country code is configured on the switch that is compliant with the regulatory domain of the country in which the Access Points are deployed, use the following command.

```
sw-3850-1# show wireless country configured
Configured Country.....: US - United States
Configured Country Codes
US - United States : 802.11a Indoor,Outdoor/ 802.11b / 802.11g
```

To enter the country code, enter the following commands:

```
sw-3850-1(config)# ap dot11 24ghz shutdown
sw-3850-1(config)# ap dot11 5ghz shutdown
sw-3850-1(config)# ap country BE
```

Changing country code could reset channel and RRM grouping configuration. If running in RRM One-Time mode, reassign channels after this command. Check customized APs for valid channel values after this command. Are you sure you want to continue? (y/n)[y]: y

```
sw-3850-1(config)# no ap dot11 24ghz shut
sw-3850-1(config)# no ap dot11 5ghz shut
sw-3850-1(config)# end
```

```
sw-3850-1# write memory

Building configuration...
Compressed configuration from 3564 bytes to 2064 bytes[OK]

sw-3850-1# show wireless country configured

Configured Country.....: BE - Belgium
Configured Country Codes
  BE - Belgium : 802.11a Indoor,Outdoor/ 802.11b / 802.11g
```

Verifying Access Points

To verify that the Access Points are joined in Cisco Catalyst 3850 Series Switch, use the following command:

```
sw-3850-1# show ap summary

Number of APs: 1

Global AP User Name: Not configured
Global AP Dot1x User Name: Not configured

AP Name                AP Model  Ethernet MAC    Radio MAC        State
-----
APa493.4cf3.232a      1042N     a493.4cf3.231a  10bd.186e.9a40   Registered
```

Troubleshooting Access Point Issues

To resolve access point joint issues, use the following debug commands:

```
sw-3850-1# debug capwap ios detail
CAPWAP Detail debugging is on

sw-3850-1# debug capwap ios error
CAPWAP Error debugging is on

sw-3850-1# debug capwap ios event
CAPWAP Event debugging is on

sw-3850-1# debug capwap ios packet
CAPWAP Packet debugging is on

sw-3850-1# debug capwap ios rf
CAPWAP Redundancy debugging is on

sw-3850-1# debug capwap ios stacking
CAPWAP Stacking debugging is on
```



CHAPTER 18

Local Web Authentication with External RADIUS Authentication

This document provides information about the global configuration commands that are required to work on an external RADIUS server using the Local Web Authentication.

- [List of Global Configuration Commands](#), page 199
- [WLAN Configuration Commands](#), page 200

List of Global Configuration Commands

Use the following commands to make the Local Web Authentication work with an external radius server:

Command or Action	Description/ Purpose/Example
radius server <i>ise</i>	Defines external radius server Example: <i>ise</i>
address ipv4 192.0.2.1 auth-port 1812 acct-port 1813 Key <i>Cisco123</i>	Defines the IP address, authentication port communication, and accounting port communication.
aaa group server radius <i>rad_ise</i>	Defines the AAA RADIUS group and specifies the relevant RADIUS server. <ul style="list-style-type: none">• RADIUS group <i>rad_ise</i>• Server name: <i>ise</i>
aaa authentication login <i>ext_ise</i> group <i>rad_ise</i>	Defines the authentication method which points to a RADIUS group. For example, the authentication method <i>ext_ise</i> points to the RADIUS group <i>rad_ise</i> .

WLAN Configuration Commands

Use the following commands to configure WLAN:

```
wlan webauth 11 local_webauth
  client vlan 263
  no security wpa
  no security wpa akm dot1x
  no security wpa wpa2
  no security wpa wpa2 ciphers aes
  security web-auth
  security web-auth authentication-list ext_ise -----> calling auth method ext_ise which
points to ise
  security web-auth parameter-map test_web
  no shutdown
```



Local Web Authentication on Converged Access

This document provides information about the global configuration commands that enable the local web authentication on a Wireless LAN controller (WLC). The document also provides information on WLAN configuration commands and global parameter maps.

- [List of Global Configuration Commands, page 201](#)
- [Information about Parameter Maps, page 202](#)
- [Additional Information on Parameter Maps, page 204](#)
- [WLAN Configuration Commands, page 204](#)
- [Troubleshooting the Configuration, page 204](#)

List of Global Configuration Commands

Use the following commands to enable the local web authentication on the WLC:

Command or Action	Description/Purpose/Example
aaa new-model	Enables the authentication, authorization, and accounting (AAA) access control model.
aaa authentication login wcm_local local	'wcm_local' is a method which you call under WLAN.
aaa authorization network default local	The default authorization is set to local.
aaa authorization credential-download default local	Configures the local database to download Extensible Authentication Protocol (EAP) credentials. Note You can use Local. aaa authorization credential-download command family to download credentials from RADIUS or Lightweight Directory Access Protocol (LDAP).

Command or Action	Description/Purpose/Example
username test password 0 test12345	Enables you to test the username and password for local authentication.
parameter-map type webauth global virtual -IP ipv4 192.0.2.1	Enables you to configure the virtual IP address which is required for external and internal Web Authentication. The Logout button uses virtual IP Central Web Authentication (CWA). However, it is not mandatory for the Logout button to have a virtual IP.
parameter-map type webauth test_web <ul style="list-style-type: none"> • type webauth • Banner c test webauth c 	It is a web authentication method in which you need to specify a name to call the web authentication method under the WLAN configuration.
ip http server	Enables the http server. It is required for HTTPS authentication.
ip http authentication local	Log in to GUI using the local authentication.
ip http secure-server	Enables you to access secure web authentication. Note To disable secure web authentication, use no ip http secure-server command.

Information about Parameter Maps

Global Parameter Maps

Use the following commands to configure the Global Parameter Maps:

```
Device# configure terminal
Device(config)# parameter-map type webauth global
Device(config-params-parameter-map)# ?
```

Use the following commands to configure the pre-parameter map for global parameter maps:

Command or Action	Description/Purpose/Example
Banner	Adds extra text on the pages that are generated.
custom-page	Designs login, expired, success, or failure pages that the user can download on the system flash.
Exit	Exits from the parameter map configuration mode.

Command or Action	Description/Purpose/Example
max-http-conns	Configures maximum number of http connections for each client. It can be configured from 1 to 200, with 20 as the default value.
No	Disables a function or to set a default value.
Redirect url	Provides the user with a custom designed page on an external server.
Timeout	Configures an initial timeout session for a user to complete authentication.
Virtual IP	Required for logout page and for external web authentication.
Watch-list	Creates a watch list for the web authentication clients. This is not required for wireless clients.

User Defined Parameter Maps

Use the following commands to configure the User Defined Parameter Maps:

```
Device# configure terminal
Device(config)# parameter-map type webauth test
Device(config-params-parameter-map)# ?
```

Use the following commands to configure the pre-parameter map for user defined parameter maps:

Command or Action	Description/Purpose/Example
Banner	Adds extra text on the pages that are generated.
Consent	Displays the terms and conditions that the user needs to accept to enable access.
custom-page	Designs login, expired, success, or failure pages that the user can download on the system flash.
Exit	Exits from the parameter map configuration mode.
max-http-conns	Configures maximum number of http connections for each client. It can be configured from 1 to 200, with 20 as the default value.
No	Disables a function or to set a default value.
Redirect url	Provides the user with a custom designed page on an external server.

Command or Action	Description/Purpose/Example
Timeout	Configures an initial timeout session for a user to complete authentication.
Type	Configures the type of parameter, such as, web authentication, consent, or web consent.

Additional Information on Parameter Maps

The following information is applicable to parameter maps:

- If the parameter-map name that is configured on the WLAN is not valid, global parameter-map configuration is used.
- If user defined parameter name exists, its values are merged with the values that are configured for the global parameter-map. If user defined parameter and global parameters have values configured for a particular field, the user defined parameter map values are used.
- Some of the parameter-map fields such as, ratelimit, needs to be removed from the configuration.
- For custom-pages, the files for login, success, failure, expired needs to be provided before the pages are used.
- If the custom pages are configured, then any banner configuration for the page is ignored.
- Virtual IP address should be configured if web authentication logout page is required or if the external web authentication is done for the logout page.
- The Authentication Bypass functionality is not supported for wireless clients.

WLAN Configuration Commands

Use the following commands to configure WLAN:

```
wlan webauth 11 local_webauth
client vlan 263
from vlan 263
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
web-auth
security web-auth authentication-list wcm_local
method from global configuration
security web-auth parameter-map test_web
type from global configuration
```

-----> client vlan. clients get ip

-----> set wlan security to

-----> call the authentication

-----> call the webauth method

Troubleshooting the Configuration

The Access Control Lists are applied to the HTTP server. If web authentication fails to load, verify the following:

```
ip http access-class ##
```




PEAP Authentication with Microsoft NPS Configuration

This document describes how to configure Protected Extensible Authentication Protocol (PEAP) with Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAP v2) authentication on a Cisco Converged Access Wireless LAN (WLAN) deployment with the Microsoft Network Policy Server (NPS) as the RADIUS server.

- [Prerequisites for WLC PEAP Authentication with Microsoft NPS Configuration, page 205](#)
- [Background Information on PEAP, page 206](#)
- [Configuring PEAP with MS-CHAP v2, page 207](#)
- [Troubleshooting WLC PEAP Authentication with Microsoft NPS Configuration Issues, page 223](#)

Prerequisites for WLC PEAP Authentication with Microsoft NPS Configuration

You should have knowledge on the following topics before you configure PEAP as described in this document.

- Basic Microsoft Windows Version 2008 installation.
- Cisco Converged Access WLAN controller installation.

Ensure that following requirements are met before you start with the configuration:

- Installation of Microsoft Windows Server Version 2008 Operating System (OS) on each of the servers in the test lab.
- Upgradation on all of the service packs.
- Installation of controllers and Lightweight Access Points (LAPs).
- Configuration of latest software updates.

Supported Platforms and Releases

The information in this document is based on the following:

- Cisco Catalyst 3850 Series Switch.
- Cisco 3602 Series LAP.
- Microsoft Windows XP with Intel PROset Supplicant.
- Microsoft Windows Version 2008 Server that runs NPS with Domain Controller Roles.
- Cisco Catalyst 3500 Series Switches.

**Note**

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information on PEAP

PEAP uses Transport Level Security (TLS) in order to create an encrypted channel between an authenticating PEAP client, such as a wireless laptop, and a PEAP authenticator, such as the Microsoft NPS or any RADIUS server. PEAP does not specify an authentication method but provides additional security for other Extensible Authentication Protocols (EAPs), such as EAP-MS-CHAP v2 that can operate through the TLS-encrypted channel that is provided by PEAP.

The PEAP authentication process divided into two main phases:

- 1 TLS-Encrypted Channel
- 2 EAP-Authenticated Communication

TLS-Encrypted Channel

The wireless client associates with the Access Point (AP) and an IEEE 802.11-based association provides an open system or shared key authentication before a secure association is created between the client and the AP. After the IEEE 802.11-based association is successfully established between the client and the AP, the TLS session is negotiated with the AP.

After authentication is successfully completed between the wireless client and the NPS, the TLS session is negotiated between the client and the NPS. The key that is derived within this negotiation is used in order to encrypt all subsequent communication.

EAP-Authenticated Communication

EAP communication, which includes EAP negotiation, occurs inside of the TLS channel that is created by PEAP within the first stage of the PEAP authentication process. The NPS authenticates the wireless client with EAP-MS-CHAP v2. The LAP and the controller only forward messages between the wireless client and

the RADIUS server. Since WLC is not the TLS endpoint, the WLAN Controller (WLC) and the LAP cannot decrypt the messages.

The following steps shows the RADIUS message sequence for a successful authentication attempt, where the user supplies valid password-based credentials with PEAP-MS-CHAP v2:

- 1 The NPS sends an identity request message to the client:
`EAP-Request/Identity`
- 2 The client responds with an identity response message:
`EAP-Response/Identity`
- 3 The NPS sends an MS-CHAP v2 challenge message:
`EAP-Request/EAP-Type=EAP MS-CHAP-V2 (Challenge)`
- 4 The client responds with an MS-CHAP v2 challenge and response:
`EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Response)`
- 5 The NPS responds with an MS-CHAP v2 success packet when the server successfully authenticates the client:
`EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (Success)`
- 6 The client responds with an MS-CHAP v2 success packet when the client successfully authenticates the server:
`EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Success)`
- 7 The NPS sends an EAP-type-length-value (TLV) that indicates successful authentication.
- 8 The client responds with an EAP-TLV status success message.
- 9 The server completes authentication and sends an EAP-Success message in plain text. If VLANs are deployed for client isolation, the VLAN attributes are included in this message.

Configuring PEAP with MS-CHAP v2

This section describes how to configure PEAP with MS-CHAP v2 authentication on a Cisco Converged Access WLC deployment with the Microsoft NPS as the RADIUS server.

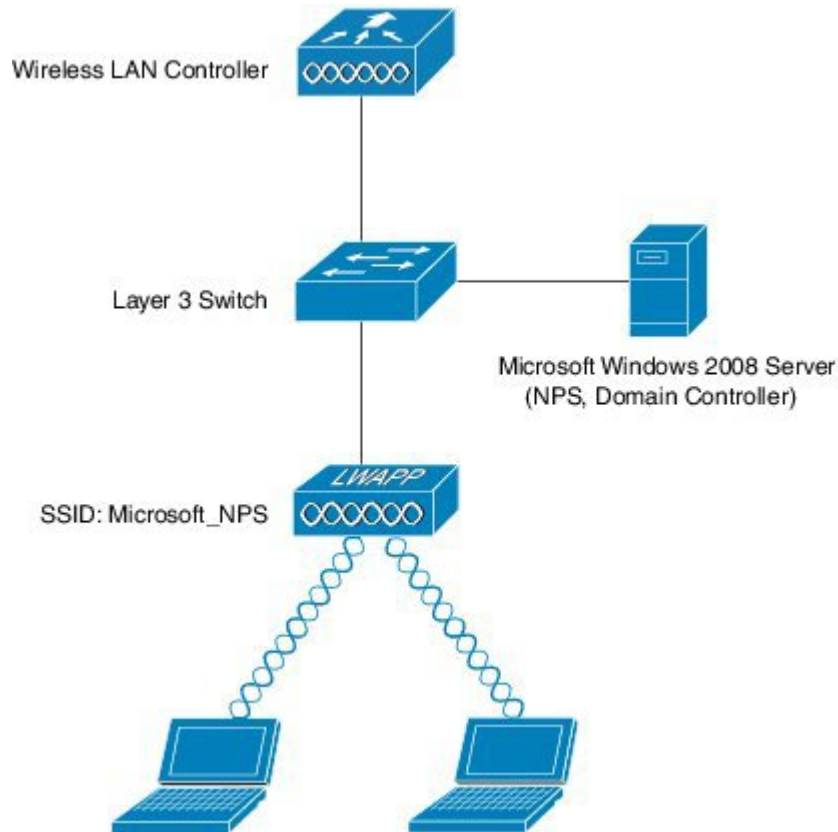
The configuration is a two-step process which includes:

- Configuring Cisco Catalyst 3850 Series Switch WLC with the CLI or GUI.
- Configuring Microsoft Windows Version 2008 server for NPS, Domain Controller, and User Accounts on the AD.

Network Diagram of PEAP with MS-CHAP v2 authentication

The following figure shows the network diagram of PEAP with MS-CHAP v2 authentication:

Figure 66: Network diagram of PEAP with MS-CHAP v2 authentication



In the above figure, the Microsoft Windows Version 2008 server performs following roles:

- Domain controller for the **wireless.com** domain
- Domain Name System (DNS) server
- Certificate Authority (CA) server
- NPS in order to authenticate the wireless users
- Active Directory (AD) in order to maintain the user database

The server connects to the wired network through a Layer 2 (L2) switch, as shown in above illustration. The WLC and the registered LAP also connect to the network through the L2 switch.

The wireless clients use Wi-Fi Protected Access 2 (WPA2) - PEAP-MS-CHAP v2 authentication in order to connect to the wireless network.

Configuring Converged Access WLCs (CLI)

Perform the following tasks to configure the WLAN for the required client VLAN and map it to the Authentication Method List using the CLI:



Note Ensure that **dot1x system auth control** is enabled on the WLC, or the dot1X does not work.

- 1 Enable the AAA new model feature.
- 2 Configure the RADIUS server.
- 3 Add the server into the Server Group.
- 4 Map the Server Group to the Method List.
- 5 Map the Method List to the WLAN.

```

aaa new-model
!
!
aaa group server radius Microsoft_NPS
server name Microsoft_NPS
!
aaa authentication dot1x Microsoft_NPS group Microsoft_NPS

aaa authorization network Microsoft_NPS group Microsoft_NPS
radius server Microsoft_NPS
address ipv4 10.104.208.96 auth-port 1645 acct-port 1646
timeout 10
retransmit 10
key Cisco123

wlan Microsoft_NPS 8 Microsoft_NPS
client vlan VLAN0020
no exclusionlist
security dot1x authentication-list Microsoft_NPS
session-timeout 1800
no shutdown

```

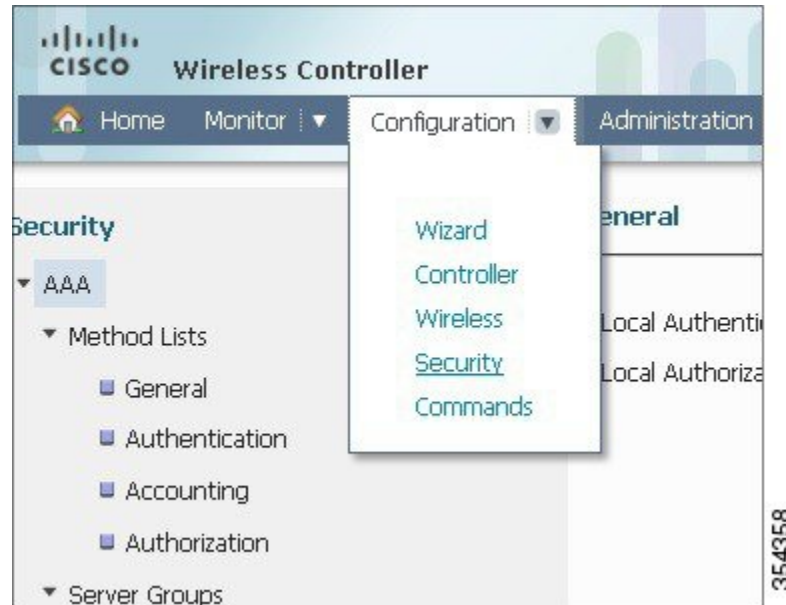
Configuring Converged Access WLCs (GUI)

Perform the following tasks to configure the Converged Access WLCs using the GUI:

- Step 1** Navigate to **Configuration > Security > AAA > Method Lists > General** and enable the **Dot1x System Auth Control** by selecting the checkbox.

Step 2 To add the RADIUS servers, navigate to **Configuration > Security > AAA**.

Figure 67: Adding the radius server



Step 3 To add or edit Server IP Address and Shared Secret fields on the Radius Server page, navigate to **Security > AAA > RADIUS > Servers**.

- Once you configure the RADIUS server, the **Server** tab should display the fresh configured Server Name (Microsoft_NPS in this example), Server IP Address, Auth Port and Acct Port.

Note Make sure that both shared secret and shared secret that is configured on the RADIUS server are matching.

Step 4 To configure a **Server Group**, navigate to **Security > AAA > Server Group**.

- Choose **Group Type** field as **Radius** on the Radius Servers Groups page.
- Choose the RADIUS server that you created in the previous step (Microsoft_NPS in this example) as **Servers In This Group** field.
- After the configuration, the **Server Group** window should display name of the server and its group name respectively

Step 5 To configure **Authentication**, navigate to **Security > AAA > Method Lists > Authentication**.

- Choose Authentication Method List **Type** field as **dot1x** on Authentication page.
- Choose **Group Type** field as **Group** on Authentication page.
- Map the Server Group that you configured (Microsoft_NPS in this example) on Authentication page.
- After the configuration, the **Authentication** Method List window should display name of the configured server group, Authentication Method List type and its Group type.

Step 6 To configure an **Authorization**, navigate to **Security > AAA > Method Lists > Authorization**.

- Choose Authentication Method List **Type** field as **network** on Authorization page.
- Choose **Group Type** field as **Group** on Authorization page.
- Map the Server Group that you configured (Microsoft_NPS in this example) on Authorization page.
- After the configuration, the **Authorization** Method List window should display name of the configured server group, Authorization Method List type as well as its Group type.

Step 7 To configure a new WLAN, navigate to **Configure > Wireless** and click **WLANs**.

- Choose **Profile Name** field as Server Group name (Microsoft_NPS in this example) under **General** tab on WLAN page.
- Check the **Status** field checkbox to disabled the status under **General** tab on WLAN page
- After configuration, the **Layer2** tab under **Security** tab on WLAN page should display the new configuration.

Note In WLAN, users can connect and become authenticated through the Microsoft NPS server with EAP authentication.

Step 8 Map the **Authentication Method** field to Server Group Name (Microsoft_NPS in this example) on **AAA Server** tab under **Security** tab on WLAN page. This mapping helps to authenticate the client to the correct server.

Configuring the Microsoft Windows Version 2008 Server

This section describes configuring Microsoft Windows Version 2008 server. The configuration is a six-step process as listed hereunder:

- 1 Configuring the server as a domain controller.
- 2 Installing and configuring the server as a CA server.
- 3 Installing the NPS.
- 4 Installing a certificate.
- 5 Configuring the NPS for PEAP authentication.
- 6 Adding users to the AD.

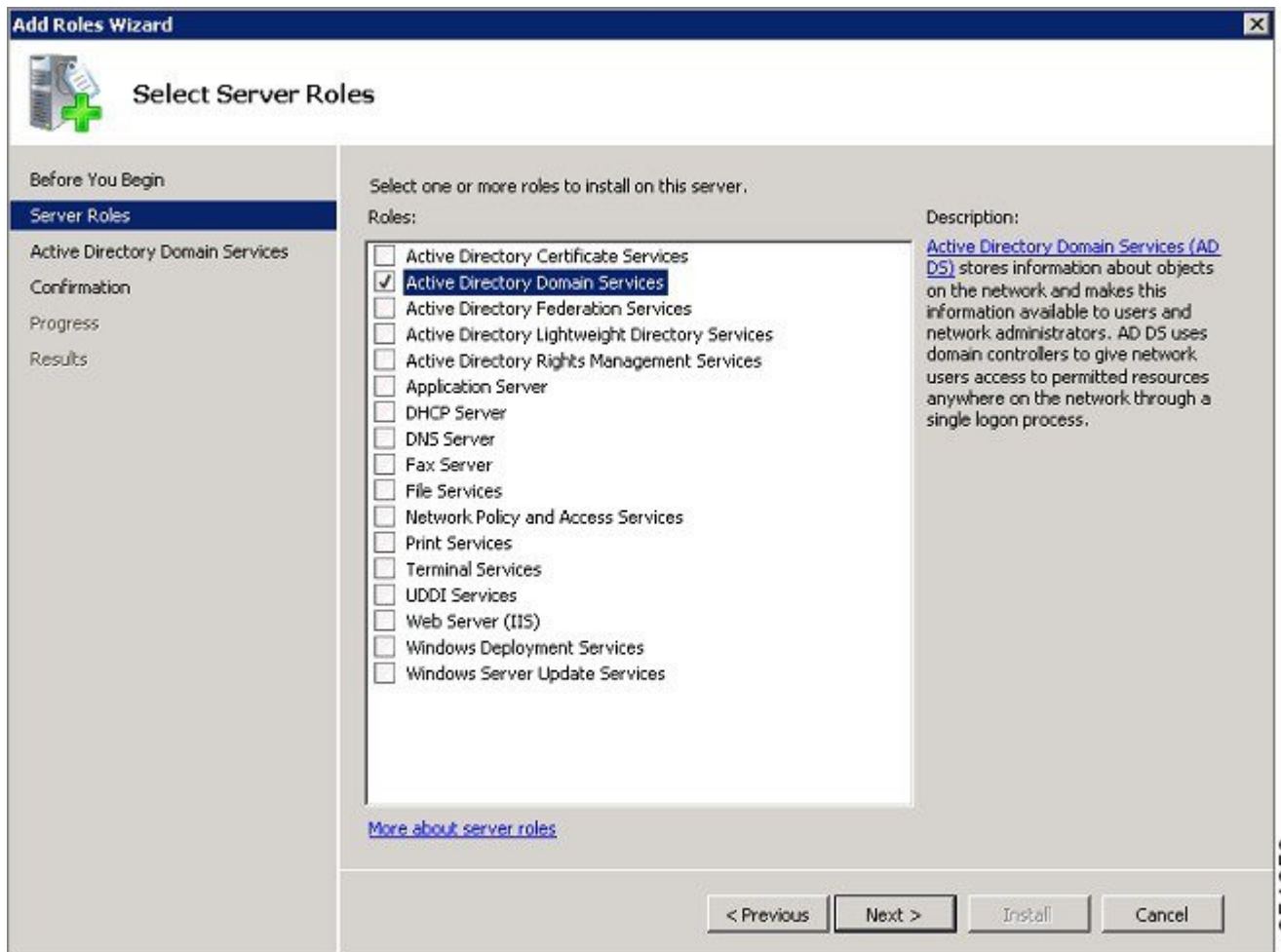
Configuring the Microsoft Windows 2008 Server as a Domain Controller

Perform the following task and follow the instructions on the screen to configure the Microsoft Windows Version 2008 server as a domain controller.

Step 1 To configure the Microsoft Windows Version 2008 server as a Domain Controller, navigate to **Start > Server Manager > Roles > Add Roles** and click **Next** on **Before you Begin** screen.

Step 2 Check the **Active Directory Domain Services** check box on **Select Server Roles** screen and click **Next**.

Figure 68: Selecting server role



Step 3 Review the **Introduction to Active Directory Domain Services** on **Active Directory Domain Services** screen and click **Next**.

Step 4 Click **Install** on **Confirm Installation Selections** screen in order to begin the installation process.

- The installation proceeds and completes.

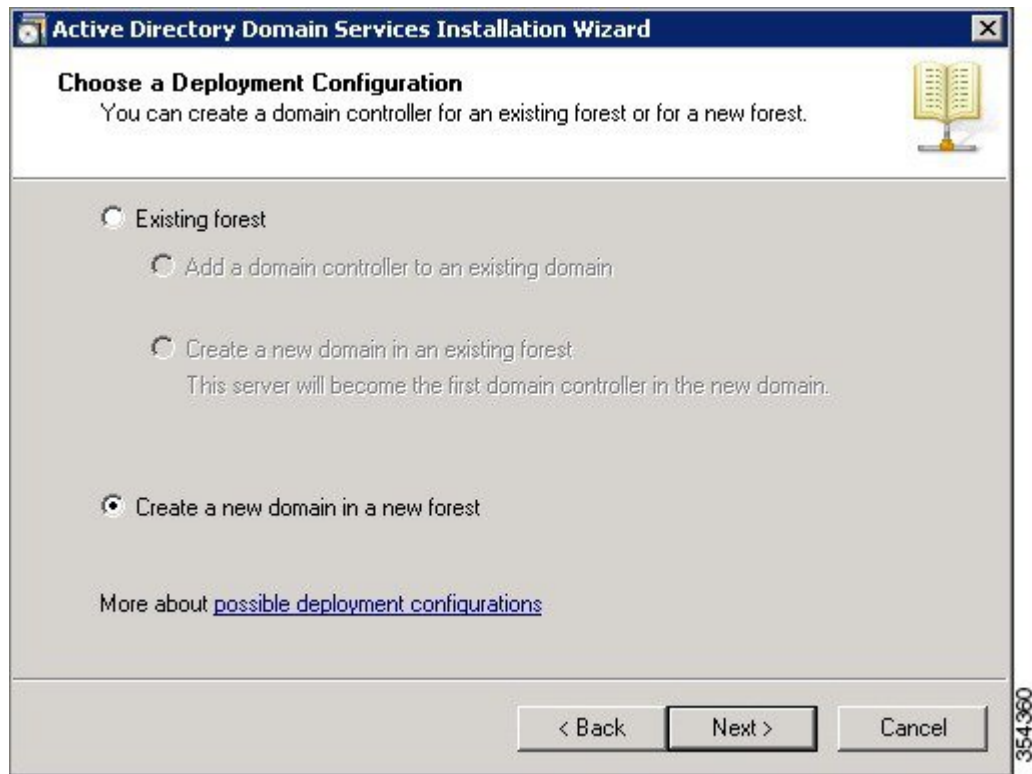
Step 5 Click **Close this wizard and launch the Active Directory Domain Services Installation Wizard** (dcpromo.exe) on **Installation Results** screen in order to continue the installation and configuration of the AD.

Step 6 Click **Next** in order to run the **Active Directory Domain Services Installation Wizard**.

Step 7 Review the information about **Operating System Compatibility** and click **Next** on **Active Directory Domain Services Installation Wizard** screen.

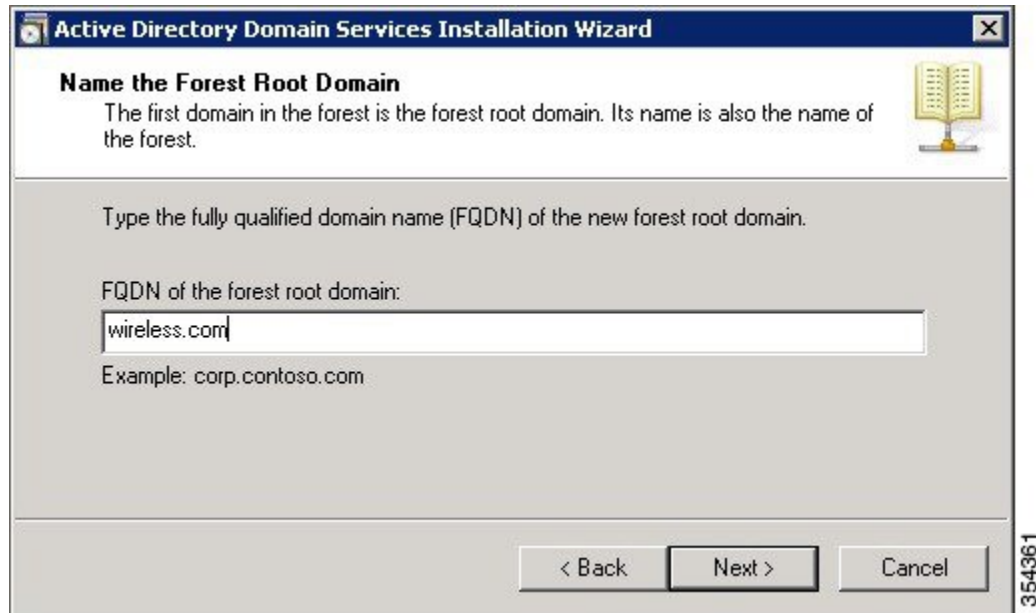
Step 8 Choose the **Create a new domain in a new forest** radio button and click **Next** in order to create a new domain.

Figure 69: Create a new domain in a new forest



Step 9 Enter the full DNS name for the new domain (**wireless.com** in this example) and click **Next**.

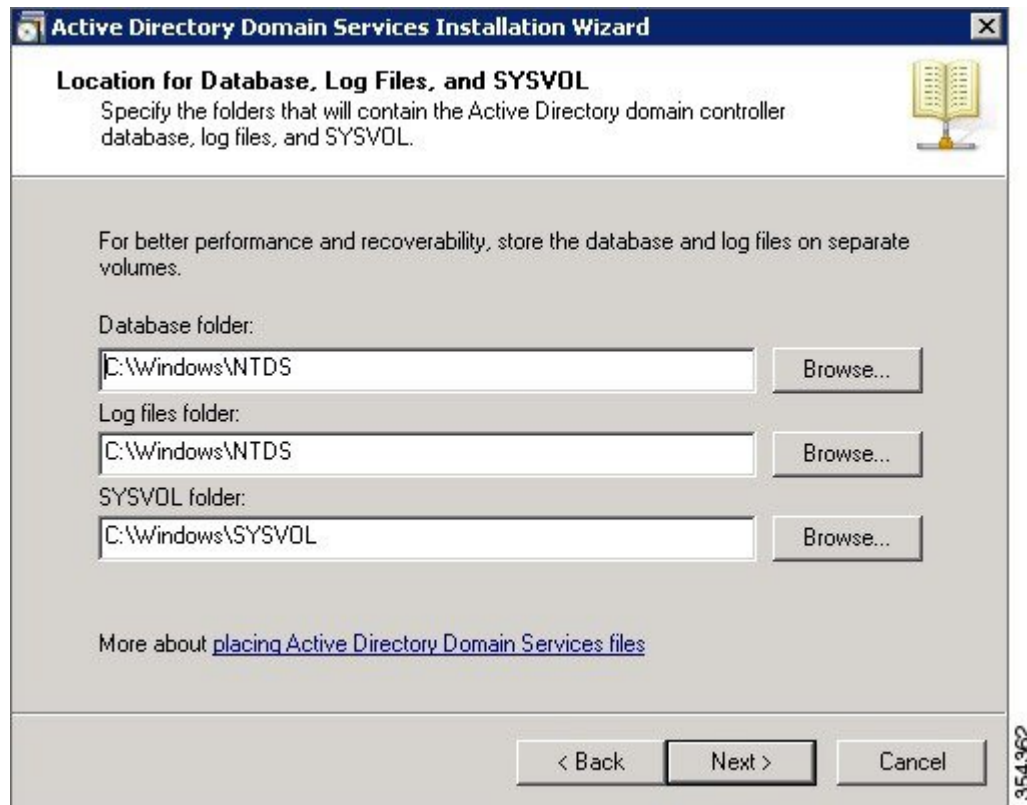
Figure 70: Entering the full DNS name



- Step 10** Choose the **Forest functional level** from the drop-down list on **Set Forest Functional Level** screen for your domain and click **Next**.
- Step 11** Choose the **Domain functional level** from the drop-down list on **Set Forest Functional Level** screen for your domain and click **Next**.
- Step 12** Check the **DNS server** check box on **Additional Domain Controller Options** screen and click **Next**.
- Step 13** Click **Yes** when the **Active Directory Domain Services Installation Wizard** pop-up window appears in order to create a new zone in the DNS for the domain.

Step 14 Choose the folders that you want the AD to use for files and click **Next**.

Figure 71: Adding folders that you want the AD



Step 15 Enter the Administrator Password and confirm the same on **Directory Services Restore Mode Administrator Password** screen, and then, click **Next**.

Step 16 Review your selections on **Summary** screen and click **Next**.
The installation proceeds.

Step 17 Click **Finish** in order to close the **Active Directory Services Installation wizard**.

Step 18 Restart the server in order for the changes to take effect.

Installing and configuring the Microsoft server as a CA server

PEAP with EAP-MS-CHAP v2 validates the RADIUS server based upon the certificate that is present on the server. Additionally, the server certificate must be issued by a public CA that is trusted by the client computer. That is, the public CA certificate already exists in the Trusted Root Certification Authority folder on the client computer certificate store.

Perform the following task and follow the instructions on the screen to configure the Microsoft Windows Version 2008 server as a CA server that issues the certificate to the NPS.

-
- Step 1** To install and configure the Microsoft Windows Version 2008 server as a CA server, navigate to **Start > Server Manager > Roles > Add Roles** and click **Next** on **Before You Begin** screen.
 - Step 2** Check the **Active Directory Certificate Services** check box on **Select Server Roles** screen and click **Next**.
 - Step 3** Review the **Introduction to Active Directory Certificate Services** on **Add Roles Wizard** screen and click **Next**.
 - Step 4** Check the **Certificate Authority** check box on **Select Server Services** screen and click **Next**.
 - Step 5** Choose the **Enterprise** radio button on **Specify Setup Type** screen and click **Next**.
 - Step 6** Choose the **Root CA** radio button on **Specify CA Type** screen and click **Next**.
 - Step 7** Choose the **Create a new private key** radio button on **Set Up Private Key** screen and click **Next**.
 - Step 8** Click **Next** in the **Configuring Cryptography for CA** window.
 - Step 9** To accept the default name of **Common name for this CA** field, click **Next** on **Configure CA Name** screen.
 - Step 10** Enter the validity period for the generated CA certificate on **Set Validity Period** screen and click **Next**.
 - Step 11** To accept the default location of **Certificate database**, click **Next** on **Configure Certificate Database** screen.
 - Step 12** Review the configuration and click **Install** in order to begin the installation of **Active Directory Certificate Services**.
 - Step 13** After the installation is completed, click **Close**.
-

Installing the NPS on the Microsoft Windows Version 2008 Server

Perform the following task and follow the instructions on the screen to install and configure the NPS on the Microsoft Windows Version 2008 server.



Note With the setup that is described in this section, the NPS is used as a RADIUS server in order to authenticate the wireless clients with PEAP authentication.

-
- Step 1** To install and configure the NPS on the Microsoft Windows Version 2008 server, navigate to **Start > Server Manager > Roles > Add Roles**, and click **Next** on **Before You Begin** screen.
 - Step 2** Check the **Network Policy and Access Services** check box on **Select Server Roles** screen and click **Next**.
 - Step 3** Review the **Introduction to Network Policy and Access Services** on **Network Policy and Access Services** screen and click **Next**.
 - Step 4** Check the **Network Policy Server** check box on **Select Role Services** screen and click **Next**.

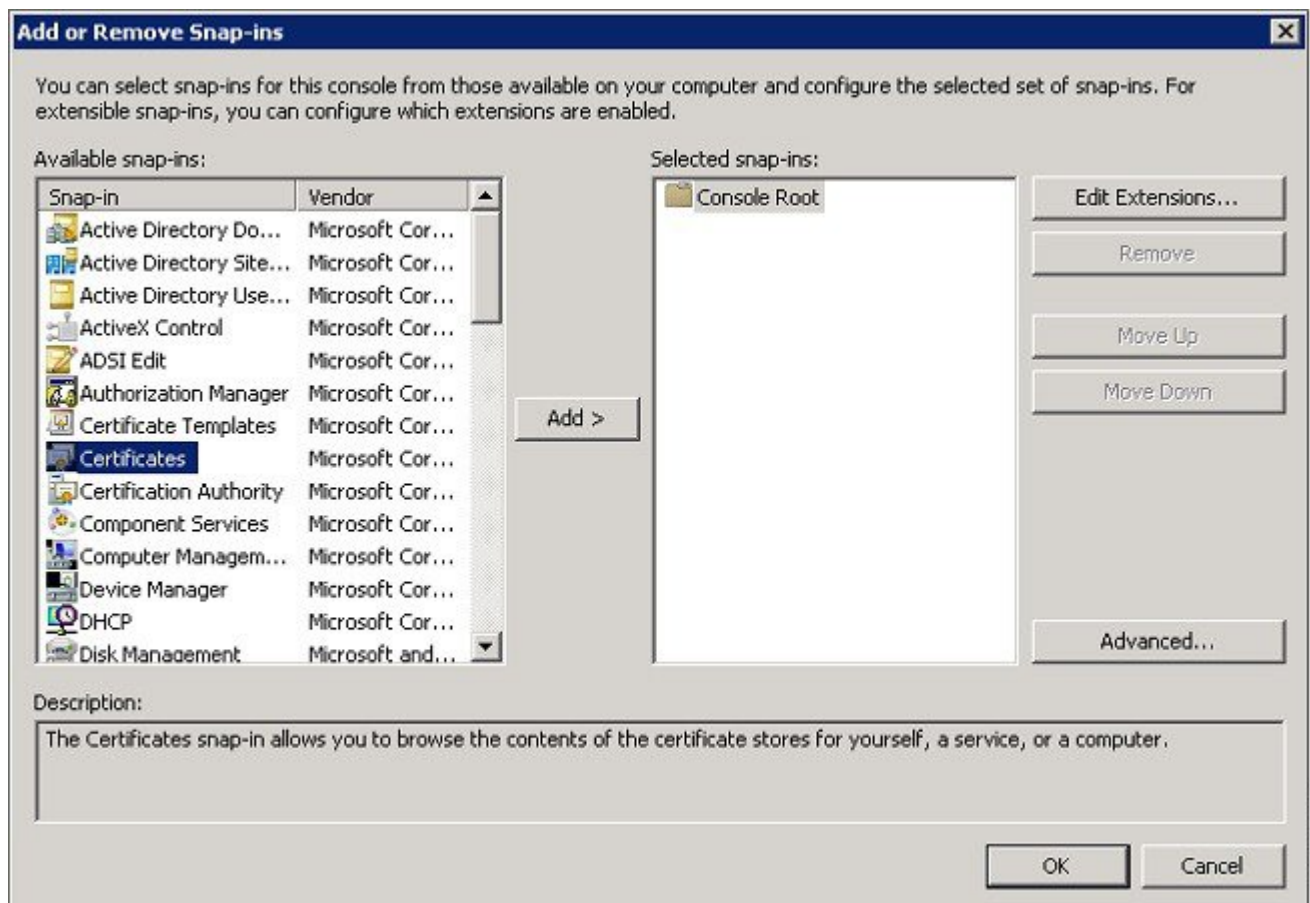
- Step 5** Review the confirmation on **Confirm Installation Selections** screen and click **Install**.
- Step 6** After the installation is complete, close the **Add Roles Wizard**.

Installing a Certificate on NPS Server

Perform the following task and follow the instructions on the screen to install the computer certificate for the NPS.

- Step 1** Click **Start**, enter the Microsoft Management Console (MMC), and press **Enter**.
- Step 2** Navigate to **File > Add/Remove Snap-in**.
- Step 3** Choose **Certificates** on **Add or Remove Snap-in** screen and click **Add**.

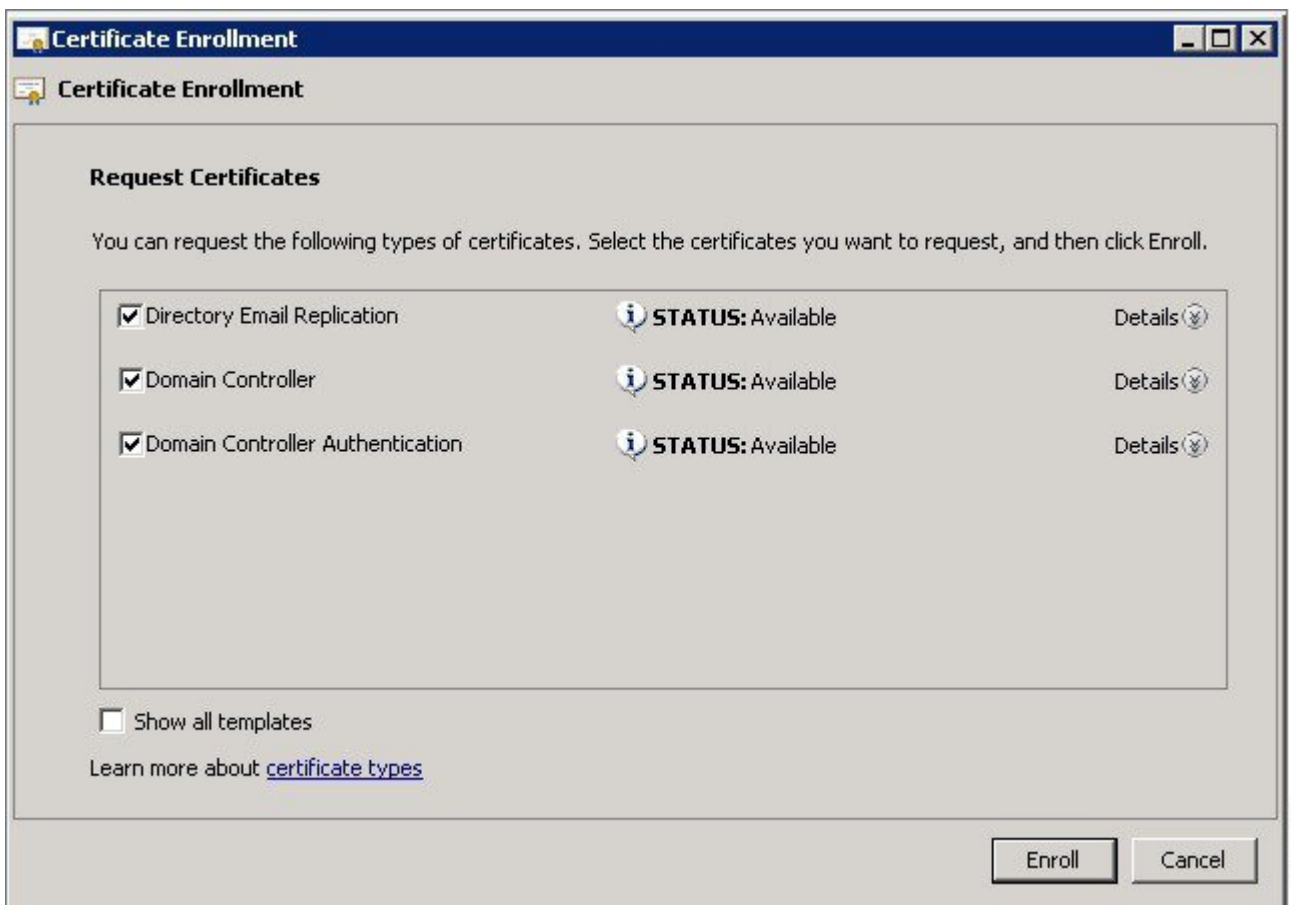
Figure 72: Adding Certificate



354363

- Step 4** Choose the **Computer account** radio button on **Certificate snap-in** screen and click **Next**.
- Step 5** Choose the **Local Computer** radio button on **Select Computer** screen and click **Finish**.
- Step 6** Click **OK** on **Add or Remove Snap-in** screen in order to return to the MMC.
- Step 7** Expand the **Certificates (Local Computer)** and **Personal** folders on **MMC**, and then click **Certificates**.
- Step 8** Right-click on the white space in the CA certificate on **MMC**, and choose **All Tasks > Request New Certificate** and click **Next** on **Certificate Enrollment** window.
- Step 9** Click the **Domain Controller** check box on **Certificate Enrollment** window, and click **Enroll**.
- Note** If the client authentication fails due to an EAP certificate error, then ensure that all of the check boxes are checked on this **Certificate Enrollment** page before you click **Enroll**. This creates three certificates.

Figure 73: Certificate Enrollment Checkboxes



354364

- Step 10** Click **Finish** on **Certificate Enrollment** window once the certificate is installed.
- The NPS certificate is now installed.

Note Ensure that Client Authentication, Server Authentication appears in the **Intended Purposes** column for the certificate on **MMU**.

Configuring the NPS for PEAP-MS-CHAP v2 Authentication

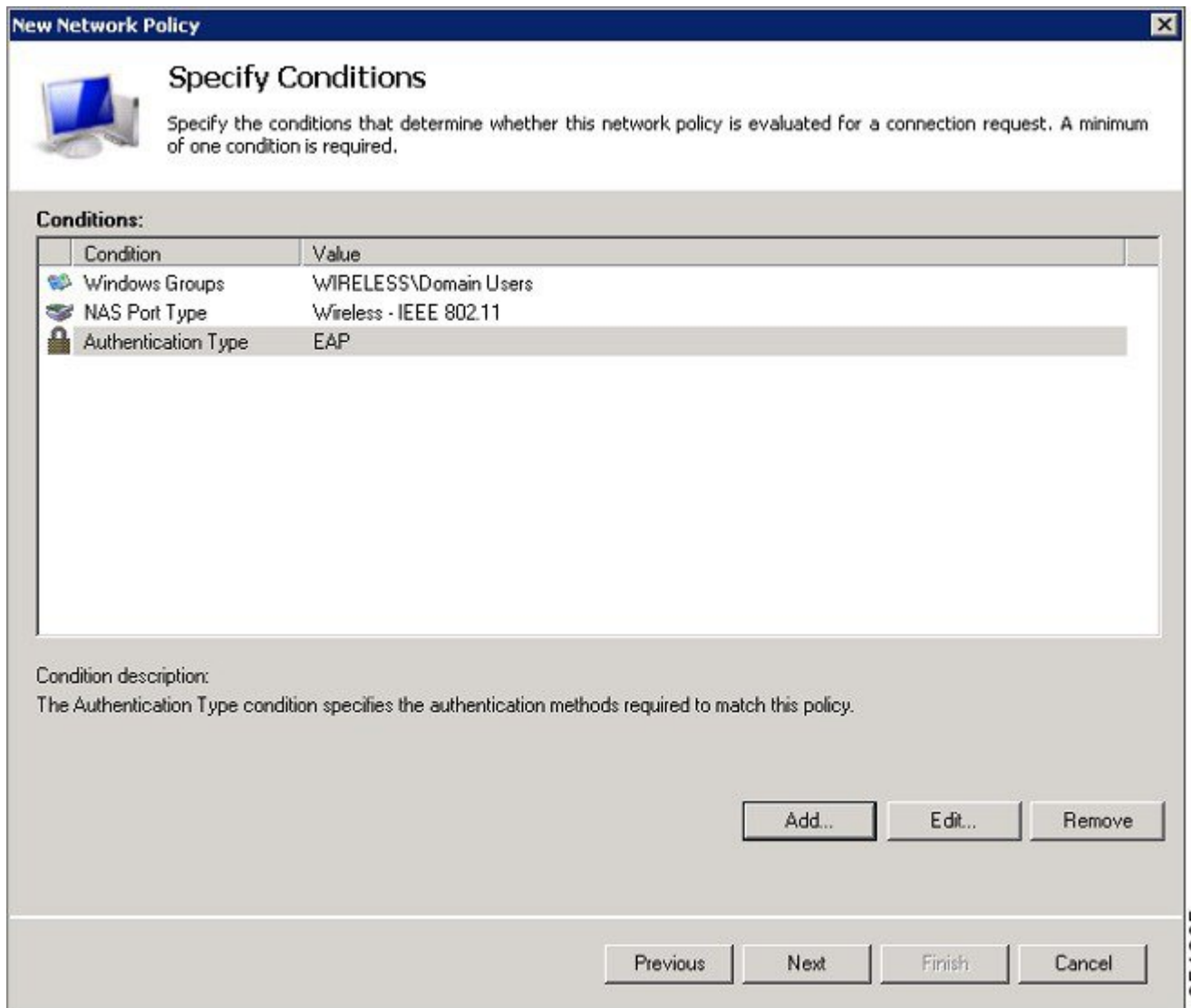
Perform the following task and follow the instructions on the screen to configure the NPS for PEAP-MS-CHAP v2 authentication.

- Step 1** To configure the NPS for PEAP-MS-CHAP v2 authentication, navigate to **Start > Administrative Tools > Network Policy Server**.
- Step 2** Right-click on **NPS (Local)** and choose **Register server in Active Directory**.
- Step 3** Click **OK** and again **OK** on **Network Policy Server** pop-up.
- Step 4** Add the WLC as an Authentication, Authorization, and Accounting (AAA) client on the NPS.
- Step 5** Expand **RADIUS Clients and Servers** folder on **Network Policy Server** window. Right-click on **RADIUS Clients** and choose **New RADIUS Client**.
- Step 6** Enter a name, the management IP address and a shared secret of the WLC on the WLC Properties window. Click **OK** to go back to the **Server Manager** window.
- Note** Enter the same shared secret that is created while configuring the Radius Server in order to configure the WLC.
- Step 7** To create a new Network Policy for the wireless users, expand **Policies** folder, right-click on **Network Policies**, and choose **New** on **Network Policy Server** screen.
- Step 8** Enter a policy name on **Specify Network Policy Name and Connection Type** screen and click **Next**.
- Step 9** To allow only wireless domain users, configure the policy (PEAP in this example) by adding following three conditions and click **Next**.

Table 1:

Condition	Value
Windows Groups	WIRELESS\Domain Users
NAS Port Type	Wireless - IEEE 802.11
Authentication Type	EAP

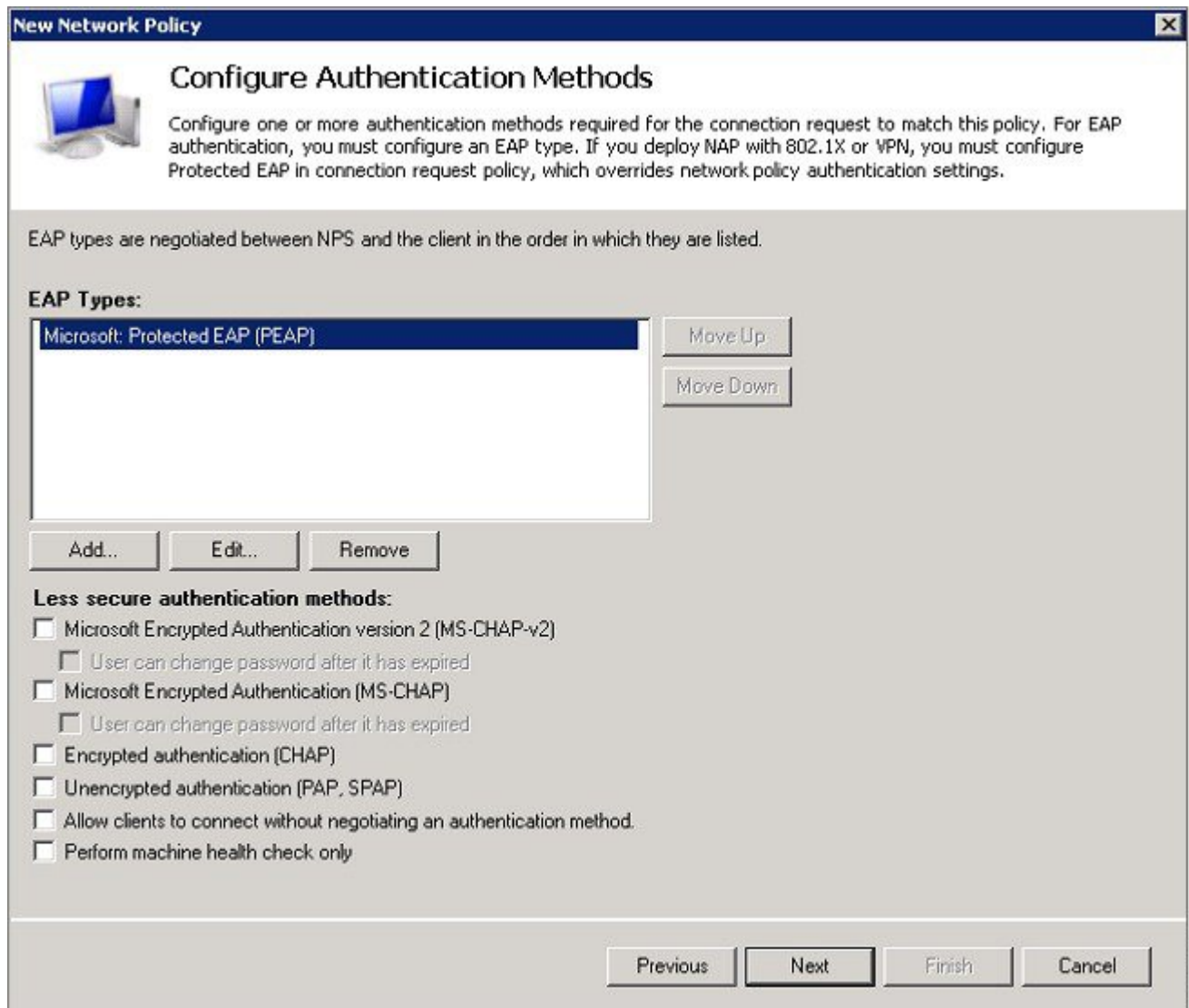
Figure 74: Specifying Conditions



- Step 10** Choose the **Access granted** radio button on **Specify Access Permission** screen in order to grant connection attempts that match this policy and click **Next**.
- Step 11** Disable all of the **Less secure authentication methods** by unchecking all the check boxes in **Configure Authentication Methods** screen.

- Step 12** Click **Add**, then choose the **Microsoft: Protected EAP (PEAP)** as EAP Type on **Configure Authentication Methods** screen, and click **OK** to enable PEAP.

Figure 75: Microsoft Protected EAP as EAP



- Step 13** Select **Microsoft: Protected EAP (PEAP)** and click **Edit**.
- Step 14** Ensure that the previously-created domain controller certificate is selected in the **Certificate issued** field and click **OK** on **Edit Protected EAP Properties** window.
- Step 15** Click **Next** on **Configure Authentication Methods** again click **Next** on **Configure Constraints** window.
- Step 16** Click **Next** on **Configure Settings** and then click **Finish** on **Completing New Network Policy** window.
- Note** Depending on your needs, you may configure **Connection Request Policies** on the NPS in order to allow the PEAP profile or the policy.

Adding Users to the Active Directory

Perform the following task and follow the instructions on the screen to add users to the AD database.

-
- Step 1** Navigate to **Start > Administrative Tools > Active Directory Users and Computers**.
 - Step 2** In the Active Directory Users and Computers console tree, expand the domain.
 - Step 3** Right-click on **Users** and **New**, and then choose **User**.
 - Step 4** In the **New Object - User** dialog box, enter the name of the wireless user. Click **Next**.
 - Step 5** In the **New Object - User** dialog box, enter a password of your choice in the **Password** and **Confirm password** fields.
 - Step 6** Uncheck the **User must change password at next logon** check box on **New Object - User** dialog box and click **Next**.
 - Step 7** Click **Finish** on **New Object - User** dialog box.
 - Step 8** Repeat Steps 2 to 5 in order to create additional user accounts.
-

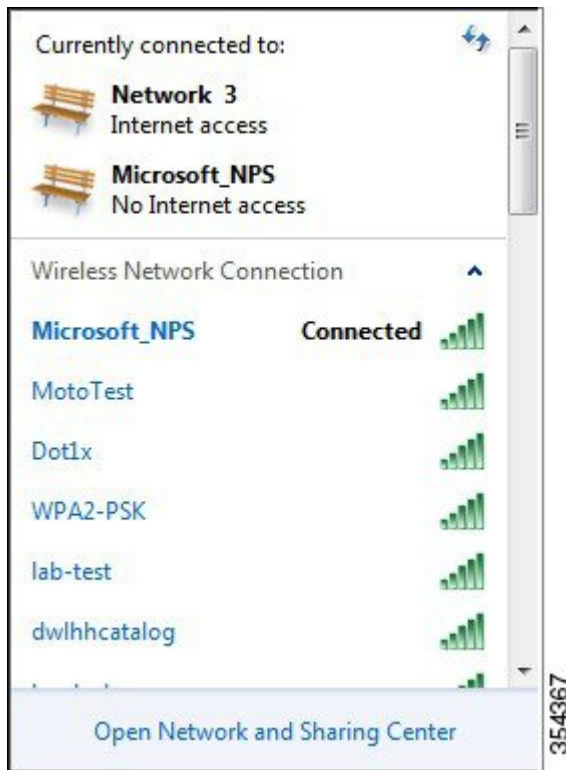
Verifying the PEAP Authentication with Microsoft NPS Configuration

Perform the following task in order to verify your configuration:

-
- Step 1** Search for the Service Set Identification (SSID) on the client machine.

Step 2 Ensure that the client is connected successfully:

Figure 76: Successful Connection



Troubleshooting WLC PEAP Authentication with Microsoft NPS Configuration Issues



Note

Cisco recommends that you use traces in order to troubleshoot wireless issues. Traces are saved in the circular buffer and are not processor intensive.

- Enable these traces in order to obtain the **L2 auth logs**:
 - `set trace group-wireless-secure level debug`
 - `set trace group-wireless-secure filter mac 0017.7C2F.B69A`
- Enable these traces in order to obtain the **dot1X AAA events**:

- **set trace wcm-dot1x aaa level debug**
- **set trace wcm-dot1x aaa filter mac 0017.7C2F.B69A**
- Enable these traces in order to receive the **DHCP events**:
 - **set trace dhcp events level debug**
 - **set trace dhcp events filter mac 0017.7C2F.B69A**
- Enable these traces in order to disable the traces and clear the buffer:
 - **set trace control sys-filtered-traces clear**
 - **set trace wcm-dot1x aaa level default**
 - **set trace wcm-dot1x aaa filter none**
 - **set trace group-wireless-secure level default**
 - **set trace group-wireless-secure filter none**

To view the traces, enter the **show trace sys-filtered-traces** command:

```
[04/23/14 21:27:51.963 IST 1 8151] 0017.7c2f.b69a Adding mobile on LWAPP AP
1caa.076f.9e10 (0)
[04/23/14 21:27:51.963 IST 2 8151] 0017.7c2f.b69a Local Policy: Created MSCB
Just AccessVLAN = 0 and SessionTimeout is 0 and apfMsTimeout is 0

[04/23/14 21:27:51.963 IST 8 8151] 0017.7c2f.b69a Local Policy:Setting local
bridging VLAN name VLAN0020 and VLAN ID 20

[04/23/14 21:27:51.963 IST 9 8151] 0017.7c2f.b69a Applying WLAN ACL policies
to client
[04/23/14 21:27:51.963 IST a 8151] 0017.7c2f.b69a No Interface ACL used for
Wireless client in WCM(NGWC)
[04/23/14 21:27:51.963 IST b 8151] 0017.7c2f.b69a Applying site-specific IPv6
override for station 0017.7c2f.b69a - vapId 8, site 'test',
interface 'VLAN0020'
[04/23/14 21:27:51.963 IST c 8151] 0017.7c2f.b69a Applying local bridging
Interface Policy for station 0017.7c2f.b69a - vlan 20,
interface 'VLAN0020'
[04/23/14 21:27:51.963 IST d 8151] 0017.7c2f.b69a
**** Inside applyLocalProfilingPolicyAction ****

04/23/14 21:27:51.963 IST f 8151] 0017.7c2f.b69a Local Profiling Values :
isValidVlan = 0, vlan = 0, isValidVlanRecdInDelete = 0, isValidSessionTimeout = 0,
sessionTimeout=0, isSessionTORecdInDelete = 0 ProtocolMap = 0 ,
applyPolicyAtRun= 0
[04/23/14 21:27:51.963 IST 10 8151] 0017.7c2f.b69a ipv4ACL = [],
ipv6ACL = [], inQoS = [unknown], outQoS = [unknown]
[04/23/14 21:27:51.963 IST 11 8151] 0017.7c2f.b69a STA - rates (4):
130 132 139 150 0 0 0 0 0 0 0 0 0 0 0 0
[04/23/14 21:27:51.963 IST 12 8151] 0017.7c2f.b69a STA - rates (12):
130 132 139 150 12 18 24 36 48 72 96 108 0 0 0 0
[04/23/14 21:27:51.963 IST 13 8151] 0017.7c2f.b69a Processing RSN IE type 48,
length 20 for mobile 0017.7c2f.b69a
[04/23/14 21:27:51.963 IST 14 8151] 0017.7c2f.b69a Received RSN IE with 0
PMKIDsfrom mobile 0017.7c2f.b69a

[04/23/14 21:27:51.964 IST 1b 8151] 0017.7c2f.b69a Change state to AUTHCHECK
(2) last state START (0)

[04/23/14 21:27:51.964 IST 1c 8151] 0017.7c2f.b69a Change state to 8021X_REQD
(3) last state AUTHCHECK (2)
```

```

[04/23/14 21:27:51.964 IST 25 8151] 0017.7c2f.b69a apfProcessAssocReq
(apf_80211.c:6272) Changing state for mobile 0017.7c2f.b69a on AP
lcaa.076f.9e10 from Associated to Associated

[04/23/14 21:27:51.971 IST 26 8151] 0017.7c2f.b69a 1XA: Initiating
authentication
[04/23/14 21:27:51.971 IST 27 8151] 0017.7c2f.b69a 1XA: Setting reauth
timeout to 1800 seconds
[04/23/14 21:27:51.971 IST 28 8151] 0017.7c2f.b69a 1XK: Set Link Secure: 0

[04/23/14 21:27:51.971 IST 29 8151] 0017.7c2f.b69a 1XA: Allocated uid 40
[04/23/14 21:27:51.971 IST 2a 8151] 0017.7c2f.b69a 1XA: Calling Auth Mgr
to authenticate client 4975000000003e uid 40
[04/23/14 21:27:51.971 IST 2b 8151] 0017.7c2f.b69a 1XA: Session Start from
wireless client

[04/23/14 21:27:51.971 IST 2c 8151] 0017.7c2f.b69a Session Manager Call Client
4975000000003e, uid 40, capwap id 7ae8c000000013, Flag 0, Audit-Session ID
0a6987b25357e2ff00000028, method list Microsoft_NPS, policy name (null)

[04/23/14 21:27:51.971 IST 2d 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
[0017.7c2f.b69a, Ca3] Session start request from Client[1] for 0017.7c2f.b69a
(method: Dot1X, method list: Microsoft_NPS, aaa id: 0x00000028), policy
[04/23/14 21:27:51.971 IST 2e 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
[0017.7c2f.b69a, Ca3] - client iif id: 4975000000003E, session ID:
0a6987b25357e2ff00000028 for 0017.7c2f.b69a

[04/23/14 21:27:51.972 IST 43 284] ACCESS-METHOD-DOT1X-DEB:
[0017.7c2f.b69a, Ca3] Posting !EAP_RESTART on Client 0x22000025
[04/23/14 21:27:51.972 IST 44 284] ACCESS-METHOD-DOT1X-DEB:
[0017.7c2f.b69a, Ca3] 0x22000025:enter connecting state
[04/23/14 21:27:51.972 IST 45 284] ACCESS-METHOD-DOT1X-DEB:
[0017.7c2f.b69a, Ca3] 0x22000025: restart connecting
[04/23/14 21:27:51.972 IST 46 284] ACCESS-METHOD-DOT1X-DEB:
[0017.7c2f.b69a, Ca3] Posting RX REQ on Client 0x22000025
[04/23/14 21:27:51.972 IST 47 284] ACCESS-METHOD-DOT1X-DEB:
[0017.7c2f.b69a, Ca3] 0x22000025: authenticating state entered
[04/23/14 21:27:51.972 IST 48 284] ACCESS-METHOD-DOT1X-DEB:
[0017.7c2f.b69a, Ca3] 0x22000025:connecting authenticating action
[04/23/14 21:27:51.972 IST 49 291] ACCESS-METHOD-DOT1X-DEB:
[0017.7c2f.b69a, Ca3] Posting AUTH_START for 0x22000025
[04/23/14 21:27:51.972 IST 4a 291] ACCESS-METHOD-DOT1X-DEB:
[0017.7c2f.b69a, Ca3] 0x22000025:entering request state
[04/23/14 21:27:51.972 IST 4b 291] ACCESS-METHOD-DOT1X-NOTF:
[0017.7c2f.b69a, Ca3] Sending EAPOL packet
[04/23/14 21:27:51.972 IST 4c 291] ACCESS-METHOD-DOT1X-INFO:
[0017.7c2f.b69a, Ca3] Platform changed src mac of EAPOL packet
[04/23/14 21:27:51.972 IST 4d 291] ACCESS-METHOD-DOT1X-NOTF:
[0017.7c2f.b69a, Ca3] Sending out EAPOL packet
[04/23/14 21:27:51.972 IST 4e 291] ACCESS-METHOD-DOT1X-INFO:
[0017.7c2f.b69a, Ca3] EAPOL packet sent to client 0x22000025

[04/23/14 21:27:52.112 IST 7d 211] Parsed CLID MAC Address = 0:23:124:47:182:154
[04/23/14 21:27:52.112 IST 7e 211] AAA SRV(00000000): process authen req
[04/23/14 21:27:52.112 IST 7f 211] AAA SRV(00000000): Authen method=SERVER_GROUP
Microsoft NPS
[04/23/14 21:27:52.112 IST 80 211] AAA SRV(00000000): Selecting SG = DIAMETER
[04/23/14 21:27:52.113 IST 81 186] ACCESS-METHOD-DOT1X-INFO:
[0017.7c2f.b69a, Ca3] Queuing an EAPOL pkt on Authenticator Q
[04/23/14 21:27:52.113 IST 82 291] ACCESS-METHOD-DOT1X-DEB:
[0017.7c2f.b69a, Ca3] Posting EAPOL EAP for 0x22000025
[04/23/14 21:27:52.278 IST 83 220] AAA SRV(00000000): protocol reply
GET CHALLENGE RESPONSE for Authentication
[04/23/14 21:27:52.278 IST 84 220] AAA SRV(00000000): Return Authentication
status=GET_CHALLENGE_RESPONSE
[04/23/14 21:27:52.278 IST 85 291] ACCESS-METHOD-DOT1X-DEB:[0017.7c2f.b69a,Ca3]
Posting EAP_REQ for 0x22000025

```

The following codeblock shows the rest of the EAP output:

```

[04/23/14 21:27:54.690 IST 12b 211] AAA SRV(00000000): process authen req
[04/23/14 21:27:54.690 IST 12c 211] AAA SRV(00000000): Authen

```

```

method=SERVER GROUP Microsoft_NPS
[04/23/14 21:27:54.690 IST 12d 211] AAA SRV(00000000): Selecting SG =
DIAMETER
[04/23/14 21:27:54.694 IST 12e 220] AAA SRV(00000000): protocol reply PASS
for Authentication
[04/23/14 21:27:54.694 IST 12f 220] AAA SRV(00000000): Return Authentication
status=PASS
[04/23/14 21:27:54.694 IST 130 189] ACCESS-METHOD-DOT1X-INFO:
[0017.7c2f.b69a, Ca3] Received an EAP Success

[04/23/14 21:27:54.695 IST 186 8151] 0017.7c2f.b69a Starting key exchange with
mobile - data forwarding is disabled
[04/23/14 21:27:54.695 IST 187 8151] 0017.7c2f.b69a 1XA: Sending EAPOL message
to mobile, WLAN=8 AP WLAN=8
[04/23/14 21:27:54.706 IST 188 8151] 0017.7c2f.b69a 1XA: Received 802.11 EAPOL
message (len 121) from mobile
[04/23/14 21:27:54.706 IST 189 8151] 0017.7c2f.b69a 1XA: Received EAPOL-Key
from mobile
[04/23/14 21:27:54.706 IST 18a 8151] 0017.7c2f.b69a 1XK: Received EAPOL-key in
PTK_START state (msg 2) from mobile
[04/23/14 21:27:54.706 IST 18b 8151] 0017.7c2f.b69a 1XK: Stopping retransmission
timer
[04/23/14 21:27:54.706 IST 18c 8151] 0017.7c2f.b69a 1XA: Sending EAPOL message
to mobile, WLAN=8 AP WLAN=8
[04/23/14 21:27:54.717 IST 18d 8151] 0017.7c2f.b69a 1XA: Received 802.11 EAPOL
message (len 99) from mobile
[04/23/14 21:27:54.717 IST 18e 8151] 0017.7c2f.b69a 1XA: Received EAPOL-Key
from mobile
[04/23/14 21:27:54.717 IST 18f 8151] 0017.7c2f.b69a 1XK: Received EAPOL-key in
PTKINITNEGOTIATING state (msg 4) from mobile
[04/23/14 21:27:54.717 IST 190 8151] 0017.7c2f.b69a 1XK: Set Link Secure: 1

[04/23/14 21:27:54.717 IST 191 8151] 0017.7c2f.b69a 1XK: Key exchange complete
- updating PEM
[04/23/14 21:27:54.717 IST 192 8151] 0017.7c2f.b69a apfMslxStateInc
[04/23/14 21:27:54.717 IST 193 8151] 0017.7c2f.b69a Change state to
L2AUTHCOMPLETE (4) last state 8021X_REQD (3)

[04/23/14 21:27:58.277 IST 1df 269] DHCPD: Sending notification of DISCOVER:
[04/23/14 21:27:58.277 IST 1e0 269] DHCPD: Sending notification of DISCOVER:
[04/23/14 21:28:05.279 IST 1e1 269] DHCPD: Adding binding to hash tree
[04/23/14 21:28:05.279 IST 1e2 269] DHCPD: DHCPPOFFER notify setup address
20.20.20.5 mask 255.255.255.0

[04/23/14 21:28:05.306 IST 1f4 8151] 0017.7c2f.b69a Change state to RUN (20)
last state DHCP_REQD (7)

```



QoS on Converged Access Controllers and Lightweight Access Points

This document describes how to configure Quality of Service (QoS) on a Cisco converged access controllers (CACs) with Lightweight Access Points (LAPs) and a Cisco Catalyst 3850 Series Switch.

- [Prerequisites, page 227](#)
- [Information about QoS, page 228](#)
- [Default Hardcoded Policies for QoS, page 230](#)
- [Configuring QoS Manually, page 234](#)
- [Verifying Configuration for QoS, page 242](#)
- [Troubleshooting QoS Configuration Issues, page 248](#)

Prerequisites

- We recommend that you have basic knowledge on the following:
 - Configure LAPs and Cisco converged access controllers.
 - Configure basic routing and QoS in a wired network.
- Ensure the Wireless Controller Module (WCM) function of the Cisco Catalyst 3850 Series Switch for basic operation is configured.
- Ensure the LAPs are registered to the WCM.

Supported Platforms and Releases

The information in this document is based on the following software and hardware versions:

- Cisco Catalyst 3850 Series Switch running on Cisco IOS XE Software Release Denali-16.1.1
- Cisco 3600 Series LAPs

**Note**

The information in this document refers to the devices in a customized lab environment. The devices have default configuration. If you are on a live network, you must understand the potential impact of all the commands.

Information about QoS

Cisco QoS refers to the ability of the network to provide better or special service to a set of users or applications to the adverse of other users or applications.

Cisco QoS provides enhanced and reliable network with the following services:

- Supports dedicated bandwidth for critical users and applications.
- Controls the jitter and latency that is required by real-time traffic.
- Manages and minimizes network congestion.
- Shapes network traffic in order to smooth the flow of traffic.
- Sets network traffic priorities.

In the past, WLANs were mainly used to transport data application traffic with low bandwidth requirements. The WLANs got expanded into vertical such as, retail, finance, education, and enterprise environments. WLANs are now used to transport high-bandwidth data applications in conjunction with time-sensitive and multimedia applications. The use of WLANs to transport high-bandwidth, time-sensitive, and multimedia applications led to the necessity for wireless QoS.

The IEEE 802.11e working group within the IEEE 802.11 standards committee has completed the standard definition and the Wi-Fi Alliance has created the Wi-Fi Multimedia (WMM) certification. However, the adoption of the 802.11e standard is still limited. Even though most devices are WMM-certified, because WMM certification is needed for 802.11n and 802.11ac certification, many wireless devices do not assign different QoS levels to packets sent to the Data Link Layer. Hence, most of the wireless devices send their traffic with no QoS marking and no relative prioritization. However, most 802.11 Voice over Wireless LAN (VoWLAN) IP phones do mark and prioritize their voice traffic.

This document focuses on QoS configuration for VoWLAN IP phones and on video-capable wi-fi devices that mark their voice traffic.

**Note**

Cisco QoS configuration for devices that do not perform internal marking is outside the scope of this document.

The 802.11e amendment defines eight user priority (UP) levels, grouped two by two into four QoS levels (access categories):

- Platinum and Voice (UP 7 and 6) - Ensures a high quality of service for voice over wireless.
- Gold and Video (UP 5 and 4) - Supports high-quality video applications.
- Silver and Best Effort (UP 3 and 0) - Supports normal bandwidth for clients. This is the default setting.
- Bronze and background (UP 2 and 1) - Provides the lowest bandwidth for guest services.

Platinum is commonly used for VoIP clients and Gold is for video clients.

This document provides a configuration example that illustrates how to configure QoS on controllers and communicate with a wired network that is configured with QoS for VoWLAN and video clients.

Configuring Wireless Network for QoS with MQC

The converged access solution uses the Modular QoS (MQC) command-line interface (CLI). Refer to the QoS Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) for additional information on the use of MQC in QoS configuration on the Cisco Catalyst 3850 Series Switch.

Configuration of QoS with MQC on converged access controllers depends on four elements:

- **Class-maps.** Class-maps are used in order to recognize traffic of interest. Class-maps use various techniques (such as existing QoS marking, access-lists, or VLANs) to identify traffic of interest.
- **Policy-maps.** Policy-maps are used in order to determine what QoS settings should be applied to the traffic of interest. Policy-maps call class-maps and apply various QoS settings (such as specific marking, priority levels, bandwidth allocation, and so on) to each class.
- **Service-policies.** Service-policies are used to apply policy-maps to strategic points of your network. In the converged access solution, service-policies can be applied to users, Service Set Identifiers (SSIDs), AP radios, and ports. Port, SSID, and client policies can be configured by the user. Radio policies are controlled by WCM. Wireless QoS policies for port, SSID, client, and radio are applied in the downstream direction when traffic is flowing from the switch or controller to wireless clients.
- **Table-maps.** Table-maps are used in order to examine incoming QoS marking and to decide outgoing QoS markings. Table-maps are positioned in policy-maps applied to SSIDs. Table-maps can be used to keep (copy) or change the marking. Table-maps can also be used to create a mapping between wired and wireless marking. Wired marking uses DSCP (L3 QoS) or 802.1p (L2 QoS). Wireless marking uses UP. Table-maps are commonly used to determine what DSCP marking should be used for each UP of interest and what UP should be used for each DSCP value of interest. Table-maps are fundamental to converged access QoS because there is no direct translation between DSCP and UP values. However, DSCP to UP table-maps also allow the *copy* instruction. In this case, the converged access solution uses the Cisco Architecture for Voice, Video, and Integrated Data (AVVID) mapping table in order to determine the DSCP to UP or UP to DSCP translation.

Label Index	Key Field	Incoming Value	Outer DSCP	CoS	UP
0	N.A.	Not checked	0	0	0
1-10	DSCP	0-7	0-7	0	0
11-18	DSCP	8-15	8-15	1	2
19-26	DSCP	16-23	16-23	2	3
27-34	DSCP	24-31	24-31	3	4
35-46	DSCP	32-39	32-39	4	5
47-48	DSCP	40-47	40-47	5	6
49-63	DSCP	48-55	48-55	6	7
64	DSCP	56-63	56-63	7	7
65	CoS	0	0	0	0
66	CoS	1	8	1	2
67	CoS	2	16	2	3
68	CoS	3	24	3	4
69	CoS	4	32	4	5
70	CoS	5	40	5	6
71	CoS	6	48	6	7
72	CoS	7	56	7	7
73	UP	0	0	0	0
74	UP	1	8	1	1
75	UP	2	16	1	2
76	UP	3	24	2	3
77	UP	4	34	3	4
78	UP	5	34	4	5
79	UP	6	46	5	6
80	UP	7	46	7	7

Default Hardcoded Policies for QoS

Converged access controllers embark hardcoded QoS policy profiles that can be applied to WLANs. The QoS policy profiles apply the metal policies (platinum, gold, and so on) that are familiar to administrators of Cisco Unified Wireless Networks (CUWN) controllers.

If your objective is not to create policies that assign specific bandwidth to voice traffic but to ensure that voice traffic receives the proper QoS marking, you can use the hardcoded policies. The hardcoded policies can be applied to the WLAN and can be different in the upstream and the downstream directions.

Platinum

The hardcoded policy for voice is known as platinum. The name cannot be changed.

The following commands describe the downstream policy of the platinum QoS level:

```
Policy-map platinum
Class class-default
  set dscp dscp table plat-dscp2dscp
  set wlan user-priority dscp table plat-dscp2up
Table-map plat-dscp2dscp
  from 45 to 45
  from 46 to 46
  from 47 to 47
  default copy
Table-map plat-dscp2up
  from 34 to 4
  from 46 to 6
  default copy
```

The following commands describe the upstream policy of the Platinum QoS level:

```
Policy-map platinum-up
Class class-default
  set dscp wlan user-priority table plat-up2dscp

Table-map plat-up2dscp
  from 4 to 34
  from 5 to 34
  from 6 to 46
  from 7 to 8
  default copy
```

Gold

The hardcoded policy for video is known as gold. The name cannot be changed.

The following commands describe the downstream policy of the gold QoS level:

```
Policy Map gold
Class class-default
  set dscp dscp table gold-dscp2dscp
  set wlan user-priority dscp table gold-dscp2u

Table Map gold-dscp2dscp
  from 45 to 34
  from 46 to 34
  from 47 to 34
  default copy

Table Map gold-dscp2up
  from 45 to 4
  from 46 to 4
  from 47 to 4
  default copy
```

The following commands describe the upstream policy of the gold QoS level:

```
Policy Map gold-up
Class class-default
  set dscp wlan user-priority table gold-up2dscp

Table Map gold-up2dscp
  from 6 to 34
```

```

from 7 to 34
default copy

```

Silver

The hardcoded policy for best effort is known as silver. The name cannot be changed.

The following commands describe the downstream policy of the silver QoS level:

```

Policy Map silver
  Class class-default
    set dscp dscp table silver-dscp2dscp
    set wlan user-priority dscp table silver-dscp2up

Table Map silver-dscp2dscp
  from 34 to 0
  from 45 to 0
  from 46 to 0
  from 47 to 0
  default copy

Table Map silver-dscp2up
  from 34 to 0
  from 45 to 0
  from 46 to 0
  from 47 to 0
  default copy

```

The following commands describe the upstream policy of the silver QoS level:

```

Policy Map silver-up
  Class class-default
    set dscp wlan user-priority table silver-up2dscp

Table Map silver-up2dscp
  from 4 to 0
  from 5 to 0
  from 6 to 0
  from 7 to 0
  default copy

```

Bronze

The hardcoded policy for background traffic is known as bronze. The name cannot be changed.

The following commands describe the downstream policy of the bronze QoS level:

```

Policy Map bronze
  Class class-default
    set dscp dscp table bronze-dscp2dscp
    set wlan user-priority dscp table bronze-dscp2up

Table Map bronze-dscp2dscp
  from 0 to 8
  from 34 to 8
  from 45 to 8
  from 46 to 8
  from 47 to 8
  default copy

Table Map bronze-dscp2up
  from 0 to 1
  from 34 to 1
  from 45 to 1
  from 46 to 1
  from 47 to 1
  default copy

```

The following commands describe the upstream policy of the bronze QoS level:

```

Policy Map bronze-up
  Class class-default
    set dscp wlan user-priority table bronze-up2dscp

```

```
Table Map bronze-up2dscp
  from 0 to 8
  from 1 to 8
  from 4 to 8
  from 5 to 8
  from 6 to 8
  from 7 to 8
  default copy
```



Note Once you have decided which table-map best matches the target traffic for a given SSID, you can apply the matching policy to your WLAN.

In the following example, one policy is applied in the downstream direction (output, from the AP to the wireless client), and one policy is applied on the upstream direction (input, from the wireless client, through the AP, to the controller):

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
Device(config)# wlan test1
Device(config-wlan)# service-policy output platinum
Device(config-wlan)# service-policy input platinum-up
Device(config-wlan)# end
```

To check the WLAN configuration, use the following commands. The commands also verify the policy applied to your WLAN.

```
Device# show wlan name test1
WLAN Profile Name      : test1
=====
Identifier              : 1
Network Name (SSID)    : test1
Status                  : Disabled
Broadcast SSID         : Enabled
Maximum number of Associated Clients : 0
AAA Policy Override    : Disabled
Network Admission Control
  NAC-State             : Disabled
Number of Active Clients : 0
Exclusion list Timeout  : 60
Session Timeout        : 1800 seconds
CHD per WLAN           : Enabled
Webauth DHCP exclusion : Disabled
Interface               : default
Interface Status       : Up
Multicast Interface    : Unconfigured
WLAN IPv4 ACL           : Unconfigured
WLAN IPv6 ACL           : Unconfigured
DHCP Server             : Default
DHCP Address Assignment Required : Disabled
DHCP Option 82         : Disabled
DHCP Option 82 Format   : AP-Mac
DHCP Option 82 ASCII Mode : Disabled
DHCP Option 82 Rid Mode : Disabled
```

QoS Service Policy - Input

```
Policy Name      : platinum-up
Policy State     : Validation Pending
```

QoS Service Policy - Output

```
Policy Name      : platinum
Policy State     : Validation Pending
```

```
QoS Client Service Policy
  Input Policy Name      : unknown
  Output Policy Name     : unknown
WMM                      : Allowed
Channel Scan Defer Priority:
  Priority (default)     : 4
```

```

Priority (default) : 5
Priority (default) : 6
Scan Defer Time (msecs) : 100
Media Stream Multicast-direct : Disabled
CCX - AironetIe Support : Enabled
CCX - Gratuitous Probe Response (GPR) : Disabled
CCX - Diagnostics Channel Capability : Disabled
Dot11-Phone Mode (7920) : Invalid
Wired Protocol : None
Peer-to-Peer Blocking Action : Disabled
Radio Policy : All
DTIM period for 802.11a radio : 1
DTIM period for 802.11b radio : 1
Local EAP Authentication : Disabled
Mac Filter Authorization list name : Disabled
Accounting list name : Disabled
802.1x authentication list name : Disabled
Security
  802.11 Authentication : Open System
  Static WEP Keys : Disabled
  802.1X : Disabled
  Wi-Fi Protected Access (WPA/WPA2) : Enabled
    WPA (SSN IE) : Disabled
    WPA2 (RSN IE) : Enabled
      TKIP Cipher : Disabled
      AES Cipher : Enabled
    Auth Key Management
      802.1x : Enabled
      PSK : Disabled
      CCKM : Disabled
  CKIP : Disabled
  IP Security : Disabled
  IP Security Passthru : Disabled
  L2TP : Disabled
  Web Based Authentication : Disabled
  Conditional Web Redirect : Disabled
  Splash-Page Web Redirect : Disabled
  Auto Anchor : Disabled
  Sticky Anchoring : Enabled
  Cranite Passthru : Disabled
  Fortress Passthru : Disabled
  PPTP : Disabled
  Infrastructure MFP protection : Enabled
  Client MFP : Optional
  Webauth On-mac-filter Failure : Disabled
  Webauth Authentication List Name : Disabled
  Webauth Parameter Map : Disabled
  Tkip MIC Countermeasure Hold-down Timer : 60
Call Snooping : Disabled
Passive Client : Disabled
Non Cisco WGB : Disabled
Band Select : Disabled
Load Balancing : Disabled
IP Source Guard : Disabled

```

Configuring QoS Manually

The hardcoded policies apply default QoS marking but do not apply bandwidth allocation. The hardcoded policies also assume that your traffic is already marked.

Perform the following steps to use a combination of policies to identify and mark voice and video traffic appropriately, to set bandwidth allocation in the downstream and upstream directions, and to use call admission control in order to limit the number of calls initiated from the wireless cell in a complex environment:

Identifying and Marking of Voice Traffic

The first step is to recognize voice and video traffic. Voice traffic can be classified into the following categories:

- Voice flow, which carries the audio part of the communication.
- Voice signaling, which carries the statistical information exchanged between voice endpoints.

The voice flow uses Real-time Transport Protocol (RTP) and User Datagram Protocol (UDP) destination ports in the range of 16384 - 32767. This is a projected range and the actual ports are usually narrower and depends on the implementation.

There are several voice signaling protocols. The configuration example that is described uses Jabber. Jabber uses the following TCP ports for connection and directory:

- TCP 80 (HTTP)
- 143 (Internet Message Access Protocol [IMAP])
- 443 (HTTPS)
- 993 (IMAP) for services such as Cisco Unified MeetingPlace or Cisco WebEx for meetings and Cisco Unity or Cisco Unity Connection for voicemail features.
- TCP 389 or 636 (Lightweight Directory Access Protocol [LDAP] server for contact searches.)
- FTP (1080)
- TFTP (UDP 69) for file transfer (such as configuration files) from peers or from server.

These services may not need a specific prioritization. Jabber uses the Session Initiation Protocol (SIP) (UDP or TCP 5060 and 5061) for voice signaling.

Video traffic uses different ports and protocols depending on your implementation.

The configuration example described uses a Tandberg PrecisionHD 720p camera for video conferences.

The Tandberg PrecisionHD 720p camera can use several codecs. The bandwidth consumed depends on the codec selected:

- C20, C40, and C60 codecs use H.323 or SIP and can consume up to 6 Mbps in point-to-point connections.
- The C90 codec uses these same protocols and can consume up to 10 Mbps in multi-site communications.

Tandberg implementation of H.323 uses UDP 970 for streaming video, UDP 971 for video signaling, UDP 972 for streaming audio, and UDP 973 for audio signaling. Tandberg cameras also use other ports, such as:

- UDP 161
- UDP 962 (Simple Network Management Protocol [SNMP])
- TCP 963 (netlog), TCP 964 (FTP)
- TCP 965 (virtual network computing [VNC])
- UDP 974 (Session Announcement Protocol [SAP])

**Note**

The additional ports may not need a specific prioritization.

A common way to identify traffic is to create class-maps that target the traffic of interest. Each class-map can point to an access-list that targets any traffic that uses the voice and the video ports. To create class-maps, use the following commands:

```
ip access-list extended JabberVOIP
permit udp any any range 16384 32767
ip access-list extended JabberSIGNALING
permit tcp any any range 5060 5061
permit udp any any range 5060 5061
ip access-list extended H323Videostream
permit udp any any eq 970
ip access-list extended H323Audiostream
permit udp any any eq 972
ip access-list extended H323VideoSignaling
permit udp any any eq 971
ip access-list extended H323AudioSignaling
permit udp any any eq 973
```

You can then create one class-map for each type of traffic. Each class-map points to the relevant access-list. To create one class-map for each type of traffic, use the following commands:

```
class-map RTPaudio
match access-group name JabberVOIP
match access-group name H323Audiostream
class-map H323realtimevideo
match access-group name H323Videostream
class-map signaling
match access-group name JabberSIGNALING
match access-group name H323VideoSignaling
match access-group name H323AudioSignaling
```

When voice traffic and video traffic have been identified through class-maps, ensure that the traffic is marked properly. The marking can be done at the WLAN level through the table-maps and also through client policy-maps.

Table-maps examine the QoS marking of incoming traffic and determine what the outgoing QoS marking should be. Thus, Table-maps are useful when incoming traffic already has QoS marking. Table-maps are used exclusively at the SSID level.

By contrast, policy-maps can target traffic identified by class-maps and are better adapted to untagged traffic of interest. The configuration example assumes that traffic from the wired side has already been marked properly before it enters the Cisco Catalyst 3850 Series Switch. If this is not the case, you can use a policy-map and apply it at the SSID level as a client policy. Because traffic from wireless clients may not have been marked, you need to mark voice and video traffic properly by ensuring the following:

- Real time voice should be marked with DSCP 46 (Expedited Forwarding [EF]).
- Video should be marked DSCP 34 (Assured Forwarding Class 41 [AF41]).
- Signaling for voice and video should be marked DSCP 24 (Class Selector Service value 3 [CS3]).

To apply these markings, create a policy-map that calls each of these classes and that marks the equivalent traffic. To create a policy-map, use the following commands:

```
policy-map taggingPolicy
class RTPaudio
set dscp ef

class H323realtimevideo
set dscp af41
```



```
class signaling
set dscp cs3
```

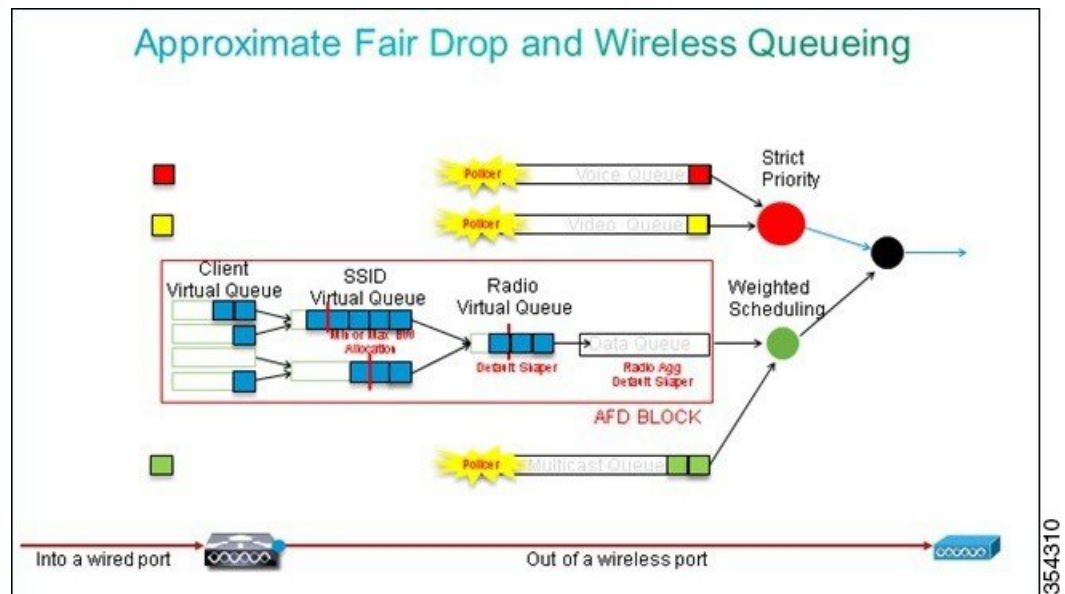
Bandwidth and Priority Management at Port Level

The next step is to determine a QoS policy for ports that come and go to APs. This step primarily applies to Cisco Catalyst 3850 Series Switches.

Cisco Catalyst 3850 Series Switches ports carry voice and video traffic that goes to or comes from wireless clients and APs. QoS configuration in this context matches the following requirements:

- 1 Allocate bandwidth.** You may want to decide how much bandwidth is allocated for each type of traffic. The bandwidth allocation can also be done at the SSID level. Set the port bandwidth allocation to define how much bandwidth can be received by each AP that serves the target SSID. The bandwidth has to be set for all SSIDs on the target AP. For a simplified configuration which has only one SSID and one AP, the port bandwidth allocation for voice and video is the same as the global bandwidth allocation for voice and video at the SSID level. Each traffic type is allocated 6 Mbps and is policed so that the allocated bandwidth is not exceeded.
- 2 Prioritize traffic.** The port has four queues. The first two queues are prioritized and reserved for real time traffic - typically voice and video, respectively. The fourth queue is reserved for non-real-time multicast traffic, and the third queue contains all other traffic. With converged access queuing logic, traffic for each client is assigned to a virtual queue, where QoS can be configured. The result of the client QoS policy is injected into the SSID virtual queue, where QoS can also be configured. Since several SSIDs can exist on a given AP radio, the result of each SSID that is present on an AP radio is injected into the AP radio virtual queue, where traffic is shaped based on the radio capacity. Traffic can be delayed or dropped at any of these stages by use of a QoS mechanism called Approximate Fair Drop (AFD). The result of this policy is then sent to the AP port (called the wireless port), where priority is given to the first two queues (up to a configurable amount of bandwidth), and then to the third and fourth queues.

Figure 77: Appropriate Fair Drop and Wireless Queuing



**Note**

You cannot use class-maps that target traffic based on access control lists (ACLs). Policies applied at the port level can target traffic based on class-maps, but these class-maps should target traffic identified by its QoS value. Once you have identified traffic based on ACLs and marked this traffic properly at the client SSID level, it would be redundant to perform a second inspection of that same traffic at the port level. When traffic reaches the port that goes to the AP, it is already marked properly.

In the following example, the general class-maps created for the SSID policy is re-used and voice RTP traffic and video real time traffic are directly targeted:

```
Class-map allvoice
match dscp ef
Class-map videoandsignaling
Match dscp af41
match dscp cs3
```

Once you have identified the traffic of interest, you can decide which policy to apply. To apply the policy, use the following commands. The default policy (called `parent_port`) is applied automatically at each port when an AP is detected.

The following example displays the default policy.

```
policy-map parent_port
class class-default
shape average 1000000000
service-policy port_child_policy
```

**Note**

It is not recommended to change the default policy.

Because the default `parent_port` policy calls the `port_child_policy`, one option is to edit the `port_child_policy` (it is not recommended to change the name). The child policy determines what traffic should go in each queue and how much bandwidth should be allocated. The first queue has the highest priority, the second queue has the second highest priority, and so on. The first two queues are reserved for real time traffic. The fourth queue is used for non-real-time multicast traffic. The third queue contains all other traffic.

In the following example, voice traffic is allocated to the first queue and video traffic to second queue and the bandwidth is allocated to each queue and to all other traffic:

In the policy mapped defined below, the priority statement associated to the voice and the 'videoandsignaling' classes allows you to assign the traffic to the relevant priority queue. However, the police rate percent statements apply only to multicast and not unicast traffic.

You need not apply the `port_child_policy` policy at the port level because it is applied automatically as soon as an AP is detected.

```
Policy-map port_child_policy
Class allvoice
  Priority level 1
  police rate percent 10
  conform-action transmit
  exceed-action drop
class videoandsignaling
  priority level 2
  police rate percent 20
  conform-action transmit
  exceed-action drop
class non-client-nrt-class
  bandwidth remaining ratio 7
class class-default
  bandwidth remaining ratio 63
```

Bandwidth and Priority Management at SSID Level

The next step is to verify the QoS policy at the SSID level. The configuration assumes that voice and video traffic are identified through the use of class-map and access-lists and is tagged properly. However, some incoming traffic that is not targeted by the access-list may not display its QoS marking. In such a case, you can decide if this traffic should be marked with a default value or left untagged. The same logic goes for traffic already marked but not targeted by the class-maps. Use the **default copy** command in a table-map to ensure that unmarked traffic is left unmarked and the tagged traffic keeps the tag and it is not remarked.

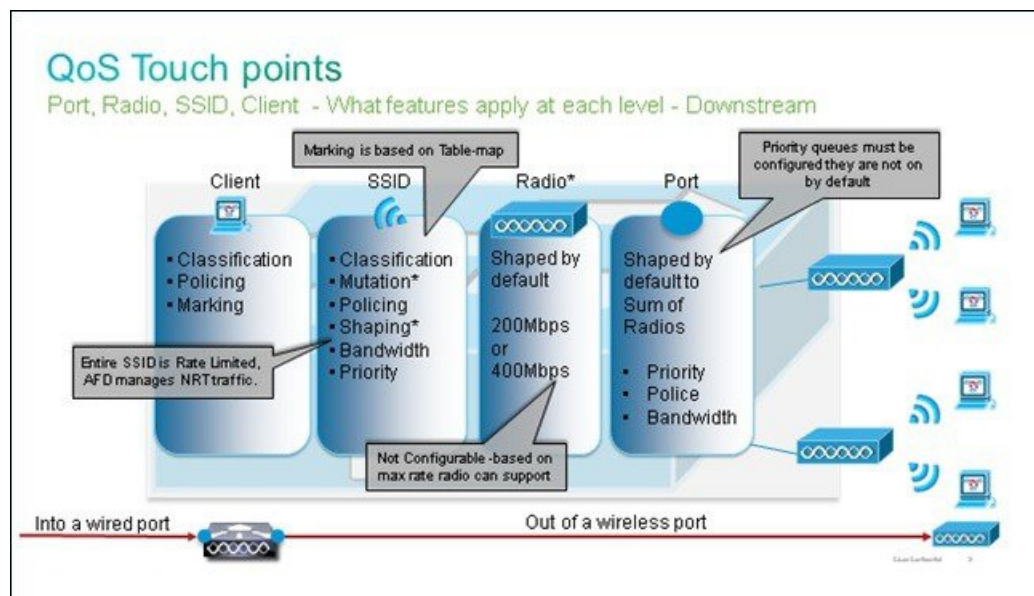
Table-maps decide the outgoing DSCP value but are also used to create an 802.11 frame to decide the frame UP value.

In the following example, incoming traffic that displays voice QoS level (DSCP 46) maintains its DSCP value and the value is mapped to the equivalent 802.11 marking (UP 6). Incoming traffic that displays video QoS level (DSCP 34) maintains its DSCP value and the value is mapped to the equivalent 802.11 marking (UP 5). Similarly, traffic marked DSCP 24 may be voice signaling and the DSCP value should be maintained and translated into the 802.11 UP 3:

```
Table-map dscp2dscp
Default copy
Table-map dscp2up
Map from 46 to 6
Map from 24 to 3
Map from 34 to 5
Default copy
```

Marking could also be done at the incoming wired level. The following figure shows what QoS actions can be taken as traffic transits from wired to wireless:

Figure 78: QoS Touch Points



The configuration example described focuses on the wireless aspect of QoS configuration and marks traffic at wireless client level. Once the marking portion has been completed, you need to allocate bandwidth. Here, 6 Mbps of bandwidth is allocated to voice traffic flows. (While this is the overall bandwidth allocation for

voice, each call would consume less - for example, 128 kbps.) The 6 Mbps bandwidth is allocated with the **police** command to reserve the bandwidth and to drop traffic in excess.

The video traffic is also allocated 6 Mbps and it is policed.

**Note**

The configuration assumes that there is only one video flow.

The signaling part of the video and voice traffic also needs to be allocated bandwidth. There are two possible strategies:

- Use the **shape average** command, which allows traffic in excess to be buffered and sent later. This logic is not efficient for the voice or video flow because the voice and video flows require consistent delay and jitter; however, it can be efficient for signaling because signaling can be slightly delayed without an effect on call quality. In the converged access solution, **shape** commands do not accept buckets configurations, which determine how much traffic in excess of the allocated bandwidth can be buffered. Therefore, a second command, **queue-buffers ratio 0**, must be added in order to specify that the bucket size is 0. If you include signaling in the rest of the traffic and use **shape** commands, signaling traffic might be dropped in times of high congestion. This might, in turn, cause the call to be dropped, because both the ends determine that communication is no longer occurring.
- To avoid the risk of dropped calls, you can include signaling in one of the priority queues. The configuration example previously defined the priority queues as voice and video and now adds signaling to the video queue.

The policy uses call admission control (CAC) for the voice flow. CAC targets wireless traffic and matches a specific UP (in this configuration example, UP 6 and 7). CAC then determines the maximum amount of bandwidth this traffic should use. In a configuration where you police voice traffic, CAC should be allocated a subset of the overall amount of bandwidth allocated for voice. For example, if voice is policed to 6 Mbps, CAC cannot exceed 6 Mbps. CAC is configured in a policy-map (called a child policy) that is integrated into the main downstream policy-map (called the parent policy). CAC is introduced with the **admit cac wmm-tspecc** command, followed by the target UPs and the bandwidth allocated to the targeted traffic.

Each call does not consume all the bandwidth allocated to voice. For example, each call may consume 64 kbps each way, which results in 128 kbps of effective bi-directional bandwidth consumption. The rate instruction determines each call bandwidth consumption, while the police statement determines the overall bandwidth allocated to voice traffic. If all calls that occur within the cell use close to the maximum allowed bandwidth, any new call that is initiated from within the cell and that causes the consumed bandwidth to exceed the maximum bandwidth allowed for voice will be denied. You can fine tune this process through configuration of CAC at the band level, as explained in Call Limitation with CAC.

Therefore, you need to configure a child policy that contains the CAC instructions and that is integrated into the main downstream policy. CAC is not configured in the upstream policy-map. CAC does apply to voice calls initiated from the cell, but, because it is a response to those calls, CAC is set only into the downstream policy-map. The upstream policy-map will be different. You cannot use the class-maps created previously because these class-maps target traffic based on an ACL. Traffic injected into the SSID policy has gone through the client policy, so you should not perform inspection on the packets a second time. Instead, target traffic with a QoS marking that results from the client policy.

If you decide not to leave signaling in the default class, you will also need to prioritize signaling.

In the following example, signaling and video are in the same class and more bandwidth is allocated to that class to accommodate the signaling part. 6 Mbps is allocated for video traffic (one Tandberg camera point-to-point flow) and 1 Mbps is allocated to signaling for all voice calls and the video flow:

```
Class-map allvoice
match dscp ef
Class-map videoandsignaling
Match dscp af41
Match dscp cs3
```

The following describes the downstream child policy:

```
Policy-map SSIDout_child_policy
class allvoice
priority level 1
police 6000000
admit cac wmm-tspec
rate 128
wlan-up 6 7
class videoandsignaling
priority level 2
police 1000000
```

The following describes the downstream parent policy:

```
policy-map SSIDout
class class-default
set dscp dscp table dscp2dscp
set wlan user-priority dscp table dscp2up
shape average 30000000
queue-buffers ratio 0
service-policy SSIDout_child_policy
```

Upstream traffic comes from wireless clients and is sent to the WCM before the traffic is sent out of a wired port or to another SSID. In both cases, you can configure policy-maps that define the bandwidth allocated to each type of traffic. The policy will probably differ based on whether the traffic is sent out of a wired port or to another SSID.

In the upstream direction, the primary concern is to decide the priority and not the bandwidth. In other words, the upstream policy-map does not allocate bandwidth to each type of traffic. Because the traffic is already at the AP and has already crossed the bottle-neck formed by the half-duplex wireless space, your goal is to bring this traffic to the controller function of the Cisco Catalyst 3850 Series Switch for further processing. When traffic is collected at the AP level, you can decide if you should trust potential existing QoS marking in order to prioritize traffic flows sent to the controller. In the following example, existing DSCP values can be trusted:

```
Policy-map SSIDin
Class class-default
set dscp dscp table dscp2dscp
```

As you create your policies, apply the policy-maps to the WLAN.

In the following example, any device connecting to the WLAN is expected to support WMM, so WMM is required:

```
wlan test1
wmm require
service-policy client input taggingPolicy
service-policy input SSIDin
service-policy output SSIDout
```

Call Limitation with CAC

The last step is to customize CAC as per your requirements. In the CAC configuration explained in the Bandwidth and Policy Management at SSID Level, the AP drops any voice packet that exceeds the allocated bandwidth.

In order to avoid the bandwidth maximum, you need to configure the WCM in order to recognize calls that are placed and calls that will cause the bandwidth to exceed. Some phones support WMM Traffic Specification (TSPEC) and inform the wireless infrastructure of the bandwidth that the projected call is expected to consume. The WCM can then refuse the call before it is placed.

Some SIP phones do not support TSPEC, but the WCM and the AP can be set to recognize call initiation packets sent to SIP ports and can use this information in order to establish that a SIP call is about to be placed. Because the SIP phone does not specify the bandwidth that is to be consumed by the call, the administrator must determine the expected bandwidth based on the codec, the sampling time, and so on.

CAC calculates the consumed bandwidth at each AP level. CAC can be set to use only the client bandwidth consumption in its calculations (static CAC) or to also consider neighboring APs and devices on the same channel (load-based CAC). We recommend that you use static CAC for SIP phones and load-based CAC for TSPEC phones.

Finally, CAC is activated on a per band basis.

In the following example, phones use SIP rather than TSPEC for their session initiation. Each call uses 64 kbps for each stream direction, load-based CAC is disabled when static CAC is enabled, and 75% of each AP bandwidth max is allocated to voice traffic:

```
ap dot11 5ghz shutdown
ap dot11 5ghz cac voice acm
no ap dot11 5ghz cac voice load-based
ap dot11 5ghz cac voice max-bandwidth 75
ap dot11 5ghz cac voice sip bandwidth 64
no ap dot11 5ghz shutdown
```

You can repeat the same configuration for the 2.4 GHz band as shown in the following example:

```
ap dot11 24ghz shutdown
ap dot11 24ghz cac voice acm
no ap dot11 24ghz cac voice load-based
ap dot11 24ghz cac voice max-bandwidth 75
ap dot11 24ghz cac voice sip bandwidth 64
no ap dot11 24ghz shutdown
```

Once CAC is applied for each band, you also need to apply SIP CAC at the WLAN level. This process enables the AP to examine Layer 4 (L4) information of the wireless client traffic for identifying queries sent to UDP 5060 indicating SIP call attempts. TSPEC operates at the 802.11 level and is natively detected by APs. SIP phones do not use TSPEC and AP must perform packet inspection to identify SIP traffic. To avoid AP to perform this inspection on all SSIDs, you need to determine which SSIDs expect SIP traffic. You can enable call snooping on those SSIDs to perform specific voice calls. You can also determine what action to perform if a SIP call needs to be rejected - disassociate the SIP client or send a SIP busy message.

In the following example, call snooping is enabled and a busy message is sent, if the SIP call needs to be rejected. With the addition of the QoS policy (Refer to Step 3), Bandwidth and Priority Management at SSID Level, this is the SSID configuration for the example WLAN:

```
wlan test1
wmm require
service-policy client input taggingPolicy
service-policy input SSIDin
service-policy output SSIDout
call-snoop
sip-cac platinum
```

Verifying Configuration for QoS

To verify the configuration, use the following commands:

show class-map

The following is an example of the class-maps configured on the platform:

```
Device# show class-map
Class Map match-any H323realtimeaudio (id 6)
  Match access-group name H323Audiostream
Class Map match-any H323realtimevideo (id 7)
  Match access-group name H323Videostream
Class Map match-any allvideo (id 10)
  Match dscp af41 (34)
Class Map match-any jabberaudiosignaling (id 11)
  Match access-group name JabberSIGNALING
Class Map match-any allvoice (id 12)
  Match dscp ef (46)
Class Map match-any RTPaudio (id 19)
  Match access-group name JabberVOIP
  Match access-group name H323Audiostream
Class Map match-any class-default (id 0)
  Match any
Class Map match-any jabberRTPaudio (id 14)
  Match access-group name JabberVOIP
Class Map match-any non-client-nrt-class (id 1)
  Match non-client-nrt
Class Map match-any H323audiosignaling (id 17)
  Match access-group name H323AudioSignaling
Class Map match-any H323videosignaling (id 18)
  Match access-group name H323VideoSignaling
Class Map match-any signaling (id 20)
  Match access-group name JabberSIGNALING
  Match access-group name H323VideoSignaling
  Match access-group name H323AudioSignaling
```

show policy-map

The following is an example of the policy-maps configured on the platform:

```
Device# show policy-map
show policy-map
  Policy Map port_child_policy
    Class non-client-nrt-class
      bandwidth remaining ratio 7
    Class allvoice
      priority level 1
      police rate percent 10
      conform-action transmit
      exceed-action drop
    Class allvideo
      priority level 2
      police rate percent 20
      conform-action transmit
      exceed-action drop
    Class class-default
      bandwidth remaining ratio 63
  Policy Map SSIDin
    Class class-default
      set dscp dscp table dscp2dscp
  Policy Map SSIDout_child_policy
    Class allvoice
      priority level 1
      police cir 6000000 bc 187500
      conform-action transmit
      exceed-action drop
      admit cac wmm-tspec
      rate 6000 (kbps)
```

```

    wlan-up 6
  Class allvideo
    priority level 2
    police cir 6000000 bc 187500
      conform-action transmit
      exceed-action drop
      admit cac wmm-tspec
      rate 6000 (kbps)
      wlan-up 4 5
  Policy Map taggingPolicy
    Class RTPaudio
      set dscp ef
    Class H323realtimevideo
      set dscp af41
    Class signaling
      set dscp cs3
  Policy Map SSIDout
    Class class-default
      set dscp dscp table dscp2dscp
      set wlan user-priority dscp table dscp2up
      shape average 30000000 (bits/sec)
      queue-buffers ratio 0
      service-policy SSIDout_child_policy
  Policy Map parent_port
    Class class-default
      shape average 1000000000 (bits/sec) op

```

show wlan

The following is an example of the WLAN configuration and service-policy parameters:

```

Device# show wlan name test1 | include Policy
AAA Policy Override : Disabled
QoS Service Policy - Input
  Policy Name : SSIDin
  Policy State : Validated
QoS Service Policy - Output
  Policy Name : SSIDout
  Policy State : Validated
QoS Client Service Policy
  Input Policy Name : taggingPolicy
  Output Policy Name : taggingPolicy
Radio Policy : All

```

show policy-map interface

The following is an example of the policy-map installed for a specific interface:

```

Device# show policy-map interface wireless ssid name test1
Remote SSID test1 iifid: 0x01023F4000000033.0x00F2E98000000003.0x00C2EB000000001F
Service-policy input: SSIDin
  Class-map: class-default (match-any)
    Match: any
      0 packets, 0 bytes
      30 second rate 0 bps
  QoS Set
    dscp dscp table dscp2dscp

Remote SSID test1 iifid: 0x01023F4000000033.0x00C8384000000004.0x00D0D08000000021

Service-policy input: SSIDin

  Class-map: class-default (match-any)
    Match: any
      0 packets, 0 bytes

```



```

    30 second rate 0 bps
  QoS Set
    dscp dscp table dscp2dscp
SSID test1 iifid: 0x01023F4000000033.0x00F2E98000000003.0x00EC3E800000001E

Service-policy input: SSIDin

Class-map: class-default (match-any)
  Match: any
    0 packets, 0 bytes
    30 second rate 0 bps
  QoS Set
    dscp dscp table dscp2dscp

Service-policy output: SSIDout

Class-map: class-default (match-any)
  Match: any
    0 packets, 0 bytes
    30 second rate 0 bps
  QoS Set
    dscp dscp table dscp2dscp
    wlan user-priority dscp table dscp2up
  shape (average) cir 30000000, bc 120000, be 120000
  target shape rate 30000000
  queue-buffers ratio 0

Service-policy : SSIDout_child_policy

Class-map: allvoice (match-any)
  Match: dscp ef (46)
    0 packets, 0 bytes
    30 second rate 0 bps
  Priority: Strict,

  Priority Level: 1
  police:
    cir 6000000 bps, bc 187500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps
    cac wmm-tspec rate 6000 kbps

Class-map: allvideo (match-any)
  Match: dscp af41 (34)
    0 packets, 0 bytes
    30 second rate 0 bps
  Priority: Strict,

  Priority Level: 2
  police:
    cir 6000000 bps, bc 187500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps
    cac wmm-tspec rate 6000 kbps

Class-map: class-default (match-any)
  Match: any
    0 packets, 0 bytes
    30 second rate 0 bps
SSID test1 iifid: 0x01023F4000000033.0x00C8384000000004.0x00DB568000000020

Service-policy input: SSIDin

Class-map: class-default (match-any)
  Match: any

```

show policy-map interface

```

    0 packets, 0 bytes
    30 second rate 0 bps
  QoS Set
    dscp dscp table dscp2dscp

Service-policy output: SSIDout

Class-map: class-default (match-any)
  Match: any
    0 packets, 0 bytes
    30 second rate 0 bps
  QoS Set
    dscp dscp table dscp2dscp
    wlan user-priority dscp table dscp2up
  shape (average) cir 30000000, bc 120000, be 120000
  target shape rate 30000000
  queue-buffers ratio 0

Service-policy : SSIDout_child_policy

Class-map: allvoice (match-any)
  Match: dscp ef (46)
    0 packets, 0 bytes
    30 second rate 0 bps
  Priority: Strict,

  Priority Level: 1
  police:
    cir 6000000 bps, bc 187500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps
    cac wmm-tspec rate 6000 kbps

Class-map: allvideo (match-any)
  Match: dscp af41 (34)
    0 packets, 0 bytes
    30 second rate 0 bps
  Priority: Strict,

  Priority Level: 2
  police:
    cir 6000000 bps, bc 187500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps
    cac wmm-tspec rate 6000 kbps

Class-map: class-default (match-any)
  Match: any
    0 packets, 0 bytes
    30 second rate 0 bps

Device(config)# show policy-map interface wireless client
Client 8853.2EDC.68EC iidid:
0x01023F4000000033.0x00F2E98000000003.0x00EC3E800000001E.0x00E0D04000000022

Service-policy input: taggingPolicy

Class-map: RTPaudio (match-any)
  Match: access-group name JabberVOIP
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: access-group name H323Audiostream
    0 packets, 0 bytes
    30 second rate 0 bps
  QoS Set
    dscp ef

```

```
Class-map: H323realtimevideo (match-any)
  Match: access-group name H323Videostream
    0 packets, 0 bytes
    30 second rate 0 bps
  QoS Set
    dscp af41

Class-map: signaling (match-any)
  Match: access-group name JabberSIGNALING
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: access-group name H323VideoSignaling
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: access-group name H323AudioSignaling
    0 packets, 0 bytes
    30 second rate 0 bps
  QoS Set
    dscp cs3
Class-map: class-default (match-any)
  Match: any
    0 packets, 0 bytes
    30 second rate 0 bps

Service-policy output: taggingPolicy

Class-map: RTPaudio (match-any)
  Match: access-group name JabberVOIP
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: access-group name H323Audiostream
    0 packets, 0 bytes
    30 second rate 0 bps
  QoS Set
    dscp ef

Class-map: H323realtimevideo (match-any)
  Match: access-group name H323Videostream
    0 packets, 0 bytes
    30 second rate 0 bps
  QoS Set
    dscp af41

Class-map: signaling (match-any)
  Match: access-group name JabberSIGNALING
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: access-group name H323VideoSignaling
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: access-group name H323AudioSignaling
    0 packets, 0 bytes
    30 second rate 0 bps
  QoS Set
    dscp cs3
Class-map: class-default (match-any)
  Match: any
    0 packets, 0 bytes
    30 second rate 0 bps
```

show platform qos policies

The following is an example of the QoS policies installed for ports, AP radios, SSIDs, and clients.

**Note**

You can only verify, but cannot change the radio policies.

```

Device# show platform qos policies PORT
-----
Loc Interface          IIF-ID          Dir Policy          State
-----
L:0 Gi1/0/20          0x01023f4000000033 OUT defportangn     INSTALLED IN HW
L:0 Gi1/0/20          0x01023f4000000033 OUT port_child_policy INSTALLED IN HW

Device(config)# show platform qos policies RADIO
-----
Loc Interface          IIF-ID          Dir Policy          State
-----
L:0 R56356842871193604 0x00c8384000000004 OUT def-1lan        INSTALLED IN HW
L:0 R68373680329064451 0x00f2e98000000003 OUT def-1lgn        INSTALLED IN HW

Device(config)# show platform qos policies SSID
-----
Loc Interface          IIF-ID          Dir Policy          State
-----
L:0 S70706569125298203 0x00fb33400000001b OUT SSIDout_child_policy INSTALLED IN HW
L:0 S69318160817324057 0x00f6448000000019 OUT SSIDout_child_policy INSTALLED IN HW
L:0 S70706569125298203 0x00fb33400000001b OUT SSIDout          INSTALLED IN HW
L:0 S69318160817324057 0x00f6448000000019 OUT SSIDout          INSTALLED IN HW
L:0 S70706569125298203 0x00fb33400000001b IN  SSIDin           INSTALLED IN HW
L:0 S69318160817324057 0x00f6448000000019 IN  SSIDin           INSTALLED IN HW

Device(config)# show platform qos policies CLIENT
-----
Loc Interface          IIF-ID          Dir Policy          State
-----
L:0 8853.2edc.68ec     0x00e0d04000000022 IN  taggingPolicy     NOT INSTALLED IN HW
L:0 8853.2edc.68ec     0x00e0d04000000022 OUT taggingPolicy     NOT INSTALLED IN HW

```

show wireless client mac-address <mac> service-policy

The following is an example of the policy-maps applied at client level:

```

Device# show wireless client mac-address 8853.2EDC.68EC service-policy output
Wireless Client QoS Service Policy
Policy Name : taggingPolicy
Policy State : Installed
Device# show wireless client mac-address 8853.2EDC.68EC service-policy in
Device# show wireless client mac-address 8853.2EDC.68EC service-policy input
Wireless Client QoS Service Policy
Policy Name : taggingPolicy
Policy State : Installed

```

Troubleshooting QoS Configuration Issues

Currently, there is no specific troubleshooting information available for this configuration.



Configuration Example: TACACS Administrator Access to Converged Access Wireless LAN Controllers

This document provides a configuration example for Terminal Access Controller Access Control System Plus (TACACS+) in a Cisco Catalyst 3850 Series, and Cisco Catalyst 3650 Series Switches for CLI and GUI. This document also provides basic tips to troubleshoot the configuration.

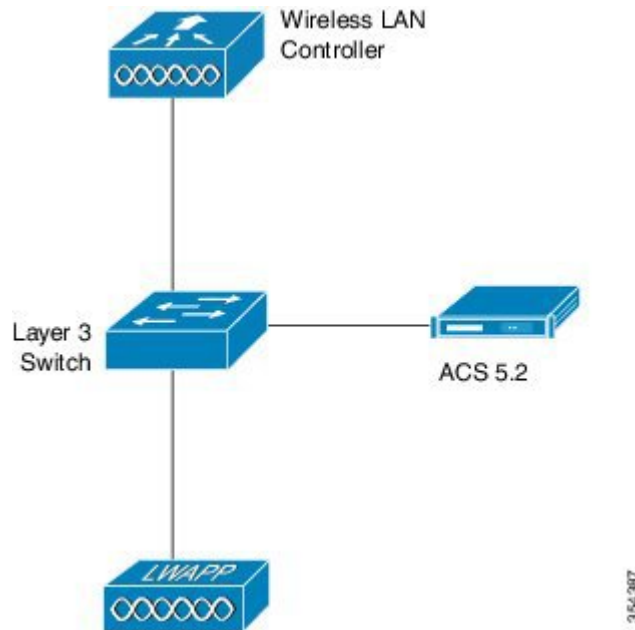
TACACS+ is a client and server protocol that provides centralized security for users who attempt to gain management access to a router or network access server. TACACS+ provides the following Authentication, Authorization, and Accounting (AAA) services:

- Authentication of users who attempt to log in to the network equipment.
 - Authorization to determine what level of access users should have.
 - Accounting to keep track of all changes the users make.
-
- [Network Diagram for TACACS Administrator Access, page 250](#)
 - [Configuring TACACS Administrator Access to the Converged Access WLCs, page 250](#)
 - [Configuring TACACS Administrator Access to Converged Access WLCs, page 251](#)
 - [Verifying TACACS Administrator Access to the Converged Access WLC, page 256](#)
 - [Troubleshooting TACACS Administrator Access to the Converged Access WLC, page 256](#)

Network Diagram for TACACS Administrator Access

The following figure displays the network diagram for TACACS Administrator Access:

Figure 79: Network Diagram for TACACS Administrator Access



Configuring TACACS Administrator Access to the Converged Access WLCs

Configuring TACACS Administrator Access to the Converged Access WLCs includes the following two steps:

- Configuring on the WLC
- Configuring on the RADIUS and TACACS server

Step 1

To define the TACACS server on the WLC, use the following commands. Ensure you configure the same shared secret on the TACACS.

```
tacacs-server host 198.51.100.71 key Cisco123
tacacs server ACS
address ipv4 198.51.100.50
key Cisco123
timeout 10
```

Step 2 To configure the server groups and map the server configured in the step 1, use the following commands.

```
aaa group server tacacs+ ACS
  server name ACS
!
```

Step 3 To configure the Authentication and the Authorization policies for administrator access, use the following commands. Provide the administrator access to TACACS group followed by local (which is the fallback).

```
aaa authentication login Admin_Access group ACS local
aaa authorization exec Admin_Access group ACS local
```

Step 4 To apply the policy to the line vty, use the following commands:

```
line vty 0 4
  authorization exec Admin_Access
  login authentication Admin_Access
line vty 5 15
  exec-timeout 0 0
  authorization exec Admin_Access
  login authentication Admin_Access
```

Step 5 To apply the policy to HTTP, use the following commands:

```
ip http server
ip http authentication aaa login-authentication Admin_Access
ip http authentication aaa exec-authorization Admin_Access
```

Configuring TACACS Administrator Access to Converged Access WLCs

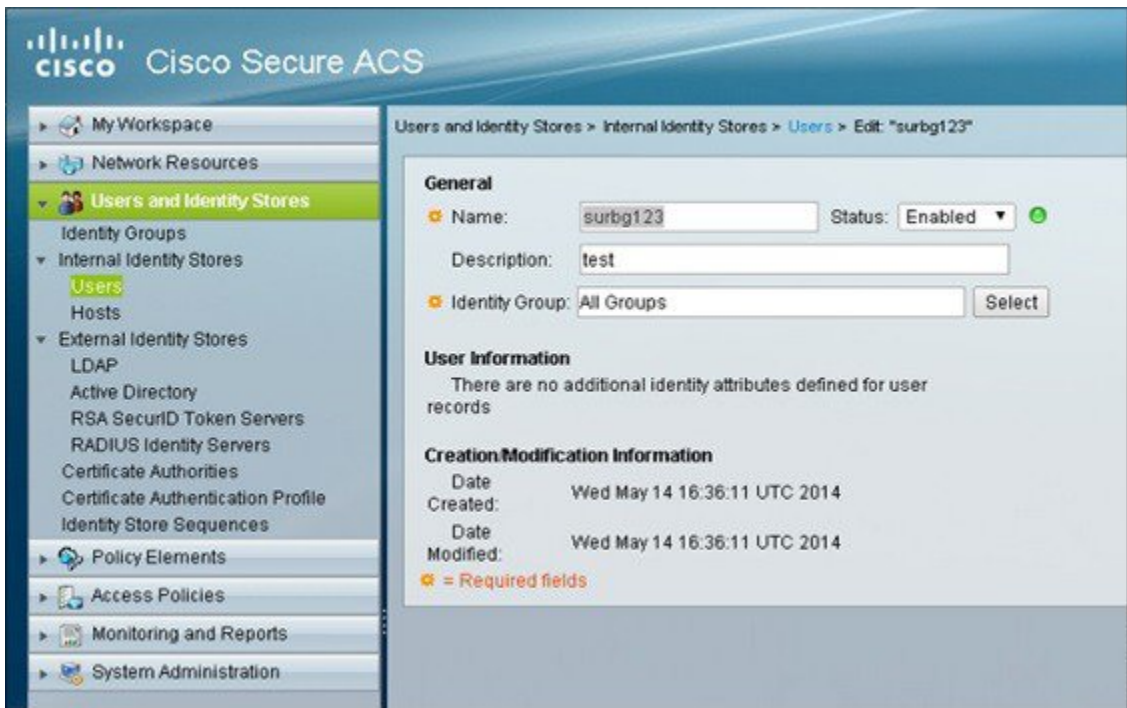
Step 1 To add WLC as the AAA client for TACACS on the ACS, navigate to **Network Resources > Network Devices**, and AAA Clients. Ensure the Shared Secret configured here matches the one configured on the WLC.

Figure 80: Add WLC as the AAA Client



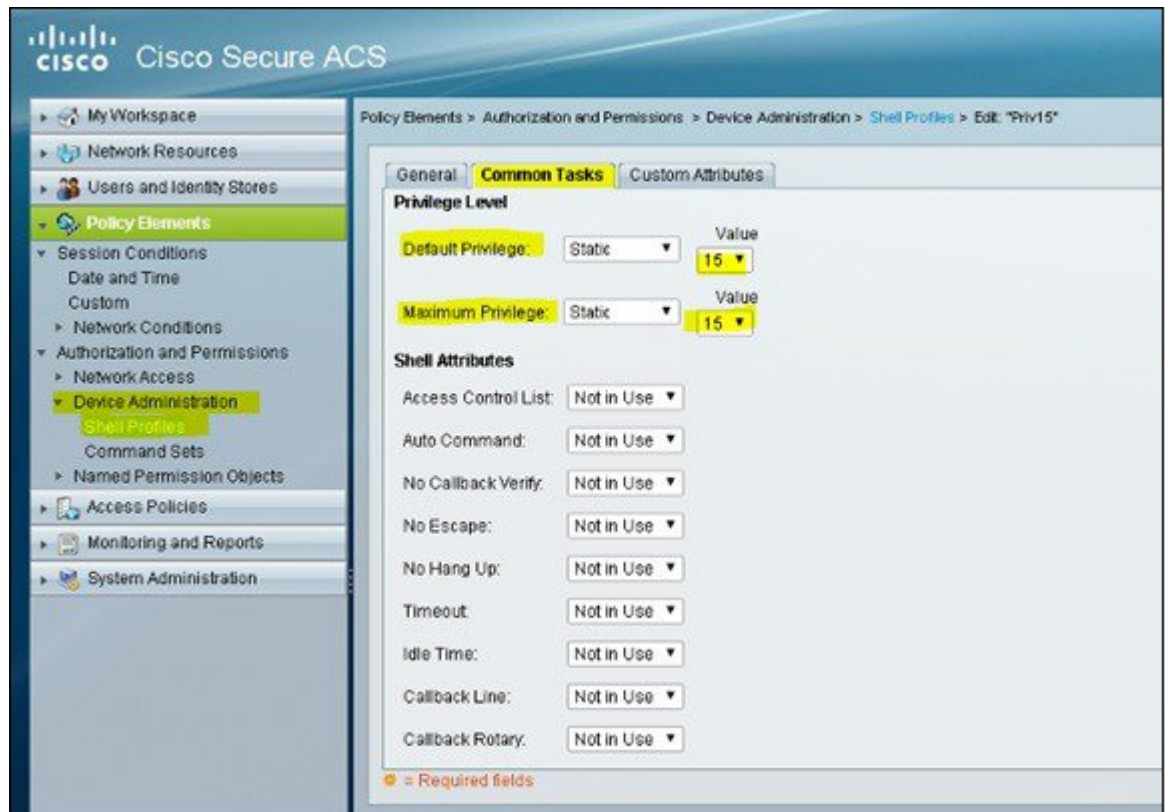
Step 2 To define the user for administrator access, navigate to **Users and Identity Stores > Internal Identity Stores > Users**

Figure 81: Define Administrator Access



- Step 3** To set the privilege levels to 15, navigate to **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles**.

Figure 82: Set Privilege Level



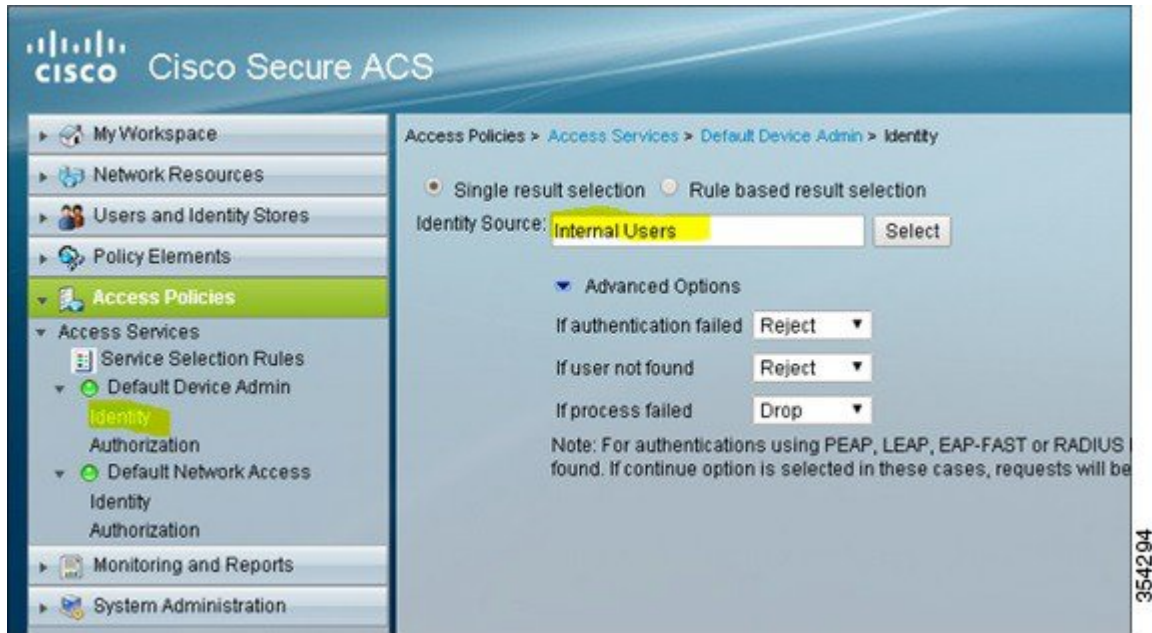
Step 4 To allow the required protocols, navigate to **Access Policies > Access Services > Default Device Admin**.

Figure 83: Enable Protocols



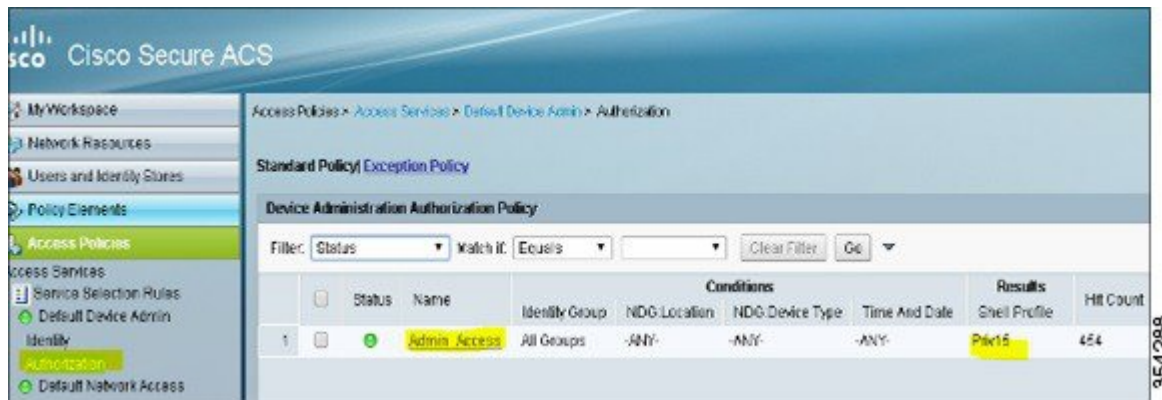
Step 5 To create an identity for the device administrator which allows internal users with authentication options, navigate to **Access Policies > Access Services > Default Device Admin > Identity** .

Figure 84: Create Identity for Device Administrator



Step 6 To allow the Priv15 authorization profile created in Step 3, navigate to **Access Policies > Access Services > Default Device Admin > Authorization**. The client authenticated successfully (internal users) is put on the Priv15 profile.

Figure 85: Enable Priv15 Authorization Profile



Verifying TACACS Administrator Access to the Converged Access WLC

Confirm that your configuration works properly by perform the following steps:

-
- Step 1** Open a browser and enter the switch IP address. The Authentication Required prompt displays.
 - Step 2** Enter the group user credentials to log in to the device.
 - Step 3** To check the Telnet or SSH access, Telnet or SSH to the switch IP address and enter the credentials. The ACS Log in details is displayed.
-

Troubleshooting TACACS Administrator Access to the Converged Access WLC

The following section provides information to troubleshoot your configuration.



Note

Refer to Important Information on before using debug commands

To troubleshoot your configuration, use the **debug tacacs** command.

debug tacacs

```
*May 14 23:11:06.396: TPLUS: Queuing AAA Authentication request 4775 for processing
*May 14 23:11:06.396: TPLUS(000012A7) login timer started 1020 sec timeout
*May 14 23:11:06.396: TPLUS: processing authentication continue request id 4775
*May 14 23:11:06.396: TPLUS: Authentication continue packet generated for 4775
*May 14 23:11:06.396: TPLUS(000012A7)/0/WRITE/962571D4: Started 10 sec timeout
*May 14 23:11:06.396: TPLUS(000012A7)/0/WRITE: wrote entire 25 bytes request
*May 14 23:11:06.398: TPLUS(000012A7)/0/READ: socket event 1
*May 14 23:11:06.398: TPLUS(000012A7)/0/READ: read entire 12 header bytes (expect
16 bytes data)
*May 14 23:11:06.398: TPLUS(000012A7)/0/READ: socket event 1
*May 14 23:11:06.398: TPLUS(000012A7)/0/READ: read entire 28 bytes response
*May 14 23:11:06.398: TPLUS(000012A7)/0/962571D4: Processing the reply packet
*May 14 23:11:06.398: TPLUS: Received authen response status GET PASSWORD (8)
*May 14 23:11:08.680: TPLUS: Queuing AAA Authentication request 4775 for processing
*May 14 23:11:08.680: TPLUS(000012A7) login timer started 1020 sec timeout
*May 14 23:11:08.680: TPLUS: processing authentication continue request id 4775
*May 14 23:11:08.680: TPLUS: Authentication continue packet generated for 4775
*May 14 23:11:08.680: TPLUS(000012A7)/0/WRITE/962571D4: Started 10 sec timeout
*May 14 23:11:08.680: TPLUS(000012A7)/0/WRITE: wrote entire 25 bytes request
*May 14 23:11:08.687: TPLUS(000012A7)/0/READ: socket event 1
*May 14 23:11:08.687: TPLUS(000012A7)/0/READ: read entire 12 header bytes (expect
6 bytes data)
*May 14 23:11:08.687: TPLUS(000012A7)/0/READ: socket event 1
*May 14 23:11:08.687: TPLUS(000012A7)/0/READ: read entire 18 bytes response
*May 14 23:11:08.687: TPLUS(000012A7)/0/962571D4: Processing the reply packet
*May 14 23:11:08.687: TPLUS: Received authen response status PASS (2)
*May 14 23:11:08.687: TPLUS: Queuing AAA Authorization request 4775 for processing
*May 14 23:11:08.687: TPLUS(000012A7) login timer started 1020 sec timeout
*May 14 23:11:08.687: TPLUS: processing authorization request id 4775
```

```
*May 14 23:11:08.687: TPLUS: Protocol set to None .....Skipping
*May 14 23:11:08.687: TPLUS: Sending AV service=shell
*May 14 23:11:08.687: TPLUS: Sending AV cmd*
*May 14 23:11:08.687: TPLUS: Authorization request created for 4775(surbg123)
*May 14 23:11:08.687: TPLUS: using previously set server 10.106.102.50 from
group SURBG_ACS
*May 14 23:11:08.688: TPLUS(000012A7)/0/NB_WAIT/93C63F04: Started 10 sec timeout
*May 14 23:11:08.690: TPLUS(000012A7)/0/NB_WAIT: socket event 2
*May 14 23:11:08.690: TPLUS(000012A7)/0/NB_WAIT: wrote entire 61 bytes request
*May 14 23:11:08.690: TPLUS(000012A7)/0/READ: socket event 1
*May 14 23:11:08.690: TPLUS(000012A7)/0/READ: Would block while reading
*May 14 23:11:08.696: TPLUS(000012A7)/0/READ: socket event 1
*May 14 23:11:08.696: TPLUS(000012A7)/0/READ: read entire 12 header bytes (expect
18 bytes data)
*May 14 23:11:08.696: TPLUS(000012A7)/0/READ: socket event 1
*May 14 23:11:08.696: TPLUS(000012A7)/0/READ: read entire 30 bytes response
*May 14 23:11:08.696: TPLUS(000012A7)/0/93C63F04: Processing the reply packet
*May 14 23:11:08.696: TPLUS: Processed AV priv-lvl=15
*May 14 23:11:08.696: TPLUS: received authorization response for 4775: PASS
```

•



Configuration Example: Unified Access WLC Guest Anchor with Converged Access

The Unified Access WLC Guest Anchor with Converged Access document describes how to configure the Cisco 5500 Series Wireless Controllers and the Cisco Catalyst 3850 Series Switch for the wireless client Guest Anchor in the new mobility deployment setup, where the Cisco 5500 Series Wireless Controller acts as the Mobility Anchor, and the Cisco Catalyst 3850 Series Switch acts as a Mobility Foreign Controller for the clients.

Additionally, the Cisco Catalyst 3850 Series Switch acts as a Mobility Agent to a Cisco Catalyst 3850 Series Switch, which acts as a Mobility Controller from where the Cisco Catalyst 3850 Series Switch acquires the Access Point (AP) license.

- [Prerequisites, page 259](#)
- [Unified Access WLC Guest Anchor with Converged Access, page 261](#)
- [Verifying the Unified WLC Guest Anchor with Converged Access Configuration, page 268](#)
- [Client-side Packet Capture, page 268](#)
- [Troubleshooting Unified WLC Guest Anchor with Converged Access Configuration Issues, page 268](#)

Prerequisites

We recommend that you have basic knowledge on the following topics before you start.

- Cisco IOS GUI or CLI with Converged Access Cisco Catalyst 3650 Series and the Cisco Catalyst 3850 Series Switches
- GUI and CLI access with the Cisco 5500 Series Wireless Controller.
- Service Set Identifier (SSID) configuration
- Web Authentication

Supported Platforms and Releases

The information in this document is based on the following software and hardware versions:

- Cisco Catalyst 3850 Series Switch Denali-16.1.1
- Cisco 5500 Series Wireless LAN Controllers Release 7.6.120
- Cisco 3600 Series Lightweight Access Points (APs)
- Cisco Catalyst 3560 Series Switches



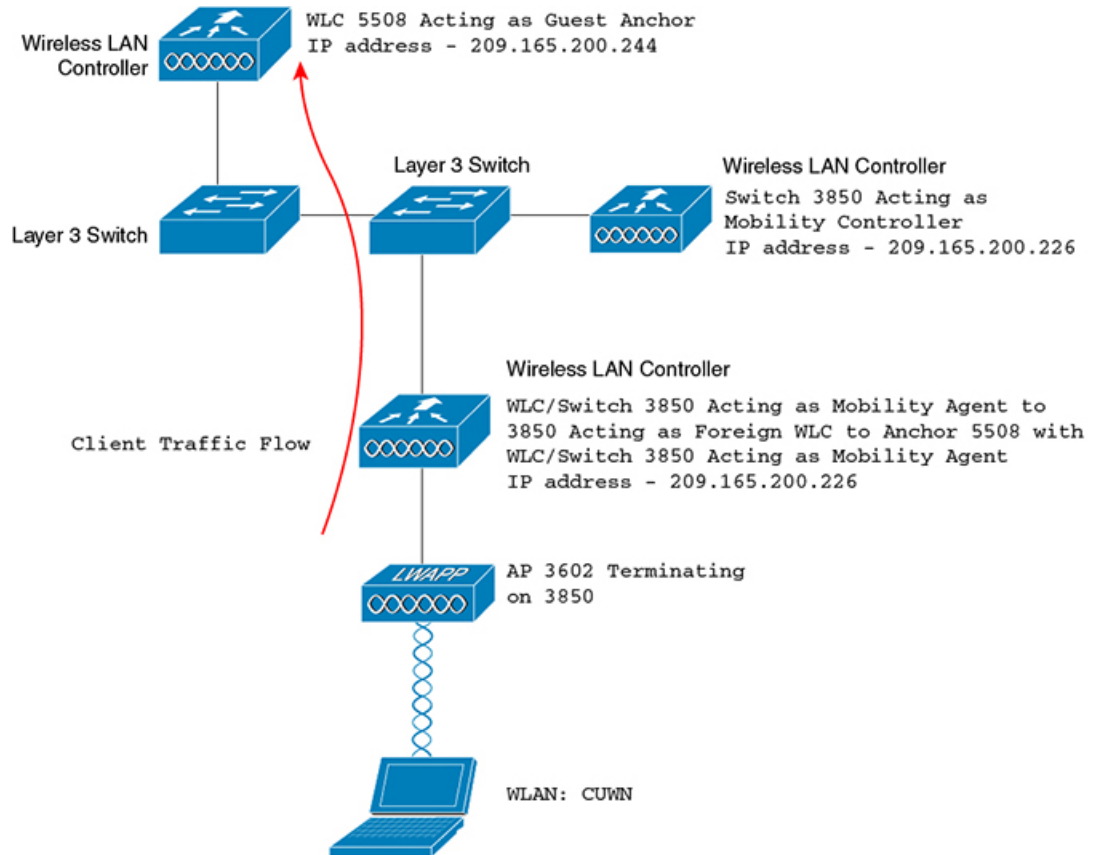
Note

The information in this document refers to the devices in a customized lab environment. The devices have default configuration. If you are on a live network, you must understand the potential impact of all the commands.

Unified Access WLC Guest Anchor with Converged Access

The following figure shows a Cisco 5500 Series Wireless Controller acting as an Anchor Controller and a Cisco Catalyst 3850 Series Switch acting as Foreign Controller and a Mobility Agent which obtains the license from Cisco Catalyst 3850 Series Switch acting as a Mobility Controller.

Figure 86: Unified Access WLC Guest Anchor with Converged Access



Note

In the network diagram, the Cisco 5500 Series Wireless Controller acts as the Anchor Controller and the Cisco Catalyst 3850 Series Switch acts as the Mobility Agent, Mobility Controller, and Foreign WLC.

At any point in time, the Anchor Controller for the Cisco Catalyst 3850 Series Switch is Cisco 5500 Series Wireless Controller and double anchoring is not supported.

Configuring Unified Access WLC includes:

- Part 1: Configuring on the Cisco 5500 Series Anchor Wireless Controller.
- Part 2: Configuring Converged Access Mobility between the Cisco 5500 Series Wireless Controller and the Cisco Catalyst 3850 Series Switch.
- Part 3 - Configuring on the Foreign Cisco Catalyst 3850 Series Switch

Network Diagram

Part 1: Configuring on the Cisco 5500 Series Anchor Wireless Controller

Step 1 To create a new WLAN on the Cisco 5500 Series Wireless Controller, navigate to **WLAN > New**.

Figure 87: Creating WLAN



Step 2 To configure Layer 3 Security, navigate to **WLAN > WLAN Edit > Security > Layer 3 enabled Web-authentication**.

Step 3 To add the Cisco 5500 Series Wireless Controller as the Anchor, navigate to **WLAN > Mobility Anchor** and change the Anchor address to **Local**.

Figure 88: Adding Wireless Controller



Step 4 To configure the WebAuth page (for example, Internal WebAuth) for client authentication, navigate to **Security > WebAuth > WebAuth**.

Step 5 Create a local net user. When prompted by the WebAuth page, the username and password created is used by the user.

Figure 89: Creating local user



Part 2: Configuring Converged Access Mobility between the Cisco 5500 Series Wireless Controller and Cisco Catalyst 3850 Series Switch

Step 1 On the Cisco 5500 Series Wireless Controller, add the Cisco Catalyst 3850 Series Switch with WLC as the Mobility Peer.

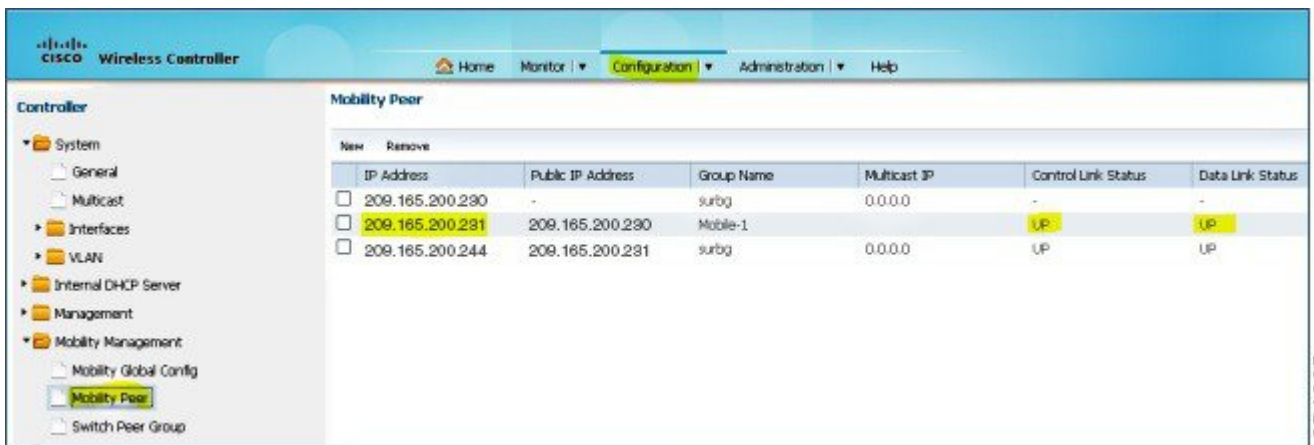
Figure 90: Adding WLC as mobility peer



354264

Step 2 On the Cisco Catalyst 3850 Series with WLC performing as a Mobility Controller, add the Cisco 5500 Series Wireless Controller as the Mobility Peer.

Figure 91: Adding wireless controller as mobility peer



354265

Step 3 Add the other Cisco Catalyst 3850 Series Switch as the Mobility Agent on the Cisco Catalyst 3850 Series Switch with WLC under the Switch Peer Group tab under Mobility Management.

Note This is an important step.

Figure 92: Adding mobility agent



354263

Step 4 On the Cisco Catalyst 3850 Series Switch, add the Cisco Catalyst 3850 Series Switch as the Mobility Controller. Once Cisco Catalyst 3850 Series Switch is added as mobility controller, the Cisco Catalyst 3850 Series Switch gets the AP license from the Cisco Catalyst 3850 Series Switch acting as Mobility Controller.

Figure 93: Adding mobility controller



354251

Part 3 - Configuring on the Foreign Catalyst 3850 Series Switch

Step 1 To configure the exact SSID or WLAN on the Cisco Catalyst 3850 Series Switch, navigate to **GUI > Configuration > Wireless > WLAN > New**.

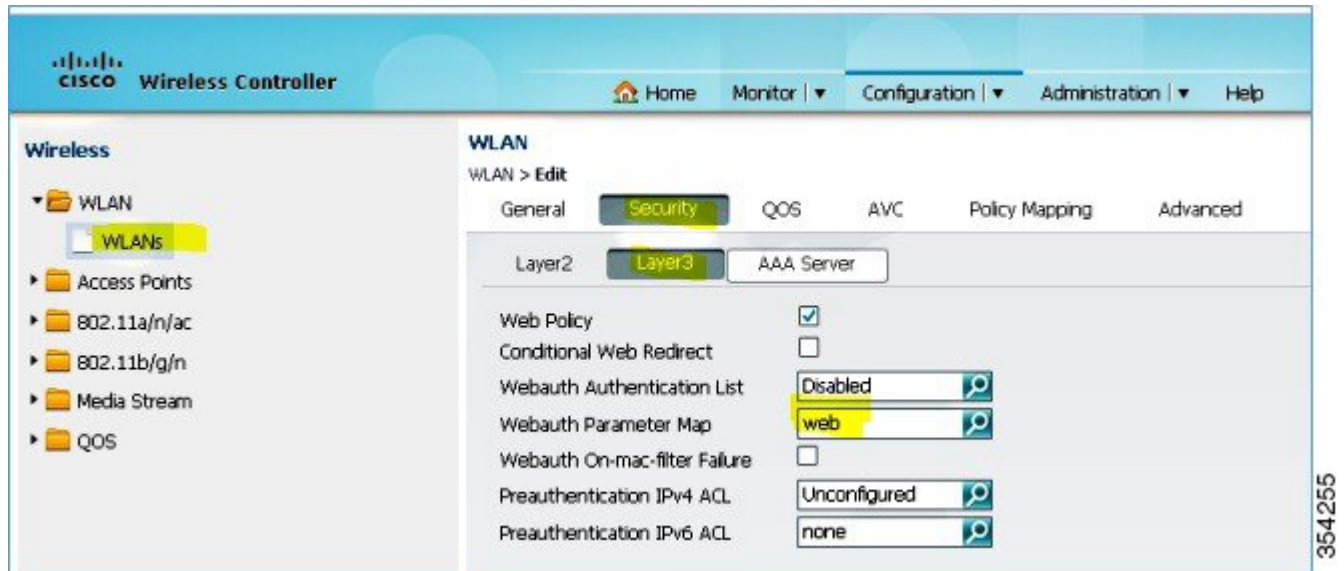
Figure 94: Configuring SSID



354257

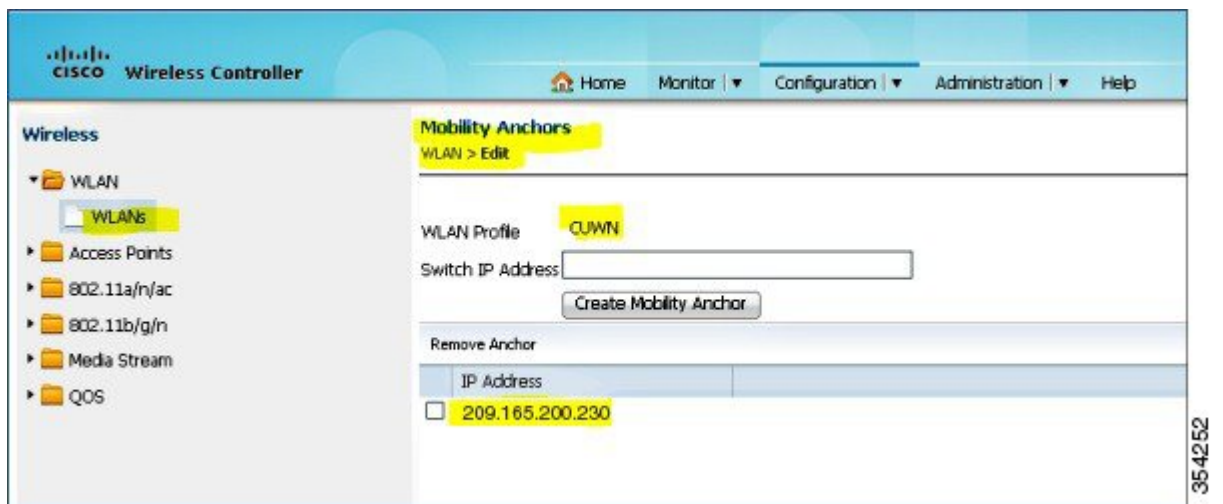
Step 2 To configure Layer 3 Security, navigate to **WLAN > WLAN Edit > Security > Layer 3 enabled Web-authentication**.

Figure 95: Configuring Layer 3 security



Step 3 Add the Cisco 5500 Series Wireless Controller IP address as the Anchor under the WLAN Mobility Anchor configuration.

Figure 96: Adding wireless controller as Anchor



Verifying the Unified WLC Guest Anchor with Converged Access Configuration

Perform the following steps to verify the unified WLC Guest Anchor with converged access configuration:

-
- Step 1** Connect to the WLAN Cisco Unified Wireless Network (CUMN).
 - Step 2** Once you receive the IP address, open a browser and try accessing any website. The first TCP packet sent is intercepted by the Cisco 5500 Series Wireless Controller. Then, the Cisco 5500 Series Wireless Controller intercepts and sends the WebAuth page.
 - Step 3** If the DNS is properly configured, you will receive the WebAuth page.
 - Step 4** Provide the username and password to get authenticated.
 - Step 5** After successful authentication, you will be redirected to the original access page.
 - Step 6** Provide the correct credentials for successful authentication.
-

Client-side Packet Capture

The following steps describe the client-side packet capture:

-
- Step 1** You will receive a IP address as described in the following figure:
 - Step 2** Open a browser and type `www.facebook.com`.
 - Step 3** The Cisco 5500 Series Wireless Controller intercepts the client's first TCP packet and pushes its virtual IP address and the internal WebAuth page.
 - Step 4** After the successful web authentication, the rest of the work flow completes.
-

Troubleshooting Unified WLC Guest Anchor with Converged Access Configuration Issues

To troubleshoot configuration, use the following commands on the Cisco 5500 Series Wireless Controller acting as a Guest Anchor:

Debug Client *client mac addr*

Debug web-auth redirect enable mac *client mac addr*

The following example describes troubleshooting using the debug commands:

```
Device# show debug

MAC Addr 1..... 00:17:7C:2F:B6:9A

Debug Flags Enabled:
  dhcp packet enabled.
  dot11 mobile enabled.
  dot11 state enabled
  dot1x events enabled.
  dot1x states enabled.
  FlexConnect ft enabled.
  pem events enabled.
  pem state enabled.
  CCKM client debug enabled.
  webauth redirect enabled.

*mmMaListen: May 19 13:36:34.276: 00:17:7c:2f:b6:9a Adding mobile on Remote AP
00:00:00:00:00:00(0)
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a override for default ap group,
marking intgrp NULL
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a Applying Interface policy on
Mobile, role Unassociated. Ms NAC State 2 Quarantine Vlan 0 Access Vlan 0

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a Re-applying interface policy
for client

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 START (0) Changing IPv4
ACL 'none' (ACL ID 255) ==> 'none' (ACL ID 255) --- (caller apf_policy.c:2219)
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 START (0) Changing IPv6
ACL 'none' (ACL ID 255) ==> 'none' (ACL ID 255) --- (caller apf_policy.c:2240)
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a apfApplyWlanPolicy: Apply WLAN
Policy over PMIPv6 Client Mobility Type
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a override from intf group to an
intf for roamed client - removing intf group from msch

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 AUTHCHECK (2) Change
state to L2AUTHCOMPLETE (4) last state AUTHCHECK (2)

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 L2AUTHCOMPLETE (4)
Change state to DHCP_REQD (7) last state L2AUTHCOMPLETE (4)

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a Resetting web IPv4 acl from
255 to 255

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a Resetting web IPv4 Flex acl
from 65535 to 65535

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a Stopping deletion of Mobile
Station: (callerId: 53)
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7) Adding
Fast Path rule type = Airespace AP - Learn IP address
on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
IPv4 ACL ID = 255, IPv
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7) Fast Path
rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206 Local Bridging Vlan = 60,
Local Bridging intf id = 13
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7) State
Update from Mobility-Incomplete to Mobility-Complete, mobility role=ExpAnchor,
client state=APF_MS_STATE_ASSOCIATED
*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Change state to DHCP_REQD (7) last state DHCP_REQD (7)

*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
pemAdvanceState2 5807, Adding TMP rule
*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
```

```

Replacing Fast Path rule
  type = Airespace AP - Learn IP address
    on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
    IPv4 ACL ID = 255,
*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Fast Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206 Local Bridging
Vlan = 60, Local Bridging intf id = 13
*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*pemReceiveTask: May 19 13:36:34.278: 00:17:7c:2f:b6:9a Set bi-dir guest tunnel
for 00:17:7c:2f:b6:9a as in Export Anchor role
*pemReceiveTask: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 Added NPU entry
of type 9, dtlFlags 0x4
*pemReceiveTask: May 19 13:36:34.278: 00:17:7c:2f:b6:9a Sent an XID frame
*pemReceiveTask: May 19 13:36:34.278: 00:17:7c:2f:b6:9a Set bi-dir guest tunnel
for 00:17:7c:2f:b6:9a as in Export Anchor role
*pemReceiveTask: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 Added NPU entry
of type 9, dtlFlags 0x4
*IPv6 Msg_Task: May 19 13:36:34.281: 00:17:7c:2f:b6:9a Pushing IPv6 Vlan Intf
ID 13: fe80:0000:0000:0000:6cla:b253:d711:0c7f , and MAC: 00:17:7C:2F:B6:9A ,
Binding to Data Plane. SUCCESS !! dhcpv6bitmap 0
*IPv6 Msg_Task: May 19 13:36:34.281: 00:17:7c:2f:b6:9a Calling mmSendIpv6AddrUpdate
for addition of IPv6: fe80:0000:0000:0000:6cla:b253:d711:0c7f , for MAC:
00:17:7C:2F:B6:9A
*IPv6 Msg_Task: May 19 13:36:34.281: 00:17:7c:2f:b6:9a mmSendIpv6AddrUpdate:4800
Assigning an IPv6 Addr fe80:0000:0000:0000:6cla:b253:d711:0c7f to the client in
Anchor state update the foreign switch 10.105.135.226
*IPv6 Msg_Task: May 19 13:36:34.281: 00:17:7c:2f:b6:9a Link Local address fe80::
6cla:b253:d711:0c7f updated to mscb. Not Advancing pem state.Current state: mscb
in apFMsMmInitial mobility state and client state APF_MS_STATE_AS
*mmMaListen: May 19 13:36:34.298: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Replacing Fast Path rule
  type = Airespace AP - Learn IP address
    on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
    IPv4 ACL ID = 255,
*mmMaListen: May 19 13:36:34.298: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Fast Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206 Local Bridging
Vlan = 60, Local Bridging intf id = 13
*mmMaListen: May 19 13:36:34.298: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*pemReceiveTask: May 19 13:36:34.298: 00:17:7c:2f:b6:9a Set bi-dir guest tunnel for
00:17:7c:2f:b6:9a as in Export Anchor role
*pemReceiveTask: May 19 13:36:34.298: 00:17:7c:2f:b6:9a 0.0.0.0 Added NPU entry of
type 9, dtlFlags 0x4
*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a Static IP client associated to
interface vlan60 which can support client subnet.
*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a 60.60.60.11 DHCP_REQD (7)
Change state to WEBAUTH_REQD (8) last state DHCP_REQD (7)

*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_REQD (8)
pemAdvanceState2 6717, Adding TMP rule
*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_REQD (8)
Replacing Fast Path rule
  type = Airespace AP Client - ACL passthru
    on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
    IPv4 ACL
*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_REQD (8)
Fast Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206 Local Bridging
Vlan = 60, Local Bridging intf id = 13
*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_REQD (8)
Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a Plumbing web-auth redirect rule
due to user logout
*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a apfAssignMscbIpAddr:1148
Assigning an Ip Addr 60.60.60.11 to the client in Anchor state update the foreign
switch 10.105.135.226
*dtlArpTask: May 19 13:36:34.565: 00:17:7c:2f:b6:9a Assigning Address 60.60.60.11
to mobile
*pemReceiveTask: May 19 13:36:34.565: 00:17:7c:2f:b6:9a Set bi-dir guest tunnel for
00:17:7c:2f:b6:9a as in Export Anchor role
*pemReceiveTask: May 19 13:36:34.565: 00:17:7c:2f:b6:9a 60.60.60.11 Added NPU entry
of type 2, dtlFlags 0x4
*pemReceiveTask: May 19 13:36:34.565: 00:17:7c:2f:b6:9a Pushing IPv6:

```

```

fe80:0000:0000:0000:6c1a:b253:d711:0c7f , and MAC: 00:17:7c:2f:b6:9a , Binding to
Data Plane. SUCCESS !!
*pemReceiveTask: May 19 13:36:34.565: 00:17:7c:2f:b6:9a Sent an XID frame

(5508-MC) >
(5508-MC) >
(5508-MC) >*DHCP Socket Task: May 19 13:36:44.259: 00:17:7c:2f:b6:9a DHCP received
op BOOTREQUEST (1) (len 314,vlan 0, port 1, encap 0xec07)
*DHCPSocket Task: May 19 13:36:44.259: 00:17:7c:2f:b6:9a DHCP (encap type 0xec07)
mstype 3fff:ff:ff:ff:ff:ff
*DHCPSocket Task: May 19 13:36:44.259: 00:17:7c:2f:b6:9a DHCP selecting relay 1 -
control block settings:
    dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
    dhcpGateway: 0.0.0.0, dhcpRelay: 0.0.0.0 VLAN: 0
*DHCPSocket Task: May 19 13:36:44.259: 00:17:7c:2f:b6:9a DHCP selected relay 1 -
60.60.60.251 (local address 60.60.60.2, gateway 60.60.60.251, VLAN 60, port 1)
*DHCPSocket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP transmitting DHCP
REQUEST (3)
*DHCPSocket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP op: BOOTREQUEST,
htype: Ethernet, hlen: 6, hops: 1
*DHCPSocket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP xid: 0xad00ada3
(2902502819), secs: 3072, flags: 0
*DHCPSocket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP chaddr:
00:17:7c:2f:b6:9a
*DHCPSocket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP ciaddr: 0.0.0.0,
yiaddr: 0.0.0.0
*DHCPSocket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP siaddr: 0.0.0.0,
giaddr: 60.60.60.2
*DHCPSocket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP requested ip:
60.60.60.11
*DHCPSocket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP sending REQUEST to
60.60.60.251 (len 358, port 1, vlan 60)
*DHCPSocket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP selecting relay 2 -
control block settings:
    dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
    dhcpGateway: 0.0.0.0, dhcpRelay: 60.60.60.2 VLAN: 60
*DHCPSocket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP selected relay 2 -
NONE (server address 0.0.0.0,local address 0.0.0.0, gateway 60.60.60.251, VLAN 60,
port 1)
*DHCPSocket Task: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP received op BOOTREPLY
(2) (len 308,vlan 60, port 1, encap 0xec00)
*DHCPSocket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP setting server from ACK
(server 60.60.60.251, yiaddr 60.60.60.11)
*DHCPSocket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP transmitting DHCP
ACK (5)
*DHCPSocket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP op: BOOTREPLY, htype:
Ethernet, hlen: 6, hops: 0
*DHCPSocket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP xid: 0xad00ada3
(2902502819), secs: 0, flags: 0
*DHCPSocket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP chaddr:
00:17:7c:2f:b6:9a
*DHCPSocket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP ciaddr: 0.0.0.0,
yiaddr: 60.60.60.11
*DHCPSocket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP siaddr: 0.0.0.0,
giaddr: 0.0.0.0
*DHCPSocket Task: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP server id:
192.168.200.1 rcvd server id: 60.60.60.251
*webauthRedirect: May 19 13:36:47.678: 0:17:7c:2f:b6:9a- received connection

*webauthRedirect: May 19 13:36:47.680: captive-bypass detection disabled, Not
checking for wispr in HTTP GET, client mac=0:17:7c:2f:b6:9a
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Preparing redirect
URL according to configured Web-Auth type
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Checking custom-web
config for WLAN ID:4
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- unable to get the hostName
for virtual IP, using virtual IP =192.168.200.1
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Global status is enabled,
checking on web-auth type
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Web-auth type Internal,
no further redirection needed. Presenting default login page to user
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- http_response_msg_body1
is <HTML><HEAD><TITLE> Web Authentication Redirect</TITLE><META http-equiv=

```

```

"Cache-control" content="no-cache"><META http-equiv="Pragma" content="n
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- http_response_msg_body2
is "></HEAD></HTML>

*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- parser host is
www.facebook.com
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- parser path is /
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- added redirect=,
URL is now https://192.168.200.1/login.html?
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- str1 is now
https://192.168.200.1/login.html?redirect=www.facebook.com/
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- clen string is
Content-Length: 312

*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Message to be sent is
HTTP/1.1 200 OK
Location: https://192.168.200.1/login.html?redirect=www.facebook.com/
Content-Type: text/html
Content-Length: 312

<HTML><HEAD
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- send data length=448
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Web-auth type External,
but unable to get URL
*webauthRedirect: May 19 13:36:47.681: 0:17:7c:2f:b6:9a- received connection

*emWeb: May 19 13:36:48.731: SSL Connection created for MAC:0:17:7c:2f:b6:9a

*webauthRedirect: May 19 13:36:51.795: 0:17:7c:2f:b6:9a- received connection

*webauthRedirect: May 19 13:36:51.795: captive-bypass detection disabled, Not
checking for wispr in HTTP GET, client mac=0:17:7c:2f:b6:9a
*webauthRedirect: May 19 13:36:51.795: 0:17:7c:2f:b6:9a- Preparing redirect URL
according to configured Web-Auth type
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- Checking custom-web
config for WLAN ID:4
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- unable to get the hostName
for virtual IP, using virtual IP =192.168.200.1
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- Global status is enabled,
checking on web-auth type
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- Web-auth type Internal,
no further redirection needed. Presenting default login page to user
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- http_response_msg_body1
is <HTML><HEAD><TITLE> Web Authentication Redirect</TITLE><META http-equiv=
"Cache-control" content="no-cache"><META http-equiv="Pragma" content="n
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- http_response_msg_body2
is "></HEAD></HTML>

*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- parser host is
www.facebook.com
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- parser path is
/favicon.ico
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- added redirect=, URL is
now https://192.168.200.1/login.html?
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- str1 is now
https://192.168.200.1/login.html?redirect=www.facebook.com/favicon.ico
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- clen string is
Content-Length: 323

*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- Message to be sent is
HTTP/1.1 200 OK
Location: https://192.168.200.1/login.html?redirect=www.facebook.com/favicon.ico
Content-Type: text/html
Content-Length: 323

*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- send data length=470
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- Web-auth type External,
but unable to get URL
*DHCp Socket Task: May 19 13:37:03.905: 00:17:7c:2f:b6:9a DHCP received op
BOOTREQUEST (1) (len 308,vlan 0, port 1, encap 0xec07)
*DHCp Socket Task: May 19 13:37:03.905: 00:17:7c:2f:b6:9a DHCP (encap type 0xec07)

```

```
mstype 3ff:ff:ff:ff:ff:ff
*DHCPSocketTask: May 19 13:37:03.905: 00:17:7c:2f:b6:9a DHCP selecting relay 1 -
control block settings:
    dhcpServer: 60.60.60.251, dhcpNetmask: 255.255.255.0,
    dhcpGateway: 60.60.60.251, dhcpRelay: 60.60.60.2 VLAN: 60

*emWeb: May 19 13:38:35.187:
ewaURLHook: Entering:url=/login.html, virtIp = 192.168.200.1, ssl_connection=1,
secureweb=1

*emWeb: May 19 13:38:35.199: WLC received client 0:17:7c:2f:b6:9a request for
Web-Auth page /login.html
*emWeb: May 19 13:38:35.199: WLC received client 0:17:7c:2f:b6:9a request for
Web-Auth page /login.html
*emWeb: May 19 13:38:47.215:
ewaURLHook: Entering:url=/login.html, virtIp = 192.168.200.1, ssl_connection=1,
secureweb=1

*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a Username entry (surbg)
created for mobile, length = 5
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a Username entry (surbg)
created in mscb for mobile, length = 5
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_REQD
(8) Change state to WEBAUTH_NOL3SEC (14) last state WEBAUTH_REQD (8)

*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a apfMsRunStateInc
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_NOL3SEC
(14) Change state to RUN (20) last state WEBAUTH_NOL3SEC (14)

*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a Session Timeout is 0 -
not starting session timer for the mobile
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a 60.60.60.11 RUN (20)
Reached PLUMBFASPATH: from line 6605
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a 60.60.60.11 RUN (20)
Replacing Fast Path rule
    type = Airespace AP Client
    on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
    IPv4 ACL ID = 255, IPv6 ACL ID =
```




CHAPTER 24

VideoStream Troubleshooting

This document describes how to troubleshoot VideoStream issues on Wireless LAN Controllers(WLC).

- [Prerequisites, page 275](#)
- [Overview of the VideoStream flow through WLC, page 275](#)
- [Troubleshooting the Videostream Issues, page 277](#)

Prerequisites

We recommend that you have knowledge on Cisco Aironet 3600 Series Access Point (AP).



Note

Refer to the [Configuring VideoStream GUI](#) section of the **VideoStream Configuration Guide Cisco IOS XE Release 3SE Cisco 3850 Series Catalyst Switch** for more information about VideoStream configuration.

Supported Platforms and Releases

This document is based on Cisco Aironet 3600 Series Access Point (AP) that runs in lightweight mode.



Note

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Overview of the VideoStream flow through WLC

This section describes an overview of the VideoStream flow through WLC and its present limitations.

VideoStream Limitations

VideoStream enables the wireless architecture to deploy multicast video streaming across the enterprise to wireless clients. The present multicast video delivery mechanism has two limitations:

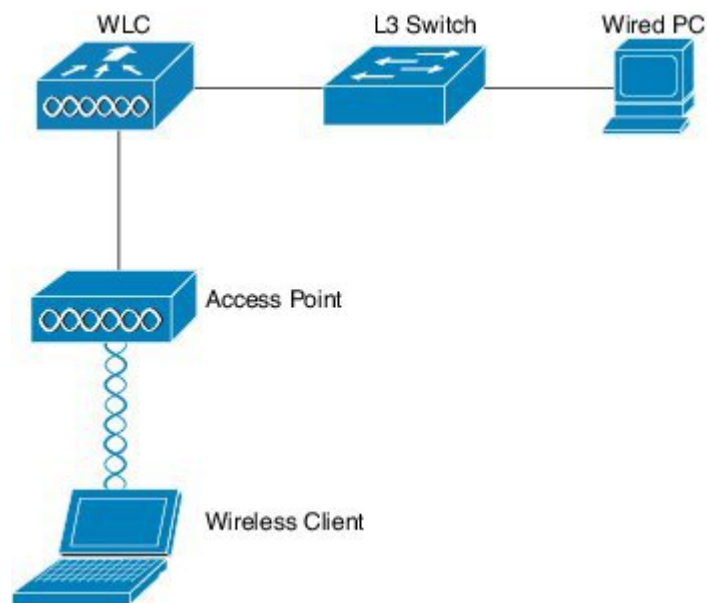
- Video packets are sent at much lower data rate, though multicast packets have highest data rate (802.11n data rate).
- Multicast packets are not acknowledged since there are multiple recipients and it is not scalable to receive acknowledgements from every client.

In order to overcome above listed limitations, VideoStream sends the video multicast packets as unicast packets over the air. With this process, an AP can use the individual data rate for each client and allows the client to acknowledge any packets that are not received

VideoStream Flow Through the WLC

The following network diagram illustrates the VideoStream flow through the WLC:

Figure 97: Network diagram of VideoStream flow through the WLC



Topology information for this setup are:

- The client MAC address is **0017.7c2f.b86e**
- The multicast video IP address is **198.51.100.10**
- Multicast with unicast is used as the multicast delivery mechanism to the AP.

The following steps describes flow of VideoStream:

- 1 The client sends an Internet Group Management Protocol (IGMP) join message where the WLC intercepts.
- 2 A WLC then creates a Mapping Group Identification (MGID) entry in order to map the flow with the client request and associated VLAN.
- 3 One of the main aspects of VideoStream that differs from regular multicast traffic is that, a WLC checks with AP to verify it has enough bandwidth required to serve the flow of VideoStream by sending Radio Resource Control (RRC) messages.
- 4 The RRC response from an AP informs the WLC, the availability of AP's bandwidth and other related statistics.
- 5 Based on the response from an AP, the WLC decides to admit the flow and sends the IGMP join message upstream. You can configure the WLC in such a way that, it forwards the flow of video streams even if there is not enough bandwidth on the AP. However, WLC marks the flow of video stream for the best effort queue or may use default action, which will not allow the stream and drop the IGMP join message.
- 6 The WLC tells the AP that the flow is acknowledged and indicates the amount of bandwidth that must be reserved for flow.
- 7 The WLC also informs the AP about WLAN-MGID mapping for the client.
- 8 The AP then keeps track of the amount of bandwidth utilized by client and bandwidth remains for each radio. This information is used when we add further streams.
- 9 When the WLC receives the multicast traffic that is destined to the client, it verifies that the VideoStream is configured and there is an MGID entry already created.
- 10 If both configuration of VideoStream and MGID entry are satisfied, then WLC forwards the streams to all of the APs that have clients which requested flow. Depending on the delivery mechanism configured, the WLC delivers the multicast streams to the APs with either *Multicast with Unicast* or *Multicast with Multicast*.
- 11 The AP replaces the destination address with a unicast address and sends the stream via unicast to each client that requests the flow. The packets include an AF41 DSCP mark (802.1p value of 4) and are sent at the data rate that is used for each individual client.

Troubleshooting the Videostream Issues

Follow the information on this section to troubleshoot the VideoStream flow through the WLC.

Verify that Multicast Direct is Enabled

To verify the multicast direct is enabled on the WLC, enter the following command:

```
Device# show wireless media-stream multicast-direct state
Multicast-direct State: Enabled
```

You can also use the **show wireless media-stream group summary** command in order to verify whether a specific multicast address is enabled:

```
Device# show wireless media-stream group summary
Number of Groups : 1

Stream Name      Start IP      End IP      Status
```

```
-----
video_stream 198.51.100.10 198.51.100.10 Enabled
```

**Note**

You must enable mutlicast-direct globally on both WLC and Wireless LAN (WLAN).

Enable Debugging on the WLC

To verify the RRC is negotiated correctly and the media stream is allowed, enable debugging on the WLC. The following are the most useful debug commands:

- **debug media-stream errors** - Command provides information about any errors that occur in the media stream process.
- **debug media-stream event** - Command provides information about the various state changes that occur.
- **debug media-stream rrc** - Command provides information about the RRC messages that are exchanged.
- **debug call-admission wireless all** - Command provides information with respect to Command Access Card (CAC) debugs.
- **debug ip igmp group_address** - Command provides information about the join process.

Example Debug Command Outputs

- The controller initially creates an MGID entry for the client once it sends an IGMP join message:

```
*May 7 22:42:23.632: %IOSXE-7-PLATFORM: 1
process wcm: mscbApMac = dca5.f4ec.df30 client_mac_addr = 0017.7c2f.b86e
slotId = 0 vapId = 2 mgid = 4161 numOfSGs = 2
rrc_status = 3
*May 7 22:42:23.632: %IOSXE-7-PLATFORM: 1
process wcm: 0017.7c2f.b86e mc2uc update client 0017.7c2f.b86e radio dca5.f4ec.df30
destIp 198.51.100.10 srcIp 0.0.0.0 mgid 4161 slot 0 vapId 2 vlan 12
```

- Once complete, the WLC understands that this particular multicast IP address is configured for media-streaming and begins the RRC process:

```
*May 7 22:42:23.632: %IOSXE-7-PLATFORM: 1
process wcm: msPolicyGetRrcQosSupport 1 4 4
*May 7 22:42:23.632: %IOSXE-7-PLATFORM: 1 process wcm:
msPolicyPlatform not AP 1100
*May 7 22:42:23.632: %IOSXE-7-PLATFORM: 1 process wcm:
0017.7c2f.b86e mc2uc qos admit 1 qos 4 pri 4
*May 7 22:42:23.632: %IOSXE-7-PLATFORM: 1 process wcm:
0017.7c2f.b86e mc2uc submit client client
0017.7c2f.b86e radio dca5.f4ec.df30 destIp
198.51.100.10 mgid 4161vapId 2 vlan 12
*May 7 22:42:23.632: %IOSXE-7-PLATFORM: 1 process wcm:
0017.7c2f.b86e FindRequestByClient not found dest
239.1.1.1 client 0017.7c2f.b86e radio dca5.f4ec.df30
source 0.0.0.0 slot 0
*May 7 22:42:23.632: %IOSXE-7-PLATFORM: 1 process wcm:
dca5.f4ec.df30 Creating request 3611 for radio
dca5.f4ec.df30
*May 7 22:42:23.632: %IOSXE-7-PLATFORM: 1 process wcm:
0017.7c2f.b86e Creating request 3611 for client
0017.7c2f.b86e
```

- The WLC then sends the RRC request:

```
*May 7 22:42:23.632: %IOSXE-7-PLATFORM: 1 process wcm:
  rrcEngineInsertAdmitRequest dest 239.1.1.1 mgid 4161
  request 3611
*May 7 22:42:23.632: %IOSXE-7-PLATFORM: 1 process wcm:
  0017.7c2f.b86e rrcEngineSendMeasureMetricsRequest sent
  request 3611 to radio dca5.f4ec.df30,
  minRate = 6000, maxRetryPercent = 80
```



Note Output shows that the WLC specifies the metrics that are necessary for the flow.

- The AP and the WLC now perform various checks before the stream is permitted. This check is performed in order to verify whether the maximum number of streams are reached or not:

```
*May 7 22:42:23.637: %IOSXE-7-PLATFORM: 1 process wcm:
  rrcEngineFindRequest look for request 3611
*May 7 22:42:23.637: %IOSXE-7-PLATFORM: 1 process wcm:
  rrcEngineFindRequest found request 3611
*May 7 22:42:23.638: %IOSXE-7-PLATFORM: 1 process wcm:
  dca5.f4ec.df30 rrcEngineProcessRadioMetrics start
  radio dca5.f4ec.df30 request 3611
*May 7 22:42:23.638: %IOSXE-7-PLATFORM: 1 process wcm:
  dca5.f4ec.df30 done rrcEngineProcessRadioMetrics
  radio dca5.f4ec.df30 request 3611
*May 7 22:42:23.643: %IOSXE-7-PLATFORM: 1 process wcm:
  rrcEngineRemoveAdmitRequest request 3611
*May 7 22:42:23.643: %IOSXE-7-PLATFORM: 1 process wcm:
  p_video = 0, p_voice = 0, pb = 476, video_qo = 0,
  video_l_r_ratio = 0, video_no = 0
*May 7 22:42:23.643: %IOSXE-7-PLATFORM: 1 process wcm:
  video_delay_hist_severe = 0, video_pkt_loss_discard =
  0, video_pkt_loss_fail = 0
*May 7 22:42:23.643: %IOSXE-7-PLATFORM: 1 process wcm:
  radio_tx_q_max_size = 1, radio_tx_q_limit = 5684,
  vi_tx_q_max_size = 0, current_rate = 52
*May 7 22:42:23.643: %IOSXE-7-PLATFORM: 1 process wcm:
  msPolicyGetStreamParameters streamName video_stream
  bandwidth 1000 pakSize 1200
*May 7 22:42:23.643: %IOSXE-7-PLATFORM: 1 process wcm:
  0017.7c2f.b86e Admit video: number of streams on
  radio is 0, number of streams on client is 0
```

- The following check is performed in order to verify whether the packet loss for the video queue has crossed the threshold or not:

```
*May 7 22:42:23.643: %IOSXE-7-PLATFORM: 1 process wcm:
  0017.7c2f.b86e Checking Link Stats for AP
  dca5.f4ec.df30(0) : pkt_loss = 0, video_pps = 0
*May 7 22:42:23.643: %IOSXE-7-PLATFORM: 1 process wcm:
  0017.7c2f.b86e pkt_discard = 0, num_video_streams = 0
*May 7 22:42:23.643: %IOSXE-7-PLATFORM: 1 process wcm:
  0017.7c2f.b86e Link Stats Criteria PASSED for AP
  dca5.f4ec.df30(0)
```

- Verification of bandwidth on the AP is performed by following check

```
*May 7 22:42:23.643: %IOSXE-7-PLATFORM: 1 process wcm:
  0017.7c2f.b86e Requested Video Media Time for AP
  dca5.f4ec.df30(0) : cfg_stream_bw = 1000 kbps
*May 7 22:42:23.643: %IOSXE-7-PLATFORM: 1 process wcm:
  0017.7c2f.b86e current_rate = 26 Mbps, new_stream_pps
  = 104 pps, video_pkt_size = 1200 bytes => req_mt
  = 3354 MT
*May 7 22:42:23.643: %IOSXE-7-PLATFORM: 1 process wcm:
```

```

0017.7c2f.b86e RRC Video BW Check for AP
dca5.f4ec.df30(0) : current chan/voice/video MT =
14875/0/0 MT
*May 7 22:42:23.643: %IOSXE-7-PLATFORM: 1 process wcm:
0017.7c2f.b86e mt remain 16375 readmit_bias 0
current_video_mt 0 media_time_req 3354
video_mt_limit 15625

```

- Once all of the criteria are passed, then stream is admitted. The **SNMP admit trap** is sent in order to inform that the media stream is permitted, which is useful in cases where the SNMP is used to monitor the streams that are allowed.

```

*May 7 22:42:23.643: %IOSXE-7-PLATFORM: 1 process wcm:
0017.7c2f.b86e Video Stream Admitted: passed all
the checks
*May 7 22:42:23.643: %IOSXE-7-PLATFORM: 1 process wcm:
0017.7c2f.b86e Mapping wme code 1 to history code 0
*May 7 22:42:23.643: %IOSXE-7-PLATFORM: 1 process wcm:
0017.7c2f.b86e Admit video: request 3611 radio
dca5.f4ec.df30, decision 1 admission 2
*May 7 22:42:23.643: %IOSXE-7-PLATFORM: 1 process wcm:
mStreamBandMc2ucAdmit besteffort 1
*May 7 22:42:23.643: %IOSXE-7-PLATFORM: 1 process wcm:
0017.7c2f.b86e Approve Admission on radio
dca5.f4ec.df30 request 3611 vlan 12 destIp
198.51.100.10 decision 1 qos 4 admitBest 1
*May 7 22:42:23.643: %IOSXE-7-PLATFORM: 1 process wcm:
0017.7c2f.b86e RRC Admission: Add history record with
cause code 0 destIp 198.51.100.10
*May 7 22:42:23.643: %IOSXE-7-PLATFORM: 1 process wcm:
0017.7c2f.b86e Sending SNMP admit trap

```

- The stream information is now added to the WLC database, and the Quality of Service (QoS) value is set for the video stream:

```

*May 7 22:42:23.643: %IOSXE-7-PLATFORM: 1 process wcm:
bcastRrcHandleClientStatus: group = 239.1.1.1
clientmac = 0017.7c2f.b86eapmac = dca5.f4ec.df30
vlanId = 12 status = 2 qos = 4 mgid = 4161
*May 7 22:42:23.643: %IOSXE-7-PLATFORM: 1 process wcm:
0017.7c2f.b86e RRC clientRecord add clientMac
0017.7c2f.b86e #of streams 1
*May 7 22:42:23.643: %IOSXE-7-PLATFORM: 1 process wcm:
0017.7c2f.b86e RadioInsertStreamRecord # of streams
is 1 on radio dca5.f4ec.df30
*May 7 22:42:23.643: %IOSXE-7-PLATFORM: 1 process wcm:
0017.7c2f.b86e Recording request 3611 destIp
198.51.100.10 qos 4 vlan 12 violation-drop 1 priority 4
sourceIp 0.0.0.0 client 0017.7c2f.b86e radio
dca5.f4ec.df30 slotId 0
*May 7 22:42:23.643: %IOSXE-7-PLATFORM: 1 process wcm:
0017.7c2f.b86e done rrcEngineProcessClientMetrics
client 0017.7c2f.b86e radio dca5.f4ec.df30 request
3611
*May 7 22:42:23.643: %IOSXE-7-PLATFORM: 1 process wcm:
locking mgid Tree in file bcast_process.c line 1988
*May 7 22:42:23.643: %IOSXE-7-PLATFORM: 1 process wcm:
unlocking mgid Tree in file bcast_process.c line 2096
*May 7 22:42:23.643: %IOSXE-7-PLATFORM: 1 process wcm:
spamLradSendMgidInfo: ap = dca5.f4ec.df30 slotId = 0,
apVapId = 2, numOfMgid = 1 mc2ucflag = 1, qos = 4

```

- The WLC forwards the IGMP join message upstream and updates the other components:

```

*May 7 22:42:23.645: (l2mcsn_process_report) Allocating MGID for Vlan:
12 (S,G): :239.1.1.1
*May 7 22:42:23.645: (l2mcast_wireless_alloc_mcast_mgid) Vlan: 12 Source:
0.0.0.0 Group: 239.1.1.1
*May 7 22:42:23.645: (l2mcast_wireless_alloc_mcast_mgid) Source: 0.0.0.0

```

```

Group: 239.1.1.1 Vlan: 12 Mgid: 4161
*May 7 22:42:23.645: (l2mcast_wireless_track_and_inform_client) Protocol:
IGMPSN Client-address: 10.105.132.254 (S,G,V): 0.0.0.0 239.1.1.1 12 Port:
Ca0, MGID: 4161 Add: Add
*May 7 22:42:25.399: IGMP(0): Set report delay time to 0.2 seconds for
239.1.1.1 on Vlan12

```

Verify the MGID Entries on the WLC

- Enter the following **show wireless multicast group summary** command in order to verify the MGID entries that form:

```
Device# show wireless multicast group summary
```

```

IPv4 groups
-----
MGID      Source      Group          Vlan
-----
4160      0.0.0.0    198.51.100.10 12

```

- In order to receive more details about the clients that are associated with a specific MGID entry, enter the **show wireless multicast group group_address vlan vlan_id** command:

```

Device# show wireless multicast group 239.1.1.1 vlan 12
Source : 0.0.0.0
Group  : 239.1.1.1
Vlan   : 12
MGID   : 4160

```

```
Number of Active Clients : 1
```

```
Client List
```

```

Client MAC Client IP Status
-----
0017.7c2f.b86e 10.105.132.254 MC2UC_ALLOWED

```

- In order to verify the specific MGID information on the AP, enter the **show capwap mcast mgid id 4161** command:

```

Device# show capwap mcast mgid id 4161
rx pkts = 6996
tx packets:
wlan : 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
slots0 : 0 6996 0 0 0 0 0 0 0 0 0 0 0 0 0 0
slots1 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
slots2 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

Normal Mcast Clients:
Reliable Mcast Clients:
Client: 0017.7c2f.b86e --- SlotId: 0 WlanId: 1 --- Qos User Priority: 4
State: ADMITTED
History - Retry Pct: 6 5 13 10 Rate (500 Kbps): 116 116 116 116

```



Note

This output shows that the client is added to the **Reliable Mcast Clients** list with a QoS priority of 4.

Troubleshooting of Video Quality on the AP

When video quality issues are reported, you can verify following data on the AP in order to troubleshoot:

- Enter the **show controller dot11radio 0 txq** command in order to view the video transmit queue statistics on the AP:

```
Device# show controller dot11radio 0 txq
(Output clipped)
----- Active ----- In-Progress ----- Counts -----
Cnt      Quo Bas Max Cl Cnt Quo Bas Sent Discard Fail Retry Multi
Uplink   0   64 0   0 0 0   5   0   0   0   0   0
Voice    0  512 0   0 0 60  0 3350 0   2   6   0
Video    0 1024 0   0 0 200 50406 0   0   878 2589
Best     0 1024 0   0 0 200 126946 0   0 20780 5170
```

It is important to take note of the video queue statistics. You must compare the number of packets that are transmitted with the number of packets that are retried due to failed transmissions.

- Enter the **show controller dot11radio 0 client** command in order to view the parameters for a specific client

```
Device# show controller dot11radio 0 client

RxPkts KBytes Dup Dec Mic TxPkts KBytes Retry RSSI SNR
0017.7c2f.b86e 99600 24688 1276 0 0 168590 157253 341 46 46
```

- With the **show controller dot11radio 0** command output, you can also view the video transmission metrics. Take note of the number of successful and failed transmissions and Q-drops that appear in each sampling period:

```
Dot11 Current Video Transmission Metrics:
Arrivals:106 Q-Drops:0 Tries:129 Agg:129 Success:106 Fail:0

Dot11 5-second Video Transmission Metrics:
Arrivals:147 Tries:195 Agg:195 Success:147 Fail:0
Radio-Q-Peak:9 Video-Q-Peak:32 Video-Q-Drops:0
Delay - Tot Msec:1392 10/20/40/40+ Msec:136/15/12/6

Dot11 1-second Video Transmission Metrics:
Q-util:71 max-tx-time:22 p-chan:483 p-video:8 L/r:18911
```

Flow Denied by the WLC

This section describes the process that occurs when there is insufficient bandwidth to permit a stream. The WLC verifies the stream requirement against the configured limits and denies the stream:

```
May 8 10:29:36.890: %IOSXE-7-PLATFORM: 1 process wcm: 0017.7c2f.b86e
RRC Video BW Check for AP dca5.f4ec.df30(0) : current
chan/voice/video MT = 16563/0/0 MT
May 8 10:29:36.890: %IOSXE-7-PLATFORM: 1 process wcm: 0017.7c2f.b86e
mt remain 14687 readmit_bias 0 current_video_mt 0 media_time_req
2392 video_mt_limit 1562
May 8 10:29:36.890: %IOSXE-7-PLATFORM: 1 process wcm: 0017.7c2f.b86e
RRC Video BW Check Failed: Insufficient Video BW for AP
dca5.f4ec.df30(0)
May 8 10:29:36.890: %IOSXE-7-PLATFORM: 1 process wcm: 0017.7c2f.b86e
Video Stream Rejected. Bandwidth constraint.
May 8 10:29:36.890: %IOSXE-7-PLATFORM: 1 process wcm: 0017.7c2f.b86e
Mapping wme code 8 to history code 1
May 8 10:29:36.890: %IOSXE-7-PLATFORM: 1 process wcm: 0017.7c2f.b86e
Deny Admission on radio dca5.f4ec.df30 request 3633 destIp
```

```
198.51.100.10 vlan 12
```



Note For test purposes, the maximum bandwidth allowed for video streaming is changed to 1,000 Kbps in this example.

Similar messages appear when the flow is denied due to any other reason, and the WLC also sends an SNMP trap:

```
May 19 10:29:36.890: %IOSXE-7-PLATFORM: 1 process wcm: 0017.7c2f.b86e  
Sending SNMP deny trap
```



Custom Web Authentication Locally Hosted on WLC or an External Server

This document provides information on custom Web Authentication that is locally hosted on a Wireless LAN Controller (WLC) or an External server, such as, Identity Services Engine (ISE).

- [Configuring Custom Web Authentication Locally Hosted on WLC, page 285](#)
- [Configuring the Custom HTML pages, page 286](#)

Configuring Custom Web Authentication Locally Hosted on WLC

The configuration for a Custom Web Authentication that is locally hosted on the WLC is similar to the Local Web Authentication and Local Web Authentication with External RADIUS Authentication. However, to configure a Custom Web Authentication, in addition to the above mentioned configuration methods, you need to download the custom page on flash and point the parameter map to use the custom pages.



Note

For more information on Custom Web Authentication that is locally hosted on WLC and Local Web Authentication with External RADIUS Authentication, refer to the following:

- Web Authentication on Converged Access-Local Web Authentication.
- Web Authentication on Converged Access - Local Web Authentication with External RADIUS Authentication

To download the custom page on flash and point the parameter map to use the custom pages, use the following commands:

```
parameter-map type webauth WEBAUTH
 type webauth
 custom-page login device flash:webauth_login.html
 custom-page login expired device flash:webauth_expire.html
 custom-page failure device flash:webauth_fail.html
 custom-page success device flash:webauth_success.html
```

**Note**

To use the Custom Web Authentication locally, define a custom page for the login page, expire page, login - success page, and login - fail page.

Configuring the Custom HTML pages

Web Authentication for Login Page

To configure the web authentication for the login page, use the following:

```
<HTML><HEAD><TITLE>Authentication Proxy Login Page</TITLE>
<script type="text/javascript">
var pxypromptwindow1;
var pxysubmitted = false;
function submitreload() {
    if (pxysubmitted == false) {
        pxypromptwindow1=window.open('', 'pxywindow1',
'resizable=no,width=350,height=350,scrollbars=yes');
        pxysubmitted = true;
        return true;
    } else {
        alert("This page can not be submitted twice.");
        return false;
    }
}
</script>
</HEAD>
<BODY>
<H1>Cisco Systems</H1><H2>Web Authentication</H2>
<FORM method=post action="/" target="pxywindow1">
    Username: <input type=text name=uname><BR><BR>
    Password: <input type=password name=pwd><BR><BR>
    <input type=submit name=ok value=OK    onClick="return submitreload();">
</FORM><noscript>
<BR>
<UL>
    <H2><FONT COLOR="red">Warning!</FONT></H2>
    <p>JavaScript should be enabled in your Web browser
        for secure authentication</p>
    <LI>Follow the instructions of your Web browser to enable
        JavaScript if you would like to have JavaScript enabled
        for secure authentication</LI>
    <BR><OR><BR><BR>
    <LI> Follow these steps if you want to keep JavaScript
        disabled or if your browser does not support JavaScript
        <OL><BR>
            <LI> Close this Web browser window</LI>
            <LI> Click on Reload button of the original browser window</LI>
        </OL></LI>
</UL>
</noscript></BODY></HTML>
```

Web Authentication for Success Page

To configure the web authentication for success page, use the following:

```
<HTML><HEAD>
<TITLE>Authentication Proxy Success Page</TITLE>
<script type="text/javascript">
    var donesubmitted = false;
    function DoneButton() {
        if (donesubmitted == false) {
            donesubmitted = true;
```

```

        window.opener.location.reload();
        window.close();
    }
    setTimeout("DoneButton()", 5000);
</script>
</HEAD>
<BODY>
<H1>Cisco Systems</H1><H2>Web Authentication</H2>
<p>Authentication Successful !</p>
<FORM>
  <input type=button name=enter value=DONE onClick="DoneButton();">
</FORM>
<noscript>
<BR>
<UL>
  <H2><FONT COLOR="red">Warning!</FONT></H2>
  <p>JavaScript should be enabled in your Web browser
    for secure authentication</p>
  <LI>Follow the instructions of your Web browser to enable
    JavaScript if you would like to have JavaScript enabled
    for secure authentication</LI>
  <BR>OR<BR><BR>
  <LI> Follow these steps if you want to keep JavaScript
    disabled or if your browser does not support JavaScript
    <OL><BR>
      <LI> Close this Web browser window</LI>
      <LI> Click on Reload button of the original browser window</LI>
    </OL></LI>
</UL>
</noscript></BODY></HTML>

```

Web Authentication for Failure page

To perform the web authentication for failure page, use the following:

```

<HTML><HEAD>
<TITLE>Authentication Proxy Failed Page</TITLE>
<script type="text/javascript">
  var donesubmitted = false;
  function DoneButton() {
    if (donesubmitted == false) {
      donesubmitted = true;
      window.opener.location.reload();
      window.close();
    }
  }
</script>
</HEAD>
<BODY>
<H1>Cisco Systems</H1><H2>Web Authentication</H2>
<p>Authentication Failed !</p>
<FORM>
  <input type=button name=enter value=DONE onClick="DoneButton();">
</FORM>
<noscript>
<BR>
<UL>
  <H2><FONT COLOR="red">Warning!</FONT></H2>
  <p>JavaScript should be enabled in your Web browser
    for secure authentication</p>
  <LI>Follow the instructions of your Web browser to enable
    JavaScript if you would like to have JavaScript enabled
    for secure authentication</LI>
  <BR>OR<BR><BR>
  <LI> Follow these steps if you want to keep JavaScript
    disabled or if your browser does not support JavaScript
    <OL><BR>
      <LI> Close this Web browser window</LI>
      <LI> Click on Reload button of the original browser window</LI>
    </OL></LI>
</UL>

```

```
</UL>  
</noscript></BODY></HTML>
```



Wireless Converged Access Chromecast Configuration Example

Converged Access allow Wi-Fi networks to support wired connectivity and keep management of wired and wireless networks as simple as possible.



Note

This document is an expansion of the Chromecast Deployment Guide. Refer to the Chromecast Deployment Guide for more details on Converged Access configuration on AireOS WLCs.

- [Prerequisites, page 289](#)
- [Configuring Chromecast Support, page 290](#)

Prerequisites

- We recommend that you have basic knowledge on Cisco Catalyst 3850 Series, Cisco Catalyst 3650 Series, Cisco Catalyst 3560-CX Series, and Cisco 2960-CX Series Switches for Converged Access in Cisco IOS Release 3.6.x or later.



Tip Refer to Converged Access Consolidated Quick Reference Templates for information about the latest available Release Notes for Converged Access Release 3.6.x or later

- Ensure that Switch Virtual Interfaces (SVIs) and DHCP pools or snooping are pre-configured.

Supported Platforms and Releases

The information in this document is based on the following:

- Cisco Catalyst 3650 Series Switches
- Cisco Catalyst 3850 Series Switches

- Cisco Catalyst 4500Sup8E Series Switches

**Note**

The information in this document refers to devices in a specific lab environment. Descriptions of the devices are provided with default configuration values. If you are on a live network, you must understand the potential impact of all the commands.

Configuring Chromecast Support

Perform the following Global and WLAN configurations to launch Chromecast support on Cisco Catalyst 3850 Series, Cisco Catalyst 3650 Series, Cisco Catalyst 3560-CX Series, and Cisco 2960-CX Series Switches for Converged Access:

Configuring Wireless Multicast Globally

Perform the following tasks to configure wireless multicast globally:

-
- Step 1** To enable the Multicast Support feature, use the **wireless multicast** command.
- Step 2** To enable Internet Group Management Protocol (IGMP) snooping, use the **ip igmp snooping** and the **ip igmp snooping querier** commands.
- Step 3** To set the mode of wireless Access point (AP) and Control and Provisioning of Wireless Access Points CAPWAP multicast to multicast-multicast, use the **ap capwap multicast** command.

```
Device# configure terminal
Device(config)# wireless multicast
Device(config)# ip igmp snooping
Device(config)# ip igmp snooping querier
Device(config)# ap capwap multicast <Multicast IP - 239.x.x.x>
```

Note Do not use multicast-unicast for AP CAPWAP multicast mode.

- Step 4** To verify IGMP settings, use the **show ip igmp groups** command.
- Step 5** To verify wireless multicast details, use the **show wireless multicast** and the **show wireless multicast group summary** commands.
- Step 6** Tune the data rates for optimal performance.

Note The configuration and the data rates provided in the following examples must be tuned for optimal values as per the requirements.

The following is sample data rate configuration for 2.4 Ghz:

```
ap dot11 24ghz rate RATE_1M disable
ap dot11 24ghz rate RATE_2M disable
ap dot11 24ghz rate RATE_5_5M disable
ap dot11 24ghz rate RATE_6M disable
ap dot11 24ghz rate RATE_9M disable
```

```
ap dot11 24ghz rate RATE_11M disable
ap dot11 24ghz rate RATE_12M mandatory
ap dot11 24ghz rate RATE_18M supported
ap dot11 24ghz rate RATE_24M supported
ap dot11 24ghz rate RATE_36M supported
ap dot11 24ghz rate RATE_48M supported
ap dot11 24ghz rate RATE_54M supported
```

The following is the sample data rate configuration for 5 Ghz:

```
ap dot11 5ghz rate RATE_6M disable
ap dot11 5ghz rate RATE_9M disable
ap dot11 5ghz rate RATE_12M mandatory
ap dot11 5ghz rate RATE_18M supported
ap dot11 5ghz rate RATE_24M supported
ap dot11 5ghz rate RATE_36M supported
ap dot11 5ghz rate RATE_48M supported
ap dot11 5ghz rate RATE_54M supported
```

Note Use broadcast forwarding to enable IGMP snooping, if IGMP snooping cannot be enabled. Use the **wireless broadcast** command for broadcast forwarding. Alternatively, forward the broadcasts to a specific VLAN using the **wireless broadcast vlan** *VLAN ID* command.

Configuring WLAN

To configure the WLAN for Chromecast, perform the following steps:

Step 1 Enable the peer-to-peer blocking mode.

Step 2 Enable the support on multicast VLAN.

The following sample is an example for configuring WLAN using external RADIUS authentication, MAC-filter, and AAA-override:

```
aaa new-model
!
!
aaa group server radius ISE
server name ISE
!
aaa authentication dot1x ISE group ISE

radius server ISE
address ipv4 x.x.x.x auth-port 1645 acct-port 1646
key XXXXX

dot1x system-auth-control

wlan Chromecast <WLAN ID> Chromecast
```

```
aaa-override
mac-filtering ISE-
client vlan <VLAN ID>
no peer-blocking
ip multicast vlan <vlanid> // If using vlan select feature//
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security dot1x authentication-list ISE
session-timeout 1800
no shutdown
```

Note Depending on your WLAN security, choose the appropriate template.



Web Passthrough Configuration Example

This document describes how to configure the web passthrough feature on a Wireless LAN Controller (WLC).

- [Prerequisites, page 293](#)
- [Web Passthrough on WLC, page 294](#)
- [Configuring Web Passthrough on Wireless LAN Controller, page 294](#)
- [Verifying the Web Passthrough Configuration, page 301](#)
- [Troubleshooting Web Passthrough Configuration Issues, page 301](#)

Prerequisites

Ensure all the initial configurations are completed on the WLC.

Supported Platforms and Releases

The information in this document is based on the following:

- Cisco Catalyst 3850 Series Switch
- Cisco Aironet 3600 Series Lightweight Access Point
- Microsoft Windows 7 Native Wireless Supplicant



Note

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command

Web Passthrough on WLC

Web passthrough is a solution that is typically used for guest access. The process of web passthrough is similar to that of web authentication, except that no authentication credentials are required for web passthrough.

In web passthrough, wireless users are redirected to the usage policy page when they try to use the Internet for the first time. Once the users accept the policy, they can browse the Internet. This redirection to the policy page is handled by the WLC.

In this example, a VLAN interface is created on a separate subnet on the WLC. Then, a separate Wireless LAN (WLAN) or Service Set Identifier (SSID) or both is created and configured with web passthrough and it is mapped to VLAN interface created.

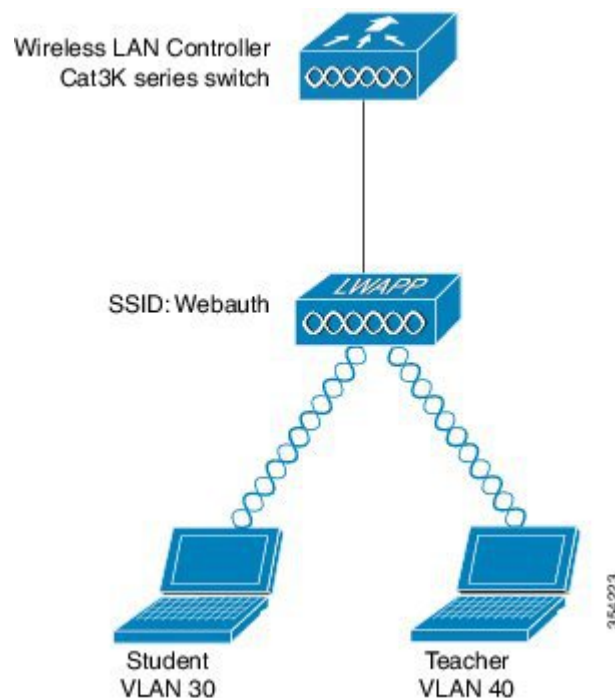

Note

Web passthrough does not provide any data encryption.

Configuring Web Passthrough on Wireless LAN Controller

The following figure shows the network diagram of the configuration:

Figure 98: Network Diagram



You can complete the configuration either using CLI or GUI.

Configuring Web Passthrough on Wireless LAN Controller using CLI

To configure DHCP snooping for the VLANs used for clients, use the following commands:

In the following example, **VLAN20** is used. The pool is configured on the same WLC. **TenGigabitEthernet 1/0/1** from Cisco Catalyst 3850 Series Switch connects to the uplink switch. If you have the DHCP server configured on the server beyond the WLC or on an external DHCP server, then you have to trust DHCP snooping and Relay information.

```
ip device tracking
ip dhcp snooping vlan 12,20,30,40
ip dhcp snooping
!
ip dhcp pool vlan20
network 20.20.20.0 255.255.255.0
default-router 20.20.20.1

interface Vlan20
ip address 20.20.20.1 255.255.255.0

interface TenGigabitEthernet1/0/1
switchport trunk native vlan 12
switchport mode trunk
ip dhcp relay information trusted
ip dhcp snooping trust

wlan webauth 4 webauth
client vlan 74
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list default
security web-auth parameter-map internal
no shutdown

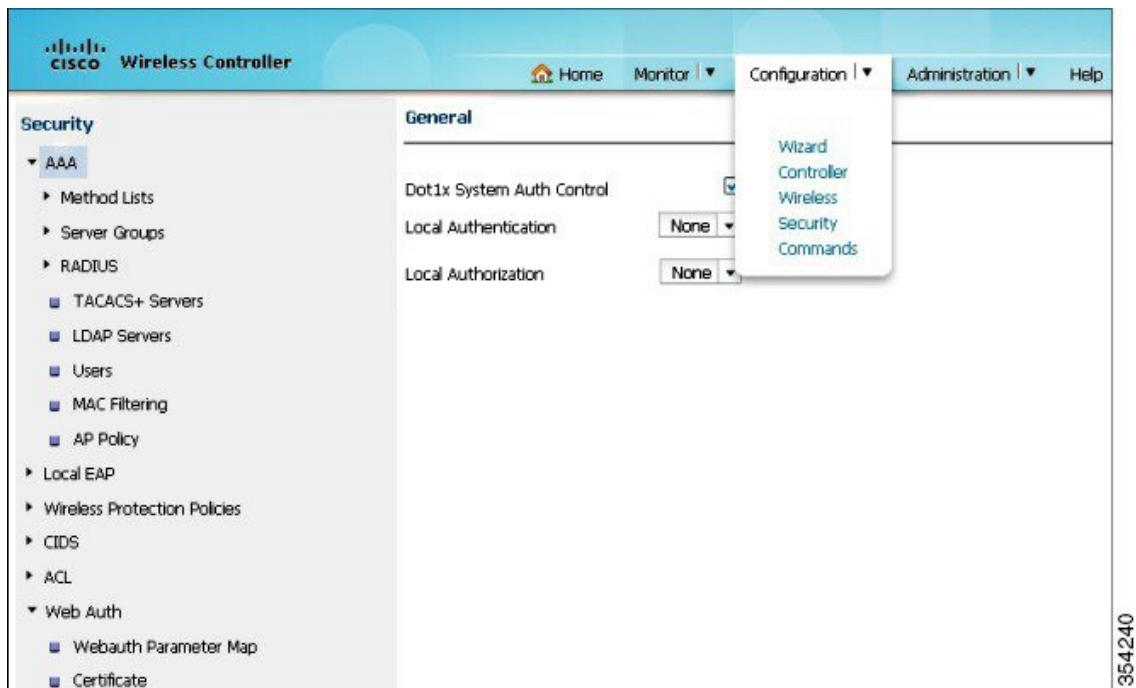
parameter-map type webauth global
virtual-ip ipv4 1.2.3.4
intercept-https-enable
parameter-map type webauth internal
type consent
```

Configuring Web Passthrough on Wireless LAN Controller (GUI)

Perform the following steps to configure the WLC on the GUI:

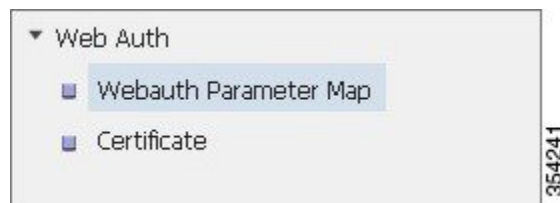
Step 1 To configure security, from the WLC GUI, navigate to **Navigation > Security**.

Figure 99: Configuring Security



Step 2 To choose **Webauth Parameter map**, on the bottom-right of the **Security** page, navigate to **Webauth > Webauth Parameter Map**.

Figure 100: Webauth Parameter Map



Step 3 Choose **global** for the default parameter map on **Webauth Parameter Map** screen.

Step 4 To configure the virtual IP address, navigate to **Webauth Parameter Map > Edit**.

Step 5 To make global parameter (Web passthrough) as consent, from the **Type** field drop-down list choose **Consent**.

Figure 101: Global Parameter as Consent

Webauth Parameter Map
Webauth Parameter Map > Edit

Parameter-map name: global

Banner: [Empty text area]

Maximum HTTP connections(1-200): 30

Timeout (1-65535 in minutes): 2

Type: consent

Turn-on Consent with Email:

Virtual IPv4 Address: 192.168.200.1

Virtual IPv4 hostname: [Empty text field]

354242

Note It is not mandatory to configure the global parameter map to consent.

Step 6 To create the parameter map, from the **Type** field drop-down list, choose **consent**. The configuration in the following figure uses **web** as the Parameter-map name, which is used under the WLAN for the users to access the Consent page.

Figure 102: Web Parameter Map

Webauth Parameter Map
Webauth Parameter Map > Edit

Parameter-map name: web

Banner: [Empty text area]

Maximum HTTP connections(1-200): 30

Timeout (1-65535 in minutes): 2

Type: consent

Turn-on Consent with Email:

354243

The following figure shows the parameter maps on the GUI:

Figure 103: Parameter Maps on the GUI

Webauth Parameter Map

New Remove

	Parameter-map name	Parameter-map type
<input type="checkbox"/>	global	Global
<input type="checkbox"/>	web	Named

354244

Step 7 To create a new WLAN, from the WLC GUI, navigate to **Configuration > Wireless > WLAN**. In the following figure, **Webauth** as the WLAN mapped to **VLAN20**.

Figure 104: Mapping Webauth to VLAN

WLAN
WLAN > Edit

General Security QOS AVC Advanced

Profile Name Webauth
Type WLAN
SSID Webauth
Status
Security Policies Web-Auth
(Modifications done under security tab will appear after applying the changes.)
Radio Policy All
Interface/Interface Group(G) VLAN0020
Broadcast SSID
Multicast VLAN Feature

354245

Step 8 Navigate to **WLAN > Edit > Security > Layer2**, and then choose **None** for Layer 2 Security:

Figure 105: Security for Layer 2

WLAN
WLAN > Edit

General Security QOS AVC Advanced

Layer2 Layer3 AAA Server

Layer 2 Security None
MAC Filtering
Fast Transition
Over the DS
Reassociation Timeout 20

354246

- Step 9** To choose the appropriate settings for **Webauth Parameter Map**, navigate to **WLAN > Edit > Security > Layer3**. For example, Web.

Figure 106: Webauth Parameter Map Settings

The screenshot shows the configuration page for a WLAN. The breadcrumb is 'WLAN > Edit'. There are tabs for 'General', 'Security', 'QOS', 'AVC', and 'Advanced'. Under the 'Security' tab, there are sub-tabs for 'Layer2', 'Layer3', and 'AAA Server'. The 'Layer3' sub-tab is selected. The configuration items are as follows:

Web Policy	<input checked="" type="checkbox"/>
Conditional Web Redirect	<input type="checkbox"/>
Webauth Profile	Local_webauth
Webauth Parameter Map	web
Webauth On-mac-filter Failure	<input type="checkbox"/>
Preauthentication IPv4 ACL	Unconfigured
Preauthentication IPv6 ACL	Unconfigured

354247

- Step 10** Save the configuration and it is ready to test.
- Step 11** A client receives the IP address, once you connect to the WLAN. When you access the internet or open the browser with the virtual IP address, the **Consent Login Page** displays. Click the **Accept** radio button.
- Note** If Domain Name Server (DNS) is configured, then any access to http / https results in Consent Login Page display.
- Step 12** Once you click Accept, the successful authentication page launches, which gives you the option to navigate to the requested page.
- Step 13** Once you click **Accept**, the successful authentication page launches, which gives you the option to navigate to the requested page

Client-side Capture

- Step 1** After the client receives the IP address, the client opens the browser, and types the virtual IP address.
- Note** If the DNS is configured properly, then there is no need to enter the virtual IP address on the browser.
- Step 2** Since WLC configuration does not use any webauth certifications, there are CERT errors in packet capture.

Step 3 After successful authentication, the client is in the **RUN** state on the WLC GUI.

Figure 107: RUN state on the WLC

The screenshot displays the 'Client' configuration page on a WLC GUI, showing the 'Client > Detail' view. The 'General' tab is selected, and the 'AVC Statistics' tab is also visible. The client is in the 'RUN' state, as indicated by the 'Policy Manager State' field.

Client Properties		AP Properties	
Mac Address	00:21:6A:89:51:CA	AP Address	CB:F9:F9:83:42:60
IPv4 Address	20.20.20.6	AP Name	SURBG-3602
IPv6 Address	None	AP Type	802.11n
User Name	0021.6a89.51ca	Wlan Profile	Webauth
Port Number	1	Status	Associated
Interface	VLAN0020	Association ID	1
Vlan ID	20	802.11 Authentication	Open System
CCX Version	4	Reason Code	1
EZE Version	1	Status Code	0
Mobility State	Local	CF Pollable	Not implemented
Policy Manager State	RUN	CF Pollable Request	Not implemented
Management Frame Protection	Disabled	Short Preamble	Not implemented
Uptime(sec)	33	PBCC	Not implemented
Power Save Mode	OFF	Channel Agility	Not implemented
Current TxRateSet	None	Fast BSS Transition	Not implemented
Data RateSet	6.0,9.0,12.0,18.0,24.0,36.0,48.0,54.0	FT Reassociation Timeout	20
		Session Timeout	1800
		WEP state	Disabled

Security Information		Client Statistics	
Security Policy Completed	Enabled	Bytes Received	0
Policy Type	N/A	Bytes Sent	0
Encryption Cypher	None	Packets Received	0
EAP type	Not Applicable	Packets Sent	0
SNMP Nac State	None	Policy Errors	0

354249

Verifying the Web Passthrough Configuration

There is no verification procedure available for this configuration.

Troubleshooting Web Passthrough Configuration Issues

Enter the debugs in following order to troubleshoot your configuration issues:

```
debug platform condition mac 48f8.b38a.f1b0
debug platform condition start
request platform software trace rotate all

debug ip http all
```

```

Device# debug ip admission all
All IP admission debugging is on

Device# show debugging
edi2#
Nov 25 03:52:57.525: IOSXE_INFRA_BIPC: Rcvd TPS bipc Status: Birth
Nov 25 03:52:57.525: TPS: BIPC channel brith
Nov 25 03:52:57.533: Enters in tps_ipc_msg_rcvd_handler
Nov 25 03:52:57.534: Queue Event buffer len = 90 ...
buffer content ...
BC FF FF FF FF FF FF 00 00 00 00 00 00 00 00 00
00 00 00 42 00 08 C0 00 00 00 00 3A 6E 7B 78 9E
A3 C5 BE 7D 02 BF 5A 66 B2 3F 9E A1 00 00 00 00
00 14 FF FF FF FF 00 00 00 00 00 00 00 00 00 00
00 01 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00
Nov 25 03:52:57.534: TPS: Rcv Msg len = 66
Nov 25 03:52:57.534: TPS: Msg name is NULL
Nov 25 03:52:57.537: Received pki_sd -1
Nov 25 03:52:57.537: Received persistent 0
Nov 25 03:52:57.537: Received seqnum 1
Nov 25 03:52:57.537: Received tp length 0tinfo is FF9FAB86A8
tp name is TP-self-signed-1652845493
Auth is 1 scep poll rate 1 max poll no 999 cert loaded 1 self 1 enrol in progress 0 regen
on renewal 0

Nov 25 03:52:57.542: Length of marshalled msg 148
Nov 25 03:52:57.542: get tp info response message send succeeded
Nov 25 03:52:57.563: Enters in tps_ipc_msg_rcvd_handler
Nov 25 03:52:57.563: Queue Event buffer len = 90 ...
buffer content ...
BC FF FF FF FF FF FF 00 00 00 00 00 00 00 00 00
00 00 00 60 00 08 C0 00 00 00 00 3A 7B C3 C6 74
1E 0D 2C C7 DA E7 80 22 A2 BB 9D 14 00 00 00 00
00 32 FF FF FF FF 00 00 00 1A 54 50 2D 73 65 6C
66 2D 73 69 67 6E 65 64 2D 31 36 35 32 38 34 35
34 39 33 00 00 00 00 02 00 00
Nov 25 03:52:57.564: TPS: Rcv Msg len = 96
Nov 25 03:52:57.564: TPS: Msg name is NULL
Nov 25 03:52:57.565: Received pki_sd -1
Nov 25 03:52:57.565: Received options 0x2
Nov 25 03:52:57.565: Received seqnum 2
Nov 25 03:52:57.565: Received chain len 0
Nov 25 03:52:57.565: Received tp_len 26
Nov 25 03:52:57.566: Received tp_label TP-self-signed-1652845493num certs 1 SS Cert 1 router
cert on chain 0 root
cert in chain 0
Cert index 1 Cert len is 655. Cert :
0x30
Nov 25 03:52:57.566: 0x82 0x2 0x8B 0x30 0x82 0x1 0xF4 0xA0 0x3 0x2 0x1 0x2 0x2 0x1 0x1 0x30
Nov 25 03:52:57.568: 0xD 0x6 0x9 0x2A 0x86 0x48 0x86 0xF7 0xD 0x1 0x1 0x5 0x5 0x0 0x30 0x61
Nov 25 03:52:57.569: 0x31 0x2F 0x30 0x2D 0x6 0x3 0x55 0x4 0x3 0x13 0x26 0x49 0x4F 0x53 0x2D
0x53
Nov 25 03:52:57.570: 0x65 0x6C 0x66 0x2D 0x53 0x69 0x67 0x6E 0x65 0x64 0x2D 0x43 0x65 0x72
0x74 0x69
Nov 25 03:52:57.572: 0x66 0x69 0x63 0x61 0x74 0x65 0x2D 0x31 0x36 0x35 0x32 0x38 0x34 0x35
0x34 0x39
Nov 25 03:52:57.573: 0x33 0x31 0x2E 0x30 0x12 0x6 0x3 0x55 0x4 0x5 0x13 0xB 0x46 0x4F 0x43
0x31
Nov 25 03:52:57.574: 0x37 0x32 0x31 0x56 0x31 0x43 0x39 0x30 0x18 0x6 0x9 0x2A 0x86 0x48
0x86 0xF7
Nov 25 03:52:57.576: 0xD 0x1 0x9 0x2 0x16 0xB 0x73 0x74 0x68 0x69 0x74 0x69 0x2D 0x65 0x64
0x69
Nov 25 03:52:57.577: 0x32 0x30 0x1E 0x17 0xD 0x31 0x35 0x31 0x30 0x31 0x34 0x31 0x32 0x30
0x31 0x33
Nov 25 03:52:57.578: 0x39 0x5A 0x17 0xD 0x32 0x30 0x30 0x31 0x30 0x31 0x30 0x30 0x30 0x30
0x30 0x30
Nov 25 03:52:57.580: 0x5A 0x30 0x61 0x31 0x2F 0x30 0x2D 0x6 0x3 0x55 0x4 0x3 0x13 0x26 0x49
0x4F
Nov 25 03:52:57.581: 0x53 0x2D 0x53 0x65 0x6C 0x66 0x2D 0x53 0x69 0x67 0x6E 0x65 0x64 0x2D
0x43 0x65
Nov 25 03:52:57.582: 0x72 0x74 0x69 0x66 0x69 0x63 0x61 0x74 0x65 0x2D 0x31 0x36 0x35 0x32

```

```

0x38 0x34
Nov 25 03:52:57.584: 0x35 0x34 0x39 0x33 0x31 0x2E 0x30 0x12 0x6 0x3 0x55 0x4 0x5 0x13 0xB
0x46
Nov 25 03:52:57.585: 0x4F 0x43 0x31 0x37 0x32 0x31 0x56 0x31 0x43 0x39 0x30 0x18 0x6 0x9
0x2A 0x86
Nov 25 03:52:57.587: 0x48 0x86 0xF7 0xD 0x1 0x9 0x2 0x16 0xB 0x73 0x74 0x68 0x69 0x74 0x69
0x2D
Nov 25 03:52:57.588: 0x65 0x64 0x69 0x32 0x30 0x81 0x9F 0x30 0xD 0x6 0x9 0x2A 0x86 0x48
0x86 0xF7
Nov 25 03:52:57.589: 0xD 0x1 0x1 0x1 0x5 0x0 0x3 0x81 0x8D 0x0 0x30 0x81 0x89 0x2 0x81 0x81
Nov 25 03:52:57.591: 0x0 0xB2 0x12 0x8F 0x83 0x42 0x99 0xF7 0xE7 0x7 0xCE 0x3D 0x81 0xF3
0xD8 0xAE
Nov 25 03:52:57.592: 0x7F 0x0 0x71 0x22 0xC4 0x12 0x96 0x20 0x2F 0x49 0x20 0x85 0x13 0xDB
0x5B 0xE7
Nov 25 03:52:57.593: 0x62 0x97 0xAB 0x22 0xA3 0xC8 0x9E 0x10 0x2C 0xC0 0x16 0xC0 0x13 0x6C
0x5F 0x2A
Nov 25 03:52:57.595: 0x59 0x7B 0x24 0x9E 0xAC 0x2F 0x1A 0xE5 0x29 0x4F 0x3C 0xEC 0x25 0xC0
0x33 0xC5
Nov 25 03:52:57.596: 0xFF 0xA5 0xEB 0x80 0xDD 0x1C 0xCD 0x4F 0xD7 0x7C 0x54 0xC3 0x69 0xAF
0xA3 0xA
Nov 25 03:52:57.597: 0x3E 0xFE 0x48 0x92 0x39 0xCC 0xAE 0xEB 0x8 0xAA 0xEB 0xD6 0x77 0x24
0x55 0x26
Nov 25 03:52:57.599: 0xF0 0x27 0x64 0x68 0x6C 0x69 0xEE 0x2B 0x43 0xD1 0xF1 0x90 0xF1 0x63
0x2C 0xF9
Nov 25 03:52:57.600: 0x9E 0x63 0x85 0xB9 0xFE 0xE0 0x55 0x74 0xC0 0xEE 0x51 0xB3 0x28 0xD7
0x53 0xFA
Nov 25 03:52:57.601: 0xBD 0x2 0x3 0x1 0x0 0x1 0xA3 0x53 0x30 0x51 0x30 0xF 0x6 0x3 0x55
0x1D
Nov 25 03:52:57.602: 0x13 0x1 0x1 0xFF 0x4 0x5 0x30 0x3 0x1 0x1 0xFF 0x30 0x1F 0x6 0x3 0x55
Nov 25 03:52:57.604: 0x1D 0x23 0x4 0x18 0x30 0x16 0x80 0x14 0x68 0xA1 0x5D 0xB0 0x64 0xE
0xA0 0x15
Nov 25 03:52:57.605: 0x29 0x9 0x5A 0x8 0x2C 0xA6 0xD 0x9C 0x11 0xF0 0x23 0xBB 0x30 0x1D 0x6
0x3
Nov 25 03:52:57.607: 0x55 0x1D 0xE 0x4 0x16 0x4 0x14 0x68 0xA1 0x5D 0xB0 0x64 0xE 0xA0 0x15
0x29
Nov 25 03:52:57.608: 0x9 0x5A 0x8 0x2C 0xA6 0xD 0x9C 0x11 0xF0 0x23 0xBB 0x30 0xD 0x6 0x9
0x2A
Nov 25 03:52:57.609: 0x86 0x48 0x86 0xF7 0xD 0x1 0x1 0x5 0x5 0x0 0x3 0x81 0x81 0x0 0x3A
0xF0
Nov 25 03:52:57.611: 0xF0 0xAA 0x6B 0x80 0x8F 0x4F 0x8 0x72 0x65 0xC2 0x2F 0x20 0xE3 0xF2
0x22 0x73
Nov 25 03:52:57.612: 0x69 0xA7 0x3E 0x6A 0x28 0xB 0x93 0x83 0x71 0x96 0xD2 0xBC 0xA 0x59
0xFE 0xDD
Nov 25 03:52:57.613: 0x17 0xFE 0x95 0x23 0x69 0x71 0xD8 0x61 0xB9 0x27 0x2D 0x2B 0x3E 0xFC
0x8D 0xCB
Nov 25 03:52:57.615: 0x88 0xCD 0xFB 0x29 0xA9 0x43 0xEA 0x1B 0xCD 0x10 0x7D 0x1 0xD0 0x50
0xE5 0x7A
Nov 25 03:52:57.616: 0xF8 0x86 0x62 0xE3 0x95 0xF0 0xE5 0x1E 0xBB 0xFE 0x9C 0xBA 0xDF 0x50
0x16 0xBB
Nov 25 03:52:57.617: 0xE9 0x6C 0xE 0xE9 0xB7 0xC5 0x82 0xB6 0x5C 0xDA 0xA3 0x0 0xA 0xAE
0x96 0x7
Nov 25 03:52:57.619: 0xCE 0xDD 0xE1 0xCC 0x5B 0xFA 0xCB 0xB4 0x15 0x4B 0x23 0xF2 0xCB 0xBA
0x1A 0x9A
Nov 25 03:52:57.620: 0x76 0x44 0x6D 0x5F 0x20 0x43 0xCE 0x71 0xA0 0xAB 0xA0 0xDB 0xC8 0x17
Nov 25 03:52:57.621:
Nov 25 03:52:57.622: Length of marshalled msg 787
Nov 25 03:52:57.625: decrypt_response message send succeeded
Nov 25 03:52:57.646: Enters in tps_ipc_msg_rcvd handler
Nov 25 03:52:57.647: Queue Event buffer len = 90 ...
buffer content ...
BC FF FF FF FF FF FF 00 00 00 00 00 00 00 00 00
00 00 00 DC 00 08 C0 00 00 00 00 3A 70 0B 9F 3B
DC 30 F1 2E CB 1F AD BB CD 58 1E E0 00 00 00 00
00 AE 54 50 2D 73 65 6C 66 2D 73 69 67 6E 65 64
2D 31 36 35 32 38 34 35 34 39 33 00 00 00 00 00
00 00 00 80 09 8F 28 96 1F 19
Nov 25 03:52:57.647: TPS: Rcv Msg len = 220
Nov 25 03:52:57.647: TPS: Msg name is NULL
Nov 25 03:52:57.649: Received Padding 1
Nov 25 03:52:57.649: Received seqnum 3
Nov 25 03:52:57.650: Received From Len 128
Nov 25 03:52:57.651: Received tp name TP-self-signed-1652845493
Nov 25 03:52:57.651: tps_tp_priv_decrypt

```

```

Nov 25 03:52:57.651: tps_srv_create_key_id
Nov 25 03:52:57.651: Received tpname: TP-self-signed-1652845493
Nov 25 03:52:57.652: KPL is TP-self-signed-1652845493
Nov 25 03:52:57.652: tps_keyid_priv_decrypt
Nov 25 03:52:57.652: Priv decryption input buffer len = 128 ...
buffer content ...
09 8F 28 96 1F 19 D8 77 0C 17 E9 04 5D 2E 1F 24
EC 6E D2 56 8C 97 2E 36 14 79 B2 73 FF A7 8B 44
08 60 62 53 1B 0D B9 5A A6 46 9E D2 F0 AB 59 02
4D C1 41 6F 5B CE BC 66 54 D1 AD 6F C4 FC 84 0E
A3 3C 0F 24 A1 C9 4C E1 59 3E C5 93 A1 93 FB 18
0A FE AA 1F F8 59 95 98 C8 58 CF 19 4E C1 FB 24
DE 91 0F 40 04 B8 3E 02 F8 1B 19 EF 13 25 F3 58
26 0F E5 7D 21 3F 8C AB 1D EC 10 D7 3A EE 88 83
../snip/
buffer too big to print, truncating.
Nov 25 03:52:57.673: Decrypted output buffer len = 48 ...
buffer content ...
03 03 F0 25 92 D5 50 31 C7 E5 F8 1D 33 EC 85 0F
6C C0 A1 63 82 ED 26 9D 1E CA DD 53 3C D5 6C CF
B3 C9 37 E1 B3 31 2F FC BE DE B8 3C 2D 3B 44 57

Nov 25 03:52:57.673: Length of marshalled msg 104
Nov 25 03:52:57.674: decrypt_response message send succeeded
Nov 25 03:53:54.065: Enters in tps_ipc_msg_rcvd_handler
Nov 25 03:53:54.066: Queue Event buffer len = 90 ...
buffer content ...
BC FF FF FF FF FF FF 00 00 00 00 00 00 00 00
00 00 00 DC 00 08 C0 00 00 00 00 3A 70 0B 9F 3B
DC 30 F1 2E CB 1F AD BB CD 58 1E E0 00 00 00 00
00 AE 54 50 2D 73 65 6C 66 2D 73 69 67 6E 65 64
2D 31 36 35 32 38 34 35 34 39 33 00 00 00 00 00
00 00 00 80 88 54 62 9D 10 1B
Nov 25 03:53:54.066: TPS: Rcv Msg len = 220
Nov 25 03:53:54.066: TPS: Msg name is NULL
Nov 25 03:53:54.066: Received Padding 1
Nov 25 03:53:54.066: Received seqnum 4
Nov 25 03:53:54.066: Received From Len 128
Nov 25 03:53:54.066: Received tp name TP-self-signed-1652845493
Nov 25 03:53:54.067: tps_tp_priv_decrypt
Nov 25 03:53:54.067: tps_srv_create_key_id
Nov 25 03:53:54.067: Received tpname: TP-self-signed-1652845493
Nov 25 03:53:54.067: KPL is TP-self-signed-1652845493
Nov 25 03:53:54.067: tps_keyid_priv_decrypt
Nov 25 03:53:54.067: Priv decryption input buffer len = 128 ...
buffer content ...
88 54 62 9D 10 1B 72 21 A2 3F 88 86 AA B5 0F D1
E3 42 8F C8 9D DE 22 95 B6 51 71 A7 00 35 BC 86
B3 1F 70 77 58 48 10 8A 43 6A 54 00 73 84 9F B2
39 73 91 AB 28 16 21 31 5D 1D FD 88 F1 89 4E 41
5A 10 90 0E 6F 78 92 7A 43 12 D0 C3 22 F5 7A 45
80 C3 7E 6B 52 58 26 82 DB 10 9A 4F 00 07 2B 21
89 99 1A CA B9 8A 69 DD 83 C4 52 E6 AE 35 F5 3E
64 C5 5D 42 06 C7 C0 AE 40 6D 18 3A 47 E6 85 64
../snip/
buffer too big to print, truncating.
Nov 25 03:53:54.088: Decrypted output buffer len = 48 ...
buffer content ...
03 03 BD 52 5A BA 99 01 B3 23 24 08 7D 2D 7A F7
D3 4F E7 7B A2 42 8F B2 45 BC 4C 34 FD 40 FB 8E
79 15 47 94 07 33 97 E1 17 76 DE 9E 41 FC A1 66

Nov 25 03:53:54.089: Length of marshalled msg 104
Nov 25 03:53:54.089: decrypt_response message send succeeded
Nov 25 03:54:17.877: [WCDB] wcdb_send_add_notify: Notifying other features about client add
Nov 25 03:54:17.877: pvlan_pre_addr_addition: vlan 74, addr 48f8.b38a.flb0
Nov 25 03:54:17.877: mat_add_addr_entry: addr:48f8.b38a.flb0 addr_type: 65793 table_type:1
table_id:74
Nov 25 03:54:17.877: matm_wl_add_addr_entry: addr:48f8.b38a.flb0 addr_type: 65793 table_type:1
table_id:74
Nov 25 03:54:17.877: Add event has already been programmed by WCM. Return.: Added
Nov 25 03:54:17.878: pvlan_post_addr_addition: vlanid:74, addr:48f8.b38a.flb0
Nov 25 03:54:17.881: ngwc_dataglean_ip_mac_add: The client_id x80000012 and ipsq flag 0 is

```

```

received from the wcdb
entry for the host mac 48f8.b38a.flb0
Nov 25 03:54:17.885: Processed SISF BT event STATE_CHANGE for addr 48f8.b38a.flb0:9.5.74.106
Nov 25 03:54:17.885: sisf_hwapi_bridging_pre_encap_setup: pre data FFA387693A network
FFA3876948
Nov 25 03:54:17.885: SISF pre_encap: pak info:
  Pak: 0xFFA3875DD8      Link Type: 1
  Dest Mac: ffff.ffff.ffff      etype: 2
  if_input: None      if_output: Ca3
  ether_sa: aaaa.0300.000c      ether_da: 24cf.2401.0032
  group: -1      vlan_id: 74, pak->vlan_id: 0
  icmpv6 type: 0      consume: 1
Nov 25 03:54:17.886: sisf_hwapi_bridging_pre_encap_setup: pak 0xFFA3875DD8 SUPPRESS_TO_WCM
as groupid=-1 , etype=2
Nov 25 03:54:17.886: sisf_hwapi_bridging_pre_encap_setup: pak 0xFFA3875DD8 Direct Forward
Nov 25 03:54:17.886: sisf_hwapi_bridging_pre_encap_setup: pak 0xFFA3875DD8 not IPv6, output
port set
Nov 25 03:54:17.886: sisf_hwapi_bridging_pre_encap_setup: Pak 0xFFA3875DD8 Set vlan, old
pak vlan 0 new pak vlan 74
Nov 25 03:54:17.886: sisf_hwapi_bridging_pre_encap_setup: pak 0xFFA3875DD8 src-mac
aaaa.0300.000c,
data-area 0c27.24cf.244a etype = 2, old pak vlan 74 new pak vlan 74 !!!
Nov 25 03:54:17.886: sisf_hwapi_bridging_pre_encap_setup: pak 0xFFA3875DD8 src-mac
aaaa.0300.000c,
data-area 0c27.24cf.244a etype = 2, old pak vlan 74 new pak vlan 74
Nov 25 03:54:17.886: sisf_hwapi_bridging_pre_encap_setup: SISF packet 0xFFA3875DD8 if_input
None etype - 2
returned for encap!!
Nov 25 03:54:17.886: capwap_oqueue, .11 format.
Nov 25 03:54:17.886: capwap_oqueue, MGID obtained is 74
Nov 25 03:54:17.887: Transmitting CAPWAP packet
Nov 25 03:54:17.887: Src IP addr: 9.5.74.10, Dest IP addr: 9.5.74.101
Device#
11/25 09:24:17.846 [mob-handoff]: [22238]: UUID: 8c0000000006d, ra: 7 (debug): 48f8.b38a.flb0

MC: Changing client state from 0 to 1
11/25 09:24:17.846 [mob-handoff]: [21656]: UUID: 8c0000000006d, ra: 7 (debug): 48f8.b38a.flb0
[1476: Handoff Complete Ack MC->MA] from 9.5.74.10:16666
11/25 09:24:17.846 [sim-cs]: [21656]: UUID: 8c0000000006d, ra: 7 (info): System IP addr :
9.5.74.10

11/25 09:24:17.846 [cond_debug]: [21656]: UUID: 8c0000000006d, ra: 7 (info): Search
condition: ft_id 43,
cond: type 16, fmt 2, id: 0x1010074, name:
11/25 09:24:17.846 [cond_debug]: [21656]: UUID: 8c0000000006d, ra: 7 (info): Condition not
found
11/25 09:24:17.846 [wcm]: [21656]: UUID: 8c0000000006e, ra: 7 (appctx): mac
48:f8:b3:8a:fl:b0
11/25 09:24:17.846 [mob-handoff]: [21656]: UUID: 8c0000000006e, ra: 7 (debug): 48f8.b38a.flb0

mmProcessInMsg:1377 MA FSM event MM_MAFSM_EV_HDOFF_COMPL_ACK: state Local -> Local
11/25 09:24:17.853 [tdllib]: [17333]: UUID: 8c00000000066, ra: 7 (debug): unmarshal: got
uuid 8c00000000066, ra 7
11/25 09:24:17.853 [smrcl]: [17333]: UUID: 8c00000000066, ra: 7 (debug): EEDGE-RCL: Rx -
[eEdge --> IOS]
OUT Callback Notify type 4 for rcl_conn_hdl = 101
11/25 09:24:17.853 [wcm]: [17333]: UUID: 8c00000000066, ra: 7 (debug): AAA-Proxy attr list
alloc:
Created attribute list = (AC00004C)
11/25 09:24:17.853 [aaa]: [17333]: UUID: 8c00000000066, ra: 7 (debug): 48f8.b38a.flb0 Start
response cb rcvd,
label: 1006632973, ASID: 09054A0A000000173CC70BBD
11/25 09:24:17.853 [aaa]: [17333]: UUID: 8c00000000066, ra: 7 (debug): 48f8.b38a.flb0
Start response cb from SANET successfully enqueued
11/25 09:24:17.853 [apf-mobile]: [21661]: UUID: 8c00000000066, ra: 7 (info): 48f8.b38a.flb0

Start response callback from SANET successfully processed
11/25 09:24:17.853 [wcm]: [17333]: UUID: 8c00000000066, ra: 7 (debug): AAA-Proxy attr list
free:
Freed attribute list = (AC00004C).
11/25 09:24:17.853 [smrcl]: [17333]: UUID: 8c00000000066, ra: 7 (debug):
ipc(mqipc/wcm/smd-wcm):End of MQIPC queue
with 2 messages in 0 ms

```

```

11/25 09:24:17.871 [tdllib]: [17333]: UUID: 8c00000000066, ra: 7 (debug): unmarshal: got
uuid 8c00000000066, ra 7
11/25 09:24:17.871 [aaa]: [17333]: UUID: 8c00000000066, ra: 7 (debug): 48f8.b38a.flb0
Policy Source received in
Bind Call: policy_src[0]: NONE
11/25 09:24:17.871 [aaa]: [17333]: UUID: 8c00000000066, ra: 7 (debug): 48f8.b38a.flb0
Policy Source received in
Bind Call: policy_src[1]: NONE
11/25 09:24:17.871 [aaa]: [17333]: UUID: 8c00000000066, ra: 7 (debug): 48f8.b38a.flb0
Policy Source received in
Bind Call: policy_src[2]: NONE
11/25 09:24:17.871 [aaa]: [17333]: UUID: 8c00000000066, ra: 7 (debug): 48f8.b38a.flb0
Policy Source received in
Bind Call: policy_src[3]: CLI
11/25 09:24:17.871 [aaa]: [17333]: UUID: 8c00000000066, ra: 7 (debug): 48f8.b38a.flb0 Bind
policy msg from SANET
successfully enqueued
11/25 09:24:17.871 [aaa]: [21661]: UUID: 8c00000000066, ra: 7 (debug): 48f8.b38a.flb0
***----- Bind policies from EPM -----***
11/25 09:24:17.871 [aaa]: [21661]: UUID: 8c00000000066, ra: 7 (debug): 48f8.b38a.flb0 Vlan:
74, Vlan Name: ,
Vlan Source: CLI
11/25 09:24:17.871 [smrcl]: [17333]: UUID: 8c00000000066, ra: 7 (debug):
ipc(mqipc/wcm/smd-wcm):End of MQIPC
queue with 2 messages in 1 ms
11/25 09:24:17.871 [aaa]: [21661]: UUID: 8c00000000066, ra: 7 (debug): 48f8.b38a.flb0
Session Timeout: 1800
11/25 09:24:17.871 [aaa]: [21661]: UUID: 8c00000000066, ra: 7 (debug): 48f8.b38a.flb0
IF NUM: 0x80000004
11/25 09:24:17.871 [aaa]: [21661]: UUID: 8c00000000066, ra: 7 (debug): 48f8.b38a.flb0
Template name:
implicit_deny_v6:implicit_deny:preauth_v6:preauth_v4:IP-Adm-V6-Int-ACL-global:IP-Adm-V4-Int-ACL-global,,
URL Present: 1
11/25 09:24:17.871 [aaa]: [21661]: UUID: 8c00000000066, ra: 7 (debug): 48f8.b38a.flb0 Qos
Level: 5, Qos Level Src:
NONE, Qos Input Name: , Qos Input Src: NONE, Qos Output Name: , Qos Output Src: NONE
11/25 09:24:17.871 [aaa]: [21661]: UUID: 8c00000000066, ra: 7 (debug): 48f8.b38a.flb0
***-----*
11/25 09:24:17.871 [apf-mobile]: [21661]: UUID: 8c00000000066, ra: 7 (info): 48f8.b38a.flb0
Processing the policy
bind call from SANET
11/25 09:24:17.871 [apf-mobile]: [21661]: UUID: 8c00000000066, ra: 7 (info): 48f8.b38a.flb0

Device Classification:Applying Session Timeout. State DHCP_REQD
Current SessionTimeout 1800 Updated Timeout 1800

11/25 09:24:17.871 [apf-mobile]: [21661]: UUID: 8c00000000066, ra: 7 (info): 48f8.b38a.flb0

Device Classification: Setting Session Timeout to 1800

11/25 09:24:17.871 [pem]: [21661]: UUID: 8c00000000066, ra: 7 (info): 48f8.b38a.flb0
Setting session timeout 1800 on mobile 48f8.b38a.flb0
11/25 09:24:17.871 [apf-mobile-state]: [21661]: UUID: 8c00000000066, ra: 7 (debug):
48f8.b38a.flb0
Session Timeout is 1800 - starting session timer for the mobile
11/25 09:24:17.871 [pem]: [21661]: UUID: 8c00000000066, ra: 7 (info): Not applying bind
vlan policy:
Policy Vlan 74, Access Vlan 74, MmRole 1

11/25 09:24:17.871 [qos]: [21661]: UUID: 8c00000000066, ra: 7 (info): 48f8.b38a.flb0 [QOS]
%:
Sending native profile info to QoS task
11/25 09:24:17.871 [pem]: [21661]: UUID: 8c00000000066, ra: 7 (info): 48f8.b38a.flb0
0.0.0.0 DHCP_REQD (7)
BIND-COMPLETE with state 7.

11/25 09:24:17.872 [qos-ipc]: [21623]: UUID: 8c00000000066, ra: 7 (info): [QOS-IPC] %:
QOS_HANDLE_NATIVE_PROFILE_CLIENT_POLICY_POST_RUN: 20 Recvd.
11/25 09:24:17.872 [pem]: [21661]: UUID: 8c00000000066, ra: 7 (info): 48f8.b38a.flb0
0.0.0.0 DHCP_REQD (7)
State Update from BIND-Incomplete to BIND-Complete, mobility role=Local, client
state=APF_MS_STATE_ASSOCIATED

```

```

11/25 09:24:17.872 [pem]: [21661]: UUID: 8c00000000066, ra: 7 (info): 48f8.b38a.flb0
0.0.0.0 DHCP_REQD (7)
pemAdvanceState2 3944, Adding TMP rule
11/25 09:24:17.872 [pem]: [21661]: UUID: 8c00000000066, ra: 7 (info): 48f8.b38a.flb0
0.0.0.0 DHCP_REQD (7)
Adding Fast Path rule
  on AP 5087.89be.7420 , slot 1 802.1P = 0

11/25 09:24:17.872 [pem]: [21661]: UUID: 8c00000000066, ra: 7 (info): 48f8.b38a.flb0
0.0.0.0 DHCP_REQD (7)
Successfully plumbed mobile rule
11/25 09:24:17.872 [apf-mobile]: [21661]: UUID: 8c00000000066, ra: 7 (info): 48f8.b38a.flb0
Successfully
processed the policy bind call from SANET
11/25 09:24:17.872 [pem]: [21652]: UUID: 8c00000000066, ra: 7 (info): PEM rcv processing
msg Add SCB(3)
11/25 09:24:17.872 [qos-ipc]: [21623]: UUID: 8c00000000066, ra: 7 (info): [QOS-IPC] %:
Regular QoS requests
can be processed...
11/25 09:24:17.872 [pem]: [21652]: UUID: 8c00000000066, ra: 7 (info): 48f8.b38a.flb0
0.0.0.0, auth_state 7 mmRole
Local !!!
11/25 09:24:17.872 [pem]: [21652]: UUID: 8c00000000066, ra: 7 (info): 48f8.b38a.flb0
***WLCLIENT IIF 0x80000012:
adding to FMAN and WDB
11/25 09:24:17.872 [capwap]: [21652]: UUID: 8c00000000066, ra: 7 (debug): Platform capability

Asic-level-load-balancing is FALSE
11/25 09:24:17.872 [apf-lb]: [21652]: UUID: 8c00000000066, ra: 7 (info): Platform not
supported
11/25 09:24:17.872 [client]: [21652]: UUID: 8c00000000066, ra: 7 (debug): IPC_ADD: WLCLIENT:
IIF 0x80000012
send station ADD to FMAN and IOSD
11/25 09:24:17.872 [tdllib]: [21652]: UUID: 8c00000000066, ra: 7 (debug): marshal: set
uuid 8c00000000066, ra 7
11/25 09:24:17.872 [client]: [21652]: UUID: 8c00000000066, ra: 7 (debug): IPC_ADD: WLCLIENT:
IIF 0x80000012
Sending station ADD to FMAN
11/25 09:24:17.872 [client]: [21652]: UUID: 8c00000000066, ra: 7 (debug): Client bitmap
is 01000000000000010
11/25 09:24:17.872 [client]: [21652]: UUID: 8c00000000066, ra: 7 (debug): MOBILITY_STATE
set
11/25 09:24:17.872 [client]: [21652]: UUID: 8c00000000066, ra: 7 (debug):
DYNAMIC POLICY_TEMPLATE set
11/25 09:24:17.873 [apf-mobile]: [21652]: UUID: 8c00000000066, ra: 7 (info): wcm_wdb create:
ipv4_addr = 0.0.0.0
11/25 09:24:17.873 [apf-mobile]: [21652]: UUID: 8c00000000066, ra: 7 (info): wcm_wdb create:
numv6 address = 0
11/25 09:24:17.873 [apf-mobile]: [21652]: UUID: 8c00000000066, ra: 7 (info): Setting WCDB
VLAN to 74
11/25 09:24:17.873 [tdllib]: [21652]: UUID: 8c00000000066, ra: 7 (debug): marshal: set
uuid 8c00000000066, ra 7
11/25 09:24:17.873 [apf-mobile]: [21652]: UUID: 8c00000000066, ra: 7 (info): WLCLIENT:
wcm_wdb client creation
message was sent successfully
11/25 09:24:17.873 [client]: [21652]: UUID: 8c00000000066, ra: 7 (debug): IPC_ADD: WLCLIENT:
IIF 0x80000012
Sending station ADD to IOSD
11/25 09:24:17.873 [pem]: [21652]: UUID: 8c00000000066, ra: 7 (info): 48f8.b38a.flb0 Tclas
Plumb needed: 0
11/25 09:24:17.881 [tdllib]: [21661]: UUID: 8c00000000066, ra: 7 (debug): unmarshal: got
uuid 8c00000000066, ra 7
11/25 09:24:17.881 [cond_debug]: [21661]: UUID: 8c00000000066, ra: 7 (info): Search
condition: ft_id 43, cond:
type 16, fmt 2, id: 0x48f8b38a, name: H□□□□
11/25 09:24:17.881 [cond_debug]: [21661]: UUID: 8c00000000066, ra: 7 (info): Condition
found
11/25 09:24:17.881 [wcm]: [21661]: UUID: 8c0000000006f, ra: 7 (appctx): mac
48:f8:b3:8a:f1:b0
11/25 09:24:17.881 [apf-mobile]: [21661]: UUID: 8c0000000006f, ra: 7 (info): 48f8.b38a.flb0
wcm_wdb received
ip binding message: client mac 48f8.b38a.flb0, ip learn type 2, v4/v6 0, ipv4 address
9.5.74.106 ,

```

```

ipv6 address 0000:0000:0000:0000:0000:0000:0000:0000, add/delete 1, options length 0, subnet
vlan 74
11/25 09:24:17.881 [apf-mobile]: [21661]: UUID: 8c0000000006f, ra: 7 (info): 48f8.b38a.flb0
wcm_wdb ip binding
message was processed
11/25 09:24:17.881 [apf-mobile]: [21661]: UUID: 8c0000000006f, ra: 7 (info): 48f8.b38a.flb0
WcdbClientUpdate:
IP Binding from WCDB ip_learn_type 2, add_or_delete 1
11/25 09:24:17.881 [apf-mobile]: [21661]: UUID: 8c0000000006f, ra: 7 (info): 48f8.b38a.flb0
IPv4 Addr: 9:5:74:106

11/25 09:24:17.882 [pem]: [21661]: UUID: 8c0000000006f, ra: 7 (info): 48f8.b38a.flb0 MS
got the IP, resetting the
Reassociation Count 0 for client
11/25 09:24:17.882 [apf-lb]: [21661]: UUID: 8c0000000006f, ra: 7 (info): 48f8.b38a.flb0
fap IP change
from 0 to 9054a6a for client 48f8.b38a.flb0
11/25 09:24:17.882 [apf-mobile]: [21661]: UUID: 8c0000000006f, ra: 7 (info): In
apfHaIpChangeAfterRunChkpt:
ssoClientHaFlag 0x0, IP 0x9054a6a 48f8.b38a.flb0
11/25 09:24:17.882 [apf-mobile]: [21661]: UUID: 8c0000000006f, ra: 7 (info): 48f8.b38a.flb0

***WLCLIENT IIF 0x80000012: IP address updated. Set flag for IPADDR_INFO
11/25 09:24:17.882 [pem-state]: [21661]: UUID: 8c0000000006f, ra: 7 (debug): 48f8.b38a.flb0
Moving to webauth
state, URL Flag is set
11/25 09:24:17.882 [pem-state]: [21661]: UUID: 8c0000000006f, ra: 7 (debug): 48f8.b38a.flb0
Change state to
WEBAUTH_REQD (8) last state DHCP_REQD (7)

11/25 09:24:17.882 [capwap]: [21661]: UUID: 8c0000000006f, ra: 7 (debug): Platform capability

Asic-level-load-balancing is FALSE
11/25 09:24:17.882 [apf-lb]: [21661]: UUID: 8c0000000006f, ra: 7 (info): Platform not
supported
11/25 09:24:17.882 [client]: [21661]: UUID: 8c0000000006f, ra: 7 (debug): IPC_UPDATE:
WLCLIENT: IIF 0x80000012
send station UPDATE to FMAN and IOSD
11/25 09:24:17.882 [tdllib]: [21661]: UUID: 8c0000000006f, ra: 7 (debug): marshal: set
uuid 8c0000000006f, ra 7
11/25 09:24:17.882 [client]: [21661]: UUID: 8c0000000006f, ra: 7 (debug): IPC_UPDATE:
WLCLIENT: IIF 0x80000012
Sending station UPDATE to FMAN
11/25 09:24:17.882 [client]: [21661]: UUID: 8c0000000006f, ra: 7 (debug): Client bitmap
is 001000000010000010
11/25 09:24:17.882 [client]: [21661]: UUID: 8c0000000006f, ra: 7 (debug): AUTH_STATE set
11/25 09:24:17.882 [client]: [21661]: UUID: 8c0000000006f, ra: 7 (debug): IPADDR_INFO set
11/25 09:24:17.882 [client]: [21661]: UUID: 8c0000000006f, ra: 7 (debug):
DYNAMIC POLICY TEMPLATE set
11/25 09:24:17.882 [client]: [21661]: UUID: 8c0000000006f, ra: 7 (debug): Not sending IP
address in WDB update
for local/anchor case
11/25 09:24:17.882 [apf-mobile]: [21661]: UUID: 8c0000000006f, ra: 7 (info): wcm_wdb create:
ipv4 addr = 0.0.0.0
11/25 09:24:17.882 [apf-mobile]: [21661]: UUID: 8c0000000006f, ra: 7 (info): wcm_wdb update:
numv6 address = 0
11/25 09:24:17.882 [tdllib]: [21661]: UUID: 8c0000000006f, ra: 7 (debug): marshal: set
uuid 8c0000000006f, ra 7
11/25 09:24:17.882 [apf-mobile]: [21661]: UUID: 8c0000000006f, ra: 7 (info): WLCLIENT:
wcm_wdb client update
message was sent successfully
11/25 09:24:17.883 [client]: [21661]: UUID: 8c0000000006f, ra: 7 (debug): IPC_UPDATE:
WLCLIENT: IIF 0x80000012
Sending station UPDATE to IOSD
11/25 09:24:17.883 [apf-mobile]: [21661]: UUID: 8c0000000006f, ra: 7 (info): 48f8.b38a.flb0

Sending IPv4 update to Controller 9.5.74.10

11/25 09:24:17.883 [sim-cs]: [21661]: UUID: 8c0000000006f, ra: 7 (info): System IP addr :
9.5.74.10

11/25 09:24:17.883 [sim-cs]: [21661]: UUID: 8c0000000006f, ra: 7 (info): System IP addr :
9.5.74.10

```



```

11/25 09:24:17.883 [mob-handoff]: [21661]: UUID: 8c0000000006f, ra: 7 (debug): 48f8.b38a.flb0
mmBuildSendClientUpdate: destIp:9.5.74.10, destType:2 callType:1
11/25 09:24:17.883 [mob-handoff]: [21661]: UUID: 8c0000000006f, ra: 7 (debug): 48f8.b38a.flb0
mmBuildMsgUpdateIpPayload:3938 Sending msg with new client IP 9.5.74.106
11/25 09:24:17.883 [mob-handoff]: [21661]: UUID: 8c0000000006f, ra: 7 (debug): 48f8.b38a.flb0
[1477: Client Update MA->MC] to 9.5.74.10:16666
11/25 09:24:17.883 [apf-mobile]: [21661]: UUID: 8c0000000006f, ra: 7 (info): 48f8.b38a.flb0
Assigning Address 9.5.74.106 to mobile
11/25 09:24:17.883 [mob-handoff]: [22238]: UUID: 8c0000000006f, ra: 7 (debug): 48f8.b38a.flb0
[1477: Client Update MA->MC] from 9.5.74.10:16666
11/25 09:24:17.883 [cond_debug]: [22238]: UUID: 8c0000000006f, ra: 7 (info): Search
condition: ft_id 43,
cond: type 16, fmt 2, id: 0x48f8b38a, name: H□□□□
11/25 09:24:17.883 [cond_debug]: [22238]: UUID: 8c0000000006f, ra: 7 (info): Condition
found
11/25 09:24:17.883 [wcm]: [22238]: UUID: 8c00000000070, ra: 7 (appctx): mac
48:f8:b3:8a:f1:b0
11/25 09:24:17.883 [mob-handoff]: [22238]: UUID: 8c00000000070, ra: 7 (debug): 48f8.b38a.flb0
Updating client
IPv4 address: 9.5.74.106 . Client learn type: 2.
11/25 09:24:35.501 [tdllib]: [17333]: UUID: 8c00000000082, ra: 7 (debug): unmarshal: got
uuid 8c00000000082, ra 7
11/25 09:24:35.501 [wcm]: [17333]: UUID: 8c00000000082, ra: 7 (debug): AAA-Proxy attr list
alloc:
Created attribute list = (EE00004D)
11/25 09:24:35.501 [smrcl]: [17333]: UUID: 8c00000000082, ra: 7 (debug): EEDGE-RCL:
policy_src[0]
in rcl_sm handler is : [0]
11/25 09:24:35.501 [smrcl]: [17333]: UUID: 8c00000000082, ra: 7 (debug): EEDGE-RCL:
policy_src[1]
in rcl_sm handler is : [0]
11/25 09:24:35.501 [smrcl]: [17333]: UUID: 8c00000000082, ra: 7 (debug): EEDGE-RCL:
policy_src[2]
in rcl_sm handler is : [0]
11/25 09:24:35.501 [smrcl]: [17333]: UUID: 8c00000000082, ra: 7 (debug): EEDGE-RCL:
policy_src[3]
in rcl_sm handler is : [4]
11/25 09:24:35.501 [aaa]: [17333]: UUID: 8c00000000082, ra: 7 (debug): AUTHC Callback rcvd
from SANET,
label: 1006632973, auth_result:0 bind result:0 eap_type: 0
11/25 09:24:35.501 [aaa]: [17333]: UUID: 8c00000000082, ra: 7 (debug): SMD policy src[0]:
0
11/25 09:24:35.501 [aaa]: [17333]: UUID: 8c00000000082, ra: 7 (debug): Qos source received
from SMD: 0 ->NONE
11/25 09:24:35.501 [aaa]: [17333]: UUID: 8c00000000082, ra: 7 (debug): SMD policy src[1]:
0
11/25 09:24:35.501 [aaa]: [17333]: UUID: 8c00000000082, ra: 7 (debug): Qos source received
from SMD: 1 ->NONE
11/25 09:24:35.501 [aaa]: [17333]: UUID: 8c00000000082, ra: 7 (debug): SMD policy src[2]:
0
11/25 09:24:35.501 [aaa]: [17333]: UUID: 8c00000000082, ra: 7 (debug): Qos source received
from SMD: 2 ->NONE
11/25 09:24:35.501 [aaa]: [17333]: UUID: 8c00000000082, ra: 7 (debug): SMD policy src[3]:
4
11/25 09:24:35.501 [aaa]: [17333]: UUID: 8c00000000082, ra: 7 (debug): Qos source received
from SMD: 3 ->CLI
11/25 09:24:35.501 [aaa]: [17333]: UUID: 8c00000000082, ra: 7 (debug): 48f8.b38a.flb0
***----- Bind policies from EPM -----***
11/25 09:24:35.501 [aaa]: [17333]: UUID: 8c00000000082, ra: 7 (debug): 48f8.b38a.flb0 Vlan:
74,
Vlan Name: VLAN0074, Vlan Source: CLI
11/25 09:24:35.501 [aaa]: [17333]: UUID: 8c00000000082, ra: 7 (debug): 48f8.b38a.flb0
Session Timeout: 1800
11/25 09:24:35.501 [aaa]: [17333]: UUID: 8c00000000082, ra: 7 (debug): 48f8.b38a.flb0
IF NUM: 0x80000004
11/25 09:24:35.501 [aaa]: [17333]: UUID: 8c00000000082, ra: 7 (debug): 48f8.b38a.flb0
Template name: IP-Adm-V4-LOGOUT-ACL:, URL Present: 0

```

```

11/25 09:24:35.501 [aaa]: [17333]:  UUID: 8c00000000082, ra: 7 (debug): 48f8.b38a.flb0
Qos Level: 5, Qos Level Src: NONE, Qos Input Name: , Qos Input Src: NONE, Qos Output Name:
, Qos Ouput Src: NONE
11/25 09:24:35.501 [aaa]: [17333]:  UUID: 8c00000000082, ra: 7 (debug): 48f8.b38a.flb0
*****
11/25 09:24:35.501 [aaa]: [17333]:  UUID: 8c00000000082, ra: 7 (debug):  AVP type=757 len=4
: 0x00000001 (1)
11/25 09:24:35.501 [aaa]: [17333]:  UUID: 8c00000000082, ra: 7 (debug): Session Label:
1006632973client mac
48f8.b38a.flb0
Auth Results 0

11/25 09:24:35.501 [pem]: [17333]:  UUID: 8c00000000082, ra: 7 (info): 48f8.b38a.flb0
WEBAUTH: received
authentication response, status=0
11/25 09:24:35.501 [smrcl]: [17333]:  UUID: 8c00000000082, ra: 7 (debug):
ipc(mqipc/wcm/smd-wcm):End of MQIPC
queue with 2 messages in 1 ms
11/25 09:24:35.502 [pem]: [21653]:  UUID: 8c00000000082, ra: 7 (info): 48f8.b38a.flb0
WEBAUTH: Received message
from webauth queue: 1
11/25 09:24:35.502 [pem]: [21653]:  UUID: 8c00000000082, ra: 7 (info): 48f8.b38a.flb0
WEBAUTH: SANET Auth
Event - Authentication Success!
11/25 09:24:35.502 [pem]: [21653]:  UUID: 8c00000000082, ra: 7 (info): 48f8.b38a.flb0 Policy
Source:
QOS IN NONE QOS OUT: NONE, VLAN:CLI
11/25 09:24:35.502 [aaa]: [21653]:  UUID: 8c00000000082, ra: 7 (debug): 48f8.b38a.flb0
Applying new AAA override for station 48f8.b38a.flb0 AllowOverRide 1
11/25 09:24:35.502 [aaa]: [21653]:  UUID: 8c00000000082, ra: 7 (debug): 48f8.b38a.flb0
Override Values:
source: 48, valid bits: 0x0101, qosLevel: -1 dscp: 0xffffffff, dot1pTag: 0xffffffff,
sessionTimeout: 1800
11/25 09:24:35.502 [aaa]: [21653]:  UUID: 8c00000000082, ra: 7 (debug): 48f8.b38a.flb0
dataAvgC: -1,
rTAvgC: -1, dataBurstC: -1 rTimeBurstC: -1, vlanIfName: , aclName:
11/25 09:24:35.502 [qos]: [21653]:  UUID: 8c00000000082, ra: 7 (info): 48f8.b38a.flb0 QoS
policies from SMD:
dot1pTag: 0xffffffff, qosLevel: -1, qos-policy-In: , qos-in-src:NONE qos-policy-out: ,
qos-out-src:NONE
sub-qos-policy-in: sub-qos-policy-out: , sub-policy-in: sub-policy-out:
11/25 09:24:35.502 [apf-mobile]: [21653]:  UUID: 8c00000000082, ra: 7 (info): 48f8.b38a.flb0
Clearing
Dhcp state for station ---
11/25 09:24:35.502 [pem]: [21653]:  UUID: 8c00000000082, ra: 7 (info): 48f8.b38a.flb0
Applying WLAN ACL
policies to client
11/25 09:24:35.502 [pem]: [21653]:  UUID: 8c00000000082, ra: 7 (info): 48f8.b38a.flb0 No
Interface
ACL used for Wireless client in WCM(NGWC)
11/25 09:24:35.502 [ap-grp]: [21653]:  UUID: 8c00000000082, ra: 7 (debug): no location
defined

11/25 09:24:35.502 [apf-mobile]: [21653]:  UUID: 8c00000000082, ra: 7 (info): 48f8.b38a.flb0
Inserting AAA
Override struct for mobile
MAC: 48f8.b38a.flb0 , source 48

```

**Note**

Debugs are processor-intensive. Hence, run the debugs in a scheduled maintenance window.



CHAPTER 28

Configuration Examples: WPA2-PSK and Open Authentication

The Configuration Examples: WPA2-PSK and Open Authentication document describes the benefits of using Wi-Fi Protected Access 2 (WPA2) in a Wireless LAN (WLAN). The document also provides the following configuration examples for implementing WPA2 on a WLAN:

- Configuring WPA2 Pre-Shared Key (PSK)
- Configuring Open Authentication
- [Prerequisites, page 311](#)
- [WPA2 PSK and Open Authentication, page 312](#)
- [Verifying WPA2-PSK and Open Authentication Configuration, page 316](#)
- [Troubleshooting WPA2-PSK and Open Authentication Configuration Issues, page 318](#)

Prerequisites

We recommend that you have knowledge about the following topics:

- Wireless Protected Access (WPA)
- WLAN Security Solutions

Supported Platforms and Releases

The information in this document is based on the following software and hardware versions:

- Cisco Aironet 3600 Series Lightweight Access Point
- Microsoft Windows 7 native wireless supplicant

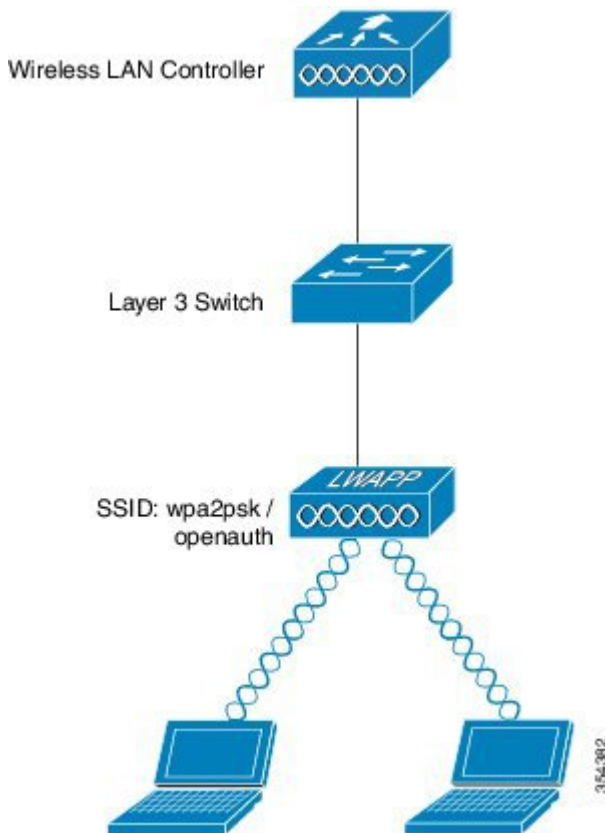
**Note**

The information in this document is based on the devices used in a specific lab environment. The devices used in this document started with a default configuration. If your network is live, make sure that you understand the potential impact of the commands.

WPA2 PSK and Open Authentication

The following figure displays the network diagram for WPA2 PSK and Open Authentication:

Figure 108: Network Diagram



Configuring WPA2-PSK Configuration using CLI

The following example describes the procedure to configure DHCP snooping for the VLANs that are used for the clients. In this example, VLAN20 is used for clients and the pool is configured on the same WLC.

The TenGigabitEthernet1/0/1 interface is connected to the uplink switch. If the DHCP server is configured on the server apart from the WLC or an external DHCP server, you must trust the DHCP snooping and relay information.

```
ip device tracking
ip dhcp snooping vlan 12,20,30,40
```

```
ip dhcp snooping
!
ip dhcp pool vlan20
 network 192.0.2.0 255.255.255.0
 default-router 192.0.2.1

interface Vlan20
 ip address 192.0.2.1 255.255.255.0

interface TenGigabitEthernet1/0/1
 switchport trunk native vlan 12
 switchport mode trunk
 ip dhcp relay information trusted
 ip dhcp snooping trust

wlan wpa2psk 1 wpa2psk
 client vlan 20
 no security wpa akm dot1x
 security wpa akm psk set-key ascii 0 Cisco123
 no shutdown
```

Configuring WPA2-PSK Configuration using GUI

Perform the following steps to configure a WPA2 PSK on the WLC GUI:

Step 1 To create a new WLAN, navigate to **Configuration > Wireless > WLAN > WLANs**.

Figure 109: Wireless Controller Page



Step 2 To enable WPA2, check the **Status** check box and then map WPA2 to the relevant interface.

Figure 110: WLAN Page

The screenshot shows the 'WLAN' configuration page with the 'Edit' sub-page selected. The 'General' tab is active, displaying the following configuration details:

Field	Value
Profile Name	wpa2psk
Type	WLAN
SSID	wpa2psk
Status	<input checked="" type="checkbox"/>
Security Policies	[WPA2][Auth(PSK)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	default
Broadcast SSID	<input checked="" type="checkbox"/>
Multicast VLAN Feature	<input type="checkbox"/>

354115

- Step 3** Click the **Security** tab, check the **WPA2 Policy** check box and the **AES** check box. From the Auth Key Mgmt drop-down list, choose **PSK** and then enter the PSK value that the client needs to connect.

Figure 111: WLAN Page

The screenshot shows the WLAN configuration interface. The 'Security' tab is selected. Under 'Layer 2 Security', 'WPA + WPA2' is chosen. In the 'WPA+WPA2 Parameters' section, 'WPA2 Policy' is checked, 'WPA2 Encryption' is set to 'AES', and 'Auth Key Mgmt' is set to 'PSK'. The 'PSK Format' is set to 'ASCII'. A password field is present with masked characters. The page number '354114' is visible in the bottom right corner.

Configuring Open Authentication using CLI

The following example describes how to configure DHCP snooping for the VLANs that are used for clients. In the following example, VLAN20 is used for clients and the pool is configured on the same WLC.

The TenGigabitEthernet1/0/1 interface is connected to the uplink switch. If you have the DHCP server configured on the server apart from the WLC or an external DHCP server, you must trust DHCP snooping and relay information.

```
ip device tracking
ip dhcp snooping vlan 12,20,30,40
ip dhcp snooping
!
ip dhcp pool vlan20
network 192.0.2.0 255.255.255.0
```

```

default-router 20.20.20.1

interface Vlan20
 ip address 192.0.2.1 255.255.255.0

interface TenGigabitEthernet1/0/1
 switchport trunk native vlan 12
 switchport mode trunk
 ip dhcp relay information trusted
 ip dhcp snooping trust

wlan open 5 open
 client vlan VLAN0020
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 session-timeout 1800
 no shutdown

```

Configuring Open Authentication using GUI

Perform the following steps to configure an open authentication in the WLC GUI:

Step 1 To create a new WLAN navigate to **Configuration > Wireless > WLAN > WLANs**.

Figure 112: Wireless Controller

Step 2 Click the **Security** tab. Set the **Layer2** tab and **Layer3** tab to none. The following figure displays the configuration results:

Figure 113: WLAN Page

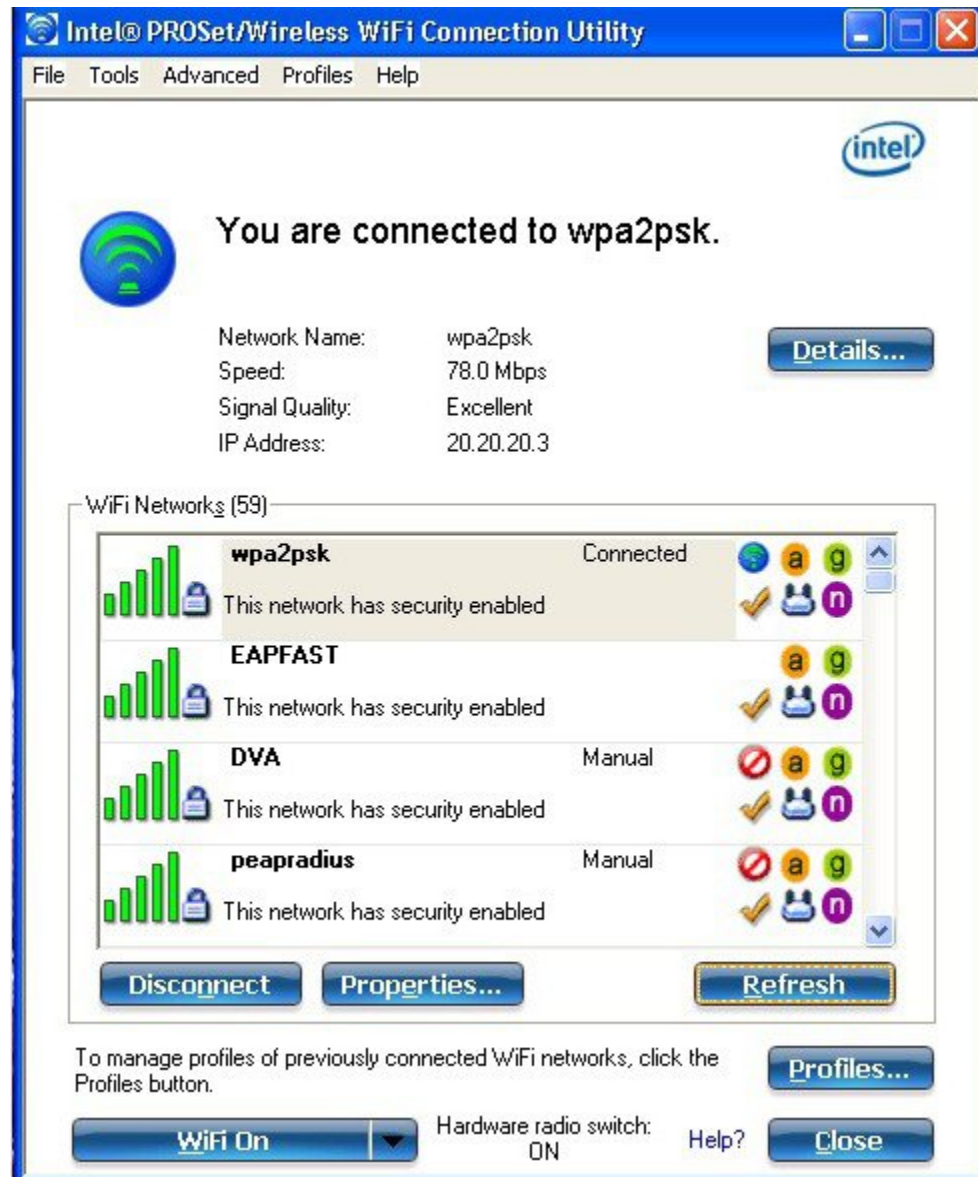
<input type="checkbox"/> open	5	open	20	Enabled
-------------------------------	---	------	----	---------

Verifying WPA2-PSK and Open Authentication Configuration

Perform the following to verify the WPA2-PSK and Open Authentication configuration:

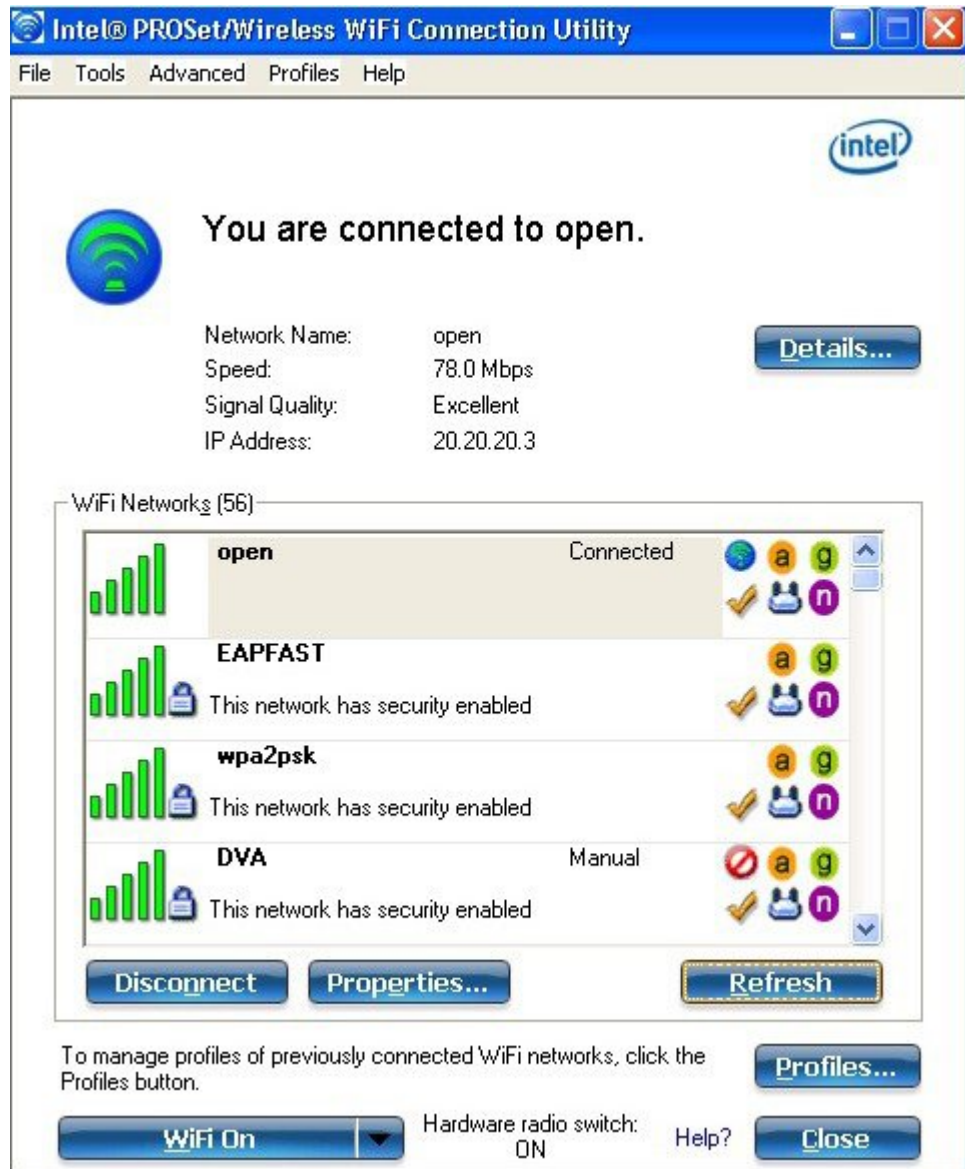
Check and confirm that the WPA2-PSK client is connected as displayed in the following figure:

Figure 114: WPA2-PSK Client Connection



Check and confirm that the client is connected to Open Authentication as displayed in the following figure:

Figure 115: Open Authentication Client Connection



Troubleshooting WPA2-PSK and Open Authentication Configuration Issues

The following is a sample output using the **debug** and **trace** commands:

```
debug client mac XXXX.XXXX.XXXX
Device# show debugging
```

```

dot11/state debugging is on
pem/events debugging is on
client/mac-addr debugging is on
dot11/detail debugging is on
mac/ filters[string 0021.5c8c.c761] debugging is on
dot11/error debugging is on
dot11/mobile debugging is on
pem/state debugging is on

set trace group-wireless-client filter mac XXXX.XXXX.XXXX
set trace wcm-dot1x event filter mac XXXX.XXXX.XXXX
set trace wcm-dot1x aaa filter mac XXXX.XXXX.XXXX
set trace aaa wireless events filter mac XXXX.XXXX.XXXX
set trace access-session core sm filter mac XXXX.XXXX.XXXX
set trace access-session method dot1x filter XXXX.XXXX.XXXX

*Sep 1 05:55:01.321: 0021.5C8C.C761 Association received from mobile on AP
C8F9.F983.4260 1 wcm: i.D^Iw for client
*Sep 1 05:55:01.321: 0021.5C8C.C761 qos upstream policy is unknown and
downstream policy is unknown 1 wcm: r client
*Sep 1 05:55:01.321: 0021.5C8C.C761 apChanged 0 wlanChanged 1 mscb ipAddr
20.20.20.3, apf RadiusOverride 0x0, numIPv6Addr=0 1 wcm: nJ^Iwy_status 0
attr len^G$8\227v^K
*Sep 1 05:55:01.321: 0021.5C8C.C761 Applying WLAN policy on MSCB. 1 wcm:
ipAddr 20.20.20.3, apf RadiusOverride 0x0, numIPv6Addr=0
*Sep 1 05:55:01.321: 0021.5C8C.C761 Scheduling deletion of Mobile Station: 1
wcm: (callerId: 50) in 1 seconds
*Sep 1 05:55:01.321: 0021.5C8C.C761 Disconnecting client due to switch of
WLANs from 6(wep) to 5(open) 1 wcm:
*Sep 1 05:55:02.193: 0021.5C8C.C761 apfMsExpireCallback (apf_ms.c: 1 wcm: 664)
Expiring Mobile!
*Sep 1 05:55:02.193: 0021.5C8C.C761 apfMsExpireMobileStation (apf_ms.c: 1 wcm:
6953) Changing state for mobile 0021.5C8C.C761 on AP C8F9.F983.4260 from
Associated to Disassociated
*Sep 1 05:55:02.193: 0021.5C8C.C761 Sent Deauthenticate to mobile on BSSID
C8F9.F983.4260 slot 1(caller apf_ms.c: 1 wcm: 7036)
*Sep 1 05:55:02.193: 0021.5C8C.C761 apfMsExpireMobileStation (apf_ms.c: 1 wcm:
7092) Changing state for mobile 0021.5C8C.C761 on AP C8F9.F983.4260 from
Disassociated to Idle
*Sep 1 05:55:02.193: 0021.5C8C.C761 20.20.20.3 RUN (20) Deleted mobile LWAPP
rule on AP [ C8F9.F983.4260 ] 1 wcm: 5C8C.C761 on AP C8F9.F983.4260 from
Disassociated to Idle
*Sep 1 05:55:02.193: 0021.5C8C.C761 20.20.20.3 RUN (20) FastSSID for the
client [ C8F9.F983.4260 ] NOTENABLED 1 wcm: C.C761 on AP C8F9.F983.4260
from Disassociated to Idle
*Sep 1 05:55:02.193: 0021.5C8C.C761 Incrementing the Reassociation Count 1 for
client (of interface VLAN0020) 1 wcm: D
*Sep 1 05:55:02.193: 0021.5C8C.C761 Clearing Address 20.20.20.3 on mobile 1
wcm: for client (of interface VLAN0020)
*Sep 1 05:55:02.193: PEM rcv processing msg Del SCB(4) 1 wcm: 0.20.3 on
mobile
*Sep 1 05:55:02.193: 0021.5C8C.C761 20.20.20.3 RUN (20) Skipping TMP rule
add 1 wcm: lient (of interface VLAN0020)
*Sep 1 05:55:02.193: 0021.5C8C.C761 20.20.20.3 RUN (20) Change state to
DHCP_REQD (7) last state RUN (20) 1 wcm:
*Sep 1 05:55:02.193: 0021.5C8C.C761 WCDB_CHANGE: 1 wcm: Client 1 m_vlan 20
Radio iif id 0xbfcdc00000003a bssid iif id 0x8959800000004a, bssid
C8F9.F983.4260
*Sep 1 05:55:02.193: 0021.5C8C.C761 WCDB_AUTH: 1 wcm: Adding opt82 len 0
*Sep 1 05:55:02.193: 0021.5C8C.C761 WCDB_CHANGE: 1 wcm: Suppressing SPI
(client pending deletion) pemstate 7 state LEARN_IP(2) vlan 20 client_id
0xac70800000004b mob=Local(1) ackflag 2 dropd 0, delete 1
*Sep 1 05:55:02.193: 0021.5C8C.C761 Sending SPI spi_epm_epm_terminate_session
successful 1 wcm: pemstate 7 state LEARN_IP(2) vlan 20 client_id
0xac70800000004b mob=Local(1) ackflag 2 dropd 0, delete 1
*Sep 1 05:55:02.194: 0021.5C8C.C761 Sending SPI spi_epm_epm_terminate_session
successful 1 wcm: pemstate 7 state LEARN_IP(2) vlan 20 client_id
0xac70800000004b mob=Local(1) ackflag 2 dropd 0, delete 1
*Sep 1 05:55:02.194: 0021.5C8C.C761 Deleting wireless client; Reason code 0,
Preset 1, AAA cause 1 1 wcm: 7 state LEARN_IP(2) vlan 20 client_id
0xac70800000004b mob=Local(1) ackflag 2 dropd 0, delete 1
*Sep 1 05:55:02.194: 0021.5C8C.C761 WCDB_DEL: 1 wcm: Successfully sent

```

```

*Sep 1 05:55:02.194: 0021.5C8C.C761 Expiring mobile state delete 1 wcm: on
code 0, Preset 1, AAA cause 1
*Sep 1 05:55:02.194: 0021.5C8C.C761 0.0.0.0 DHCP_REQD (7) Handling pemDelScb
Event skipping delete 1 wcm: state LEARN_IP(2) vlan 20 client_id
0xac708000000004b mob=Local(1) ackflag 2 dropd 0, delete 1
*Sep 1 05:55:02.197: 0021.5C8C.C761 WCDB SPI response msg handler client code
1 mob state 1 1 wcm: g delete
*Sep 1 05:55:02.197: 0021.5C8C.C761 apfProcessWcdbClientDelete: 1 wcm: Delete
ACK from WCDB.
*Sep 1 05:55:02.197: 0021.5C8C.C761 WCDB_DELACK: 1 wcm: wcdbAckRecvdFlag
updated
*Sep 1 05:55:02.197: 0021.5C8C.C761 WCDB_DELACK: 1 wcm: Client IIF Id dealloc
SUCCESS w/ 0xac708000000004b.
*Sep 1 05:55:02.197: 0021.5C8C.C761 Invoked platform delete and cleared handle
1 wcm: w/ 0xac708000000004b.
*Sep 1 05:55:02.197: 0021.5C8C.C761 Deleting mobile on AP C8F9.F983.4260 (1)
1 wcm: w/ 0xac708000000004b.
*Sep 1 05:55:02.197: 0021.5C8C.C761 Unlinked and freed mscb 1 wcm:
8F9.F983.4260 (1)
*Sep 1 05:55:02.197: WCDB_IIF: 1 wcm: Ack Message ID: 0xac708000000004b code
1003
*Sep 1 05:55:02.379: 0021.5C8C.C761 Adding mobile on LWAPP AP C8F9.F983.4260
(1) 1 wcm: xac7080000.D^Iwb.
*Sep 1 05:55:02.379: 0021.5C8C.C761 Creating WL station entry for client -
rc 0 1 wcm:
*Sep 1 05:55:02.379: 0021.5C8C.C761 Association received from mobile on AP
C8F9.F983.4260 1 wcm: 0.D^Iwb.
*Sep 1 05:55:02.379: 0021.5C8C.C761 qos upstream policy is unknown and
downstream policy is unknown 1 wcm:
*Sep 1 05:55:02.379: 0021.5C8C.C761 apChanged 0 wlanChanged 0 mscb ipAddr
0.0.0.0, apf RadiusOverride 0x0, numIPv6Addr=0 1 wcm: \2105H□□^Iwlient_id
0xac708000^G$8\227v^K
*Sep 1 05:55:02.379: 0021.5C8C.C761 Applying WLAN policy on MSCB. 1 wcm:
ipAddr 0.0.0.0, apf RadiusOverride 0x0, numIPv6Addr=0
*Sep 1 05:55:02.379: 0021.5C8C.C761 Applying WLAN ACL policies to client 1
wcm: 0.0.0.0, apf RadiusOverride 0x0, numIPv6Addr=0
*Sep 1 05:55:02.379: 0021.5C8C.C761 No Interface ACL used for Wireless client
in WCM(NGWC) 1 wcm: usOverride 0x0, numIPv6Addr=0
*Sep 1 05:55:02.379: 0021.5C8C.C761 Applying site-specific IPv6 override for
station 0021.5C8C.C761 - vapId 5, site 'default-group', interface
'VLAN0020' 1 wcm:
*Sep 1 05:55:02.379: 0021.5C8C.C761 Applying local bridging Interface Policy
for station 0021.5C8C.C761 - vlan 20, interface 'VLAN0020' 1 wcm: erface
'VLAN0020'
*Sep 1 05:55:02.379: 0021.5C8C.C761 STA - rates (8): 1 wcm:
140 18 152 36 176 72 96 108 0 0 0 0 0 0
*Sep 1 05:55:02.379: 0021.5C8C.C761 new capwap_wtp_iif_id b6818000000038,
sm capwap_wtp_iif_id 0 1 wcm: 8C.C761 - vlan 20, interface 'VLAN0020'
*Sep 1 05:55:02.379: 0021.5C8C.C761 WCDB_ADD: 1 wcm: Radio IIFID
0xbfcfdc00000003a, BSSID IIF Id 0xbb30c0000000046, COS 4
*Sep 1 05:55:02.379: Load Balancer: 1 wcm: Success, Resource allocated are:
Active Switch number: 1, Active Asic number : 0, Reserve Switch number 0
Reserve Asic number 0. AP Asic num 0
*Sep 1 05:55:02.379: 0021.5C8C.C761 WCDB_ADD: 1 wcm: Anchor Sw 1, Doppler 0
*Sep 1 05:55:02.380: 0021.5C8C.C761 WCDB_ALLOCATE: 1 wcm: Client IIF Id alloc
SUCCESS w/ client 8e7bc000000004d (state 0).
*Sep 1 05:55:02.380: 0021.5C8C.C761 iifid Clearing Ack flag 1 wcm: F Id alloc
SUCCESS w/ client 8e7bc000000004d (state 0).
*Sep 1 05:55:02.380: 0021.5C8C.C761 WCDB_ADD: 1 wcm: Adding opt82 len 0
*Sep 1 05:55:02.380: 0021.5C8C.C761 WCDB_ADD: 1 wcm: Cleaering Ack flag
*Sep 1 05:55:02.380: 0021.5C8C.C761 WCDB_ADD: 1 wcm: ssid open bssid
C8F9.F983.4260 vlan 20 auth=ASSOCIATION(0) wlan(ap-group/global) 5/5
client 0 assoc 1 mob=Unassoc(0) radio 1 m_vlan 20 ip 0.0.0.0 src
0xb68180000000038 dst 0x0 cid 0x8e7bc000000004d glob rsc id 14dhcpsrv
0.0.0.0 ty
*Sep 1 05:55:02.380: 0021.5C8C.C761 WCDB_ADD: 1 wcm: mscb iifid
0x8e7bc000000004d msinfo iifid 0x0
*Sep 1 05:55:02.380: 0021.5C8C.C761 0.0.0.0 START (0) Initializing policy 1
wcm: info iifid 0x0
*Sep 1 05:55:02.380: 0021.5C8C.C761 0.0.0.0 START (0) Change state to
AUTHCHECK (2) last state AUTHCHECK (2) 1 wcm: -group/global) 5/5 client 0
assoc 1 mob=Unassoc(0) radio 1 m_vlan 20 ip 0.0.0.0 src 0xb68180000000038
dst 0x0 cid 0x8e7bc000000004d glob rsc id 14dhcpsrv 0.0.0.0 ty

```

```

*Sep 1 05:55:02.380: 0021.5C8C.C761 0.0.0.0 AUTHCHECK (2) Change state to
L2AUTHCOMPLETE (4) last state L2AUTHCOMPLETE (4) 1 wcm: 5/5 client 0 assoc
1 mob=Unassoc(0) radio 1 m_vlan 20 ip 0.0.0.0 src 0xb6818000000038 dst 0x0
cid 0x8e7bc00000004d glob_rsc id 14dhcpsrv 0.0.0.0 ty
*Sep 1 05:55:02.380: 0021.5C8C.C761 WCDB CHANGE: 1 wcm: Client 1 m_vlan 20
Radio iif id 0xbfcdc00000003a bssid iif id 0xbb30c000000046, bssid
C8F9.F983.4260
*Sep 1 05:55:02.380: 0021.5C8C.C761 WCDB_AUTH: 1 wcm: Adding opt82 len 0
*Sep 1 05:55:02.380: 0021.5C8C.C761 WCDB_LLM: 1 wcm: NoRun Prev Mob 0, Curr
Mob 0 llmReq 1, return False
*Sep 1 05:55:02.380: 0021.5C8C.C761 auth state 1 mob state 0 setWme 0 wme 1
roam_sent 0 1 wcm: rn False
*Sep 1 05:55:02.380: 0021.5C8C.C761 WCDB_CHANGE: 1 wcm: auth=L2_AUTH(1) vlan
20 radio 1 client_id 0x8e7bc00000004d mobility=Unassoc(0) src_int
0xb6818000000038 dst_int 0x0 ackflag 0 reassoc_client 0 llm_notif 0 ip
0.0.0.0 ip_learn_type UNKNOWN
*Sep 1 05:55:02.380: 0021.5C8C.C761 WCDB_CHANGE: 1 wcm: In L2 auth but l2ack
waiting lflag not set,so set
*Sep 1 05:55:02.380: 0021.5C8C.C761 0.0.0.0 L2AUTHCOMPLETE (4) DHCP Not
required on AP C8F9.F983.4260 vapId 5 apVapId 5for this client 1 wcm:
68180000000038 dst_int 0x0 ackflag 0 reassoc_client 0 llm_notif 0 i$=6v.0.0.0
it^Dv^\7HnP6v^D6H15Ht^Dv$6H8^r^D6H>&5v8^r^D6H>&5v^D6Ht^M^Lw^\7H8^r
*Sep 1 05:55:02.380: WCDB_IIF: 1 wcm: Ack Message ID: 0x8e7bc00000004d code
1001
*Sep 1 05:55:02.380: 0021.5C8C.C761 Not Using WMM Compliance code qosCap 00 1
wcm: quired on AP C8F9.F983.4260 vapId 5 apVapId 5for this client
*Sep 1 05:55:02.380: 0021.5C8C.C761 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed
mobile LWAPP rule on AP C8F9.F983.4260 vapId 5 apVapId 5 1 wcm: client
*Sep 1 05:55:02.380: 0021.5C8C.C761 0.0.0.0 L2AUTHCOMPLETE (4) Change state
to DHCP_REQD (7) last state DHCP_REQD (7) 1 wcm: apVapId 5
*Sep 1 05:55:02.380: 0021.5C8C.C761 WCDB CHANGE: 1 wcm: Client 1 m_vlan 20
Radio iif id 0xbfcdc00000003a bssid iif id 0xbb30c000000046, bssid
C8F9.F983.4260
*Sep 1 05:55:02.380: 0021.5C8C.C761 WCDB_AUTH: 1 wcm: Adding opt82 len 0
*Sep 1 05:55:02.380: 0021.5C8C.C761 WCDB_CHANGE: 1 wcm: Suppressing SPI
(Mobility state not known) pemstate 7 state LEARN_IP(2) vlan 20 client_id
0x8e7bc00000004d mob=Unassoc(0) ackflag 1 dropd 0
*Sep 1 05:55:02.380: 0021.5C8C.C761 Incrementing the Reassociation Count 1 for
client (of interface VLAN0020) 1 wcm: EARN_IP(2) vlan 20 client_id
0x8e7bc00000004d mob=Unassoc(0) ackflag 1 dropd 0
*Sep 1 05:55:02.380: 0021.5C8C.C761 apfPemAddUser2 (apf_policy.c: 1 wcm: 161)
Changing state for mobile 0021.5C8C.C761 on AP C8F9.F983.4260 from Idle
to Associated
*Sep 1 05:55:02.380: 0021.5C8C.C761 Scheduling deletion of Mobile Station: 1
wcm: (callerId: 49) in 1800 seconds
*Sep 1 05:55:02.380: 0021.5C8C.C761 Ms Timeout = 1800, Session Timeout = 1800
1 wcm: llerId: 49) in 1800 seconds
*Sep 1 05:55:02.381: 0021.5C8C.C761 Sending Assoc Response to station on BSSID
C8F9.F983.4260 (status 0) ApVapId 5 Slot 1 1 wcm: .F983.4260 from Idle to
Associated
*Sep 1 05:55:02.381: 0021.5C8C.C761 apfProcessAssocReq (apf_80211.c: 1 wcm:
5260) Changing state for mobile 0021.5C8C.C761 on AP C8F9.F983.4260
from Associated to Associated
*Sep 1 05:55:02.381: 0021.5C8C.C761 0.0.0.0 DHCP_REQD (7) pemAdvanceState2:
1 wcm: MOBILITY-INCOMPLETE with state 7.
*Sep 1 05:55:02.381: 0021.5C8C.C761 0.0.0.0 DHCP_REQD (7) pemAdvanceState2:
1 wcm: MOBILITY-INCOMPLETE with state 7.
*Sep 1 05:55:02.381: 0021.5C8C.C761 0.0.0.0 DHCP_REQD (7) pemAdvanceState2:
1 wcm: MOBILITY-COMPLETE with state 7.
*Sep 1 05:55:02.381: 0021.5C8C.C761 0.0.0.0 DHCP_REQD (7) State Update from
Mobility-Incomplete to Mobility-Complete, mobility role=Local, client
state=APF_MS_STATE ASSOCIATED 1 wcm: 1 dropd 0
*Sep 1 05:55:02.381: 0021.5C8C.C761 0.0.0.0 DHCP_REQD (7) pemAdvanceState2
3611, Adding TMP rule 1 wcm: o Mobility-Complete, mobility role=Local,
client state=APF_MS_STATE ASSOCIATED
*Sep 1 05:55:02.381: 0021.5C8C.C761 0.0.0.0 DHCP_REQD (7) Adding Fast Path
rule on AP C8F9.F983.4260 , slot 1 802.1P = 0 1 wcm: role=Local, client
state=APF_MS_STATE ASSOCIATED
*Sep 1 05:55:02.381: 0021.5C8C.C761 0.0.0.0 DHCP_REQD (7) Successfully
plumbed mobile rule 1 wcm: F9.F983.4260 , slot 1 802.1P = 0^M
*Sep 1 05:55:02.381: 0021.5C8C.C761 WCDB CHANGE: 1 wcm: Client 1 m_vlan 20
Radio iif id 0xbfcdc00000003a bssid iif id 0xbb30c000000046, bssid
C8F9.F983.4260

```

```

*Sep 1 05:55:02.381: 0021.5C8C.C761 WCDB_AUTH: 1 wcm: Adding opt82 len 0
*Sep 1 05:55:02.381: 0021.5C8C.C761 WCDB_LLM: 1 wcm: NoRun Prev Mob 0, Curr
  Mob 1 llmReq 1, return False
*Sep 1 05:55:02.381: 0021.5C8C.C761 WCDB_CHANGE: 1 wcm: Suppressing SPI (ACK
  message not recvd) pemstate 7 state LEARN_IP(2) vlan 20 client_id
  0x8e7bc00000004d mob=Local(1) ackflag 1 dropd 1
*Sep 1 05:55:02.381: 0021.5C8C.C761 Error updating wcdb on mobility complete
  1 wcm: not recvd) pemstate 7 state LEARN_IP(2) vlan 20 client_id
  0x8e7bc00000004d mob=Local(1) ackflag 1 dropd 1
*Sep 1 05:55:02.381: PEM rcv processing msg Epm spi response(12) 1 wcm:
  complete
*Sep 1 05:55:02.381: 0021.5C8C.C761 aaa attribute list length is 79 1 wcm:
  complete
*Sep 1 05:55:02.381: 0021.5C8C.C761 Sending SPI spi_epm_epm_session_create
  successfull 1 wcm: ) pemstate 7 state LEARN_IP(2) vlan 20 client_id
  0x8e7bc00000004d mob=Local(1) ackflag 1 dropd 1
*Sep 1 05:55:02.381: PEM rcv processing msg Add SCB(3) 1 wcm:
  pm_session_create successfull
*Sep 1 05:55:02.381: 0021.5C8C.C761 0.0.0.0, auth_state 7 mmRole Local !!! 1
  wcm: successfull
*Sep 1 05:55:02.381: 0021.5C8C.C761 0.0.0.0, auth_state 7 mmRole Local,
  updating wcdb not needed 1 wcm: 7 state LEARN_IP(2) vlan 20 client_id
  0x8e7bc00000004d mob=Local(1) ackflag 1 dropd 1
*Sep 1 05:55:02.381: 0021.5C8C.C761 Tclas Plumb needed: 1 wcm: 0
*Sep 1 05:55:02.384: EPM: 1 wcm: Session create resp - client handle
  8e7bc00000004d session b8000020
*Sep 1 05:55:02.384: EPM: 1 wcm: Netflow session create resp - client handle
  8e7bc00000004d sess b8000020
*Sep 1 05:55:02.384: PEM rcv processing msg Epm spi response(12) 1 wcm:
  le 8e7bc00000004d sess b8000020
*Sep 1 05:55:02.384: 0021.5C8C.C761 Received session_create_response for
  client handle 40105511256850509 1 wcm: LEARN_IP(2) vlan 20 client_id
  0x8e7bc00000004d mob=Local(1) ackflag 1 dropd 1
*Sep 1 05:55:02.384: 0021.5C8C.C761 Received session_create_response with EPM
  session handle 3087007776 1 wcm:
*Sep 1 05:55:02.384: 0021.5C8C.C761 Send request to EPM 1 wcm: ate_response
  with EPM session handle 3087007776
*Sep 1 05:55:02.384: 0021.5C8C.C761 aaa attribute list length is 5 1 wcm: e
  with EPM session handle 3087007776
*Sep 1 05:55:02.384: 0021.5C8C.C761 Sending Activate request for session
  handle 3087007776 successful 1 wcm: 6
*Sep 1 05:55:02.384: 0021.5C8C.C761 Post-auth policy request sent! Now wait
  for post-auth policy ACK from EPM 1 wcm: N_IP(2) vlan 20 client_id
  0x8e7bc00000004d mob=Local(1) ackflag 1 dropd 1
*Sep 1 05:55:02.384: 0021.5C8C.C761 WCDB SPI response msg handler client code
  0 mob state 0 1 wcm: licy ACK from EPM
*Sep 1 05:55:02.384: 0021.5C8C.C761 WcdbClientUpdate: 1 wcm: L2 Auth ACK from
  WCDB
*Sep 1 05:55:02.384: 0021.5C8C.C761 WCDB_L2ACK: 1 wcm: wcdbAckRecvdFlag
  updated
*Sep 1 05:55:02.384: 0021.5C8C.C761 WCDB_CHANGE: 1 wcm: Client 1 m_vlan 20
  Radio iif id 0xbfc0c00000003a bssid iif id 0xbb30c000000046, bssid
  C8F9.F983.4260
*Sep 1 05:55:02.384: 0021.5C8C.C761 WCDB_AUTH: 1 wcm: Adding opt82 len 0
*Sep 1 05:55:02.384: 0021.5C8C.C761 WCDB_LLM: 1 wcm: NoRun Prev Mob 0, Curr
  Mob 1 llmReq 1, return False
*Sep 1 05:55:02.385: 0021.5C8C.C761 auth state 2 mob state 1 setWme 0 wme 1
  roam sent 0 1 wcm: rn False
*Sep 1 05:55:02.385: 0021.5C8C.C761 WCDB_CHANGE: 1 wcm: auth=LEARN_IP(2) vlan
  20 radio 1 client_id 0x8e7bc00000004d mobility=Local(1) src_int
  0xb6818000000038 dst_int 0x0 ackflag 2 reassoc_client 0 llm_notif 0 ip
  0.0.0.0 ip_learn_type UNKNOWN
*Sep 1 05:55:02.385: EPM: 1 wcm: Init feature, client handle 8e7bc00000004d
  session b8000020 authz ec00000e
*Sep 1 05:55:02.385: EPM: 1 wcm: Activate feature client handle
  8e7bc00000004d sess b8000020 authz ec00000e
*Sep 1 05:55:02.385: PEM rcv processing msg Epm spi response(12) 1 wcm: 004d
  sess b8000020 authz ec00000e
*Sep 1 05:55:02.385: 0021.5C8C.C761 Received activate_features_resp for client
  handle 40105511256850509 1 wcm: 004d mobility=Local(1) src_int
  0xb6818000000038 dst_int 0x0 ackflag 2 reassoc_client 0 llm_notif 0
  ip$=6v0.0.0 ipt^_Dv^\7HnP6v^D6H15Ht^_Dv$6H8^ r^D6H>&5v8^
  r^D6H>&5v^D6Ht^M^Lw^\7H8^ r

```

```

*Sep 1 05:55:02.385: 0021.5C8C.C761 Received activate_features_resp for EPM
  session handle 3087007776 1 wcm: 9
*Sep 1 05:55:02.385: EPM: 1 wcm: Policy enforcement - client handle
  8e7bc00000004d session 2800000e authz ec00000e
*Sep 1 05:55:02.385: EPM: 1 wcm: Netflow policy enforcement - client handle
  8e7bc00000004d sess 2800000e authz ec00000e msg_type 0 policy_status 0 attr
  len 0
*Sep 1 05:55:02.385: PEM rcv processing msg Epm spi response(12) 1 wcm: e
  8e7bc00000004d sess 2800000e authz ec00000e msg_type 0 policy_status 0 attr
  len 0
*Sep 1 05:55:02.385: 0021.5C8C.C761 Received policy_enforcement_response for
  client handle 40105511256850509 1 wcm: 00e msg_type 0 policy_status 0 attr
  len 0
*Sep 1 05:55:02.385: 0021.5C8C.C761 Received policy_enforcement_response for
  EPM session handle 671088654 1 wcm: 09
*Sep 1 05:55:02.385: 0021.5C8C.C761 Received response for
  _EPM_SPI_ACTIVATE_FEATURES request sent for client 1 wcm: 00e msg_type 0
  policy_status 0 attr len 0
*Sep 1 05:55:02.385: 0021.5C8C.C761 Received _EPM_SPI_STATUS_SUCCESS for
  request sent for client 1 wcm: for client
*Sep 1 05:55:02.385: 0021.5C8C.C761 Post-auth policy ACK recvd from EPM, unset
  flag on MSCB 1 wcm: ient
*Sep 1 05:55:02.400: 0021.5C8C.C761 WCDB_IP_BIND: 1 wcm: w/ IPv4 20.20.20.3
  ip_learn_type DHCP add_delete 1,options length 0
*Sep 1 05:55:02.400: 0021.5C8C.C761 WcdbClientUpdate: 1 wcm: IP Binding from
  WCDB ip_learn_type 1, add_or_delete 1
*Sep 1 05:55:02.400: 0021.5C8C.C761 IPv4 Addr: 1 wcm: 20:20:20:3
*Sep 1 05:55:02.400: 0021.5C8C.C761 MS got the IP, resetting the Reassociation
  Count 0 for client 1 wcm: delete 1
*Sep 1 05:55:02.400: 0021.5C8C.C761 20.20.20.3 DHCP_REQD (7) Change state to
  RUN (20) last state RUN (20) 1 wcm: length 0
*Sep 1 05:55:02.400: 0021.5C8C.C761 WCDB CHANGE: 1 wcm: Client 1 m vlan 20
  Radio iif id 0xbfc00000003a bssid iif id 0xbb30c000000046, bssid
  C8F9.F983.4260
*Sep 1 05:55:02.400: 0021.5C8C.C761 WCDB AUTH: 1 wcm: Adding opt82 len 0
*Sep 1 05:55:02.401: 0021.5C8C.C761 WCDB_LLM: 1 wcm: prev Mob state 1 curr
  Mob State 1 llReq flag 0
*Sep 1 05:55:02.401: 0021.5C8C.C761 auth state 4 mob state 1 setWme 0 wme 1
  roam_sent 0 1 wcm: g 0
*Sep 1 05:55:02.401: 0021.5C8C.C761 WCDB CHANGE: 1 wcm: auth=RUN(4) vlan 20
  radio 1 client id 0x8e7bc00000004d mobility=Local(1) src_int
  0xb6818000000038 dst_int 0x0 ackflag 2 reassoc_client 0 llm_notif 0 ip
  20.20.20.3 ip_learn_type DHCP
*Sep 1 05:55:02.401: 0021.5C8C.C761 20.20.20.3 RUN (20) Reached
  PLUMBFASPATH: 1 wcm: from line 4430
*Sep 1 05:55:02.401: 0021.5C8C.C761 20.20.20.3 RUN (20) Replacing Fast Path
  rule on AP C8F9.F983.4260 , slot 1 802.1P = 0
  1 wcm: 0xb6818000000038 dst_int 0x0 ackflag 2 reassoc_client 0 llm_notif 0 ip
  20.20.20.3 ip_learn_type DHCP
  r^D6H>&5v^D6Ht^M^Lw^7H8^ r
*Sep 1 05:55:02.401: 0021.5C8C.C761 20.20.20.3 RUN (20) Successfully plumbed
  mobile rule 1 wcm: C8F9.F983.4260 , slot 1 802.1P = 0^M
*Sep 1 05:55:02.401: 0021.5C8C.C761
  Sending IPv4 update to Controller 10.105.135.176 1 wcm: e
*Sep 1 05:55:02.401: 0021.5C8C.C761 Assigning Address 20.20.20.3 to mobile 1
  wcm: 05.135.176
*Sep 1 05:55:02.401: PEM rcv processing msg Add SCB(3) 1 wcm: 20.20.3 to
  mobile
*Sep 1 05:55:02.401: 0021.5C8C.C761 20.20.20.3, auth_state 20 mmRole Local !!!
  1 wcm: 135.176
*Sep 1 05:55:02.401: 0021.5C8C.C761 20.20.20.3, auth_state 20 mmRole Local,
  updating wcdb not needed 1 wcm: 3.4260 , slot 1 802.1P = 0^M
*Sep 1 05:55:02.401: 0021.5C8C.C761 Tclas Plumb needed: 1 wcm: 0
*Sep 1 05:55:20.083: 0021.5C8C.C761
  Client stats update: 1 wcm: Time now in sec 1378014920, Last Acct Msg Sent at
  1378014902 sec

```

