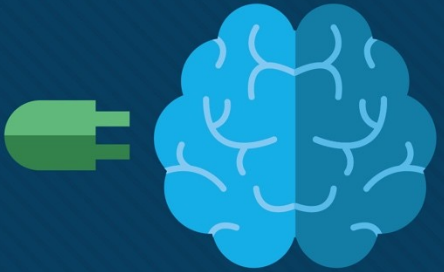
Chapter 20: Authenticating Wireless Clients
Chapter 21: Troubleshooting Wireless Connectivity



Instructor Materials

CCNP Enterprise: Core Networking

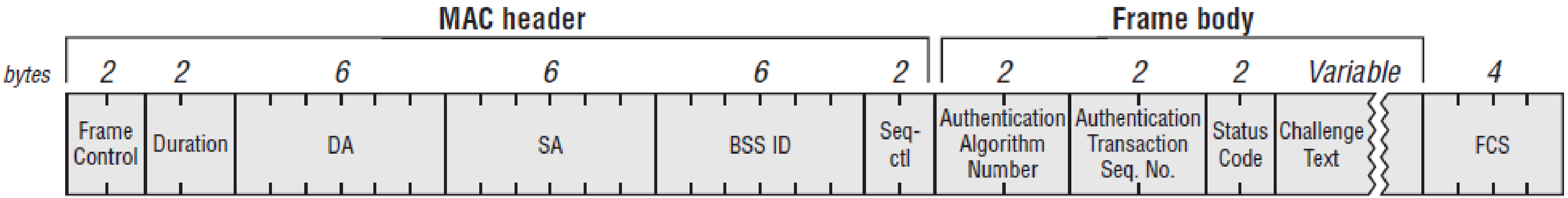
Open Authentication

Authentication

Once a client station is discover a SSID (Probe Request/Response or listening to Beacons) it move to Join phase. This exchange comprise of at least 4 frames

1. Authentication (Request)
2. Authentication (Response)
3. Association Request
4. Association Response

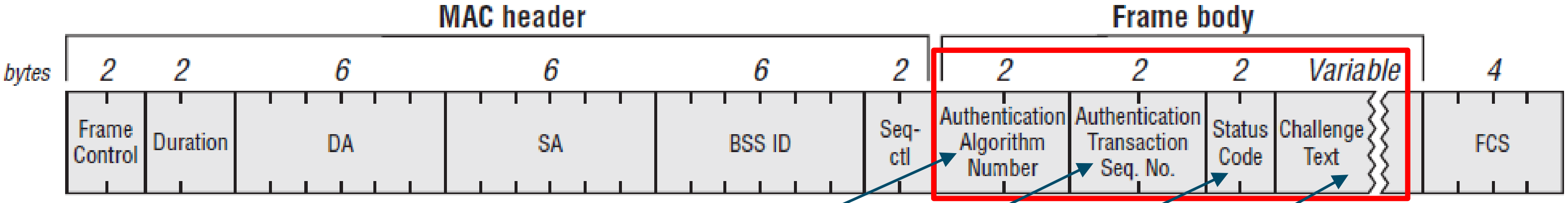
Authentication frame format



	MAC header						Frame body				
bytes	2	2	6	6	6	2	2	2	2	Variable	4
	Frame Control	Duration	DA	SA	BSS ID	Seq-ctl	Authentication Algorithm Number	Authentication Transaction Seq. No.	Status Code	Challenge Text	FCS

Open Authentication

Authentication frame format



Authentication Frame consist of the following fields

1. Authentication Algorithm Number
   - 0 for Open System
   - 1 for Shared Key
2. Authentication Transaction Sequence Number
   - Current state of progress
3. Status Code
   - 0 for Success
   - Unspecified failures
4. Challenge Text
   - Used in Shared Key Authentiction frame 2 & 3

Authentication frame field values & usages

Table below summarizes the authentication frame field values & usages.

Authentication algorithm	Authentication transaction sequence no.	Status code	Challenge text
Open System	1	Reserved	Not present
Open System	2	Status	Not present
Shared Key	1	Reserved	Not present
Shared Key	2	Status	Present
Shared Key	3	Reserved	Present
Shared Key	4	Status	Not present

Open Authentication

Authentication frame exchange

- The initial purpose of the authentication frame is to validate the device type (verify that the requesting station has proper 802.11 capability to join the cell).
- This exchanged is based on simple two-frame (Auth Request & Auth Response) called Open System.

- In IEEE 802.11-1997 standard included a **WEP** shared key exchange authentication mechanism called "**Shared Key**" where 4 authentication frame exchange.
- **When more complex authentication like 802.1X/EAP in place, Open System is used first & then complex method followed by Association frames**.

Authentication frame field values & usages

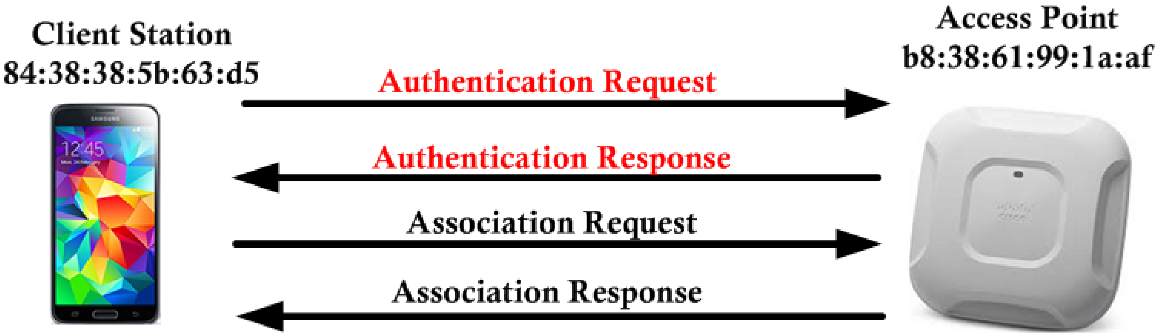
Table below summarizes the authentication frame field values & usages.

Authentication algorithm	Authentication transaction sequence no.	Status code	Challenge text
Open System	1	Reserved	Not present
Open System	2	Status	Not present
Shared Key	1	Reserved	Not present
Shared Key	2	Status	Present
Shared Key	3	Reserved	Present
Shared Key	4	Status	Not present

- The initial purpose of the authentication frame is to validate the device type (verify that the requesting station has proper 802.11 capability to join the cell).
- This exchanged is based on simple two-frame (Auth Request & Auth Response) called Open System.

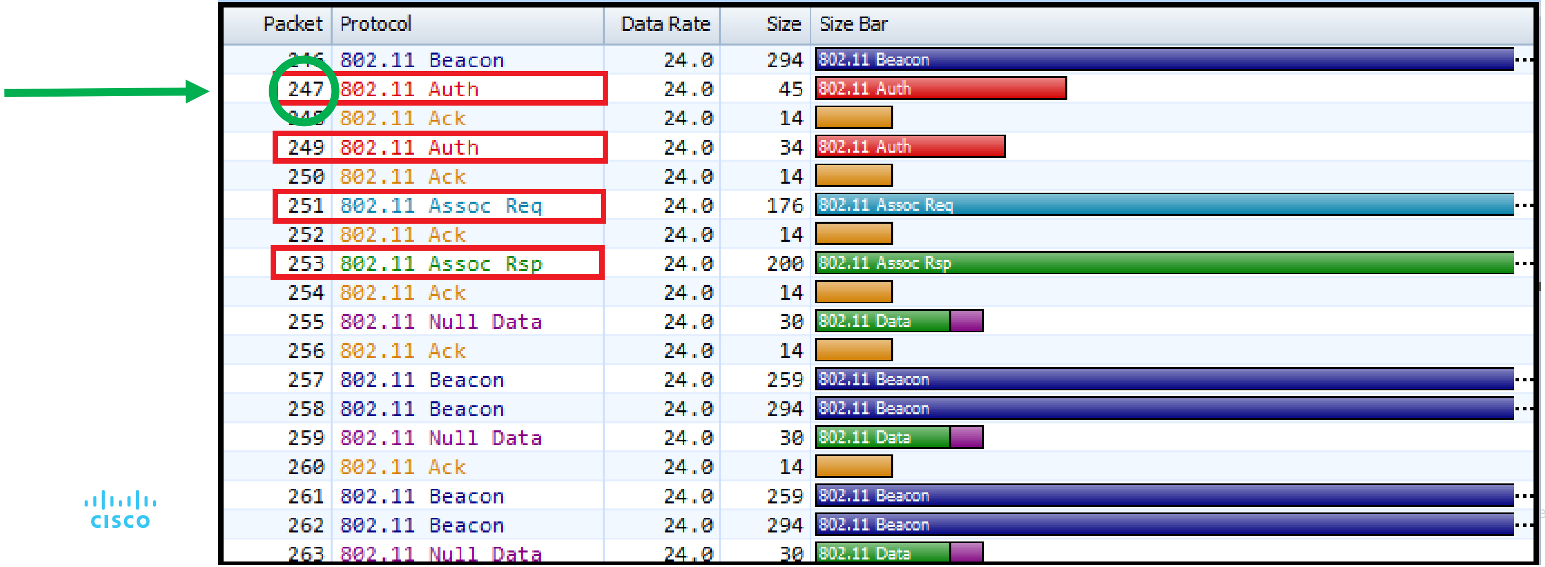
Open Authentication

Authentication details – Open System



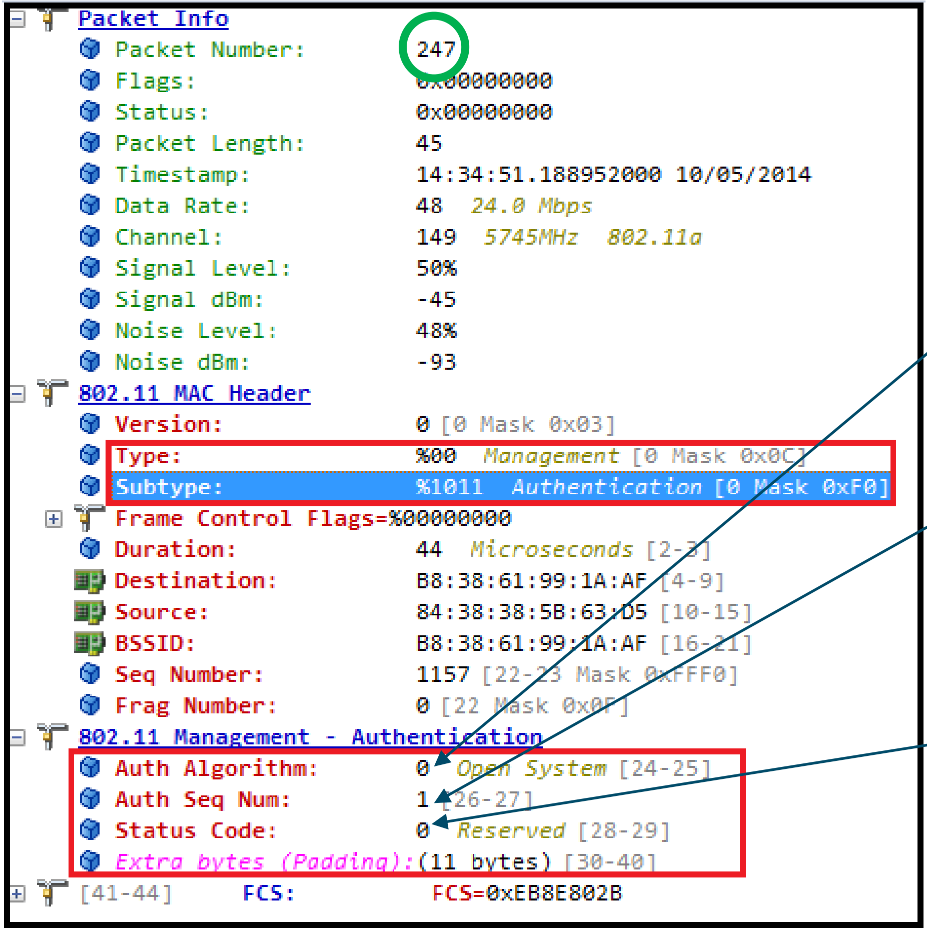
Client Station
84:38:38:5b:63:d5

Access Point
b8:38:61:99:1a:af



Packet	Protocol	Data Rate	Size	Size Bar
246	802.11 Beacon	24.0	294	802.11 Beacon
247	802.11 Auth	24.0	45	802.11 Auth
248	802.11 Ack	24.0	14	
249	802.11 Auth	24.0	34	802.11 Auth
250	802.11 Ack	24.0	14	
251	802.11 Assoc Req	24.0	176	802.11 Assoc Req
252	802.11 Ack	24.0	14	
253	802.11 Assoc Rsp	24.0	200	802.11 Assoc Rsp
254	802.11 Ack	24.0	14	
255	802.11 Null Data	24.0	30	802.11 Data
256	802.11 Ack	24.0	14	
257	802.11 Beacon	24.0	259	802.11 Beacon
258	802.11 Beacon	24.0	294	802.11 Beacon
259	802.11 Null Data	24.0	30	802.11 Data
260	802.11 Ack	24.0	14	
261	802.11 Beacon	24.0	259	802.11 Beacon
262	802.11 Beacon	24.0	294	802.11 Beacon
263	802.11 Null Data	24.0	30	802.11 Data

Authentication details – Open System – 1

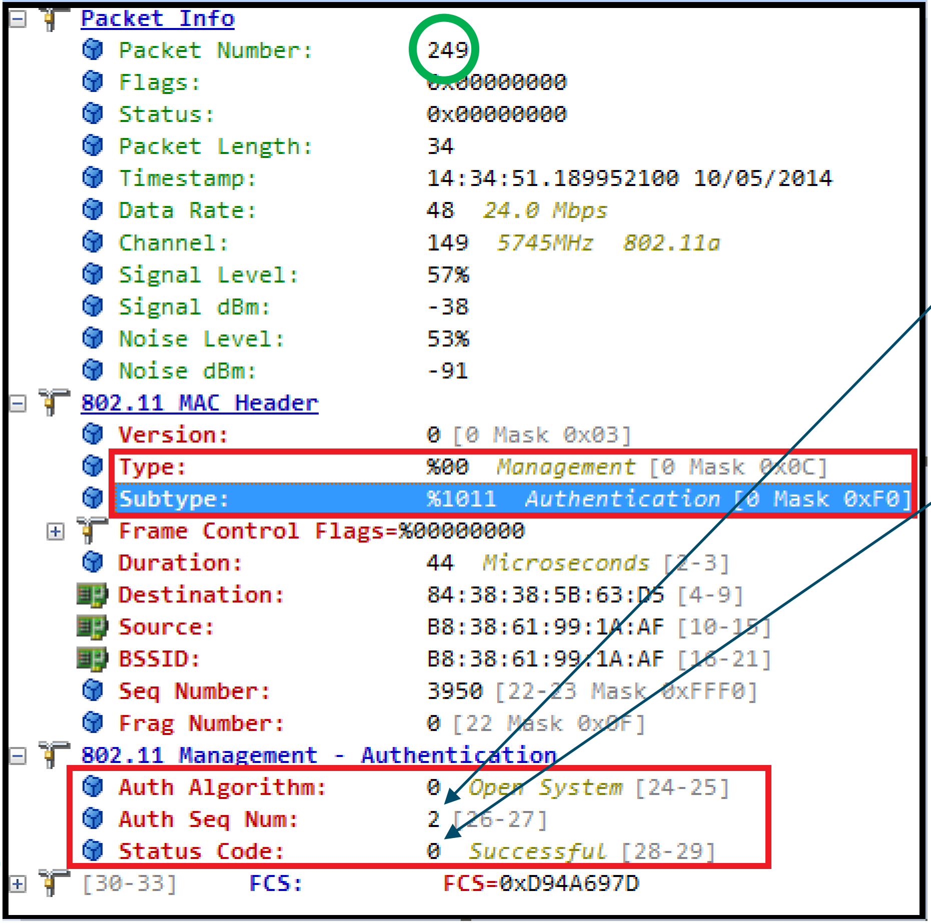


```
⊟ Packet Info
     Packet Number:         247
     Flags:                 0x00000000
     Status:                0x00000000
     Packet Length:         45
     Timestamp:             14:34:51.188952000 10/05/2014
     Data Rate:             48  24.0 Mbps
     Channel:               149  5745MHz  802.11a
     Signal Level:          50%
     Signal dBm:            -45
     Noise Level:           48%
     Noise dBm:             -93
⊟ 802.11 MAC Header
     Version:               0 [0 Mask 0x03]
     Type:                  %00  Management [0 Mask 0x0C]
     Subtype:               %1011  Authentication [0 Mask 0xF0]
  ⊞ Frame Control Flags=%00000000
     Duration:              44  Microseconds [2-3]
     Destination:           B8:38:61:99:1A:AF [4-9]
     Source:                84:38:38:5B:63:D5 [10-15]
     BSSID:                 B8:38:61:99:1A:AF [16-21]
     Seq Number:            1157 [22-23 Mask 0xFFF0]
     Frag Number:           0 [22 Mask 0x0F]
⊟ 802.11 Management - Authentication
     Auth Algorithm:        0  Open System [24-25]
     Auth Seq Num:          1 [26-27]
     Status Code:           0  Reserved [28-29]
     Extra bytes (Padding):(11 bytes) [30-40]
⊞ [41-44]     FCS:          FCS=0xEB8E802B
```

First Authentication Frame (Authentication Request, frame 247)

- Authentication Algorithm Number is 0 (indicate **Open System**).
- Auth Seq Number is 1 indicate this is the **first Authentication Frame** in the given exchange.
- Status code is **Reserved** for the first frame (refer the table above)

Authentication details – Open System – 2



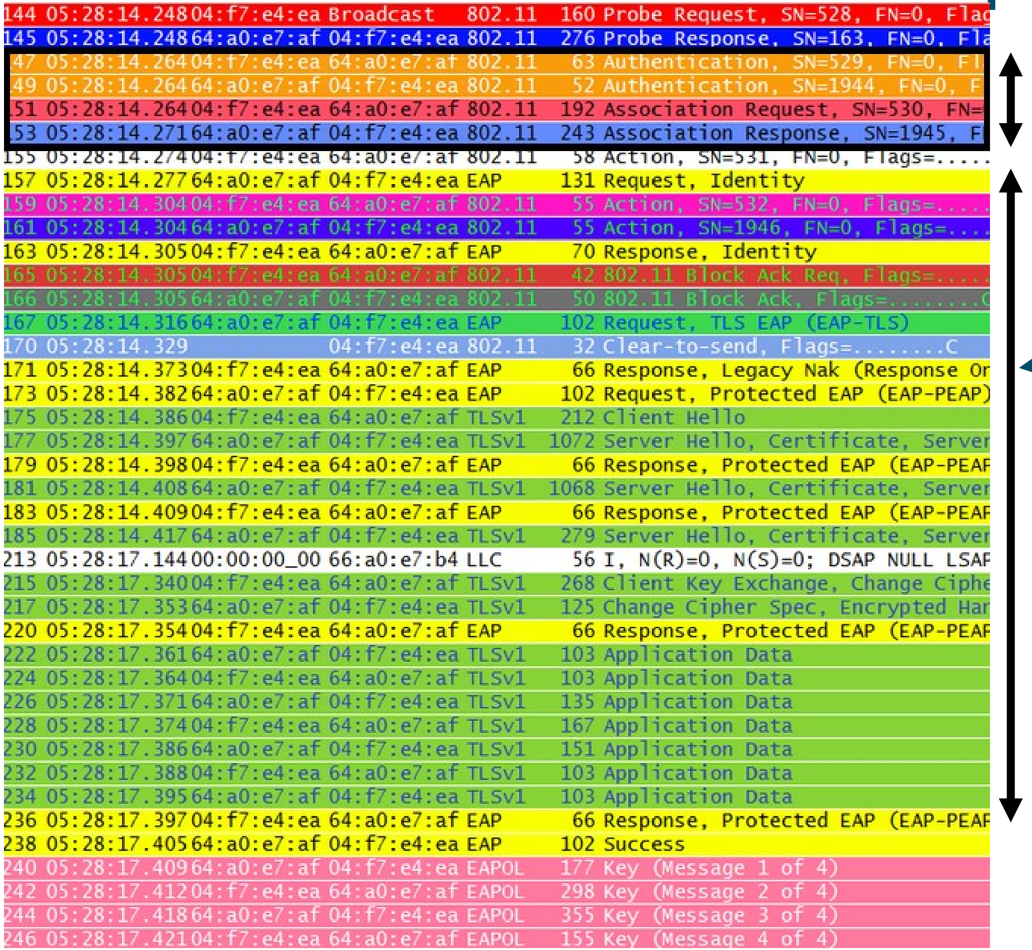
```
⊟ Packet Info
     Packet Number:          249
     Flags:                  0x00000000
     Status:                 0x00000000
     Packet Length:          34
     Timestamp:              14:34:51.189952100 10/05/2014
     Data Rate:              48  24.0 Mbps
     Channel:                149  5745MHz  802.11a
     Signal Level:           57%
     Signal dBm:             -38
     Noise Level:            53%
     Noise dBm:              -91
⊟ 802.11 MAC Header
     Version:                0 [0 Mask 0x03]
     Type:                   %00  Management [0 Mask 0x0C]
     Subtype:                %1011  Authentication [0 Mask 0xF0]
  ⊞ Frame Control Flags=%00000000
     Duration:               44  Microseconds [2-3]
     Destination:            84:38:38:5B:63:D5 [4-9]
     Source:                 B8:38:61:99:1A:AF [10-15]
     BSSID:                  B8:38:61:99:1A:AF [16-21]
     Seq Number:             3950 [22-23 Mask 0xFFF0]
     Frag Number:            0 [22 Mask 0x0F]
⊟ 802.11 Management - Authentication
     Auth Algorithm:         0  Open System [24-25]
     Auth Seq Num:           2 [26-27]
     Status Code:            0  Successful [28-29]
⊞ [30-33]      FCS:          FCS=0xD94A697D
```

Second Auth Frame (Auth Response, frame 249)

- Auth Seq Number is 2 indicating this is **Auth Response** frame.
- Status code is 0 indicating **successful** Open System Authentication.

Open Authentication

Authentication details – Open System – 3 ...



```
144 05:28:14.248 04:f7:e4:ea Broadcast   802.11  160 Probe Request, SN=528, FN=0, Flag
145 05:28:14.248 64:a0:e7:af 04:f7:e4:ea 802.11  276 Probe Response, SN=163, FN=0, Fla
 47 05:28:14.264 04:f7:e4:ea 64:a0:e7:af 802.11   63 Authentication, SN=529, FN=0, Fl
 49 05:28:14.264 64:a0:e7:af 04:f7:e4:ea 802.11   52 Authentication, SN=1944, FN=0, F
 51 05:28:14.264 04:f7:e4:ea 64:a0:e7:af 802.11  192 Association Request, SN=530, FN=
 53 05:28:14.271 64:a0:e7:af 04:f7:e4:ea 802.11  243 Association Response, SN=1945, F
155 05:28:14.274 04:f7:e4:ea 64:a0:e7:af 802.11   58 Action, SN=531, FN=0, Flags=.....
157 05:28:14.277 64:a0:e7:af 04:f7:e4:ea EAP     131 Request, Identity
159 05:28:14.304 04:f7:e4:ea 64:a0:e7:af 802.11   55 Action, SN=532, FN=0, Flags=.....
161 05:28:14.304 64:a0:e7:af 04:f7:e4:ea 802.11   55 Action, SN=1946, FN=0, Flags=....
163 05:28:14.305 04:f7:e4:ea 64:a0:e7:af EAP      70 Response, Identity
165 05:28:14.305 04:f7:e4:ea 64:a0:e7:af 802.11   42 802.11 Block Ack Req, Flags=.....
166 05:28:14.305 64:a0:e7:af 04:f7:e4:ea 802.11   50 802.11 Block Ack, Flags=........C
167 05:28:14.316 64:a0:e7:af 04:f7:e4:ea EAP     102 Request, TLS EAP (EAP-TLS)
170 05:28:14.329             04:f7:e4:ea 802.11   32 Clear-to-send, Flags=........C
171 05:28:14.373 04:f7:e4:ea 64:a0:e7:af EAP      66 Response, Legacy Nak (Response Or
173 05:28:14.382 64:a0:e7:af 04:f7:e4:ea EAP     102 Request, Protected EAP (EAP-PEAP)
175 05:28:14.386 04:f7:e4:ea 64:a0:e7:af TLSv1   212 Client Hello
177 05:28:14.397 64:a0:e7:af 04:f7:e4:ea TLSv1  1072 Server Hello, Certificate, Server
179 05:28:14.398 04:f7:e4:ea 64:a0:e7:af EAP      66 Response, Protected EAP (EAP-PEAF
181 05:28:14.408 64:a0:e7:af 04:f7:e4:ea TLSv1  1068 Server Hello, Certificate, Server
183 05:28:14.409 04:f7:e4:ea 64:a0:e7:af EAP      66 Response, Protected EAP (EAP-PEAF
185 05:28:14.417 64:a0:e7:af 04:f7:e4:ea TLSv1   279 Server Hello, Certificate, Server
213 05:28:17.144 00:00:00_00 66:a0:e7:b4 LLC      56 I, N(R)=0, N(S)=0; DSAP NULL LSAF
215 05:28:17.340 04:f7:e4:ea 64:a0:e7:af TLSv1   268 Client Key Exchange, Change Ciphe
217 05:28:17.353 64:a0:e7:af 04:f7:e4:ea TLSv1   125 Change Cipher Spec, Encrypted Har
220 05:28:17.354 04:f7:e4:ea 64:a0:e7:af EAP      66 Response, Protected EAP (EAP-PEAF
222 05:28:17.361 64:a0:e7:af 04:f7:e4:ea TLSv1   103 Application Data
224 05:28:17.364 04:f7:e4:ea 64:a0:e7:af TLSv1   103 Application Data
226 05:28:17.371 64:a0:e7:af 04:f7:e4:ea TLSv1   135 Application Data
228 05:28:17.374 04:f7:e4:ea 64:a0:e7:af TLSv1   167 Application Data
230 05:28:17.386 64:a0:e7:af 04:f7:e4:ea TLSv1   151 Application Data
232 05:28:17.388 04:f7:e4:ea 64:a0:e7:af TLSv1   103 Application Data
234 05:28:17.395 64:a0:e7:af 04:f7:e4:ea TLSv1   103 Application Data
236 05:28:17.397 04:f7:e4:ea 64:a0:e7:af EAP      66 Response, Protected EAP (EAP-PEAF
238 05:28:17.405 64:a0:e7:af 04:f7:e4:ea EAP     102 Success
240 05:28:17.409 64:a0:e7:af 04:f7:e4:ea EAPOL   177 Key (Message 1 of 4)
242 05:28:17.412 04:f7:e4:ea 64:a0:e7:af EAPOL   298 Key (Message 2 of 4)
244 05:28:17.418 64:a0:e7:af 04:f7:e4:ea EAPOL   355 Key (Message 3 of 4)
246 05:28:17.421 04:f7:e4:ea 64:a0:e7:af EAPOL   155 Key (Message 4 of 4)
```

- Even in a 802.1X/EAP Authentication, **Always Open System** Authentication occur **first**
- Then **followed by EAP** Authentication & 4 Way handshake prior to encrypt data.

- *Here is 802.11r FT Association where 802.1X frame exchange after the Open System Authentication & Association completes.*

Open Authentication

- To join and use a wireless network, wireless clients must first discover a basic service set (BSS) and then request permission to associate with it. At that point, clients should be authenticated by some means before they can become functioning members of a wireless LAN.
- The sections that follow explain four types of client authentication you will likely encounter on the CCNP and CCIE Enterprise ENCOR 350-401 exam and in common use.
- With each type, you will begin by creating a new WLAN on the wireless LAN controller, assigning a controller interface, and enabling the WLAN. Because wireless security is configured on a per-WLAN basis, all of the configuration tasks related to this chapter occur in the WLAN > Edit Security tab.

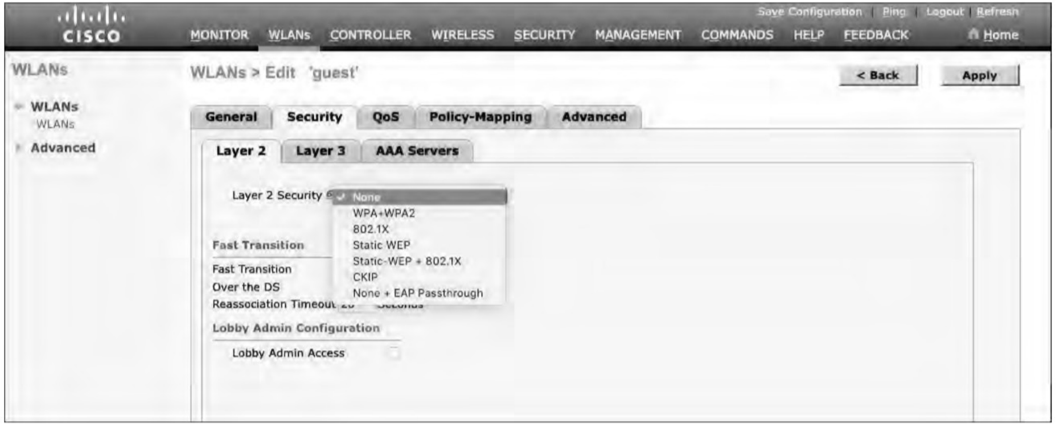
Open Authentication

- Recall that a wireless client device must send 802.11 authentication request and association request frames to an AP when it asks to join a wireless network.
- The original 802.11 standard offered only two choices to authenticate a client: Open Authentication and WEP.
- Open Authentication offers open access to a WLAN. The only requirement is that a client must use an 802.11 authentication request before it attempts to associate with an AP. No other credentials are needed.
- You have probably seen a WLAN with Open Authentication when you have visited a public location.
- If any client screening is used at all, it comes in the form of Web Authentication.

Open Authentication

Creating a WLAN with Open Authentication

- Create a new WLAN and map it to the correct VLAN.
- Go to the General tab and enter the SSID string, apply the appropriate controller interface, and change the status to Enabled.
- Next, select the Security tab to configure the WLAN security and user authentication parameters. Select the Layer 2 tab and then use the Layer 2 Security drop-down menu to select None for Open Authentication, as shown in Figure 20-2.
- When you are finished configuring the WLAN, click the Apply button.



WLANs > Edit 'guest'

Layer 2 Security: None

Fast Transition

Fast Transition

Over the DS

Reassociation Timeout 20 Seconds

Lobby Admin Configuration

Lobby Admin Access

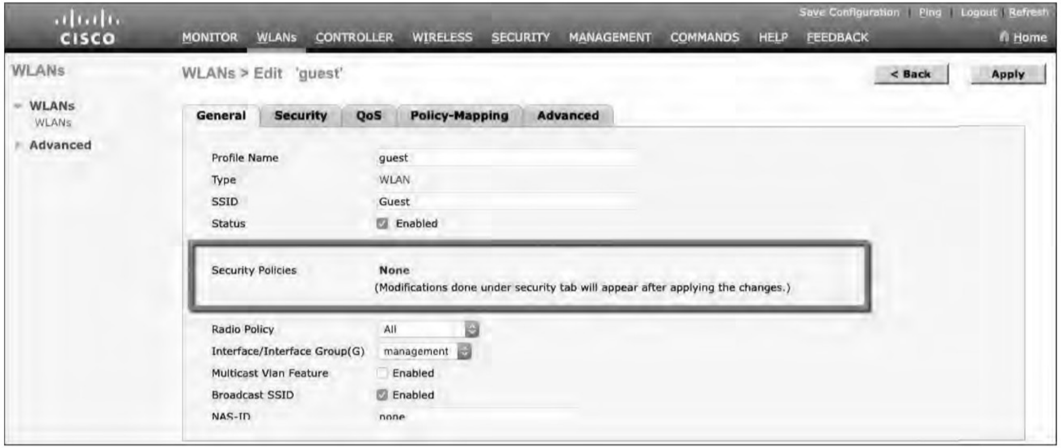
Figure 20-2 *Configuring Open Authentication for a WLAN*

Open Authentication

Creating a WLAN with Open Authentication (Cont.)

You can verify the WLAN and its security settings from the WLANs > Edit General tab, as shown in Figure 20-3 or from the list of WLANs, as shown in Figure 20-4.

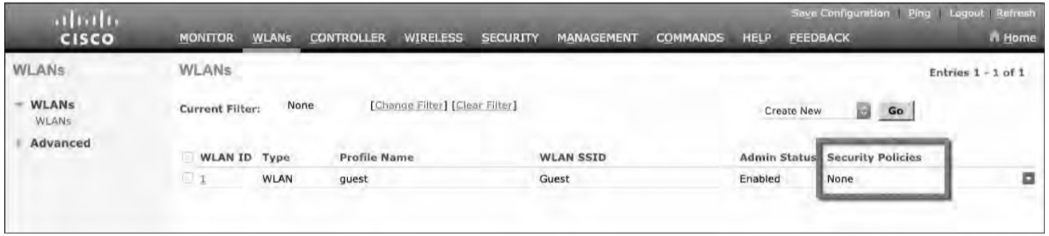
In both figures, the Security Policies field is shown as None. You can also verify that the WLAN status is enabled and active.



WLANs > Edit 'guest'

Profile Name	guest
Type	WLAN
SSID	Guest
Status	☑ Enabled
Security Policies	None (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	management
Multicast Vlan Feature	□ Enabled
Broadcast SSID	☑ Enabled
NAS-ID	none

Figure 20-3 *Verifying Open Authentication in the WLAN Configuration*



WLANs

Entries 1 - 1 of 1

Current Filter: None [Change Filter] [Clear Filter]

□ WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
□ 1	WLAN	guest	Guest	Enabled	None

Figure 20-4 *Verifying Open Authentication from List of WLANs*

Authenticating with Pre-Shared Key

- To secure wireless connections on a WLAN, you can leverage one of the Wi-Fi Protected Access (WPA) versions: WPA (also known as WPA1), WPA2, or WPA3.
- Each version is certified by the Wi-Fi Alliance so that wireless clients and APs using the same version are known to be compatible.
- The WPA versions also specify encryption and data integrity methods to protect data passing over the wireless connections.
- All three WPA versions support two client authentication modes, Pre-Shared Key (PSK) or 802.1x, depending on the scale of the deployment.

Authenticating with Pre-Shared Key

Wi-Fi Protected Access PSK

Beyond authentication, the Wi-Fi Protected Access also specify encryption and data integrity methods to protect data in the wireless connections. There are following WPA versions:

- WPA (also known as WPA1, did not need new HW)
- **WPA2**
- **WPA3**

All three WPA versions support two client authentication modes, Pre-Shared Key (PSK) or 802.1x, depending on the scale of the deployment. These are also known as personal mode and enterprise mode, respectively.

Personal mode:

- A key string must be shared or configured on every client and AP before the clients can connect to the wireless network.
- The pre-shared key is normally kept confidential so that unauthorized users have no knowledge of it.
- Clients and APs work through a four-way handshake procedure that uses the pre-shared key string to construct and exchange encryption key material that can be openly exchanged. When that process is successful, the AP can authenticate the client, and the two can secure data frames that are sent over the air.

Simultaneous Authentication of Equals (SAE)

With WPA-Personal and WPA2-Personal modes, a malicious user can eavesdrop and capture the four-way handshake between a client and an AP. A dictionary attack can be used to automate the guessing of the pre-shared key. If successful, the malicious user can then decrypt the wireless data or even join the network, posing as a legitimate user.

WPA3-Personal avoids such an attack by strengthening the key exchange between clients and APs through a method known as Simultaneous Authentication of Equals (SAE). Rather than a client authenticating against a server or AP, the client and AP can initiate the authentication process equally and even simultaneously.

Even if a password or key is compromised, WPA3-Personal offers forward secrecy, which prevents attackers from being able to use a key to unencrypt data that has already been transmitted over the air.

The personal mode of any WPA version is usually easy to deploy in a small environment.

Authenticating with Pre-Shared Key

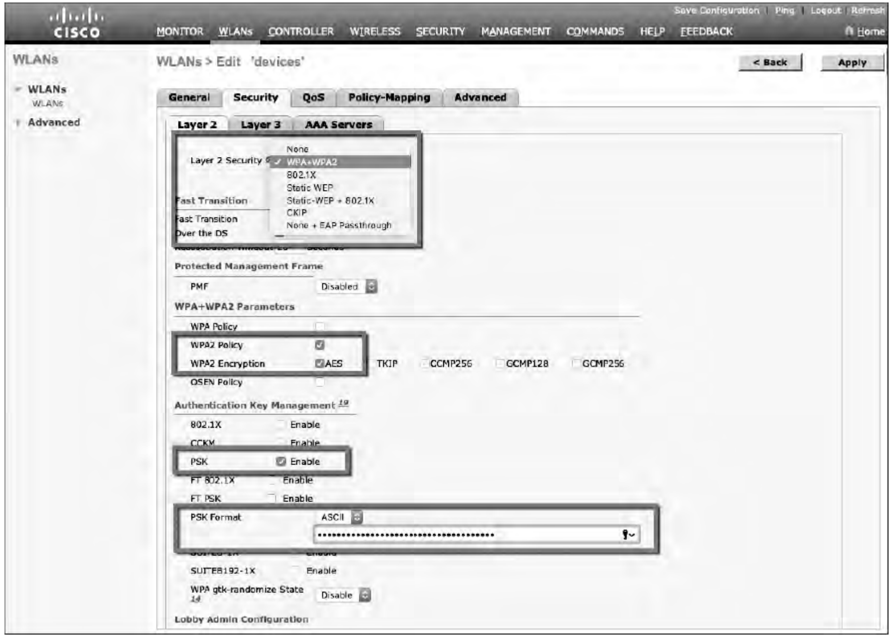
Configuring PSK

You can configure WPA2 or WPA3 personal mode and the pre-shared key with these steps:

Step 1. Navigate to WLANs, select Create New or select the WLAN ID of an existing WLAN to edit. Make sure the parameters on the General tab are set appropriately.

Step 2. Next, select the Security > Layer 2 tab. In the Layer 2 Security drop-down menu, select the appropriate WPA version for the WLAN. In Figure 20-5, WPA+WPA2 has been selected for the WLAN named devices.

Step 3. Under WPA+WPA2 Parameters, the WPA version has been narrowed to only WPA2 by unchecking the box next to WPA and checking both WPA2 Policy and WPA2 Encryption AES.



WLANs > Edit 'devices'

Layer 2 Security ✓ WPA+WPA2

Fast Transition

Fast Transition Over the DS

Protected Management Frame

PMF Disabled

WPA+WPA2 Parameters

WPA Policy □

WPA2 Policy ☑

WPA2 Encryption ☑AES □TKIP □CCMP256 □GCMP128 □GCMP256

OSEN Policy □

Authentication Key Management 19

802.1X □ Enable

CCKM □ Enable

PSK ☑ Enable

FT 802.1X □ Enable

FT PSK □ Enable

PSK Format ASCII

••

SUITEB192-1X □ Enable

WPA gtk-randomize State 14 Disable

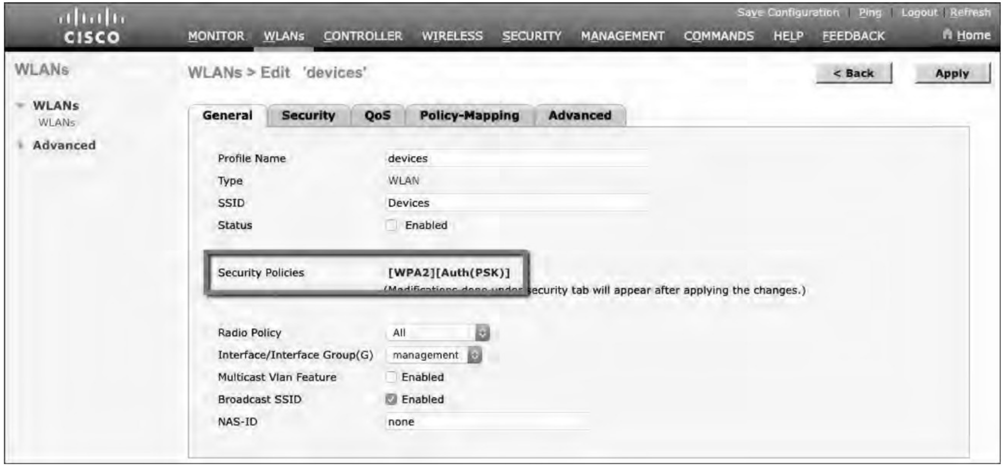
Lobby Admin Configuration

Figure 20-5 *Selecting the WPA2 Personal Security Suite for a WLAN*

Authenticating with Pre-Shared Key

Verifying PSK

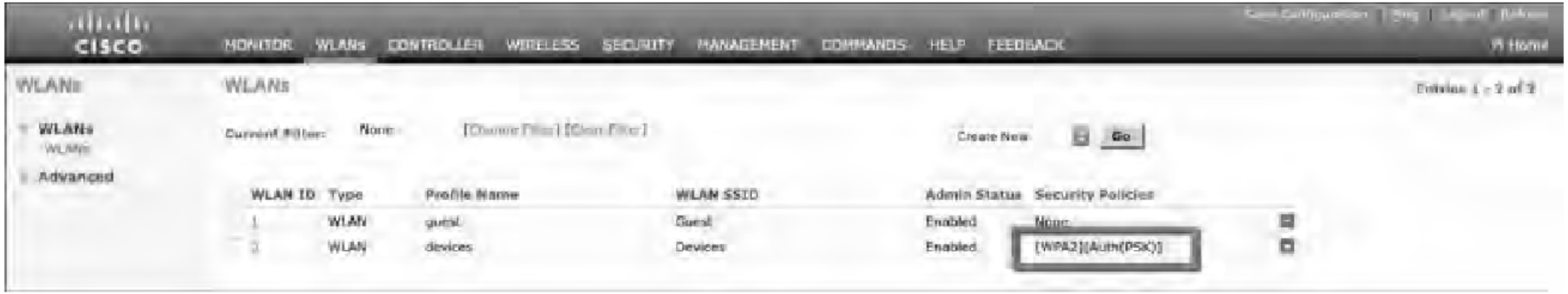
You can verify the WLAN and its security settings from the WLANs > Edit General tab, as shown in Figure 20-6 or from the list of WLANs, as shown in Figure 20-7. In both figures, the Security Policies field is shown as [WPA2][Auth(PSK)]. You can also verify that the WLAN status is enabled and active.


Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Home
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General
Security
QoS
Policy-Mapping
Advanced

WLANs > Edit 'devices'

Profile Name	devices
Type	WLAN
SSID	Devices
Status	□ Enabled
Security Policies	[WPA2][Auth(PSK)]
	(Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	management
Multicast Vlan Feature	□ Enabled
Broadcast SSID	☑ Enabled
NAS-ID	none

Figure 20-6 *Verifying PSK Authentication in the WLAN Configuration*


Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Home
WLANs
WLANs
WLANs
Advanced
Create New
Go

WLANs

Entries 1 - 2 of 2

Current Filter: None [Change Filter] [Clear Filter]

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	guest	Guest	Enabled	None
2	WLAN	devices	Devices	Enabled	[WPA2][Auth(PSK)]

Figure 20-7 *Verifying PSK Authentication from the List of WLANs*

Authenticating with EAP

- Rather than build additional authentication methods into the 802.11 standard, Extensible Authentication Protocol (EAP) offers a more flexible and scalable authentication framework.
- EAP is extensible and does not consist of any one authentication method. Instead, EAP defines a set of common functions that actual authentication methods can use to authenticate users.
- It can integrate with the IEEE 802.1x port-based access control standard. When 802.1x is enabled, it limits access to a network medium until a client authenticates. This means that a wireless client might be able to associate with an AP but will not be able to pass data to any other part of the network until it successfully authenticates.

802.1x Client Authentication Roles

With Open Authentication and PSK authentication, wireless clients are authenticated locally at the AP without further intervention. The scenario changes with 802.1x; the client uses Open Authentication to associate with the AP, and then the actual client authentication process occurs at a dedicated authentication server.

Figure 20-8 shows the three-party 802.1x arrangement, which consists of the following entities:

- **Supplicant -** The client device that is requesting access.
- **Authenticator -** The network device that provides access to the network (usually a wireless LAN controller [WLC]).
- **Authentication server (AS) -** The device that takes user or client credentials and permits or denies network access based on a user database and policies (usually a RADIUS server).

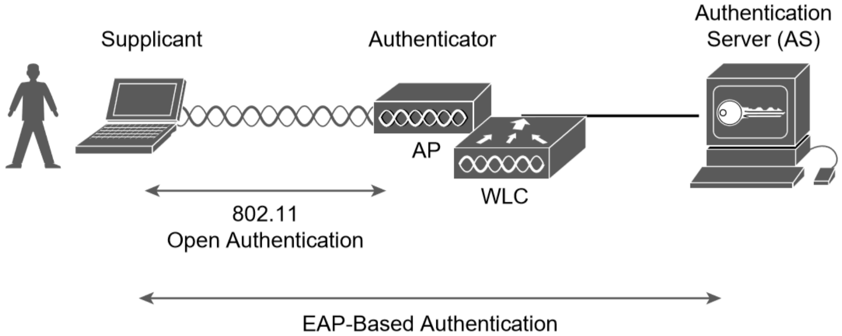


Figure 20-8 *802.1x Client Authentication Roles*

The controller becomes a middleman in the client authentication process, controlling user access with 802.1x and communicating with the authentication server using the EAP framework.

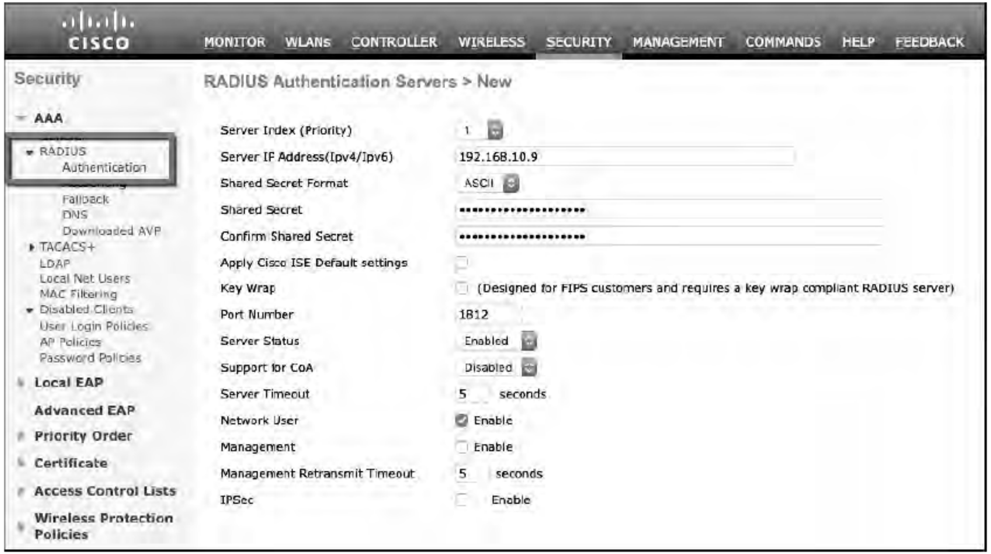
Authenticating with EAP

Configuring EAP-Based Authentication with External RADIUS Servers

Cisco WLCs can use either external RADIUS servers located somewhere on the wired network or a local EAP server located on the WLC.

You should begin by configuring one or more external RADIUS servers on the controller. Navigate to Security > AAA > RADIUS > Authentication.

- Click the New button to define a new server or select the Server Index number to edit an existing server definition.
- Enter the server's IP address and the shared secret key that the controller will use to communicate with the server.



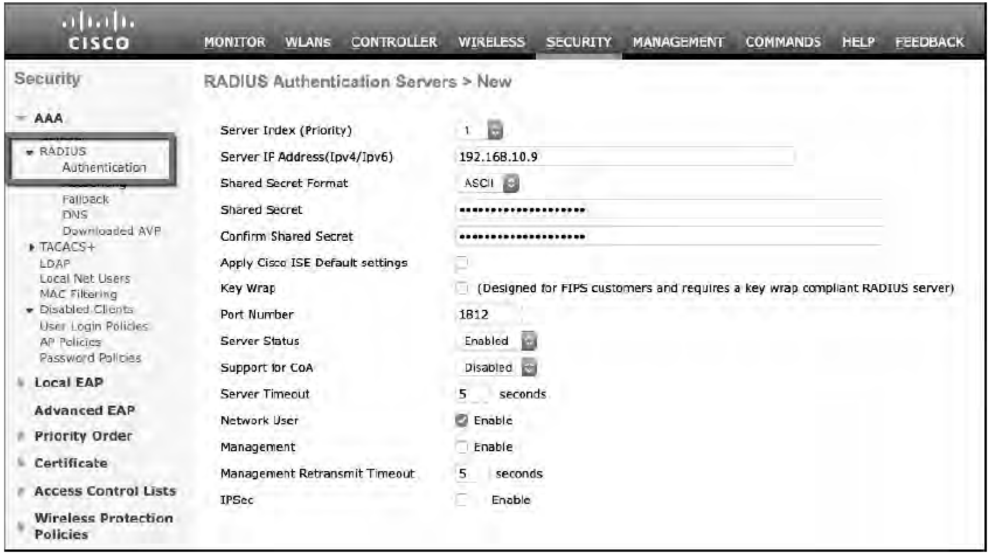
RADIUS Authentication Servers > New

Server Index (Priority)	1
Server IP Address(Ipv4/Ipv6)	192.168.10.9
Shared Secret Format	ASCII
Shared Secret	••••••••••••••••••••
Confirm Shared Secret	••••••••••••••••••••
Apply Cisco ISE Default settings	□
Key Wrap	□ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for CoA	Disabled
Server Timeout	5 seconds
Network User	☑ Enable
Management	□ Enable
Management Retransmit Timeout	5 seconds
IPSec	□ Enable

Figure 20-9 *Defining a RADIUS Server for WPA2 Enterprise Authentication*

Configuring EAP-Based Authentication with External RADIUS Servers (Cont.)

- Make sure that the RADIUS port number is correct.
- The server status should be Enabled, as selected from the drop-down menu. You can disable a server to take it out of service if needed.
- To authenticate wireless clients, check the Enable box next to Network User. Click the Apply button to apply the new settings.



RADIUS Authentication Servers > New

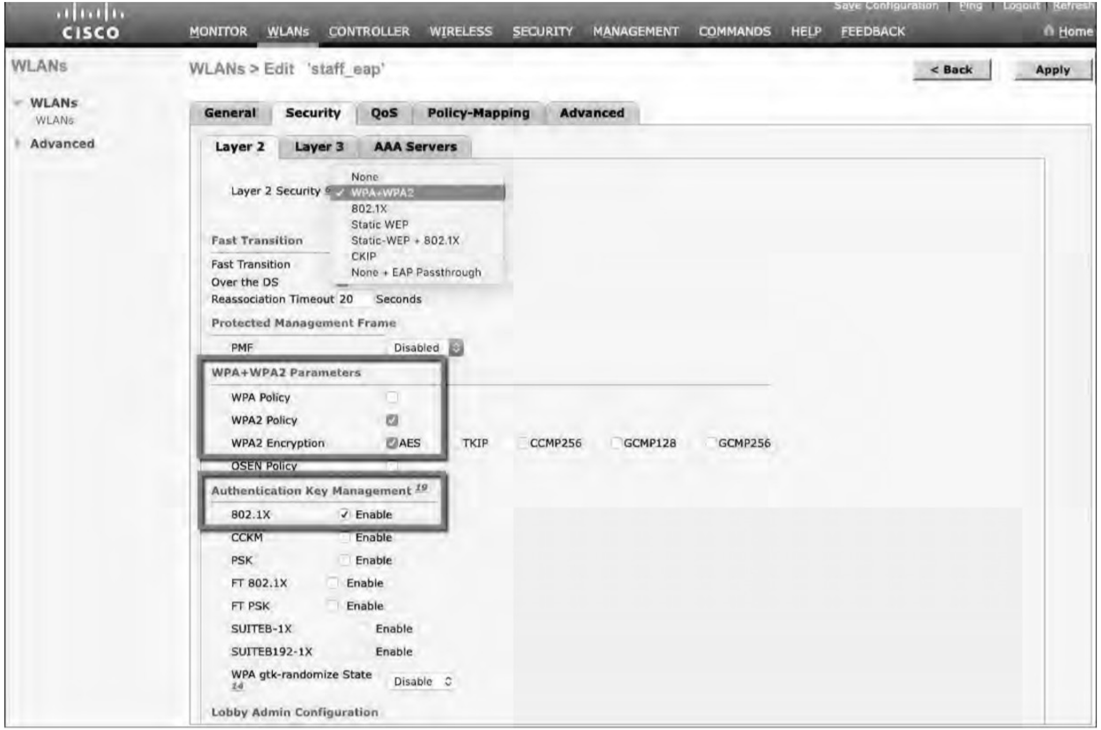
Server Index (Priority)	1
Server IP Address(Ipv4/Ipv6)	192.168.10.9
Shared Secret Format	ASCII
Shared Secret	••••••••••••••••••••
Confirm Shared Secret	••••••••••••••••••••
Apply Cisco ISE Default settings	□
Key Wrap	□ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for CoA	Disabled
Server Timeout	5 seconds
Network User	☑ Enable
Management	□ Enable
Management Retransmit Timeout	5 seconds
IPSec	□ Enable

Figure 20-9 *Defining a RADIUS Server for WPA2 Enterprise Authentication*

Configuring EAP-Based Authentication with External RADIUS Servers (Cont.)

Next, you need to enable 802.1x authentication on the WLAN. Navigate to WLANs and select a new or existing WLAN to edit.

Figure 20-10 illustrates the settings that are needed on the WLAN named staff_eap.



WLANs > Edit 'staff_eap'

Layer 2 Security: None / ✓ WPA+WPA2 / 802.1X / Static WEP / Static-WEP + 802.1X / CKIP / None + EAP Passthrough

Fast Transition

Fast Transition

Over the DS

Reassociation Timeout 20 Seconds

Protected Management Frame

PMF Disabled

WPA+WPA2 Parameters

WPA Policy □

WPA2 Policy ☑

WPA2 Encryption ☑ AES □ TKIP □ CCMP256 □ GCMP128 □ GCMP256

OSEN Policy □

Authentication Key Management [19]

802.1X ✓ Enable

CCKM □ Enable

PSK □ Enable

FT 802.1X □ Enable

FT PSK □ Enable

SUITEB-1X Enable

SUITEB192-1X Enable

WPA gtk-randomize State [14] Disable

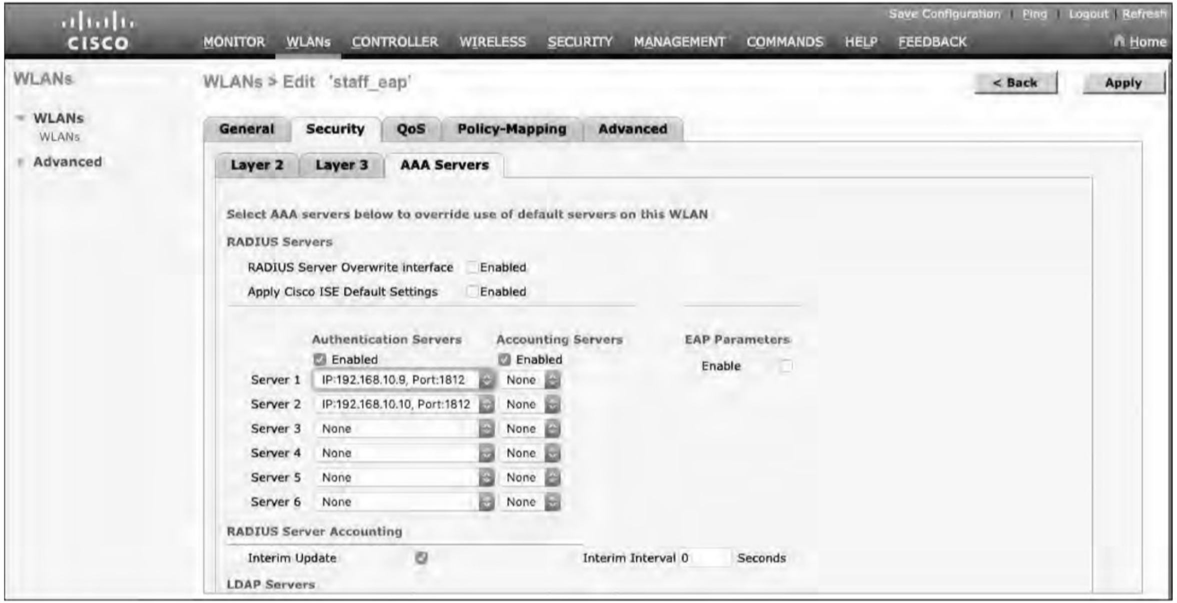
Lobby Admin Configuration

Figure 20-10 *Enabling WPA2 Enterprise Mode with 802.1x Authentication*

Configuring EAP-Based Authentication with External RADIUS Servers (Cont.)

By default, a controller uses the global list of RADIUS servers in the order you have defined under Security > AAA > RADIUS > Authentication.

You can override that list on the AAA Servers tab, where you can define which RADIUS servers will be used for 802.1x authentication.



WLANs > Edit 'staff_eap'

Select AAA servers below to override use of default servers on this WLAN

RADIUS Servers

RADIUS Server Overwrite interface □ Enabled

Apply Cisco ISE Default Settings □ Enabled

	Authentication Servers	Accounting Servers
	☑ Enabled	☑ Enabled
Server 1	IP:192.168.10.9, Port:1812	None
Server 2	IP:192.168.10.10, Port:1812	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

EAP Parameters

Enable □

RADIUS Server Accounting

Interim Update ☑ Interim Interval 0 Seconds

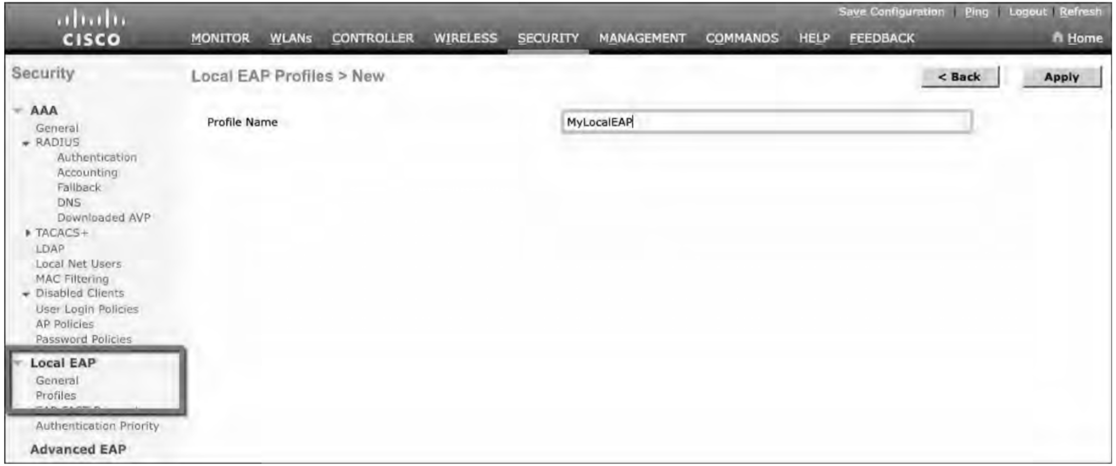
LDAP Servers

Figure 20-11 *Selecting RADIUS Servers to Authenticate Clients in the WLAN*

Authenticating with EAP

Configuring EAP-Based Authentication with Local EAP

- If your environment is small or you do not have a RADIUS server in production, you can use an authentication server that is built in to the WLC. This is called Local EAP, and it supports LEAP, EAP-FAST, PEAP, and EAP-TLS.
- Define and enable the local EAP service on the controller. Navigate to Security > Local EAP > Profiles and click the New button. Enter a name for the Local EAP profile, which will be used to define the authentication server methods.



Local EAP Profiles > New

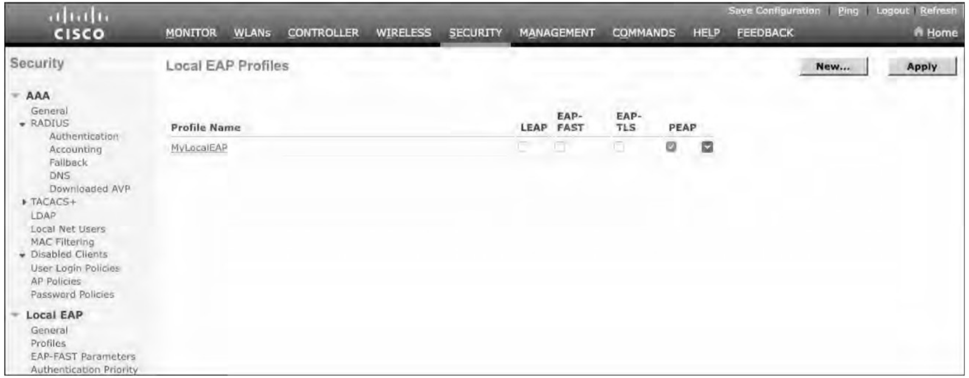
Profile Name: MyLocalEAP

Figure 20-12 *Defining a Local EAP Profile on a Controller*

In Figure 20-12, a new profile called MyLocalEAP has been defined.

Configuring EAP-Based Authentication with Local EAP (Cont.)

Now you should see the new profile listed, along with the authentication methods it supports, as shown in Figure 20-13. From this list, you can check or uncheck the boxes to enable or disable each method.

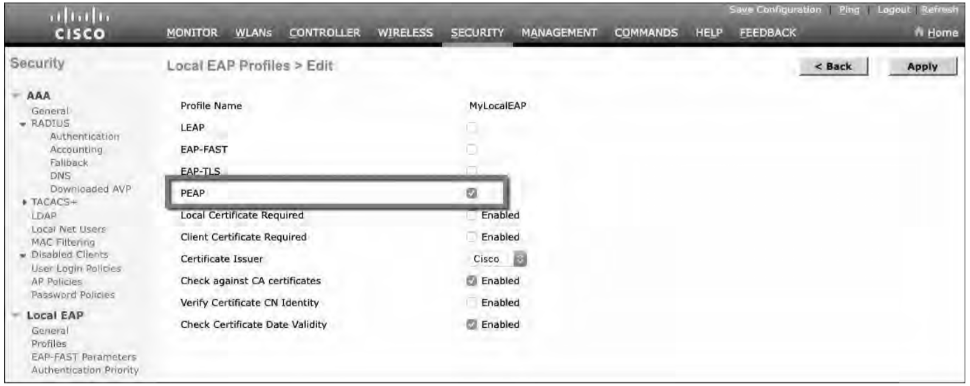


Local EAP Profiles

Profile Name	LEAP	EAP-FAST	EAP-TLS	PEAP
MyLocalEAP	☐	☐	☐	☑

Figure 20-13 *Displaying Configured Local EAP Profiles*

Select the profile name to edit its parameters. In Figure 20-14, the profile named MyLocalEAP has been configured to use PEAP. Click the Apply button to activate your changes.



Local EAP Profiles > Edit

Profile Name	MyLocalEAP
LEAP	☐
EAP-FAST	☐
EAP-TLS	☐
PEAP	☑
Local Certificate Required	☐ Enabled
Client Certificate Required	☐ Enabled
Certificate Issuer	Cisco
Check against CA certificates	☑ Enabled
Verify Certificate CN Identity	☐ Enabled
Check Certificate Date Validity	☑ Enabled

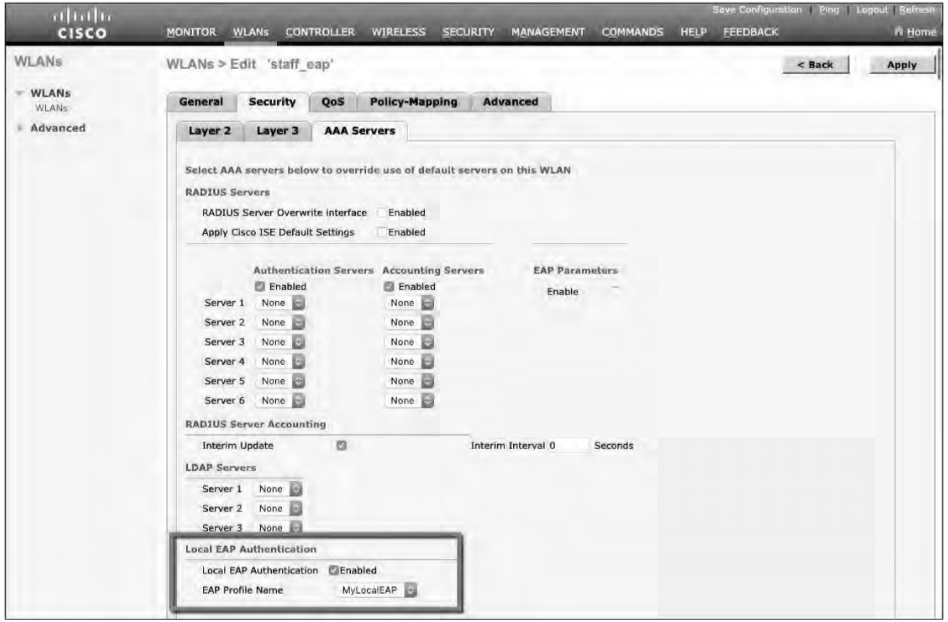
Figure 20-14 *Configuring a Local EAP Profile to Use PEAP*

Authenticating with EAP

Configure WLAN to Local EAP

Next, you need to configure the WLAN to use the Local EAP server rather than a regular external RADIUS server. Navigate to WLANs, select the WLAN ID, and then select the Security > Layer 2 tab and enable WPA2, AES, and 802.1x as before.

If you have defined any RADIUS servers in the global list under Security > AAA > RADIUS > Authentication or any specific RADIUS servers in the WLAN configuration, the controller will use those first. Local EAP will then be used as a backup method.



WLANs > Edit 'staff_eap'

Select AAA servers below to override use of default servers on this WLAN

RADIUS Servers

RADIUS Server Overwrite interface □ Enabled

Apply Cisco ISE Default Settings □ Enabled

	Authentication Servers	Accounting Servers
	☑ Enabled	☑ Enabled
Server 1	None	None
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

EAP Parameters

Enable

RADIUS Server Accounting

Interim Update ☑ Interim Interval 0 Seconds

LDAP Servers

Server 1	None
Server 2	None
Server 3	None

Local EAP Authentication

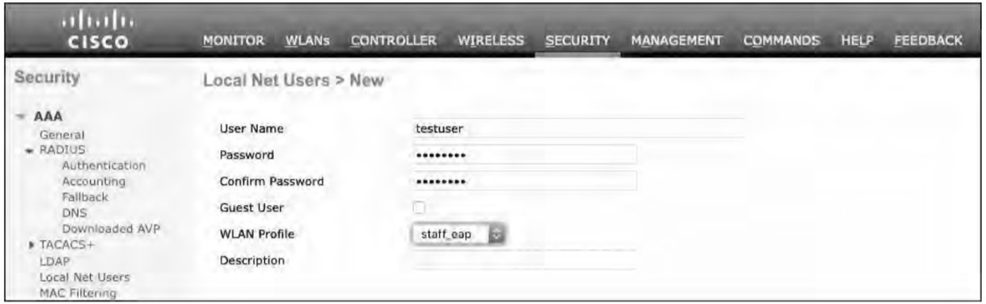
Local EAP Authentication ☑ Enabled

EAP Profile Name MyLocalEAP

Figure 20-15 *Enabling Local EAP Authentication for a WLAN*

Authenticating with EAP
Verifying Configuration

Because the Local EAP server is local to the controller, you will have to maintain a local database of users or define one or more LDAP servers on the controller. You can create users by navigating to Security > AAA > Local Net Users. In Figure 20-16, a user named testuser has been defined and authorized for access to the staff_eap WLAN.

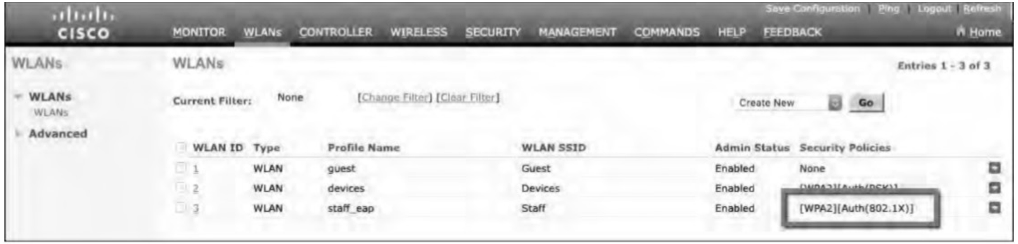


Local Net Users > New

User Name	testuser
Password	••••••••
Confirm Password	••••••••
Guest User	□
WLAN Profile	staff_eap
Description	

Figure 20-16 *Creating a Local User for Local EAP Authentication*

You can verify the WLAN and its security settings from the list of WLANs by selecting WLANs > WLAN, as shown in Figure 20-17.



WLANs

Entries 1 - 3 of 3

Current Filter: None

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	guest	Guest	Enabled	None
2	WLAN	devices	Devices	Enabled	[WPA2][Auth(PSK)]
3	WLAN	staff_eap	Staff	Enabled	[WPA2][Auth(802.1X)]

Figure 20-17 *Verifying EAP Authentication on a WLAN*

Authenticating with WebAuth

- You might have noticed that none of the authentication methods described so far involve direct interaction with the end user.
- Web Authentication (WebAuth) is different because it presents the end user with content to read and interact with before granting access to the network.
- WebAuth can be used as an additional layer in concert with Open Authentication, PSK-based authentication, and EAP-based authentication.

Local Web Authentication

Web Authentication can be handled locally on the WLC for smaller environments through Local Web Authentication (LWA). You can configure LWA in the following modes:

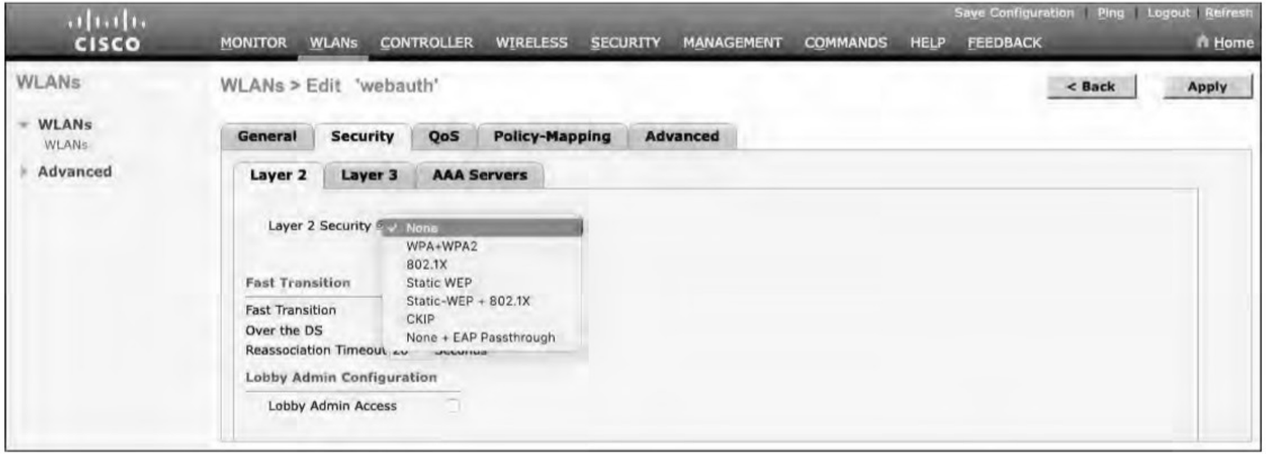
- LWA with an internal database on the WLC
- LWA with an external database on a RADIUS or LDAP server
- LWA with an external redirect after authentication
- LWA with an external splash page redirect, using an internal database on the WLC
- LWA with passthrough, requiring user acknowledgment

When there are many controllers providing Web Authentication, it makes sense to use LWA with an external database on a RADIUS server, such as ISE, and keep the user database centralized. The next logical progression is to move the Web Authentication page onto the central server, too. This is called Central Web Authentication (CWA).

Authenticating with WebAuth

Configure WebAuth on WLAN

- First create the new WLAN and map it to the correct VLAN.
- Go to the General tab and enter the SSID string, apply the appropriate controller interface, and change the status to Enabled.
- On the Security tab, select the Layer 2 tab to choose a wireless security scheme to be used on the WLAN.



WLANs > Edit 'webauth'

Layer 2 Security ✓ None

Fast Transition

Fast Transition

Over the DS

Reassociation Timeout 20 Seconds

Lobby Admin Configuration

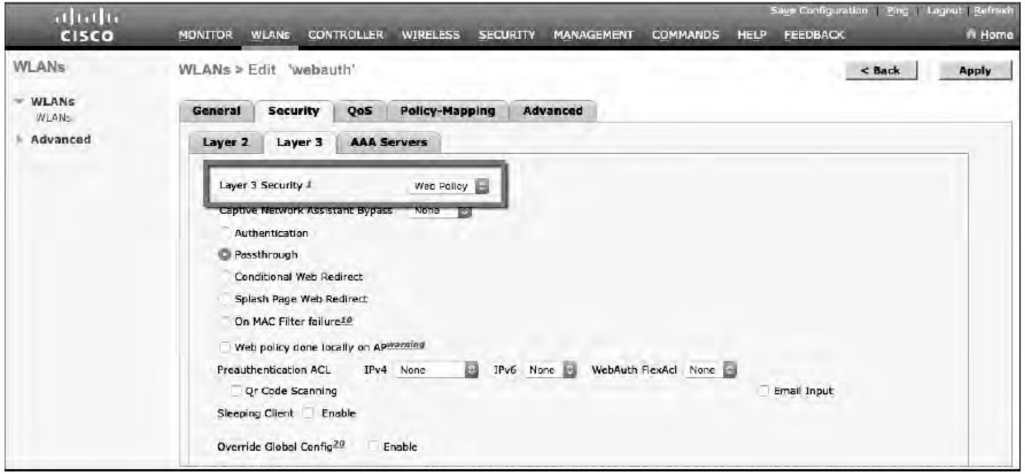
Lobby Admin Access □

Figure 20-18 *Configuring Open Authentication for WebAuth*

In Figure 20-18, the WLAN is named webauth, the SSID is Guest_webauth, and Open Authentication will be used because the None method has been selected.

Configure WebAuth on WLAN (Cont.)

- Next, select the Security > Layer 3 tab and choose the Layer 3 Security type Web Policy, as shown in Figure 20-19.
- When the Authentication radio button is selected (the default), Web Authentication will be performed locally on the WLC by prompting the user for credentials that will be checked against RADIUS, LDAP, or local EAP servers.
- In the figure, Passthrough has been selected, which will display web content such as an acceptable use policy to the user and prompt for acceptance.
- Through the other radio buttons, WebAuth can redirect the user to an external web server for content and interaction. Click the Apply button to apply the changes to the WLAN configuration.



WLANs > Edit 'webauth'

Layer 3 Security [1] Web Policy

Captive Network Assistant Bypass None

○ Authentication

● Passthrough

○ Conditional Web Redirect

○ Splash Page Web Redirect

○ On MAC Filter failure[10]

□ Web policy done locally on AP[warning]

Preauthentication ACL IPv4 None IPv6 None WebAuth FlexAcl None

□ Qr Code Scanning □ Email Input

Sleeping Client □ Enable

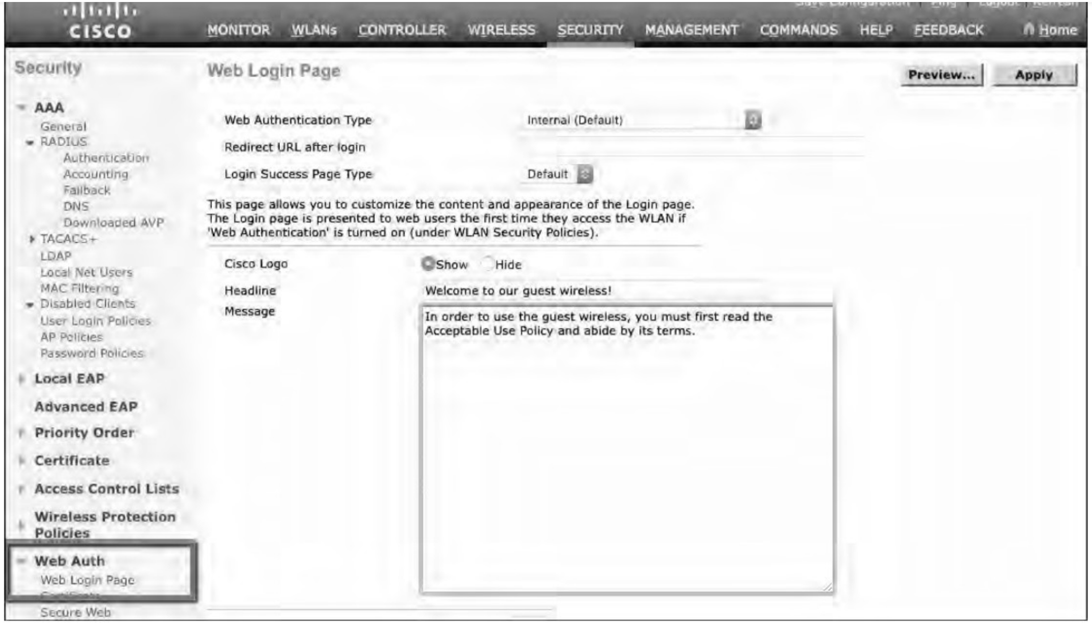
Override Global Config[20] □ Enable

Figure 20-19 *Configuring WebAuth with Passthrough Authentication*

Configure WebAuth on WLAN (Cont.)

You will need to configure the WLC's local web server with content to display during a WebAuth session.

Navigate to Security > Web Auth > Web Login Page, as shown in Figure 20-20. By default, internal WebAuth is used. You can enter the web content that will be displayed to the user by defining a text string to be used as the headline, as well as a block of message text.



Web Login Page

Web Authentication Type: Internal (Default)

Redirect URL after login

Login Success Page Type: Default

This page allows you to customize the content and appearance of the Login page. The Login page is presented to web users the first time they access the WLAN if 'Web Authentication' is turned on (under WLAN Security Policies).

Cisco Logo ● Show ○ Hide

Headline: Welcome to our guest wireless!

Message: In order to use the guest wireless, you must first read the Acceptable Use Policy and abide by its terms.

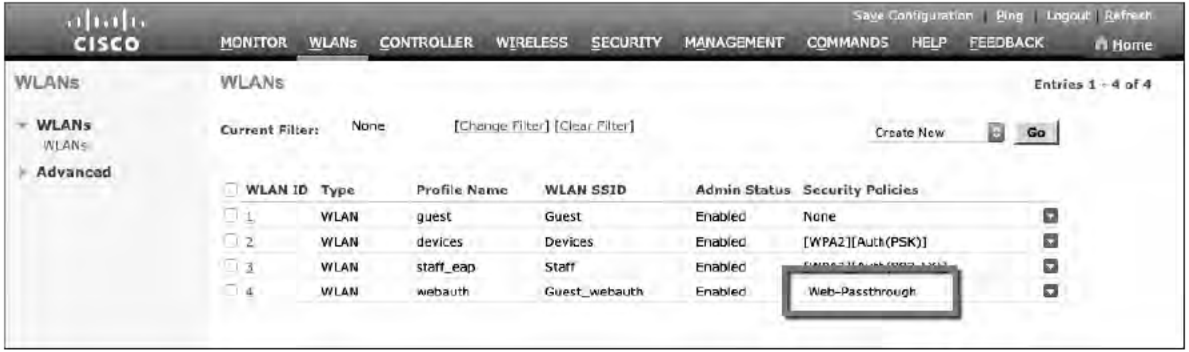
Figure 20-20 *Configuring the WebAuth Page Content*

Authenticating with WebAuth

Verifying WebAuth on a WLAN

You can verify the WebAuth security settings from the list of WLANs by selecting WLANs > WLAN.

In Figure 20-22, WLAN 4 with SSID Guest_webauth is shown to use the Web-Passthrough security policy. You can also verify that the WLAN status is enabled and active.



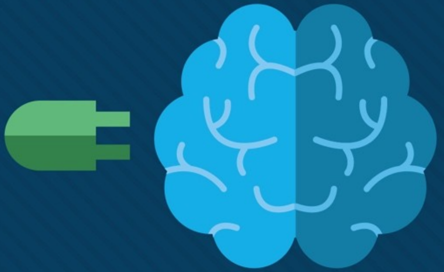
WLANs

Entries 1 - 4 of 4

Current Filter: None [Change Filter] [Clear Filter]

□ WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
□ 1	WLAN	guest	Guest	Enabled	None
□ 2	WLAN	devices	Devices	Enabled	[WPA2][Auth(PSK)]
□ 3	WLAN	staff_eap	Staff	Enabled	[WPA2][Auth(802.1X)]
□ 4	WLAN	webauth	Guest_webauth	Enabled	Web-Passthrough

Figure 20-22 *Verifying WebAuth Authentication on a WLAN*



Chapter 21: Troubleshooting Wireless Connectivity

Instructor Materials

CCNP Enterprise: Core Networking

Troubleshooting Client Connectivity from WLC

- Most of your time managing and monitoring a wireless network will be spent in the wireless LAN controller GUI.

- You can access a wealth of troubleshooting information from the controller, if you know the client's MAC address.

Troubleshooting Client Connectivity from WLC

When one or more network users report that they are having problems, your first course of action should be to gather more information, ask questions, and try to notice patterns or similarities in the answers you receive.

- Information from the user such as, “I cannot connect” or “The Wi-Fi is down” might mean that the user’s device cannot associate, cannot get an IP address, or cannot authenticate.
- If you get reports from many people in the same area, perhaps an AP is misconfigured or malfunctioning.
- Reports from many areas or from a single service set identifier (SSID) may indicate problems with a controller configuration.

Conditions for a Successful Wireless Association

If you receive a report of only one wireless user having problems, it might not make sense to spend time troubleshooting a controller, where many users are supported. Instead, you should focus on that one user's client device and its interaction with an AP.

Figure 21-1 illustrates the following conditions that must be met for a successful association:

- The client is within RF range of an AP and asks to associate.
- The client authenticates.
- The client requests and receives an IP address.

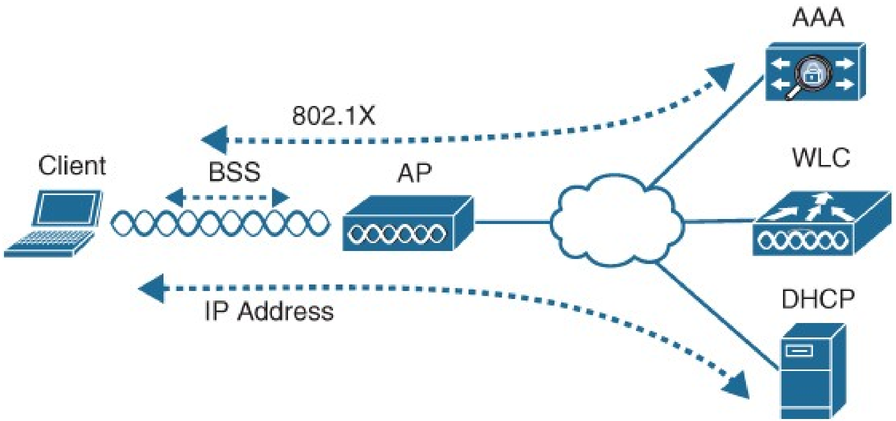


Figure 21-1 *Conditions for a Successful Wireless Association*

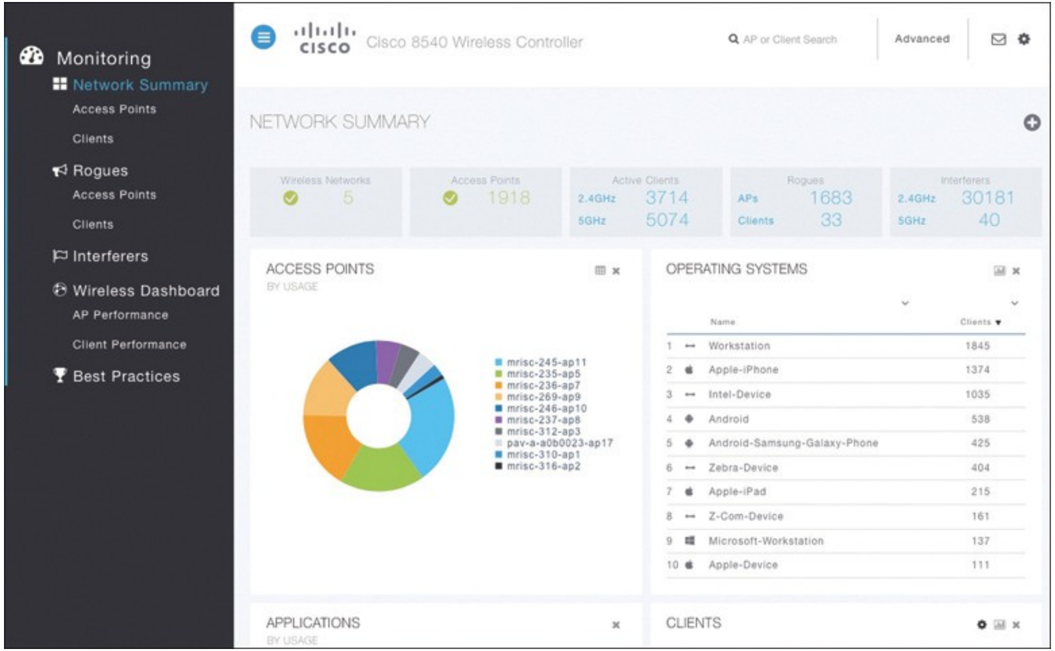
Troubleshooting Client Connectivity from WLC

Cisco WLC GUI

Cisco WLCs have two main GUI presentations, one for monitoring and one for more advanced configuration and monitoring.

When you open a browser to the WLC management address, you see the default screen that is shown in Figure 21-2.

The default screen displays network summary dashboard information on the right portion and monitoring tools in the list on the left.



NETWORK SUMMARY

Wireless Networks	Access Points	Active Clients		Rogues		Interferers	
✓ 5	✓ 1918	2.4GHz	3714	APs	1683	2.4GHz	30181
		5GHz	5074	Clients	33	5GHz	40

OPERATING SYSTEMS

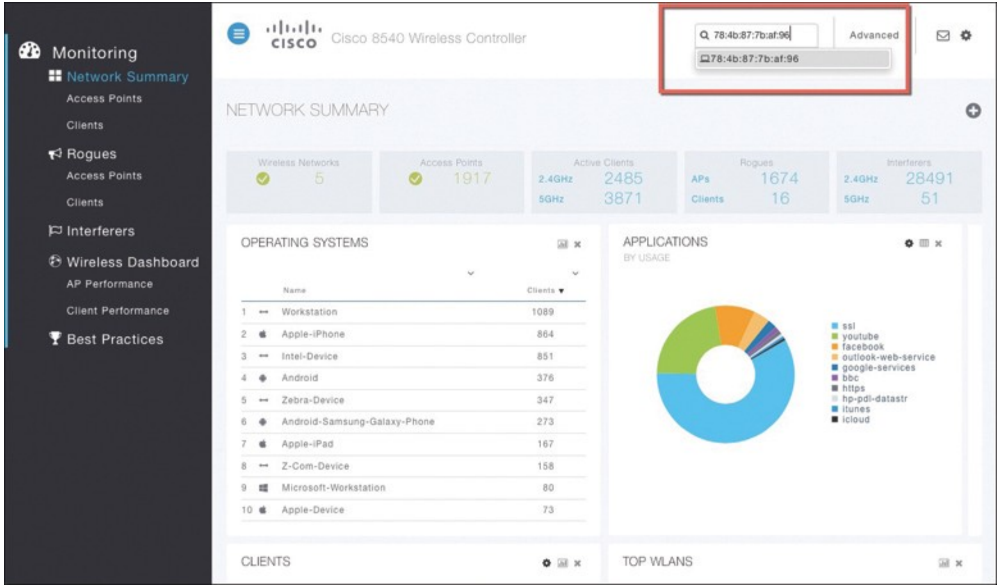
	Name	Clients ▾
1	Workstation	1845
2	Apple-iPhone	1374
3	Intel-Device	1035
4	Android	538
5	Android-Samsung-Galaxy-Phone	425
6	Zebra-Device	404
7	Apple-iPad	215
8	Z-Com-Device	161
9	Microsoft-Workstation	137
10	Apple-Device	111

Figure 21-2 *The Initial Default WLC Display*

Searching for a Client in the WLC GUI

If you know a specific wireless client's MAC address, you can enter it into the search bar at the top right of the screen.

For example, in Figure 21-3, 78:4b:87:7b:af:96 is the target of the search. Because that MAC address is known to the controller, a match is shown with a client icon below the search bar.



78:4b:87:7b:af:96

78:4b:87:7b:af:96

OPERATING SYSTEMS

	Name	Clients ▼
1	Workstation	1089
2	Apple-iPhone	864
3	Intel-Device	851
4	Android	376
5	Zebra-Device	347
6	Android-Samsung-Galaxy-Phone	273
7	Apple-iPad	167
8	Z-Com-Device	158
9	Microsoft-Workstation	80
10	Apple-Device	73

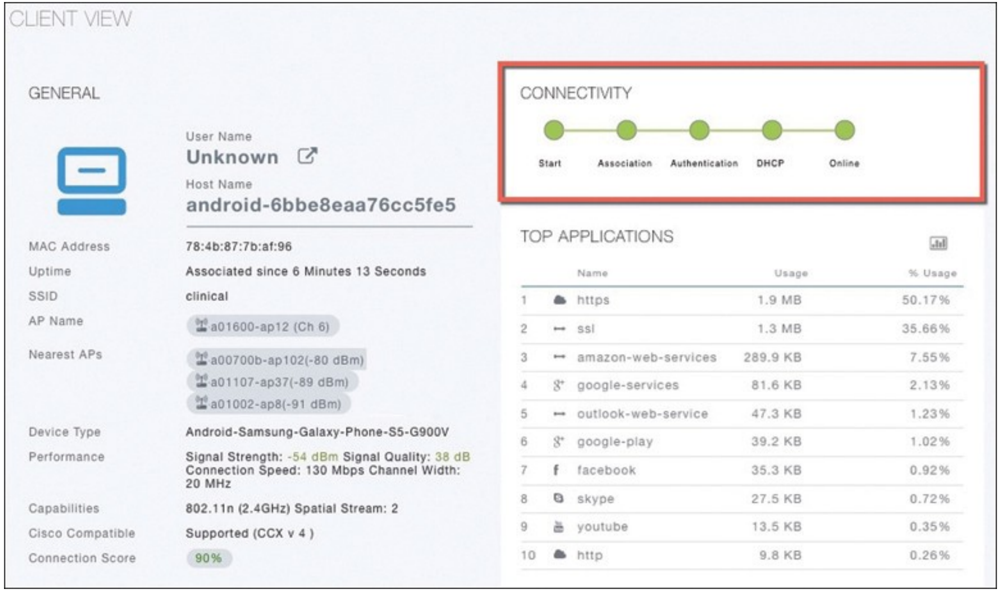
Figure 21-3 *Searching for a Client in the WLC GUI*

Troubleshooting Client Connectivity from WLC

Client Search Results

The resulting details about the client are displayed in the Client View screen, shown in Figure 21-4.

From this output, you can see many details about the client device listed in the left portion of the screen, and you can see connectivity and application information displayed on the right.



CLIENT VIEW

GENERAL

User Name
Unknown

Host Name
android-6bbe8eaa76cc5fe5

MAC Address	78:4b:87:7b:af:96
Uptime	Associated since 6 Minutes 13 Seconds
SSID	clinical
AP Name	a01600-ap12 (Ch 6)

Nearest APs	a00700b-ap102(-80 dBm)
	a01107-ap37(-89 dBm)
	a01002-ap8(-91 dBm)

Device Type	Android-Samsung-Galaxy-Phone-S5-G900V
Performance	Signal Strength: -54 dBm Signal Quality: 38 dB Connection Speed: 130 Mbps Channel Width: 20 MHz
Capabilities	802.11n (2.4GHz) Spatial Stream: 2
Cisco Compatible	Supported (CCX v 4)
Connection Score	90%

CONNECTIVITY

TOP APPLICATIONS

	Name	Usage	% Usage
1	https	1.9 MB	50.17%
2	ssl	1.3 MB	35.66%
3	amazon-web-services	289.9 KB	7.55%
4	google-services	81.6 KB	2.13%
5	outlook-web-service	47.3 KB	1.23%
6	google-play	39.2 KB	1.02%
7	facebook	35.3 KB	0.92%
8	skype	27.5 KB	0.72%
9	youtube	13.5 KB	0.35%
10	http	9.8 KB	0.26%

Figure 21-4 *Client Search Results*

Troubleshooting Client Connectivity from WLC

Checking the Client's Connection Status

Before a controller will permit a client to fully associate with a basic service set (BSS), the client must progress through a sequence of states. Each state refers to a policy that the client must meet before moving on to the next state:

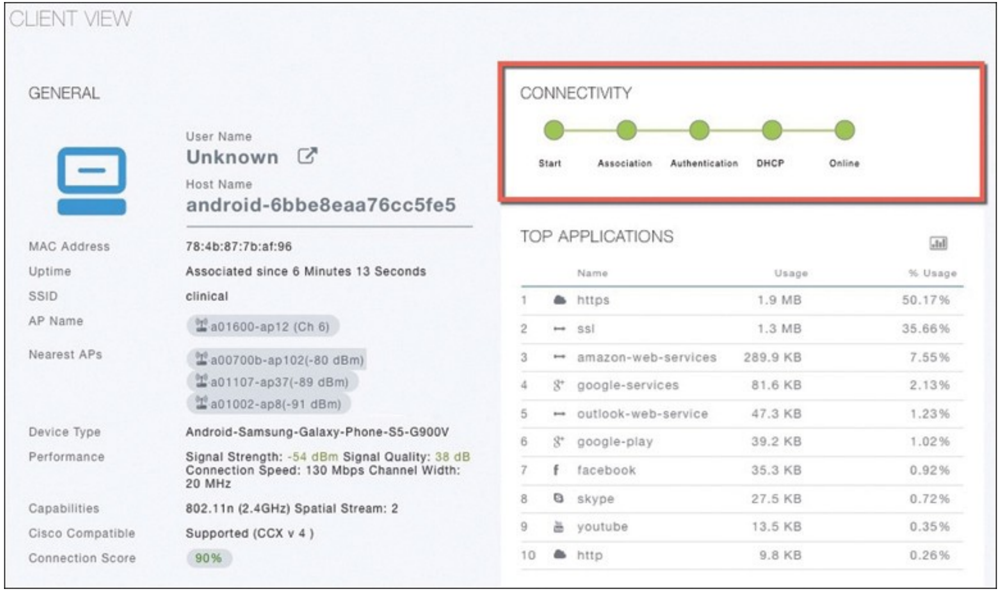
1. **Start -** Client activity has just begun.
2. **Association -** The client has requested 802.11 authentication and association with an AP.
3. **Authentication -** The client must pass a Layer 2 Pre-Shared Key (PSK) or 802.1x authentication policy.
4. **DHCP -** The WLC is waiting to learn the client's IP address from a Dynamic Host Configuration Protocol (DHCP) server.
5. **Online -** The client has passed Layer 2 and Layer 3 policies, successfully associated, and can pass traffic.

Troubleshooting Client Connectivity from WLC

Checking the Client’s Association and Signal Status

Information such as the wireless client’s username (if known), hostname, wireless MAC address, wireless connection uptime, and the SSID used can be viewed in the left portion of the Client View screen.

In Figure 21-4, the username is not known because the client does not authenticate itself with a username.



CLIENT VIEW

GENERAL

User Name
Unknown

Host Name
android-6bbe8eaa76cc5fe5

MAC Address	78:4b:87:7b:af:96
Uptime	Associated since 6 Minutes 13 Seconds
SSID	clinical
AP Name	a01600-ap12 (Ch 6)

Nearest APs	a00700b-ap102(-80 dBm)
	a01107-ap37(-89 dBm)
	a01002-ap8(-91 dBm)

Device Type	Android-Samsung-Galaxy-Phone-S5-G900V
Performance	Signal Strength: -54 dBm Signal Quality: 38 dB Connection Speed: 130 Mbps Channel Width: 20 MHz
Capabilities	802.11n (2.4GHz) Spatial Stream: 2
Cisco Compatible	Supported (CCX v 4)
Connection Score	90%

CONNECTIVITY

TOP APPLICATIONS

	Name	Usage	% Usage
1	https	1.9 MB	50.17%
2	ssl	1.3 MB	35.66%
3	amazon-web-services	289.9 KB	7.55%
4	google-services	81.6 KB	2.13%
5	outlook-web-service	47.3 KB	1.23%
6	google-play	39.2 KB	1.02%
7	facebook	35.3 KB	0.92%
8	skype	27.5 KB	0.72%
9	youtube	13.5 KB	0.35%
10	http	9.8 KB	0.26%

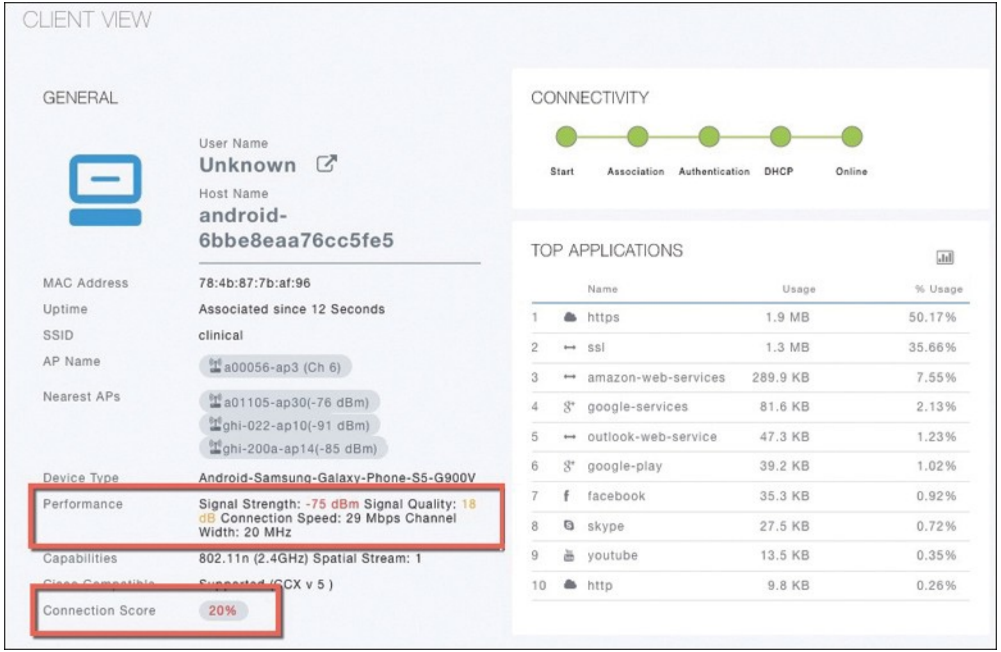
Figure 21-4 *Client Search Results*

Troubleshooting Client Connectivity from WLC

WLC Information About a Poorly Performing Client

In Figure 21-5 the AP is receiving the client’s signal strength at −76 dBm and the SNR at 18 dB (both rather low values), causing the current data rate to fall to 29 Mbps. A quick look at the Connection Score value reveals a low 20%.

It is safe to assume that the client has moved too far away from the AP where it is associated, causing the signal strength to become too low to support faster performance.



CLIENT VIEW

GENERAL

User Name
Unknown

Host Name
android-6bbe8eaa76cc5fe5

MAC Address	78:4b:87:7b:af:96
Uptime	Associated since 12 Seconds
SSID	clinical
AP Name	a00056-ap3 (Ch 6)

Nearest APs	a01105-ap30(-76 dBm)
	ghi-022-ap10(-91 dBm)
	ghi-200a-ap14(-85 dBm)

Device Type	Android-Samsung-Galaxy-Phone-S5-G900V
Performance	Signal Strength: -75 dBm Signal Quality: 18 dB Connection Speed: 29 Mbps Channel Width: 20 MHz
Capabilities	802.11n (2.4GHz) Spatial Stream: 1
Cisco Compatible	Supported (CCX v 5)
Connection Score	20%

CONNECTIVITY

TOP APPLICATIONS

	Name	Usage	% Usage
1	https	1.9 MB	50.17%
2	ssl	1.3 MB	35.66%
3	amazon-web-services	289.9 KB	7.55%
4	google-services	81.6 KB	2.13%
5	outlook-web-service	47.3 KB	1.23%
6	google-play	39.2 KB	1.02%
7	facebook	35.3 KB	0.92%
8	skype	27.5 KB	0.72%
9	youtube	13.5 KB	0.35%
10	http	9.8 KB	0.26%

Figure 21-5 *WLC Information About a Poorly Performing Client*

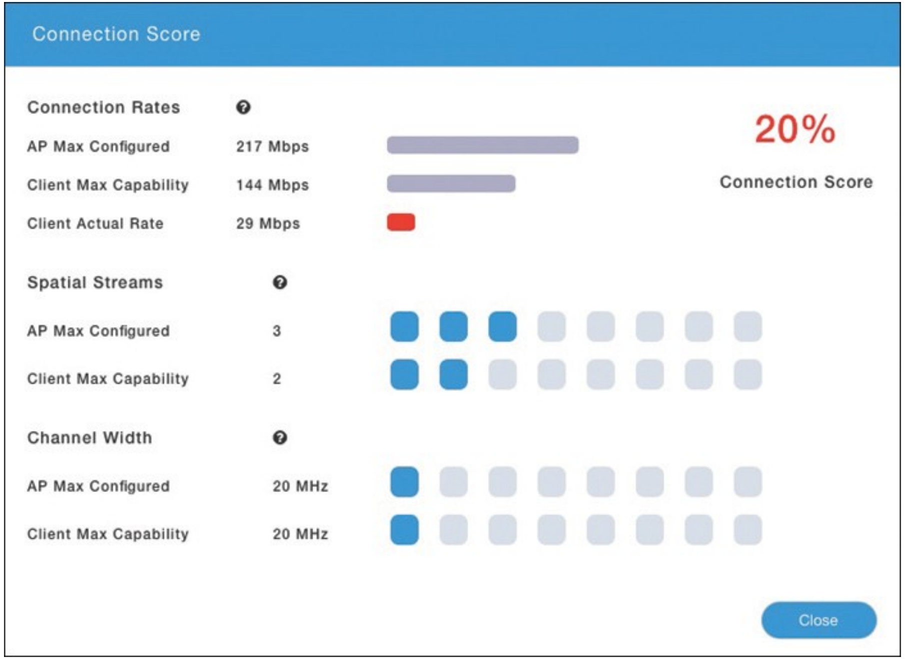
Troubleshooting Client Connectivity from WLC

WLC Information About a Poorly Performing Client

Clicking on the Connection Score value displays further details in a popup window, as shown in Figure 21-6.

The 20% value is the result of the client’s current data rate (29 Mbps) divided by the lower of the AP or client maximum data rate (144 Mbps).

The Client Actual Rate and Connection Score values are indicators of current performance, and the other graphs show what is possible on the AP and the client.



Connection Score

Connection Rates
AP Max Configured 217 Mbps
Client Max Capability 144 Mbps
Client Actual Rate 29 Mbps

20%
Connection Score

Spatial Streams
AP Max Configured 3
Client Max Capability 2

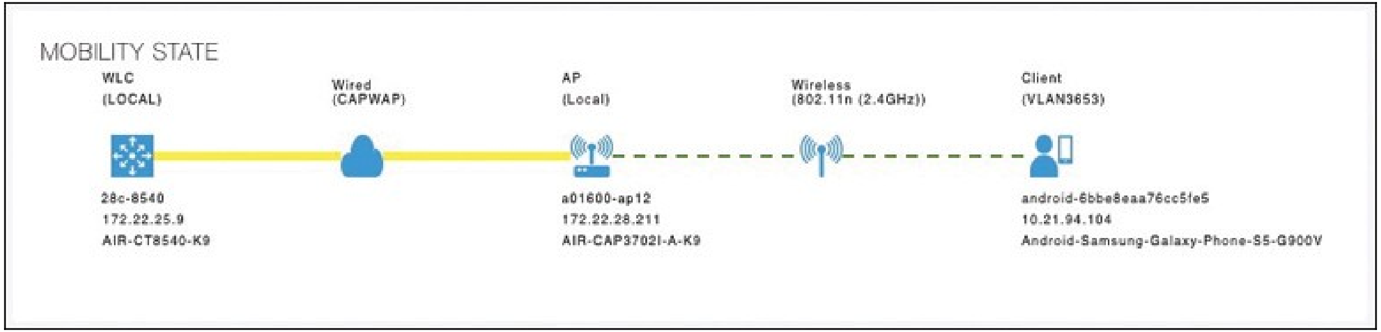
Channel Width
AP Max Configured 20 MHz
Client Max Capability 20 MHz

Figure 21-6 *Displaying Detailed Client Performance Information*

Troubleshooting Client Connectivity from WLC

Checking the Client’s Mobility State

- The WLC Client Search information includes a handy end-to-end graphical representation of a client’s wireless connection.
- When you scroll down below the General and Connectivity sections, you see a topology diagram like the one shown in Figure 21-7.
- The WLC’s name, management IP address, and model are displayed. Following the connection toward the right, you can see the AP name, IP address, and model where the client is associated. Moving further to the right, you can see that the client is associated to the AP. The client device is displayed with identifying information such as the device name, device type, VLAN number, and IP address.



MOBILITY STATE

WLC (LOCAL)
28c-8540
172.22.25.9
AIR-CT8540-K9

Wired (CAPWAP)

AP (Local)
a01600-ap12
172.22.28.211
AIR-CAP3702I-A-K9

Wireless (802.11n (2.4GHz))

Client (VLAN3653)
android-6bbe8eaa76cc5fe5
10.21.94.104
Android-Samsung-Galaxy-Phone-S5-G900V

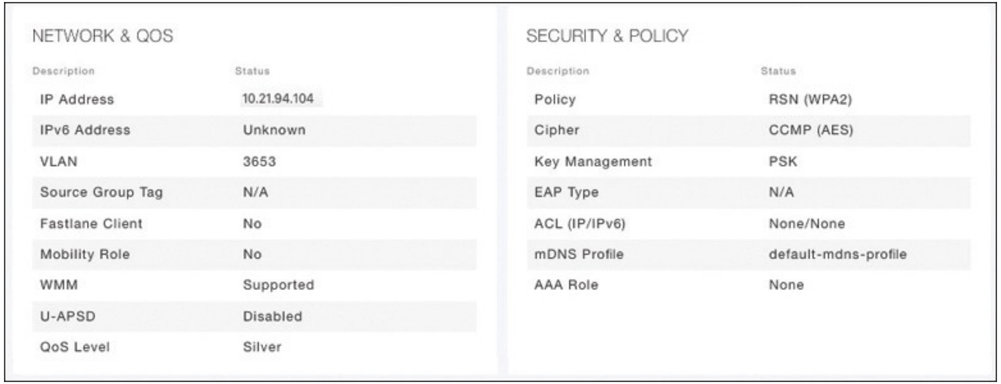
Figure 21-7 *Displaying the Client Mobility State*

Troubleshooting Client Connectivity from WLC

Checking the Client’s Wireless Policies

By scrolling further down in the Client Search information, you can verify information about network, QoS, security, and other policies that affect the client, as shown in Figure 21-8.

You can quickly learn the client’s IP address, VLAN number, QoS policy level used by the WLAN, security policy (WPA2), encryption cipher (CCMP AES), and authentication type (PSK with no EAP).



NETWORK & QOS

Description	Status
IP Address	10.21.94.104
IPv6 Address	Unknown
VLAN	3653
Source Group Tag	N/A
Fastlane Client	No
Mobility Role	No
WMM	Supported
U-APSD	Disabled
QoS Level	Silver

SECURITY & POLICY

Description	Status
Policy	RSN (WPA2)
Cipher	CCMP (AES)
Key Management	PSK
EAP Type	N/A
ACL (IP/IPv6)	None/None
mDNS Profile	default-mdns-profile
AAA Role	None

Figure 21-8 *Displaying the Wireless Policies Used by a Client*

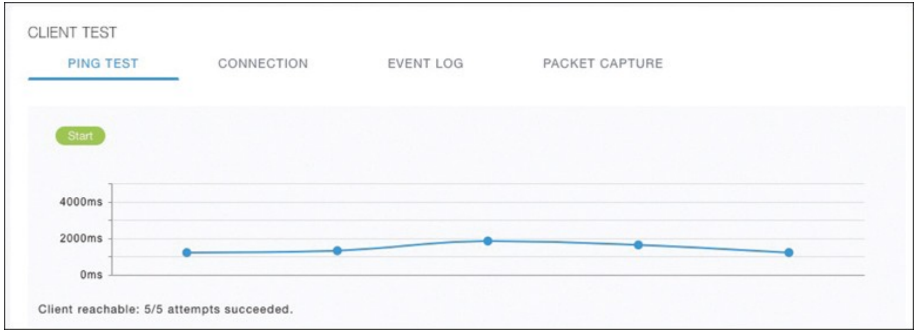
Troubleshooting Client Connectivity from WLC

Testing a Wireless Client

When you search for a specific client, the information displayed is of a static nature because it is obtained as a snapshot at the time of the search. The client search will need to be refreshed to get up-to-date data. You can also obtain dynamic data by testing a client in real time.

By scrolling to the bottom of the client search information, you can see the Client Test section, which offers links to four client testing tools:

- **Ping Test**: The WLC sends five ICMP echo packets to the client's IP address and measures the response time, as shown in Figure 21-9.



Client reachable: 5/5 attempts succeeded.

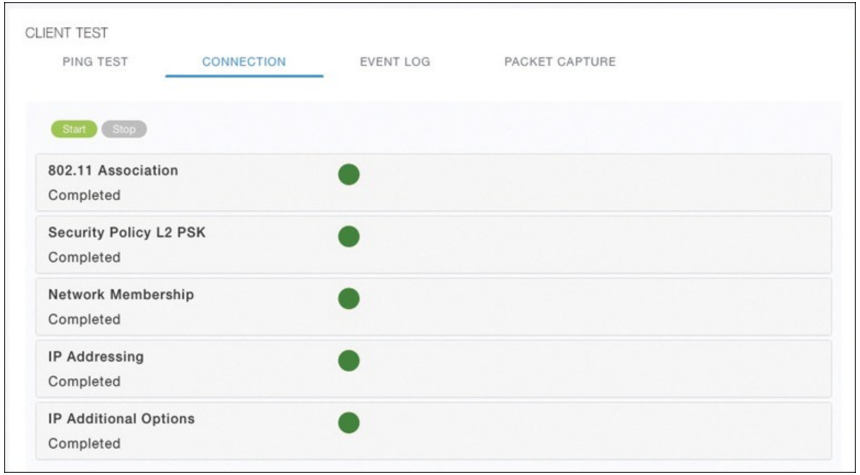
Figure 21-9 *Testing Ping Response Times Between the WLC and Client*

Troubleshooting Client Connectivity from WLC

Testing a Wireless Client (Cont.)

Connection: The WLC debugs the client for up to three minutes and checks each policy step as the client attempts to join the wireless network.

Figure 21-10 shows a client that has successfully joined, and Figure 21-11 shows a client that failed Layer 2 authentication with a pre-shared key because its key did not match the key configured on the WLC.



802.11 Association ●
Completed

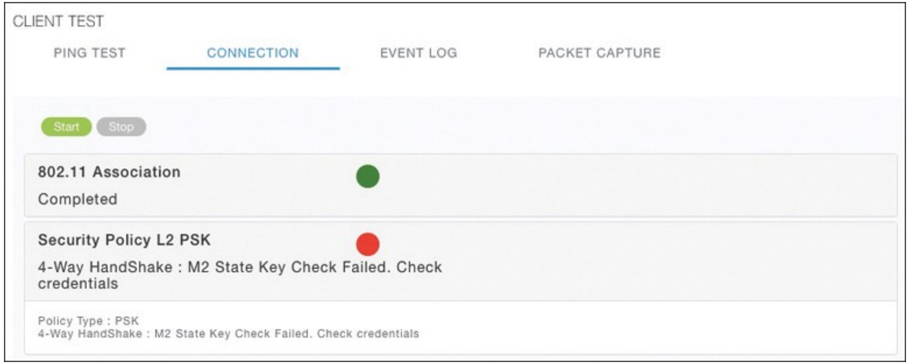
Security Policy L2 PSK ●
Completed

Network Membership ●
Completed

IP Addressing ●
Completed

IP Additional Options ●
Completed

Figure 21-10 *Performing a Connection Test on a Successful Wireless Client*



802.11 Association ●
Completed

Security Policy L2 PSK ●
4-Way HandShake : M2 State Key Check Failed. Check credentials

Policy Type : PSK
4-Way HandShake : M2 State Key Check Failed. Check credentials

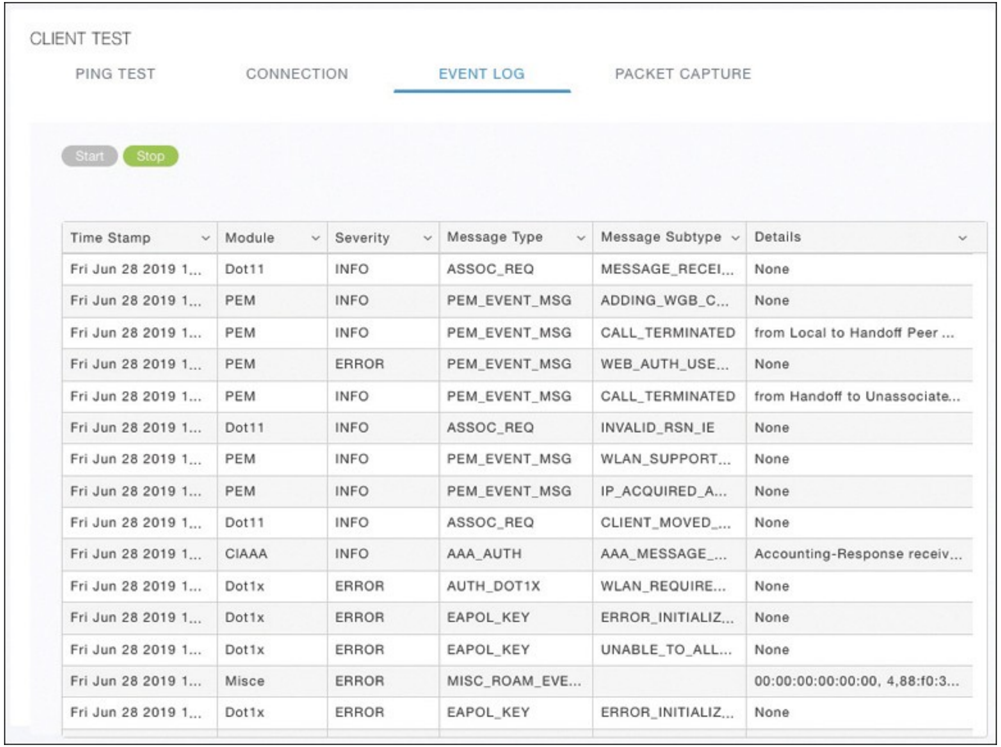
Figure 21-11 *Performing a Connection Test on a Failed Wireless Client*

Troubleshooting Client Connectivity from WLC

Testing a Wireless Client (Cont.)

Event Log: The WLC collects and displays a log of events as the client attempts to join the wireless network, as shown in Figure 21-12.

This information is very complex and detailed and is usually more suited for Cisco TAC engineers.



Time Stamp	Module	Severity	Message Type	Message Subtype	Details
Fri Jun 28 2019 1...	Dot11	INFO	ASSOC_REQ	MESSAGE_RECEI...	None
Fri Jun 28 2019 1...	PEM	INFO	PEM_EVENT_MSG	ADDING_WGB_C...	None
Fri Jun 28 2019 1...	PEM	INFO	PEM_EVENT_MSG	CALL_TERMINATED	from Local to Handoff Peer ...
Fri Jun 28 2019 1...	PEM	ERROR	PEM_EVENT_MSG	WEB_AUTH_USE...	None
Fri Jun 28 2019 1...	PEM	INFO	PEM_EVENT_MSG	CALL_TERMINATED	from Handoff to Unassociate...
Fri Jun 28 2019 1...	Dot11	INFO	ASSOC_REQ	INVALID_RSN_IE	None
Fri Jun 28 2019 1...	PEM	INFO	PEM_EVENT_MSG	WLAN_SUPPORT...	None
Fri Jun 28 2019 1...	PEM	INFO	PEM_EVENT_MSG	IP_ACQUIRED_A...	None
Fri Jun 28 2019 1...	Dot11	INFO	ASSOC_REQ	CLIENT_MOVED_...	None
Fri Jun 28 2019 1...	CIAAA	INFO	AAA_AUTH	AAA_MESSAGE_...	Accounting-Response receiv...
Fri Jun 28 2019 1...	Dot1x	ERROR	AUTH_DOT1X	WLAN_REQUIRE...	None
Fri Jun 28 2019 1...	Dot1x	ERROR	EAPOL_KEY	ERROR_INITIALIZ...	None
Fri Jun 28 2019 1...	Dot1x	ERROR	EAPOL_KEY	UNABLE_TO_ALL...	None
Fri Jun 28 2019 1...	Misce	ERROR	MISC_ROAM_EVE...		00:00:00:00:00:00, 4,88:f0:3...
Fri Jun 28 2019 1...	Dot1x	ERROR	EAPOL_KEY	ERROR_INITIALIZ...	None

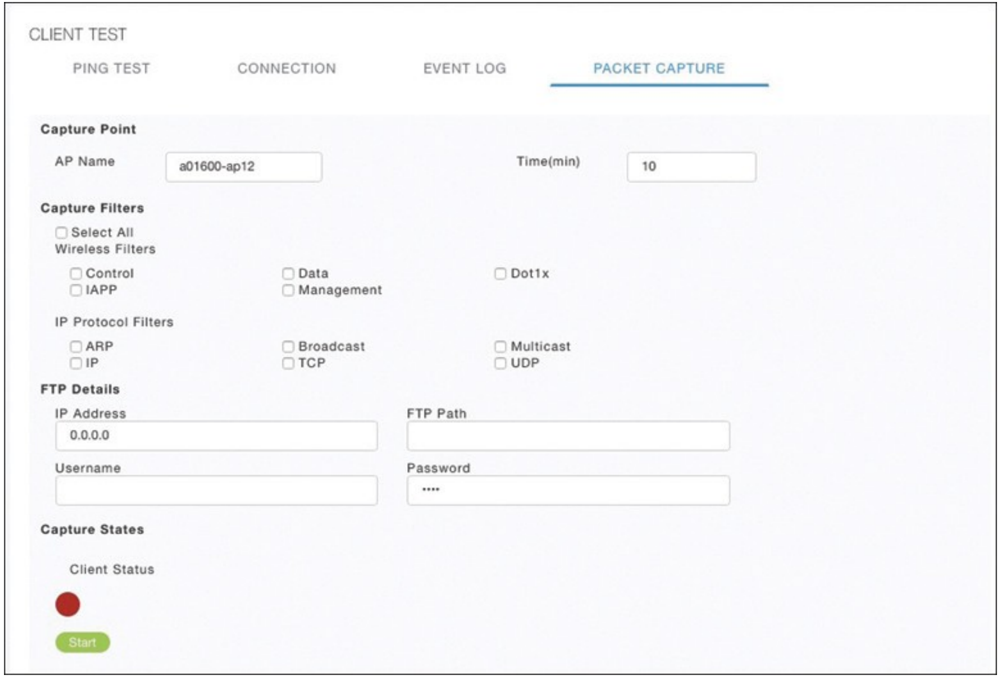
Figure 21-12 *Collecting an Event Log of a Client Join Attempt*

Troubleshooting Client Connectivity from WLC

Testing a Wireless Client (Cont.)

Packet Capture: The WLC enables a wireless packet capture at the AP where the client attempts to join, as shown in Figure 21-13.

The captured data is saved to a specified FTP server, where it can be downloaded and analyzed using a packet analysis tool like Wireshark or LiveAction Omnipeek.



Capture Point

AP Name: a01600-ap12 Time(min): 10

Capture Filters

□ Select All

Wireless Filters

□ Control □ Data □ Dot1x
□ IAPP □ Management

IP Protocol Filters

□ ARP □ Broadcast □ Multicast
□ IP □ TCP □ UDP

FTP Details

IP Address: 0.0.0.0 FTP Path:

Username: Password: ····

Capture States

Client Status ●

Figure 21-13 *Performing a Packet Capture of a Wireless Client*

Troubleshooting Connectivity at the AP

- In cases where you get reports from multiple users who are all having problems in the same general area, you might need to focus your efforts on an AP.

- The problem could be as simple as a defective radio, where no clients are receiving a signal. In that case, you might have to go onsite to confirm that the transmitter is not working correctly.

Troubleshooting Connectivity Problems at the AP

The split-MAC architecture creates several different points where you can troubleshoot. Successfully operating the lightweight AP and providing a working BSS require the following:

- The AP must have connectivity to its access layer switch.
- The AP must have connectivity to its WLC, unless it is operating in FlexConnect mode.

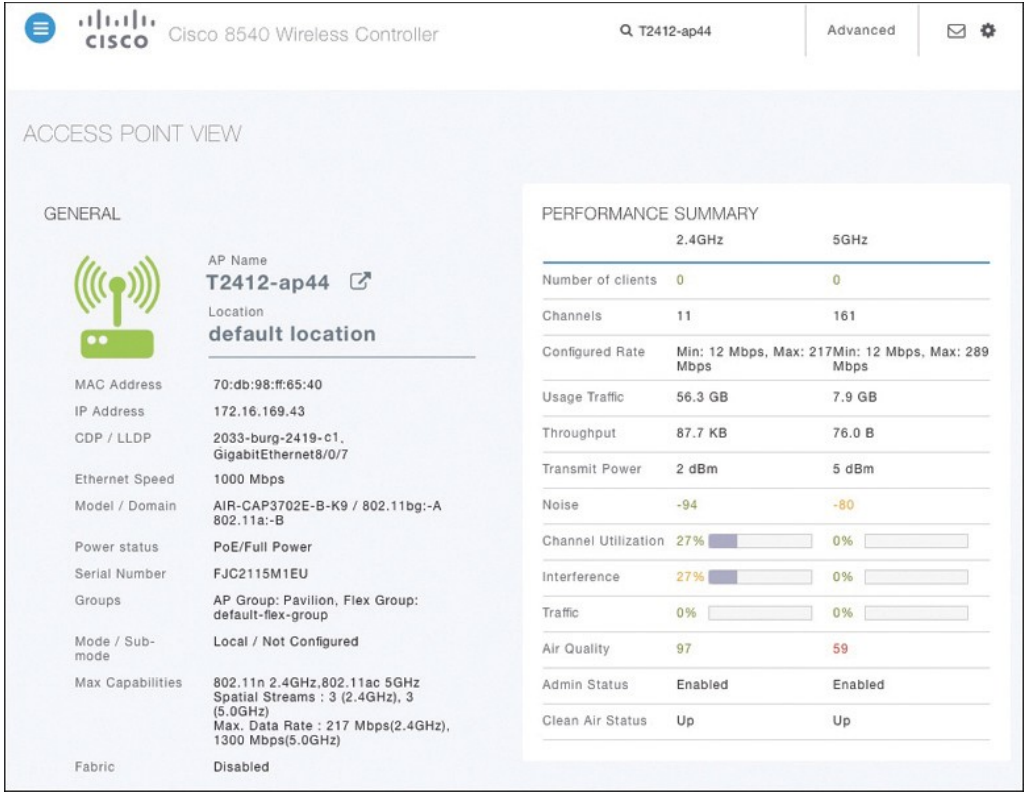
Troubleshooting Connectivity Problems at the AP

Displaying Information About an AP

First, verify the connectivity between an AP and a controller.

The easiest approach is to simply look for the AP in the list of live APs that have joined the controller. If you know which controller the AP should join, open a management session to it. Enter the AP's name in the search bar.

If the search reveals a live AP that is joined to the controller, information is displayed in the Access Point View screen, as shown in Figure 21-14.



ACCESS POINT VIEW

GENERAL

AP Name
T2412-ap44

Location
default location

MAC Address	70:db:98:ff:65:40
IP Address	172.16.169.43
CDP / LLDP	2033-burg-2419-c1, GigabitEthernet8/0/7
Ethernet Speed	1000 Mbps
Model / Domain	AIR-CAP3702E-B-K9 / 802.11bg:-A 802.11a:-B
Power status	PoE/Full Power
Serial Number	FJC2115M1EU
Groups	AP Group: Pavilion, Flex Group: default-flex-group
Mode / Sub-mode	Local / Not Configured
Max Capabilities	802.11n 2.4GHz,802.11ac 5GHz Spatial Streams : 3 (2.4GHz), 3 (5.0GHz) Max. Data Rate : 217 Mbps(2.4GHz), 1300 Mbps(5.0GHz)
Fabric	Disabled

PERFORMANCE SUMMARY

	2.4GHz	5GHz
Number of clients	0	0
Channels	11	161
Configured Rate	Min: 12 Mbps, Max: 217 Mbps	Min: 12 Mbps, Max: 289 Mbps
Usage Traffic	56.3 GB	7.9 GB
Throughput	87.7 KB	76.0 B
Transmit Power	2 dBm	5 dBm
Noise	-94	-80
Channel Utilization	27%	0%
Interference	27%	0%
Traffic	0%	0%
Air Quality	97	59
Admin Status	Enabled	Enabled
Clean Air Status	Up	Up

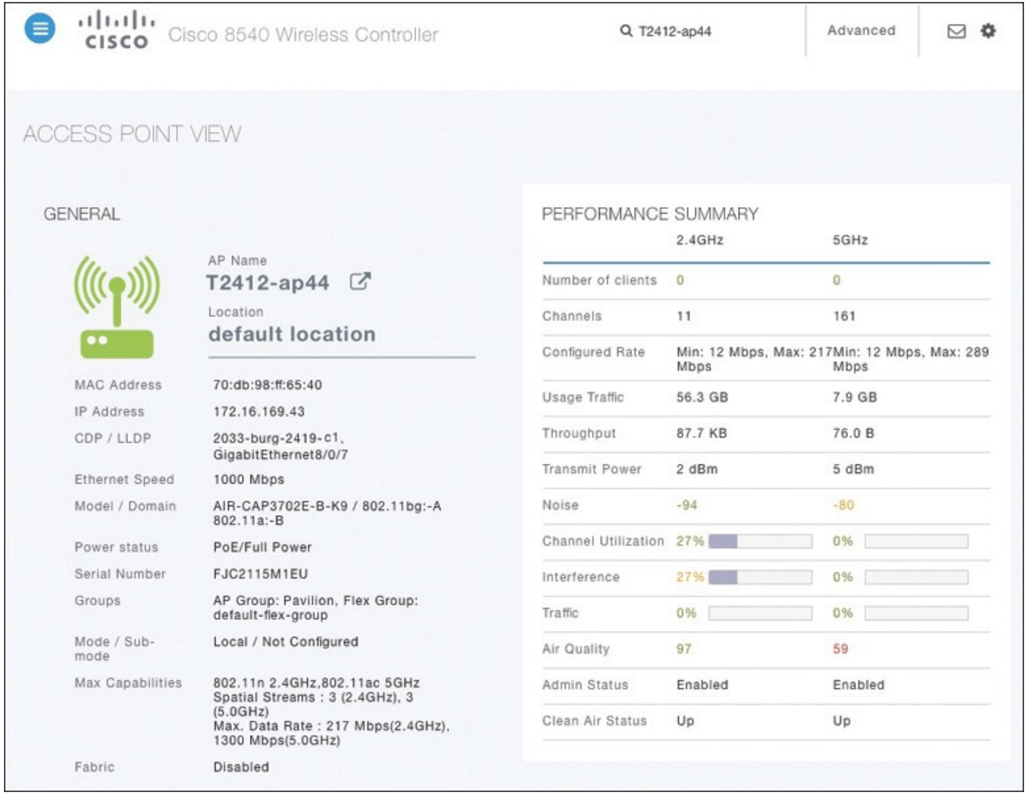
Figure 21-14 *Displaying Information About an AP*

Troubleshooting Connectivity Problems at the AP

Displaying Information About an AP (Cont.)

In Figure 21-14 the AP is named T2412-ap4, has an IP address and a valid CDP entry that shows the switch name and port number where it is connected. The AP has a live Ethernet connection with a switch and has working Power over Ethernet (PoE).

In the right portion of the Access Point View screen, you can verify parameters related to the AP's wireless performance and RF conditions.



ACCESS POINT VIEW

GENERAL

AP Name
T2412-ap44

Location
default location

MAC Address	70:db:98:ff:65:40
IP Address	172.16.169.43
CDP / LLDP	2033-burg-2419-c1, GigabitEthernet8/0/7
Ethernet Speed	1000 Mbps
Model / Domain	AIR-CAP3702E-B-K9 / 802.11bg:-A 802.11a:-B
Power status	PoE/Full Power
Serial Number	FJC2115M1EU
Groups	AP Group: Pavilion, Flex Group: default-flex-group
Mode / Sub-mode	Local / Not Configured
Max Capabilities	802.11n 2.4GHz,802.11ac 5GHz Spatial Streams : 3 (2.4GHz), 3 (5.0GHz) Max. Data Rate : 217 Mbps(2.4GHz), 1300 Mbps(5.0GHz)
Fabric	Disabled

PERFORMANCE SUMMARY

	2.4GHz	5GHz
Number of clients	0	0
Channels	11	161
Configured Rate	Min: 12 Mbps, Max: 217 Mbps	Min: 12 Mbps, Max: 289 Mbps
Usage Traffic	56.3 GB	7.9 GB
Throughput	87.7 KB	76.0 B
Transmit Power	2 dBm	5 dBm
Noise	-94	-80
Channel Utilization	27%	0%
Interference	27%	0%
Traffic	0%	0%
Air Quality	97	59
Admin Status	Enabled	Enabled
Clean Air Status	Up	Up

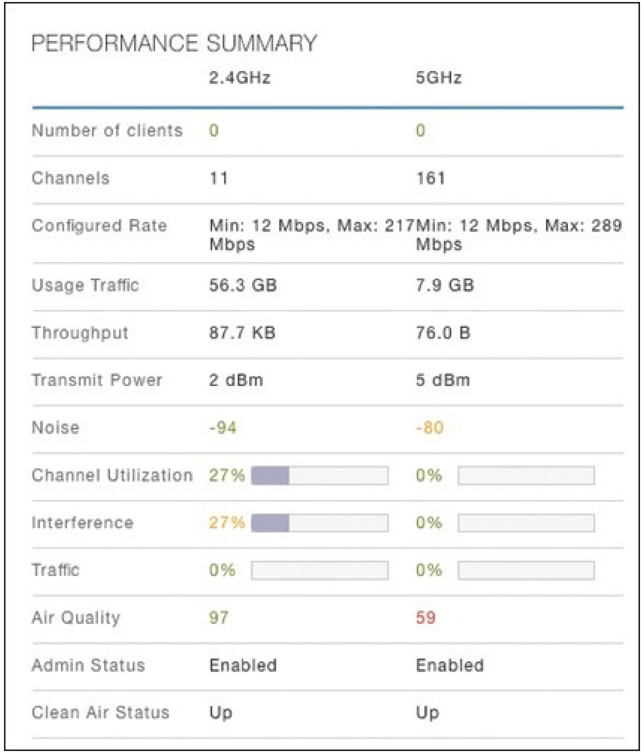
Figure 21-14 *Displaying Information About an AP*

Troubleshooting Connectivity Problems at the AP

Performance Summary Information

Another important indicator is the noise level on a channel. Ideally, the noise level should be as low as possible, usually around −90 or −100 dBm, so that 802.11 signals can be received intelligibly and accurately.

Figure 21-15 lists the 5 GHz channel 161 as having a high noise level of −80 dBm—something that is not normal or ideal.



PERFORMANCE SUMMARY

	2.4GHz	5GHz
Number of clients	0	0
Channels	11	161
Configured Rate	Min: 12 Mbps, Max: 217 Mbps	Min: 12 Mbps, Max: 289 Mbps
Usage Traffic	56.3 GB	7.9 GB
Throughput	87.7 KB	76.0 B
Transmit Power	2 dBm	5 dBm
Noise	-94	-80
Channel Utilization	27%	0%
Interference	27%	0%
Traffic	0%	0%
Air Quality	97	59
Admin Status	Enabled	Enabled
Clean Air Status	Up	Up

Figure 21-15 *Performance Summary Information*

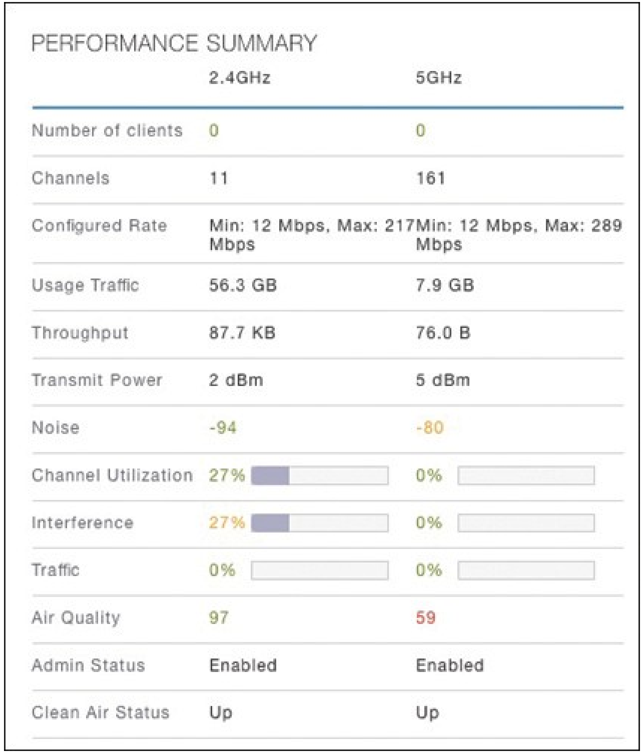
Troubleshooting Connectivity Problems at the AP

Performance Summary Information (Cont.)

The channel information also shows an index of air quality. This is a measure of how competing and interfering devices affect the airtime quality or performance on a channel, presented as a number from 0 (worst) to 100 (best).

The AP shows the air quality of channel 11 as 97, which is very good. However, channel 161 is 59, which is of concern.

You can scroll further down in the Access Point View screen to see detailed information about the AP including a list of clients it is supporting, RF troubleshooting information, clean air assessments, and a tool to reboot the AP.



PERFORMANCE SUMMARY

	2.4GHz	5GHz
Number of clients	0	0
Channels	11	161
Configured Rate	Min: 12 Mbps, Max: 217 Mbps	Min: 12 Mbps, Max: 289 Mbps
Usage Traffic	56.3 GB	7.9 GB
Throughput	87.7 KB	76.0 B
Transmit Power	2 dBm	5 dBm
Noise	-94	-80
Channel Utilization	27%	0%
Interference	27%	0%
Traffic	0%	0%
Air Quality	97	59
Admin Status	Enabled	Enabled
Clean Air Status	Up	Up

Figure 21-15 *Performance Summary Information*

Displaying Information About RF Interferers

In Figure 21-16, the RF Troubleshoot tab has been selected to display interferer data for the channels in the 5 GHz band.

There are no interfering neighbor or rogue APs, but there is a clean air interferer in channel 161 - the channel that the AP is using.

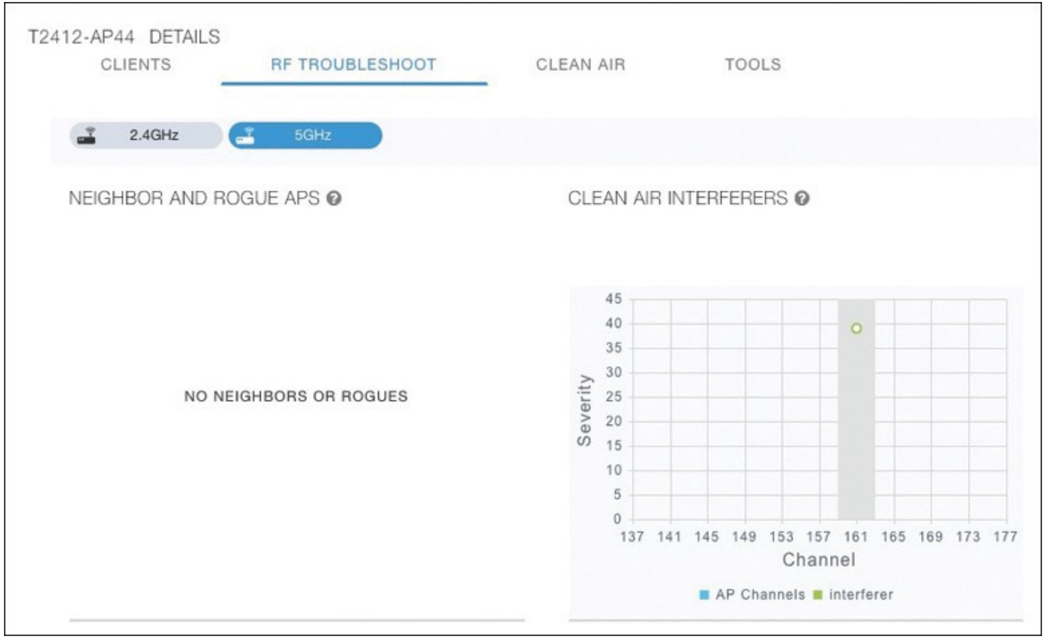


Figure 21-16 *Displaying Information About RF Interferers*

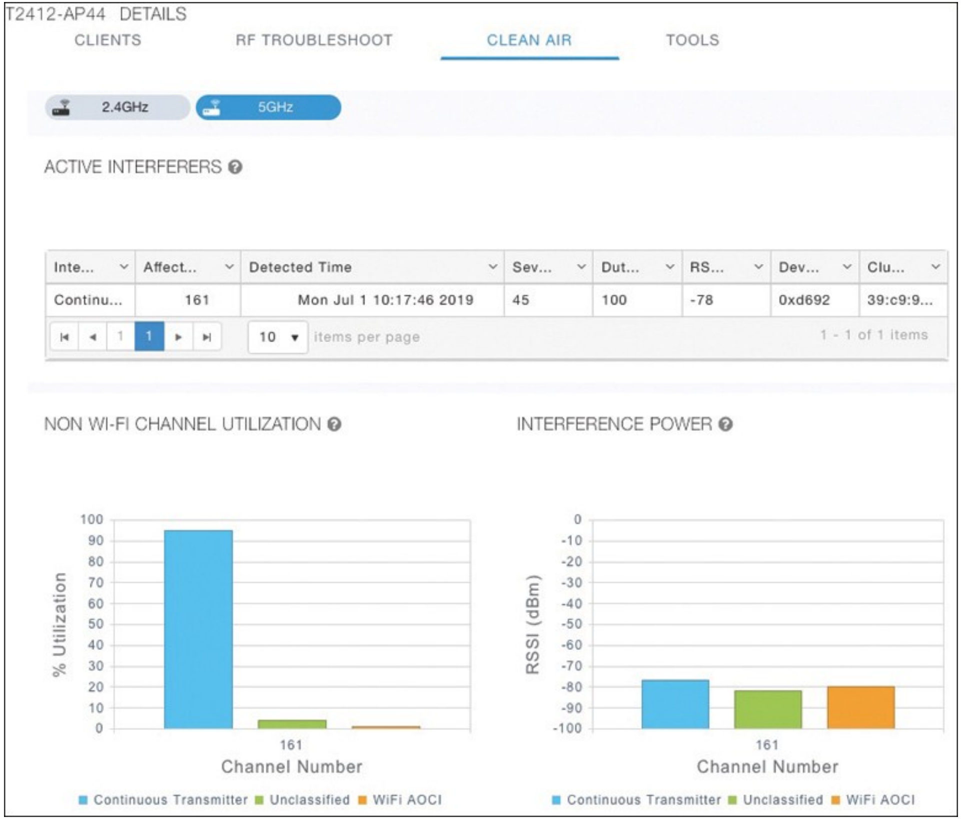
Troubleshooting Connectivity Problems at the AP

Displaying Information About Clean Air

Select the Clean Air tab to see more details about the interfering devices that have been detected.

In Figure 21-17, the Active Interferers table lists one continuous transmitter device with a severity level of 45, a duty cycle of 100%, and an RSSI value of −78 dBm.

The severity level indicates how badly the interferer is affecting the channel. The duty cycle represents the percentage of time the device is actually transmitting.



Inte...	Affect...	Detected Time	Sev...	Dut...	RS...	Dev...	Clu...
Continu...	161	Mon Jul 1 10:17:46 2019	45	100	-78	0xd692	39:c9:9...

10 items per page　1 - 1 of 1 items

Figure 21-17 *Displaying Information*

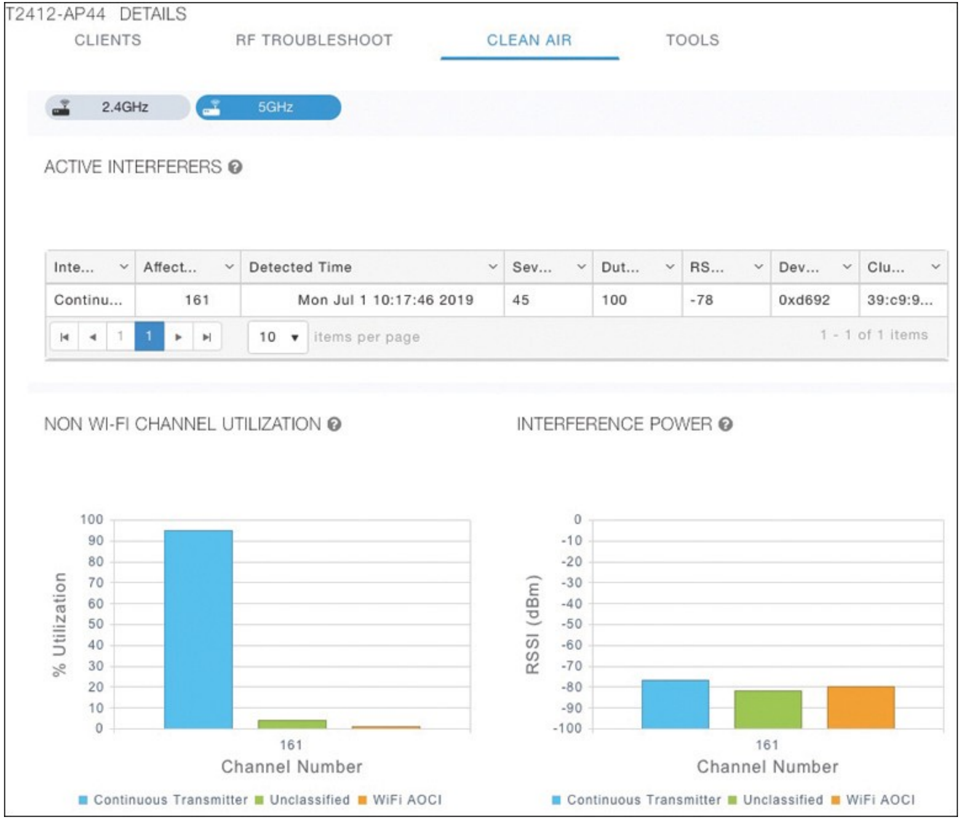
Troubleshooting Connectivity Problems at the AP

Displaying Information About Clean Air (Cont.)

The two bar graphs represent the percentage of time the device is using the channel and the received signal strength level of the device.

If users are complaining about problems when they are around this AP, you should focus your efforts on tracking down the continuously transmitting device.

The best outcome is if the device can be disabled or moved to an unused channel. If not, you will likely have to reconfigure the AP to use a different channel to move away from the interference.



Inte...	Affect...	Detected Time	Sev...	Dut...	RS...	Dev...	Clu...
Continu...	161	Mon Jul 1 10:17:46 2019	45	100	-78	0xd692	39:c9:9...

1 | 10 items per page | 1 - 1 of 1 items

Figure 21-17 *Displaying Information*

cisco