

Figure 1-1 The principles of intent-based networking

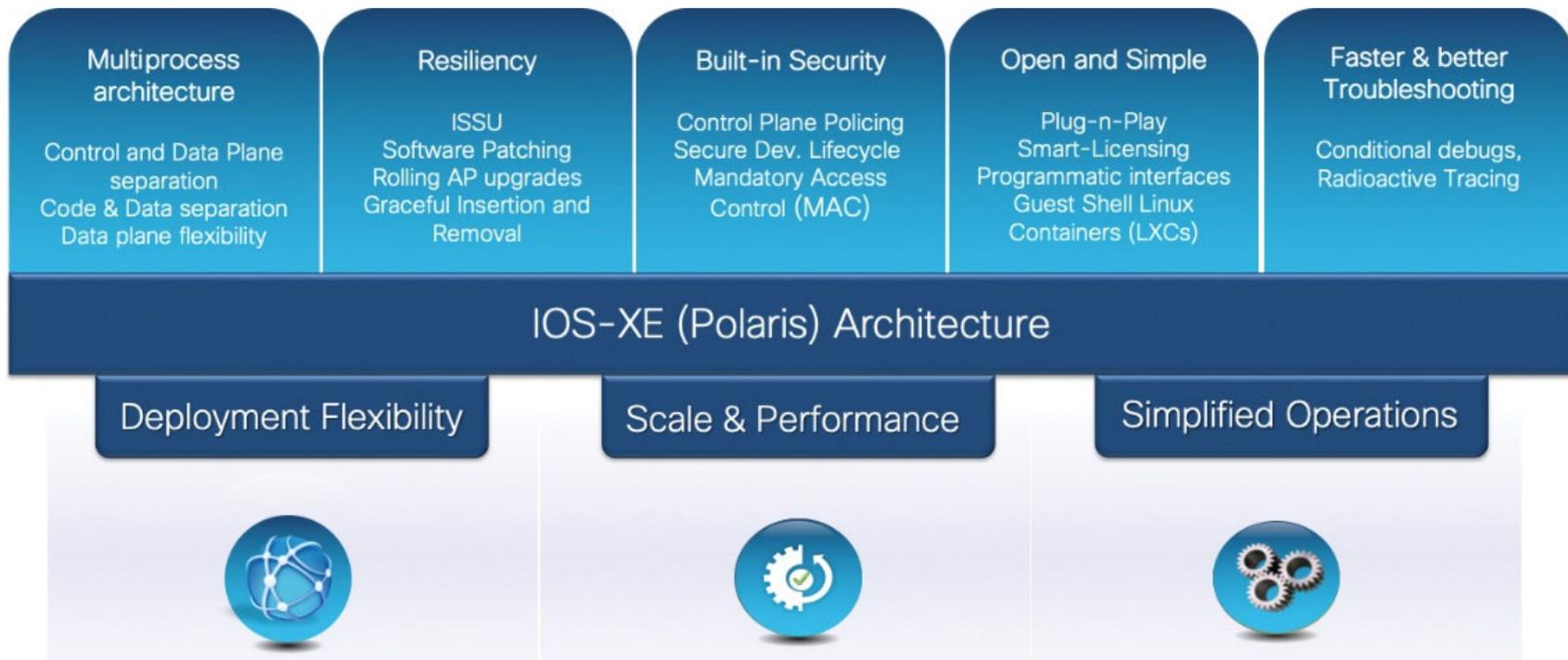


Figure 1-2 IOS-XE: A modern networking operating system

Catalyst 9800 wireless controller



QFP
QuantumFlow Processor

- Flexible, fully Programmable
- Feature-Rich
- Scalable
- Advanced on-chip QoS
- Secure
- Extensible Architecture

C9800 embedded in Catalyst 9000 switches



UADP
Unified Access Data Plane

- Flexible, Programmable
- High-Performance
- Scalable
- Advanced on-chip QoS
- Secure
- Extensible Architecture

Unlocking the power of Catalyst wireless at hardware speeds

Figure 1-3 Catalyst 9800 is built on programmable silicon

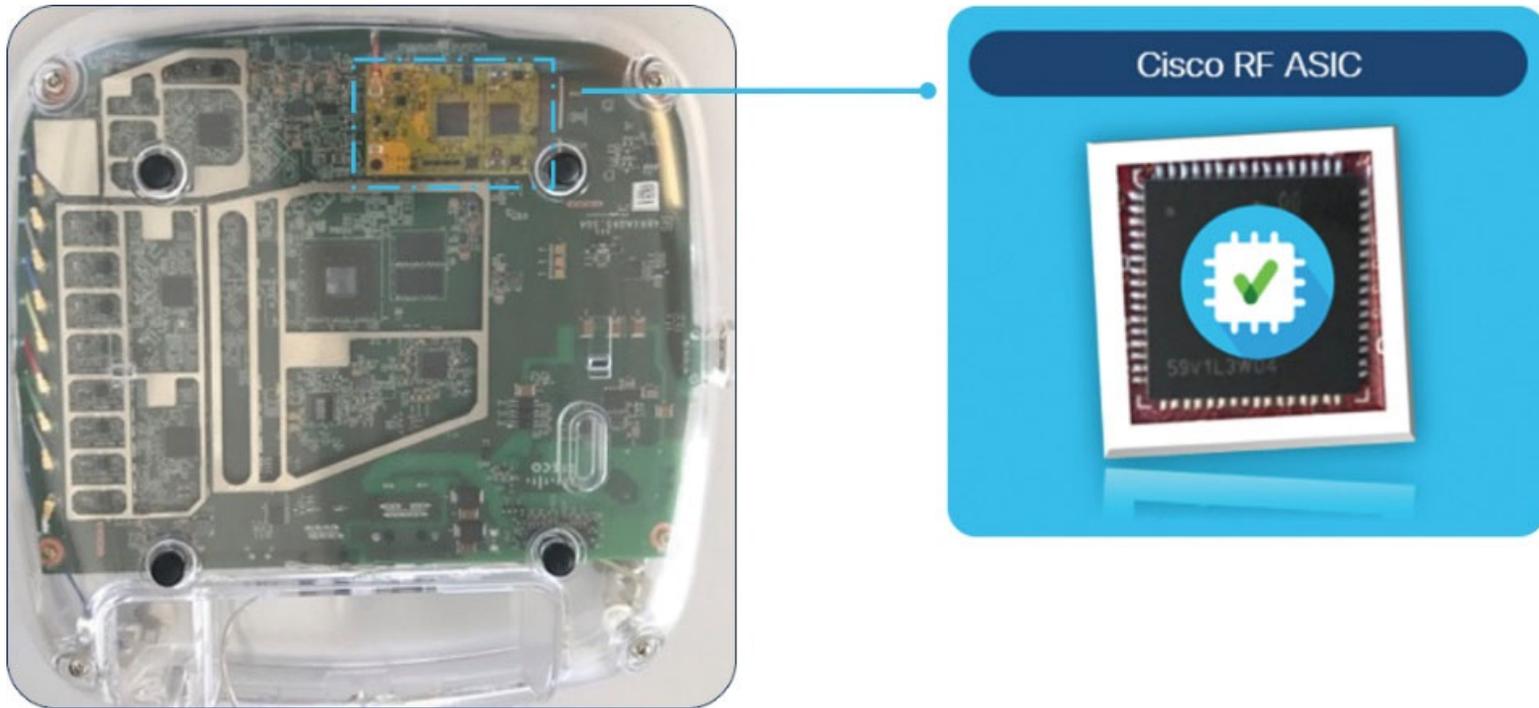


Figure 1-4 Cisco RF ASIC: Software-defined radio using a Mini-PCIe slot

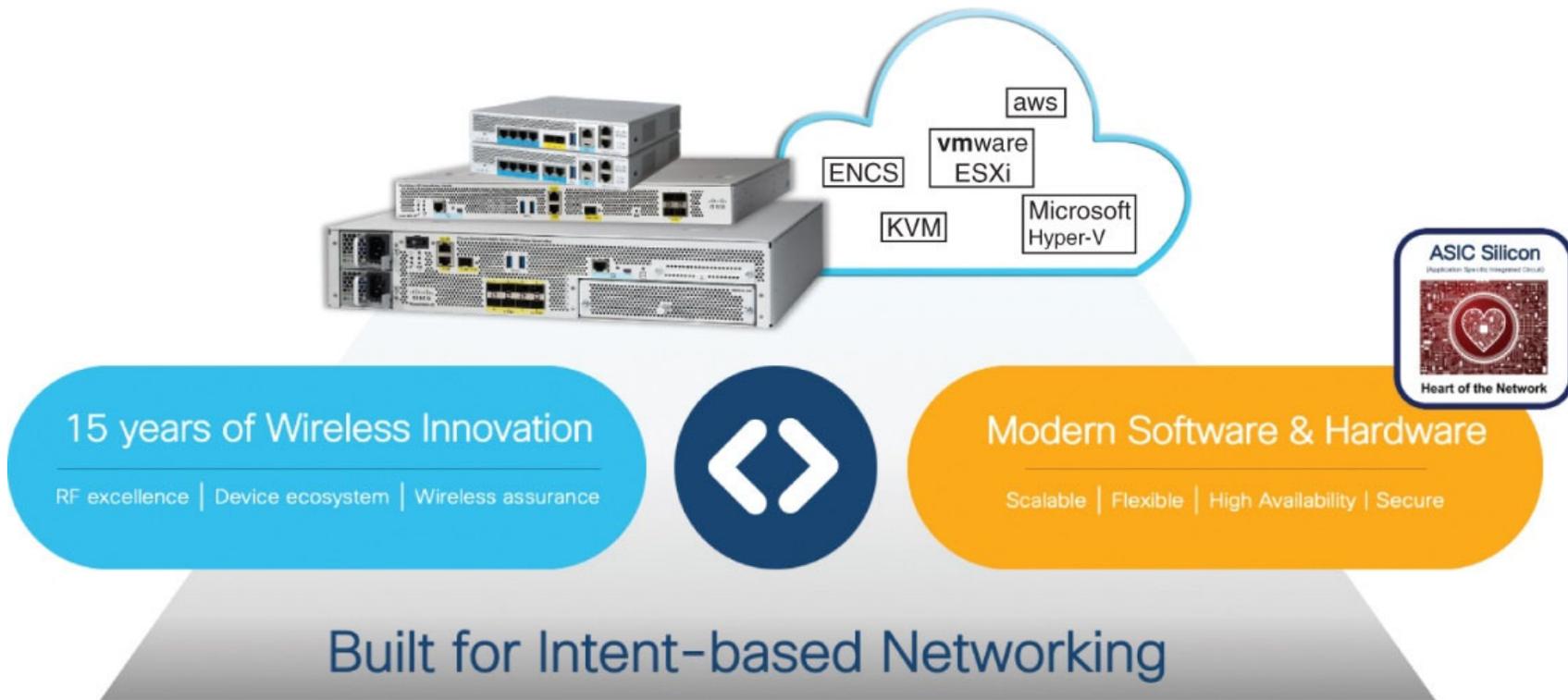


Figure 1-5 Catalyst 9800 built for intent-based networking



Figure 1-6 Catalyst 9800 flexible management options

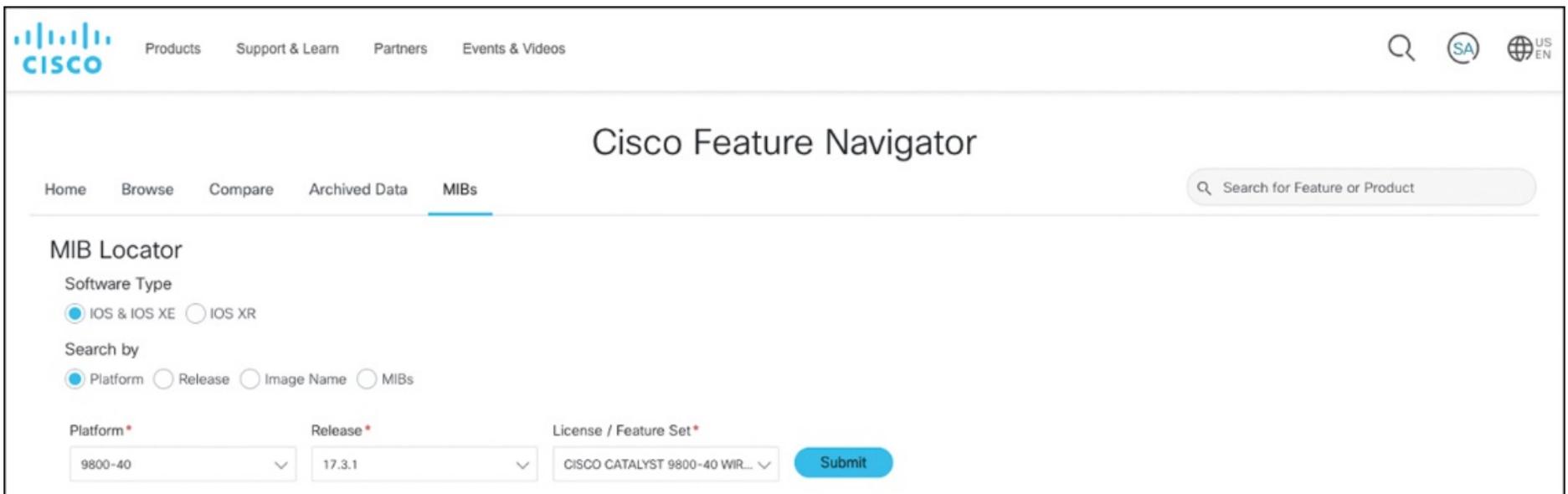


Figure 1-7 Cisco Feature Navigator

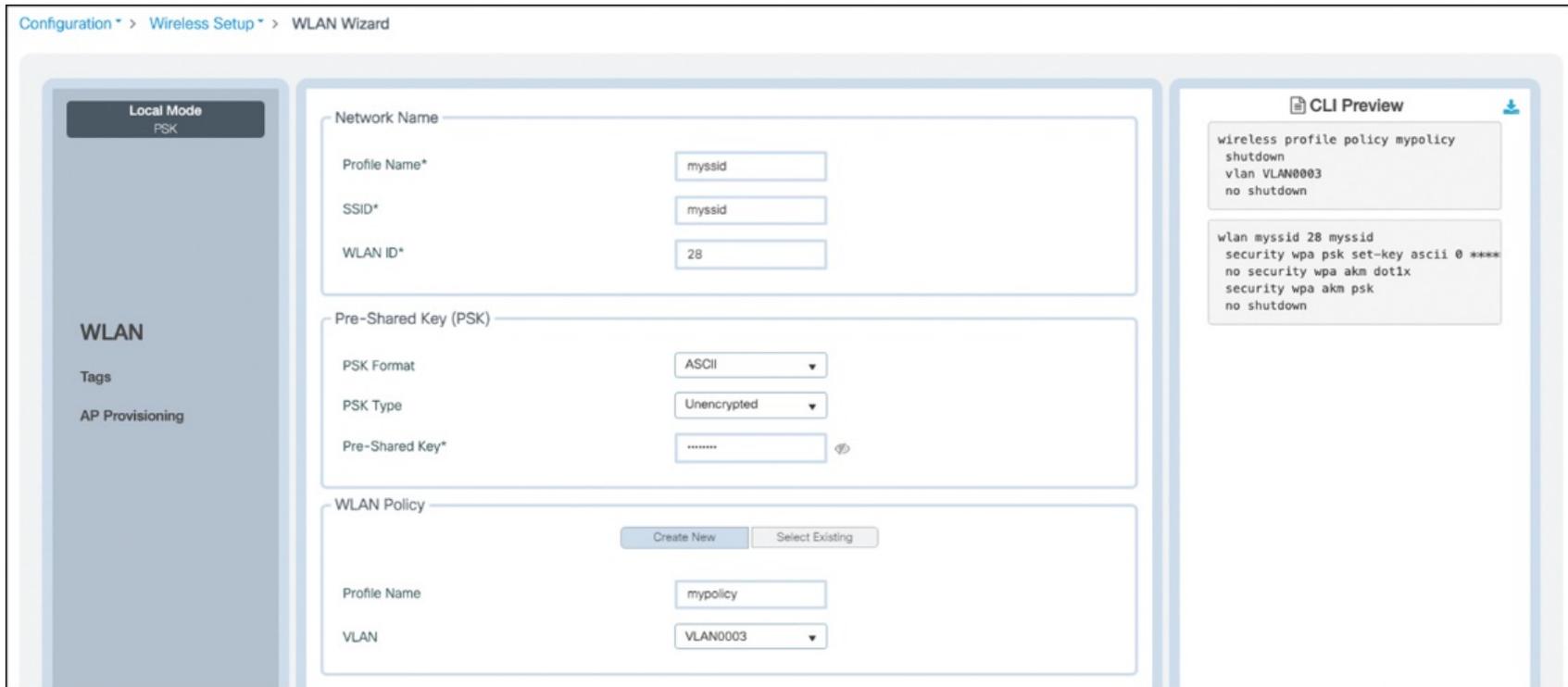


Figure 1-8 Setting up a PSK SSID with the WLAN Wizard

Wireless Setup Flow Overview

This screen allows you to design Wireless LAN Configuration. It involves creating Policies and Tags. Once the design is completed, they can be deployed to the Access Points right here.

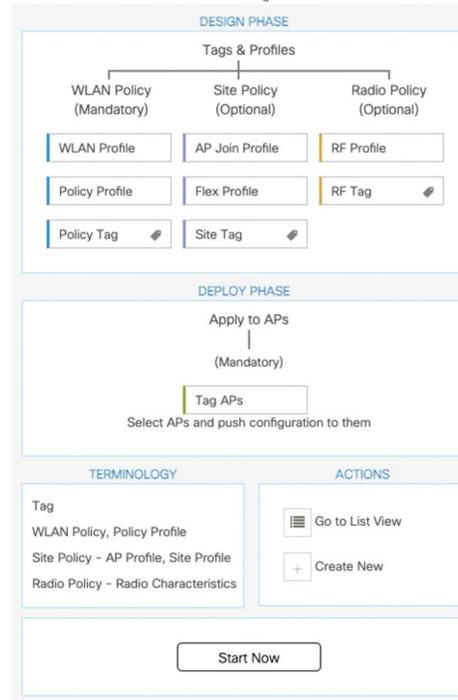


Figure 1-9 The Advanced Setup Wizard

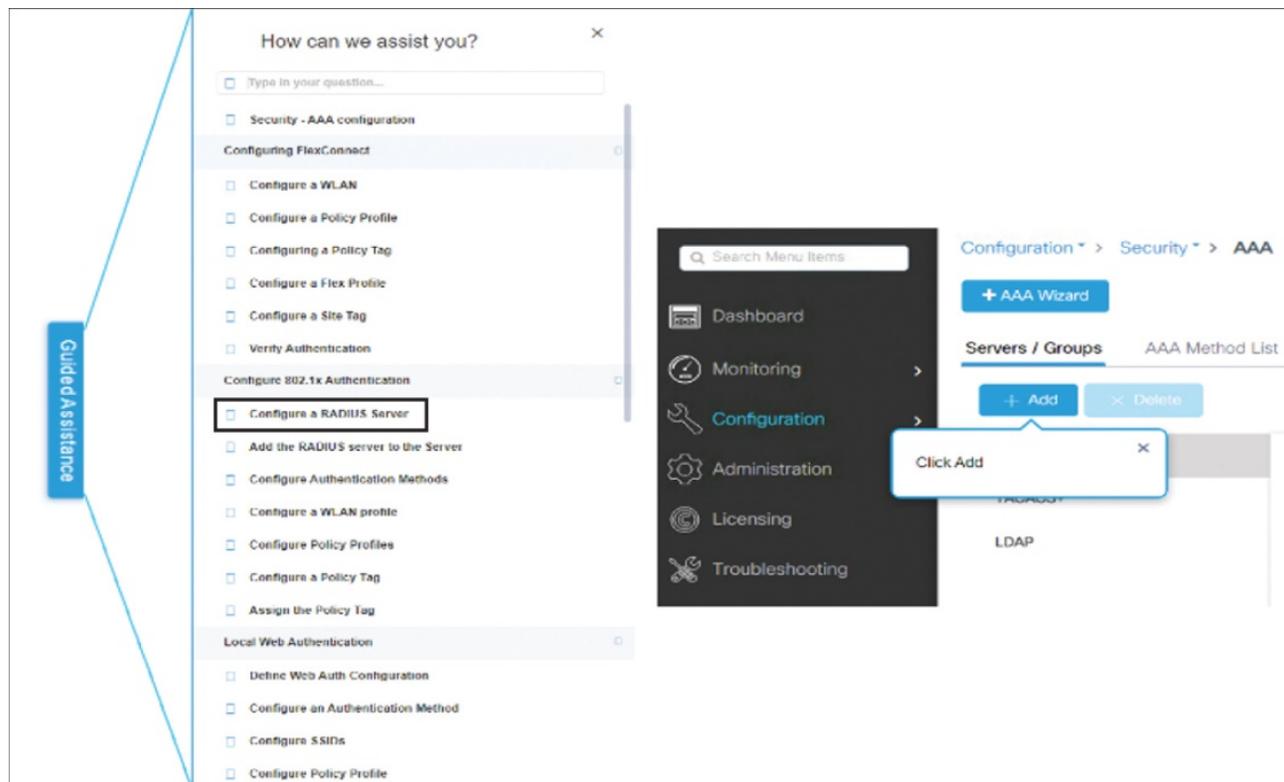


Figure 1-10 Guided Assistance tool

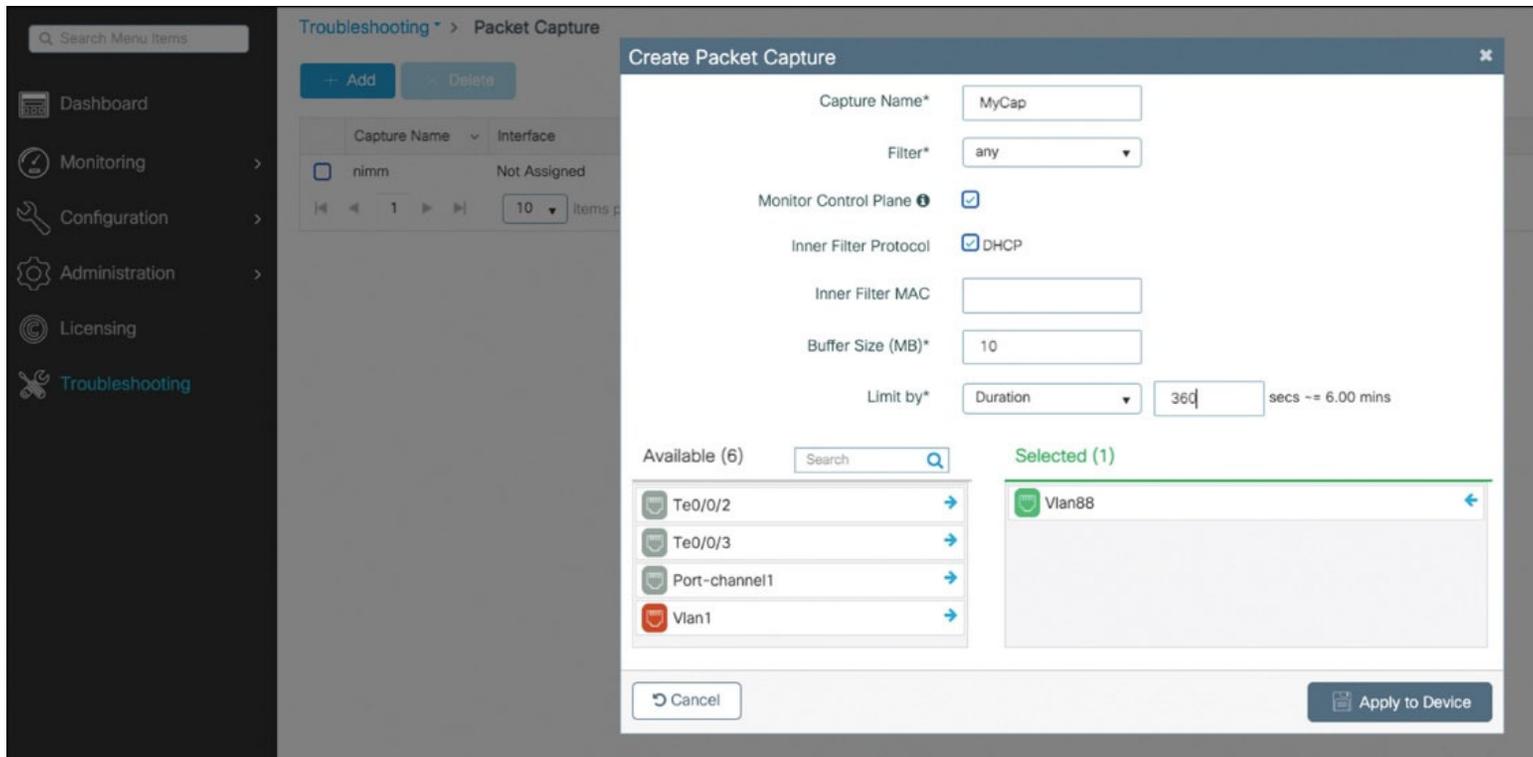


Figure 1-11 Defining a Packet Capture on C9800's GUI

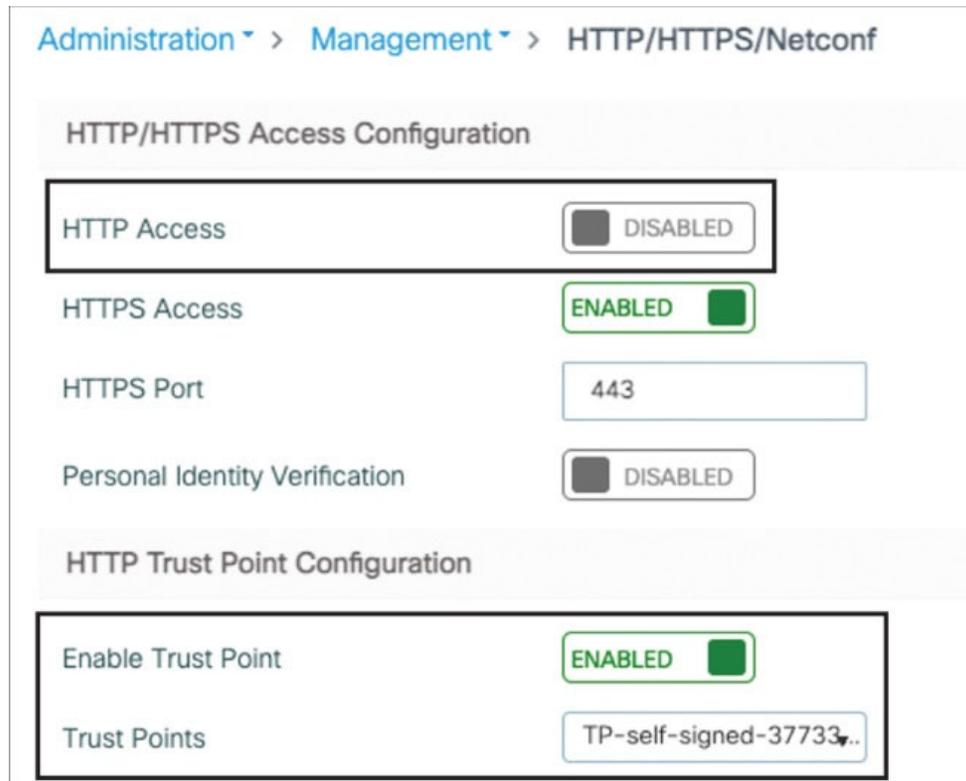


Figure 1-12 Disabling HTTP web access and selecting a specific trustpoint for HTTPS

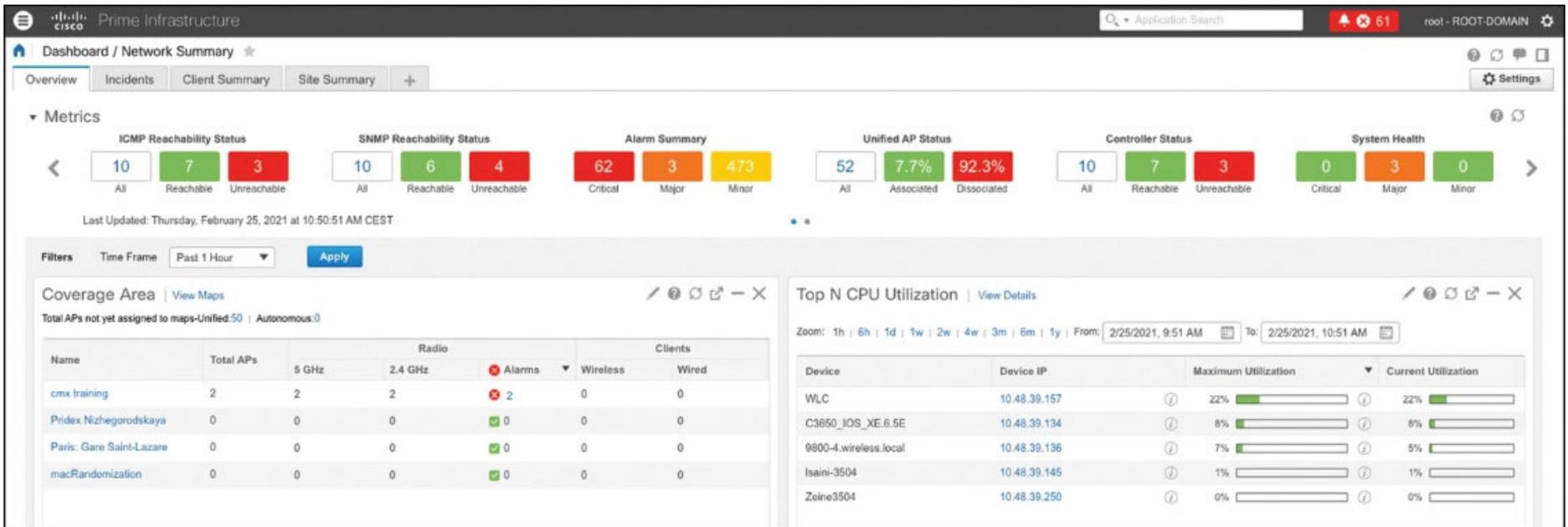


Figure 1-13 Prime Infrastructure dashboard

Administration > Management > SNMP

SNMP Mode **ENABLED**

General SNMP Views **Community Strings** V3 User Groups V3 Users Hosts Wireless Traps

+ Add **× Delete**

	Community Name
<input type="checkbox"/>	PI37

1 10 items per page

Figure 1-14 SNMP configuration of the C9800

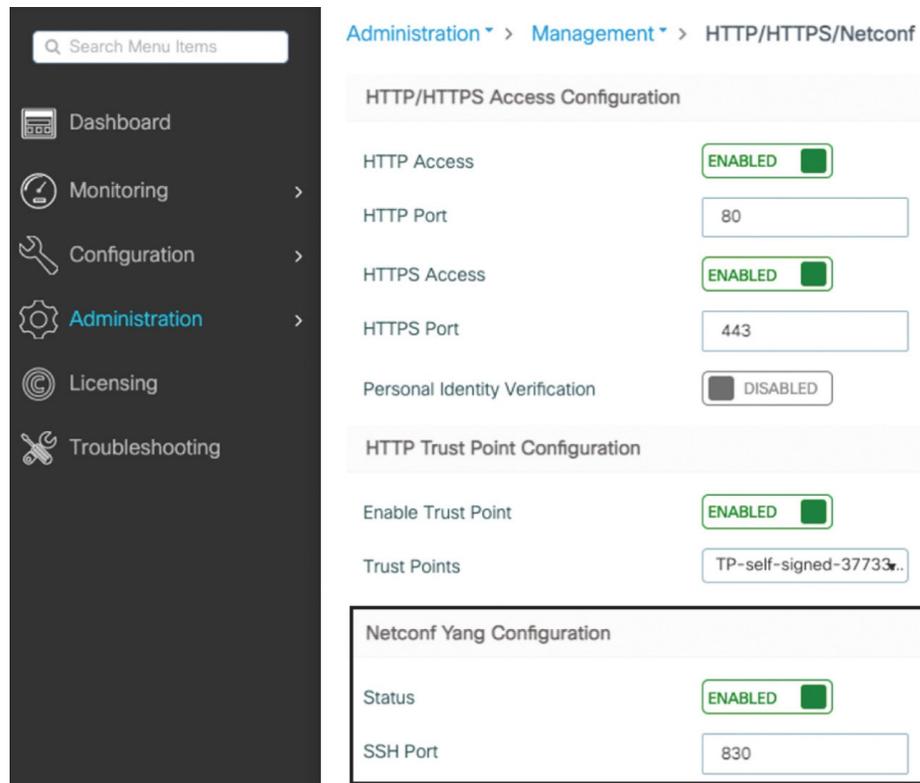


Figure 1-15 Enabling NETCONF on the Catalyst 9800 GUI

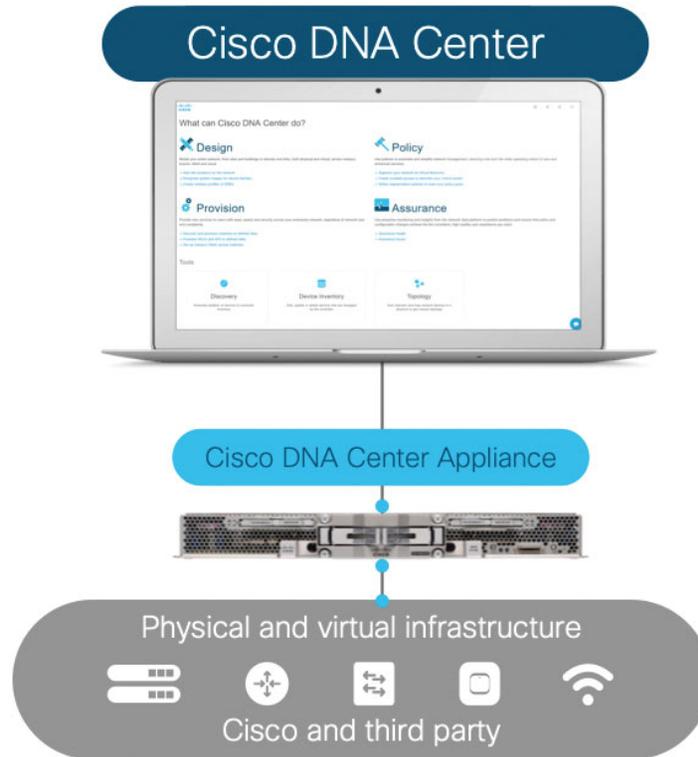


Figure 1-16 Cisco DNA Center

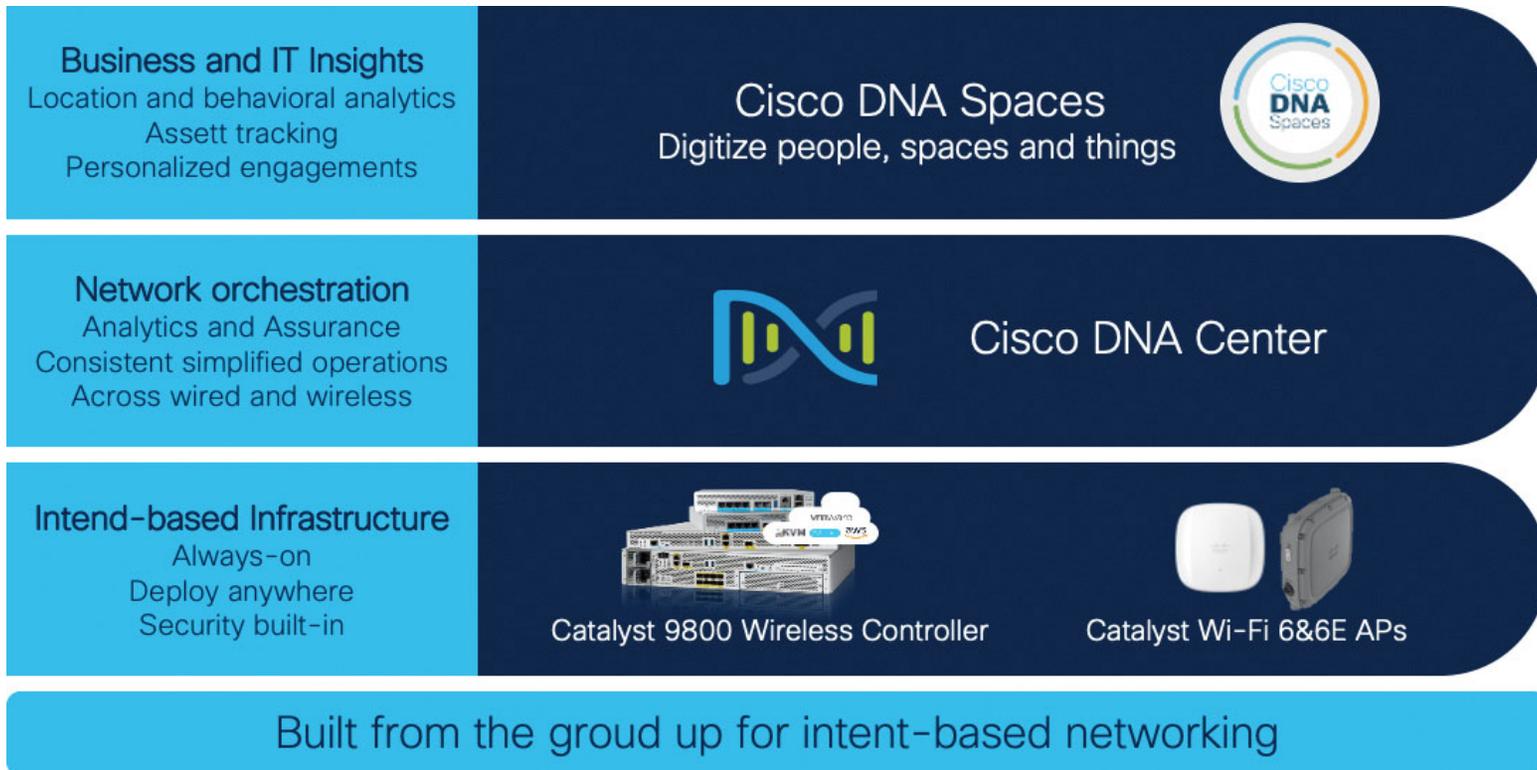


Figure 1-17 Cisco next-generation wireless stack

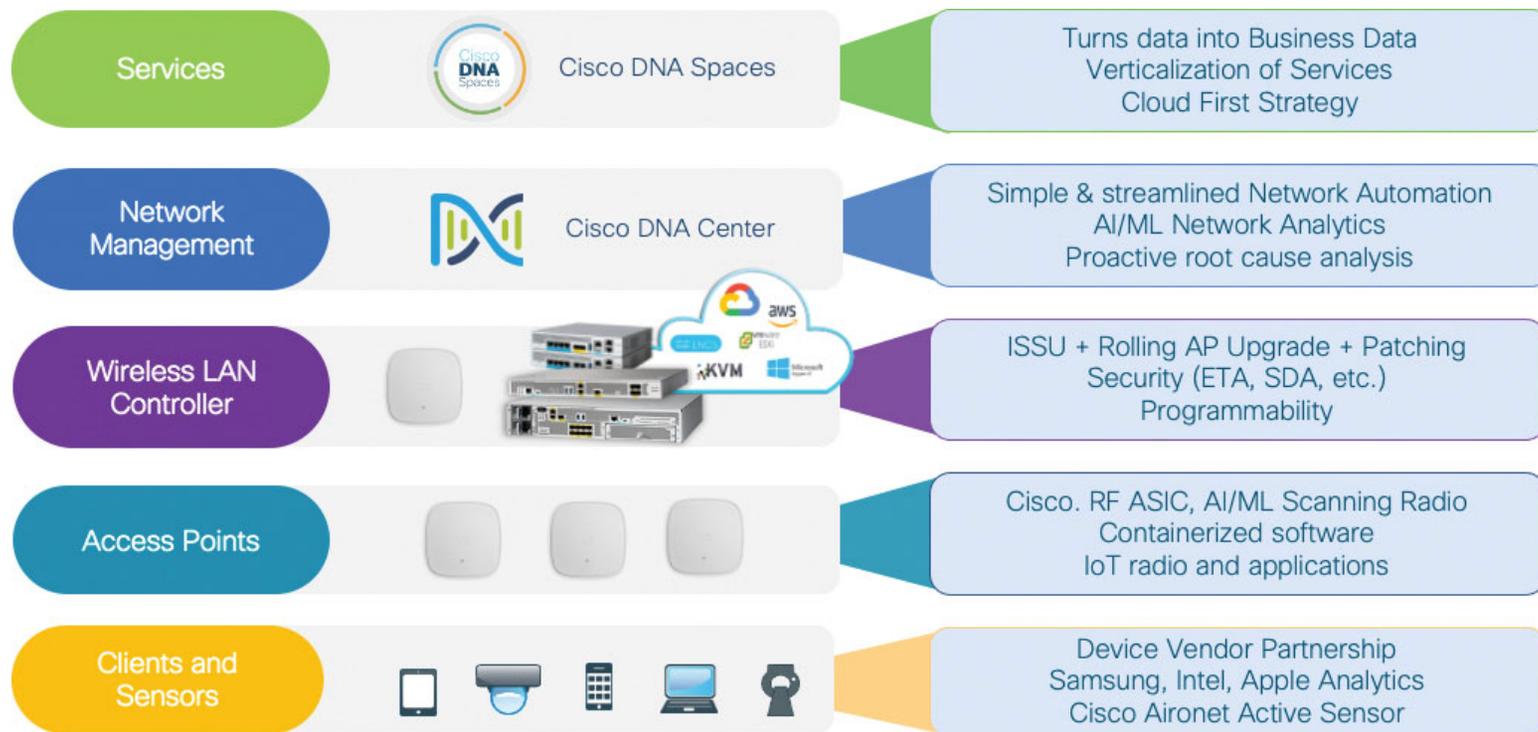


Figure 1-18 Wireless innovation at each later of the stack

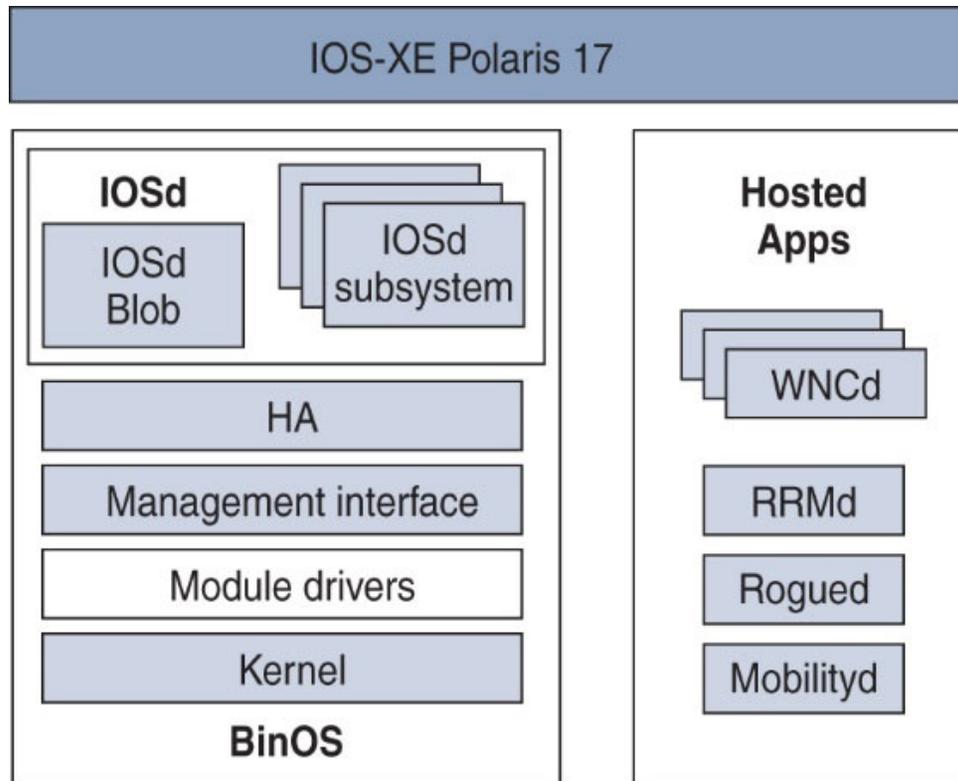


Figure 2-1 IOS-XE general software architecture

Previous software architecture vs Catalyst Wireless Controller

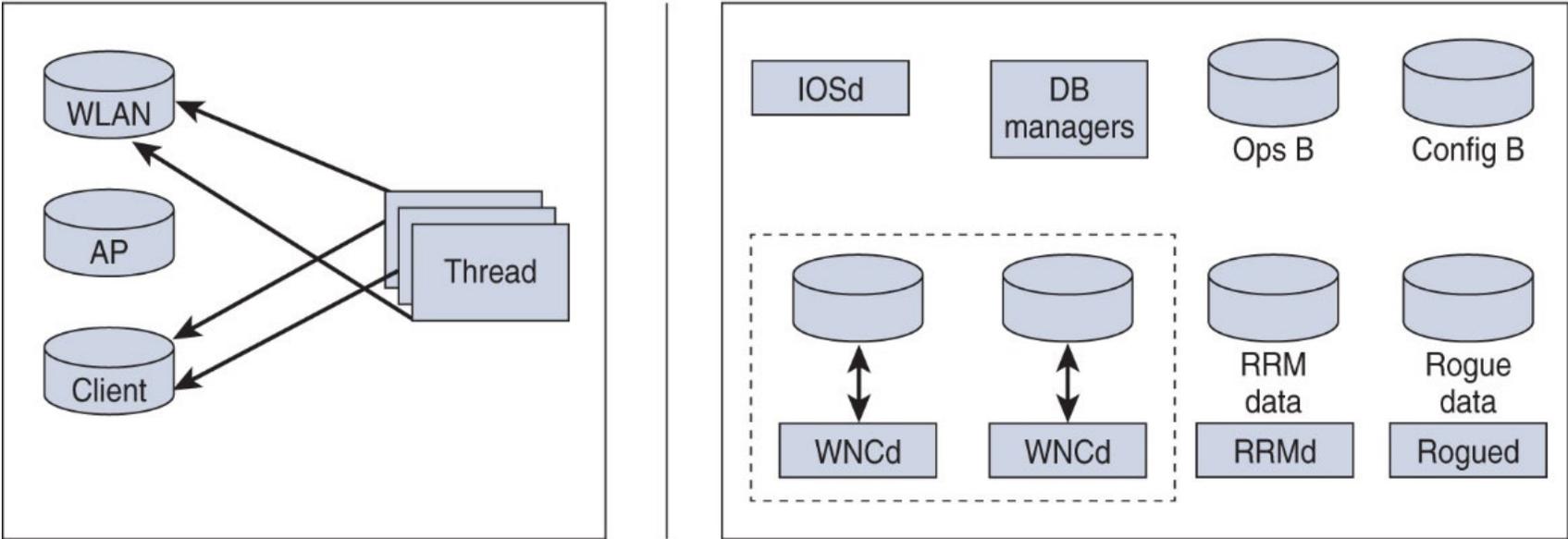


Figure 2-2 The old wireless architecture on the left compared to the Catalyst Wireless architecture on the right

From *Understanding and Troubleshooting Cisco Catalyst 9800 Series Wireless Controller* by Simone Arena, Francisco Sedano Crippa, Nicolas Darchis and Sudha Katgeri(9780137492329) Cisco Press
 Copyright© 2023 Cisco Systems, Inc. All rights reserved

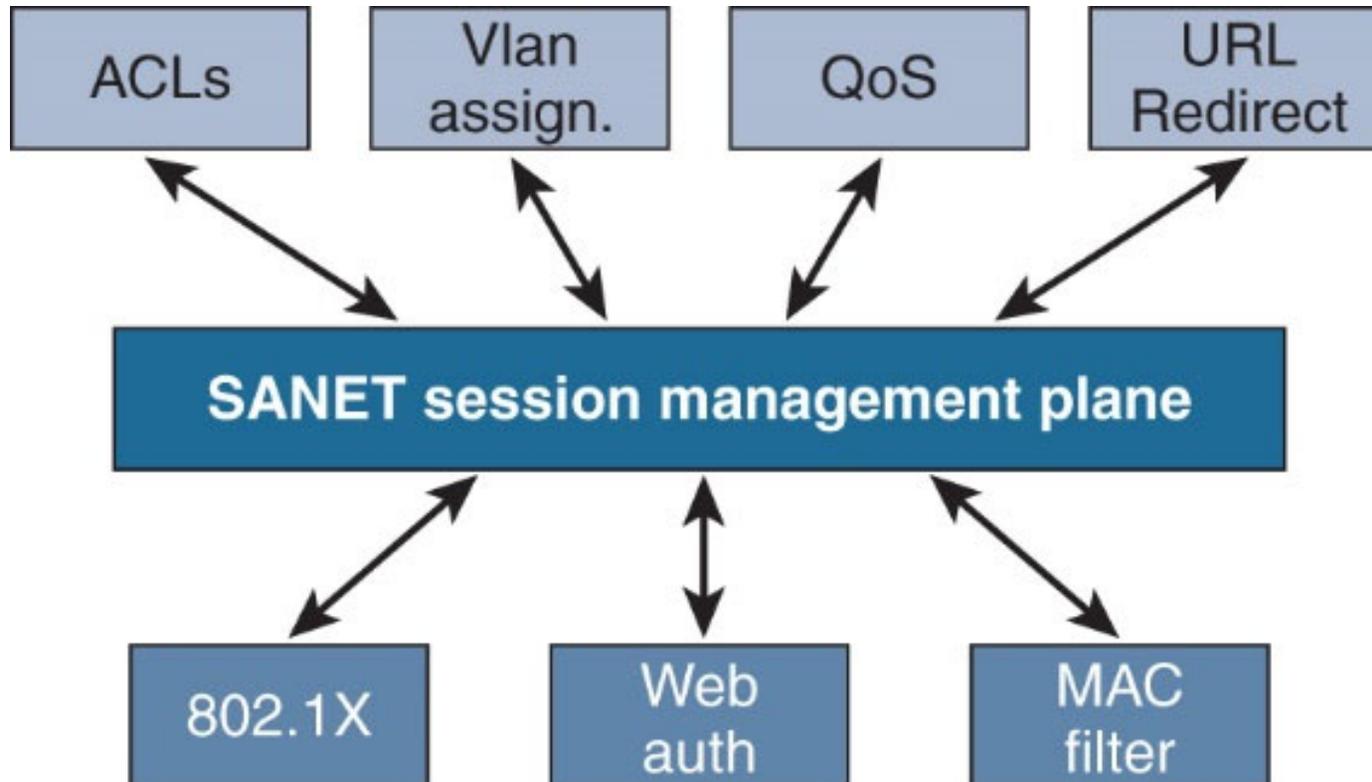
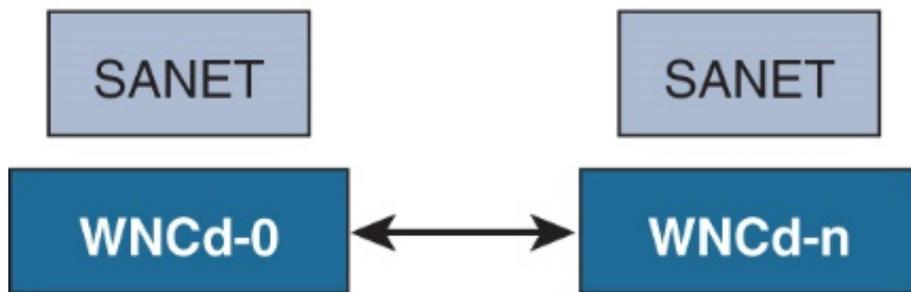


Figure 2-3 SANET library responsibilities

Wired services



Wired and common services

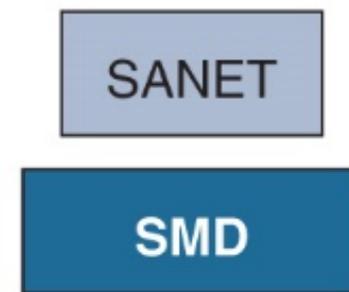


Figure 2-4 WNCd processes and the AAA task split between the existing SMD process and the new SANET libraries inside WNCds

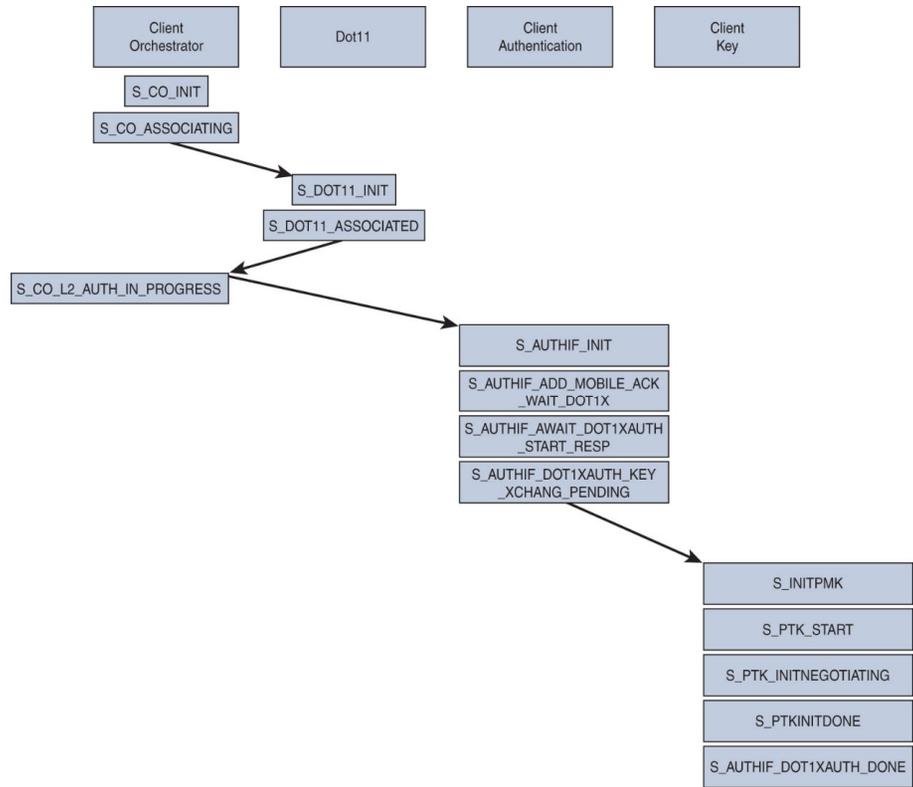


Figure 2-5 Client state machine on a WPA2 Enterprise SSID

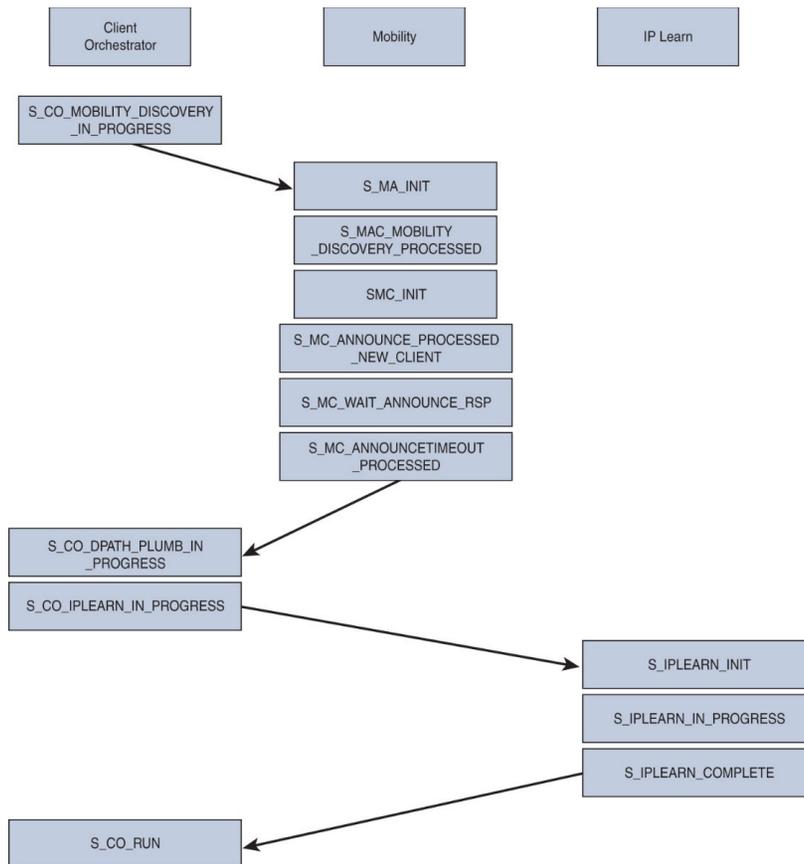


Figure 2-6 Client state machine on a WPA2 Enterprise SSID (continued)

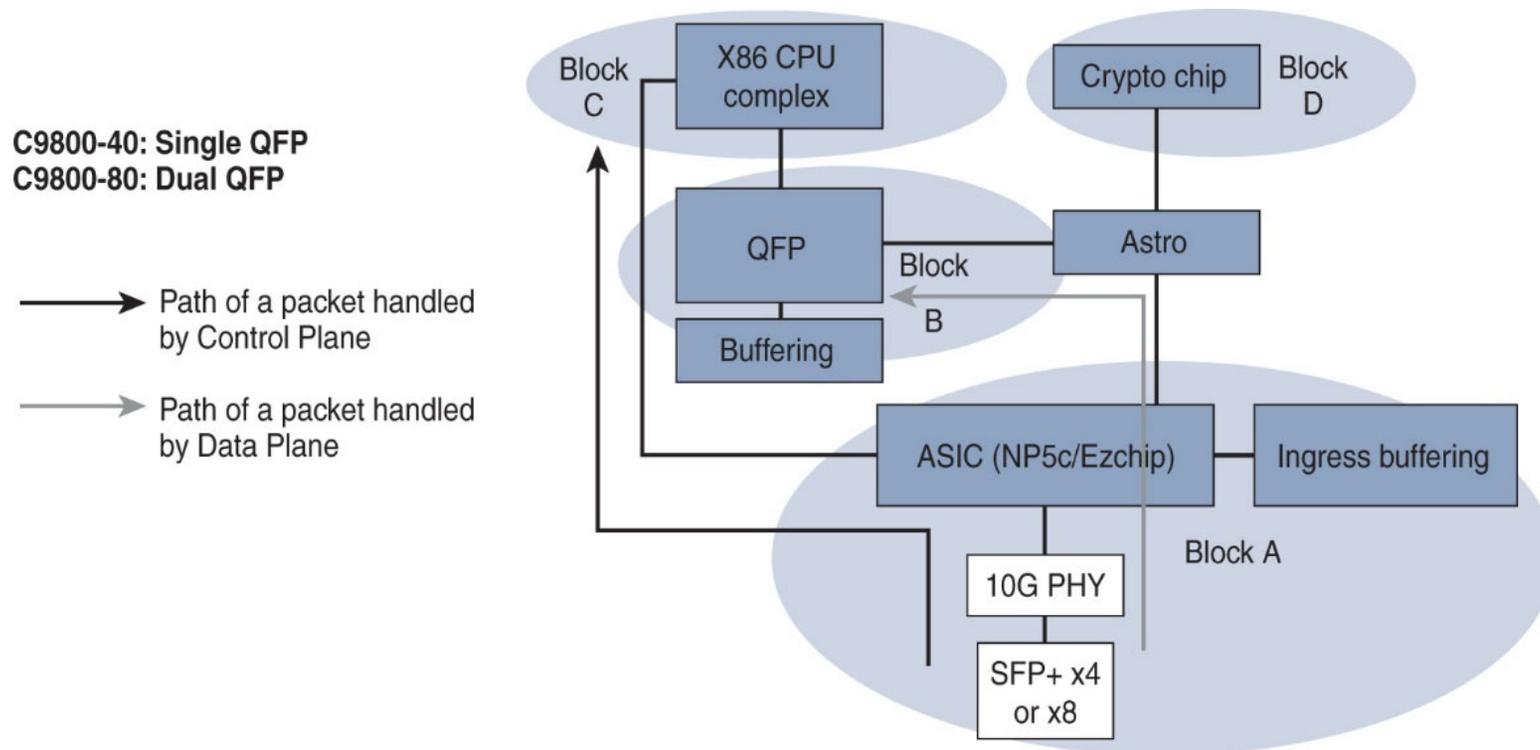


Figure 2-7 Block diagram of the life of a packet in the 9800 appliance's dataplane

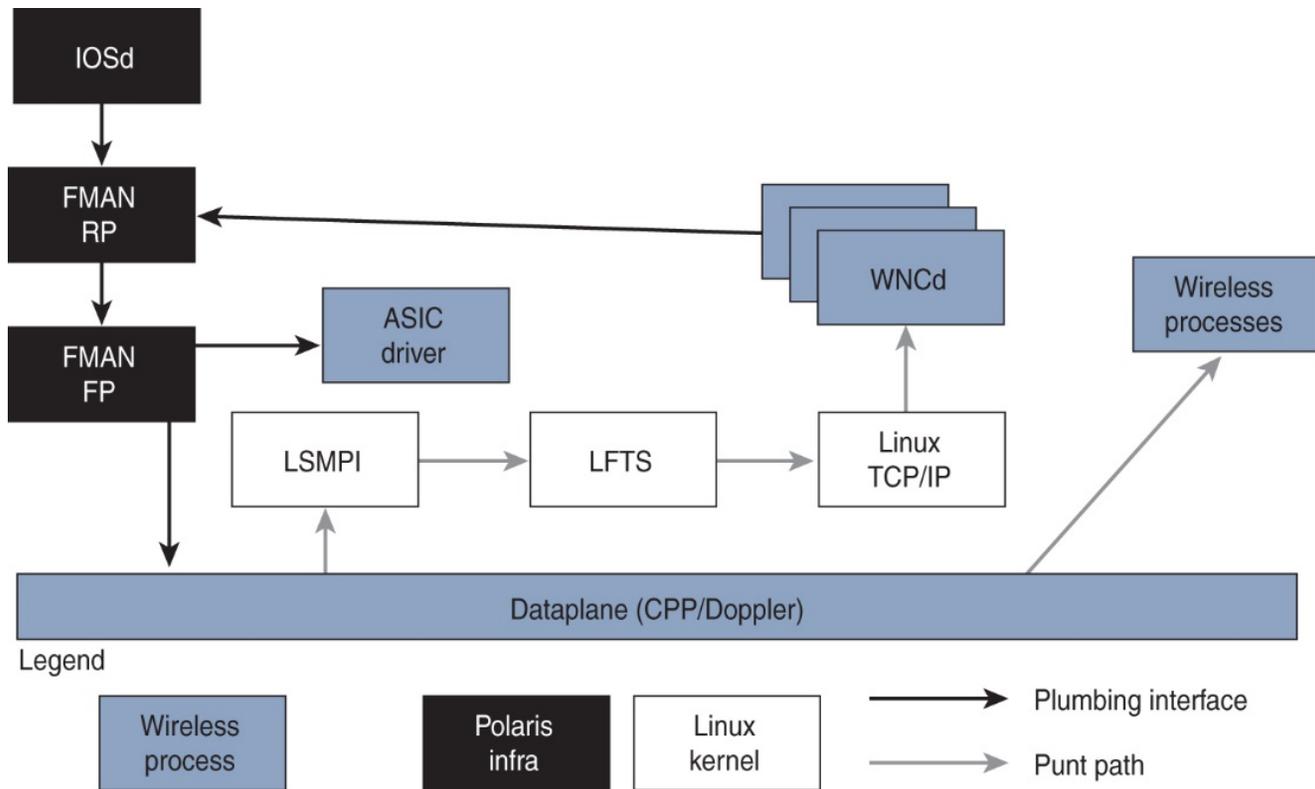


Figure 2-8 Control Plane packet processing



Figure 2-9 A 9800-40 appliance

From *Understanding and Troubleshooting Cisco Catalyst 9800 Series Wireless Controller* by Simone Arena, Francisco Sedano Crippa, Nicolas Darchis and Sudha Katgeri(9780137492329) Cisco Press
Copyright© 2023 Cisco Systems, Inc. All rights reserved



Figure 2-10 A 9800-80 appliance

From *Understanding and Troubleshooting Cisco Catalyst 9800 Series Wireless Controller* by Simone Arena, Francisco Sedano Crippa, Nicolas Darchis and Sudha Katgeri(9780137492329) Cisco Press
Copyright© 2023 Cisco Systems, Inc. All rights reserved



Figure 2-11 A 9800-L-C appliance

From *Understanding and Troubleshooting Cisco Catalyst 9800 Series Wireless Controller* by Simone Arena, Francisco Sedano Crippa, Nicolas Darchis and Sudha Katgeri(9780137492329) Cisco Press
Copyright© 2023 Cisco Systems, Inc. All rights reserved

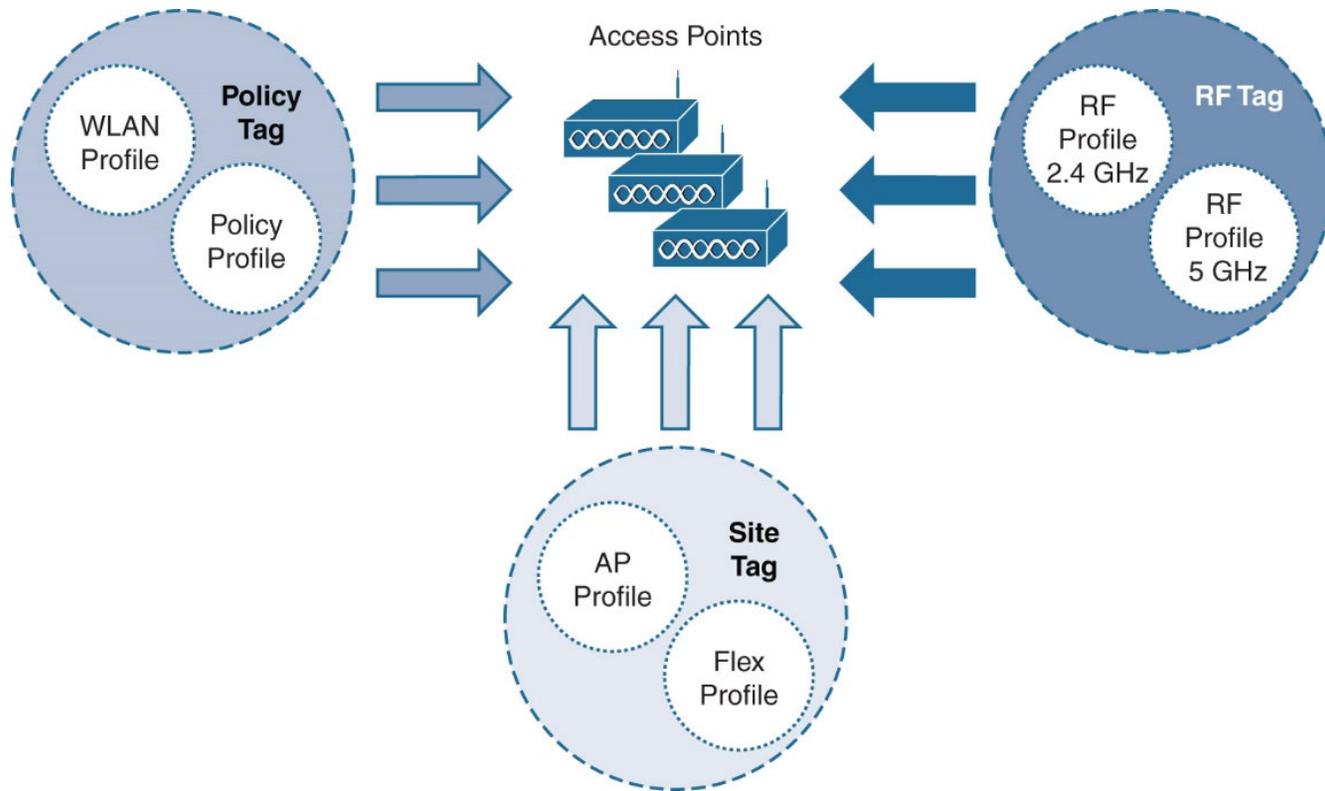


Figure 3-1 Profiles and tags and AP assignment

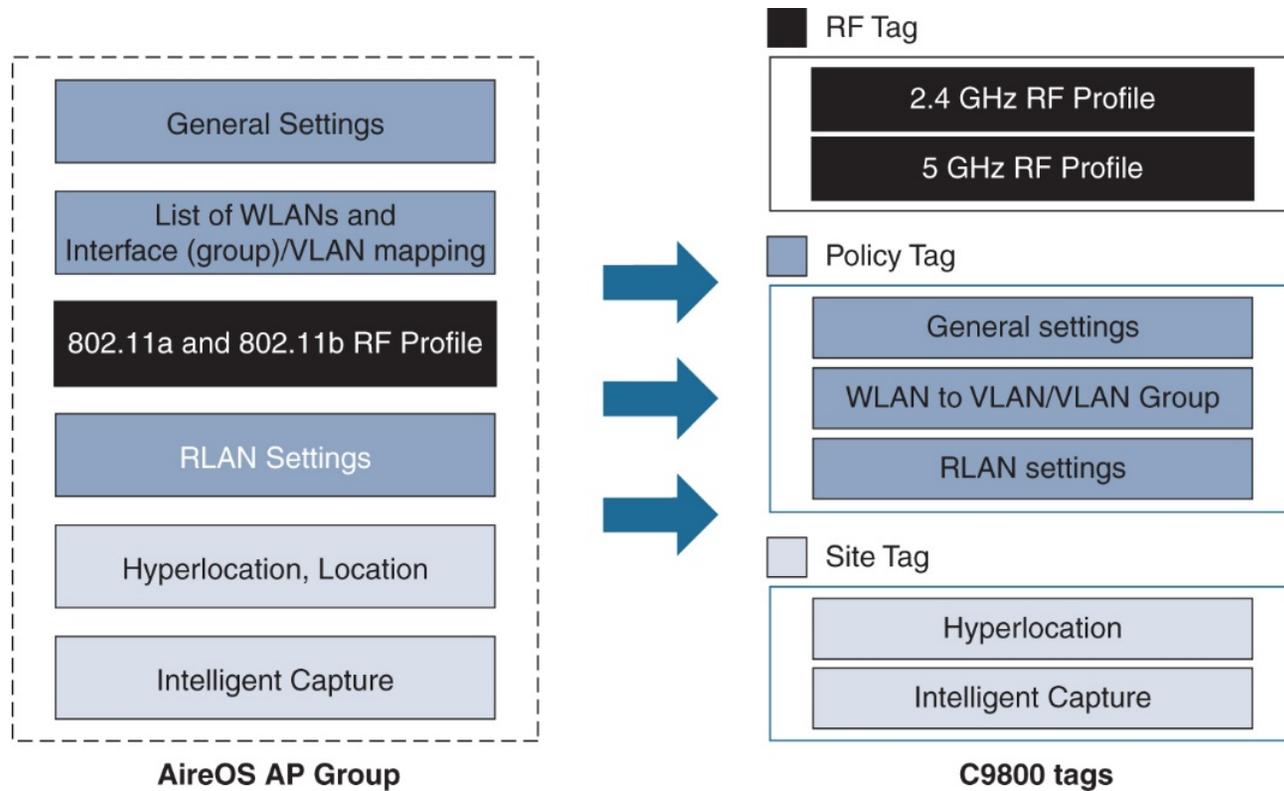


Figure 3-2 AireOS AP Group to C9800 site tags mapping

Edit Site Tag

⚠ Changing Site type may result in rejoin of APs that are associated to this Site Tag

Name*	default-site-tag
Description	default site tag
AP Join Profile	default-ap-profile ▼
Flex Profile	default-flex-profile ▼ default-flex-profile
Fabric Control Plane Name	

Enable Local Site

Figure 3-3 Setting the site tag as FlexConnect = nonlocal site

▼ All Access Points

Number of AP(s): 3

AP Name	AP Model	Slots	Admin Status	IP Address	Base Radio MAC	AP Mode	Operation Status	Configuration Status	Policy Tag	Site Tag	RF Tag	Tag Source
AP-3800i-SJ	AIR-AP3802i-B-K9	2	✓	172.16.11.10	006b.f19c.5080	Local	Registered	Healthy	PT_US-WE_SJC-2_Floor2_6d981	building24	TYPICAL	Static
AP3700_f9a0-SJ	AIR-CAP3702E-A-K9	3	✓	172.16.11.11	5897.bd37.f9a0	Local	Registered	Healthy	PT_US-WE_SJC-2_Floor3_59278	building24	TYPICAL	Static
AP2800-f960-SJ	AIR-AP2802i-B-K9	2	✓	172.16.11.12	f80b.cbd6.f960	Local	Registered	Healthy	PT_US-WE_SJC-2_Floor3_59278	building24	TYPICAL	Static

10 items per page

Figure 3-4 AP tags in the GUI

Configuration > Wireless > Access Points

▼ All Access Points

Number of AP(s): 3

AP Name	AP Model	Slots	Admin Status	IP Address	Base Radio MAC	AP Mode	Operation Status	Configuration Status	Policy Tag	Site Tag	RF Tag	Tag Source	Location
AP-3800i-SJ	AIR-AP3802I-B-K9	2	✓	172.16.11.10	006b.f19c.5080	Local	Registered	Healthy	PT_US-WE_SJC-2_Floor2_6d981	building24	TYPICAL	Static	Global/US-WEST/SJ24/Floor2

AP Operational Configuration Viewer

```

graph TD
    AP[AP-3800i-SJ] --- WP[WLANs and Policies  
PT_US-WE_SJC-...]
    AP --- SP[Site properties  
building24  
Local]
    AP --- RP[RF properties  
TYPICAL]
    
    WP --- W1[WLAN : sj-psk_Global_NF_...  
Policy : sj-psk_Global_NF_...  
VLAN ID : vlan210  
Security : WPA2 (PSK)]
    WP --- W2[WLAN : sj-dot1x_Global_N...  
Policy : sj-dot1x_Global_N...  
VLAN ID : vlan210  
Security : WPA2]
    
    SP --- APJoin[AP Join : default-ap-profile  
LED State : ✓  
Rogue Detection : ✓]
    
    RP --- B5[5 GHz Band : Typical_Client_De...  
Status : ✓]
    RP --- B24[2.4 GHz Band : Typical_Client_...  
Status : ✓]
  
```

Figure 3-5 AP tags details in the GUI

c9800-SJ-11#sh ap tag summary
Number of APs: 3

AP Name	AP Mac	Site Tag Name	Policy Tag Name	RF Tag Name	Misconfigured	Tag Source
AP-3800i-SJ	00a6.ca36.25f2	building24	PT_US-WE_SJC-2_Floor2_6d981	TYPICAL	No	Static
AP3700_f9a0-SJ	5897.bd2b.3388	building24	PT_US-WE_SJC-2_Floor3_59278	TYPICAL	No	Static
AP2800-f960-SJ	2c33.1180.70fa	building24	PT_US-WE_SJC-2_Floor3_59278	TYPICAL	No	Static

Figure 3-6 AP tag summary

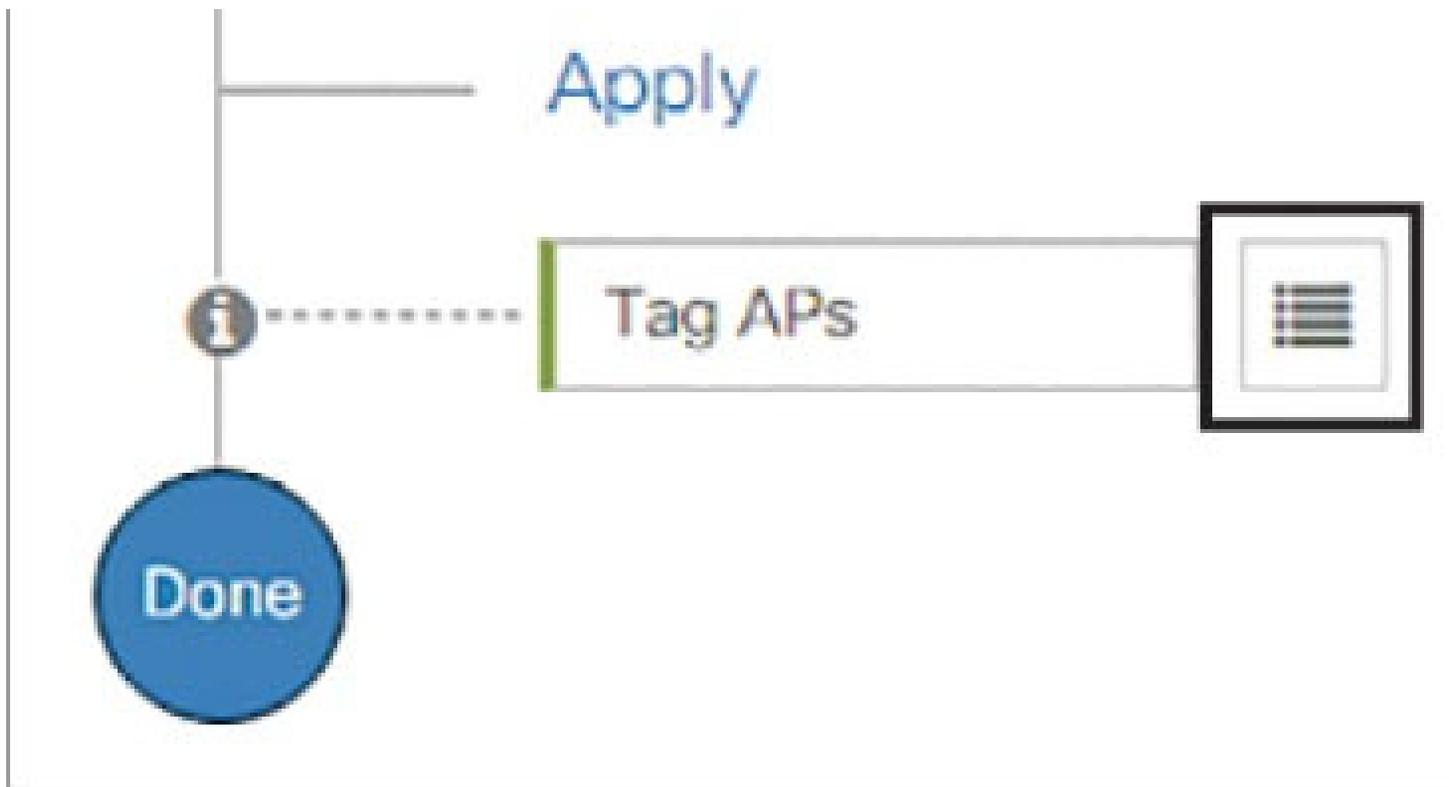


Figure 3-7 Click the menu icon to select APs and assign tags

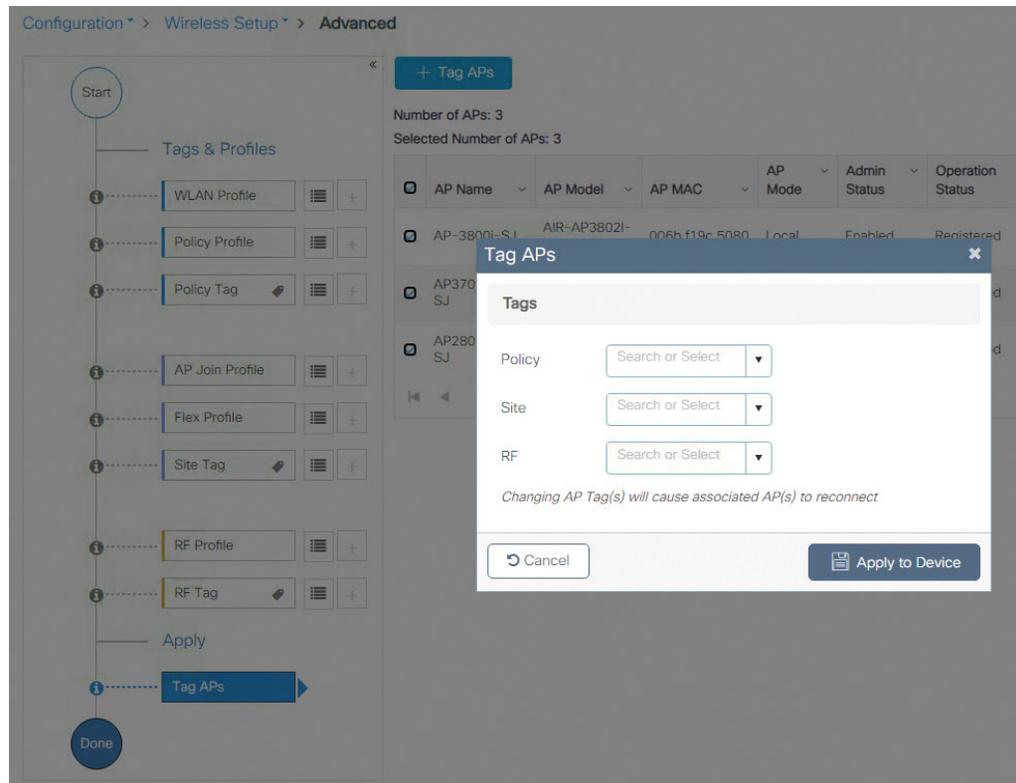


Figure 3-8 Assign the tags to the selected APs

Edit AP

General Interfaces High Availability Inventory ICap Advanced Support Bundle

General		Tags	
AP Name*	<input type="text" value="AP-1815T"/>	Policy	<input type="text" value="OEAP-tag"/>
Location*	<input type="text" value="default location"/>	Site	<input type="text" value="OEAP-site"/>
Base Radio MAC	700f.6a3c.1e80	RF	<input type="text" value="default-rf-tag"/>
Ethernet MAC	7079.b3e0.c3f0	<input type="checkbox"/> Write Tag Config to AP	

Figure 3-9 Starting with release 17.4.1, the write tag is available in the GUI

Configuration > Tags & Profiles > Tags

Policy Site RF **AP**

Tag Source Static Location **Filter**

+ Add × Delete

	Priority		Rule Name		AP name regex
⏪	0	⏩		10	items per page

Figure 3-10 Go to the Filter tab to define the tag filter

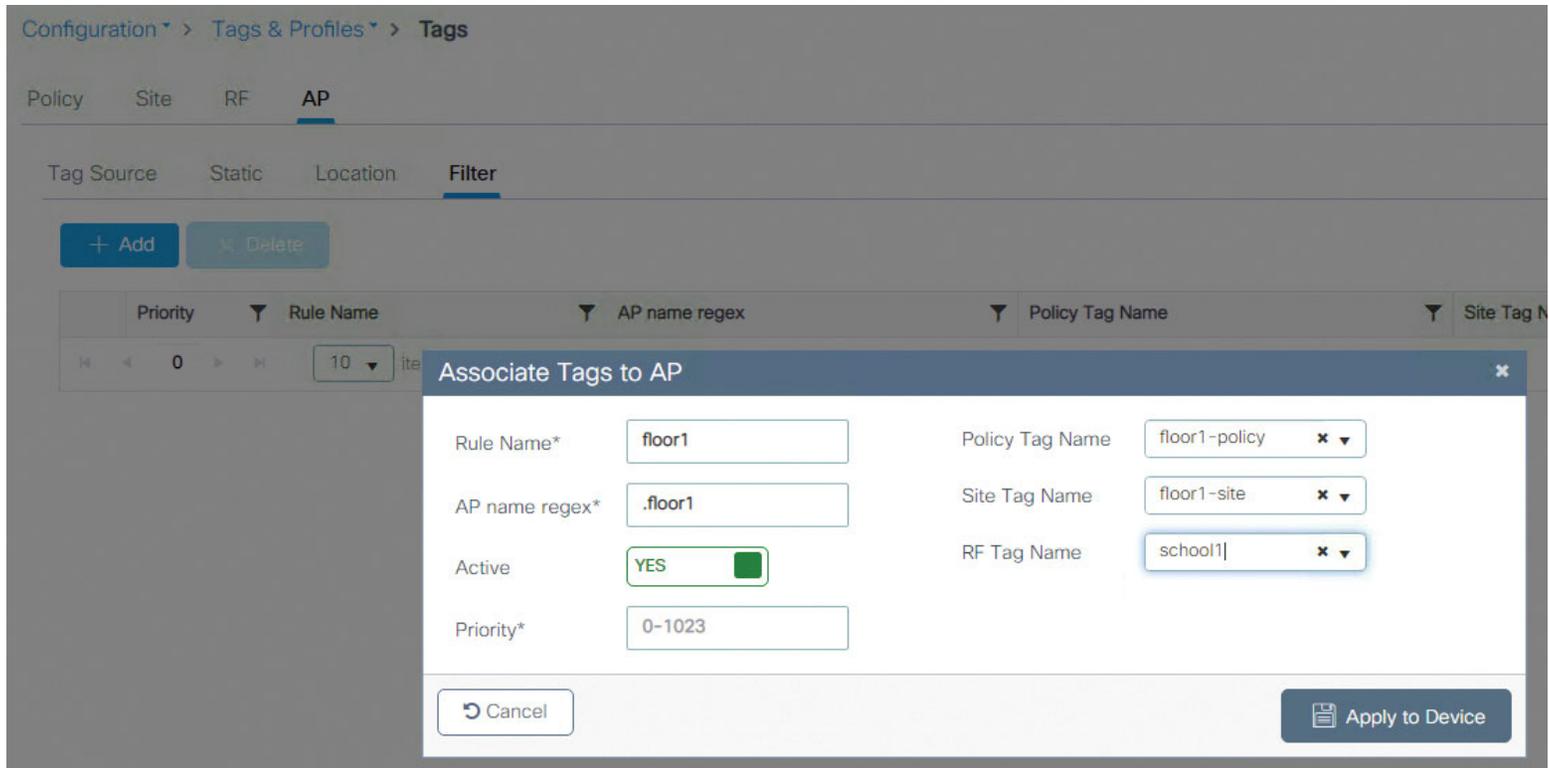


Figure 3-11 A tag filter

 AP-list - Notepad

File Edit Format View Help

```
80e8.6fd8.61e0,OEAP-policy-tag,OEAP-site,default-rf-tag  
c4f7.d54d.0b7c,OEAP-policy-tag,OEAP-site,default-rf-tag
```

Figure 3-12 CSV import file format example

Configuration > Tags & Profiles > Tags

Policy Site RF **AP**

Tag Source **Static** Location Filter

Select CSV File

Number of AP Tag mappings selected : 0

<input type="checkbox"/>	AP MAC Address	Policy Tag Name	Site Tag Name
<input type="checkbox"/>	7079.b3e0.c3f0	OEAP-tag	OEAP-site
<input type="checkbox"/>	80e8.6fd8.61e0	flex-tag	flex-site
<input type="checkbox"/>	c4f7.d54d.0b7c	flex-tag	flex-site

Figure 3-13 Selecting the file to load the AP to tag mapping

Configuration > Layer2 > VLAN

SVI VLAN **VLAN Group**

+ Add × Delete

VLAN GROUP NAME
<input type="checkbox"/> students

Edit VLAN Group: students

VLAN Group Name*

VLAN List* (Ex: 1,2,5-7)

Figure 3-14 VLAN group definition

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in

General **Access Policies** QOS and AVC Mobility

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification **Enabled** ⓘ

Local Subscriber Policy Name

VLAN

VLAN/VLAN Group

Figure 3-15 VLAN group assignment within the policy profile

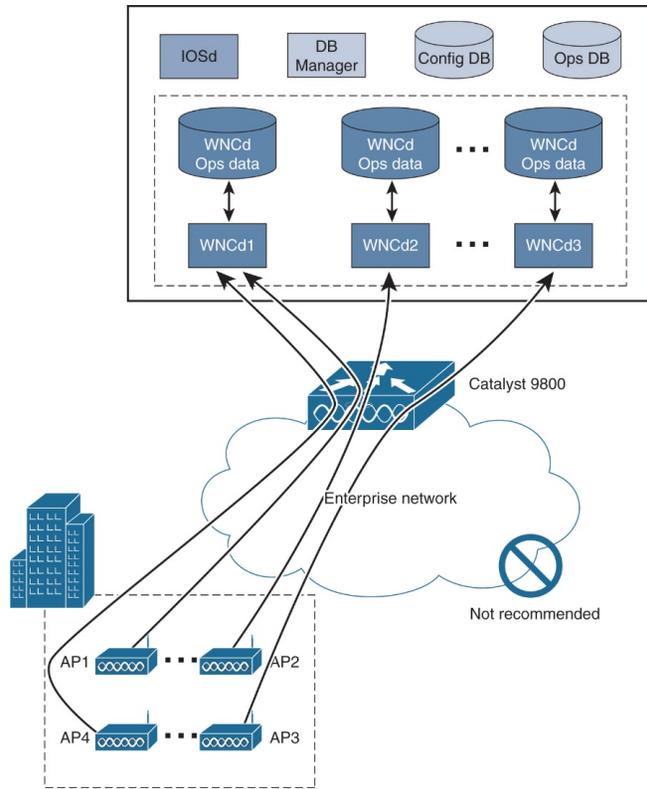


Figure 3-16 APs to WNCd distribution using the default-site-tag

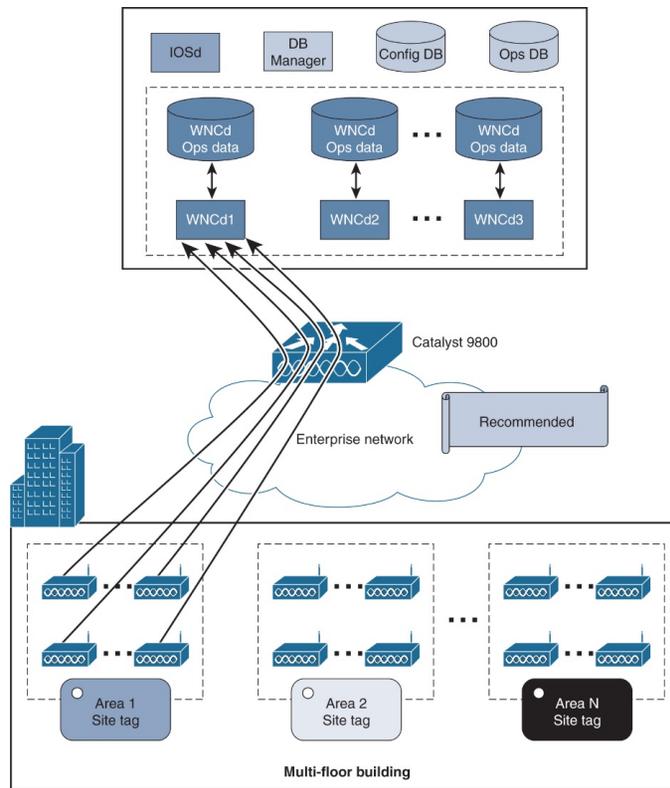


Figure 3-17 APs to WNCd distribution using custom site tag per roaming domain

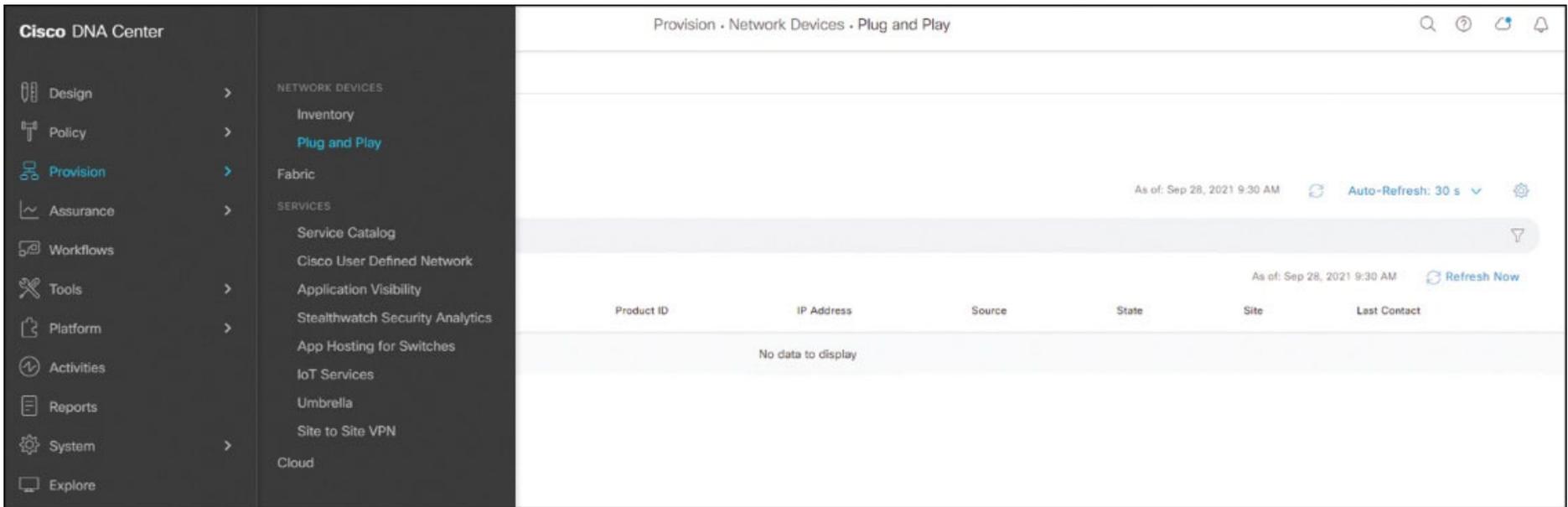


Figure 4-1 Plug and Play provision flow

Inventory **Plug and Play**

DEVICE STATUS **Unclaimed (1)** Error (0) Provisioned (32) All (33)

Devices (1)

Last updated: 1:40 PM

🔄 Refresh

+ Add Devices

🔍 Filter | Actions ▾

🔍 Find

<input type="checkbox"/>	#	Device Name	Serial Number	Product ID	IP Address	Source	Onboarding Progress	Site	Last Contact	⋮
<input type="checkbox"/>	1	WLC	TTM22490UKK	C9800-40-K9	128.107.234.24	Network	<div style="width: 40%;"></div> 40%	N/A	Oct 27, 2020 01:40 PM	

Figure 4-2 C9800 ready to be claimed in Plug and Play dashboard

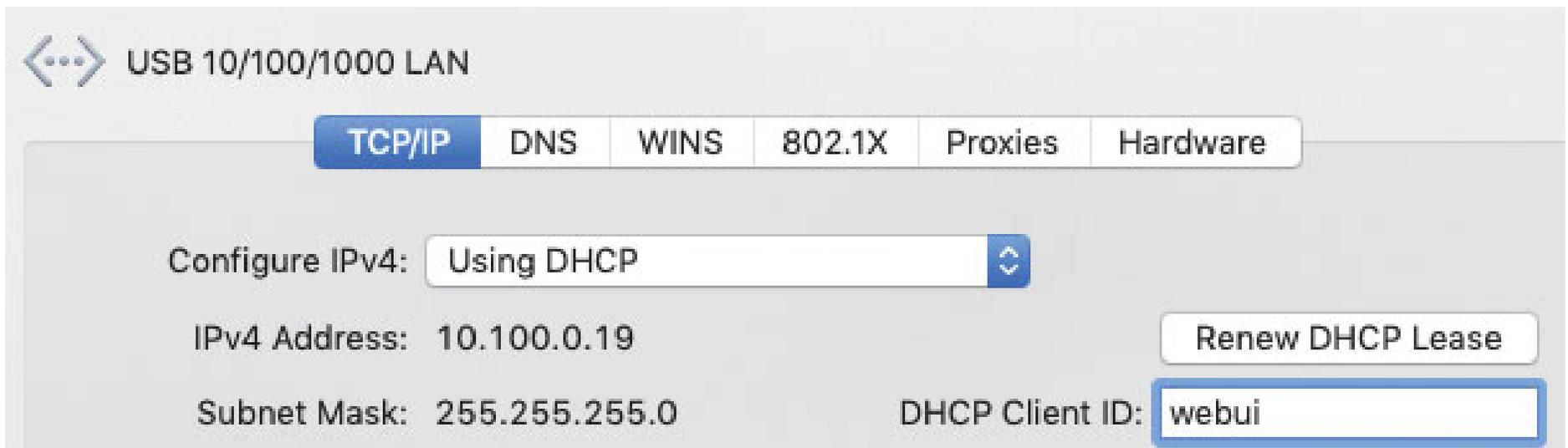
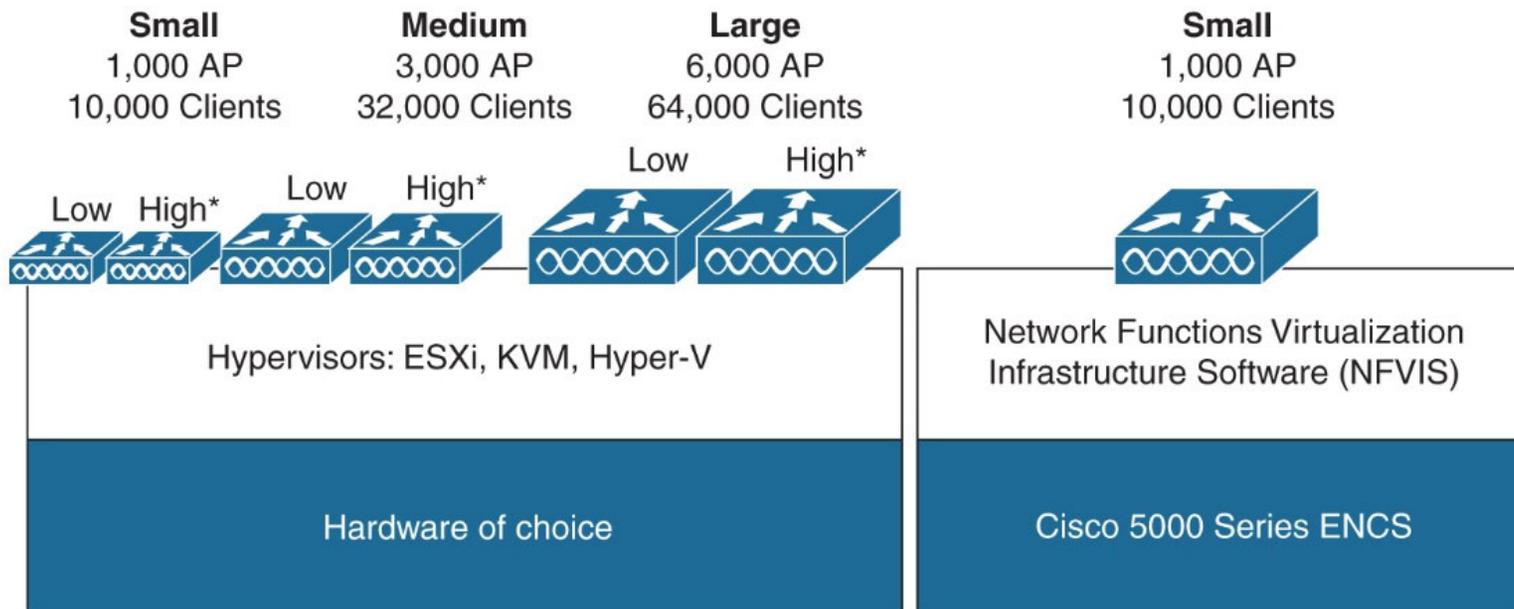


Figure 4-3 DHCP client ID setting on Mac



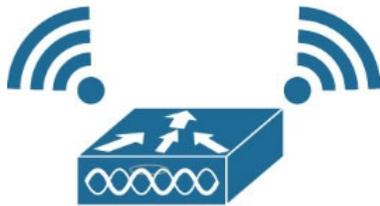
***High throughput only available with ESXi and KVM (note available with Hyper-V)**

Figure 4-4 Cisco Catalyst 9800-CL for private cloud

 Add port group - TrunkPort

Name	TrunkPort
VLAN ID	4095
Virtual switch	vSwitch0
▼ Security	
Promiscuous mode	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Inherit from vSwitch
MAC address changes	<input type="radio"/> Accept <input checked="" type="radio"/> Reject <input type="radio"/> Inherit from vSwitch
Forged transmits	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Inherit from vSwitch

Figure 4-5 Security settings on VMware port group



Runs Cisco IOS XE C9800 Wireless Controller on Catalyst Access Points	Modern OS, scalable, open and programmable, supports telemetry
Supports Advanced Enterprise Feature Set	High Availability, aWIPS, Umbrella, SMU, ClearAir, FRA
Easy to deploy and manage	Use mobile app or WebUI to deploy, manage, and monitor, Cisco DNA Center
Investment protection	Migrate Access Points to controller for more than 100 Access Points

Figure 4-6 Cisco EWC-AP characteristics

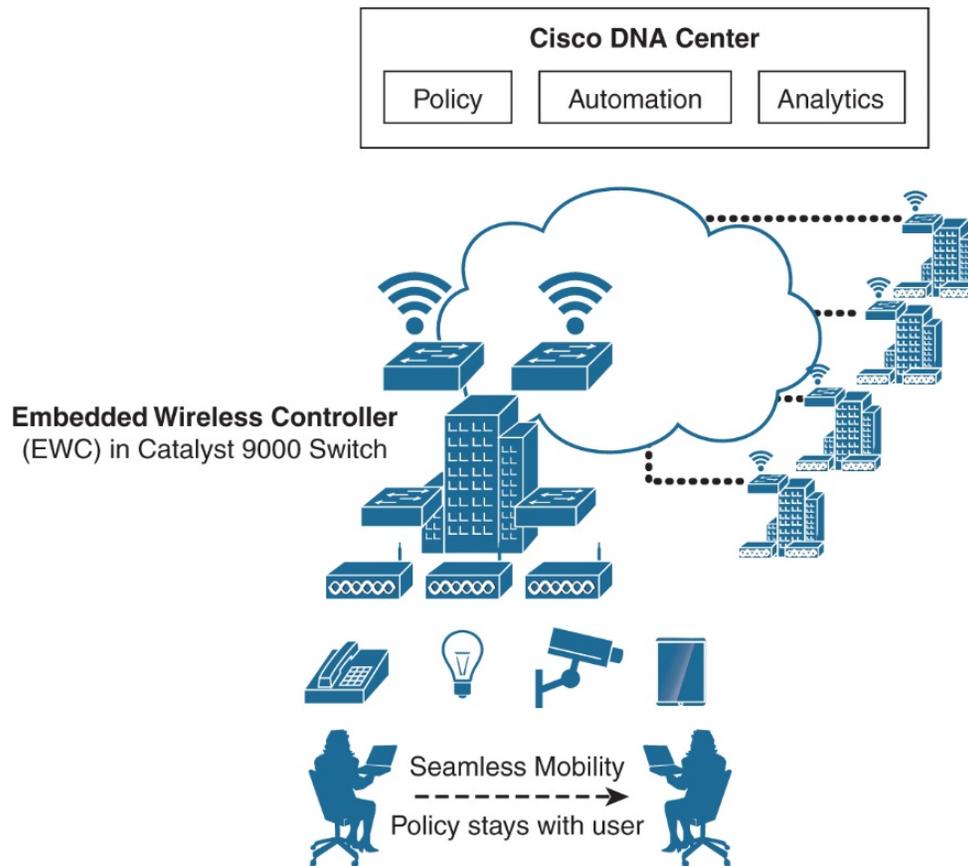


Figure 4-7 Cisco Embedded Wireless Controller (EWC) in Catalyst 9000 switches for SDA

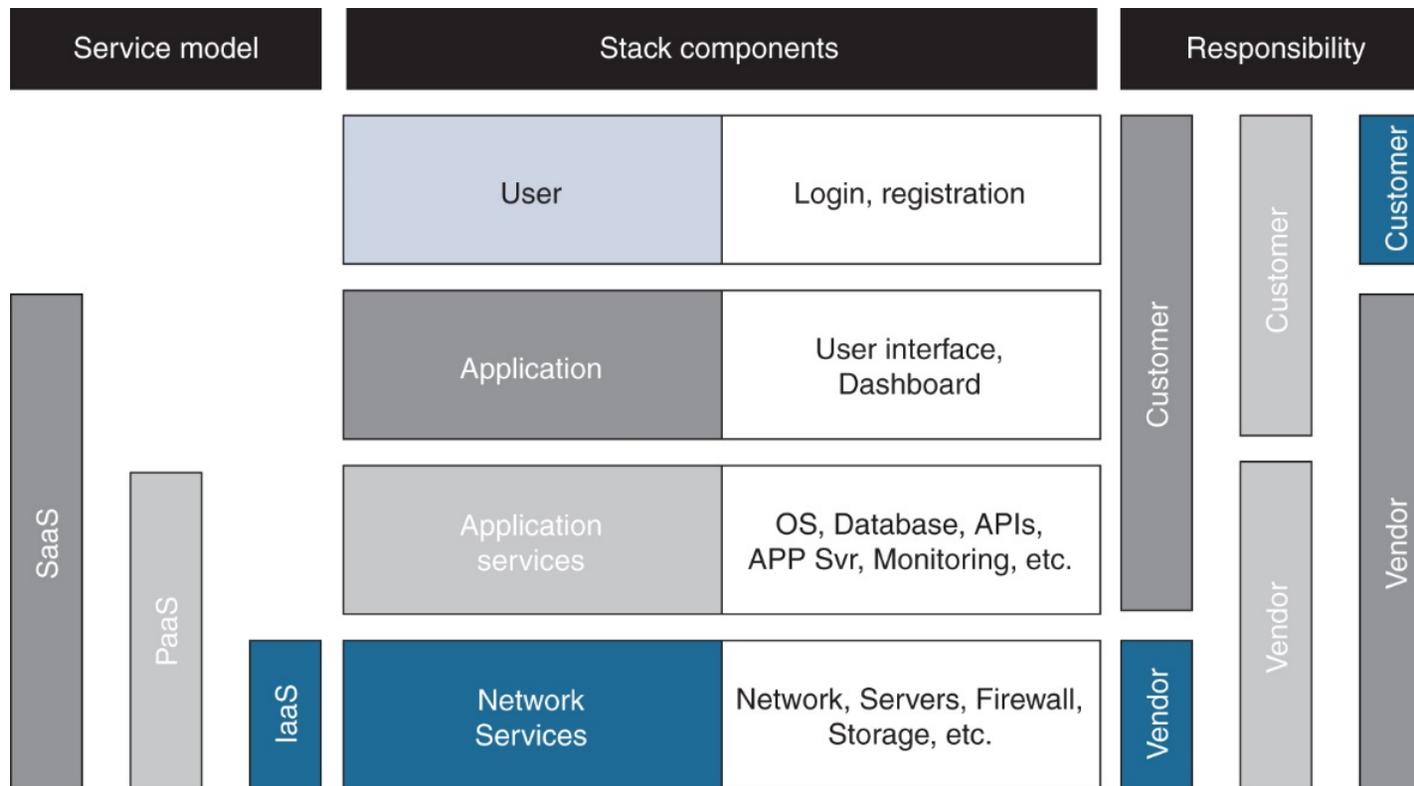


Figure 4-8 Public cloud service models

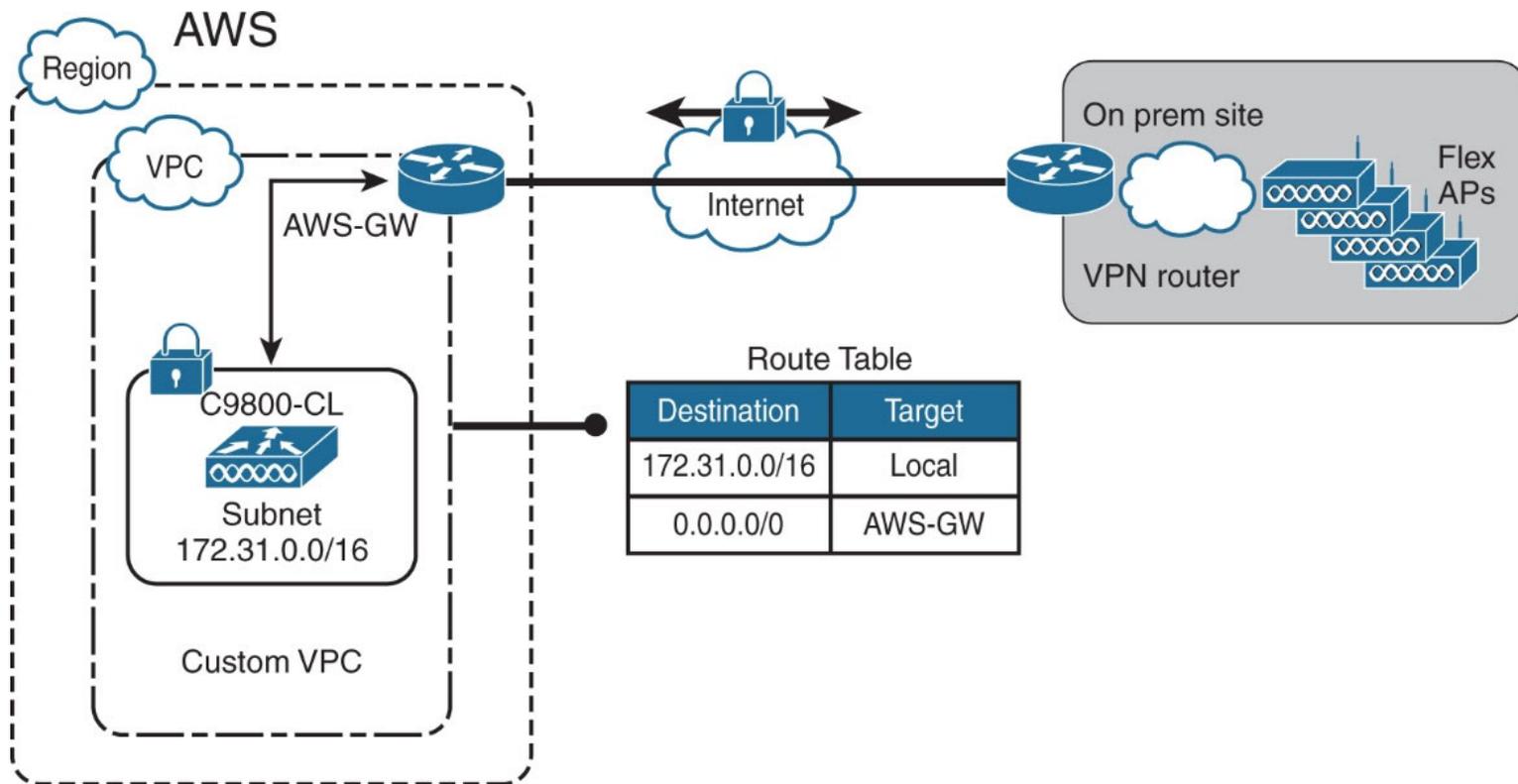


Figure 4-9 Managed VPN deployment mode on the public cloud

Configuration > Security > AAA Show Me How >

[+ AAA Wizard](#)

Servers / Groups AAA Method List **AAA Advanced**

Global Config	Authorize APs against MAC	<input type="checkbox"/> DISABLED
RADIUS Fallback	Authorize APs against Serial Number	<input checked="" type="checkbox"/> ENABLED ⓘ
Attribute List Name	Authorization Method List	default ▾
Device Authentication		

[AP Policy](#)

Password Policy

AAA Interface

Figure 4-10 Authorize APs against serial number

1. General Settings

Deployment Mode	<input type="text" value="Standalone"/>
Host Name*	<input type="text" value="WLC"/>
Country	<input type="text" value="US"/> +
Date	<input type="text" value="29 Sep 2021"/> 📅
Time / Timezone	<input type="text" value="12:11:03"/> ⌚ / <input type="text" value="Central"/>
NTP Servers	<input type="text" value="Enter NTP Server"/> +
	<i>Added NTP servers</i>
	<input type="text"/>
AAA Servers	<input type="text" value="Enter Radius Server IP"/> <input type="text" value="Enter Key"/> 👁️ +
	<i>Added AAA servers</i>
	<input type="text"/>

Figure 4-11 Day 0 Configuration Setup Wizard

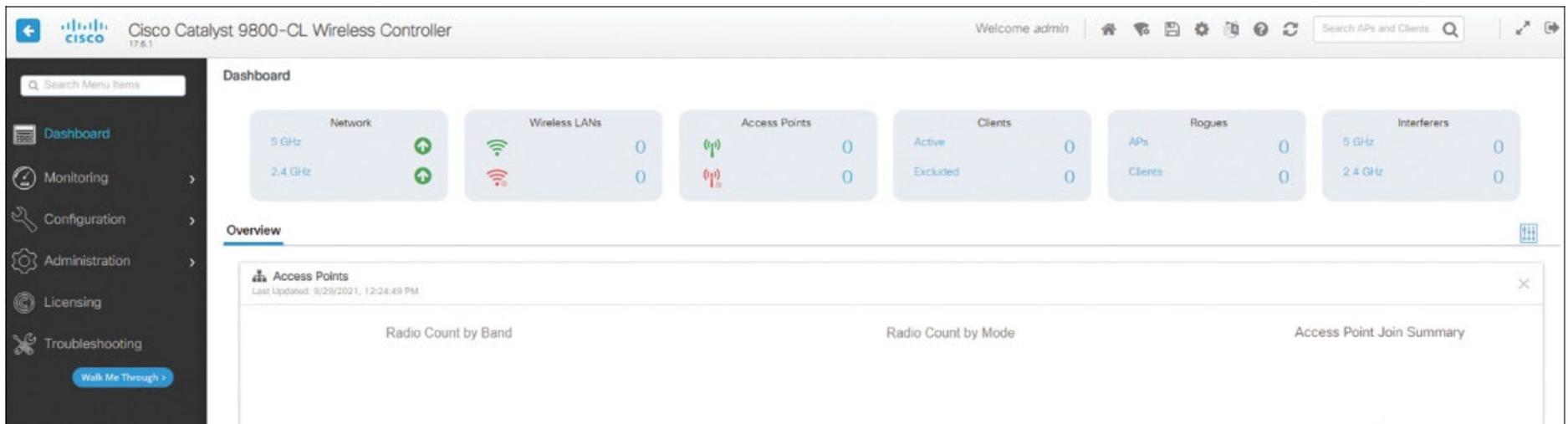


Figure 4-12 Catalyst 9800 wireless LAN controller main dashboard

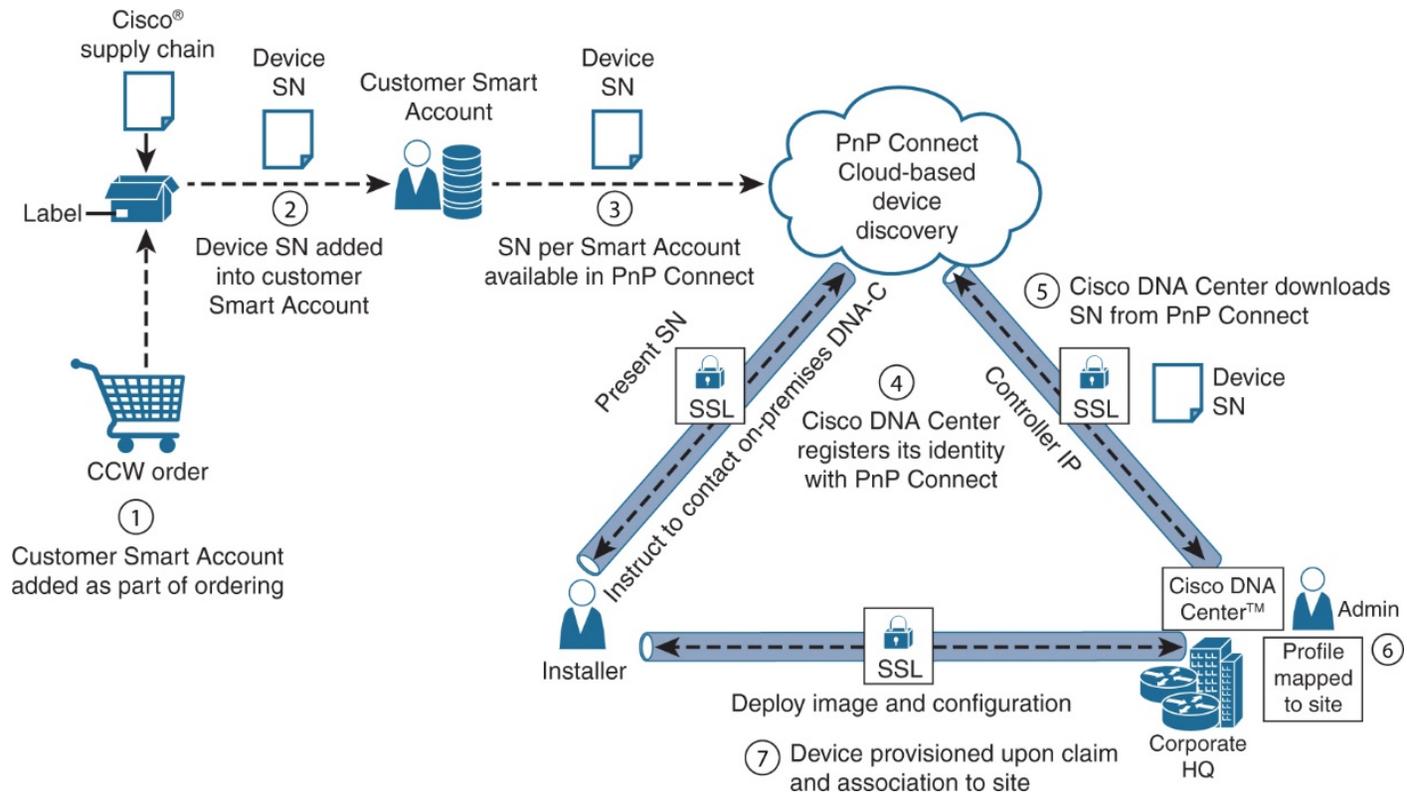


Figure 4-13 AP end-to-end onboarding process with PnP

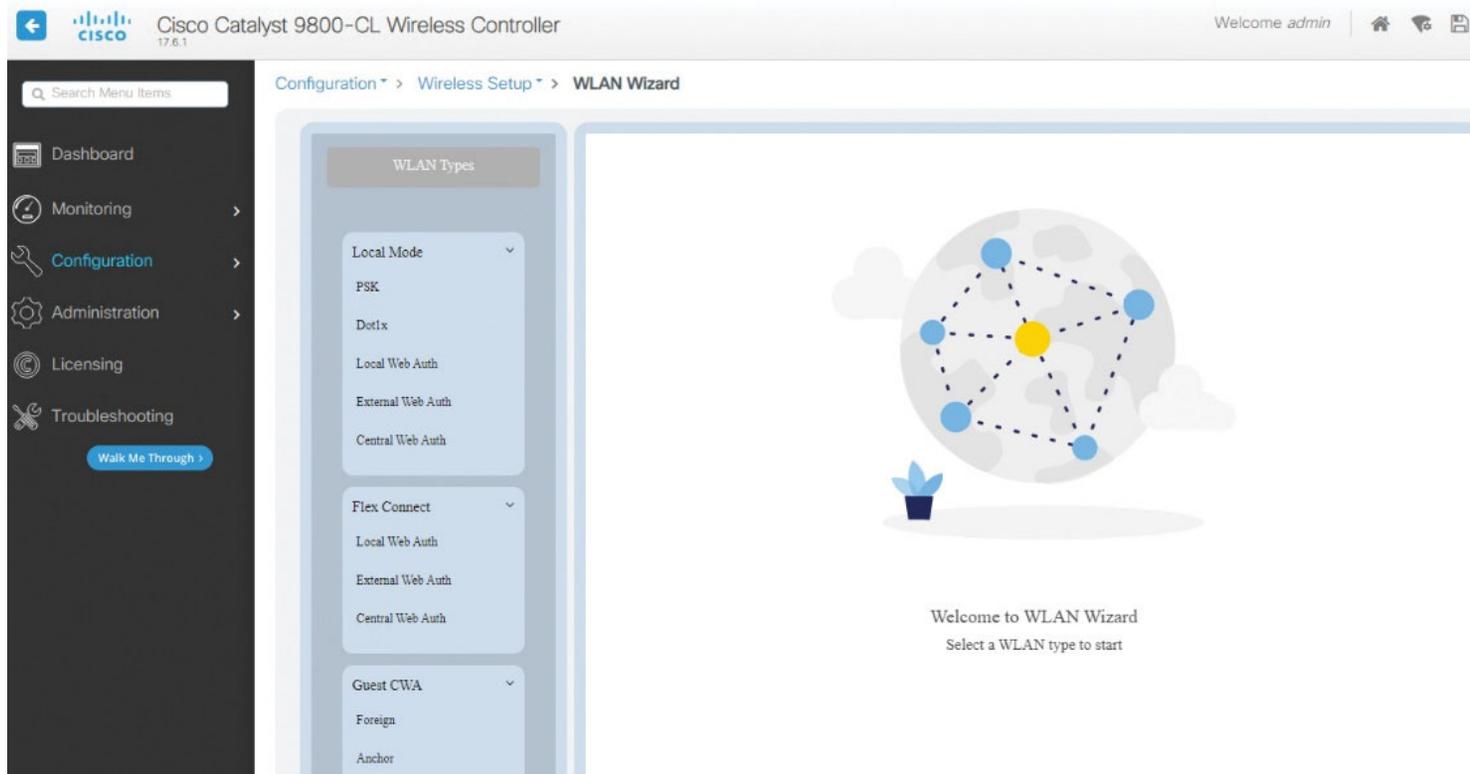


Figure 4-14 WLAN Wizard

Configuration > Wireless Setup > WLAN Wizard

Local Mode
PSK

WLAN

Tags

AP Provisioning

Network Name

Profile Name*

SSID*

WLAN ID*

Pre-Shared Key (PSK)

PSK Format

PSK Type

Pre-Shared Key*

WLAN Policy

Policy Profile Name

VLAN

CLI Preview

```
wireless profile policy mypolicy
shutdown
vlan VLAN0201
no shutdown

wlan LoveC9800 1 LoveC9800
security upa psk set-key ascii 0 *****
no security upa akm dot1x
security upa akm psk
no shutdown
```

Figure 4-15 WLAN Wizard, CLI preview

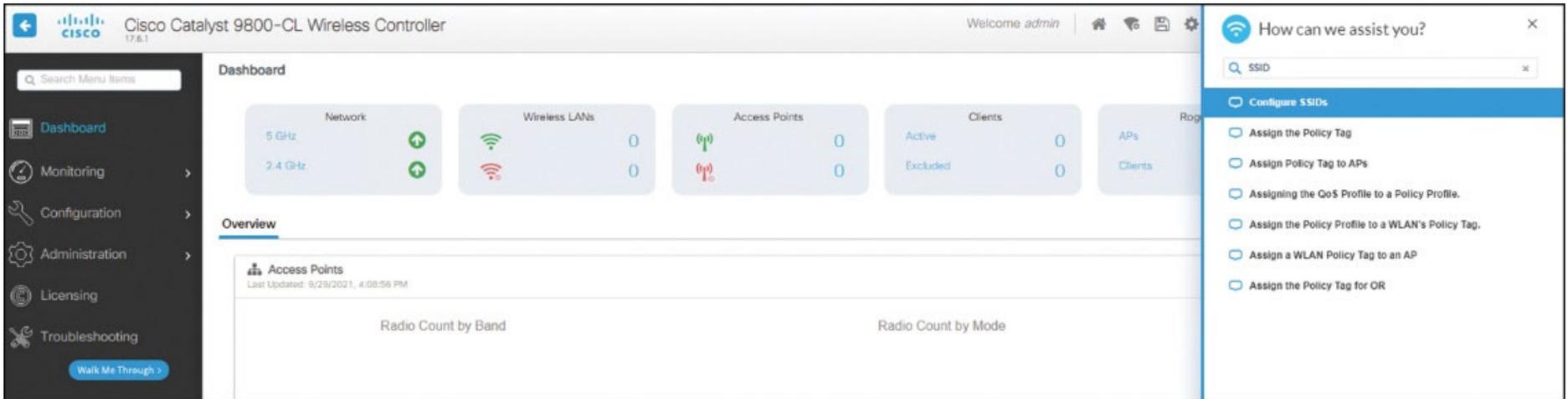


Figure 4-16 Walk Me configuration tool

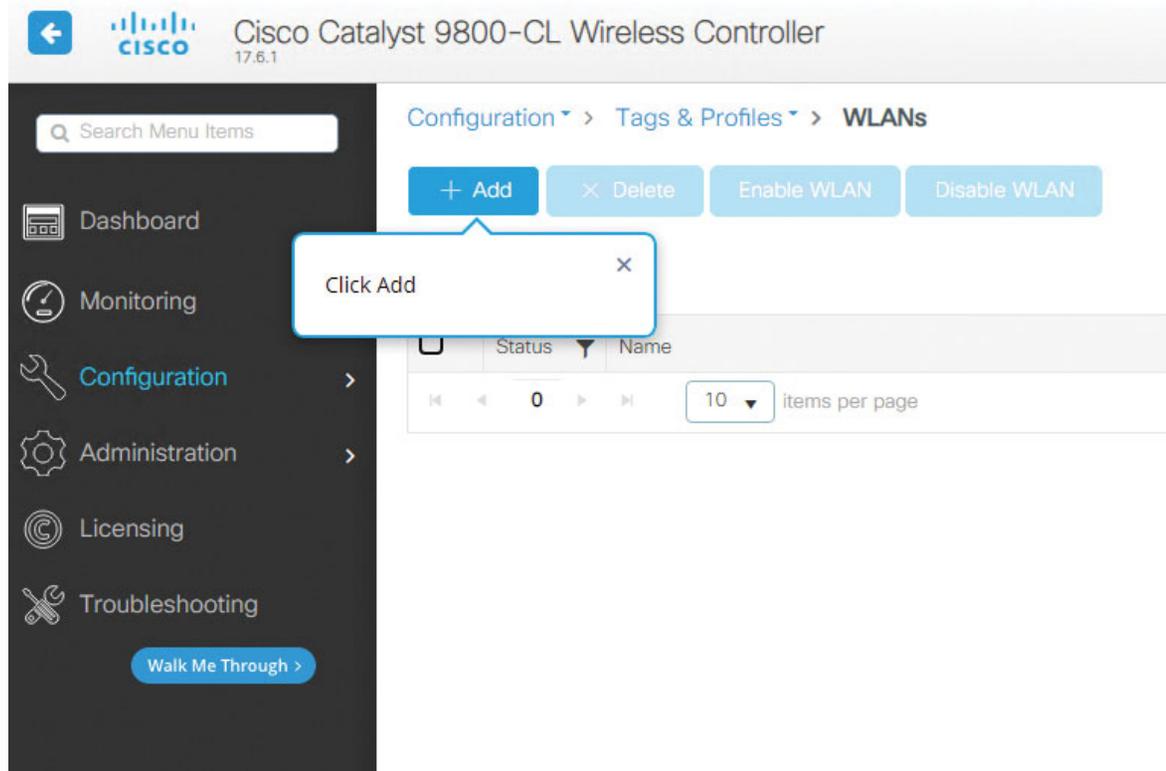


Figure 4-17 WLAN creation in Walk Me

Configuration > Security > ACL

+ Add - Delete Associate Interfaces

ACL Name	Type
<input type="checkbox"/> nicoflex	IPv4 Extended
<input type="checkbox"/> nicorole	IPv4 Role-based
<input type="checkbox"/> preauth_v4	IPv4 Extended
<input checked="" type="checkbox"/> testACL	IPv4 Extended
<input type="checkbox"/> implicit_deny_v6	IPv6
<input type="checkbox"/> implicit_permit_v6	IPv6
<input type="checkbox"/> preauth_v6	IPv6

10 items per page

Edit ACL

ACL Name* testACL ACL Type IPv4 Extended

Rules

Sequence* 1 Action permit

Source Type any

Destination Type Network

Destination IP* 192.168.1.0 Destination Wildcard* 0.0.0.255

Protocol tcp

Source Port eq Select Port* www((http)80)

Destination Port None

Log DSCP None

Save Cancel

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP
<input type="checkbox"/> 1	permit	any		192.168.1.0	0.0.0.255	tcp	eq www		None

10 items per page 1 - 1 of 1 item

Figure 5-1 Creating an ACL on the Catalyst 9800

Edit Policy Profile
✕

General
Access Policies
QOS and AVC
Mobility
Advanced

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification Disabled ⓘ

Local Subscriber Policy Name

VLAN

VLAN/VLAN Group

Multicast VLAN

WLAN ACL

IPv4 ACL

IPv6 ACL

URL Filters

Pre Auth

Post Auth

Figure 5-2 Access policies of the policy profile on the C9800

Edit WLAN ✕

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Advanced Add To Policy Tags

Layer2 **Layer3** AAA

Web Policy

Web Auth Parameter Map

Authentication List ⓘ

For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device

[<< Hide](#)

On Mac Filter Failure

Splash Web Redirect

Preauthentication ACL

IPv4

IPv6

Figure 5-3 Layer3 WLAN security settings where the preauthentication ACL can be configured

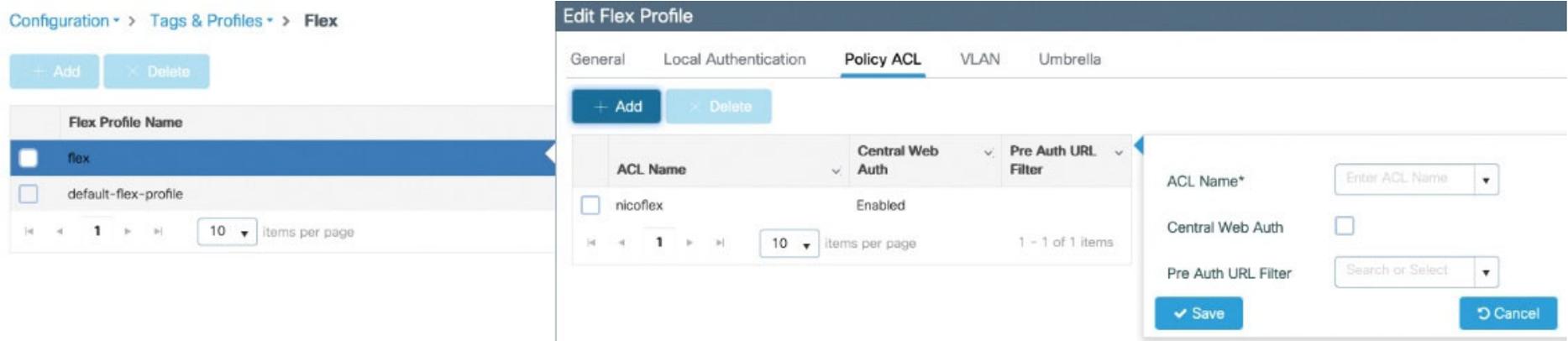


Figure 5-4 The Flex profile Policy ACL tab allows you to download ACLs to the APs

Edit Enhanced URL Filter

List Name*

	URL	Preference	Action	Validity	Invalidated URL
<input type="checkbox"/>	meraki.com	2	PERMIT	VALID	0
<input type="checkbox"/>	*.cisco.com	1	DENY	VALID	0

◀ ◁ **1** ▷ ▶ 10 items per page 1 - 2 of 2 items

Figure 5-5 URL filter configuration

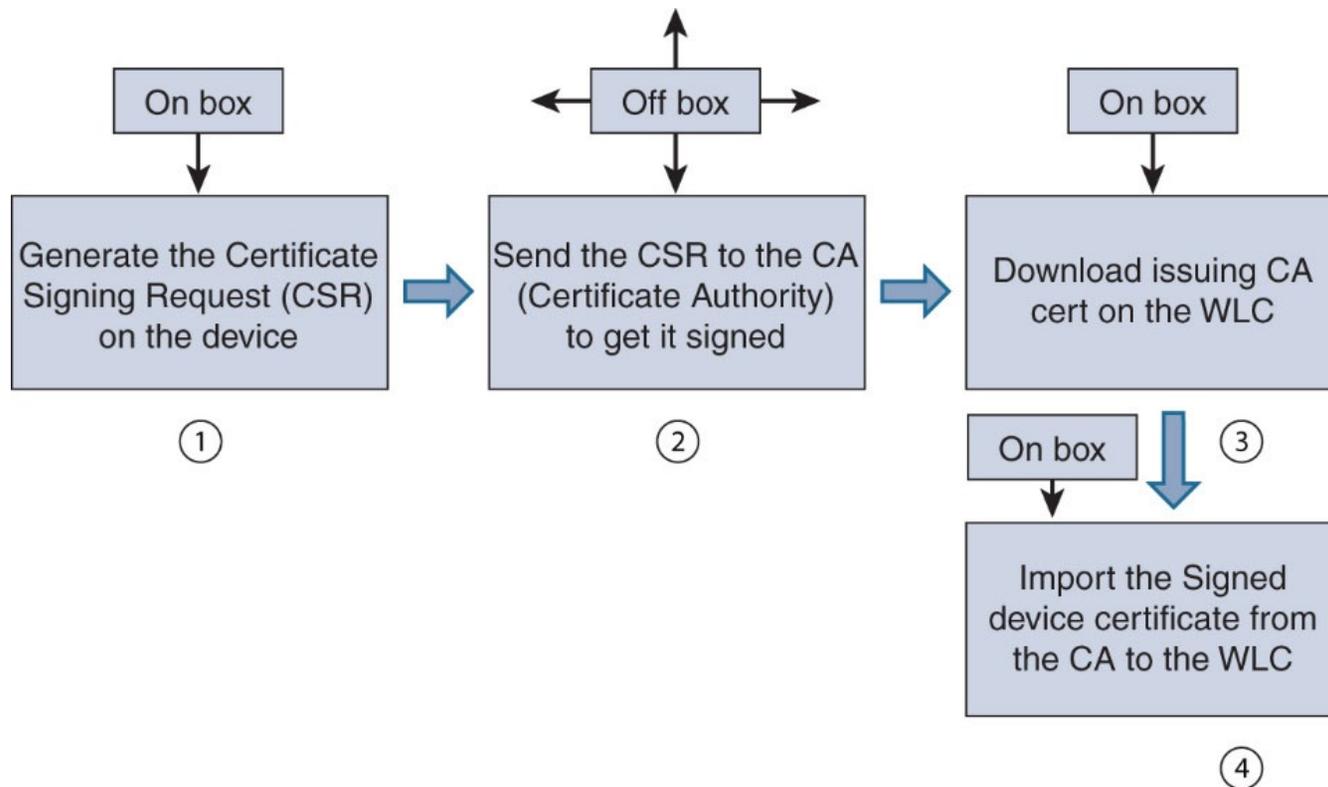


Figure 5-6 Adding a certificate by generating the question on the controller

Configuration > Security > PKI Management

Trustpoints CA Server **Key Pair Generation** Add Certificate

+ Add

Key Name	Key Type	Key Exportable	Zeroise Key
ssh-key	RSA	No	Zeroise
TP-self-signed-899645931	RSA	No	Zeroise
WLC_CA	RSA	No	Zeroise
vasa.p12	RSA	No	Zeroise
myc9800-CL_WLC_TP	RSA	Yes	Zeroise
paolokey	RSA	Yes	Zeroise
bigchain.pfx	RSA	No	Zeroise
SLA-KeyPair2	RSA	Yes	Zeroise
SLA-KeyPair	RSA	Yes	Zeroise
ssh-key.server	RSA	No	Zeroise

10 items per page 1 - 10 of 10 items

Key Name*

Key Type* RSA Key EC Key

Modulus Size*

Key Exportable*

Figure 5-7 Creating a key pair for use with a certificate

Configuration > Security > PKI Management

Trustpoints CA Server Key Pair Generation **Add Certificate**

Generate CSR

- Input certificate attributes and send generated CSR to CA

Authenticate Root CA

- Copy and paste the root certificate of CA received in .pem format that signed the CSR

Import Device Certificate

- Copy and paste the certificate signed by the CA

Import PKCS12 Certificate

- Signed certificate can be received in pkcs12 format from the CA
- Use this section to load the signed certificate directly

Generate Certificate Signing Request

Certificate Name*	<input type="text" value="Enter Certificate Name"/>	Key Name*	<input type="text" value="Search or Select"/> +
Country Code	<input type="text"/>	State	<input type="text"/>
Location	<input type="text"/>	Organizational Unit	<input type="text"/>
Organisation	<input type="text"/>	Domain Name	<input type="text"/>

Generate

Figure 5-8 Generate a certificate signing request from the WebUI

• **Generate CSR**

- Input certificate attributes and send generated CSR to CA

• **Authenticate Root CA**

- Copy and paste the root certificate of CA received in .pem format that signed the CSR

• **Import Device Certificate**

- Copy and paste the certificate signed by the CA

• **Import PKCS12 Certificate**

- Signed certificate can be received in pkcs12 format from the CA
- Use this section to load the signed certificate directly

> **Generate Certificate Signing Request**

▼ **Authenticate Root CA**

Trustpoint*

Search or Select ▼

Root CA Certificate (.pem)*

Authenticate

Figure 5-9 Authenticating the CA that issued your device certificate

- ⊗ **Generate CSR**
 - Input certificate attributes and send generated CSR to CA
- ⊗ **Authenticate Root CA**
 - Copy and paste the root certificate of CA received in .pem format that signed the CSR
- ⊗ **Import Device Certificate**
 - Copy and paste the certificate signed by the CA
- ⊗ **Import PKCS12 Certificate**
 - Signed certificate can be received in pkcs12 format from the CA
 - Use this section to load the signed certificate directly

> Generate Certificate Signing Request

> Authenticate Root CA

✓ **Import Device Certificate**

Trustpoint* ▼
Trustpoint label is required

Signed Certificate (.pem)*

Figure 5-10 Adding the device signed certificate received from the CA

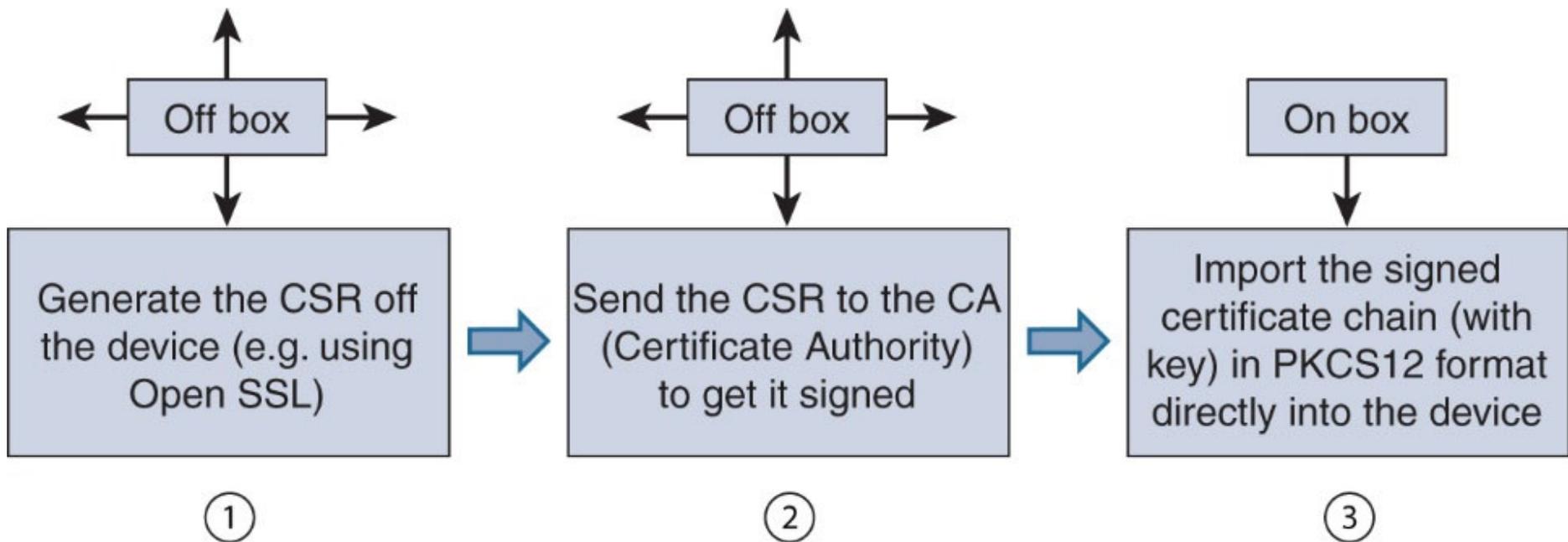


Figure 5-11 Adding a certificate when the private key was generated outside of the 9800

Configuration > Security > PKI Management

Trustpoints CA Server Key Pair Generation **Add Certificate**

Generate CSR

- Input certificate attributes and send generated CSR to CA

Authenticate Root CA

- Copy and paste the root certificate of CA received in .pem format that signed the CSR

Import Device Certificate

- Copy and paste the certificate signed by the CA

Import PKCS12 Certificate

- Signed certificate can be received in pkcs12 format from the CA
- Use this section to load the signed certificate directly

> Generate Certificate Signing Request

> Authenticate Root CA

> Import Device Certificate

▼ Import PKCS12 Certificate

Transport Type

Desktop (HTTPS) ▼

Source File Path*

Select File

Certificate Password*

Import

Figure 5-12 Adding a certificate chain in PKCS12 format to the WLC

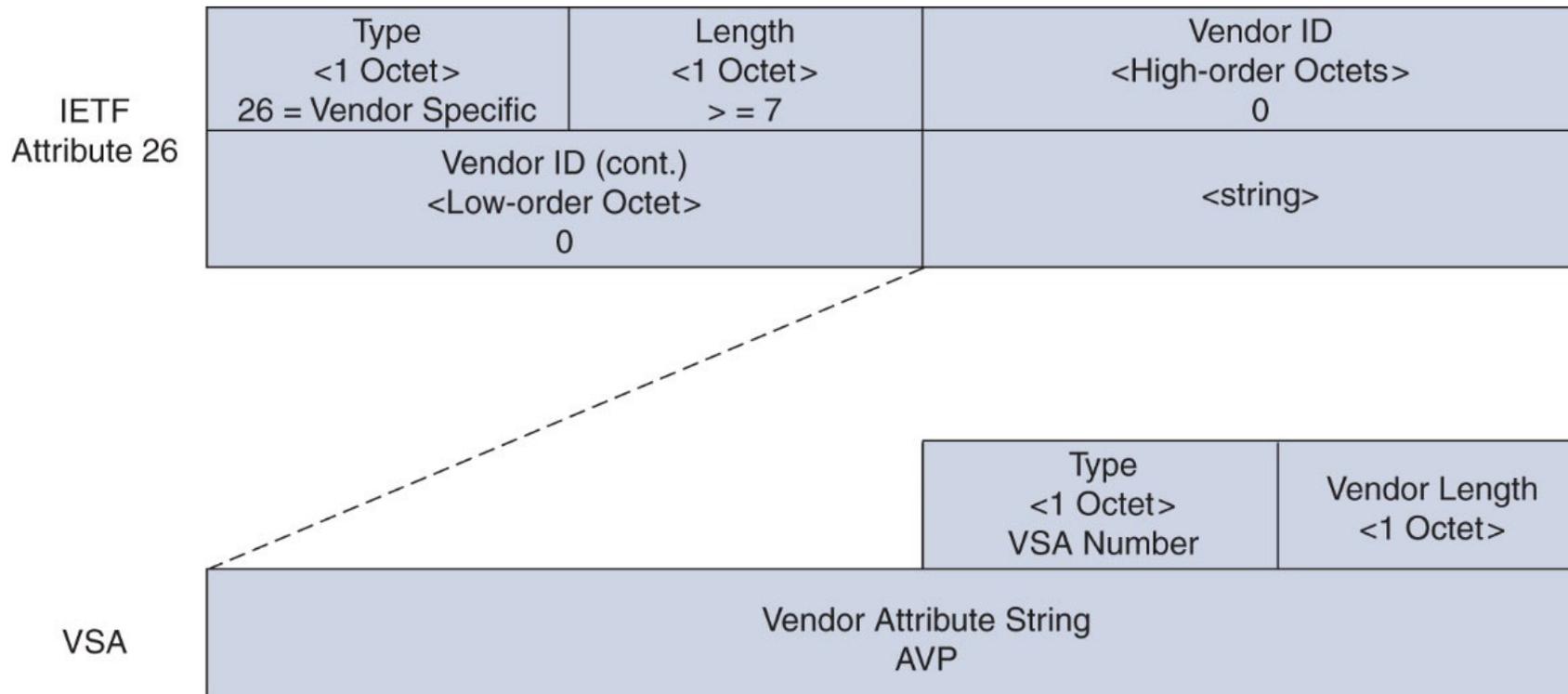


Figure 5-13 RADIUS AV-pair format

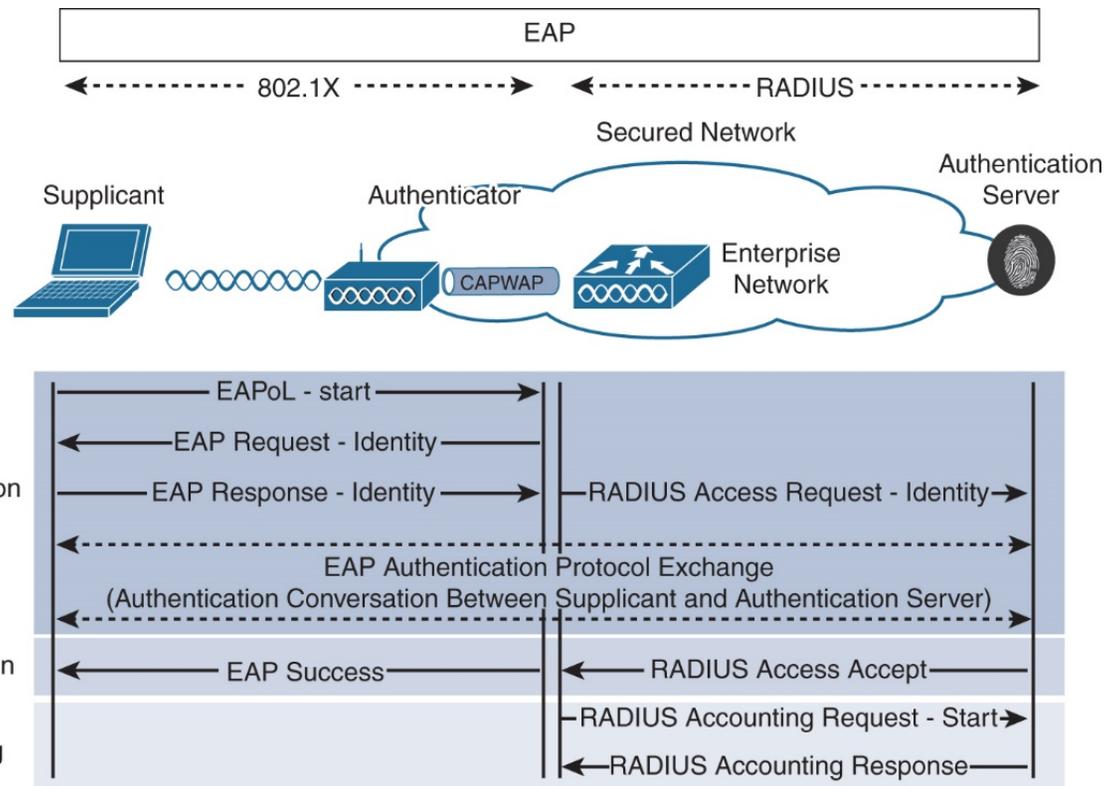


Figure 5-14 Workflow of an EAP authentication between a supplicant and authentication server

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups **Create AAA Radius Server**

+ Add

RADIUS

TACACS+

LDAP

Name*	<input type="text"/>
Server Address*	<input type="text" value="IPv4/IPv6/Hostname"/>
PAC Key	<input type="checkbox"/>
Key Type	Clear Text ▼
Key* ⓘ	<input type="text"/>
Confirm Key*	<input type="text"/>
Auth Port	<input type="text" value="1812"/>
Acct Port	<input type="text" value="1813"/>
Server Timeout (seconds)	<input type="text" value="1-1000"/>
Retry Count	<input type="text" value="0-100"/>
Support for CoA	ENABLED <input checked="" type="checkbox"/>

Figure 5-15 RADIUS server creation on the C9800 WebUI

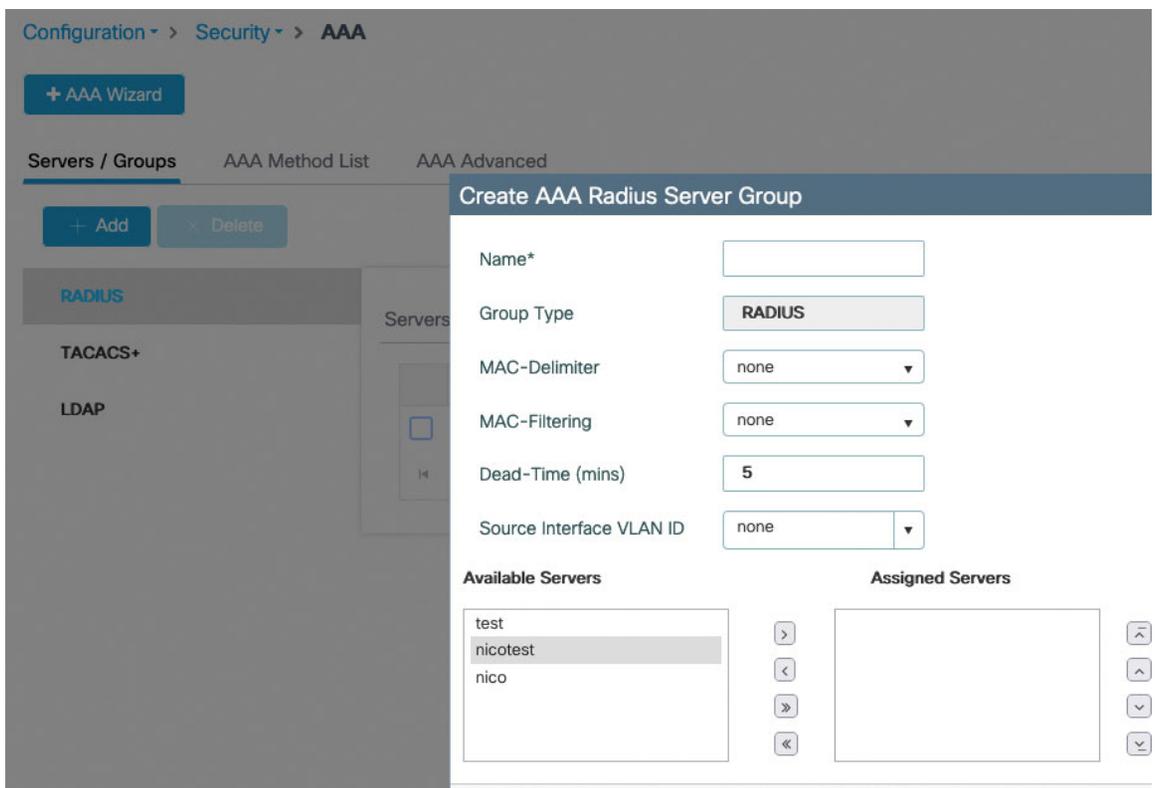


Figure 5-16 RADIUS server group configuration

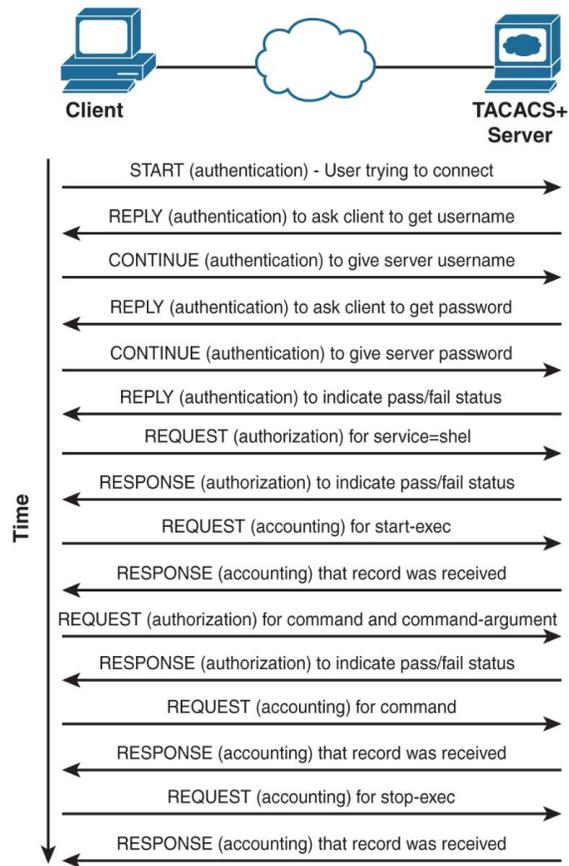


Figure 5-17 TACACS workflow

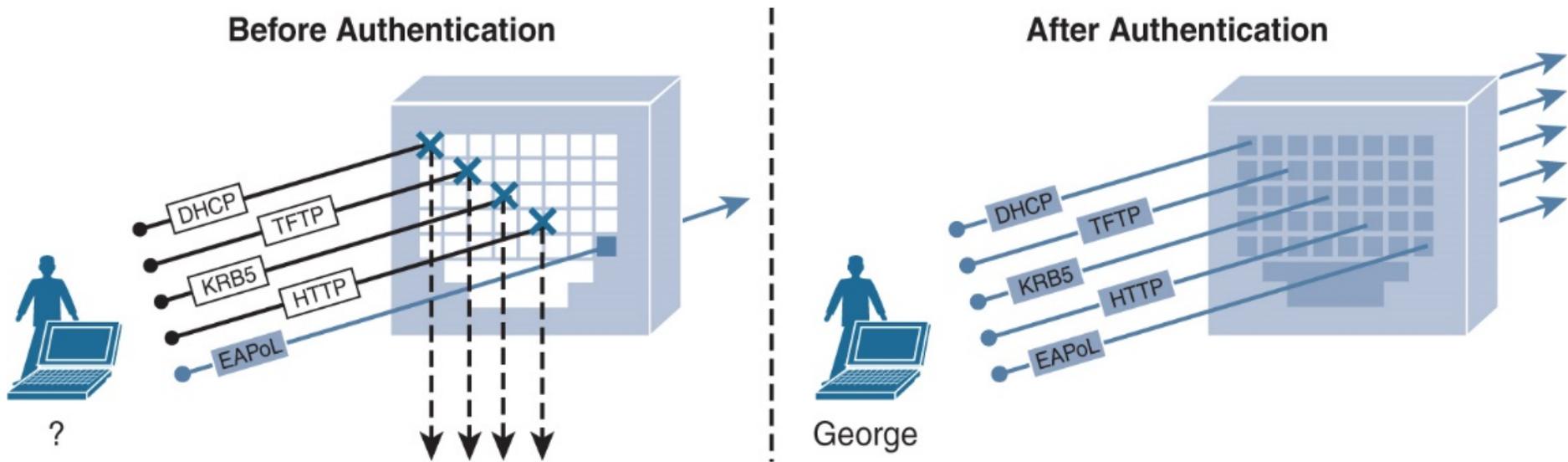


Figure 5-18 802.1X port-based authentication system

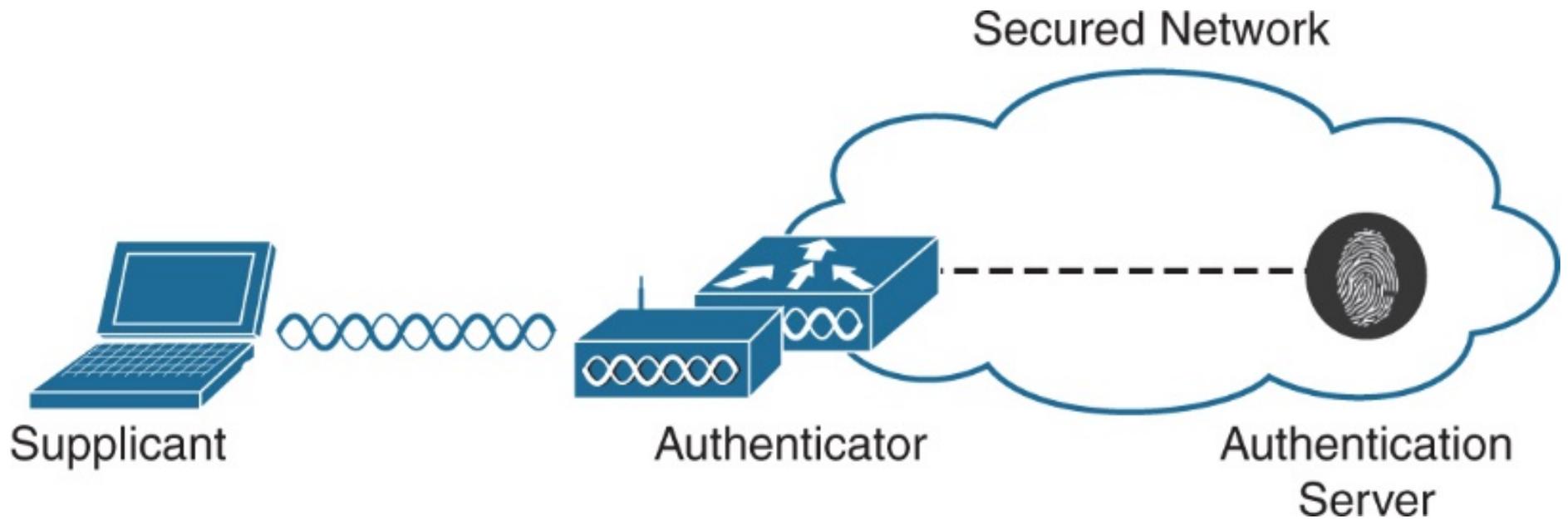


Figure 5-19 802.1X components

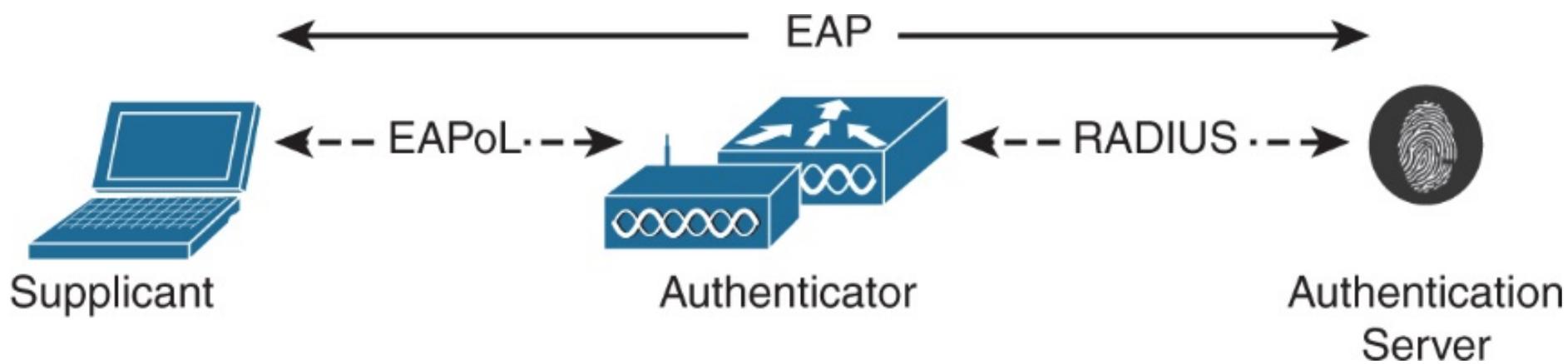


Figure 5-20 EAP authentication workflow

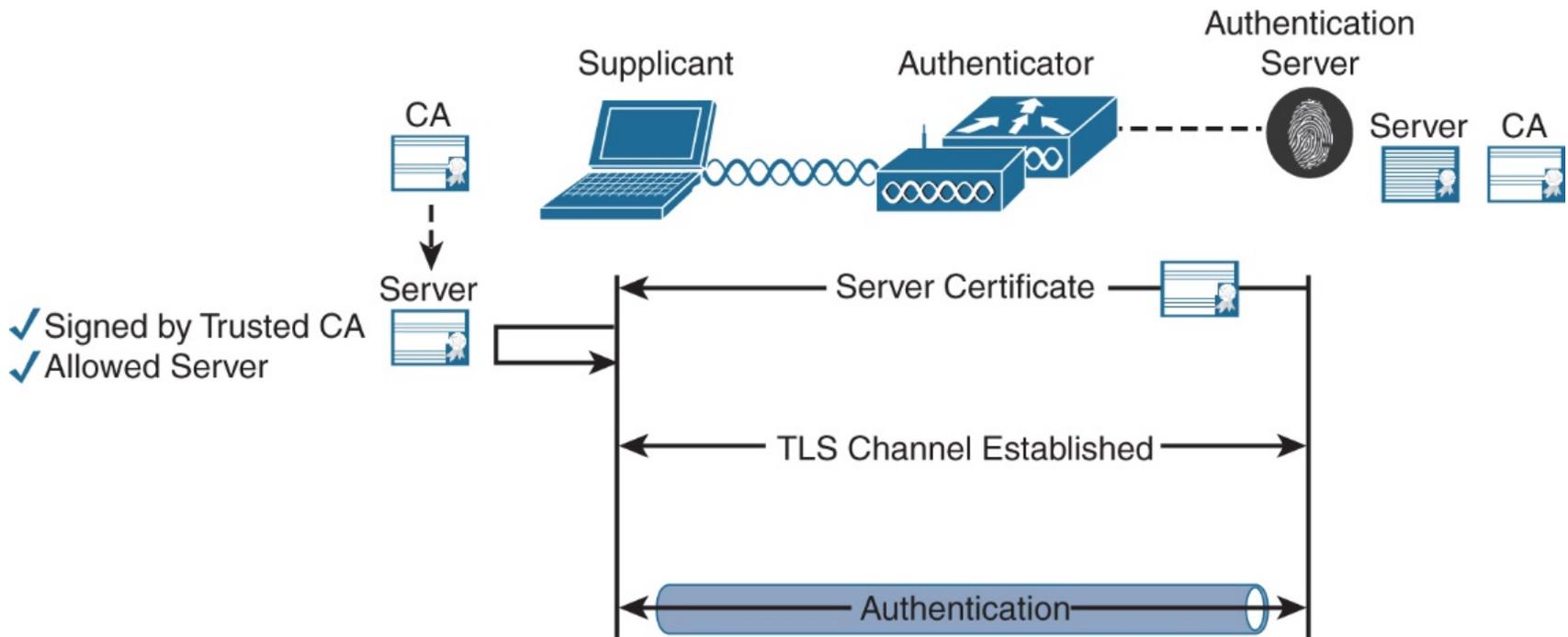


Figure 5-21 PEAP authentication high-level workflow

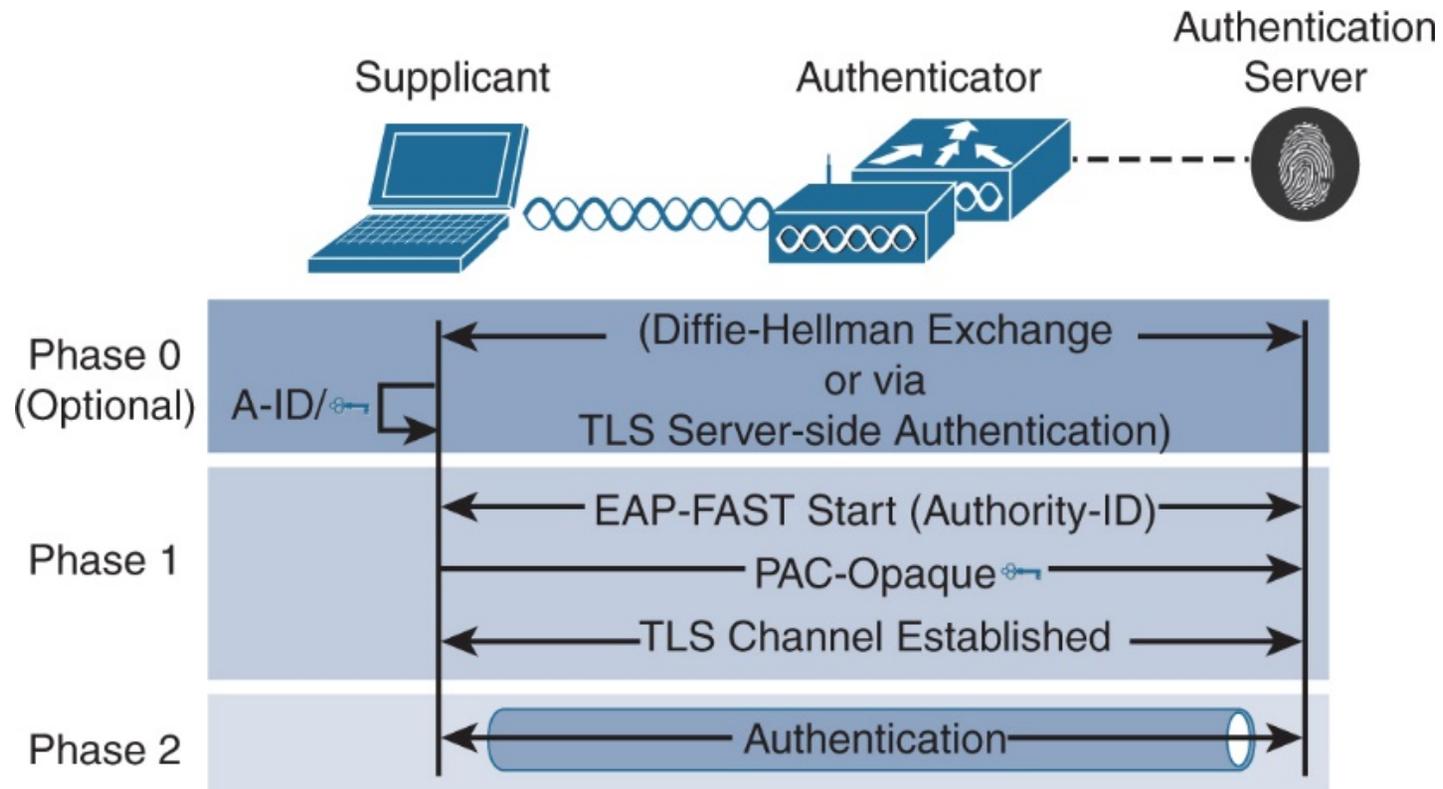


Figure 5-22 EAP-FAST high-level overview

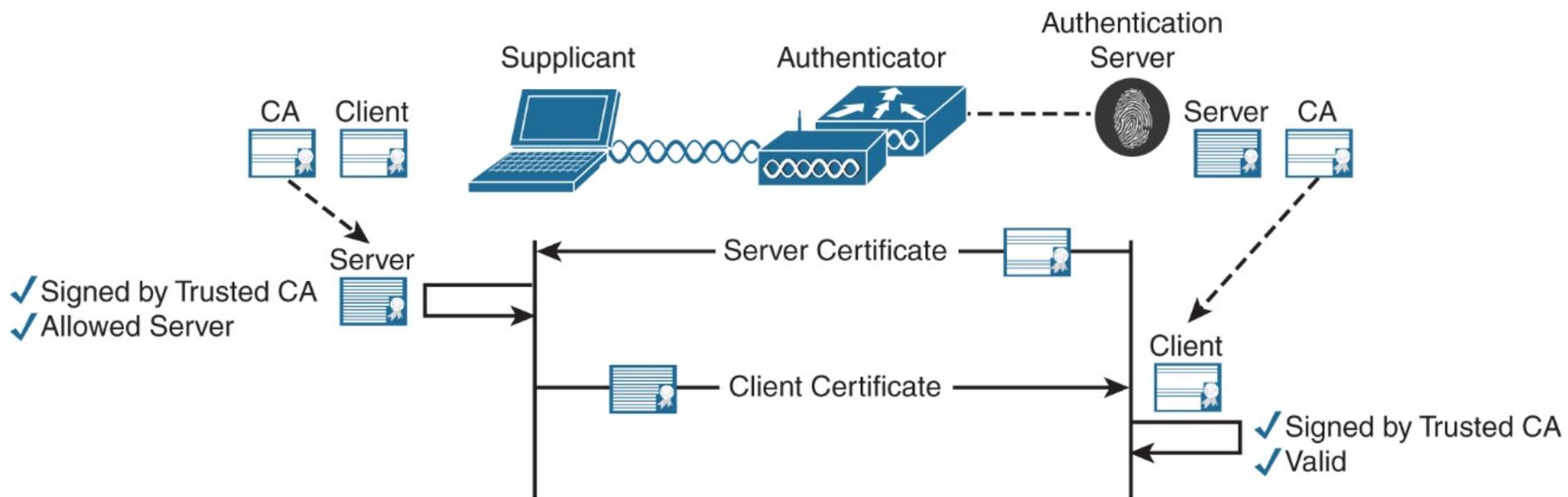


Figure 5-23 EAP-TLS high-level overview

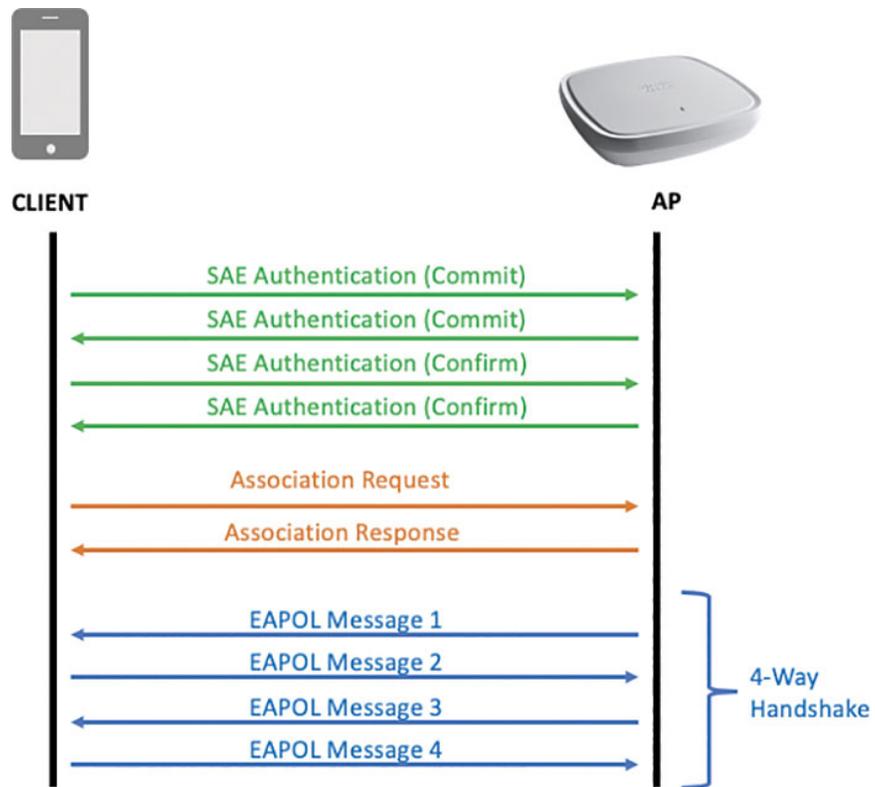


Figure 5-24 WPA3 SAE workflow

✕
Add WLAN

WPA Parameters

WPA Policy

WPA2 Policy

GTK Randomize

OSEN Policy

WPA2 Encryption AES(CCMP128)

MPSK

+
🗑️

	Priority	Key Format	Password Type
<input type="checkbox"/>	1	ASCII	Unencrypted

Auth Key Mg

Priority *

Key Format

Password Type

↶ Cancel

📄 Apply to Device

Figure 5-25 MPSK configuration in WLAN settings

Add WLAN
✕

General
Security
Advanced

Layer2
Layer3
AAA

Layer 2 Security Mode WPA + WPA2 ▼

MAC Filtering

Protected Management Frame

PMF Disabled ▼

WPA Parameters

WPA Policy

Lobby Admin Access

Fast Transition Disabled ▼

Over the DS

Reassociation Timeout 20

MPSK Configuration

MPSK

↶ Cancel

📄 Apply to Device

Figure 5-26 WPA 2 PSK SSID settings

Add WLAN ✕

WPA Policy	<input type="checkbox"/>
WPA2 Policy	<input checked="" type="checkbox"/>
GTK Randomize	<input type="checkbox"/>
OSEN Policy	<input type="checkbox"/>
WPA2 Encryption	<input checked="" type="checkbox"/> AES(CCMP128) <input type="checkbox"/> CCMP256 <input type="checkbox"/> GCMP128 <input type="checkbox"/> GCMP256
Auth Key Mgmt	<input type="checkbox"/> 802.1x <input checked="" type="checkbox"/> PSK <input type="checkbox"/> Easy-PSK

Figure 5-27 WPA2 PSK Layer2 security settings

PSK Format	ASCII ▼
PSK Type	Unencrypted ▼
Pre-Shared Key* 

Figure 5-28 WPA2 PSK SSID key configuration

```

▼ Tag: RSN Information
  Tag Number: RSN Information (48)
  Tag length: 20
  RSN Version: 1
  ▼ Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
    Group Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
    Group Cipher Suite type: AES (CCM) (4)
    Pairwise Cipher Suite Count: 1
  ▼ Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
    ► Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
    Auth Key Management (AKM) Suite Count: 1
  ▼ Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK
    ► Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) PSK
    ► RSN Capabilities: 0x0028

```

Figure 5-29 RSN information element of a beacon frame of a WPA PSK SSID

Add WLAN ✕

General
Security
Advanced

Layer2
Layer3
AAA

Layer 2 Security Mode	<input type="text" value="WPA3"/>	Lobby Admin Access	<input type="checkbox"/>
MAC Filtering	<input type="checkbox"/>	Fast Transition	<input type="text" value="Disabled"/>
Protected Management Frame		Over the DS	<input type="checkbox"/>
PMF	<input type="text" value="Required"/>	Reassociation Timeout	<input type="text" value="20"/>
Association Comeback Timer*	<input type="text" value="1"/>		
SA Query Time*	<input type="text" value="200"/>		

↶ Cancel

📄 Apply to Device

Figure 5-30 SAE WLAN example configuration

WPA3 Policy	<input checked="" type="checkbox"/>
WPA2/WPA3 Encryption	<input checked="" type="checkbox"/> AES(CCMP128)
	<input type="checkbox"/> CCMP256
	<input type="checkbox"/> GCMP128
	<input type="checkbox"/> GCMP256
Auth Key Mgmt	<input type="checkbox"/> 802.1x
	<input type="checkbox"/> CCKM
	<input checked="" type="checkbox"/> SAE
	<input type="checkbox"/> OWE
	<input type="checkbox"/> FT + 802.1x
	<input type="checkbox"/> 802.1x-SHA256

Figure 5-31 Ciphers option example for SAE

Anti Clogging Threshold*	<input type="text" value="1500"/>
Max Retries*	<input type="text" value="5"/>
Retransmit Timeout*	<input type="text" value="400"/>
PSK Format	<input type="text" value="ASCII"/> ▼
PSK Type	<input type="text" value="Unencrypted"/> ▼
Pre-Shared Key*	<input type="text" value="..... "/> 

Figure 5-32 PSK configuration for SAE

```

▼ Tag: RSN Information
  Tag Number: RSN Information (48)
  Tag length: 26
  RSN Version: 1
  ▼ Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
    Group Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
    Group Cipher Suite type: AES (CCM) (4)
    Pairwise Cipher Suite Count: 1
  ▼ Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
    ► Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
    Auth Key Management (AKM) Suite Count: 1
  ▼ Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) SAE (SHA256)
    ► Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) SAE (SHA256)
    ► RSN Capabilities: 0x00e8
    PMKID Count: 0
    PMKID List
  ▼ Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (128)
    Group Management Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
    Group Management Cipher Suite type: BIP (128) (6)

```

Figure 5-33 SAE advertised in the SSID beacon RSN IE

[General](#)
[Security](#)
[Advanced](#)
[Add To Policy Tags](#)

[Layer2](#)
[Layer3](#)
[AAA](#)

Layer 2 Security Mode WPA + WPA2 ▼

MAC Filtering

Authorization List* ISEautz ▼ ⓘ

Protected Management Frame

PMF Disabled ▼

Lobby Admin Access

Fast Transition Disabled ▼

Over the DS

Reassociation Timeout 20

MPSK Configuration

MPSK

Figure 5-34 iPSK SSID security settings part 1

WPA2 Encryption	<input checked="" type="checkbox"/> AES(CCMP128) <input type="checkbox"/> CCMP256 <input type="checkbox"/> GCMP128 <input type="checkbox"/> GCMP256
Auth Key Mgmt	<input type="checkbox"/> 802.1x <input checked="" type="checkbox"/> PSK <input type="checkbox"/> Easy-PSK <input type="checkbox"/> CCKM <input type="checkbox"/> FT + 802.1x <input type="checkbox"/> FT + PSK <input type="checkbox"/> 802.1x-SHA256 <input type="checkbox"/> PSK-SHA256
PSK Format	ASCII ▾
PSK Type	Unencrypted ▾
Pre-Shared Key*

Figure 5-35 iPSK SSID security settings part 2

✓	Specificdevice - PSKCisco123	 Radius·Calling-Station-ID EQUALS E8-7F-95-53-20-12	PSK-Cisco123 ×
✓	Specificarea-PSKIoT	 Radius·Called-Station-ID CONTAINS FactoryArea	PSKWireless123 ×

Figure 5-36 ISE authorization policies for IPSK

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List **AAA Advanced**

Global Config	Local Authentication	None
RADIUS Fallback	Local Authorization	None
Attribute List Name	Radius Server Load Balance	<input checked="" type="checkbox"/> DISABLED
Device Authentication	Interim Update	<input type="checkbox"/>
AP Policy	<< Hide	
Password Policy	Radius Attributes	
AAA Interface	Accounting	Authentication
	Called-station-id	ap-macaddress-s...
	Called-station-id case	ap-ethmac-only
	MAC-Delimiter	ap-ethmac-ssid
	Username Case	ap-group-name
	Username Delimiter	ap-label-address
		ap-label-address-ssid
		ap-location
		ap-macaddress
		ap-macaddress-ssid

Figure 5-37 Customization of the called-station-id RADIUS field

Advanced Attributes Settings

⋮	Cisco:cisco-av-pair	▼	=	psk=Wireless123	▼	-
⋮	Cisco:cisco-av-pair	▼	=	psk-mode=ascii	▼	- +

Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = psk=Wireless123
cisco-av-pair = psk-mode=ascii

Figure 5-38 ISE authorization result

<input type="checkbox"/>		EnhancedOpen	 3	EnhancedOpen	[WPA3][OWE][AES]
<input type="checkbox"/>		Open	 4	Open	[open]

Figure 5-39 A pair of Open/Enhanced Open SSIDs for Enhanced Open Transition mode

General

Security

Advanced

Add To Policy Tags

Profile Name*

EnhancedOpen

SSID*

EnhancedOpen

WLAN ID*

3

Status

ENABLED

Broadcast SSID

DISABLED

Radio Policy ⓘ

[Show slot configuration](#)

5 GHz

ENABLED

2.4 GHz

ENABLED

802.11b/g Policy
(2.4 GHz)

802.11b/g ▼

Figure 5-40 Enhanced Open SSID general settings

General **Security** Advanced Add To Policy Tags

Layer2 Layer3 AAA

Layer 2 Security Mode

MAC Filtering

Protected Management Frame

PMF

Association Comeback Timer*

SA Query Time*

Figure 5-41 Enhanced Open security settings part 1

WPA3 Policy	<input checked="" type="checkbox"/>
WPA2/WPA3 Encryption	<input checked="" type="checkbox"/> AES(CCMP128) <input type="checkbox"/> CCMP256 <input type="checkbox"/> GCMP128 <input type="checkbox"/> GCMP256
Auth Key Mgmt	<input type="checkbox"/> 802.1x <input type="checkbox"/> CCKM <input type="checkbox"/> SAE <input checked="" type="checkbox"/> OWE <input type="checkbox"/> FT + 802.1x <input type="checkbox"/> 802.1x-SHA256
Transition Mode WLAN ID	<input type="text" value="4"/>

Figure 5-42 Enhanced Open SSID security settings part 2

General		Security	Advanced	Add To Policy Tags
Layer2		Layer3	AAA	
Layer 2 Security Mode	None ▼		Lobby Admin Access	<input type="checkbox"/>
MAC Filtering	<input type="checkbox"/>		Fast Transition	Disabled ▼
OWE Transition Mode	<input checked="" type="checkbox"/>		Over the DS	<input type="checkbox"/>
Transition Mode WLAN ID*	3		Reassociation Timeout	20

Figure 5-43 Regular open SSID linked with transition mode to an Enhanced Open SSID

WLAN Profile Name	EnhancedOpen
Wireless LAN Network Name (SSID)	EnhancedOpen
Client Entry Create Time	21 seconds
Policy Type	WPA3
Encryption Cipher	CCMP (AES)
Authentication Key Management	OWE

Figure 5-44 Security details of a client connected to an Enhanced Open SSID

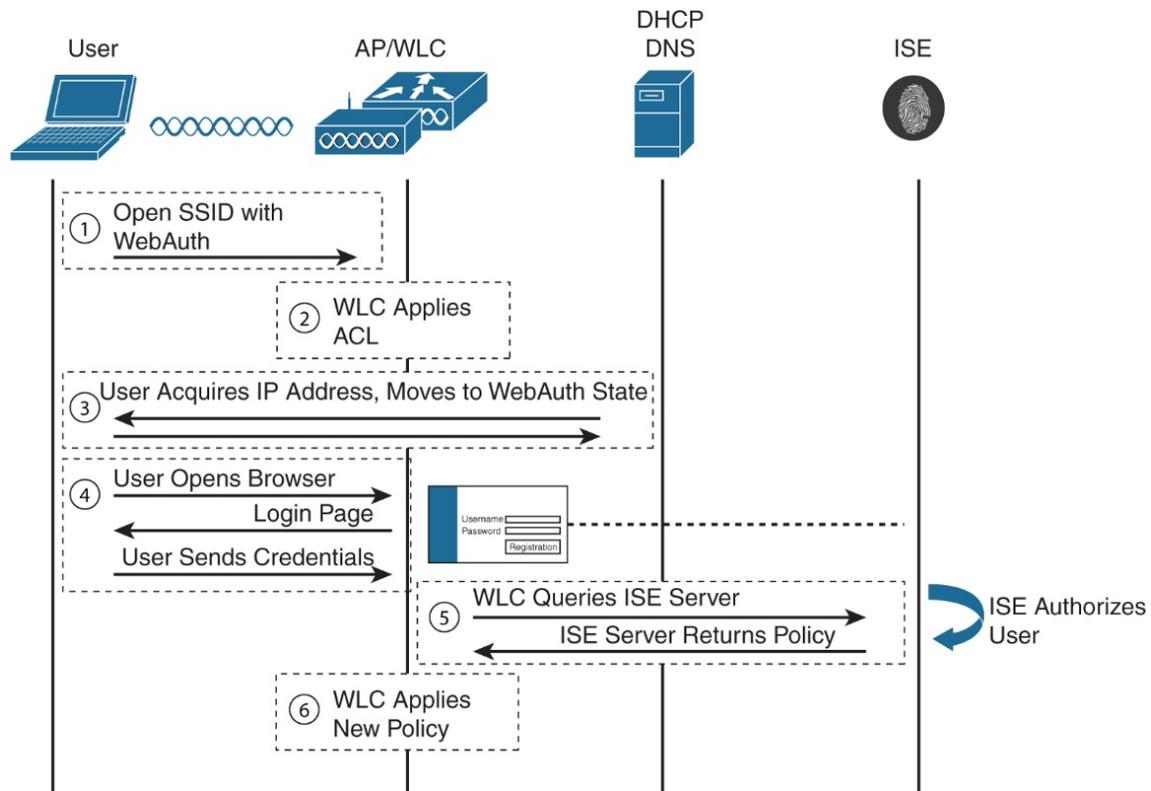


Figure 5-45 Local web authentication workflow

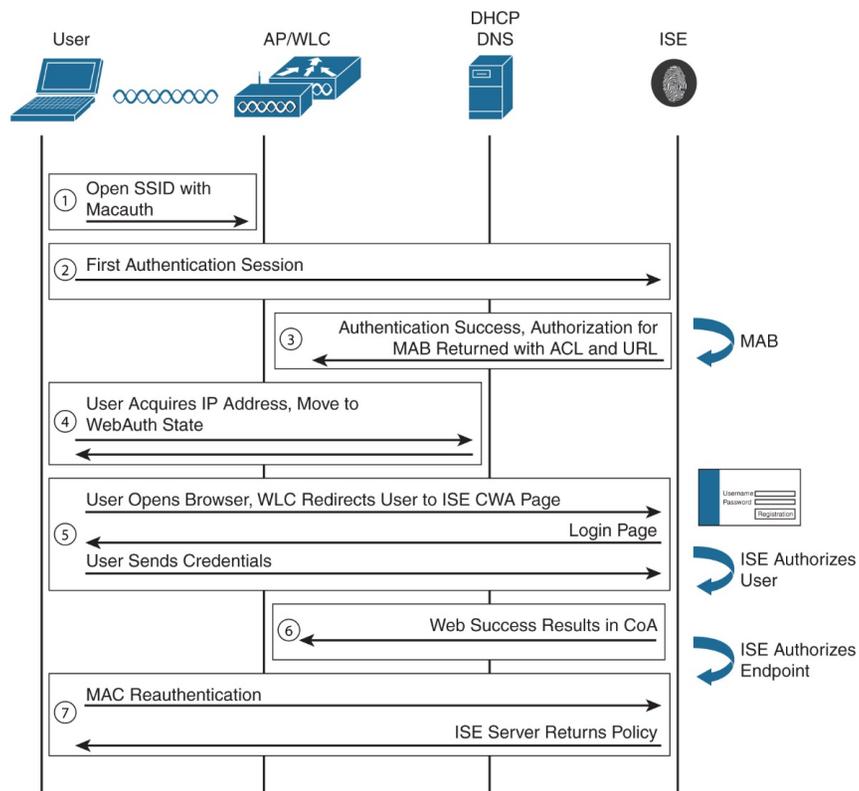


Figure 5-46 Central Web Authentication workflow

Edit Web Auth Parameter

General Advanced

Parameter-map name

Banner Type None Banner Text Banner Title File Name

Maximum HTTP connections

Init-State Timeout(secs)

Type

Virtual IPv4 Address

Trustpoint

Virtual IPv4 Hostname

Virtual IPv6 Address

Web Auth Intercept HTTPs

Watch List Enable

Watch List Expiry Timeout(secs)

Captive Bypass Portal

Disable Success Window

Disable Logout Window

Guided Assistance

Figure 5-47 Do not enable Captive Bypass Portal unless you really have a good reason

VTY		
VTY Line	<input type="text" value="Ex: 0 or 1-5"/>	View VTY options
VTY Transport Mode	<input type="text" value="None"/>	
Authentication List	<input type="text"/>	AAA Servers
Authorization List	<input type="text"/>	AAA Servers

Figure 5-48 VTY configuration for CLI access in the HTTP/Netconf web page

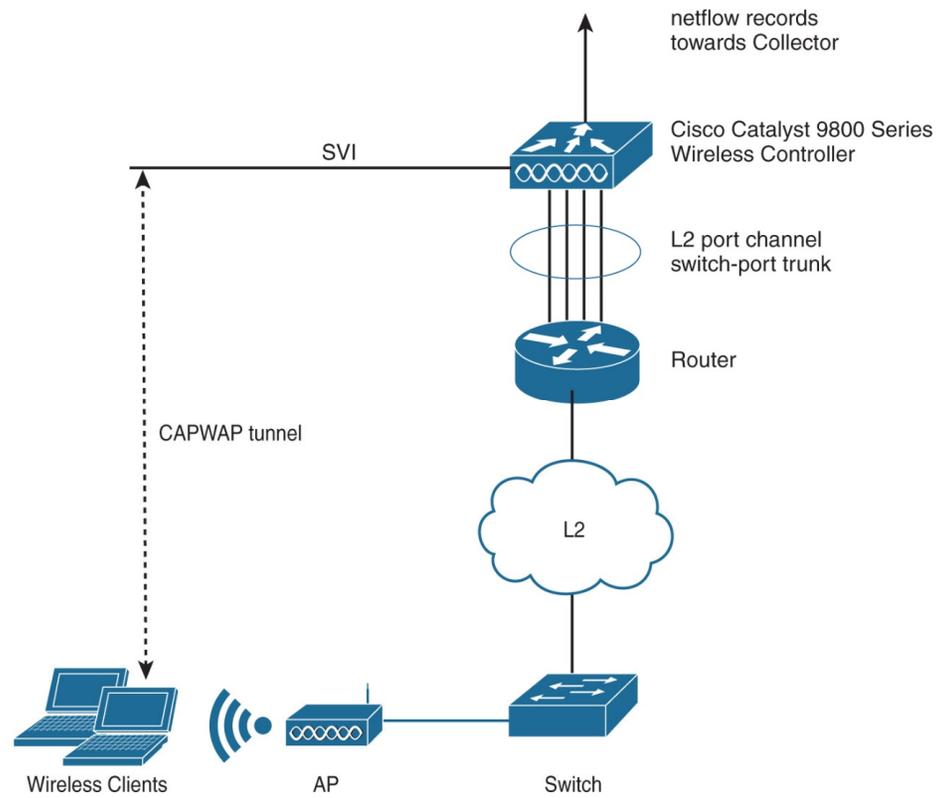


Figure 5-49 ETA workflow topology

Configuration ▾ > Security ▾ > Threat Defense > umbrella

Registration Token*

E434F41F3E120813C0FCC6437DD732F9002629B!

[Click here to get your Token](#)

Organization ID

2501054

Allowed Domains

Type Domain or Regex and press Enter



Enable DNS packets encryption

Umbrella Parameter Map

Type parameter map name and press Enter

Figure 5-50 Umbrella global configuration on the 9800

DNS Layer Security

DNS Layer
Security
Parameter Map

Not Configured



[Clear](#)

Flex DHCP Option
for DNS

ENABLED



Flex DNS Traffic
Redirect



IGNORE

Figure 5-51 DNS Layer Security (formerly called Umbrella) section of a policy profile.

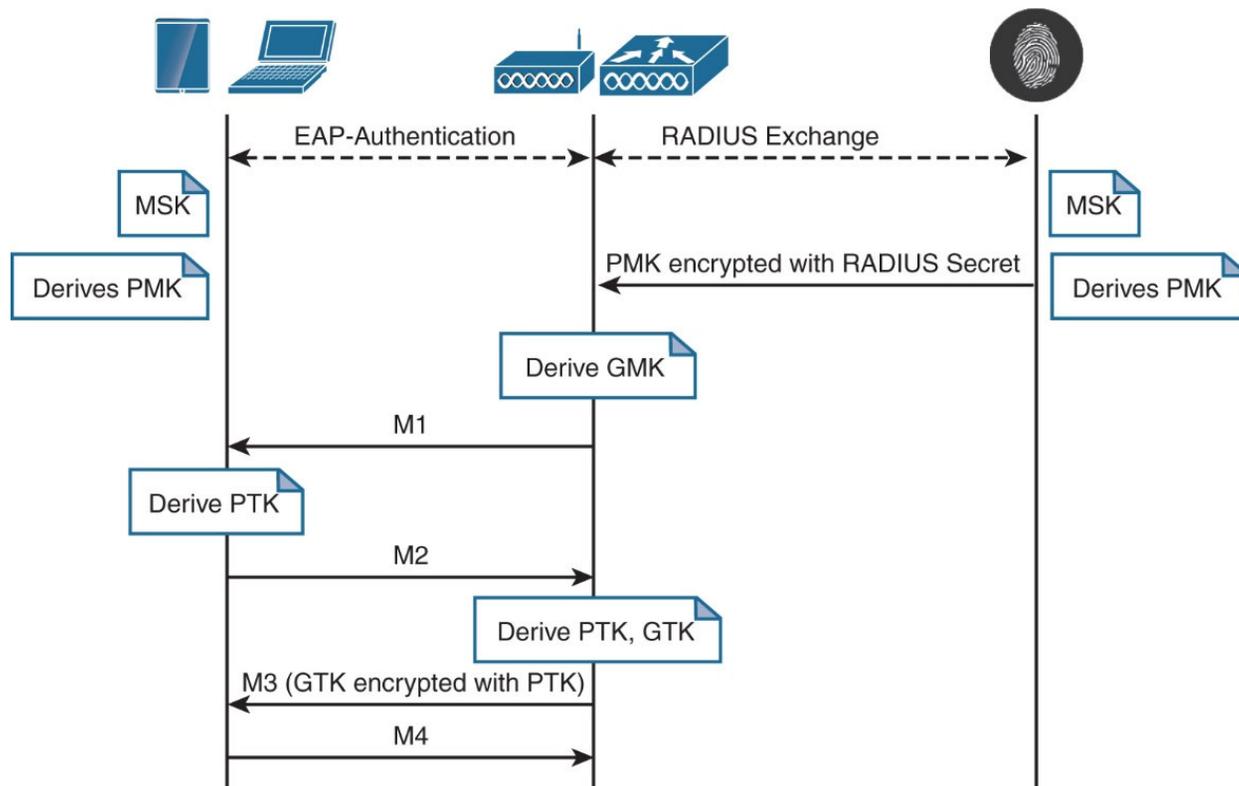


Figure 6-1 802.11 key management and distribution

No.	Time	Source	Destination	Length	Info
1716	0.022097	e2:2e:04:18:04:24	Cisco_9f:c3:2a	108	Authentication, SN=3813, FN=0, Flags=.....C
1718	0.001447	Cisco_9f:c3:2a	e2:2e:04:18:04:24	108	Authentication, SN=0, FN=0, Flags=.....C
1720	0.001086	e2:2e:04:18:04:24	Cisco_9f:c3:2a	361	Reassociation Request, SN=3814, FN=0, Flags=.....C, SSID=slowroampsk
1723	0.002113	Cisco_9f:c3:2a	e2:2e:04:18:04:24	287	Reassociation Response, SN=1, FN=0, Flags=.....C
1725	0.001293	Cisco_9f:c3:2a	e2:2e:04:18:04:24	221	Key (Message 1 of 4)
1731	0.020722	e2:2e:04:18:04:24	Cisco_9f:c3:2a	221	Key (Message 2 of 4)
1733	0.000607	Cisco_9f:c3:2a	e2:2e:04:18:04:24	255	Key (Message 3 of 4)
1735	0.012708	e2:2e:04:18:04:24	Cisco_9f:c3:2a	199	Key (Message 4 of 4)
1743	0.000052	e2:2e:04:18:04:24	Cisco_b1:6c:fd	144	QoS Data, SN=0, FN=0, Flags=.p....TC

Figure 6-2 WPA/WPA2 PSK reassociation (slow roam)

No.	Time	Source	Destination	Protocol	Length	Info
4713	16:54:43.246686	Apple_64:5d:e5	68:7d:b4:5e:43:8f	802.11	69	Authentication, SN=2755, FN=0, Flags=.....C
4715	16:54:43.248163	68:7d:b4:5e:43:8f	Apple_64:5d:e5	802.11	69	Authentication, SN=0, FN=0, Flags=.....C
4717	16:54:43.248853	Apple_64:5d:e5	68:7d:b4:5e:43:8f	802.11	211	Reassociation Request, SN=2756, FN=0, Flags=.....C, SSID=cvoice
4719	16:54:43.263550	68:7d:b4:5e:43:8f	Apple_64:5d:e5	802.11	183	Reassociation Response, SN=1, FN=0, Flags=.....C
4721	16:54:43.266930	68:7d:b4:5e:43:8f	Apple_64:5d:e5	EAP	72	Request, Identity
4723	16:54:43.269581	Apple_64:5d:e5	68:7d:b4:5e:43:8f	EAP	76	Response, Identity
4725	16:54:43.276763	68:7d:b4:5e:43:8f	Apple_64:5d:e5	EAP	73	Request, TLS EAP (EAP-TLS)
4727	16:54:43.278065	Apple_64:5d:e5	68:7d:b4:5e:43:8f	EAP	75	Response, Legacy Nak (Response Only)
4729	16:54:43.284187	68:7d:b4:5e:43:8f	Apple_64:5d:e5	EAP	73	Request, Protected EAP (EAP-PEAP)
4731	16:54:43.285117	Apple_64:5d:e5	68:7d:b4:5e:43:8f	TLSv1.2	260	Client Hello
4736	16:54:43.302692	68:7d:b4:5e:43:8f	Apple_64:5d:e5	EAP	1079	Request, Protected EAP (EAP-PEAP)
4738	16:54:43.303598	Apple_64:5d:e5	68:7d:b4:5e:43:8f	EAP	73	Response, Protected EAP (EAP-PEAP)
4740	16:54:43.307753	68:7d:b4:5e:43:8f	Apple_64:5d:e5	TLSv1.2	351	Server Hello, Certificate, Server Key Exchange, Server Hello Done
4742	16:54:43.317178	Apple_64:5d:e5	68:7d:b4:5e:43:8f	TLSv1.2	203	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
4744	16:54:43.323470	68:7d:b4:5e:43:8f	Apple_64:5d:e5	TLSv1.2	124	Change Cipher Spec, Encrypted Handshake Message
4746	16:54:43.324119	Apple_64:5d:e5	68:7d:b4:5e:43:8f	EAP	73	Response, Protected EAP (EAP-PEAP)
4748	16:54:43.328433	68:7d:b4:5e:43:8f	Apple_64:5d:e5	TLSv1.2	107	Application Data
4750	16:54:43.329524	Apple_64:5d:e5	68:7d:b4:5e:43:8f	TLSv1.2	111	Application Data
4752	16:54:43.333737	68:7d:b4:5e:43:8f	Apple_64:5d:e5	TLSv1.2	137	Application Data
4754	16:54:43.334653	Apple_64:5d:e5	68:7d:b4:5e:43:8f	TLSv1.2	165	Application Data
4756	16:54:43.346834	68:7d:b4:5e:43:8f	Apple_64:5d:e5	TLSv1.2	153	Application Data
4758	16:54:43.347552	Apple_64:5d:e5	68:7d:b4:5e:43:8f	TLSv1.2	108	Application Data
4760	16:54:43.351714	68:7d:b4:5e:43:8f	Apple_64:5d:e5	TLSv1.2	106	Application Data
4762	16:54:43.352310	Apple_64:5d:e5	68:7d:b4:5e:43:8f	EAP	73	Response, Protected EAP (EAP-PEAP)
4764	16:54:43.366697	68:7d:b4:5e:43:8f	Apple_64:5d:e5	EAP	71	Success
4766	16:54:43.367407	68:7d:b4:5e:43:8f	Apple_64:5d:e5	EAPOL	184	Key (Message 1 of 4)
4768	16:54:43.368210	Apple_64:5d:e5	68:7d:b4:5e:43:8f	EAPOL	202	Key (Message 2 of 4)
4770	16:54:43.370090	68:7d:b4:5e:43:8f	Apple_64:5d:e5	EAPOL	274	Key (Message 3 of 4)
4772	16:54:43.370773	Apple_64:5d:e5	68:7d:b4:5e:43:8f	EAPOL	162	Key (Message 4 of 4)

Figure 6-3 WPA/WPA2 EAP reassociation (slow roam)

No.	Time	Source	Destination	Length	Info
554	0.002172	92:4c:d7:78:89:f8	Cisco_23:c6:4f	108	Authentication, SN=1823, FN=0, Flags=.....C
556	0.000992	Cisco_23:c6:4f	92:4c:d7:78:89:f8	108	Authentication, SN=3128, FN=0, Flags=.....C
558	0.000985	92:4c:d7:78:89:f8	Cisco_23:c6:4f	347	Association Request, SN=1824, FN=0, Flags=.....C, SSID=OKC
559	0.000136	92:4c:d7:78:89:f8	Cisco_23:c6:4f	347	Association Request, SN=1824, FN=0, Flags=...R...C, SSID=OKC
561	0.004662	Cisco_23:c6:4f	92:4c:d7:78:89:f8	269	Association Response, SN=3129, FN=0, Flags=.....C
563	0.027169	Cisco_23:c6:4f	92:4c:d7:78:89:f8	109	Request, Identity
569	0.008778	92:4c:d7:78:89:f8	Cisco_23:c6:4f	115	Response, Identity
573	0.021785	Cisco_23:c6:4f	92:4c:d7:78:89:f8	110	Request, Protected EAP (EAP-PEAP)
575	0.006260	92:4c:d7:78:89:f8	Cisco_23:c6:4f	241	Client Hello
599	0.000000	Cisco_23:c6:4f	92:4c:d7:78:89:f8	101	Request, Protected EAP (EAP-PEAP)
602	0.001996	92:4c:d7:78:89:f8	Cisco_23:c6:4f	110	Response, Protected EAP (EAP-PEAP)
604	0.003478	Cisco_23:c6:4f	92:4c:d7:78:89:f8	1321	Server Hello, Certificate, Server Key Exchange, Server Hello Done
606	0.007491	92:4c:d7:78:89:f8	Cisco_23:c6:4f	236	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
608	0.001755	Cisco_23:c6:4f	92:4c:d7:78:89:f8	165	Change Cipher Spec, Encrypted Handshake Message
610	0.002876	92:4c:d7:78:89:f8	Cisco_23:c6:4f	110	Response, Protected EAP (EAP-PEAP)
612	0.001465	Cisco_23:c6:4f	92:4c:d7:78:89:f8	144	Application Data
614	0.002854	92:4c:d7:78:89:f8	Cisco_23:c6:4f	150	Application Data
616	0.001802	Cisco_23:c6:4f	92:4c:d7:78:89:f8	144	Application Data
618	0.002206	92:4c:d7:78:89:f8	Cisco_23:c6:4f	152	Application Data
620	0.001553	Cisco_23:c6:4f	92:4c:d7:78:89:f8	150	Application Data
622	0.002853	92:4c:d7:78:89:f8	Cisco_23:c6:4f	150	Application Data
624	0.001847	Cisco_23:c6:4f	92:4c:d7:78:89:f8	108	Success
626	0.000466	Cisco_23:c6:4f	92:4c:d7:78:89:f8	221	Key (Message 1 of 4)
628	0.007728	92:4c:d7:78:89:f8	Cisco_23:c6:4f	221	Key (Message 2 of 4)
630	0.001235	Cisco_23:c6:4f	92:4c:d7:78:89:f8	255	Key (Message 3 of 4)
633	0.000585	92:4c:d7:78:89:f8	Cisco_23:c6:4f	199	Key (Message 4 of 4)
634	0.000000	92:4c:d7:78:89:f8	Cisco_23:c6:4f	199	Key (Message 4 of 4)
2026	0.022106	92:4c:d7:78:89:f8	Cisco_9f:c3:2f	108	Authentication, SN=2190, FN=0, Flags=.....C
2028	0.001362	Cisco_9f:c3:2f	92:4c:d7:78:89:f8	108	Authentication, SN=0, FN=0, Flags=.....C
2030	0.001320	92:4c:d7:78:89:f8	Cisco_9f:c3:2f	371	Reassociation Request, SN=2191, FN=0, Flags=.....C, SSID=OKC
2033	0.003157	Cisco_9f:c3:2f	92:4c:d7:78:89:f8	287	Reassociation Response, SN=1, FN=0, Flags=.....C
2035	0.001324	Cisco_9f:c3:2f	92:4c:d7:78:89:f8	221	Key (Message 1 of 4)
2043	0.034286	92:4c:d7:78:89:f8	Cisco_9f:c3:2f	239	Key (Message 2 of 4)
2045	0.001272	Cisco_9f:c3:2f	92:4c:d7:78:89:f8	255	Key (Message 3 of 4)
2048	0.000248	92:4c:d7:78:89:f8	Cisco_9f:c3:2f	199	Key (Message 4 of 4)

Figure 6-4 Packet capture: OKC fast roam in local mode deployment

```

> IEEE 802.11 Reassociation Request, Flags: .....C
v IEEE 802.11 Wireless Management
  > Fixed parameters (10 bytes)
  v Tagged parameters (271 bytes)
    > Tag: SSID parameter set: OKC
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: Power Capability Min: -9, Max: 17
    > Tag: Supported Channels
    v Tag: RSN Information
      Tag Number: RSN Information (48)
      Tag length: 38
      RSN Version: 1
      > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
        Pairwise Cipher Suite Count: 1
      > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
        Auth Key Management (AKM) Suite Count: 1
      > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) WPA
      > RSN Capabilities: 0x008c
        PMKID Count: 1
      v PMKID List
        PMKID: efdd9cb1ef752e98d80db8433376cbab
    > Tag: RM Enabled Capabilities (5 octets)
    > Tag: Supported Operating Classes
    > Tag: HT Capabilities (802.11n D1.10)

```

Figure 6-5 OKC fast roam RSN IE

Configuration > Tags & Profiles > WLANs

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity

General Security **Advanced** Add To Policy Tags

Coverage Hole Detection	<input checked="" type="checkbox"/>	Universal Admin	<input type="checkbox"/>
Aironet IE ⓘ	<input type="checkbox"/>	OKC	<input type="checkbox"/>

Figure 6-6 Disabling OKC for FlexConnect local authorization

Monitoring > Wireless > Clients

Client

Clients Sleeping C 360 View General QOS Statistics ATF Statistics **Mobility History** Call Statistics

× Delete ↻

Selected 0 out of 1 Client

Client MAC Address
e22e.0418.0424

Recent association history:

AP Name	BSSID	AP Slot	Assoc Time	Instance	Mobility Role	Run Latency (ms)	Roam Type
sudha-9130	04eb.409f.c32b	1	01/04/2022 08:27:08	0	Local	105	802.11i Fast
sudha-9120	c064.e423.c64b	1	01/04/2022 08:25:34	0	Local	1414	N/A

Figure 6-7 Monitoring the client roam type on the C9800

Edit WLAN

General **Security** Advanced Add To Policy Tags

Layer2 Layer3 AAA

Layer 2 Security Mode

MAC Filtering

Protected Management Frame

PMF

WPA Parameters

WPA Policy

WPA2 Policy

GTK Randomize

OSEN Policy

WPA2 Encryption AES(CCMP128)
 CCMP256
 GCMP128
 GCMP256

Auth Key Mgmt 802.1x
 PSK
 Easy-PSK
 CCKM
 FT + 802.1x
 FT + PSK
 802.1x-SHA256
 PSK-SHA256

CCKM Timestamp Tolerance*

Lobby Admin Access

Fast Transition

Over the DS

Reassociation Timeout

MPSK Configuration

MPSK

Figure 6-8 Configuring CCKM on the C9800

```
> IEEE 802.11 Beacon frame, Flags: .....C
  v IEEE 802.11 Wireless Management
    > Fixed parameters (12 bytes)
    v Tagged parameters (383 bytes)
      > Tag: SSID parameter set: 11renable
      > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
      > Tag: DS Parameter set: Current Channel: 100
      > Tag: Traffic Indication Map (TIM): DTIM 1 of 1 bitmap
      > Tag: Country Information: Country Code US, Environment Unknown (0x04)
      > Tag: Power Constraint: 3
      > Tag: TPC Report Transmit Power: 0, Link Margin: 0
      > Tag: RSN Information
      v Tag: Mobility Domain
        Tag Number: Mobility Domain (54)
        Tag length: 3
        Mobility Domain Identifier: 0x34ac
        FT Capability and Policy: 0x00
        .... ..0 = Fast BSS Transition over DS: 0x0
        .... ..0. = Resource Request Protocol Capability: 0x0
      > Tag: QBSS Load Element 802.11e CCA Version
```

Figure 6-9 802.11r FT Beacon MDIE

```

> IEEE 802.11 Beacon frame, Flags: .....C
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (383 bytes)
    > Tag: SSID parameter set: 11renable
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 100
    > Tag: Traffic Indication Map (TIM): DTIM 1 of 1 bitmap
    > Tag: Country Information: Country Code US, Environment Unknown (0x04)
    > Tag: Power Constraint: 3
    > Tag: TPC Report Transmit Power: 0, Link Margin: 0
    v Tag: RSN Information
      Tag Number: RSN Information (48)
      Tag length: 20
      RSN Version: 1
      > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
        Pairwise Cipher Suite Count: 1
        > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
          Auth Key Management (AKM) Suite Count: 1
          v Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) FT over IEEE 802.1X
            v Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) FT over IEEE 802.1X
              Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
              Auth Key Management (AKM) type: FT over IEEE 802.1X (3)
            > RSN Capabilities: 0x0028
      > Tag: Mobility Domain
  
```

Figure 6-10 802.11r FT Beacon RSN IE AKM

```

> IEEE 802.11 Association Response, Flags: .....C
  IEEE 802.11 Wireless Management
    Fixed parameters (6 bytes)
    Tagged parameters (276 bytes)
      Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
      Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
      Tag: HT Capabilities (802.11n D1.10)
      Tag: HT Information (802.11n D1.10)
      Tag: Extended Capabilities (10 octets)
      Tag: VHT Capabilities
      Tag: VHT Operation
      Tag: Mobility Domain
      Tag: Fast BSS Transition
        Tag Number: Fast BSS Transition (55)
        Tag length: 96
        MIC Control: 0x0000
        0000 0000 .... = Element Count: 0
        MIC: 00000000000000000000000000000000
        ANonce: 0000000000000000000000000000000000000000000000000000000000000000
        SNonce: 0000000000000000000000000000000000000000000000000000000000000000
        Subelement ID: PMK-R1 key holder identifier (R1KH-ID) (1)
        Length: 6
        PMK-R1 key holder identifier (R1KH-ID): 84e87e81d09a
        Subelement ID: PMK-R0 key holder identifier (R0KH-ID) (3)
        Length: 4
        PMK-R0 key holder identifier (R0KH-ID): 33457d3f

```

Figure 6-11 802.11r FT association response

No.	Time	Source	Destination	Length	Info
285	0.002251	MurataMa_60:29:3e	Cisco_23:c6:4c	108	Authentication, SN=271, FN=0, Flags=.....C
287	0.001038	Cisco_23:c6:4c	MurataMa_60:29:3e	108	Authentication, SN=938, FN=0, Flags=.....C
289	0.001673	MurataMa_60:29:3e	Cisco_23:c6:4c	358	Association Request, SN=272, FN=0, Flags=.....C, SSID=11renable
291	0.004228	Cisco_23:c6:4c	MurataMa_60:29:3e	372	Association Response, SN=939, FN=0, Flags=.....C
293	0.004293	Cisco_23:c6:4c	MurataMa_60:29:3e	109	Request, Identity
295	0.024719	MurataMa_60:29:3e	Cisco_23:c6:4c	115	Response, Identity
299	0.088306	Cisco_23:c6:4c	MurataMa_60:29:3e	110	Request, Protected EAP (EAP-PEAP)
301	0.003845	MurataMa_60:29:3e	Cisco_23:c6:4c	241	Client Hello
308	0.000000	Cisco_23:c6:4c	MurataMa_60:29:3e	101	Request, Protected EAP (EAP-PEAP)
310	0.003464	MurataMa_60:29:3e	Cisco_23:c6:4c	110	Response, Protected EAP (EAP-PEAP)
312	0.003413	Cisco_23:c6:4c	MurataMa_60:29:3e	1321	Server Hello, Certificate, Server Key Exchange, Server Hello Done
314	0.010654	MurataMa_60:29:3e	Cisco_23:c6:4c	236	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
316	0.002056	Cisco_23:c6:4c	MurataMa_60:29:3e	165	Change Cipher Spec, Encrypted Handshake Message
318	0.002469	MurataMa_60:29:3e	Cisco_23:c6:4c	110	Response, Protected EAP (EAP-PEAP)
320	0.002267	Cisco_23:c6:4c	MurataMa_60:29:3e	144	Application Data
322	0.002323	MurataMa_60:29:3e	Cisco_23:c6:4c	150	Application Data
324	0.001642	Cisco_23:c6:4c	MurataMa_60:29:3e	144	Application Data
326	0.003633	MurataMa_60:29:3e	Cisco_23:c6:4c	152	Application Data
328	0.001511	Cisco_23:c6:4c	MurataMa_60:29:3e	150	Application Data
330	0.002657	MurataMa_60:29:3e	Cisco_23:c6:4c	150	Application Data
332	0.001764	Cisco_23:c6:4c	MurataMa_60:29:3e	108	Success
334	0.000000	Cisco_23:c6:4c	MurataMa_60:29:3e	221	Key (Message 1 of 4)
336	0.020090	MurataMa_60:29:3e	Cisco_23:c6:4c	342	Key (Message 2 of 4)
338	0.002610	Cisco_23:c6:4c	MurataMa_60:29:3e	391	Key (Message 3 of 4)
341	0.000000	MurataMa_60:29:3e	Cisco_23:c6:4c	199	Key (Message 4 of 4)
342	0.000000	MurataMa_60:29:3e	Cisco_23:c6:4c	199	Key (Message 4 of 4)
367	0.046878	MurataMa_60:29:3e	Broadcast	462	QoS Data, SN=2, FN=0, Flags=.p....TC
397	0.024374	MurataMa_60:29:3e	Broadcast	144	QoS Data, SN=3, FN=0, Flags=.p....TC
412	0.002264	MurataMa_60:29:3e	10.6.1.12	274	QoS Data, SN=4, FN=0, Flags=.p....TC
868	0.022004	MurataMa_60:29:3e	Cisco_9f:c3:2c	243	Authentication, SN=466, FN=0, Flags=.....C
870	0.001272	Cisco_9f:c3:2c	MurataMa_60:29:3e	239	Authentication, SN=0, FN=0, Flags=.....C
872	0.001386	MurataMa_60:29:3e	Cisco_9f:c3:2c	480	Reassociation Request, SN=467, FN=0, Flags=.....C, SSID=11renable
875	0.002663	Cisco_9f:c3:2c	MurataMa_60:29:3e	467	Reassociation Response, SN=1, FN=0, Flags=.....C
899	0.012668	MurataMa_60:29:3e	Cisco_b1:6c:fd	144	QoS Data, SN=1, FN=0, Flags=.p....TC
901	0.007196	MurataMa_60:29:3e	Broadcast	144	QoS Data, SN=2, FN=0, Flags=.p....TC

Figure 6-12 802.11r (FT) initial association and roam (over-the-air)

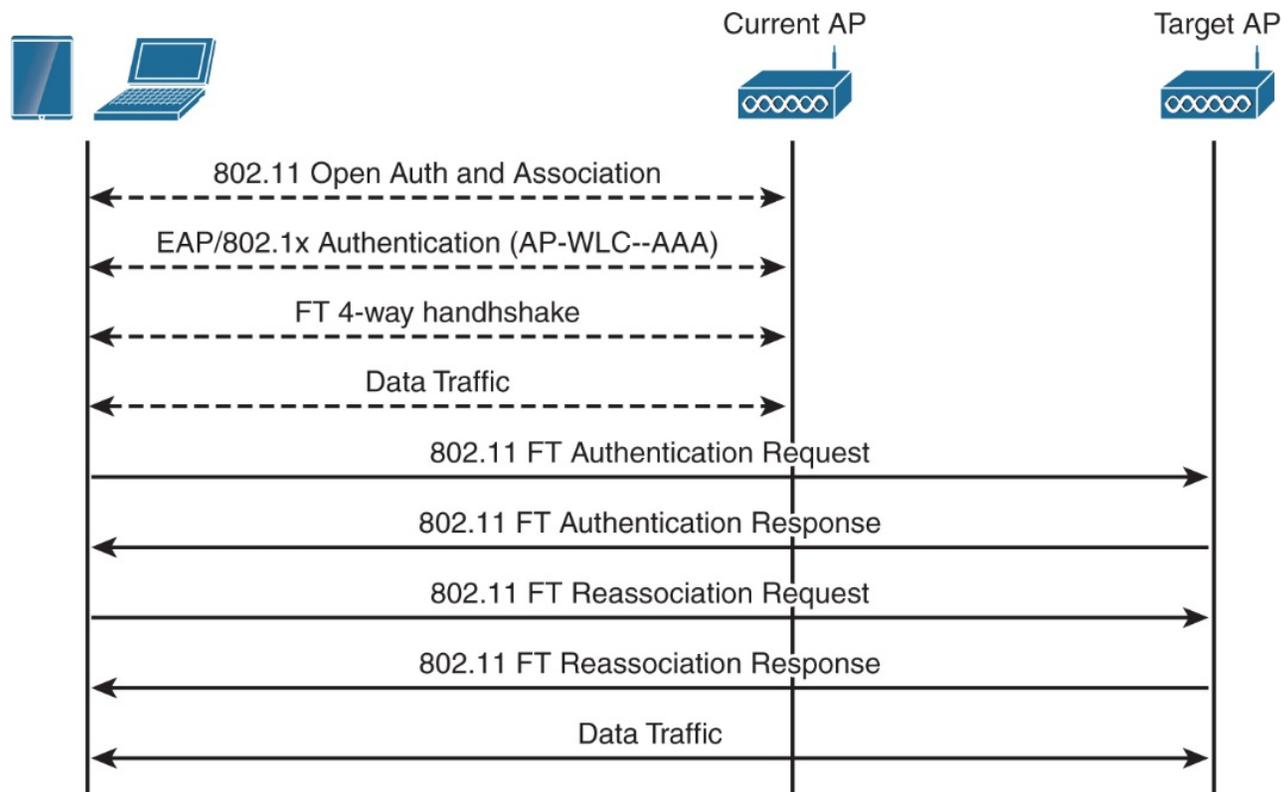


Figure 6-13 FT roam over-the-air

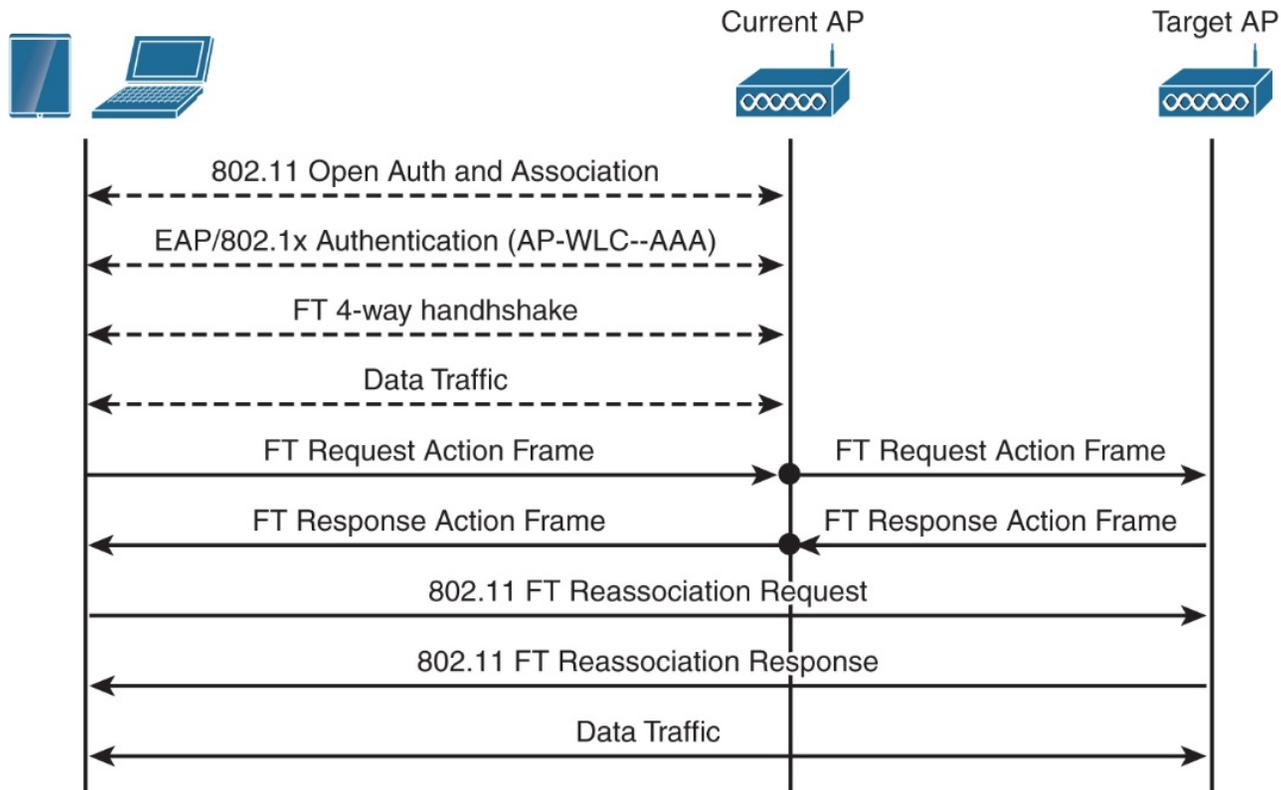


Figure 6-14 FT roam over-the-DS

```

> IEEE 802.11 Beacon frame, Flags: .....C
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (360 bytes)
    > Tag: SSID parameter set: 11rmixed
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: Traffic Indication Map (TIM): DTIM 1 of 1 bitmap
    > Tag: Country Information: Country Code US, Environment Unknown (0x04)
    > Tag: Power Constraint: 0
    v Tag: RSN Information
      Tag Number: RSN Information (48)
      Tag length: 24
      RSN Version: 1
      > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
      Pairwise Cipher Suite Count: 1
      > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
        Auth Key Management (AKM) Suite Count: 2
        v Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) WPA 00:0f:ac (Ieee 802.11) FT over IEEE 802.1X
          v Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) WPA
            Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
            Auth Key Management (AKM) type: WPA (1)
          v Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) FT over IEEE 802.1X
            Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
            Auth Key Management (AKM) type: FT over IEEE 802.1X (3)
        > RSN Capabilities: 0x0028
      > Tag: QBSS Load Element 802.11e CCA Version
      > Tag: RM Enabled Capabilities (5 octets)
      > Tag: Mobility Domain

```

Figure 6-15 AKM in RSN IE in beacon of mixed-mode FT WLAN

```
> IEEE 802.11 Beacon frame, Flags: .....C
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (360 bytes)
    v Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (11) (11)
      Tag Number: Vendor Specific (221)
      Tag length: 5
      OUI: 00:40:96 (Cisco Systems, Inc.)
      Vendor Specific OUI Type: 11
      Aironet IE type: Unknown (11) (11)
      Aironet IE data: 89
```

Figure 6-16 Aironet IE in beacon of mixed-mode FT WLAN

```

> IEEE 802.11 Beacon frame, Flags: .....C
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (382 bytes)
    > Tag: SSID parameter set: 11radapt
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 100
    > Tag: Traffic Indication Map (TIM): DTIM 1 of 1 bitmap
    > Tag: Country Information: Country Code US, Environment Unknown (0x04)
    > Tag: Power Constraint: 3
    > Tag: TPC Report Transmit Power: 0, Link Margin: 0
    v Tag: RSN Information
      Tag Number: RSN Information (48)
      Tag length: 20
      RSN Version: 1
      > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
        Pairwise Cipher Suite Count: 1
      > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
        Auth Key Management (AKM) Suite Count: 1
      v Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) WPA
        v Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) WPA
          Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
          Auth Key Management (AKM) type: WPA (1)
      > RSN Capabilities: 0x0028
    > Tag: Mobility Domain

```

Figure 6-17 AKM in RSN IE of beacon of adaptive FT WLAN

```
> IEEE 802.11 Beacon frame, Flags: .....C
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (382 bytes)
    > Tag: SSID parameter set: 11radapt
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    v Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (11) (11)
      Tag Number: Vendor Specific (221)
      Tag length: 5
      OUI: 00:40:96 (Cisco Systems, Inc.)
      Vendor Specific OUI Type: 11
      Aironet IE type: Unknown (11) (11)
      Aironet IE data: c9
```

Figure 6-18 Aironet IE in beacon of adaptive FT WLAN

Monitoring > Wireless > Clients

Client

360 View

General

QOS Statistics

ATF Statistics

Mobility History

Call Statistics

Recent association history:

AP Name	BSSID	AP Slot	Assoc Time	Instance	Mobility Role	Run Latency (ms)	Roam Type
sudha-9130	04eb.409f.c32c	1	01/04/2022 18:55:37	0	Local	6	802.11R
sudha-9120	c064.e423.c64c	1	01/04/2022 18:55:23	0	Local	723	N/A

Figure 6-19 Monitoring the mobility history of a client on the C9800 GUI

Configuration > Tags & Profiles > WLANs

Edit WLAN

Per WLAN	<input type="text" value="0"/>	6	7
Per AP Per WLAN	<input type="text" value="0"/>	Scan Defer Time	<input type="text" value="100"/>
Per AP Radio Per WLAN	<input type="text" value="200"/>	Assisted Roaming (11k)	
11v BSS Transition Support		<input type="checkbox"/> Prediction Optimization <input checked="" type="checkbox"/> Neighbor List <input type="checkbox"/> Dual Band Neighbor List	
BSS Transition	<input checked="" type="checkbox"/>		
Dual Neighbor List	<input type="checkbox"/>		
BSS Max Idle Service	<input checked="" type="checkbox"/>		

Figure 6-20 Configuring an 802.11k on the C9800 WLAN Profile

Configuration ▾ > Wireless ▾ > Wireless Global

Default Mobility Domain *	<input type="text" value="default"/>	Assisted Roaming	
RF Group Name*	<input type="text" value="default"/>	Denial Maximum*	<input type="text" value="5"/>
Maximum Login Sessions Per User*	<input type="text" value="0"/>	Floor Bias(dBm)*	<input type="text" value="15"/>
Management Via Wireless	<input checked="" type="checkbox"/>	Prediction Minimum*	<input type="text" value="3"/>

Figure 6-21 Configuring assisted roaming parameters on the C9800

Configuration > Tags & Profiles > WLANs

Edit WLAN

Per AP Radio Per WLAN:

Time:

11v BSS Transition Support

- BSS Transition
- Dual Neighbor List
- BSS Max Idle Service
- BSS Max Idle Protected
- Directed Multicast Service

Configuration of '11v BSS Disassociation Imminent' is supported from Command Line Interface (CLI) only

Assisted Roaming (11k)

- Prediction Optimization
- Neighbor List
- Dual Band Neighbor List

DTIM Period (in beacon intervals)

- 5 GHz Band (1-255)
- 2.4 GHz Band (1-255)

Figure 6-22 Configuring an 802.11v BSS transition on the C9800

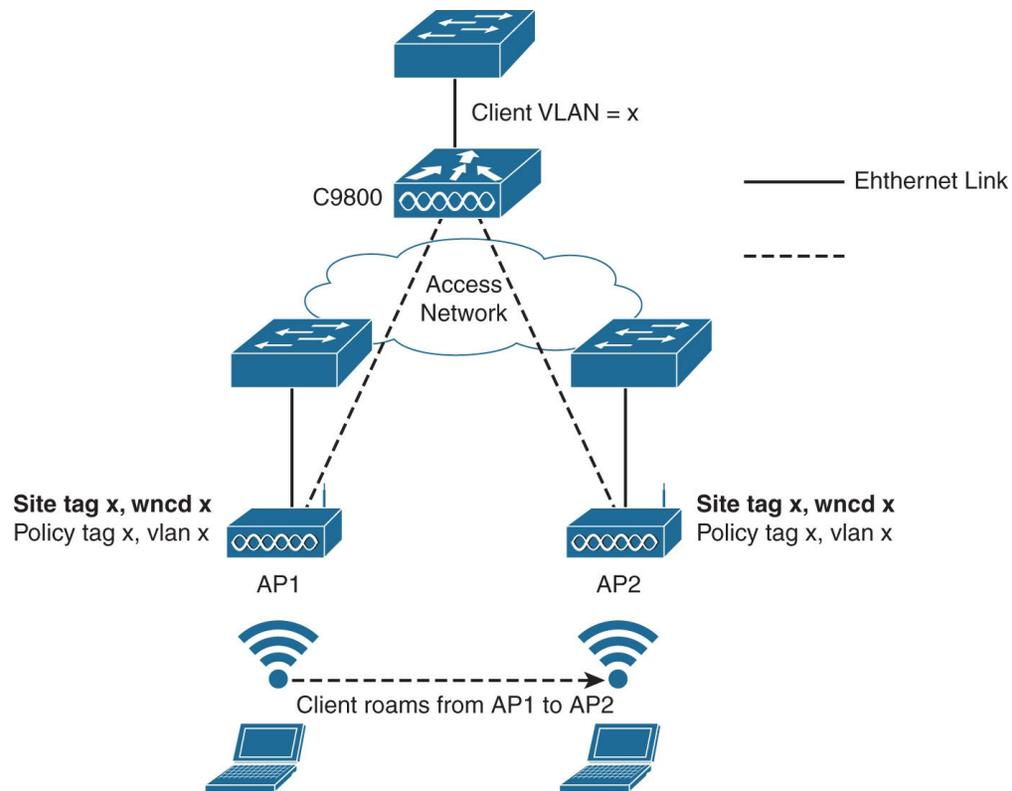


Figure 6-23 Intra-controller Intra-WNCd roaming on the C9800

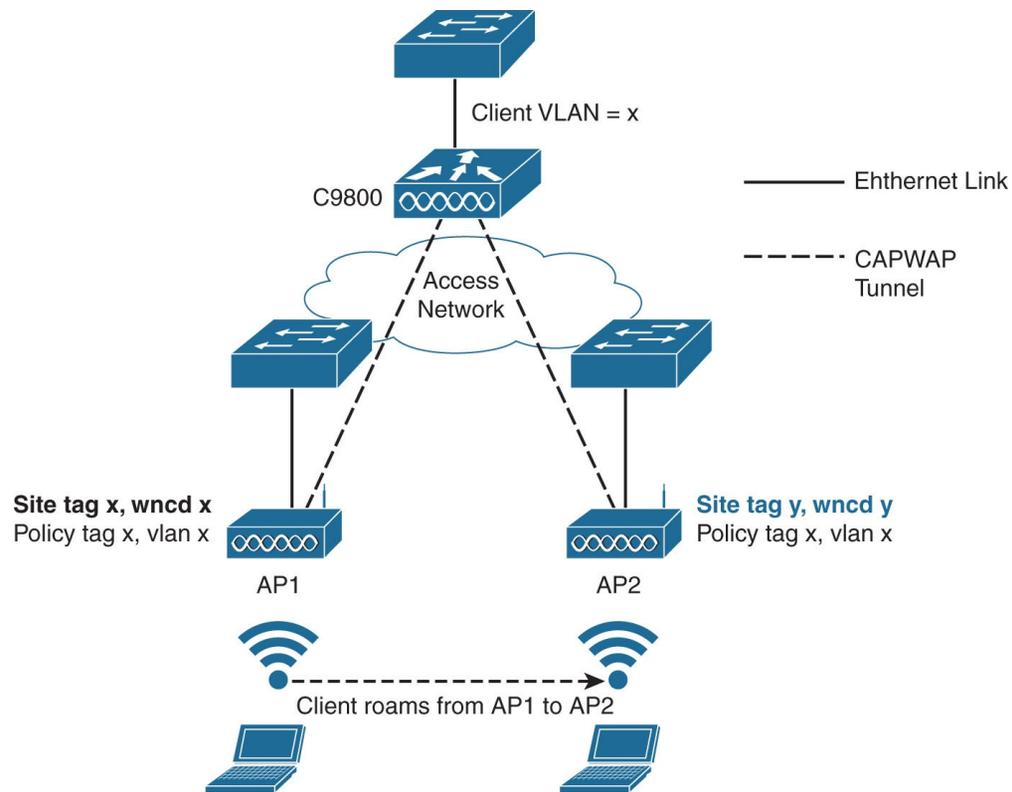


Figure 6-24 Intra-controller inter-WNCd roaming on the C9800

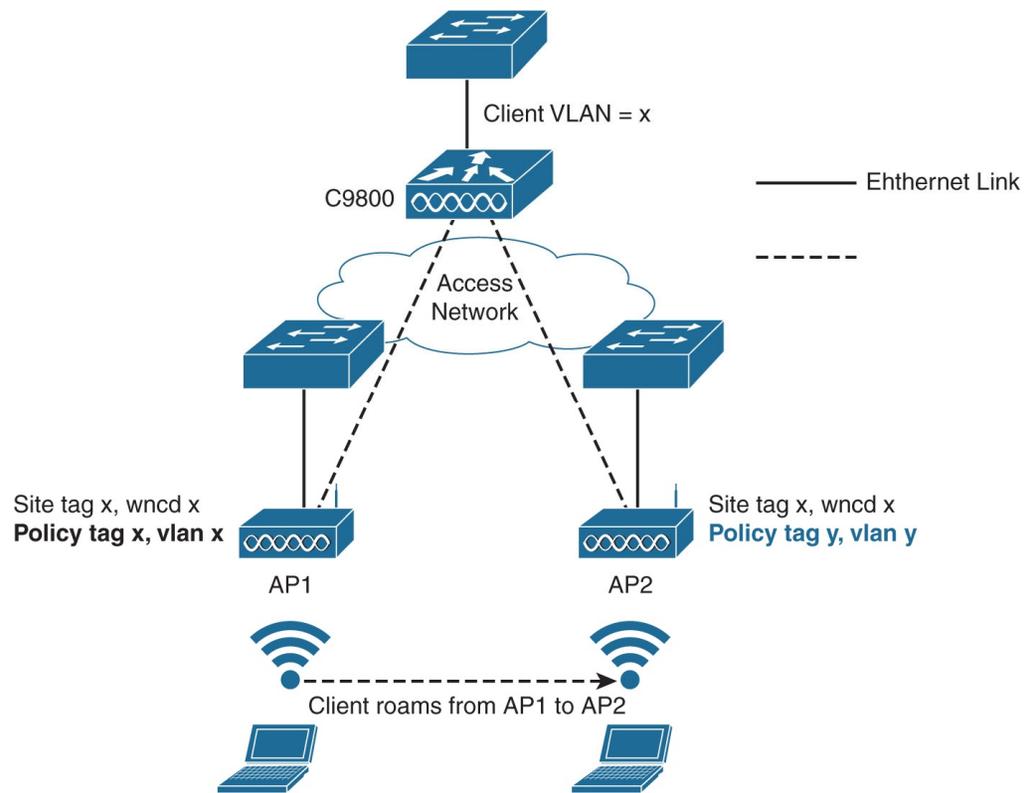


Figure 6-25 Intra-controller inter-policy profile roaming on the C9800

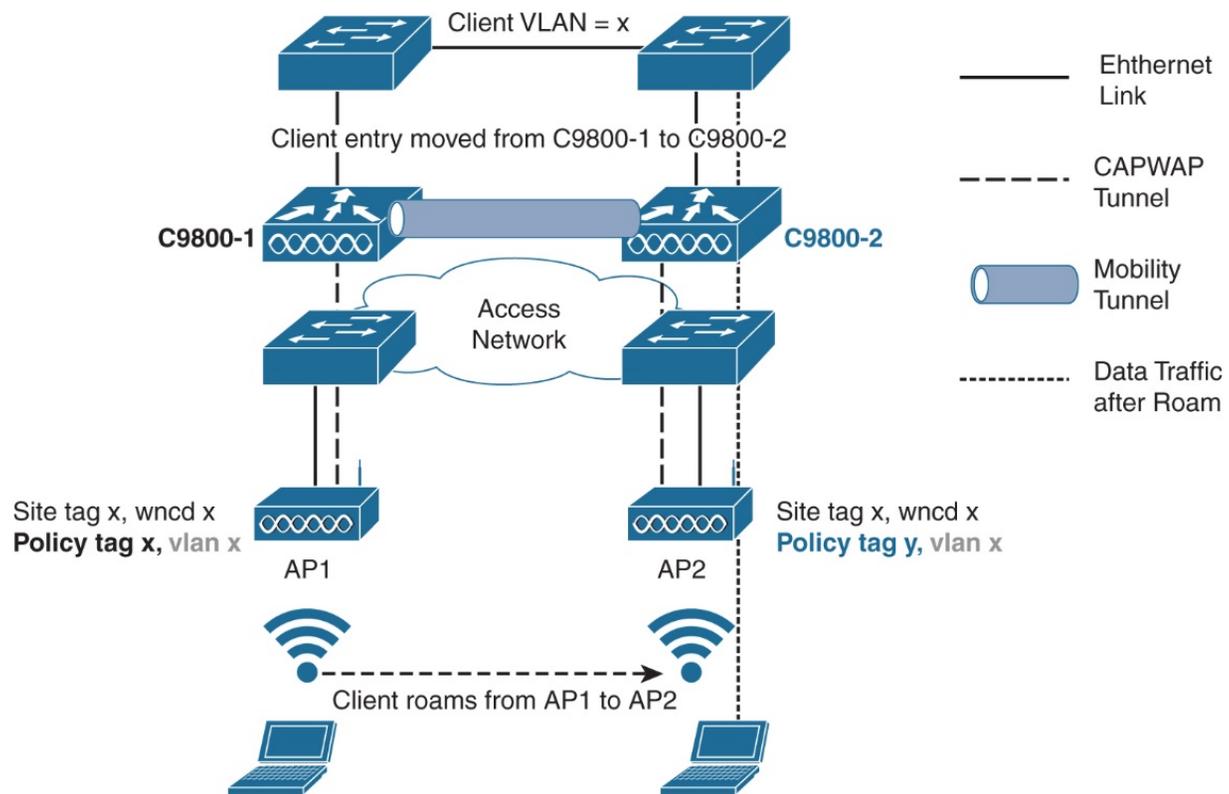


Figure 6-26 Layer 2 CAPWAP Mobility Tunnel C9800

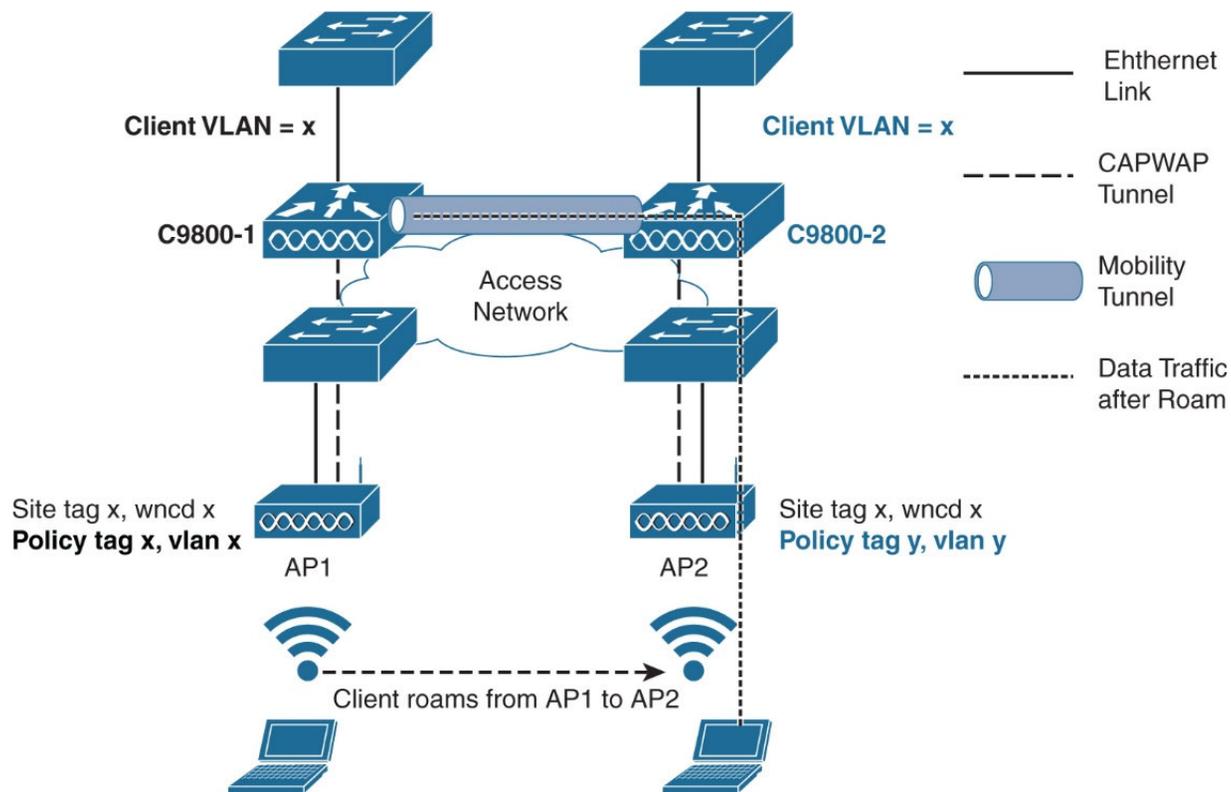


Figure 6-27 Layer 3 inter-controller roaming on the C9800

Edit Policy Profile

 Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for this Policy profile.

General Access Policies QOS and AVC **Mobility** Advanced

Mobility Anchors

Export Anchor

Static IP Mobility **ENABLED**

Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.

Figure 6-28 Configuring Static IP Mobility on the C9800

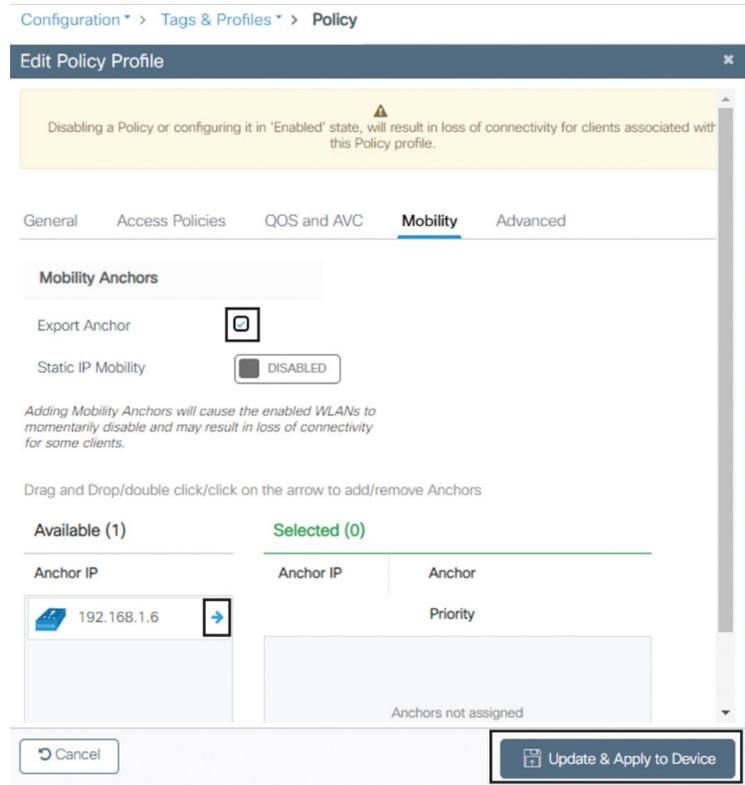


Figure 6-29 Configuring auto anchoring on the C9800

Configuration > Wireless > **Mobility**

Global Configuration Peer Configuration

Mobility Group Name*	<input type="text" value="default"/>
Multicast IPv4 Address	<input type="text" value="0.0.0.0"/>
Multicast IPv6 Address	<input type="text" value="::"/>
Keep Alive Interval (sec)*	<input type="text" value="10"/>
Mobility Keep Alive Count*	<input type="text" value="3"/>
Mobility DSCP Value*	<input type="text" value="48"/>
Mobility MAC Address	<input type="text" value="d478.9b3c.5e8b"/>
DTLS High Cipher Only*	<input checked="" type="checkbox"/> ENABLED



Figure 6-30 Configuring secure mobility on the C9800

Configuration > Wireless > Mobility

Global Configuration Peer Configuration

▼ Mobility Peer Configuration

+ Add × Delete ↻

Add Mobility Peer

MAC Address* 00b0.e1f3.2000

Peer IPv4/IPv6 Address* 192.168.1.6 ⇄ Ping Test

Public IPv4/IPv6 Address 192.168.1.6

Group Name* aireos ▼

Data Link Encryption DISABLED

SSC Hash Enter SSC Hash (must contain 40 characters)

↻ Cancel Apply to Device

Figure 6-31 Configuring mobility peers on the C9800

Configuration > Wireless > Mobility

Global Configuration Peer Configuration

▼ Mobility Peer Configuration

[+ Add](#) [× Delete](#) 

	MAC Address	IP Address	Public IP	Group Name	Multicast IPv4	Multicast IPv6	Status	PMTU	SSC Hash
	d478.9b3c.5e8b	192.168.1.5	N/A	default	0.0.0.0	::	N/A	N/A	f5d4c4b7d803604ab8152a063254
<input type="checkbox"/>	00b0.e1f3.2000	192.168.1.6	192.168.1.6	aireos	0.0.0.0	::	Up	1385	

10 items per page 1 - 2 of 2 items

Figure 6-32 Monitoring mobility tunnel status on the C9800

The screenshot displays the Cisco AireOS WLC configuration interface for a Mobility Group Member. The top navigation bar includes the Cisco logo and menu items: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP. The user is logged in as 'User:katgeri(ReadWrite)' and is on the 'Home' page. The main content area is titled 'Mobility Group Member > New' and contains the following configuration fields:

- Member IP Address(lpv4/lpv6): 192.168.1.5
- Member MAC Address: d4:78:9b:3c:5e:8b
- Group Name: default
- Secure Mobility: Enabled
- Data Tunnel Encryption: Disabled
- High Cipher: Disabled
- Hash: none

A note at the bottom of the configuration area reads: "1. Hash, Secure mobility and Data Tunnel Encryption are not supported for IPv6 members". The left sidebar shows the navigation menu with 'Mobility Management' expanded and 'Mobility Groups' selected.

Figure 6-33 Configuring secure mobility on AireOS WLC

Configuration > Wireless > Access Points

> All Access Points

> 5 GHz Radios

> 2.4 GHz Radios

> Dual-Band Radios

▼ Country

[Click here](#) for list of access point models and protocols supported per country and regulatory domain.

Apply

Selected Country BE , CA , QA , ZA

Regulatory Domain

802.11a/n/ac: [Indoor: -AEM, Outdoor: -ABEMN]

802.11b/g/n: [Indoor: -AE, Outdoor: -ABEN]

Search

	Country Code	Name
<input type="checkbox"/>	AE	United Arab Emirates
<input type="checkbox"/>	AL	Albania
<input type="checkbox"/>	AR	Argentina
<input type="checkbox"/>	AT	Austria
<input type="checkbox"/>	AU	Australia
<input type="checkbox"/>	BA	Bosnia
<input type="checkbox"/>	BB	Barbados
<input type="checkbox"/>	BD	Bangladesh

Figure 7-1 The country configuration page

Configuration > Wireless > Access Points

▼ All Access Points

Number of AP(s): 2

AP Name	AP Model	Slots	Admin Status	IP Address	Base Radio MAC	AP Mode
9130-etage	C9130AXI-E	3	✓	91.181.218.194	488b.0a35.1540	Flex
3700-rez	AIR-CAP3702I-E-K9	2	✓	91.181.218.194	88f0.3169.d390	Flex

1 items per page

> 5 GHz Radios

Edit AP

General Interfaces High Availability Inventory ICap **Advanced** Support Bundle

Advanced

Country Code*	BE	AP Retransmit Config Parameters	
Multiple Countries	BE, CA, QA, ZA	AP Retransmit Count	5
Statistics Timer	180	AP Retransmit Interval	3
AP Image Management			
CAPWAP MTU	1485	Predownload	Swap
AP Link Latency	Disabled	AP Crash Data	
AP TCP MSS Adjust	Enabled	Download to bootflash	Get Crash File
AP TCP MSS Size	1250		

Figure 7-2 Country selection for each AP

```

▼ Tagged parameters (366 bytes)
  ▶ Tag: SSID parameter set: Darchis
  ▶ Tag: Supported Rates 18, 24(B), 36, 48, 54, [Mbit/sec]
  ▶ Tag: DS Parameter set: Current Channel: 64
  ▶ Tag: Traffic Indication Map (TIM): DTIM 1 of 1 bitmap
  ▼ Tag: Country Information: Country Code BE, Environment Unknown (0x04)
    Tag Number: Country Information (7)
    Tag length: 72
    Code: BE
    Environment: Unknown (0x04)
    ▶ Country Info: First Channel Number: 36, Number of Channels: 1, Maximum Transmit Power Level: 23 dBm
    ▶ Country Info: First Channel Number: 40, Number of Channels: 1, Maximum Transmit Power Level: 23 dBm
    ▶ Country Info: First Channel Number: 44, Number of Channels: 1, Maximum Transmit Power Level: 23 dBm
    ▶ Country Info: First Channel Number: 48, Number of Channels: 1, Maximum Transmit Power Level: 23 dBm
    ▶ Country Info: First Channel Number: 52, Number of Channels: 1, Maximum Transmit Power Level: 23 dBm
    ▶ Country Info: First Channel Number: 56, Number of Channels: 1, Maximum Transmit Power Level: 23 dBm
    ▶ Country Info: First Channel Number: 60, Number of Channels: 1, Maximum Transmit Power Level: 23 dBm
    ▶ Country Info: First Channel Number: 64, Number of Channels: 1, Maximum Transmit Power Level: 23 dBm
    ▶ Country Info: First Channel Number: 100, Number of Channels: 1, Maximum Transmit Power Level: 30 dBm
    ▶ Country Info: First Channel Number: 104, Number of Channels: 1, Maximum Transmit Power Level: 30 dBm
    ▶ Country Info: First Channel Number: 108, Number of Channels: 1, Maximum Transmit Power Level: 30 dBm
    ▶ Country Info: First Channel Number: 112, Number of Channels: 1, Maximum Transmit Power Level: 30 dBm
    ▶ Country Info: First Channel Number: 116, Number of Channels: 1, Maximum Transmit Power Level: 30 dBm

```

Figure 7-3 Country information element in an AP beacon



Figure 7-4 A steel-heavy industrial environment where reflections cause problems

From *Understanding and Troubleshooting Cisco Catalyst 9800 Series Wireless Controller* by Simone Arena, Francisco Sedano Crippa, Nicolas Darchis and Sudha Katgeri(9780137492329) Cisco Press
Copyright© 2023 Cisco Systems, Inc. All rights reserved



Figure 7-5 A heavy door that can cause a lot of signal attenuation and typically breaks roaming



Figure 7-6 An atrium is an open space with no attenuation connecting several floors, a Wi-Fi interference nightmare

Configuration > Radio Configurations > RRM

5 GHz Band 2.4 GHz Band FRA

General Coverage DCA TPC RF Grouping Spatial Reuse

Profile Threshold For Traps

Reset to Defaults

Interference Percentage*	10
Clients*	12
Noise*	-70
Utilization Percentage*	80
Throughput*	1000000

Noise/Interference/Rogue/CleanAir/SI Monitoring Channels ⓘ

Channel List	Country Channels ▾
RRM Neighbor Discover Type	Transparent ▾

Monitor Intervals

Neighbor Packet Frequency (seconds)*	180
Reporting Interval (seconds)*	180
Neighbor Timeout factor*	20

Figure 7-7 Configuring RRM data collection settings

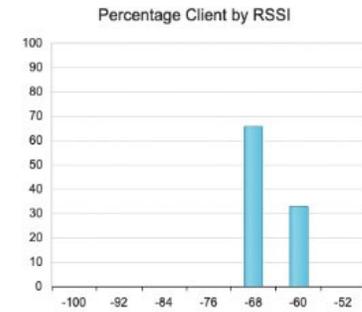
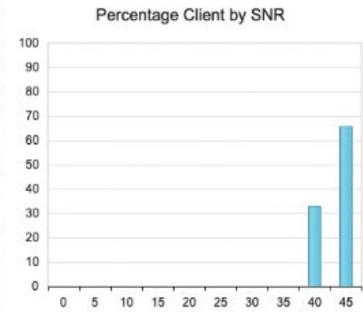
Number of all 5 GHz radios: 3

AP Name	AP Model	Slot No	Base Radio MAC	IP Address	Admin Status	Oper Status
9130- etage	C9130AXI-E	1	488b.0a35.1540	80.201.104.122	✓	
9130- etage	C9130AXI-E	2	488b.0a35.1540	80.201.104.122	⊘	
3700-rez	AIR- CAP3702I- E-K9	1	88f0.3169.d390	80.201.104.122	✓	

10 items per page

5 GHz Band

Client Count : 3



Neighboring APs

Base Radio MAC	Slot No	Channel	Channel Width (MHz)	RF Group Leader	RSSI (dBm)
88f0.3169.d39f	1	100	80	172.31.46.79	-71

10 items per page 1 - 1 of 1 items

Figure 7-8 Monitoring AP neighbors

Restart

Group Mode Automatic Leader Off

Group Role Static-Leader

Group Update Interval 600 second(s)

Group Leader myc9800-CL (172.31.46.79)

Group Members

Total Group Members : 1

Group Name default

Protocol Version 2

+ Add - Delete

Controller Name	IPv4 Address	IPv6 Address	Joined	Join Failure Reason
myc9800-CL	172.31.46.79	::	Yes	N/A

10 items per page

Figure 7-9 RF grouping monitoring and configuration page

Configuration > Radio Configurations > RRM

5 GHz Band 2.4 GHz Band FRA

General Coverage DCA **TPC** RF Grouping Spatial Reuse

Power Assignment Method

Automatic

On Demand

Fixed

Max Power Level Assignment*

30

Min Power Level Assignment*

-10

Power Threshold*

-70

TPC Channel Aware

DISABLED

Power Assignment Leader

myc9800-CL (172.31.46.79)

Apply

Transmit Power Update Interval

600 second(s)

Last Run:

43 second(s) ago

Power Neighbor Count:

3

Invoke Power Update Once

Figure 7-10 TPC settings

Configuration > Radio Configurations > RRM

5 GHz Band

2.4 GHz Band

FRA

General

Coverage

DCA

TPC

RF Grouping

Spatial Reuse

Enable Coverage Hole Detection

Data RSSI Threshold*

-80

Voice RSSI Threshold*

-80

Minimum Failed Client per AP*

3

Percent Coverage Exception Level per AP*

25

Voice Packet Count*

100

Data Packet Count*

50

Voice Packet Percentage*

50

Data Packet Percentage*

50

Figure 7-11 Coverage hole detection algorithm settings

Configuration > Radio Configurations > RRM

5 GHz Band 2.4 GHz Band FRA

General Coverage **DCA** TPC RF Grouping Spatial Reuse

Dynamic Channel Assignment Algorithm

Channel Assignment Mode

Automatic

Freeze Invoke Channel Update Once

Off

Interval

Anchortime

Avoid Foreign AP Interference

Avoid Cisco AP load

Avoid Non 5 GHz Noise

Avoid Persistent Non-wifi Interference

Channel Assignment Leader myc9800-CL (172.31.46.79)

Last Auto Channel Assignment 286 second(s) ago

DCA Channel Sensitivity

Channel Width 20 MHz 40 MHz 80 MHz 160 MHz Best

Dynamic Bandwidth Selection Max Channel Width 20 MHz 40 MHz 80 MHz Max Allowed

Figure 7-12 DCA settings

Configuration > Wireless > Access Points

> All Access Points

5 GHz Radios

Number of AP(s): 3

AP Name	Slot No	Base Radio MAC	Admin Status	Operation Status	Policy Tag	Site Tag	RF Tag	Channel	Power Level
9130-etage	1	488b.0a35.1540	✓	⬆️	NicoHouseEtage	Nicohouse	NicehouseRF	(64,60,52,56)	*1/7 (16 dBm)
9130-etage	2	488b.0a35.1540	⊘	⬇️	NicoHouseEtage	Nicohouse	NicehouseRF	(36)*	*8/8 (-4 dBm)
3700-rez	1	88f0.3169.d390	✓	⬆️	NicoHouseprod	Nicohouse	NicehouseRF	(100,104,108,112)	*1/6 (17 dBm)

10 items per page

1 - 3 of 3 items

Figure 7-13 Manual channel configuration result

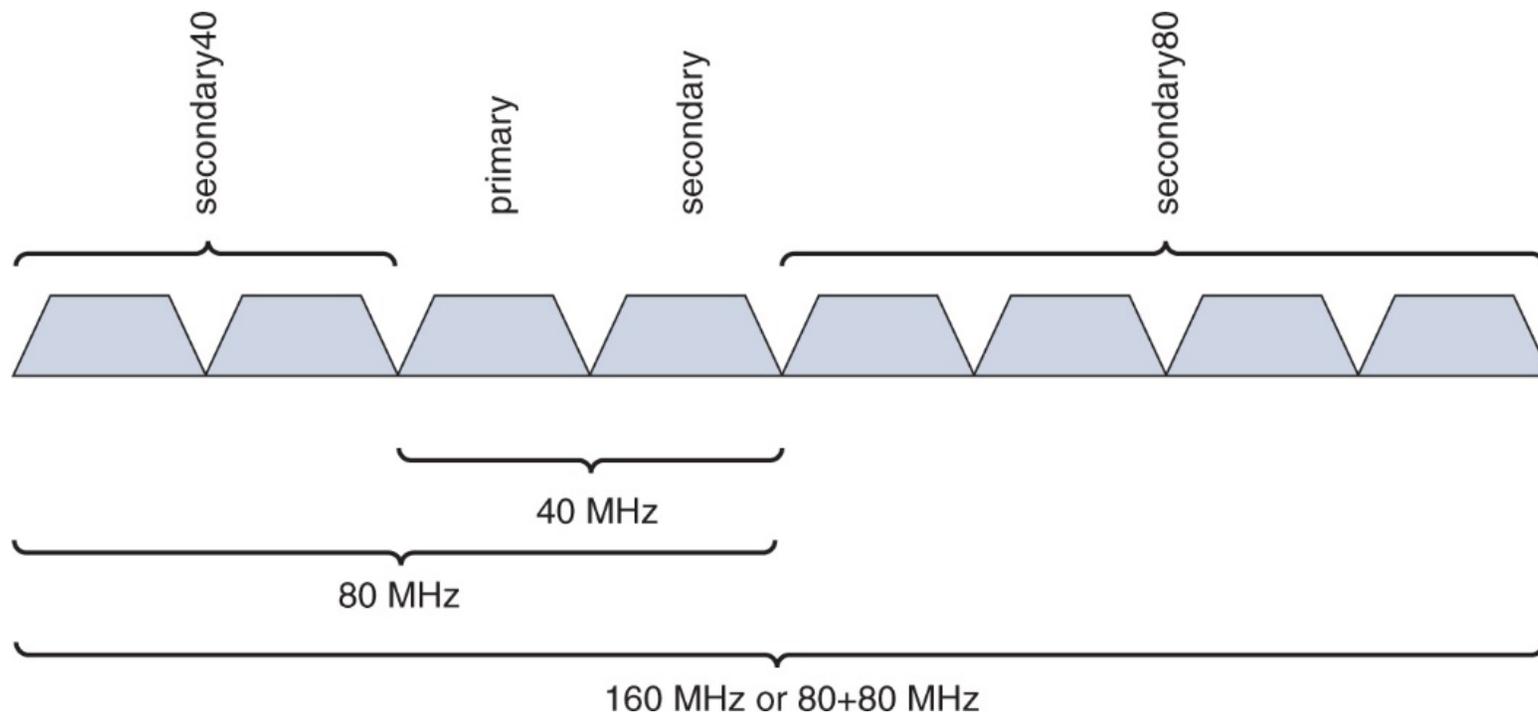


Figure 7-14 Complex primary and secondary channel plans for various channel widths

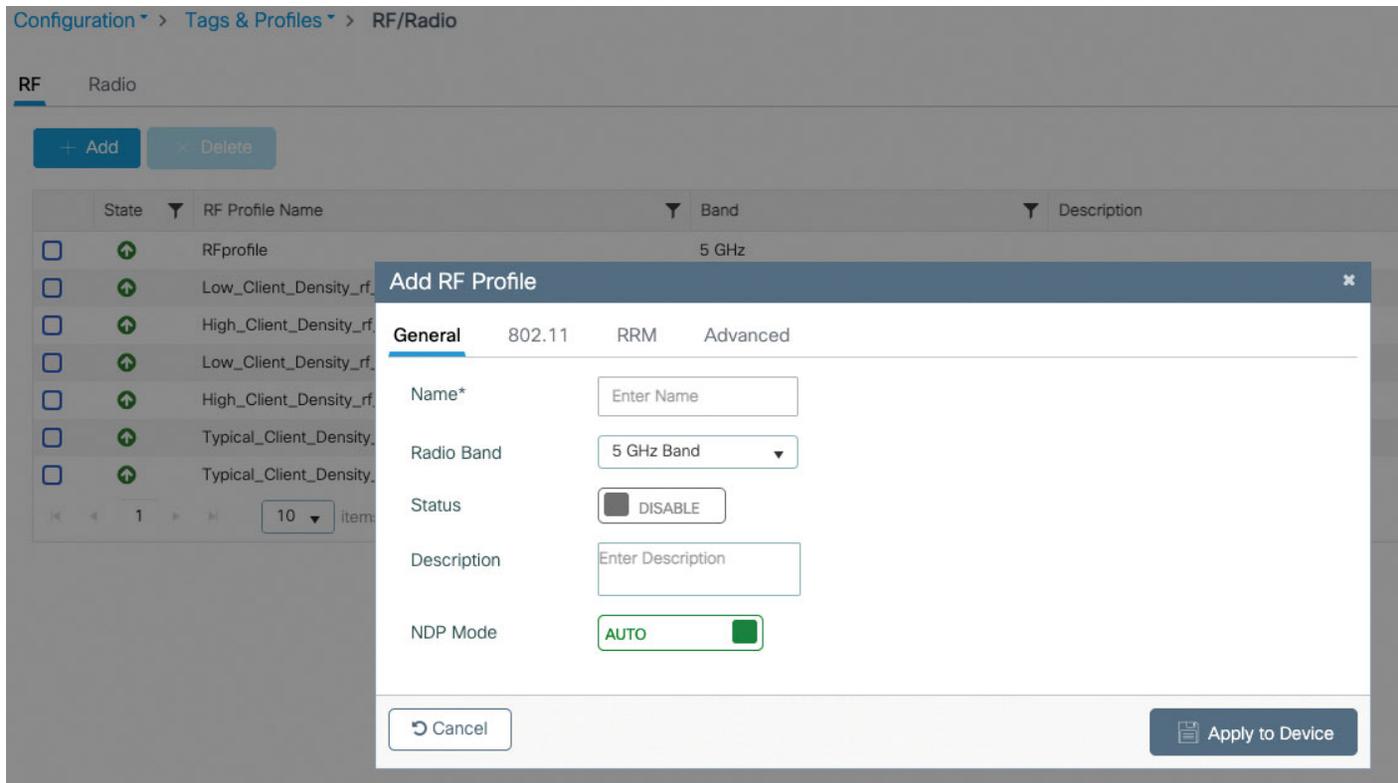


Figure 7-15 RF profile general configuration

Configuration > Tags & Profiles > RF/Radio

RF Radio

+ Add - Delete

State	RF Profile Name	Band
<input type="checkbox"/>	RFprofile	5 GHz
<input type="checkbox"/>	Low_Client_Density_rf_5gh	5 GHz
<input type="checkbox"/>	High_Client_Density_rf_5gh	5 GHz
<input type="checkbox"/>	Low_Client_Density_rf_24gh	2.4 GHz
<input type="checkbox"/>	High_Client_Density_rf_24gh	2.4 GHz
<input type="checkbox"/>	Typical_Client_Density_rf_5gh	5 GHz
<input type="checkbox"/>	Typical_Client_Density_rf_24gh	2.4 GHz

1 10 items per page

Edit RF Profile

⚠ Changes may result in loss of connectivity for clients that are associated to APs with this profile.

General **802.11** RRM Advanced

Operational Rates

6 Mbps

9 Mbps

12 Mbps

18 Mbps

24 Mbps

36 Mbps

48 Mbps

54 Mbps

802.11n MCS Rates

Enabled Data Rates:

[0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31]

Enable	MCS Index
<input checked="" type="checkbox"/>	0
<input checked="" type="checkbox"/>	1
<input checked="" type="checkbox"/>	2
<input checked="" type="checkbox"/>	3
<input checked="" type="checkbox"/>	4
<input checked="" type="checkbox"/>	5
<input checked="" type="checkbox"/>	6
<input checked="" type="checkbox"/>	7
<input checked="" type="checkbox"/>	8
<input checked="" type="checkbox"/>	9

1 2 3 4

10 items per page

1 - 10 of 32 items

Figure 7-16 RF profile configuration

General 802.11 **RRM** Advanced

General Coverage TPC **DCA**

Dynamic Channel Assignment

Avoid AP Foreign AP Interference

Channel Width 20 MHz 40 MHz 80 MHz 160 MHz
 Best

DCA Channels 36 40 44 48 52 56
 60 64 100 104 108 112
 116 120 124 128 132 136
 140

High Speed Roam

Mode Enable

Neighbor Timeout*

Client Network Preference

Figure 7-17 RF profile DCA configuration

Edit RF Profile

General 802.11 RRM **Advanced**

High Density Parameters

Max Clients*

Multicast Data Rate (Mbps)

Rx Snp Threshold (dbm)

Client Distribution

Load Balancing Window*

Load Balancing Denial Count*

ATF Configuration

Status DISABLED

Bridge Client Access DISABLED

Airtime Allocation

FRA

Client Aware

11ax Parameters

OBSS PD DISABLED

Non-SRG OBSS PD Max Threshold (dBm)

Figure 7-18 RF profile advanced configuration

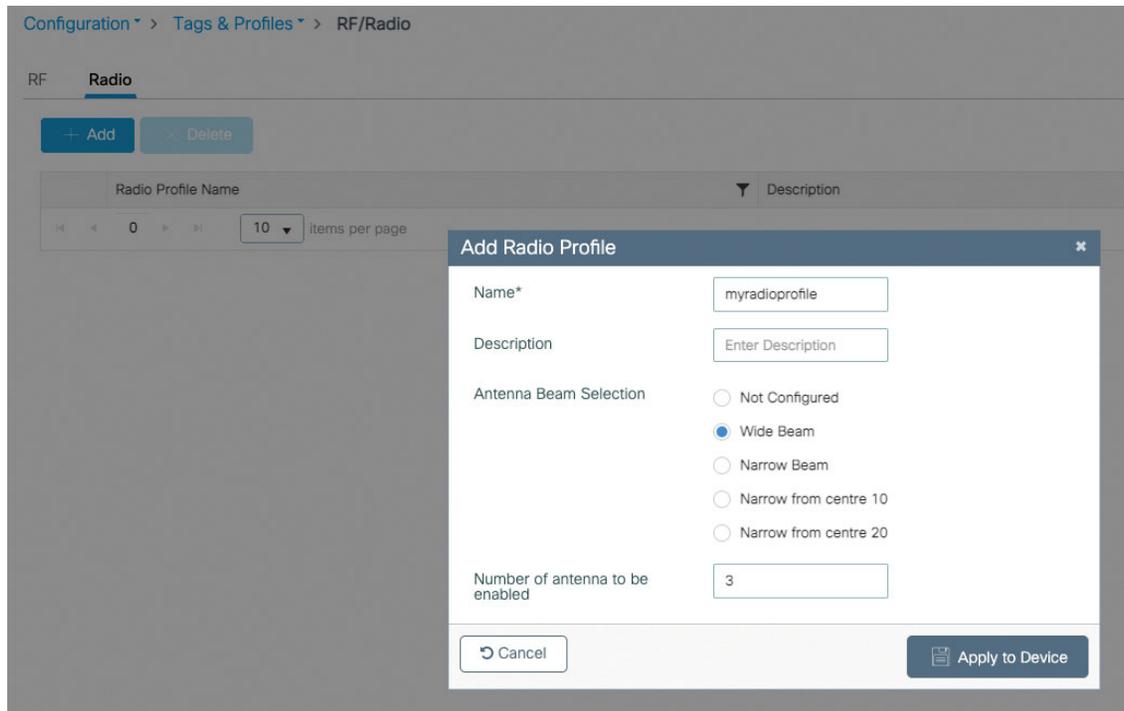


Figure 7-19 Radio profile configuration

Add RF Tag ✕

Name*	<input type="text" value="Enter Name"/>
Description	<input type="text" value="Enter Description"/>
5 GHz Band RF Profile	<input type="text" value="Global Config"/> ▼
2.4 GHz Band RF Profile	<input type="text" value="Global Config"/> ▼
5 GHz Slot 1 Radio Profile	<input type="text" value="myradioprofile"/> ▼
5 GHz Slot 2 Radio Profile	<input type="text" value="Search or Select"/> ▼
2.4 GHz Slot 0 Radio Profile	<input type="text" value="Search or Select"/> ▼

Figure 7-20 RF tag configuration

Monitoring > Wireless > CleanAir Statistics

5 GHz Band **2.4 GHz Band**

Interference Devices Air Quality Report Worst Air Quality Report

AP Name	Interferer Type	Affected Channel	Severity	Duty Cycle	RSSI	Device ID	Cluster ID
3700-rez	BT Link	1	3	1	-76	0xee34	dd00.0000.0a59
3700-rez	BT Link	1	--	1	-78	0xee36	dd00.0000.0a5b
3700-rez	BT Discovery	1	5	2	-75	0xee37	dd00.0000.0a5c

10 items per page 1 - 3 of 3 items

Figure 7-21 2.4 GHz CleanAir Interferer device report

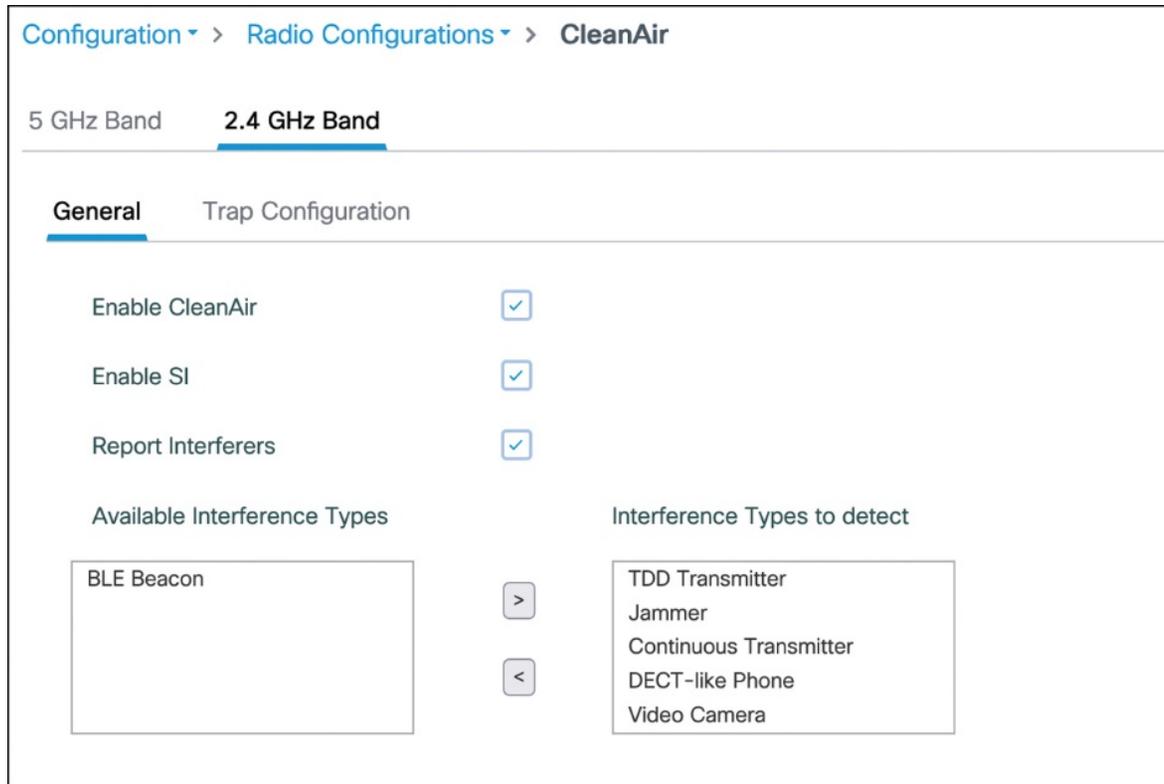


Figure 7-22 The CleanAir configuration page

Configuration > Wireless > Access Points > Edit AP

▼ All Access Points
Number of AP(s): 2

AP Name	AP Model	Slots	Admin Status
9130-etage	C9130AXI-E	3	✓
3700-rez	AIR-CAP3702I-E-K9	2	✓

10 items per page

- 5 GHz Radios
- 2.4 GHz Radios
- Dual-Band Radios
- Country

General | Interfaces | High Availability | Inventory | ICap | Advanced | Support Bundle

General		Version	
AP Name*	9130-etage	Primary Software Version	17.3.3.26
Location*	etage	Predownloaded Status	N/A
Base Radio MAC	488b.0a35.1540	Predownloaded Version	N/A
Ethernet MAC	70f0.960a.6470	Next Retry Time	N/A
Admin Status	ENABLED	Boot Version	1.1.2.4
AP Mode	Flex	IOS Version	17.3.3.26
Operation Status	Registered	Mini IOS Version	0.0.0.0
Fabric Status	Disabled	IP Config	
LED State	DISABLED	CAPWAP Preferred Mode	IPv4
LED Brightness Level	8	DHCP IPv4 Address	91.181.218.194
CleanAir NSI Key	40690a9b090004ed0025010e0a0a001c	Static IP (IPv4/IPv6)	<input type="checkbox"/>

Figure 7-23 Obtaining the CleanAir key for a given AP

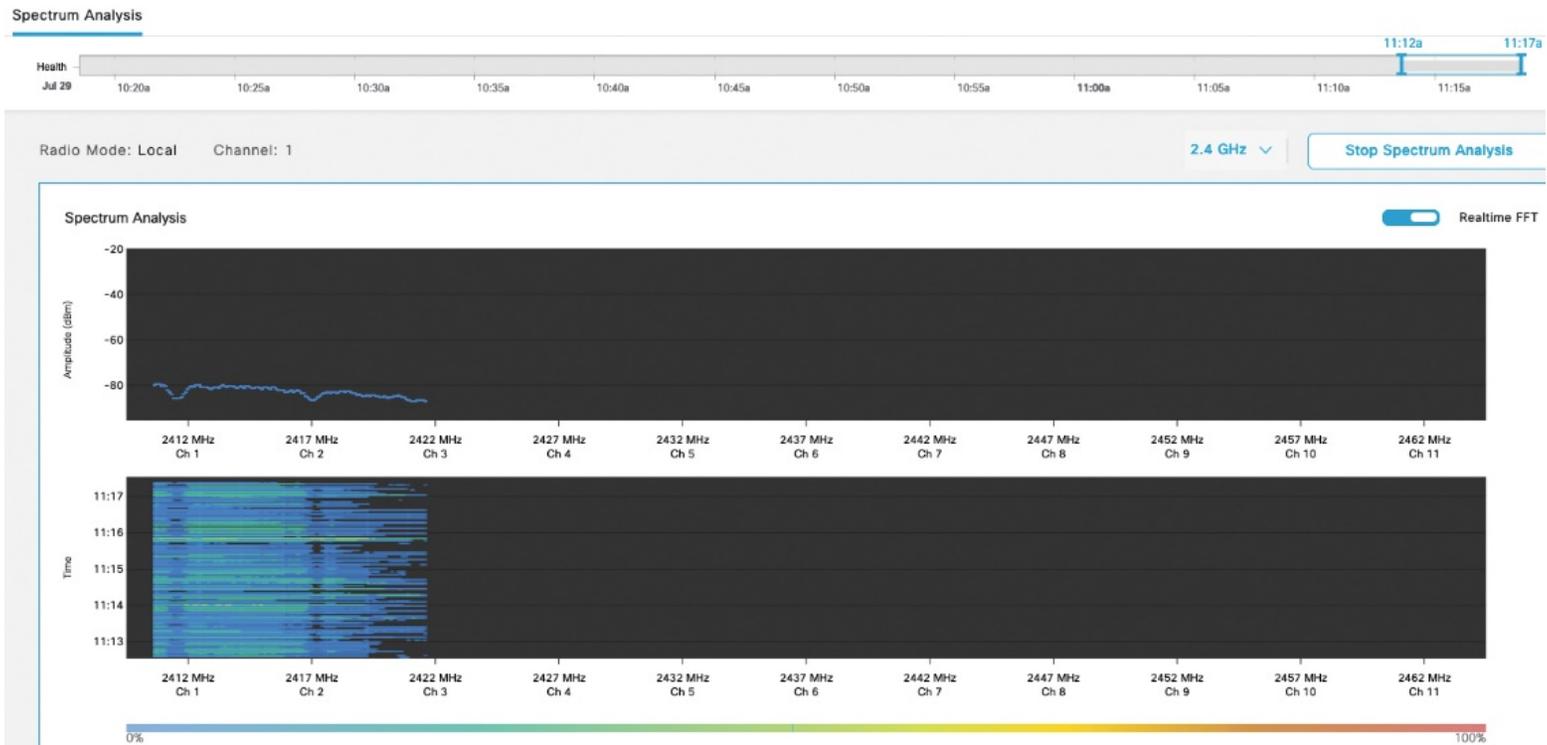


Figure 7-24 Cisco DNA Center spectrum live view

	Slot 0 (2.4 GHz)	Slot 1 (5 GHz)
Radio Type	802.11ax - 2.4 GHz	802.11ax - 5 GHz
Radio Role	Remote	Remote
Admin Status	Enabled	Enabled
Number of Clients	3	2
Current Channel	6	64
Power Level ⓘ	*3/8 (9 dBm)	*1/7 (16 dBm)
Channel Utilization	15%	1%
Transmit Utilization	0%	1%
Receive Utilization	0%	0%

Figure 7-25 Radio statistics of an AP from the C9800 web interface

Configuration > Wireless > Advanced

Show Me How 

Load Balancing

Band Select

Optimized Roaming

High Density

Preferred Calls

RFID

Cellular Steering

Band Select 

Cycle Count*

2

Cycle Threshold (milliseconds)*

200

Age Out Suppression (seconds)*

20

Age Out Dual Band (seconds)*

60

Client RSSI (dBm)*

-80

Client Mid RSSI (dBm)*

-80

Figure 7-26 Band Select global configuration

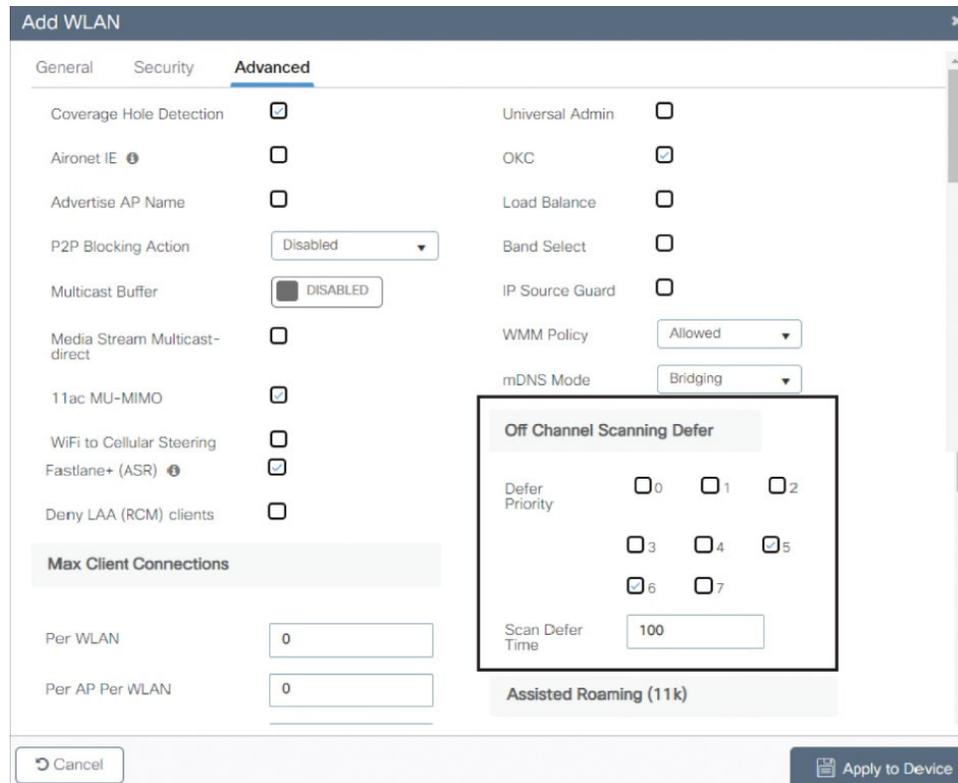


Figure 7-27 Off-Channel Scanning Defer setting

Add WLAN
✕

Configuration of '11v BSS Disassociation Imminent' is supported from Command Line Interface (CLI) only

11ax

- Enable 11ax ⓘ
- Downlink OFDMA
- Uplink OFDMA
- Downlink MU-MIMO
- Uplink MU-MIMO
- BSS Target Wake Up Time

Device Analytics

- Advertise Support
- Advertise PC Analytics Support ⓘ
- Share Data with Client

11k Beacon Radio Measurement
Client Scan Report

- On Association
- On Roam

↶ Cancel

Apply to Device

Figure 7-28 WLAN 11ax features configuration

From *Understanding and Troubleshooting Cisco Catalyst 9800 Series Wireless Controller* by Simone Arena, Francisco Sedano Crippa, Nicolas Darchis and Sudha Katgeri(9780137492329) Cisco Press
Copyright© 2023 Cisco Systems, Inc. All rights reserved

5 GHz Band 2.4 GHz Band

▲ 5 GHz Network is operational. Configuring EDCA Profile and DFS Channel Switch Announcement Mode will result in loss of connectivity of clients.

Help

EDCA Parameters

EDCA Profile

Client Load Based Configuration ENABLED

DFS (802.11h)

▲ DTPC Support is enabled. Please disable it at [Network](#) to configure Power Constraint

Power Constraint*

Channel Switch Status

Channel Switch Announcement Mode

Smart DFS

11ax Parameters

Target Wakeup Time

Target Wakeup Time Broadcast

Multiple Bssid

BSS Color

OBSS PD

Non-SRG OBSS PD Max Threshold (dBm)*

Figure 7-29 Global 11ax features configuration

Configuration > Radio Configurations > RRM

5 GHz Band 2.4 GHz Band FRA

General Coverage DCA TPC RF Grouping **Spatial Reuse**

BSS Color Assignment Mode	Automatic	
BSS Color Assignment Leader*	WLC (192.168.1.133) (2a02:a03f:b00f:3800::c41)	
Last Run*	86 second(s) ago	

Figure 7-30 OBSS coloring configuration

Edit Radios 5 GHz Band

Configure
Detail

<div style="background-color: #f0f0f0; padding: 5px; margin-bottom: 10px;">General</div> <p>AP Name: APA453-0E7B-DBE4</p> <p>Admin Status: ENABLED <input checked="" type="checkbox"/></p> <p>CleanAir Admin Status: ENABLED <input checked="" type="checkbox"/></p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">Antenna Parameters</div> <p>Antenna Type: External</p> <p>Antenna Mode: Omni</p> <p>Self-Identifying Antenna (SIA): Not Present</p> <p>Antenna A: <input checked="" type="checkbox"/></p> <p>Antenna B: <input checked="" type="checkbox"/></p> <p>Antenna C: <input checked="" type="checkbox"/></p> <p>Antenna D: <input checked="" type="checkbox"/></p>	<div style="background-color: #f0f0f0; padding: 5px; margin-bottom: 10px;">RF Channel Assignment</div> <p>Current Channel: 64</p> <p>Channel Width: 40 MHz</p> <p>Assignment Method: Global</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">Tx Power Level Assignment</div> <p>Current Tx Power Level: 1</p> <p>Assignment Method: Global</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">BSS Color</div> <p>BSS Color Configuration: Global</p> <p>BSS Color Status: ENABLED <input checked="" type="checkbox"/></p> <p>Current BSS Color: 44</p>
---	---

Figure 7-31 AP-specific BSS color options

Configuration > Radio Configurations > RRM

5 GHz Band 2.4 GHz Band **FRA**

Flexible Radio Assignment

FRA Status*	<input type="checkbox"/> DISABLED
FRA Interval*	1 Hour ▼
FRA Sensitivity*	medium ▼
Last Run	0 second(s) ago
Last Run Time	0 second(s)
Client Aware	<input type="checkbox"/>
Client Select*	50
Client Reset*	5

Figure 7-32 FRA settings on the Catalyst 9800 controller

Configuration > Radio Configurations > Network

5 GHz Band 2.4 GHz Band

General

5 GHz Network Status

⚠ 5 GHz Network is operational. Configuring Beacon Interval, Fragmentation Threshold, DTPC Support will result in loss of connectivity of clients.

Beacon Interval*

Fragmentation Threshold(bytes)*

DTPC Support

Tri-Radio Mode

Figure 7-33 Global tri-radio setting

Configuration > Wireless > Access Points

> All Access Points

5 GHz Radios

Number of AP(s): 3

AP Name	Slot No	Base Radio MAC	Admin Status
9130-etage	1	488b.0a35.1540	✓
9130-etage	2	488b.0a35.1540	⊘
3700-rez	1	88f0.3169.d390	✓

1 10 items per page

> 2.4 GHz Radios

Edit Radios 5 GHz Band

Configure Detail

General

AP Name: 9130-etage

Admin Status: **ENABLED**

CleanAir Admin Status: **ENABLED**

Global Tri-Radio Mode: **Enabled** ⓘ

Dual Radio Mode: Auto (Disabled) Enabled Disabled

Role Assignment

Assignment Method: Auto (Client Serving) Client Serving Monitor

RF Channel Assignment

Current Channel: 64

Channel Width: 80 MHz

Assignment Method: Custom

Channel Number: 64

Antenna Parameters

Figure 7-34 Global tri-radio setting

Configuration > Security > Wireless Protection Policies

Rogue Policies Rogue AP Rules Client Exclusion Policies

General

Rogue Detection Security Level:

Expiration timeout for Rogue APs (seconds)*:

Validate Rogue Clients against AAA:

Validate Rogue APs against AAA:

Rogue Polling Interval (seconds):

Detect and Report Adhoc Networks:

Rogue Detection Client Number Threshold*:

Rogue Init Timer (seconds)*:

AP Authentication:

AP Authentication Alarm Threshold*:

Syslog Notification:

Auto Contain

Auto Containment Level:

Auto Containment only for Monitor Mode APs:

Using our SSID:

Valid client on Rogue AP:

Adhoc Rogue AP:

MFP Configuration

Global MFP State:

AP Impersonation Detection:

MFP Key Refresh Interval (hours)*:

[Apply](#)

Figure 7-35 Rogue detection settings

Add Rogue AP Rule ✕

Rule Name*

Rule Type

State

Figure 7-36 A friendly rogue AP rule

Edit Rogue AP Rule

Rule Name*	<input style="width: 90%;" type="text" value="evil"/>	
Rule Type	<input style="width: 90%;" type="text" value="Malicious"/>	
State	<input style="width: 90%;" type="text" value="Contain"/>	
Match Operation	<input style="width: 90%;" type="text" value="Any"/>	
Enable Rule	<input checked="" type="checkbox"/>	
Add Condition	<input style="width: 90%;" type="text"/>	
Minimum RSSI	<input style="width: 90%;" type="text" value="-80"/>	<input style="background-color: #00a6c9; color: white; padding: 2px 10px; border: none;" type="button" value="× Delete"/>
Manage SSID	<input checked="" type="checkbox"/>	<input style="background-color: #00a6c9; color: white; padding: 2px 10px; border: none;" type="button" value="× Delete"/>
	<input style="width: 90%;" type="text"/>	<input style="width: 30px; height: 20px;" type="button" value="+"/>
User Configured SSID	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div>	<input style="width: 30px; height: 20px;" type="button" value="−"/> <input style="width: 60px; height: 20px;" type="button" value="× Delete"/>

Figure 7-37 A malicious rogue AP rule

Edit AP Join Profile

General Client CAPWAP AP Management **Security** ICap QoS

Rogues

Rogue Detection

Rogue Detection Minimum RSSI

Rogue Detection Transient Interval (seconds)

Rogue Detection Report Interval (seconds)

Rogue Containment Automatic Rate Selection

Auto Containment on FlexConnect Standalone

aWIPS

aWIPS Enable

Figure 7-38 AP join rogue detection settings

Configuration ▾ > Security ▾ > Wireless Protection Policies

Rogue Policies	RLDP	Rogue AP Rules	Client Exclusion Policies
Configure all of these events			<input type="checkbox"/>
Excessive 802.11 Association Failures			<input checked="" type="checkbox"/>
Excessive 802.1X Authentication Failures			<input checked="" type="checkbox"/>
Excessive 802.1X Authentication Timeout			<input checked="" type="checkbox"/>
IP Theft or IP Reuse			<input checked="" type="checkbox"/>
Excessive Web Authentication Failures			<input checked="" type="checkbox"/>

Figure 7-39 Client exclusion policies on the C9800

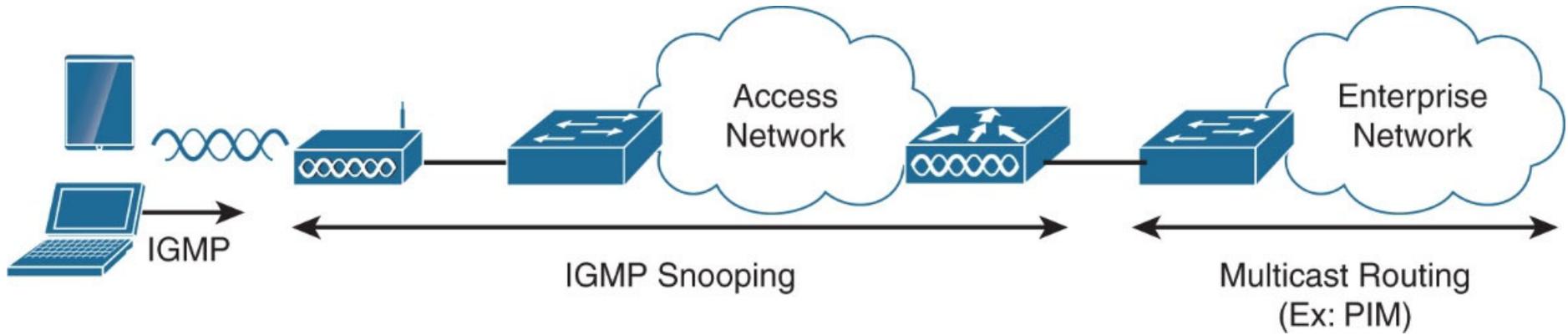


Figure 8-1 Multicast in wireless

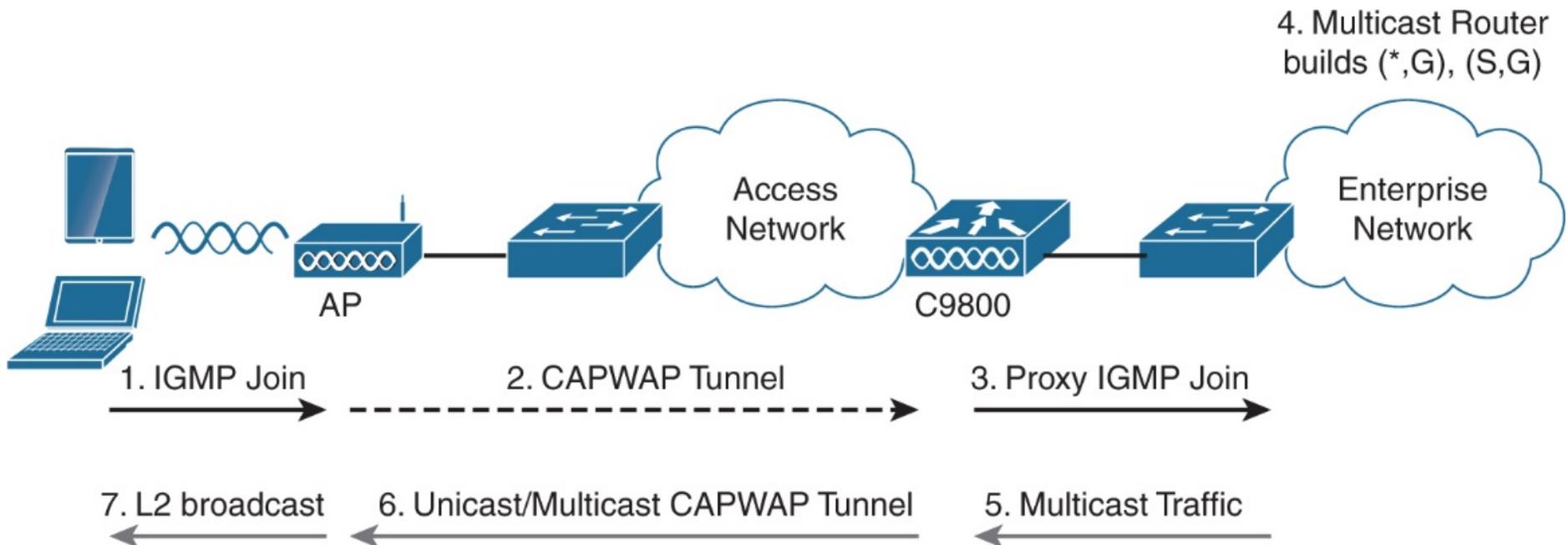


Figure 8-2 Multicast packet flow in wireless

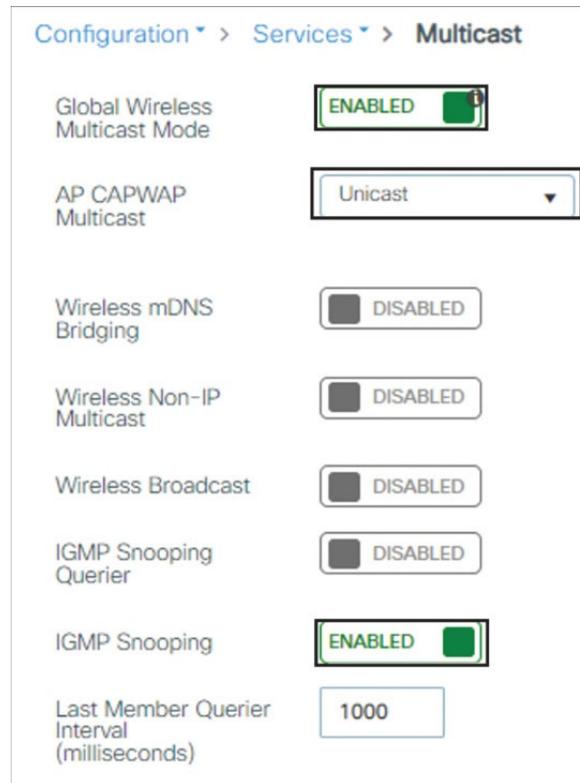


Figure 8-3 Enabling Multicast and MoU/MoM on the C9800

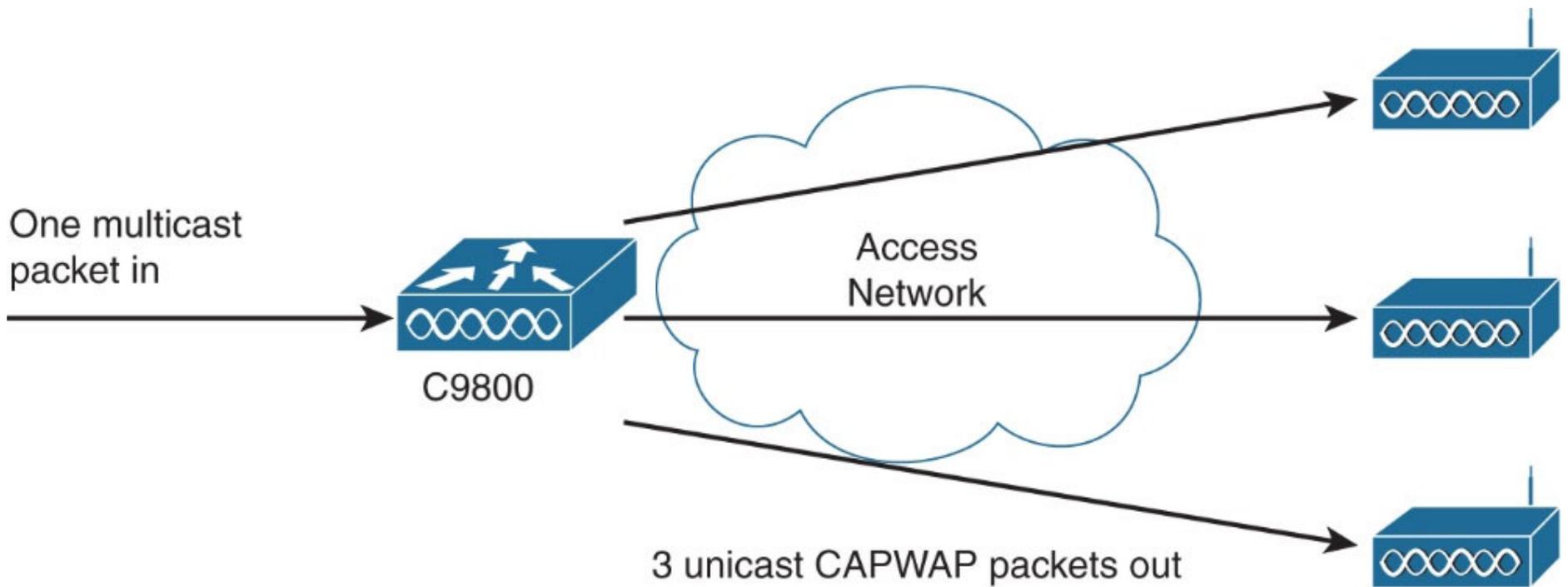


Figure 8-4 MoU: the C9800 creating copies for each multicast packet

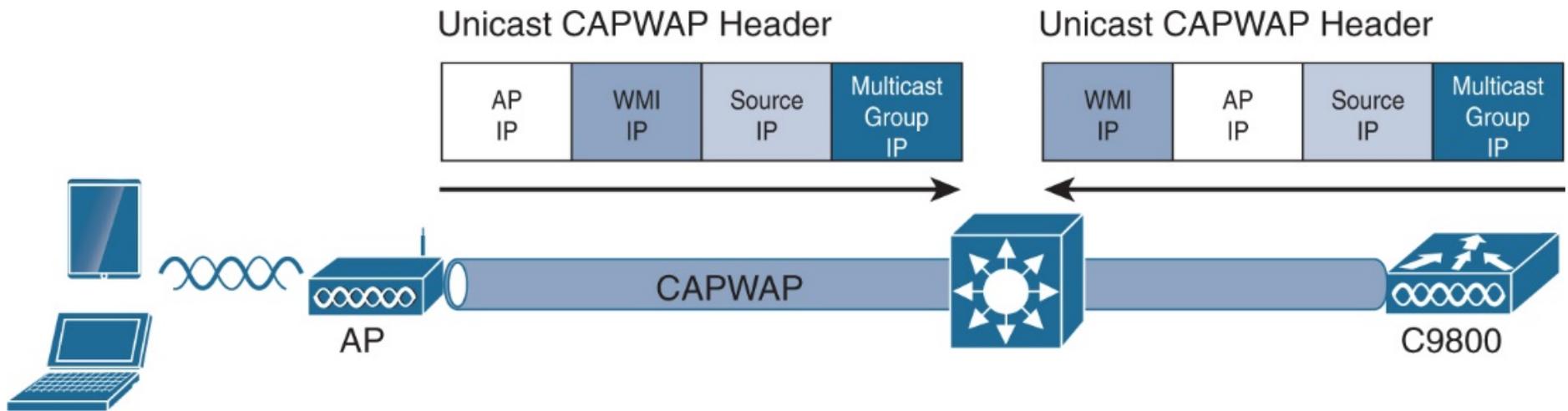


Figure 8-5 Packet format in MoU mode

```
> Frame 284: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits)
> Ethernet II, Src: Cisco_3c:5e:8b (d4:78:9b:3c:5e:8b), Dst: Cisco_b1:6c:c3 (e0:0e:da:b1:6c:c3)
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 10.5.1.11
> User Datagram Protocol, Src Port: 5247, Dst Port: 5248
> Control And Provisioning of Wireless Access Points - Data
> IEEE 802.11 QoS Data, Flags: .....F.
> Logical-Link Control
> Internet Protocol Version 4, Src: 10.15.1.2, Dst: 234.5.6.14
> User Datagram Protocol, Src Port: 8910, Dst Port: 8910
> Data (32 bytes)
```

The diagram shows a network packet structure. Two specific lines are highlighted with black boxes: 'Internet Protocol Version 4, Src: 192.168.1.5, Dst: 10.5.1.11' and 'Internet Protocol Version 4, Src: 10.15.1.2, Dst: 234.5.6.14'. A blue callout box labeled 'Outer CAPWAP Unicast Header' points to the first highlighted line. Another blue callout box labeled 'CAPWAP Payload' points to the second highlighted line.

Figure 8-6 Multicast packet snippet from the C9800 to the AP in MoM mode

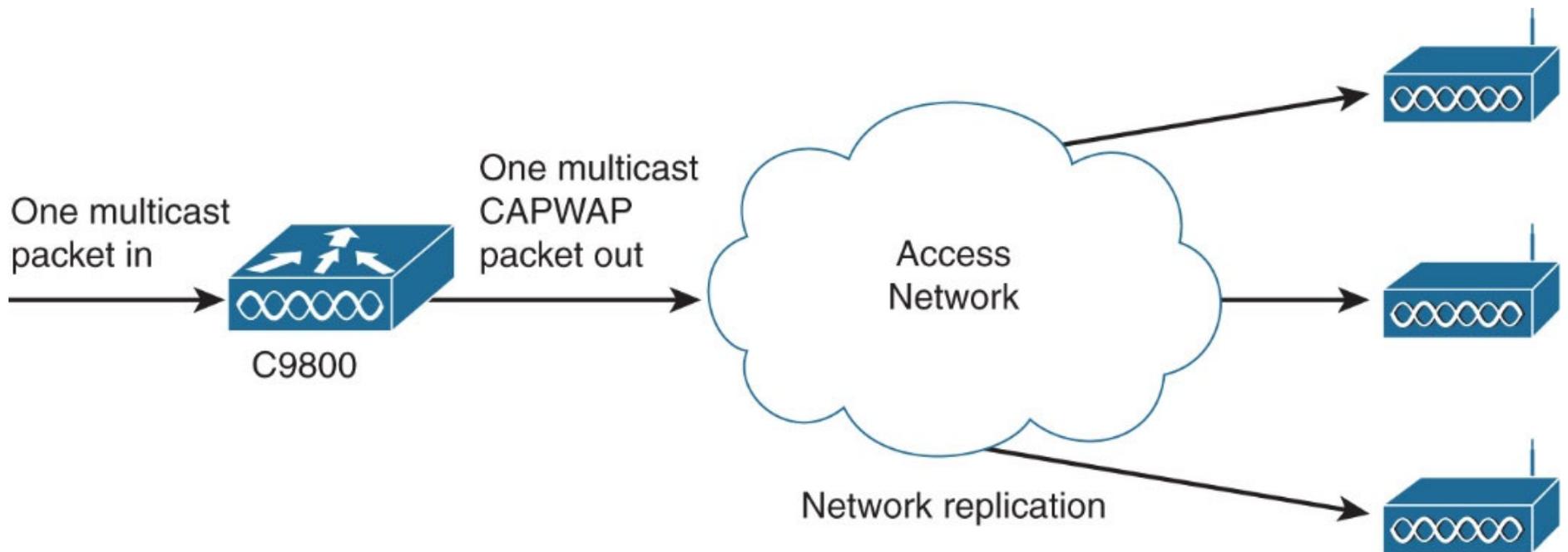


Figure 8-7 MoM: Network creates copies of multicast packets

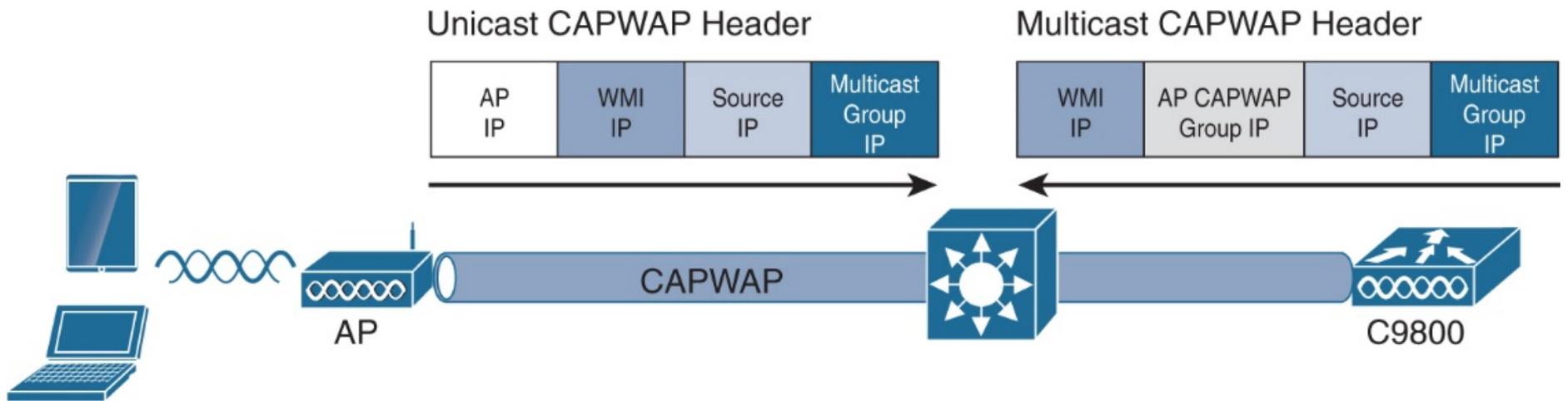


Figure 8-8 Packet format in MoM

```
> Frame 34: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits)
> Ethernet II, Src: Cisco_3c:5e:8b (d4:78:9b:3c:5e:8b), Dst: IPv4mcast_0a:0a:0a (01:00:5e:0a:0a:0a)
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 239.10.10.10
> User Datagram Protocol, Src Port: 5247, Dst Port: 5247
> Control And Provisioning of Wireless Access Points - Data
> IEEE 802.11 QoS Data, Flags: .....F.
> Logical-Link Control
> Internet Protocol Version 4, Src: 10.15.1.2, Dst: 234.5.6.13
> User Datagram Protocol, Src Port: 8910, Dst Port: 8910
> Data (32 bytes)
```

The diagram shows a network packet capture snippet. Two specific lines are highlighted with black boxes and callout arrows pointing to blue labels. The first callout, 'Outer CAPWAP Multicast Header', points to the line: 'Internet Protocol Version 4, Src: 192.168.1.5, Dst: 239.10.10.10'. The second callout, 'CAPWAP Payload', points to the line: 'Internet Protocol Version 4, Src: 10.15.1.2, Dst: 234.5.6.13'.

Figure 8-9 Multicast packet snippet from the C9800 to the AP in MoU mode

Configuration > Services > Multicast

Global Wireless Multicast Mode	<input checked="" type="checkbox"/> ENABLED
AP CAPWAP Multicast	<input type="text" value="Multicast"/>
AP CAPWAP IPv4 Multicast group Address	<input type="text" value="239.10.10.10"/>
AP CAPWAP IPv6 Multicast group Address	<input type="text" value="::"/>
Wireless mDNS Bridging	<input type="checkbox"/> DISABLED
Wireless Non-IP Multicast	<input type="checkbox"/> DISABLED
Wireless Broadcast	<input type="checkbox"/> DISABLED
IGMP Snooping Querier	<input type="checkbox"/> DISABLED
IGMP Snooping	<input checked="" type="checkbox"/> ENABLED
Last Member Querier Interval (milliseconds)	<input type="text" value="1000"/>

Figure 8-10 Configuring MoM on the C9800

Configuration > Tags & Profiles > Policy

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in

General **Access Policies** QOS and AVC Mobility

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification **Disabled** ⓘ

Local Subscriber Policy Name

VLAN

VLAN/VLAN Group

Multicast VLAN

Figure 8-11 Configuring VLAN Select or multicast VLAN on the C9800 wireless policy profile

Configuration > Services > Multicast

Wireless Broadcast and Wireless Non-IP Multicast

+ Add

VLAN ID	Non-IP Multicast	Broadcast
1	Enabled	Enabled
15	Enabled	Enabled
150	Enabled	Enabled
999	Enabled	Enabled
1002	Enabled	Enabled
1003	Enabled	Enabled
1004	Enabled	Enabled
1005	Enabled	Enabled

1 - 8 of 8 items

i In case both Non-IP Multicast and Broadcast are enabled, the VLAN will not list on the table.

Figure 8-12 Default settings of wireless broadcast and non-IP multicast per VLAN when wireless multicast is enabled

Configuration > Services > Multicast

Global Wireless Multicast Mode	<input checked="" type="checkbox"/> ENABLED
AP CAPWAP Multicast	Multicast
AP CAPWAP IPv4 Multicast group Address	239.10.10.10
AP CAPWAP IPv6 Multicast group Address	::
Wireless mDNS Bridging	<input type="checkbox"/> DISABLED
Wireless Non-IP Multicast	<input checked="" type="checkbox"/> ENABLED
Wireless Broadcast	<input checked="" type="checkbox"/> ENABLED
IGMP Snooping Querier	<input type="checkbox"/> DISABLED
IGMP Snooping	<input checked="" type="checkbox"/> ENABLED
Last Member Querier Interval (milliseconds)	1000

Figure 8-13 Configuring wireless broadcast and non-IP multicast forwarding

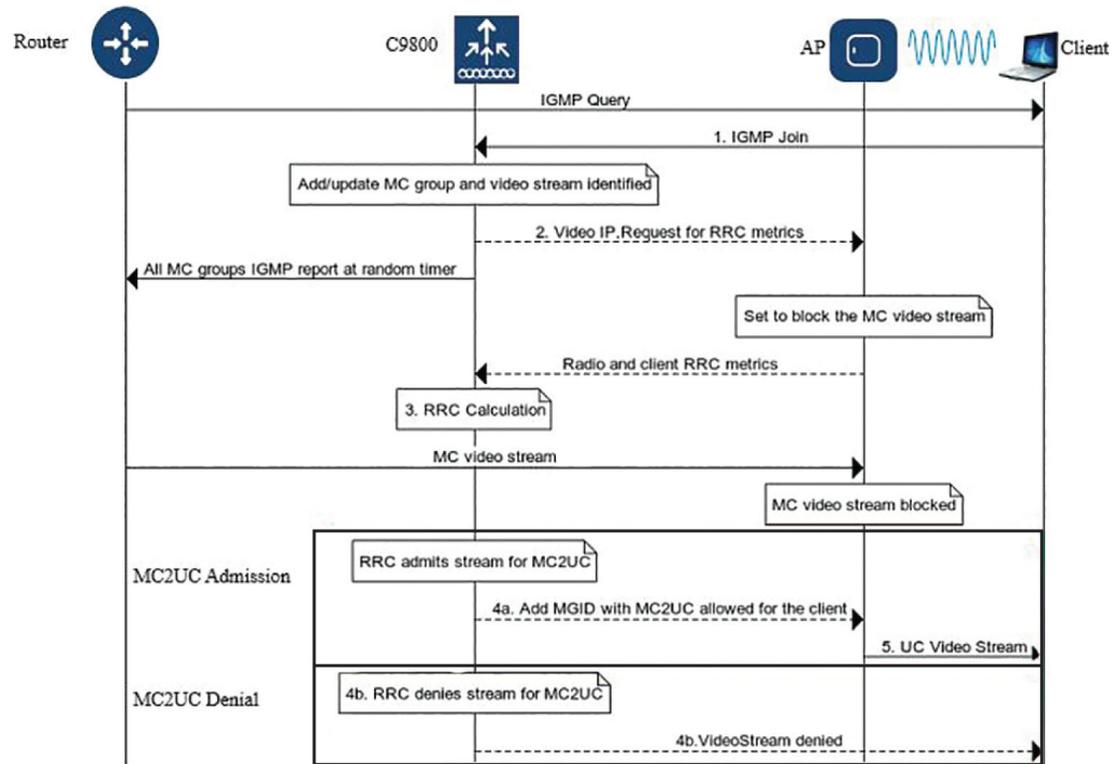


Figure 8-14 Media Stream packet flow

Configuration > Wireless > Media Stream

General Streams

Multicast Direct Enable

Session Message Config

Session Announcement State

Session Announcement URL

Session Announcement Email

Session Announcement Phone

Session Announcement Note

Figure 8-15 Configuring Media Stream globally

Configuration > Wireless > Media Stream

General **Streams**

+ Add Add Media Stream

General

Stream Name*	<input type="text"/>
Multicast Destination Start IPv4/IPv6 Address*	<input type="text"/>
Multicast Destination End IPv4/IPv6 Address*	<input type="text"/>
Maximum Expected Bandwidth (Kbps)*	<input type="text" value="1000"/>

Resource Reservation Control (RRC) Parameters

Average Packet Size*	<input type="text" value="1200"/>
Policy	<input type="text" value="admit"/>
Priority	<input type="text" value="4"/>
QOS	<input type="text" value="Video"/>
Violation	<input type="text" value="Drop"/>

Figure 8-16 Configuring multicast stream details with their characteristics

Configuration > Radio Configurations > Media Parameters

5 GHz Band 2.4 GHz Band

Media

General

Unicast Video Redirect

Multicast Direct Admission Control

Media Stream Admission Control (ACM)

Maximum Media Stream RF bandwidth (%)*

Maximum Media Bandwidth (%)*

Client Minimum Phy Rate (kbps)

Maximum Retry Percent (%)*

Media Stream - Multicast Direct Parameters

Multicast Direct Enable

Max streams per Radio

Max streams per Client

Best Effort QoS Admission

Voice

Call Admission Control (CAC)

Admission Control (ACM)

Traffic Stream Metrics

Metrics Collection

Stream Size*

Max Streams*

Inactivity Timeout

[Apply](#)

Figure 8-17 Configuring Media Stream on 2.4 GHz and 5 GHz bands

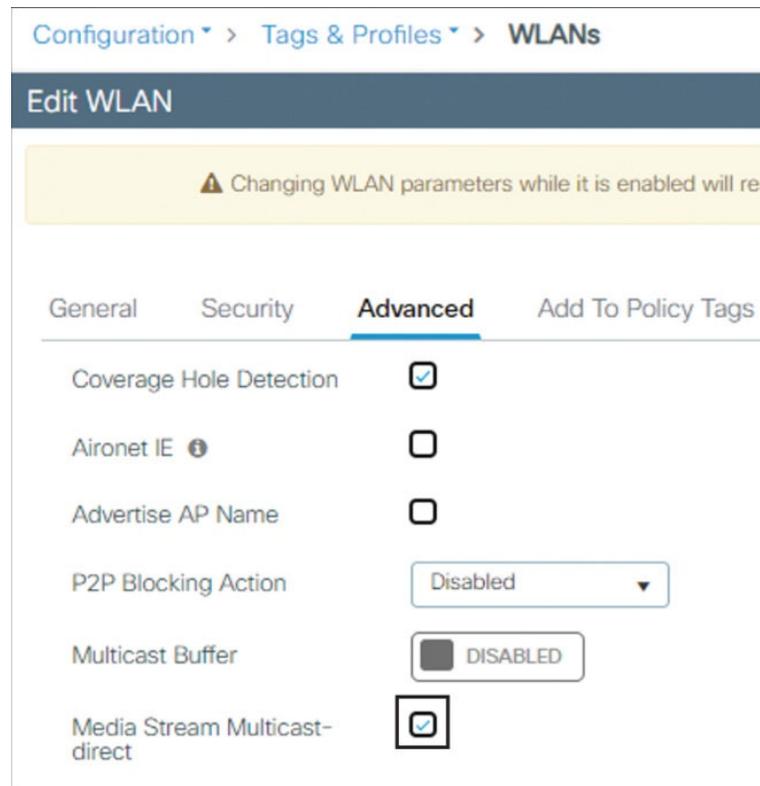


Figure 8-18 Enabling Media Stream on a client WLAN profile

Monitoring > General > Multicast

Layer 2 Layer 3 **Media Stream Clients**

Local Mode Flex Connect Fabric Media Stream

Client MAC	Stream Name	IP Address	AP-Name	Radio	WLAN	QOS	Status
aaaa.bbbb.cccc	video20	239.5.6.20	sudha-9130	2.4 GHz	3	video	Admitted

10 items per page 1 - 1 of 1 items

Figure 8-19 Monitoring a client admitted to the MC2UC Media Stream

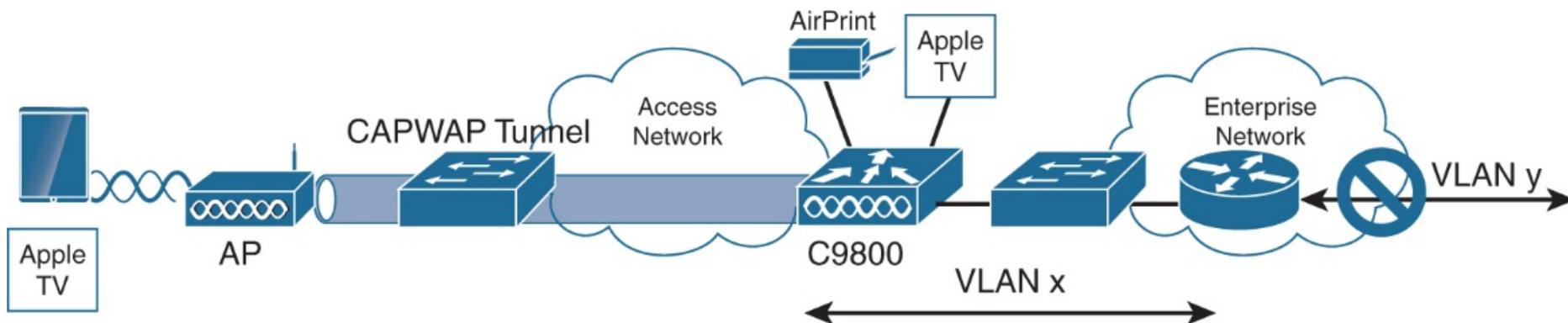


Figure 8-20 Default mDNS bridging in action

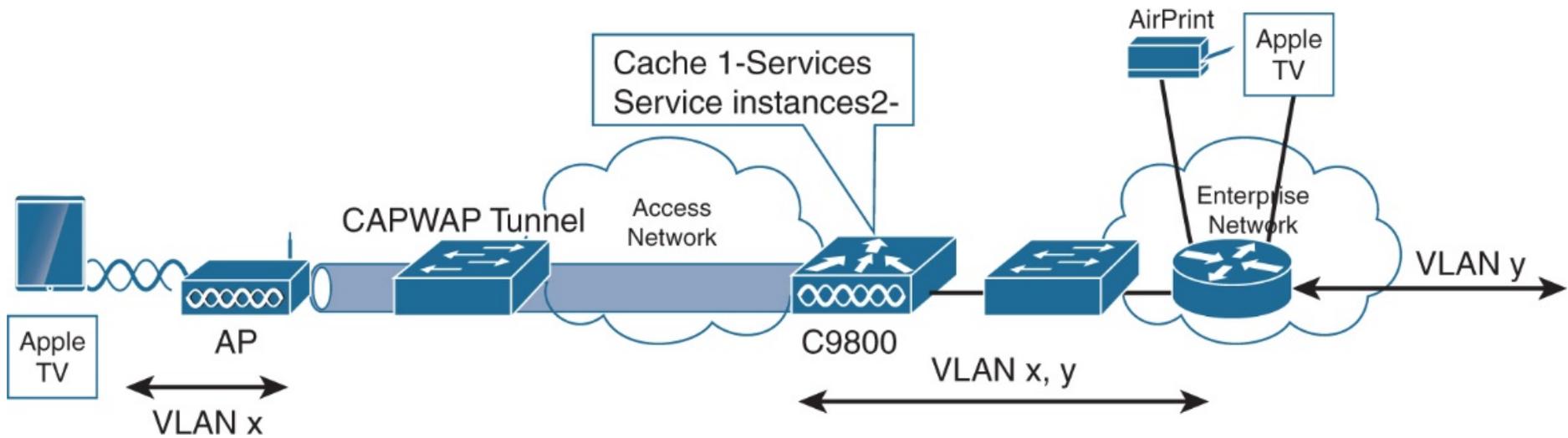


Figure 8-21 mDNS gateway in action

Configuration > Services > mDNS

Global

Service Policy

mDNS Flex Profile

mDNS Gateway

ENABLED

Transport

ipv4 ▼

Active-Query Timer (Minutes) *

30

mDNS-AP Service Policy

default-mdns-ser... ▼

[Clear](#)

Figure 8-22 Configuring the C9800 as mDNS gateway globally

Configuration > Tags & Profiles > WLANs

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General Security **Advanced** Add To Policy Tags

Coverage Hole Detection	<input checked="" type="checkbox"/>	Universal Admin	<input type="checkbox"/>
Aironet IE ⓘ	<input type="checkbox"/>	OKC	<input checked="" type="checkbox"/>
Advertise AP Name	<input type="checkbox"/>	Load Balance	<input type="checkbox"/>
P2P Blocking Action	Disabled ▾	Band Select	<input type="checkbox"/>
Multicast Buffer	DISABLED	IP Source Guard	<input type="checkbox"/>
Media Stream Multicast-direct	<input type="checkbox"/>	WMM Policy	Allowed ▾
11ac MU-MIMO	<input checked="" type="checkbox"/>	mDNS Mode	Gateway ▾

Figure 8-23 Enabling the MDNS gateway on the WLAN

Configuration > Tags & Profiles > Policy

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy

General Access Policies QOS and AVC Mobility **Advanced**

WLAN Timeout		Fabric Profile	<input type="checkbox"/> Search or Select ▼
Session Timeout (sec)	<input type="text" value="1800"/>	Link-Local Bridging	<input type="checkbox"/>
Idle Timeout (sec)	<input type="text" value="300"/>	mDNS Service Policy	default-mDNS-servi ▼ airparrot-policy
Idle Threshold (bytes)	<input type="text" value="0"/>	Hotspot Server	Search or Select ▼
Client Exclusion Timeout	<input checked="" type="checkbox"/> <input type="text" value="60"/>		

Figure 8-24 Configuring an mDNS service policy on a wireless policy profile

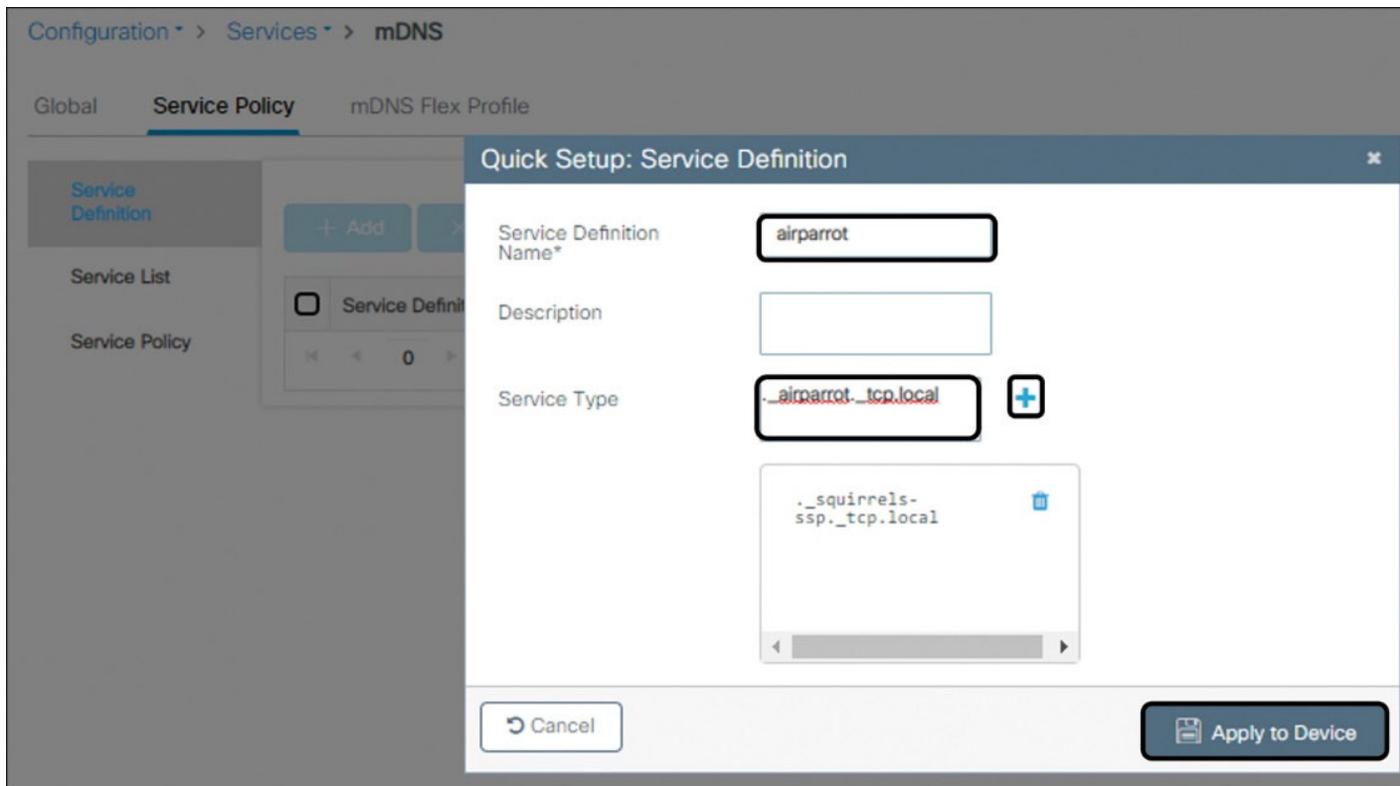


Figure 8-25 Creating a custom service definition

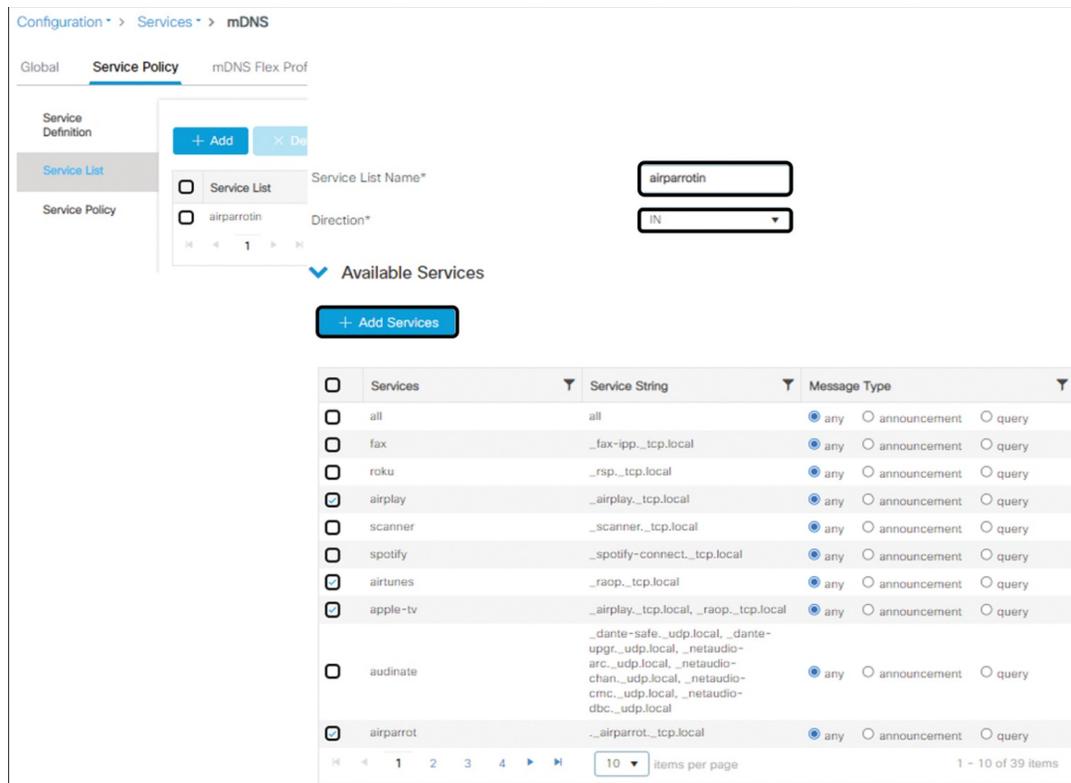


Figure 8-26 Creating a service list mapping custom service definitions and services from the master service list

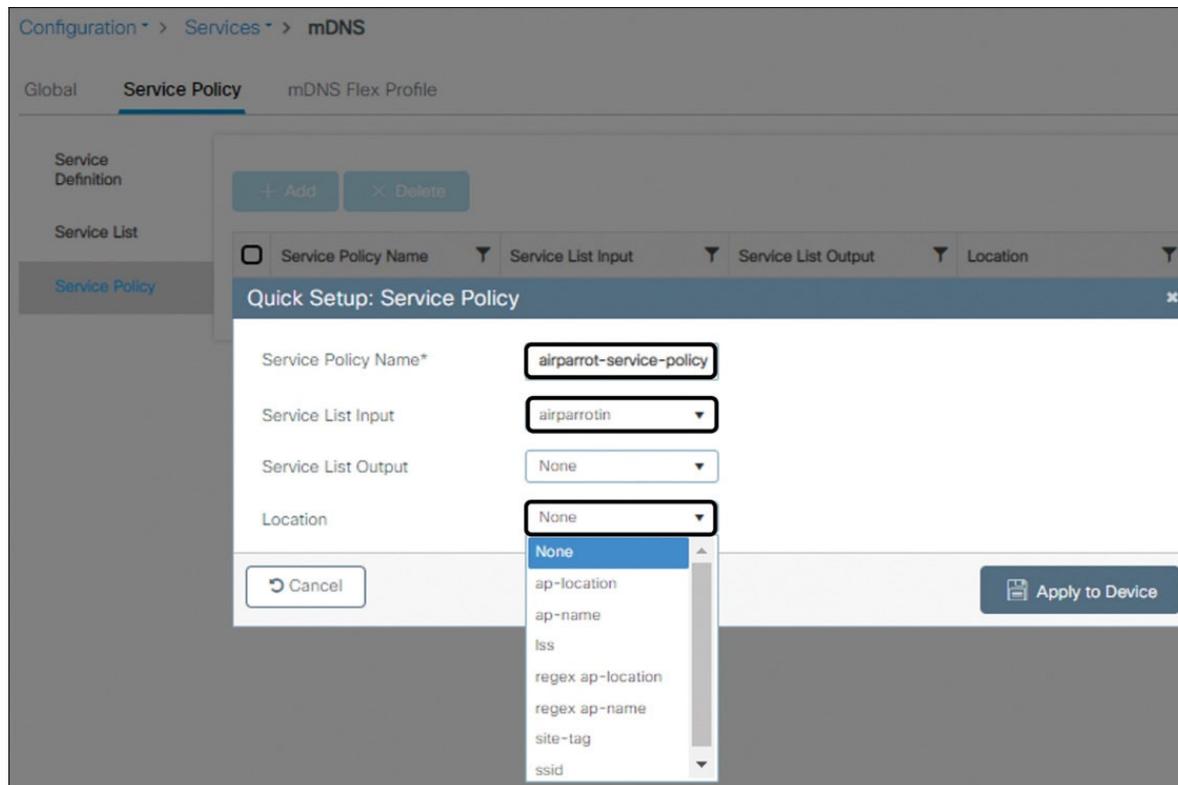


Figure 8-27 Creating a service policy and mapping service filters

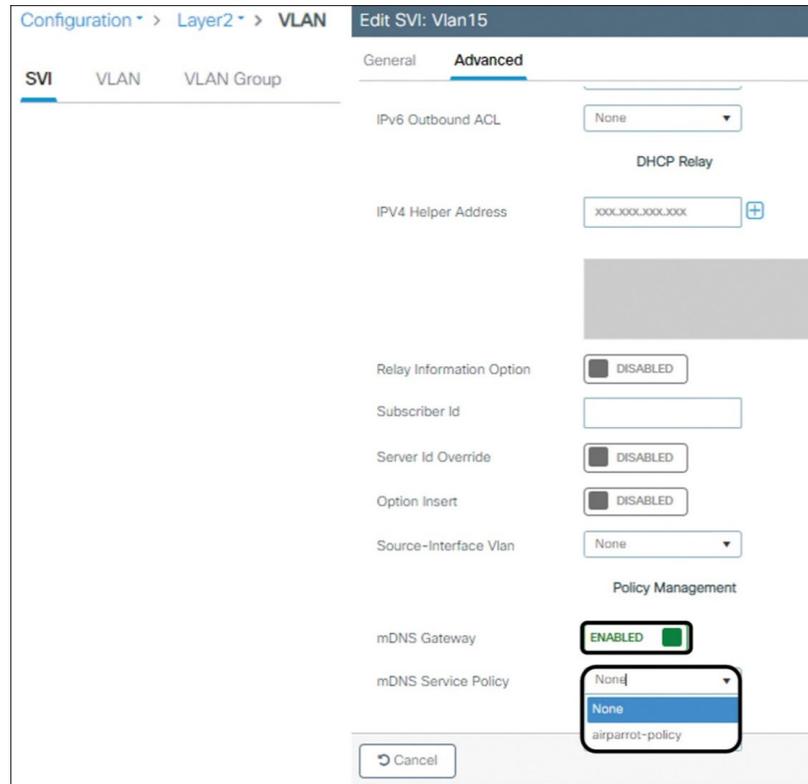


Figure 8-28 Enabling the mDNS gateway on a VLAN SVI

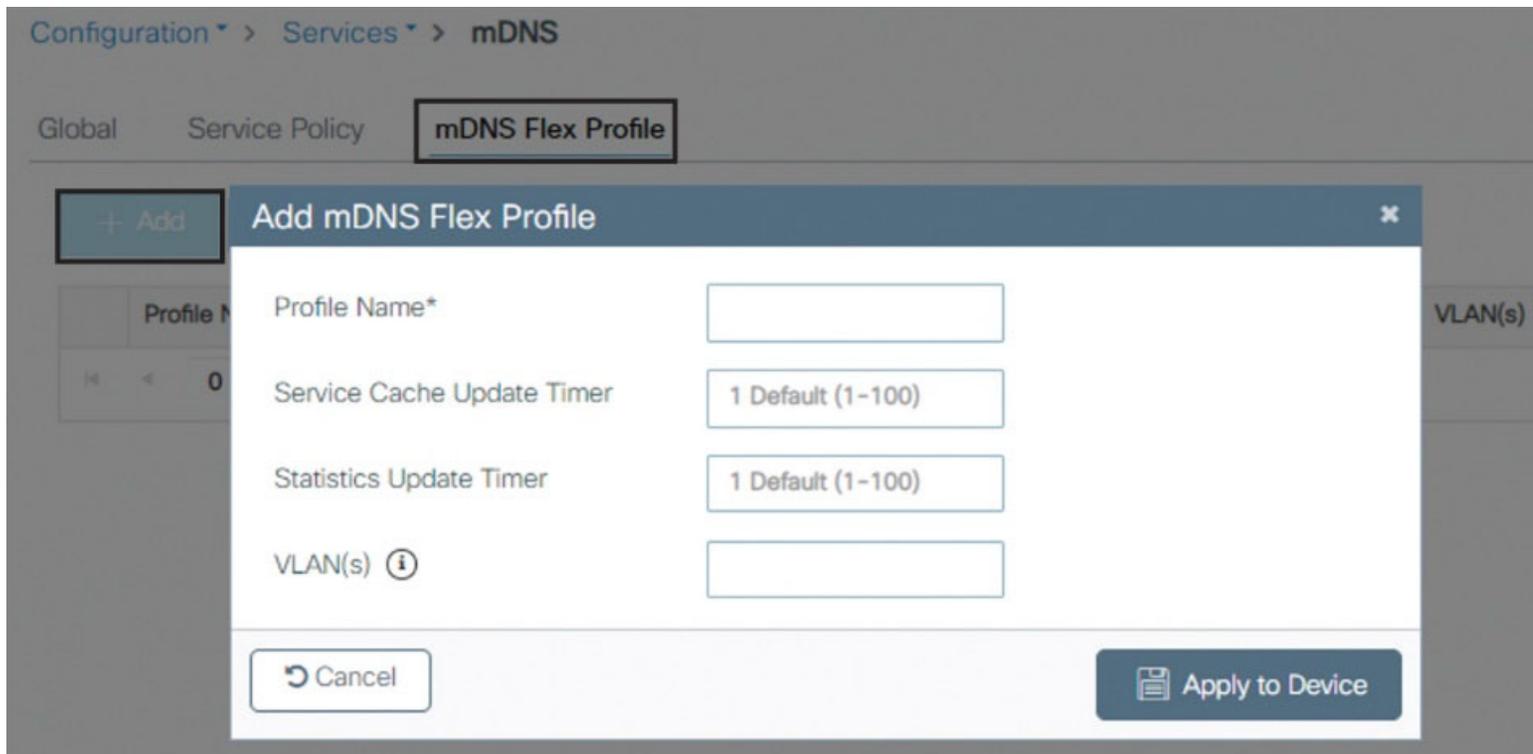


Figure 8-29 Defining an mDNS Flex profile



Figure 9-1 Simplified view on an enterprise network

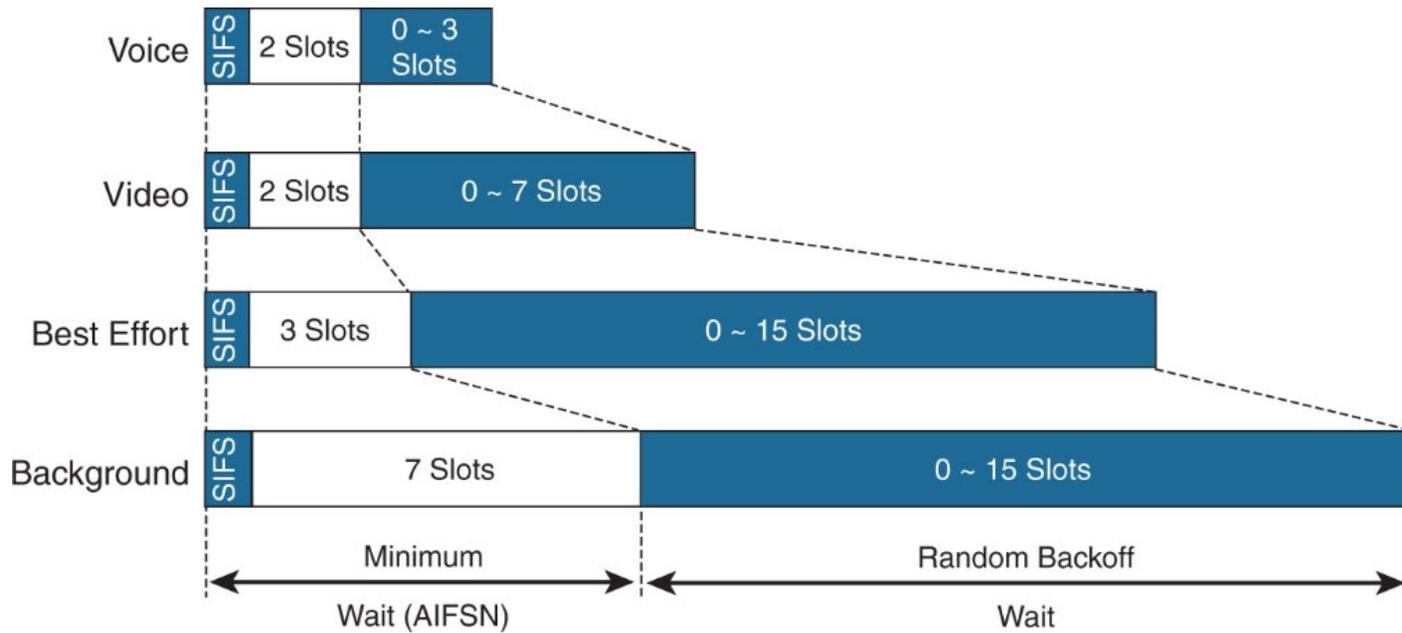


Figure 9-2 EDCA slots for each access category

EDCA/WMM AC	TXOP (μ s)	TXOP (Units)
Voice	2080	65
Video	4096	128
Best Effort	2528	79
Background	2528	79

Figure 9-3 TXOP values for each access category

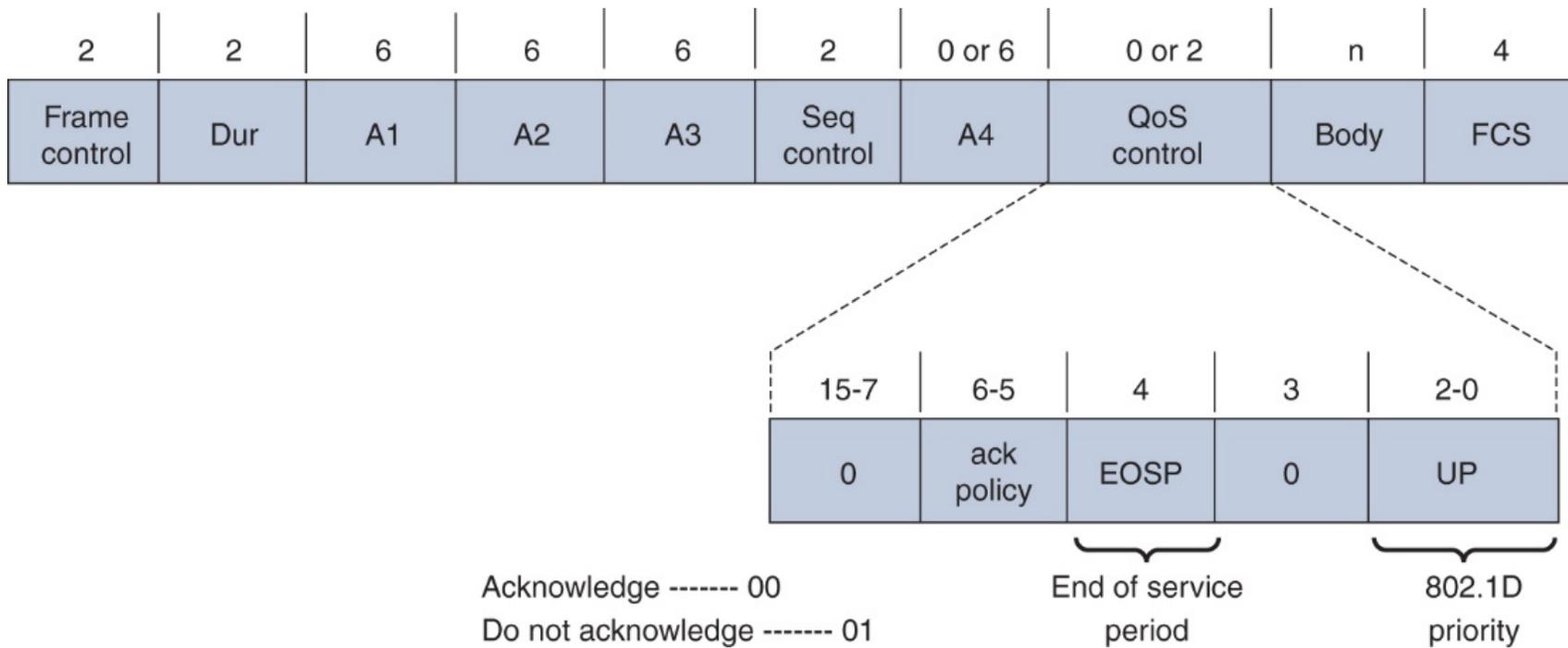


Figure 9-4 The UP (802.1D) bits in the 802.11 header

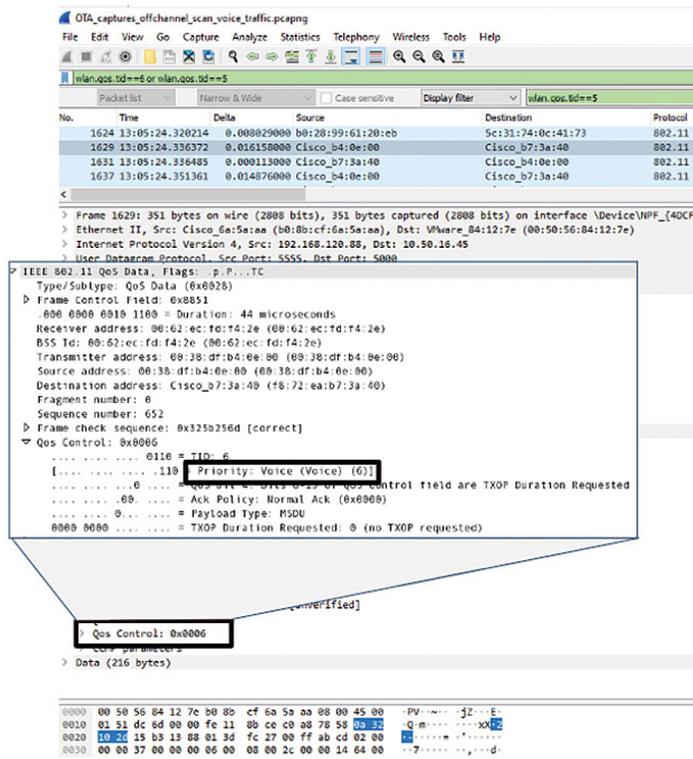


Figure 9-5 The UP value in a real over-the-air capture

Access Category (AC)	UP values
Background (AC_BK)	1,2
Best Effort (AC_BE)	0,3
Video (AC_VI)	4,5
Voice (AC_VO)	6,7

Figure 9-6 Table with UP to Access Categories mapping

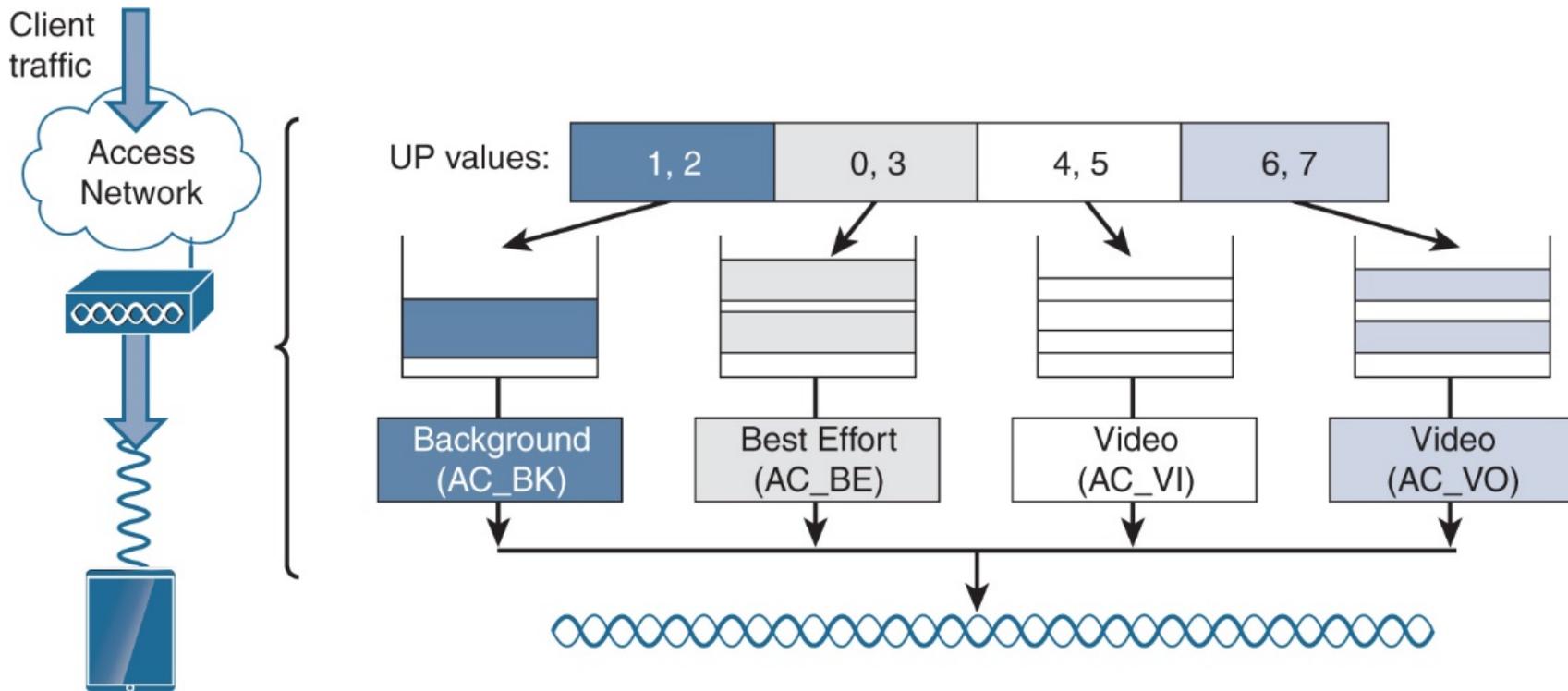


Figure 9-7 Client UP value to queue mapping at the AP

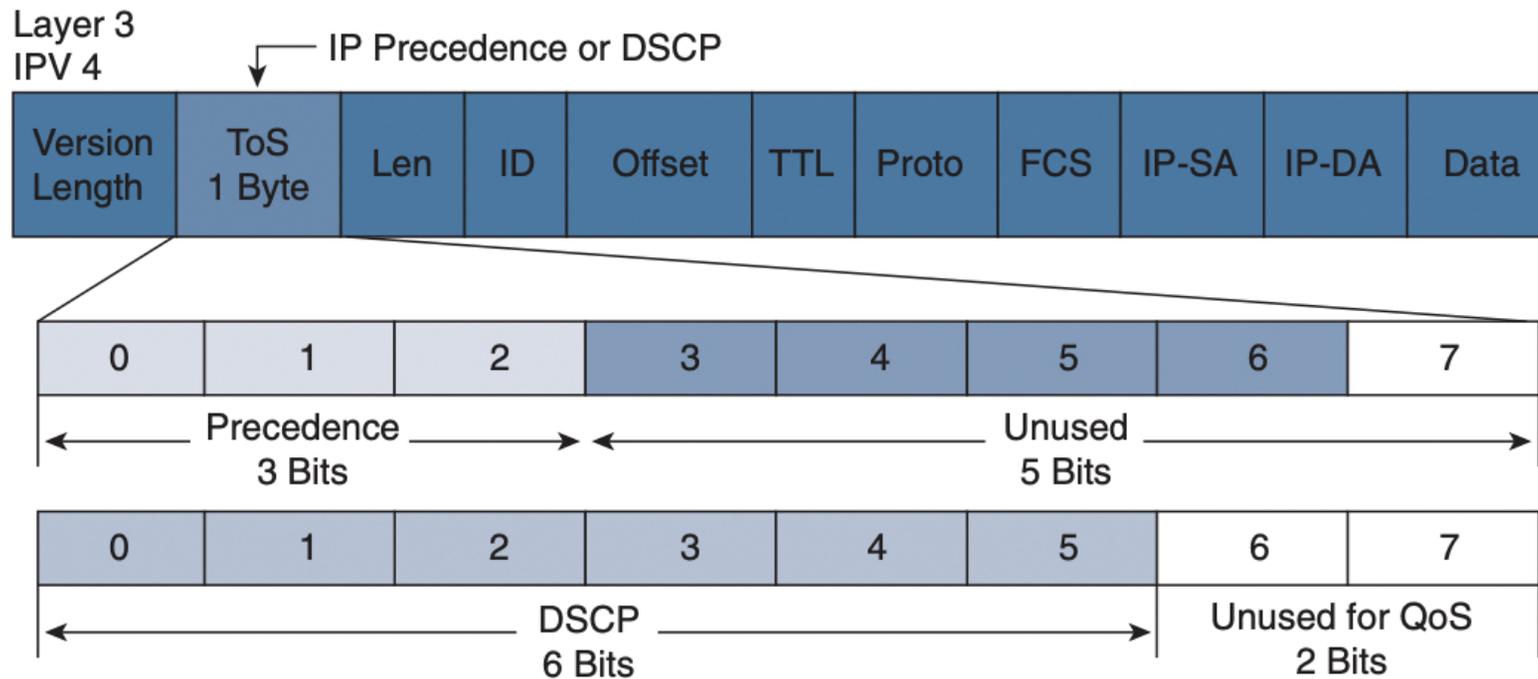
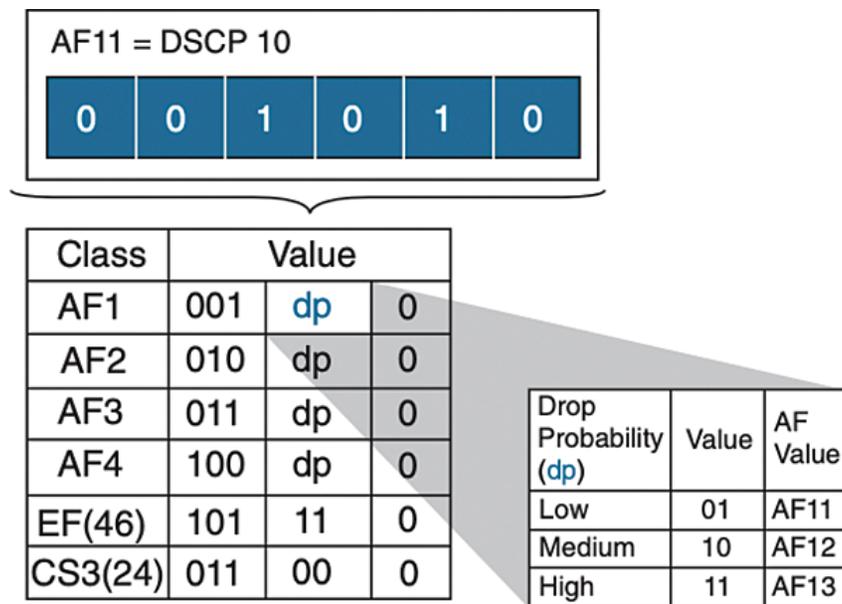


Figure 9-8 DSCP value in the IPv4 header



AF = Assured Forwarding (DSCP 10 to DSCP 38)
 EF = Expedited Forwarding (DSCP 46)
 CS = Class Selector. Used to preserve partial backward compatibility with IP precedence.

Figure 9-9 Class Selector and DP bits

DSCP Class	DSCP (bin)	DSCP (hex)	DSCP (dec)
none	000000	0x00	0
cs1	001000	0x08	8
af11	001010	0x0A	10
af12	001100	0x0C	12
af13	001110	0x0E	14
cs2	010000	0x10	16
af21	010010	0x12	18
af22	010100	0x14	20
af23	010110	0x16	22
cs3	011000	0x18	24
af31	011010	0x1A	26
af32	011100	0x1C	28
af33	011110	0x1E	30
cs4	100000	0x20	32
af41	100010	0x22	34
af42	100100	0x34	36
af43	100110	0x26	38
cs5	100100	0x28	40
ef	101110	0x2E	46
cs6	110000	0x30	48
cs7	111000	0x38	56

Figure 9-10 DSCP classes and the associated values

RFC 4594-Based Model	DSCP
Network Control	(CS7)
Internetwork Control	CS6
Voice + DSCP-Admit	EF +44
Broadcast Video	CS5
Multimedia Conferencing	AF4
Real-time Interaction	CS4
Multimedia Streaming	AF3
Signaling	CS3
Transactional Data	AF2
OAM	CS2
Bulk Data	AF1
Scavenger	CS1
Best Effort	DF

Figure 9-11 DSCP classes and the associated values

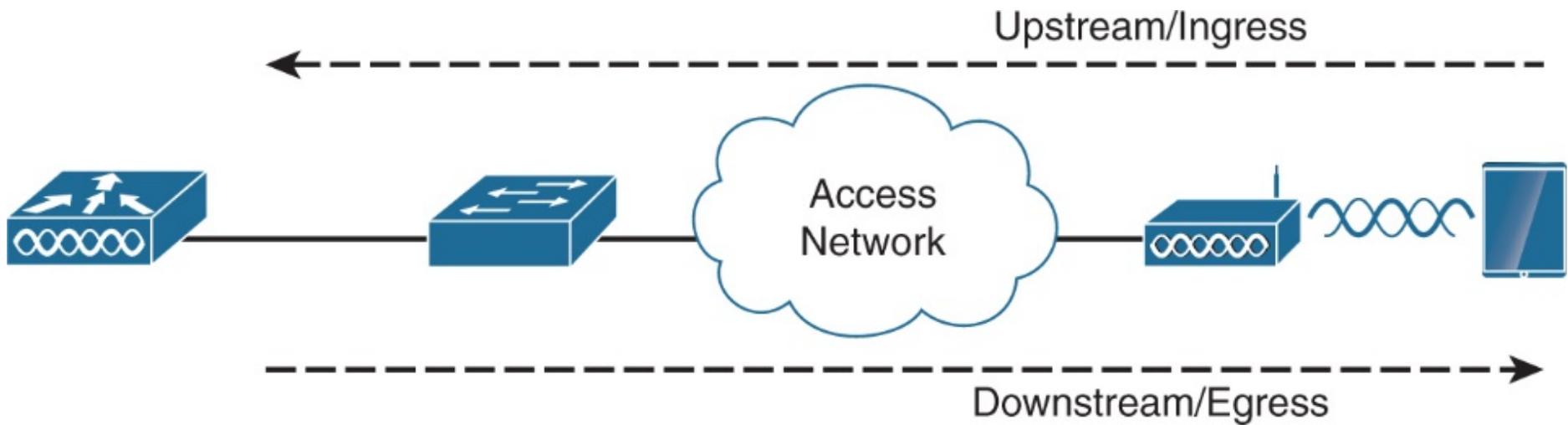


Figure 9-12 Upstream and downstream directions

IETF DiffServ Service Class	DSCP name	DSCP value	UP	Access Category
Network Control (Reserved)	CS7	56	0	AC_BE
Network Control or Internet-work	CS6	48	0	AC_BE
Voice (and Voice-admit)	EF	46, 44	6	AC_VO
Signaling	CS5	40	5	AC_VI
Multimedia Conferencing	AF41,AF42, AF43	34, 36, 38	4	AC_VI
Real-Time Interactive	CS4	32	5	AC_VI
Multimedia Streaming	AF31, AF32, AF33	26, 28, 30	4	AC_VI
Broadcast Video	CS3	24	4	AC_VI
Low-Latency Data	AF21, AF22, AF23	18, 20, 22	3	AC_BE
OAM	CS2	16	0	AC_BE
High-Throughput Data	AF11, AF12, AF13	10, 12, 14	2	AC_BK
Standard	DF (default forwarding)	0	0	AC_BE
Low-Priority Data	CS1	8	1	AC_BK

Figure 9-13 DSCP to UP mapping based on RFC 8325

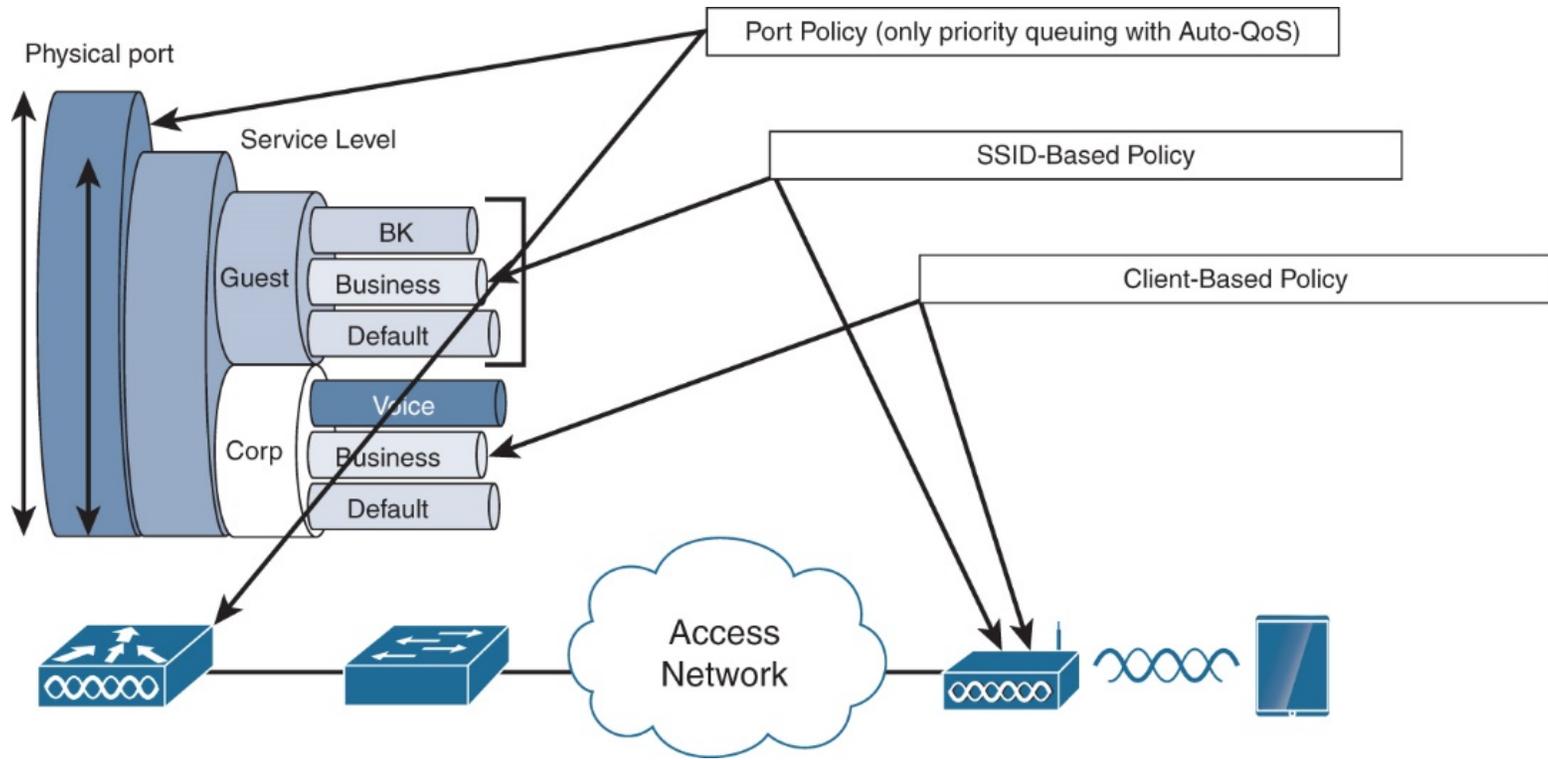


Figure 9-14 QoS policy targets

Classification ACL

```
ip access-list extended AutoQos-4.0-Output-Acl-CAPWAP-C
10 permit udp any eq 5246 16666 any
```

Class-map definition

```
class-map match-any AutoQos-4.0-Output-CAPWAP-C-Class
match access-group name AutoQos-4.0-Output-Acl-CAPWAP-C
class-map match-any AutoQos-4.0-Output-Voice-Class
match dscp ef
```

Policy-map definition

```
policy-map AutoQos-4.0-wlan-Port-Output-Policy
class AutoQos-4.0-Output-CAPWAP-C-Class
priority level 1
class AutoQos-4.0-Output-Voice-Class
priority level 2
class class-default
```

Service-policy attachment

```
interface TenGigabitEthernet0/0/0
service-policy output AutoQos-4.0-wlan-Port-Output-Policy
```

Figure 9-15 MQC policy

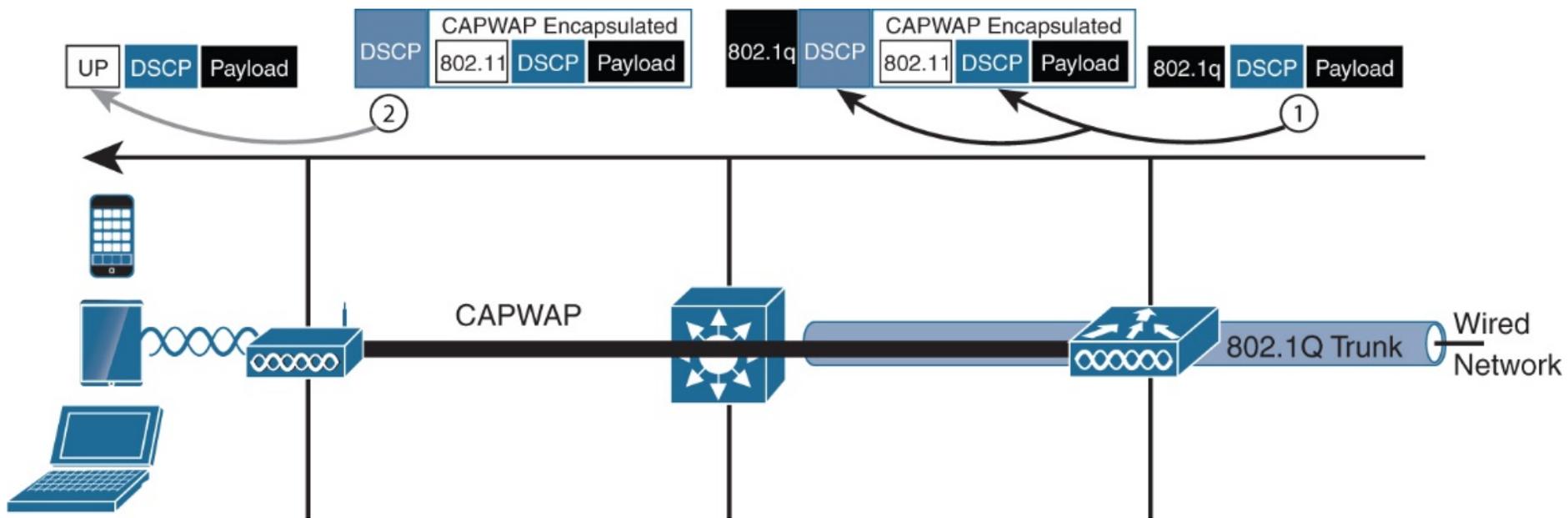


Figure 9-16 "Trust" DSCP in the downstream direction

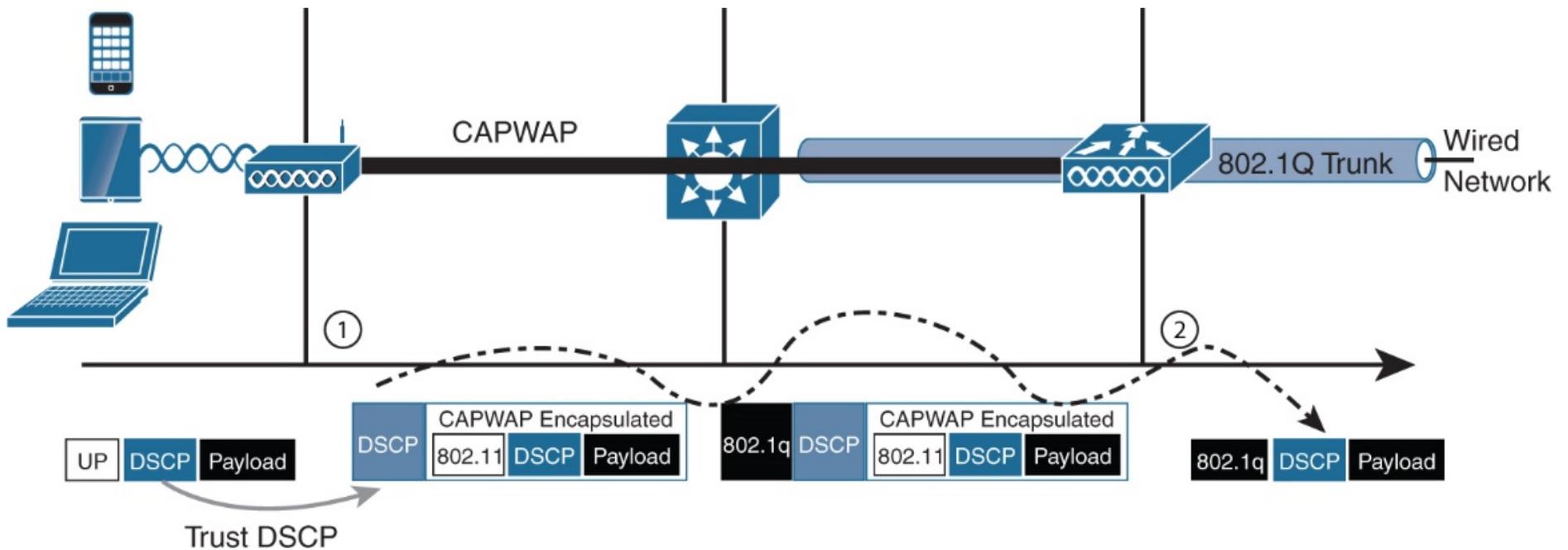


Figure 9-17 "Trust" DSCP in the upstream direction

The screenshot displays the configuration interface for QoS policies. On the left is a dark sidebar menu with a search bar and icons for Dashboard, Monitoring, Configuration (highlighted in blue), Administration, Licensing, and Troubleshooting. The main content area shows a breadcrumb trail: Configuration > Services > QoS. Below the breadcrumb are two buttons: a blue '+ Add' button and a light blue 'x Delete' button. A table lists existing policies:

	Policy Name
<input type="checkbox"/>	AVC_flex
<input type="checkbox"/>	QoS-flex

At the bottom of the table is a pagination control showing '1' of 10 items, with a dropdown menu set to '10' items.

Figure 9-18 Click Add to start configuring a new QoS policy

Configuration > Services > QoS

Add QoS

Auto QoS DISABLED

Policy Name*

Description

Match Type	Match Value	Mark Type	Mark Value	Police Value (kbps)	Drop	AVC/User Defined	Actions
<p>Navigation: 0 items per page No items to display</p> <p>Buttons: + Add Class-Maps X Delete</p>							

Figure 9-19 Start adding the classification logic

Add QoS

Policy Name*

Description

Match Type	Match Value	Mark Type	Mark Value	Police Value (kbps)	Drop	AVC/User Defined	Actions
0 items per page No items to display							
+ Add Class-Maps		× Delete					
AVC/User Defined	AVC						
Match	<input checked="" type="radio"/> Any <input type="radio"/> All						
Drop	<input checked="" type="checkbox"/>						
Match Type	protocol						
Available Protocol(s)				Selected Protocol(s)			
<input type="text" value="picasa"/> <input type="text" value="pim"/> <input type="text" value="pim-rp-disc"/> <input type="text" value="pinterest"/>				<input type="text" value="ping"/>			

Figure 9-20 Configuring a policy to match and drop ping traffic

Add QoS

Match Type	Match Value	Mark Type	Mark Value	Police Value (kbps)	Drop	AVC/User Defined	Actions
<input type="checkbox"/>	protocol	ping	None	8	Enabled	AVC	

1 items per page 1 - 1 of 1 items

AVC/User Defined:

Match: Any All

Mark Type:

Mark Value:

Drop:

Police(kbps):

Match Type:

Available Protocol(s)

- facetime
- fasttrack
- fasttrack-static
- fatserve

Selected Protocol(s)

- facebook-video
- facebook-media
- facebook-audio
- facebook

Figure 9-21 Configuring a policy to match and mark down Facebook traffic

Add QoS

Policy Name*

Description

Match Type	Match Value	Mark Type	Mark Value	Police Value (kbps)	Drop	AVC/User Defined	Actions
<input type="checkbox"/> protocol	ping	None		8	Enabled	AVC	
<input type="checkbox"/> protocol	facebook-video,facebook-media,facebook-audio,facebook	DSCP	8		Disabled	AVC	

10 items per page 1 - 2 of 2 items

[+ Add Class-Maps](#) [x Delete](#)

Class Default

Mark Police(kbps)

Drag and Drop, double click to add/remove Profiles from Selected Profiles

Figure 9-22 Configuring a policy for class-default

Add QoS

Class Default

Mark	<input type="text" value="DSCP"/>	Police(kbps)	<input type="text" value="8 - 10000000"/>
Value	<input type="text" value="0"/>		

Drag and Drop, double click or click on the button to add/remove Profiles from Selected Profiles

Available (2)		Selected (1)		
Profiles		Profiles	Ingress	Egress
 OEAP-policy 		 flex-policy	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> 
 default-policy-profile 				

Figure 9-23 Assigning the policy to the policy profile(s)

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled'

General Access Policies **QoS and AVC**

Auto QoS None ▼

QoS SSID Policy

Egress test ✕ ▼

Ingress test ✕ ▼

QoS Client Policy

Egress Search or Select ▼

Ingress QoS-flex
AVC_flex

SIP-CAC test

Figure 9-24 Assigning the policy at SSID or client level, or both

Authorization Profiles > QoS_AAA

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

▶ Common Tasks

▼ Advanced Attributes Settings

<input type="text" value="Cisco:cisco-av-pair"/>	=	<input type="text" value="ip:sub-qos-policy-in=MyPolicy"/>	-
<input type="text" value="Cisco:cisco-av-pair"/>	=	<input type="text" value="ip:sub-qos-policy-out=MyPolicy"/>	+

▼ Attributes Details

```

Access Type = ACCESS_ACCEPT
cisco-av-pair = ip:sub-qos-policy-in=MyPolicy
cisco-av-pair = ip:sub-qos-policy-out=MyPolicy
  
```

Figure 9-25 Authorization profile in ISE for AAA QoS override

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled'

General

Access Policies

QOS and AVC

Auto QoS

None ▼

QoS SSID Policy

None

Enterprise

Voice

Egress

Guest

Ingress

Fastlane

Figure 9-26 Auto QoS configuration under the Policy profile

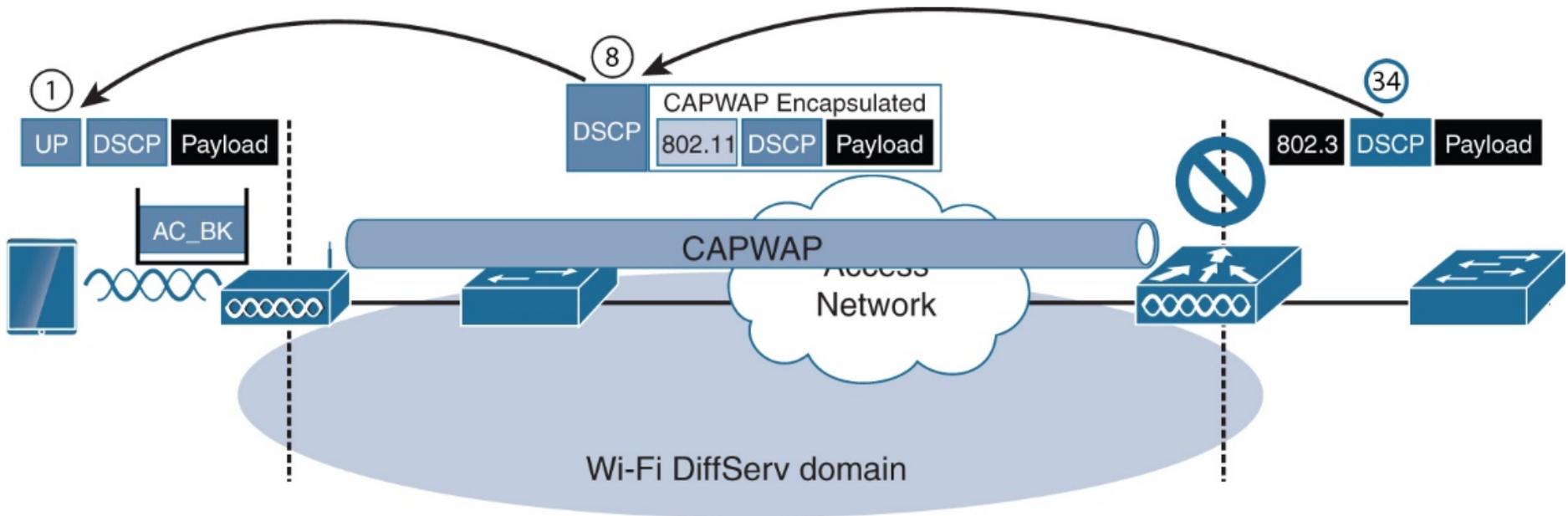


Figure 9-27 Bronze QoS profile, downstream

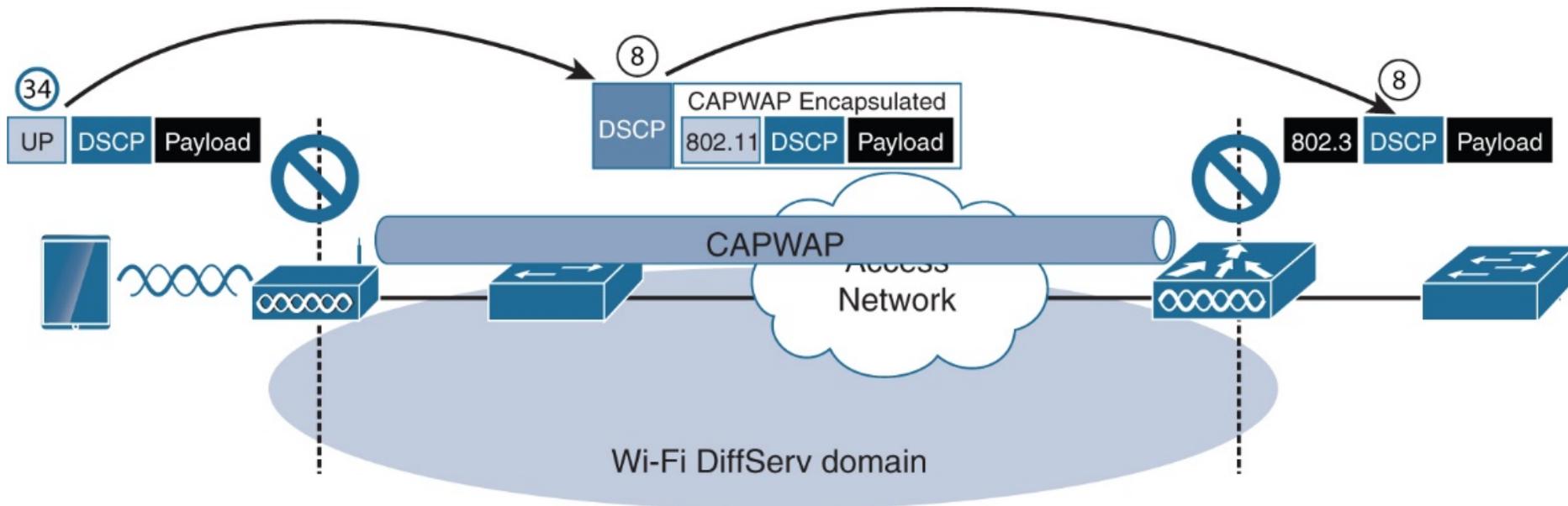


Figure 9-28 Bronze QoS profile, upstream

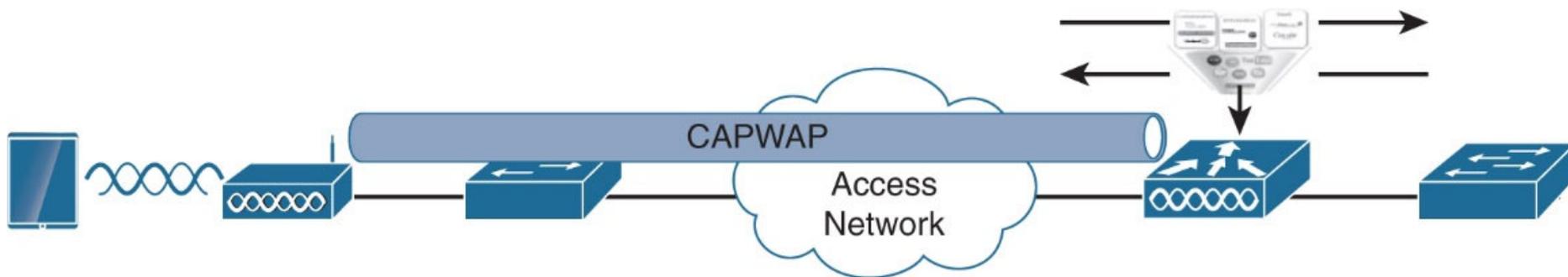


Figure 9-29 AVC in local mode and Flex central switching is applied at the WLC

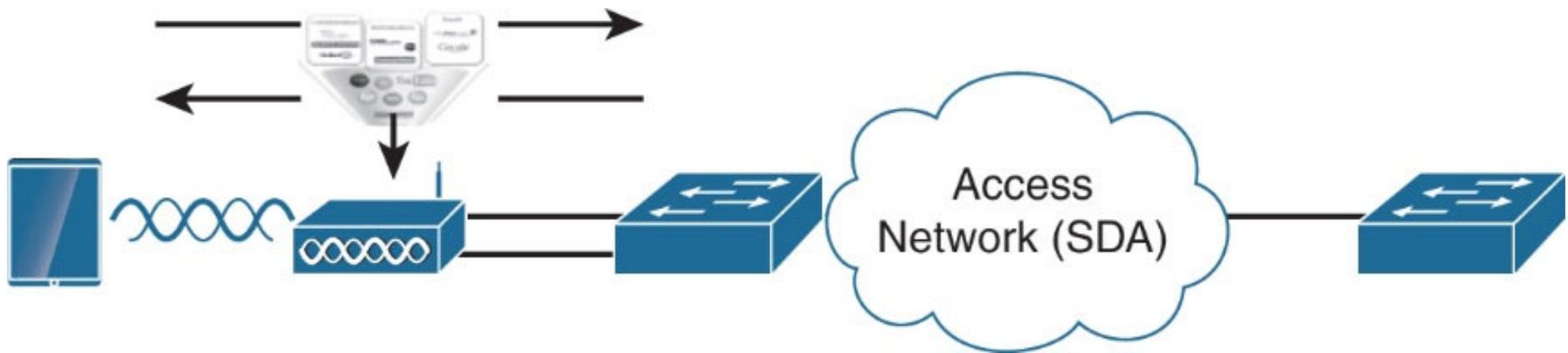


Figure 9-30 AVC in FlexConnect local switching and SDA wireless is applied at the AP

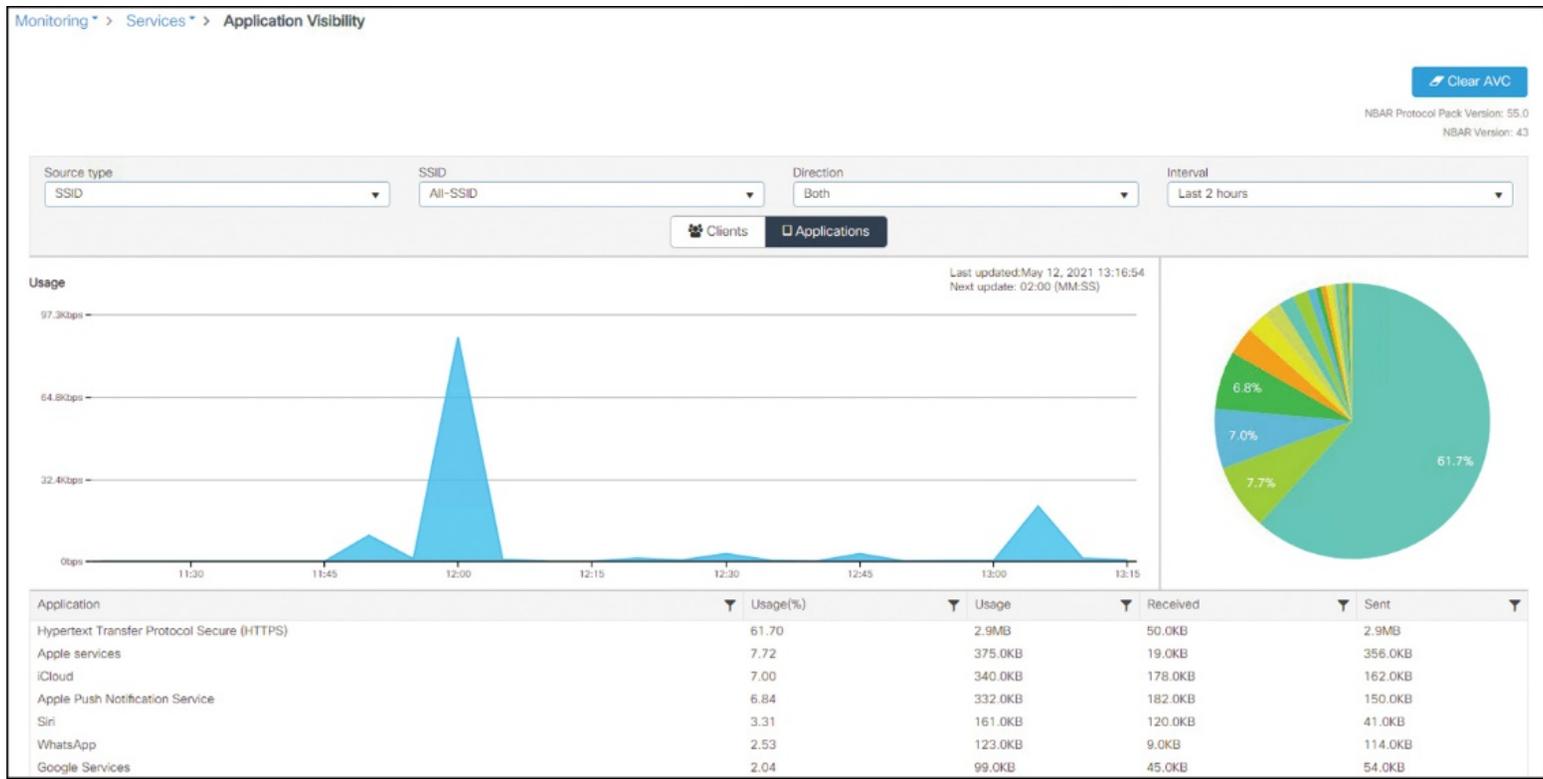


Figure 9-31 Monitoring AVC

From *Understanding and Troubleshooting Cisco Catalyst 9800 Series Wireless Controller* by Simone Arena, Francisco Sedano Crippa, Nicolas Darchis and Sudha Katgeri(9780137492329) Cisco Press
 Copyright© 2023 Cisco Systems, Inc. All rights reserved

Configuration > Radio Configurations > Parameters

5 GHz Band 2.4 GHz Band

⚠ 5 GHz Network is operational. Configuring EDCA Profile

EDCA Parameters

EDCA Profile

- wmm-default
- wmm-default**
- custom-voice
- optimized-video-voice
- optimized-voice
- svp-voice
- fastlane

DFS (802.11h)

⚠ DTPC Support is enabled. Please... con

Figure 9-32 EDCA profile settings for a 5 GHz network

Edit Policy Profile

General Access Policies **QoS and AVC**

Auto QoS Fastlane ▼

QoS SSID Policy

Egress platinum x ▼

Ingress platinum-up x ▼

Figure 9-33 Recommended policy profile settings for an SSID with voice traffic

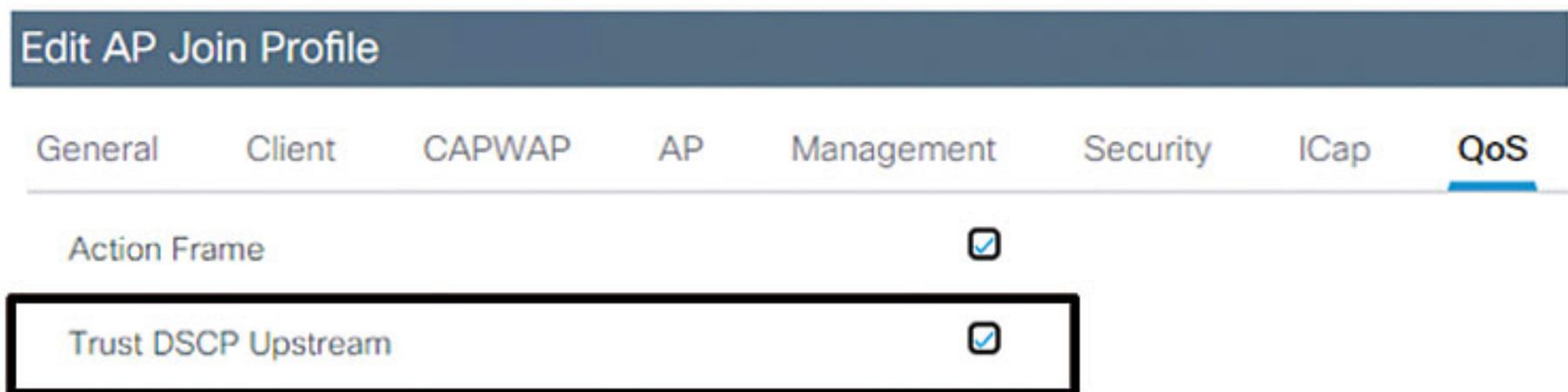


Figure 9-34 Trust DSCP settings under the AP Join Profile



Figure 10-1 Redundancy port on the C9800L-C, C9800L-F, C9800-40, and C9800-80

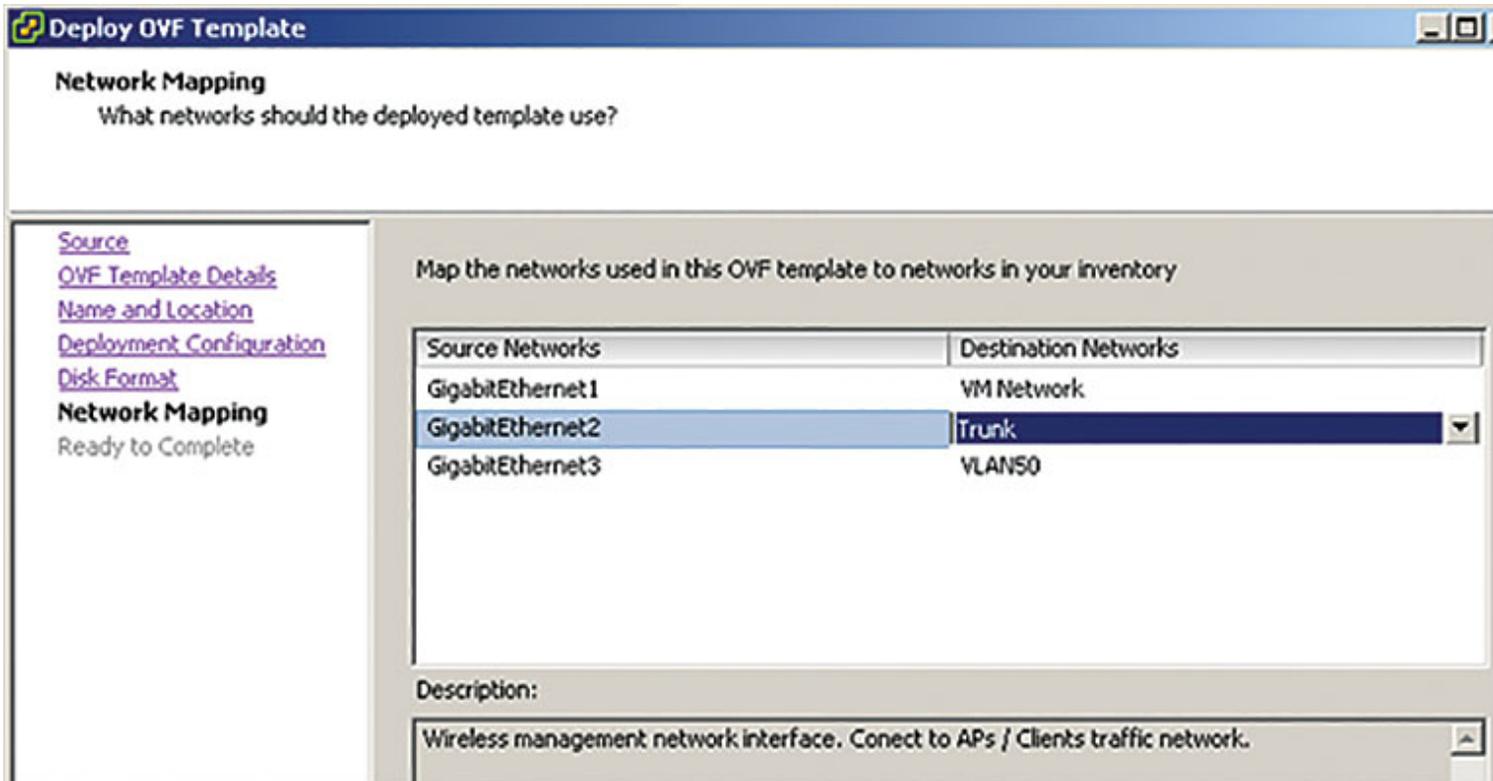


Figure 10-2 vNIC mapping for a C9800-CL over ESXi

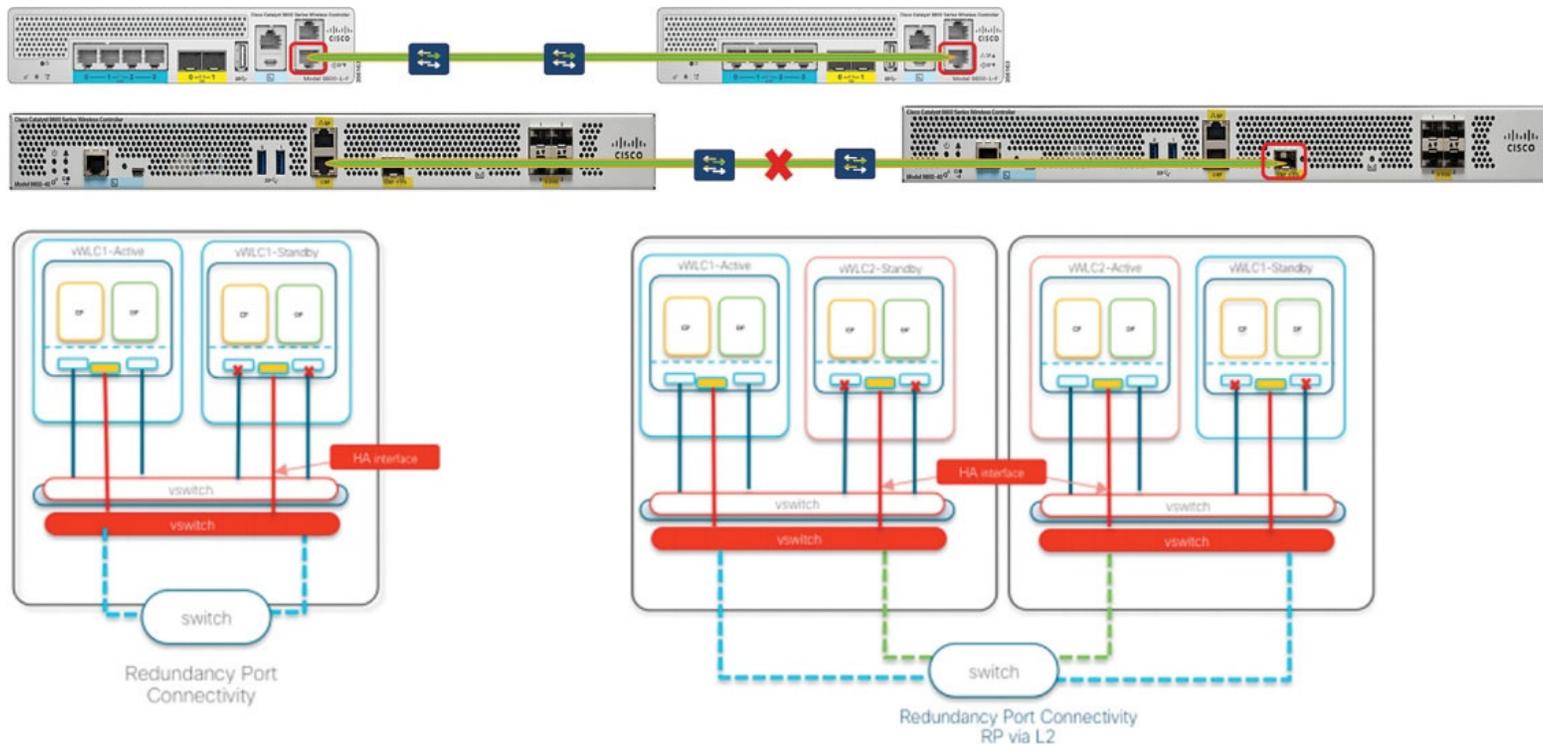


Figure 10-3 RP-to-RP connectivity between two C9800-L-Cs, two C9800-40s, and two C9800-CLs

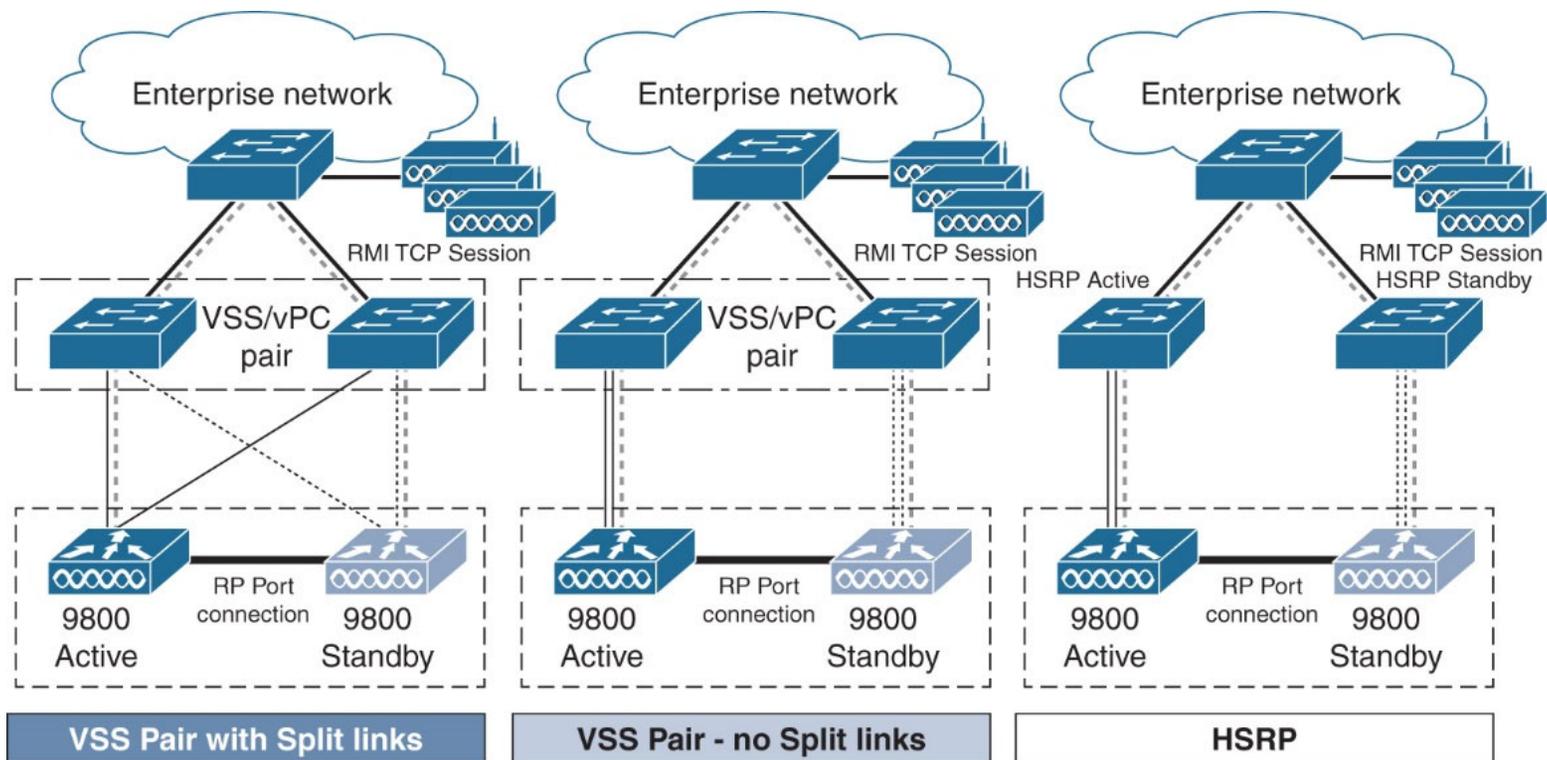


Figure 10-4 Supported topologies from an RP+RMI C9800 HA pair

Administration ▾ > Device

General	Redundancy Configuration	<input type="checkbox"/> DISABLED
FTP/SFTP/TFTP	Active Chassis Priority*	1
Redundancy		

Figure 10-5 Enabling the HA SSO

Administration > Device

General	Redundancy Configuration	ENABLED <input checked="" type="checkbox"/>
FTP/SFTP/TFTP	Redundancy Pairing Type	<input checked="" type="radio"/> RMI+RP <input type="radio"/> RP
Redundancy	RMI IP for Chassis 1*	192.168.1.15
	RMI IP for Chassis 2*	192.168.1.17
	Management Gateway Failover	ENABLED <input checked="" type="checkbox"/>
	Gateway Failure Interval (seconds)	8
	Local IP	169.254.1.15
	Remote IP	169.254.1.17
	Keep Alive Timer	1 x 100 (milliseconds)
	Keep Alive Retries	5
	Chassis Renumber	1
	Active Chassis Priority*	2
	Standby Chassis Priority*	1

Figure 10-6 Configuring SSO redundancy on a C9800

```

C9800-L-X-K9 platform with 16777216 Kbytes of main memory

File size is 0x000015cf
Located packages.conf
Image size 5583 inode num 26, bks cnt 2 blk size 8*512
#
File size is 0x023f44c5
Located C9800-L-rpboot.17.06.01.SPA.pkg
Image size 37700805 inode num 506916, bks cnt 9205 blk size 8*512
#####
#####
#####
#####
#####
Boot image size = 37700805 (0x23f44c5) bytes

ROM:RSA Self Test Passed
ROM:Sha512 Self Test Passed

Package header rev 3 structure detected
Calculating SHA-1 hash...done
validate_package_cs: SHA-1 hash:
    calculated 2f5b2f34:80f4af8a:b3b586c1:d41ca412:7736d66f
    expected   2f5b2f34:80f4af8a:b3b586c1:d41ca412:7736d66f
Validating main package signatures

RSA Signed RELEASE Image Signature Verification Successful.
Image validated
Aug 29 20:43:36.605: %PMAN-3-PROC_EMPTY_EXEC_FILE: R0/0: pvp: Empty executable used for process
bt_logger

Waiting for remote chassis to join

```

Figure 10-7 Chassis initialization before HA pairing

```
*Aug 29 15:10:59.998: %STACKMGR-6-STACK_LINK_CHANGE: Chassis 2 R0/0: stack_mgr: Stack port 1 on
Chassis 2 is up
*Aug 29 15:10:59.998: %STACKMGR-6-STACK_LINK_CHANGE: Chassis 2 R0/0: stack_mgr: Stack port 2 on
Chassis 2 is up
*Aug 29 15:11:00.191: %STACKMGR-6-CHASSIS_ADDED: Chassis 2 R0/0: stack_mgr: Chassis 2 has been added
to the stack.
*Aug 29 15:11:01.468: %PMAN-3-PROC_EMPTY_EXEC_FILE: Chassis 2 R0/0: pvp: Empty executable used for
process bt_logger
*Aug 29 15:11:01.497: %STACKMGR-6-CHASSIS_ADDED: Chassis 2 R0/0: stack_mgr: Chassis 2 has been added
to the stack.
*Aug 29 15:11:03.409: %PMAN-3-PROC_EMPTY_EXEC_FILE: Chassis 2 R0/0: pvp: Empty executable used for
process bt_logger
*Aug 29 15:11:03.497: %STACKMGR-6-CHASSIS_ADDED: Chassis 2 R0/0: stack_mgr: Chassis 2 has been added
to the stack.
*Aug 29 15:11:03.746: %STACKMGR-6-ACTIVE_ELECTED: Chassis 2 R0/0: stack_mgr: Chassis 1 has been
elected ACTIVE.
*Aug 29 15:11:04.390: %PMAN-3-PROC_EMPTY_EXEC_FILE: Chassis 2 R0/0: pvp: Empty executable used for
process bt_logger
*Aug 29 15:11:04.987: %RIF_MGR_FSM-6-RP_LINK_UP: Chassis 2 R0/0: rif_mgr: The RP link is UP.
*Aug 29 15:11:04.987: %STACKMGR-1-DUAL_ACTIVE_CFG_MSG: Chassis 2 R0/0: stack_mgr: Dual Active
Detection link is available now
```

Figure 10-8 Active election

```
*Aug 29 20:44:57.925: %RIF_MGR_FSM-6-GW_REACHABLE_ACTIVE: Chassis 1 R0/0: rif_mgr: Gateway reachable
from Active
*Aug 29 20:45:08.545: %IOSXE_REDUNDANCY-6-PEER: Active detected chassis 2 as standby.
*Aug 29 20:45:08.540: %STACKMGR-6-STANDBY_ELECTED: Chassis 1 R0/0: stack_mgr: Chassis 2 has been
elected STANDBY.
```

Figure 10-9 Standby election

```
*Aug 29 20:44:07.123: %EWLC_HA_LIB_MESSAGE-6-BULK_SYNC_STATE_INFO: Chassis 1 R0/0: wncmgrd: INFO: Bulk sync status : COLD
```

Figure 10-10 Standby comes up cold prior to the bulk sync

```
*Aug 29 20:45:17.087: %VOICE_HA-7-STATUS: NONE->SSO; SSO mode will not take effect until after a
platform reload.
*Aug 29 20:45:18.589: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
(raw-event=PEER_FOUND(4))

*Aug 29 20:45:18.589: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
(raw-event=PEER_REDUNDANCY_STATE_CHANGE(5))

*Aug 29 20:45:20.149: Syncing vlan database
*Aug 29 20:45:20.165: Vlan Database sync done from bootflash:vlan.dat to stby-bootflash:vlan.dat (616
bytes)
*Aug 29 20:45:30.534: %CRYPTO_ENGINE-4-CSDL_COMPLIANCE_RSA_WEAK_KEYS: RSA keypair
CISCO_IDEVID_SUDI_LEGACY is in violation of Cisco security compliance guidelines and will be rejected
by future releases.
*Aug 29 20:45:51.774: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart License
Utility (CSLU) : Unable to resolve server hostname/domain name
*Aug 29 20:47:21.226: %RIF_MGR_FSM-6-RMI_LINK_UP: Chassis 1 R0/0: rif_mgr: The RMI link is UP.
*Aug 29 20:47:23.646: %HA_CONFIG_SYNC-6-BULK_CFGSYNC_SUCCEED: Bulk Sync succeeded
*Aug 29 20:47:23.686: %VOICE_HA-7-STATUS: VOICE HA bulk sync done.
*Aug 29 20:47:24.725: %RF-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)
```

Figure 10-11 Standby comes up hot after the bulk sync

```
9800L#redundancy force-switchover
Proceed with switchover to standby RP? [confirm]
Manual Swact = enabled

Chassis 1 reloading, reason - Non participant detected

*Aug 31 07:26:52.680: RMI-GW-NOTICE: Forced switchover notification received

*Aug 31 07:26:53.782: %RF-5-RF_RELOAD: Self reload. Reason: redundancy force-switchover
Aug 31 07:26:54.805: %PMAN-5-EXITACTION: C0/0: pvp: Process manager is exiting:
Aug 31 07:26:54.842: %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting:

*Aug 31 07:26:54.060: %SYS-5-SWITCHOVER: Switchover requested by red_switchover_process. Reason:
redundancy force-switchover.Aug 31 07:27:00.884: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is
exiting: process exit with reload fru code
```

Figure 10-12 SSO switchover on the active C9800

```
9800L-stby#Ewlc: triggered dual-active recovery, setting hostname to 9800L, Mode: 4
*Aug 31 07:26:53.881: %REDUNDANCY-3-SWITCHOVER: RP switchover (PEER_NOT_PRESENT)
*Aug 31 07:26:53.881: %REDUNDANCY-3-REDUNDANCY_ALARMS: Unable to assert REDUNDANCY alarm

*Aug 31 07:26:53.881: %REDUNDANCY-3-REDUNDANCY_ALARMS: Unable to assert REDUNDANCY alarm

*Aug 31 07:26:53.881: %REDUNDANCY-3-SWITCHOVER: RP switchover (PEER_DOWN)
*Aug 31 07:26:53.881: %REDUNDANCY-3-SWITCHOVER: RP switchover (PEER_REDUNDANCY_STATE_CHANGE)
*Aug 31 07:26:54.164: SNMPHA-CHKPT: chkpt: msg is NULL

*Aug 31 07:26:54.556: SNMPHA-CHKPT: chkpt: msg is NULL

*Aug 31 07:26:54.676: WLC-HA-Notice: RF Progression event: RF_PROG_ACTIVE_FAST, Switchover triggered
*Aug 31 07:26:54.681: %LINK-3-UPDOWN: Interface Lsmpi0, changed state to up
*Aug 31 07:26:54.681: %LINK-3-UPDOWN: Interface EOBC0, changed state to up
*Aug 31 07:26:54.710: RMI-HAINFRA-INFO: Configured primary IP 192.168.1.5/255.255.255.0 on active(mgmt)
*Aug 31 07:26:54.710: RMI-HAINFRA-INFO: Configured secondary IP 192.168.1.17/255.255.255.0 on
active(mgmt)
*Aug 31 07:26:54.731: %VOICE_HA-2-SWITCHOVER_IND: SWITCHOVER, from STANDBY_HOT to ACTIVE state.
```

Figure 10-13 SSO switchover on the standby C9800

```

9800L#show chassis rmi
Chassis/Stack Mac Address : d478.9b3c.5e80 - Local Mac Address
Mac persistency wait time: Indefinite
Local Redundancy Port Type: Twisted Pair

```

Chassis#	Role	Mac Address	Priority	H/W Version	Current State	IP	RMI-IP
*1	Active	d478.9b3c.5e80	1	V02	Ready	169.254.1.15	192.168.1.15
2	Standby	d478.9b3c.5f60	1	V02	Ready	169.254.1.17	192.168.1.17

```

9800L#show redundancy states
my state = 13 -ACTIVE
peer state = 8 -STANDBY HOT
Mode = Duplex
Unit = Primary
Unit ID = 1

Redundancy Mode (Operational) = sso
Redundancy Mode (Configured) = sso
Redundancy State = sso
Maintenance Mode = Disabled
Manual Swact = enabled
Communications = Up

client count = 150
client_notification_TMR = 30000 milliseconds
RF debug mask = 0x0
Gateway Monitoring = Enabled
Gateway monitoring interval = 8 secs

```

Figure 10-14 HA monitoring from the active C9800

```

9800L-stby#show chassis rmi
Chassis/Stack Mac Address : d478.9b3c.5e80 - Local Mac Address
Mac persistency wait time: Indefinite
Local Redundancy Port Type: Twisted Pair

```

Chassis#	Role	Mac Address	Priority	H/W Version	Current State	IP	RMI-IP
1	Active	d478.9b3c.5e80	1	V02	Ready	169.254.1.15	192.168.1.15
*2	Standby	d478.9b3c.5f60	1	V02	Ready	169.254.1.17	192.168.1.17

```

9800L-stby#show redundancy states
my state = 8 -STANDBY HOT
peer state = 13 -ACTIVE
Mode = Duplex
Unit = Primary
Unit ID = 2

Redundancy Mode (Operational) = sso
Redundancy Mode (Configured) = sso
Redundancy State = sso
Maintenance Mode = Disabled
Manual Swact = cannot be initiated from this the standby unit
Communications = Up

client count = 150
client_notification_TMR = 30000 milliseconds
RF debug mask = 0x0
Gateway Monitoring = Enabled
Gateway monitoring interval = 8 secs

```

Figure 10-15 HA monitoring from the standby C9800

Monitoring > General > System

Inventory Memory Utilization CPU Utilization Wireless Interface Management Summary **Redundancy**

General Active Statistics Standby Statistics

My State	ACTIVE	Redundancy State	sso
Peer State	STANDBY HOT	Manual Swact	enabled
Unit	Primary	Communications	Up
Unit ID	1	Standby Failures	1
Redundant Mode (Operational)	sso	Switchovers System Experienced	0
Redundancy Mode(Configured)	sso		

Chassis Details

Chassis	Role	MAC Address	Priority	H/W Version	Current State	IP Address	RMI IP Address	Mobility MAC Address	Image Version	Device Uptime
*1	Active	d4/8.9b3c.5e80	1	V02	Ready	169.254.1.15	192.168.1.15	d4/8.9b3c.5e8b	17.6.1	11 hours, 21 minutes
2	Standby	d4/8.9b3c.5f60	1	V02	Ready	169.254.1.17	192.168.1.17	0000.0000.0000	17.6.1	7 hours, 29 minutes

10 items per page 1 - 2 of 2 items

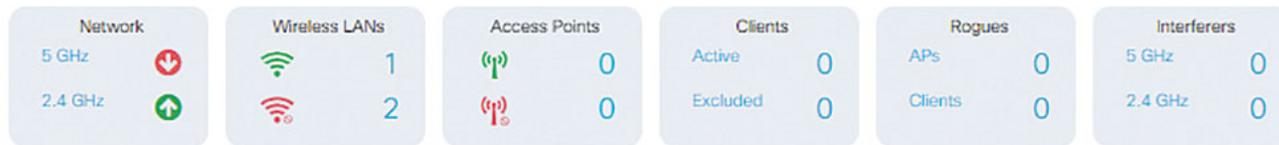
Switchover Details

Index	Previous Active	Current Active	Switch Over Time	Switch Over Reason
-------	-----------------	----------------	------------------	--------------------

10 items per page No items to display

Figure 10-16 HA state monitoring from the active C9800 GUI

Dashboard



Overview

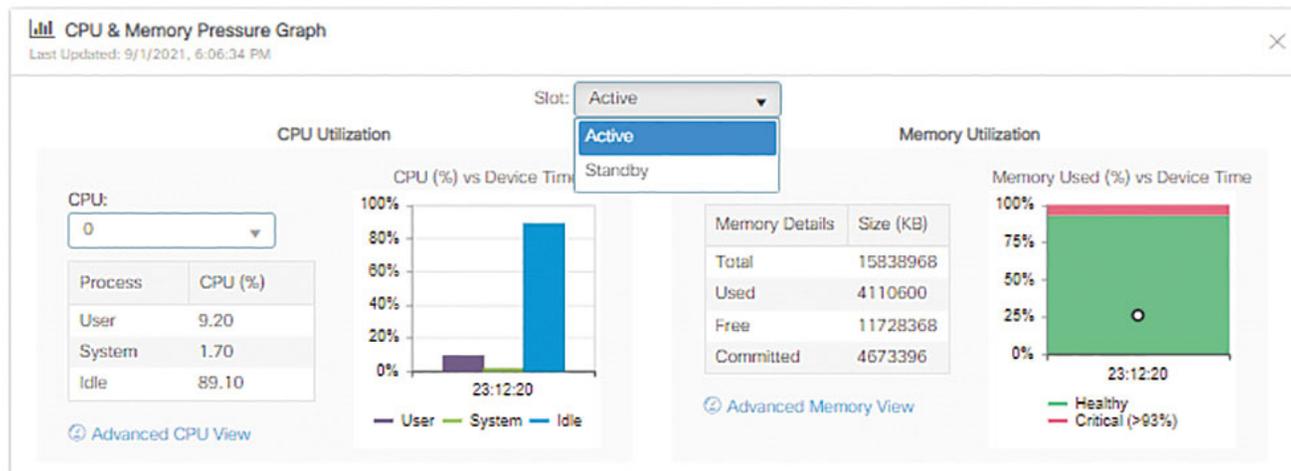


Figure 10-17 HA active and standby resource monitoring from the active C9800 GUI

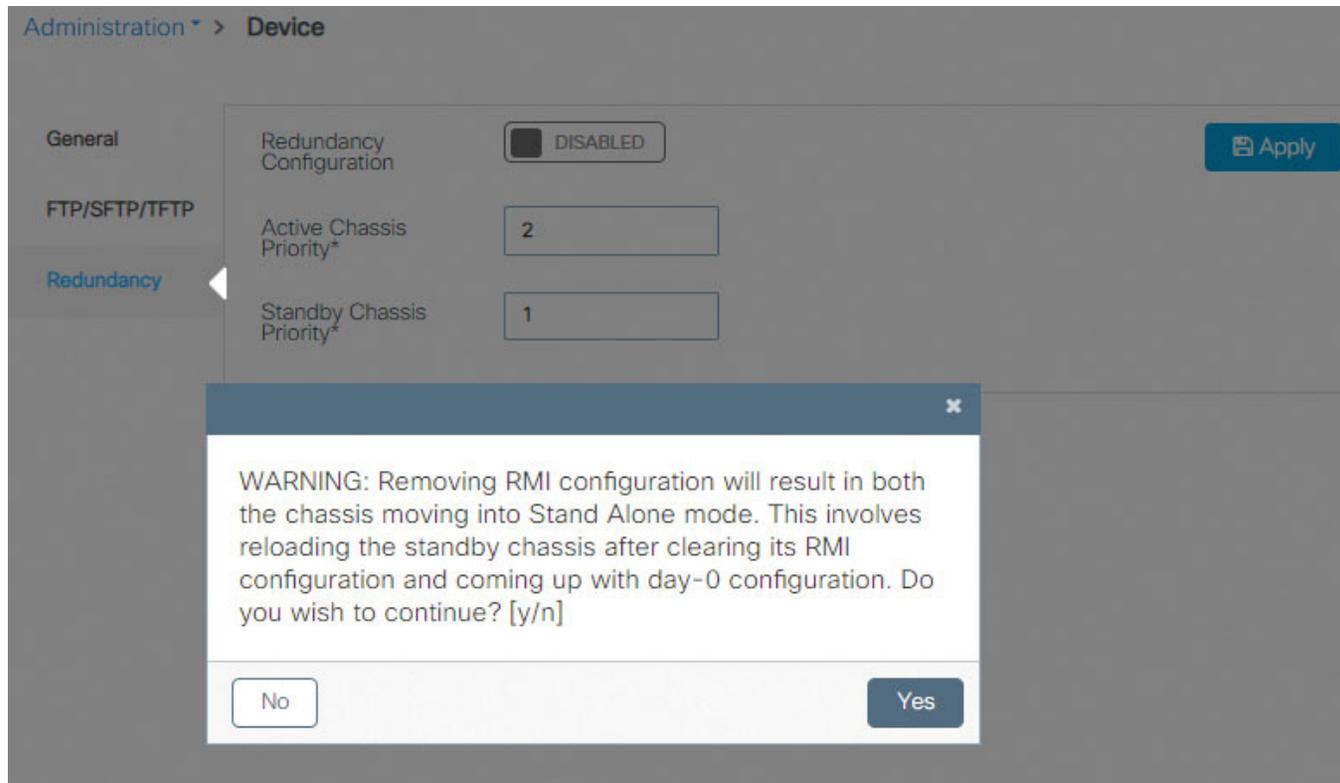


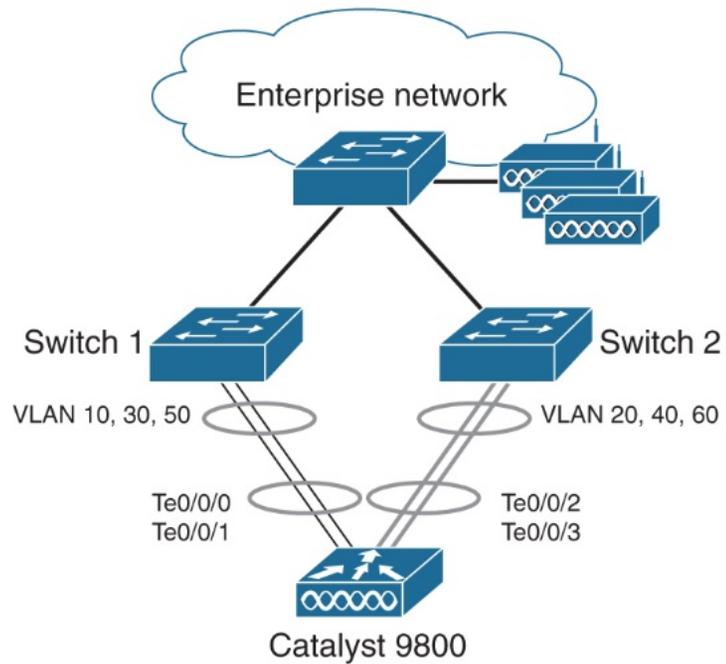
Figure 10-18 Disabling HA SSO

Configuration > Wireless > Mobility

Global Configuration	Peer Configuration
Mobility Group Name*	<input type="text" value="default"/>
Multicast IPv4 Address	<input type="text" value="0.0.0.0"/>
Multicast IPv6 Address	<input type="text" value="::"/>
Keep Alive Interval (sec)*	<input type="text" value="10"/>
Mobility Keep Alive Count*	<input type="text" value="3"/>
Mobility DSCP Value*	<input type="text" value="48"/>
Mobility MAC Address	<input type="text" value="<Mobility MAC>"/>
DTLS High Cipher Only*	<input type="checkbox"/> DISABLED

Figure 10-19 Mobility MAC Configuration

Single controller w/Multi-chassis LAG



SSO Pair w/Multi-chassis LAG

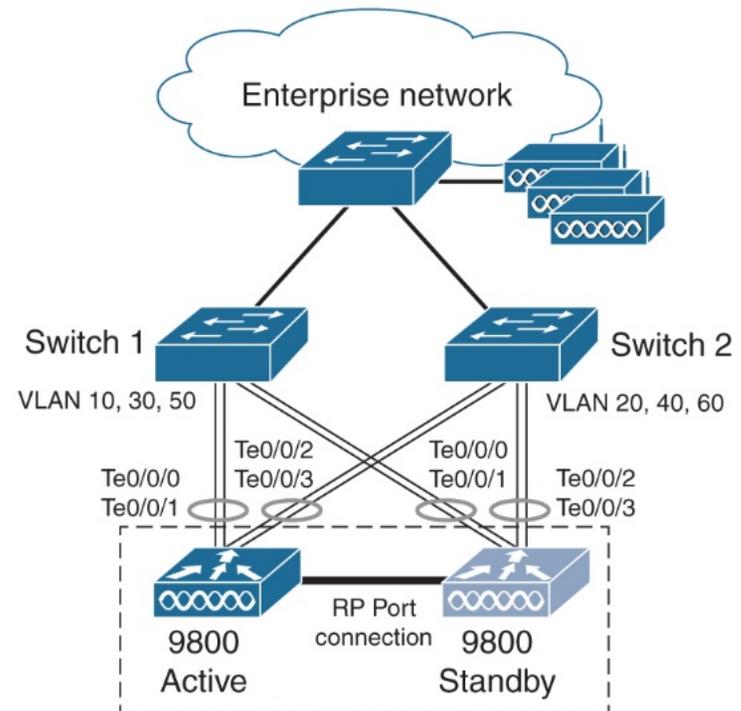


Figure 10-20 C9800 to switch connections with Multi-Chassis LAG

Configuration > Tags & Profiles > AP Join

+ Add X Delete

AP Join Profile Name
<input type="checkbox"/> default-ap-profile

1 10 Items per page

Edit AP Join Profile

General Client **CAPWAP** AP Management Security ICap QoS

High Availability Advanced

CAPWAP Timers

Fast Heartbeat Timeout(sec)*

Heartbeat Timeout(sec)*

Discovery Timeout(sec)*

Primary Discovery Timeout(sec)*

Primed Join Timeout(sec)*

Retransmit Timers

Count*

Interval (sec)*

AP Fallback to Primary

Enable

Backup Primary Controller

Name

IPv4/IPv6 Address

Backup Secondary Controller

Name

IPv4/IPv6 Address

Figure 10-21 N+1 HA configuration on access points

Configuration > Wireless > Access Points

▼ All Access Points

Total APs : 1

AP Name	AP Model
9120	C9120AXI-B

10 items per page

Edit AP

- General
- Interfaces
- High Availability**
- Inventory
- ICap
- Advanced
- Support Bundle

	Name	Management IP Address (IPv4/IPv6)
Primary Controller	<input type="text"/>	<input type="text" value="1"/>
Secondary Controller	<input type="text"/>	<input type="text"/>
Tertiary Controller	<input type="text"/>	<input type="text"/>
AP failover priority	<input type="text" value="Low"/>	

Figure 10-22 N+1 HA Configuration on AP Join Profile

Configuration > Wireless > Access Points

▼ All Access Points

Current Active
EWCAP-4150

Current Standby
EWCAP-863C

Preferred Active
Not Configured

Number of AP(s): 3

-

AP Name	AP Model	EWC Capable	Image Type	Slots	Admin Status	IP Address	Base Radio MAC	AP Mode
<input type="radio"/> sudha-2800	AIR-AP2802I-B-K9	No	CAPWAP	2	<input checked="" type="checkbox"/>	192.168.1.95	002a.10bf.5d00	Flex
<input type="radio"/> EWCAP-863C	C9115AXI-B	Yes	EWC	2	<input checked="" type="checkbox"/>	192.168.1.68	502f.a876.44e0	Flex
<input type="radio"/> EWCAP-4150	C9115AXI-B	Yes (Internal)	EWC	2	<input checked="" type="checkbox"/>	192.168.1.40	d478.9bb9.3580	Flex

Figure 10-23 Active and Standby EWC-APs

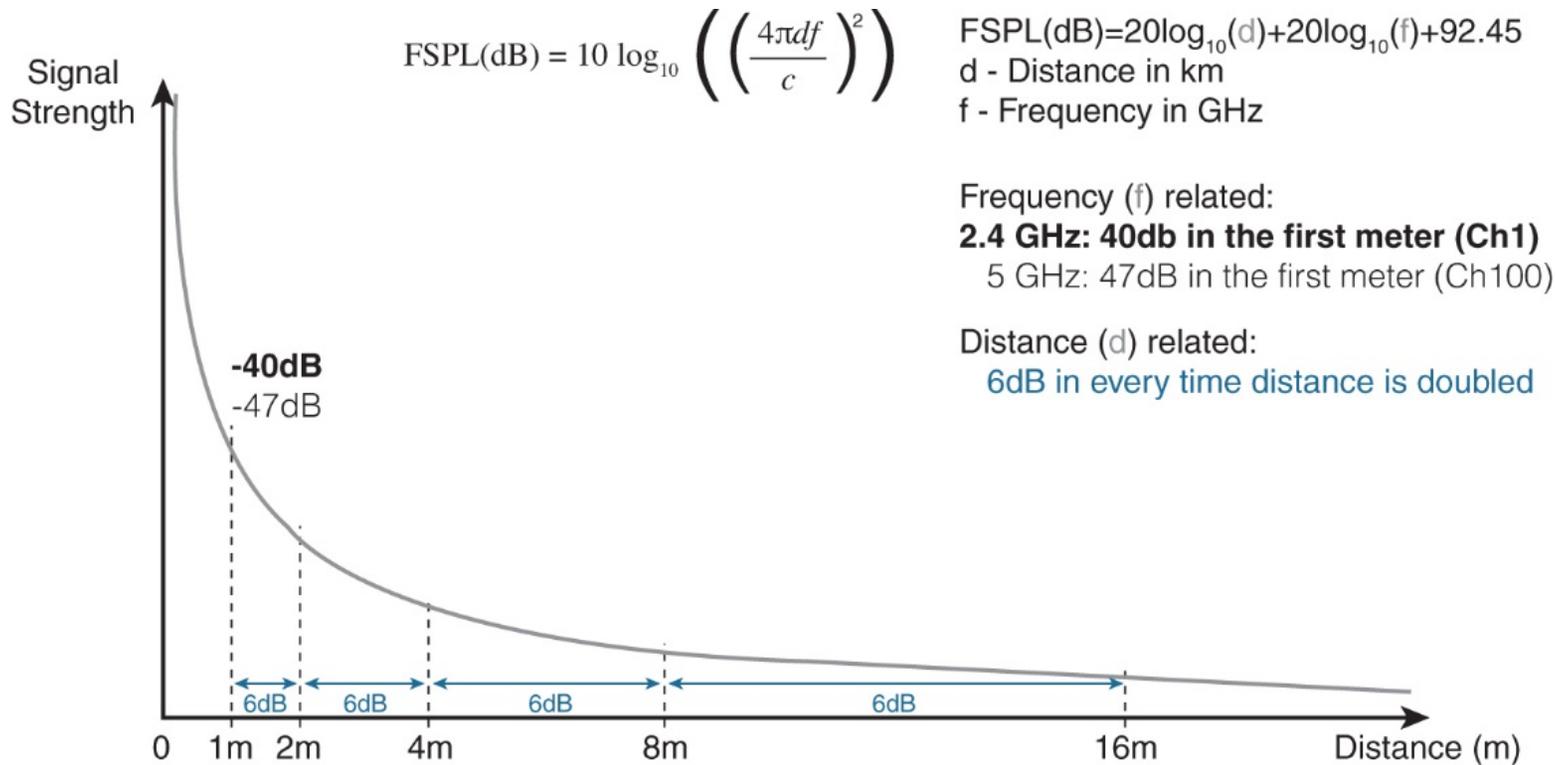


Figure 11-1 Free space path loss; a 6 dB decrease every time distance is doubled

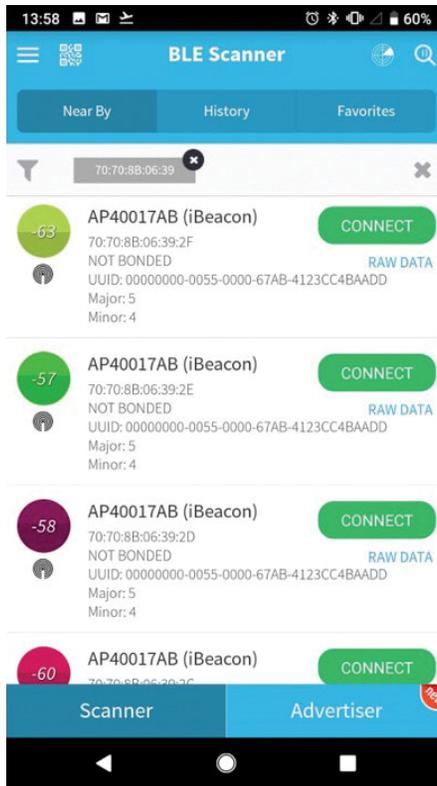


Figure 11-2 A BLE scanner application running on a smartphone

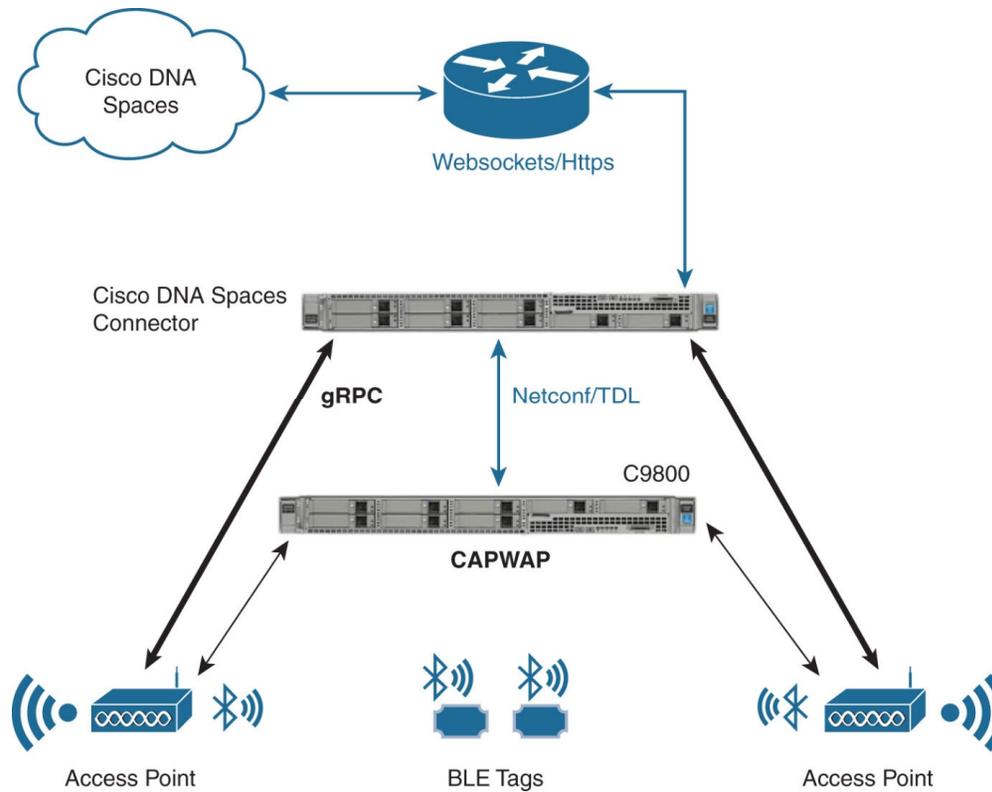


Figure 11-3 Cisco DNA Spaces Bluetooth telemetry architecture

Cisco DNA Spaces Connector DNAS ▾

Set up HTTP Proxy
If the machine is sitting behind a proxy, Connector won't be able to interact with cloud without setting up the proxy [Setup](#) [Skip](#)

Configure Token
Without the token, connector will not be able to be started [Setup](#)

Privacy Settings
Setup your MAC salt, Username salt and IPAddress salt [Setup](#) [Skip](#)

Connector [Download Logs](#) [Restart Connector](#) Token not configured ●

Username: dnasadmin	Server Time: Wed Sep 01 2021 11:11:41 GMT+0200 (Central European Summer Time)	Version: ova-2.3.495
Hostname: DNAS	NTP Status: address= pool.ntp.org status=active (running)	---
MAC Address: 00:0c:29:d5:2c:05	since=Fri 2021-08-27 16:29:13 CEST	
IP Address: 192.168.1.97	Proxy Status: Proxy is not configured	
Gateway: 192.168.1.1	Proxy: ---	
Netmask: 255.255.255.0	Cloud Reachable: True	
DNS Server: 8.8.8.8	AAA Status: AAA=Disabled	
Domain: nico.com	Connector Name: ---	

Cloud Control Channel ●	Cloud Data Channel ●	Controller Channel								
		<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">IP Address ▾</th> <th style="width: 30%;">Connected At ▾</th> <th style="width: 30%;">Msg Rate/Second ▾</th> <th style="width: 10%;">Status ▾</th> </tr> </thead> <tbody> <tr> <td colspan="4" style="text-align: center; height: 50px;"> No Data </td> </tr> </tbody> </table>	IP Address ▾	Connected At ▾	Msg Rate/Second ▾	Status ▾	No Data			
IP Address ▾	Connected At ▾	Msg Rate/Second ▾	Status ▾							
No Data										

Figure 11-4 CiscoDNA Spaces connector initial WebUI screen

Connect via Spaces Connector

Spaces Connector is an easy way to get your wireless network connected to Cisco DNA Spaces. No need to upgrade Wireless LAN Controllers or reconfigure your wireless network.

- 1 Install Spaces Connector OVA**
Download and install Spaces Connector OVA as a virtual machine.
[Download Spaces Connector ?](#)
- 2 Configure Spaces Connector**
You will need a token to configure Spaces Connector. You need to connect to `https://<your connector IP>/` from a browser to configure the token. You can optionally configure Spaces Connector to connect via HTTPS proxy.

0 / 4 connector(s) active[Create a new token](#)
[View Connectors](#)
- 3 Add Controllers**
Add and associate controllers to your Cisco DNA Spaces Connector(s)

0 / 1 controller(s) active[Add Controllers](#)
[View Controllers](#)
- 4 Import Maps**
Prime/DNAC map requires in order to work Locate & detect, Asset tracker, and IOT services, and proximity Report

19 buildings imported

91 floors imported

[Import/Sync Maps](#)
[Map Upload History](#)
[Manage Maps](#)
- 5 Setup location hierarchy**
Once the maps imported, you can add them into location hierarchy

Figure 11-5 DNA Spaces Setup >Wireless page allowing you to generate tokens

Connector [Download Logs](#) [Copy Key Hash](#) [Restart Connector](#) Running ●

Username:	dnasadmin	Server Time:	Wed Sep 01 2021 11:26:41 GMT+0200 (Central European Summer Time)	Version:	ova-2.3.495
Hostname:	DNAS	NTP Status:	address= pool.ntp.org status=active (running) since=Fri 2021-08-27 16:29:13 CEST	Docker Version:	v2.0.555
Tenant ID:	13575	Proxy Status:	Proxy is not configured		
MAC Address:	00:0c:29:d5:2c:05	Proxy:	---		
IP Address:	192.168.1.97	Cloud Reachable:	True		
Gateway:	192.168.1.1	AAA Status:	AAA=Disabled		
Netmask:	255.255.255.0	Connector Name:	DNASc9800book		
DNS Server:	8.8.8.8				
Domain:	nico.com				

Cloud Control Channel ●	Cloud Data Channel ●	Controller Channel								
Connected At: Wed Sep 01 2021 11:14:19 GMT+0200 (Central European Summer Time) Status: Connected	Connected At: Wed Sep 01 2021 11:14:20 GMT+0200 (Central European Summer Time) Status: Connected Outgoing message rate: 0 events/second	<table border="1"> <thead> <tr> <th>IP Address</th> <th>Connected At</th> <th>Msg Rate/Second</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td colspan="4" style="text-align: center;">No Data</td> </tr> </tbody> </table>	IP Address	Connected At	Msg Rate/Second	Status	No Data			
IP Address	Connected At	Msg Rate/Second	Status							
No Data										

Figure 11-6 Cisco DNA Spaces WebUI page after successful connection to the cloud

Add Controller

Connector

DNASc9800book ^

Controller IP

192.168.1.133

Controller Name

lab9800L

Controller Type

Catalyst WLC / Catalyst 98... ^

Netconf Username

admin

Netconf Password

..... 

Enable Password

..... 

Figure 11-7 Cisco DNA Spaces connector Add Controller page

Catalyst WLC CLI Commands

```
en
conf t
nmsp enable
aaa new-model
username 000c29d52c05 mac aaa attribute list cmx_000c29d52c05
aaa attribute list cmx_000c29d52c05
attribute type password f19ed055bd6a61140be156534249480ea189a45d04153820a4ede7d9852f2cf5
aaa authorization credential-download wcm_loc_serv_cert local
```

Test Connectivity

Save & Close

Figure 11-8 DNA Spaces connector CLI commands overview

1 OpenRoaming Profiles
Configure an OpenRoaming hotspot profile for your network

0

OpenRoaming profile(s) created [Create OpenRoaming Profile](#)

To set up OpenRoaming, start by creating your OpenRoaming profile

2 Hotspot-enabled Connectors
OpenRoaming Profiles can run on your Hotspot-enabled connector instances

AireOS/Catalyst Meraki API

0

Connectors have Hotspot enabled [Enable Hotspot for Connector\(s\)](#)

You need at least 1 connector that is hotspot-enabled for OpenRoaming to work

3 Network configuration
Configure Network configuration for your OpenRoaming network

AireOS/Catalyst controllers Meraki Networks

0/1

Controllers are configured with Profiles

Controllers	OpenRoaming Profile	Connector	# of APs	Type	Controller Status	Last Configured	Action
WLC	Not Configured	DNASc9800book	2	Catalyst WLC	Active	-	

Figure 11-9 Cisco DNA Spaces OpenRoaming page

Create an OpenRoaming Profile ✕

1 Set Access Policy 2 Pick an SSID 3 Configure Carrier Offload 4 Summary

Access Policy

Set your policy on who can access your OpenRoaming network

Select the types of users who can access OpenRoaming

- Accept all authenticated users (Default)
- Accept only users who provide their identity (e.g. email)
- Accept users with specified identity types
- Accept only your users (You will need to be added as an identity provider)

Preferred Credentials

Set your policy on who can access your OpenRoaming network

- I do not have preferred credentials
- I have preferred credentials, which I want to use

[Cancel](#) [Previous](#) [Next](#)

Figure 11-10 Cisco DNA Spaces OpenRoaming profile access policy page

Create an OpenRoaming Profile ✕

✓
Set Access Policy

2
Pick an SSID

3
Configure Carrier Offload

4
Summary

SSID Details

Enter the SSID details for this OpenRoaming Profile - this is a secure SSID different from your guest SSID.

i If you are entering an existing SSID, please ensure the SSID matches exactly on the network

SSID Name

OpenRo

∨ **Advanced**

Default status

Enable Disable

Fast Transition (802.11r)

Adaptive Enable Disable

Need Help?

[SSID Configuration for OpenRoaming](#) 🔗

Cancel
Previous
Next

Figure 11-11 Cisco DNA Spaces OpenRoaming profile SSID configuration page

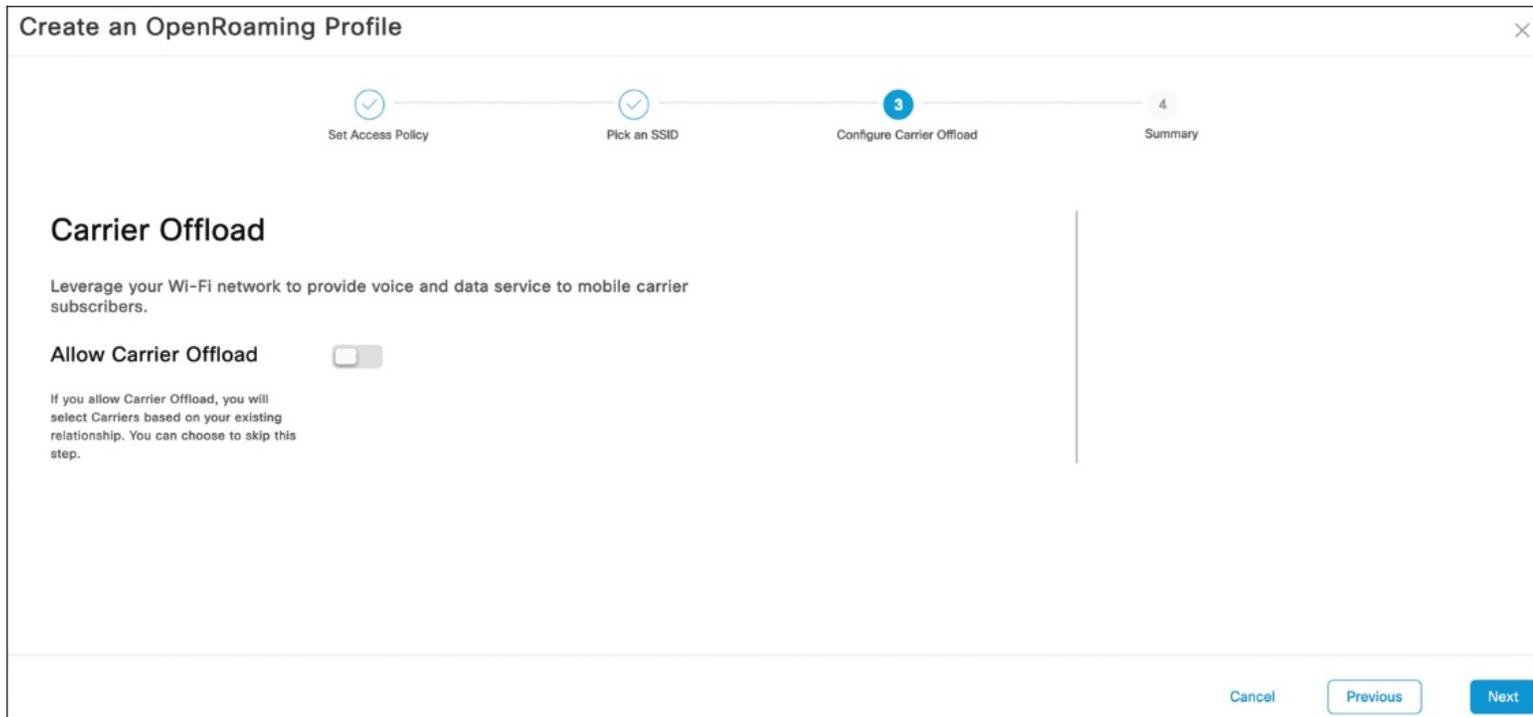


Figure 11-12 Cisco DNA Spaces OpenRoaming profile carrier offload page

Connector Hotspot

Hotspot Download Logs Restart Hotspot Running

Username:	dnasadmin	Hostname:	DNAS
Tenant ID:	13575	MAC Address:	00:0c:29:d5:2c:05
IP Address:	192.168.1.97	Gateway:	192.168.1.1
Netmask:	255.255.255.0	DNS Server:	8.8.8.8
Domain:	nico.com	Server Time:	Wed Sep 01 2021 15:45:52 GMT+0200 (Central European Summer Time)
NTP Status:	address= pool.ntp.org status=active (running) since=Fri 2021-08-27 16:29:13 CEST	Proxy Status:	Proxy is not configured
Cloud Reachable:	True	Proxy:	---
Connector Name:	DNASc9800book	AAA Status:	AAA=Disabled
		Version:	ova-2.3.495

Figure 11-13 Cisco DNA Spaces home page with the hotspot tab

3 Network configuration

Configure Network configuration for your OpenRoaming network

AireOS/Catalyst controllers Meraki Networks

1 / 1 Controllers are configured with Profiles

Controllers	OpenRoaming Profile	Connector	# of APs	Type	Controller Status	Last Configured	Action
WLC	Not Configured	DNASc9800book	0	Catalyst WLC	Active	-	

First | Previous | 1 | Next | Last

(1 - 1 of 1) : 1 pages

Figure 11-14 Cisco DNA Spaces network configuration section

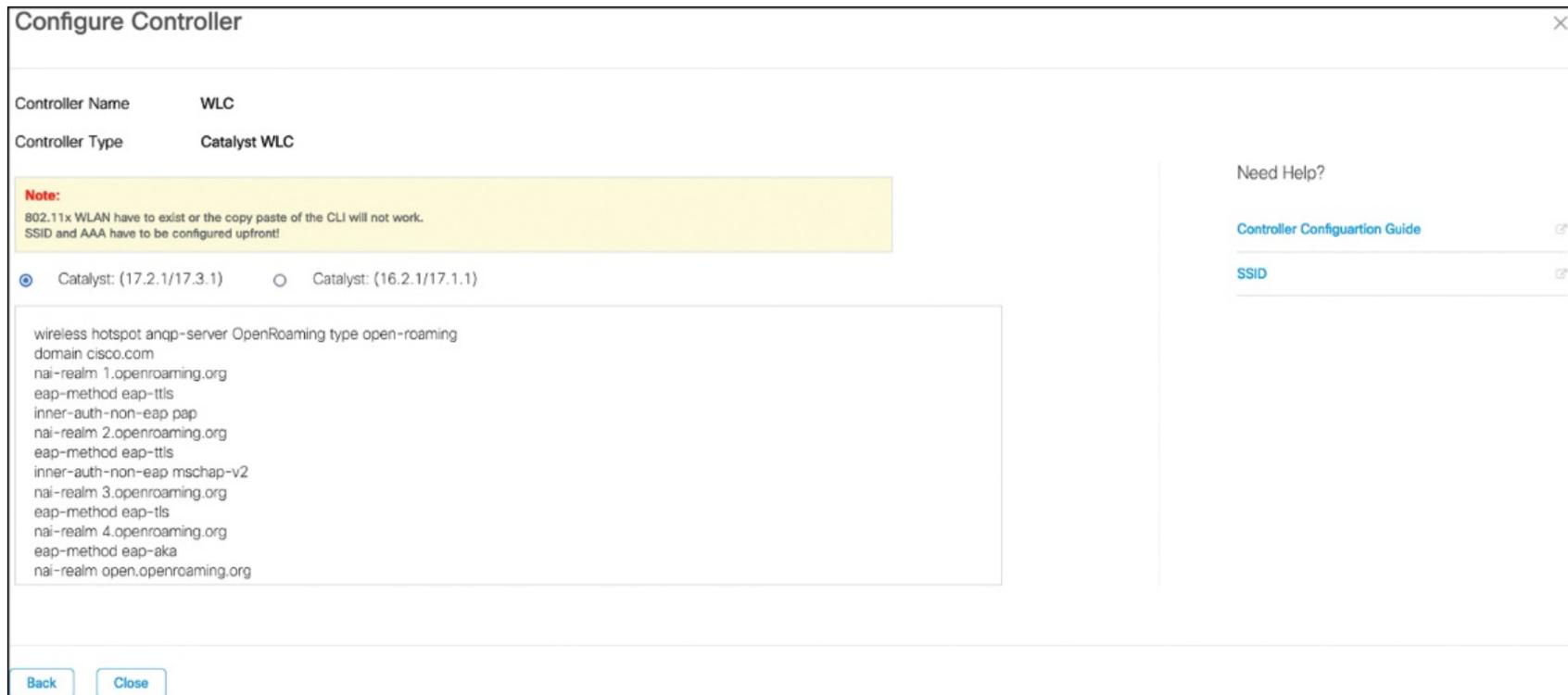


Figure 11-15 Cisco DNA Spaces controller configuration page shows you the command it pushes



Figure 11-16 WLC OpenRoaming configuration page

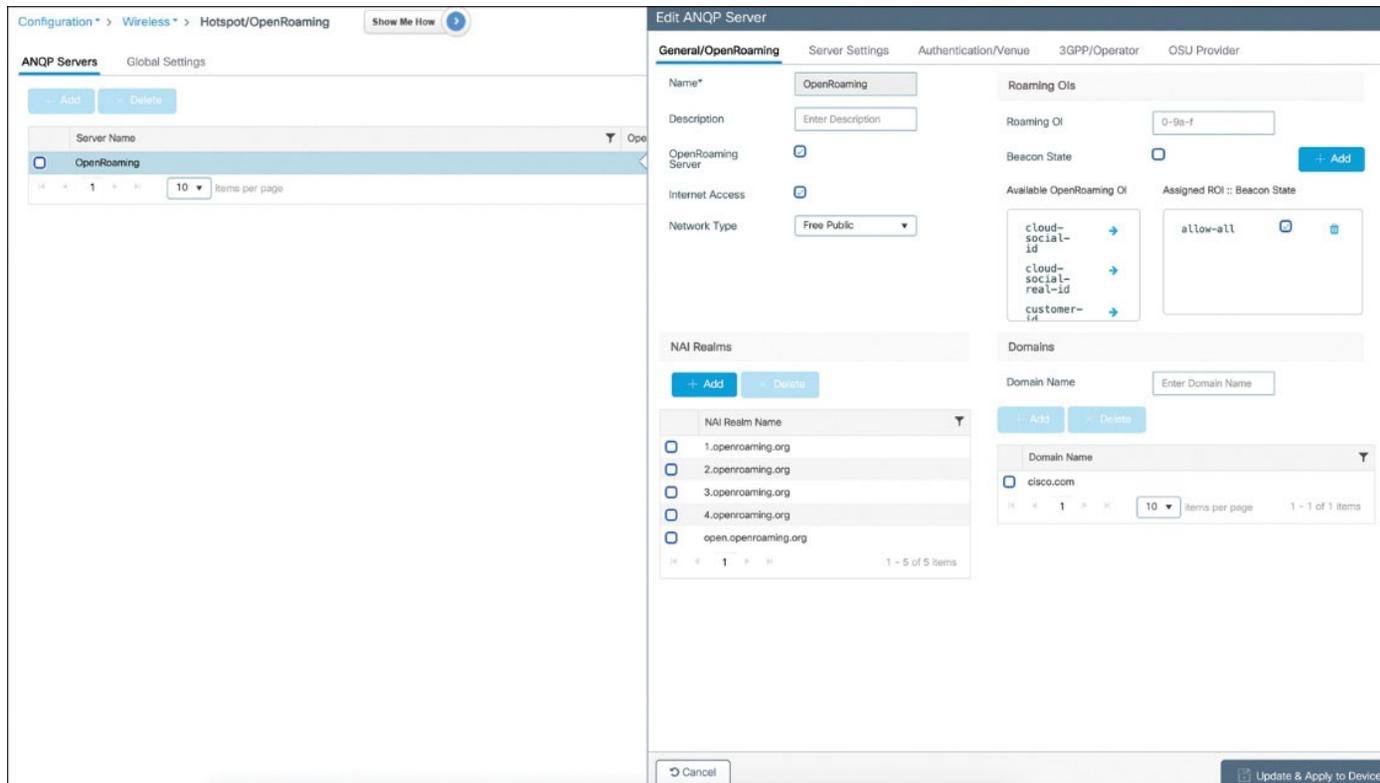


Figure 11-17 WLC OpenRoaming configuration page

Client

360 View General QOS Statistics ATF Statistics Mobility History Call Statistics

General



User Name
fd32d1e4-5345-42c2-9f53-6bf6a5aa5ed8@apple.openroaming.net

MAC Address ce9a.dafe.21ad [Deauthenticate](#)

Uptime(sec) 1011 seconds

WLAN Name OpenRo

AP Name [9130-etage \(Ch: 52\)](#)

Client Performance Signal Strength: -42 dBm Signal Quality: 64 dB
Ch BW(Negotiated/Capable): 20 MHz/80 MHz

Capabilities 802.11ax - 5 GHz

Fabric Status Disabled

Top Applications

No data available

Figure 11-18 OpenRoaming user details on the 9800 WLC

Edit Web Auth Parameter

General **Advanced**

Redirect to external server

Redirect for log-in

Redirect On-Success

Redirect On-Failure

Redirect Append for AP MAC Address

Redirect Append for Client MAC Address

Redirect Append for WLAN SSID

Portal IPv4 Address

Portal IPv6 Address

Express WiFi Key Type

Customized page

Login Failed Page

Login Page

Logout Page

Login Successful Page

Figure 11-19 WLC advanced webauth parameter map configuration screen

The screenshot shows a configuration window titled "Add URL Filter". It has the following fields and controls:

- List Name*:** A text input field containing "DNASpaces".
- Type:** A dropdown menu set to "PRE-AUTH".
- Action:** A radio button labeled "PERMIT" which is selected (checked).
- URLs:** A text area with the instruction "Enter a URL every new line" above it. The text "splash.dnaspaces.io|" is entered in the area.
- Buttons:** "Cancel" and "Apply to Device" are located at the bottom of the window.

Figure 11-20 WLC URL filter allows you to define URLs accessible in the pre-auth phase

AP Gateway Stats

0/60
AP Gateways deployed

0
Advanced BLE Gateway

0
Base BLE Gateway

Access Point Gateways



Deploy DNA Spaces Gateway to your Cisco Access Points

Catalyst 9800 WLC with software version 17.3.1 or above is required. Requires DNAS connector. Currently older WLC(AireOS), eWC, and Meraki are not supported.

You need to have APs with bluetooth capabilities, all new WiFi 6 APs 91XX series, 4800 are supported.

such as 1815, 2800, 3800 support limited gateway functionality, and may require adding a Cisco bluetooth dongle.

Add AP Gateway(s)

Figure 11-21 Cisco DNA Spaces IoT Services menu

Deploy Gateways

1 Choose Gateway Type — 2 Choose Access Points — 3 Review

Select Gateway

Choose the gateway types(s) that you want to deploy in your locations

BLE Gateway

Enables configuration of BLE radio within compatible access points. Radio can be configured to Transmit BLE or Scan for BLE, as well as activate and manage compatible BLE Beacons procured via the DNA Spaces End-Device Marketplace

Cancel

Next

Figure 11-22 Cisco DNA Spaces BLE gateway configuration

Cisco DNA Spaces NET

Home **AP Beacons** Floor Beacons Zigbee COMING SOON

Transmit

IBeacon

0

Transmit

Eddystone UID

0

Transmit

Eddystone URL

1

Filters Actions Bulk Request History

<input type="checkbox"/>	Mac Address	AP Name	AP PID	Label	Profile Type
<input type="checkbox"/>	04:eb:40:9e:b0:80 Out of Sync	AP04EB.409E.0944	C9130AXI-B	Axel - outside box	Eddystone URL Eddystone URL

1 Records

Profile Type* **EDDYSTONE URL** ✓

Eddystone URL* **http://gayag.com**

Label **Axel - outside box**

Power **-21 dBm** Adv. TxPower **0 dBm**

Adv. Interval **0 ms** Mac Address **04:eb:40:9e:b0:80**

BLE Mode **Native** BLE Mac **80:6f:b0:31:f6:22**

AP Name **AP04EB.409E.0944** Firmware **n/a**

AP PID **C9130AXI-B** Last Heard **May 6th, 2020 04:26:24 AM**

Settings

BLE

BLE Mode

S Scan Enable There is a request in progress to enable Scan Mode
Scans for bluetooth devices

T Transmit ✓
Only does beacon transmitting

Figure 11-23 Cisco DNA Spaces allows you to choose the BLE mode of your AP

The screenshot displays the Cisco DNA Spaces interface for managing an Access Point. The left pane shows a summary of AP Gateways (1/3 deployed) and a table of APs. The right pane provides detailed configuration options for a specific AP, including app management for BLE Gateway.

Mac Address	Name	Description
dc:8c:37:4a:ea:80	ap-4800-7	Cisco Aironet 4800 Series (IEEE 802.11ac) Access Po
dc:8c:37:47:38:40	ap-4800-8	Cisco Aironet 4800 Series (IEEE 802.11ac) Access Po
dc:8c:37:11:02:a0	ap-4800-9	Cisco Aironet 4800 Series (IEEE 802.11ac) Access Po

Figure 11-24 Access Point app management in Cisco DNA Spaces

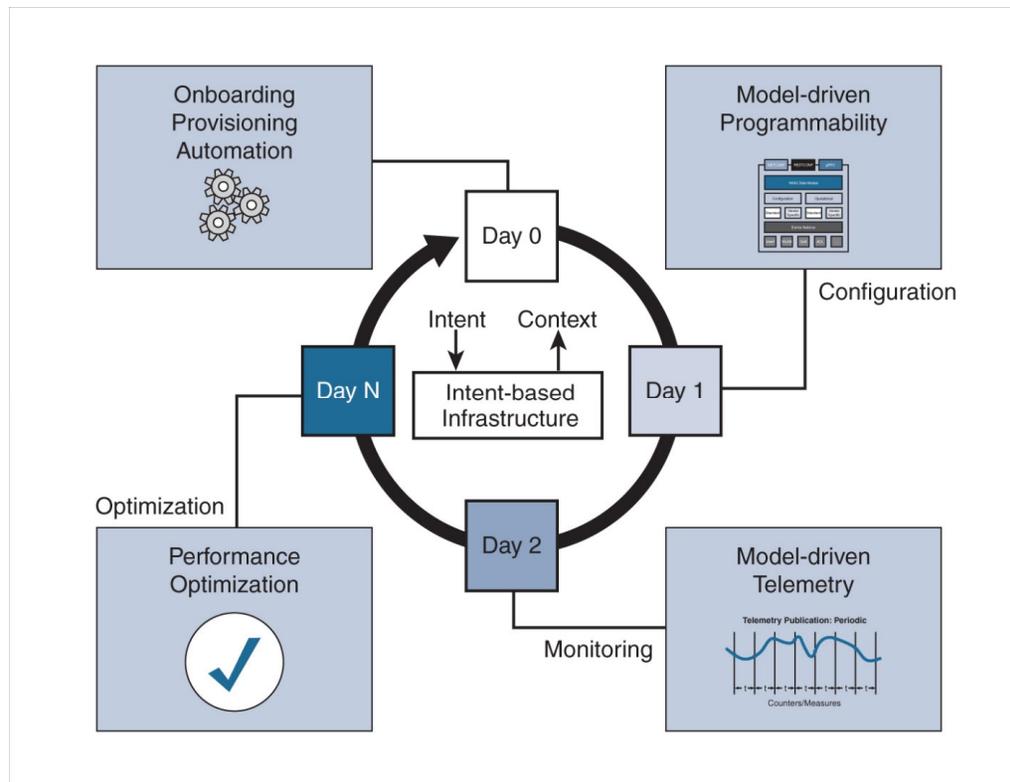


Figure 12-1 Programmability is used along all deployment phases

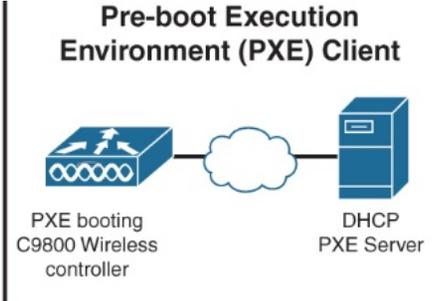
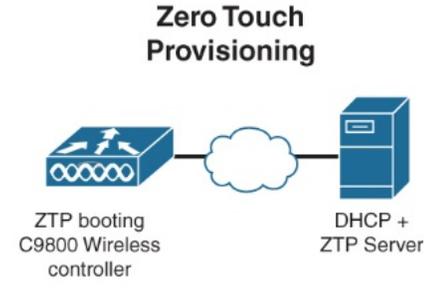
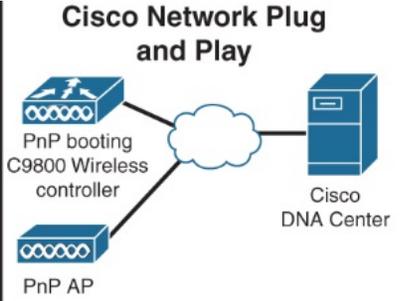
	 <p>Pre-boot Execution Environment (PXE) Client</p>	 <p>Zero Touch Provisioning</p>	 <p>Cisco Network Plug and Play</p>
Image source	Network	Device	Device
Interfaces	Open/Standards based	Open/Standards based	"Turn-key" solution
Key Values	Ideal for heterogeneous/multi-Vendor network environments	Ideal for heterogeneous/multi-Vendor network environments	<ul style="list-style-type: none"> • Optimized for Cisco enterprise networks • Highly secure • Scalable

Figure 12-2 Day 0 protocols

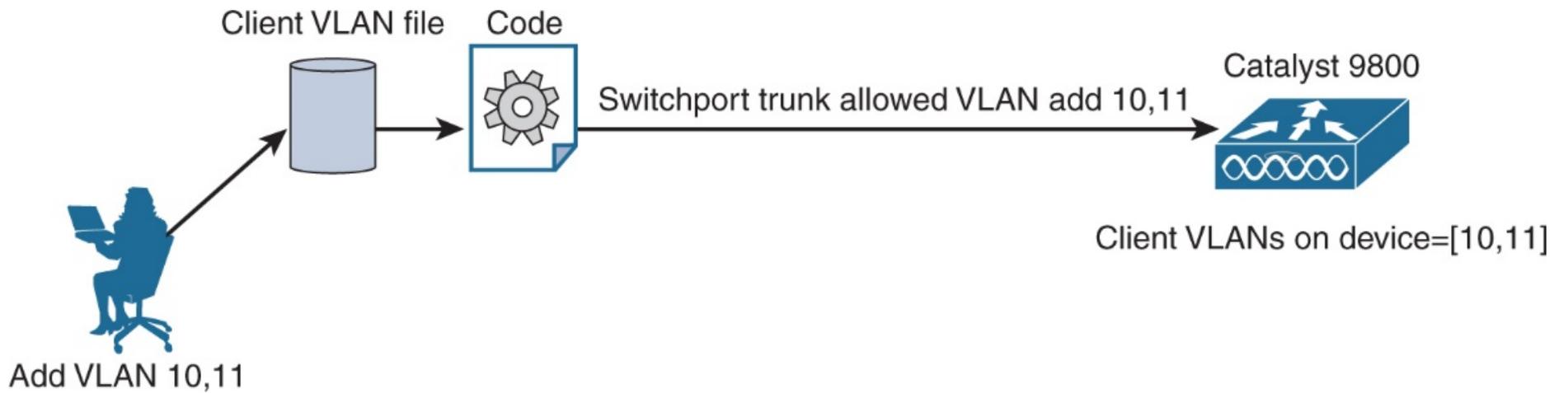


Figure 12-3 Adding client VLANs using the imperative model

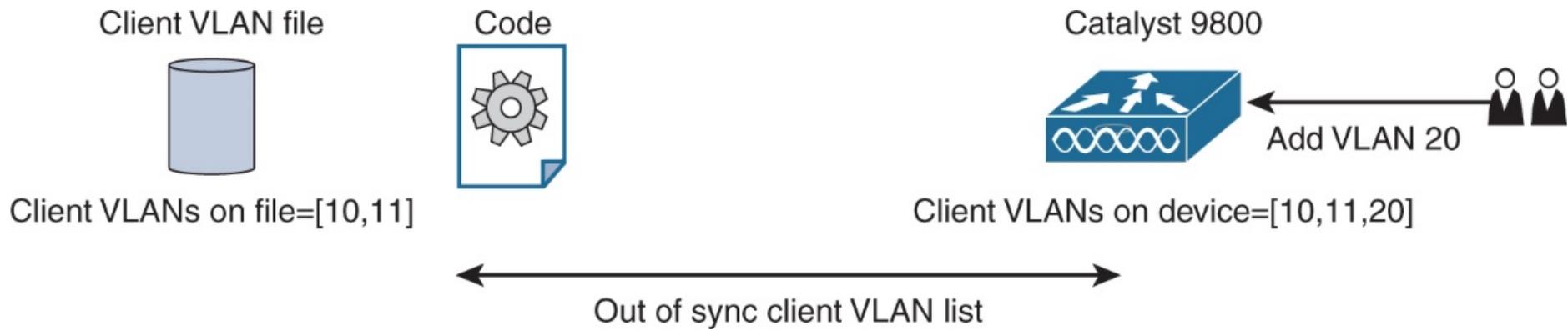


Figure 12-4 Inconsistency by using imperative models

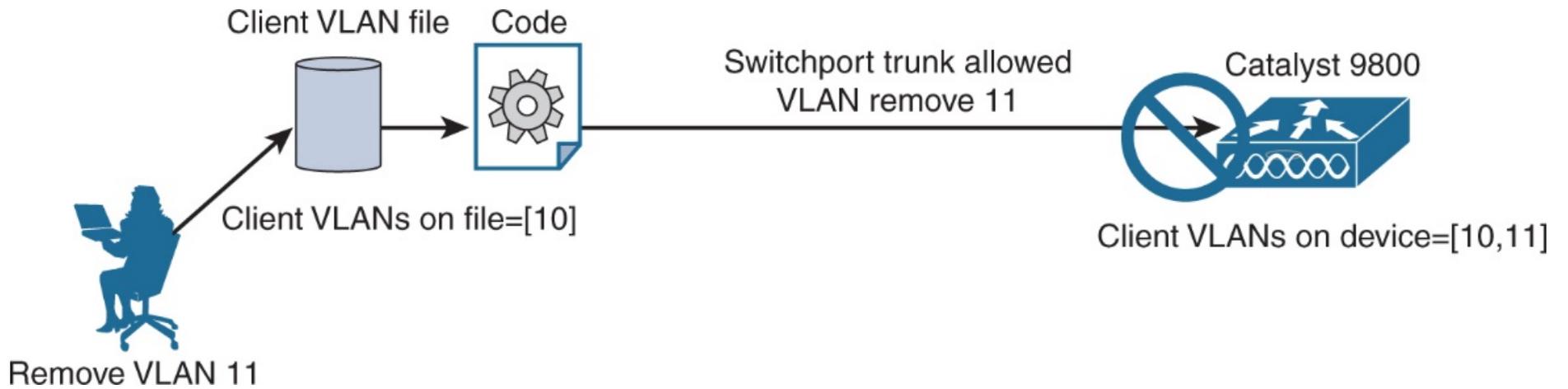


Figure 12-5 Errors when using imperative models

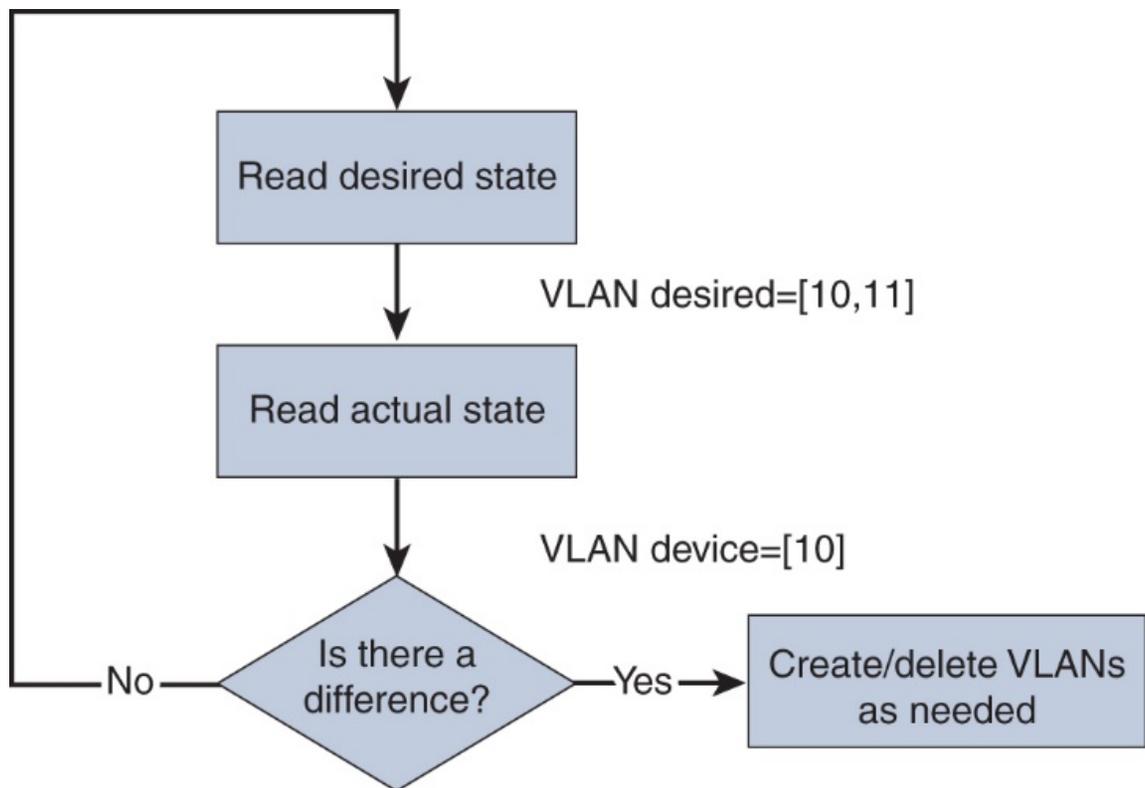


Figure 12-6 Declarative (closed-loop) model

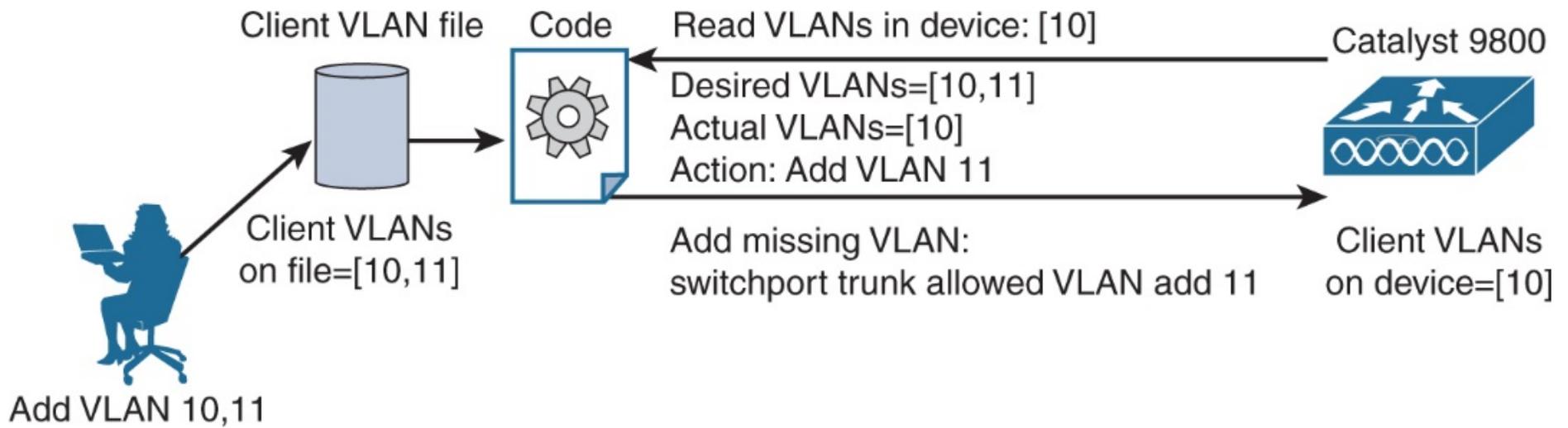


Figure 12-7 Updating data using declarative models

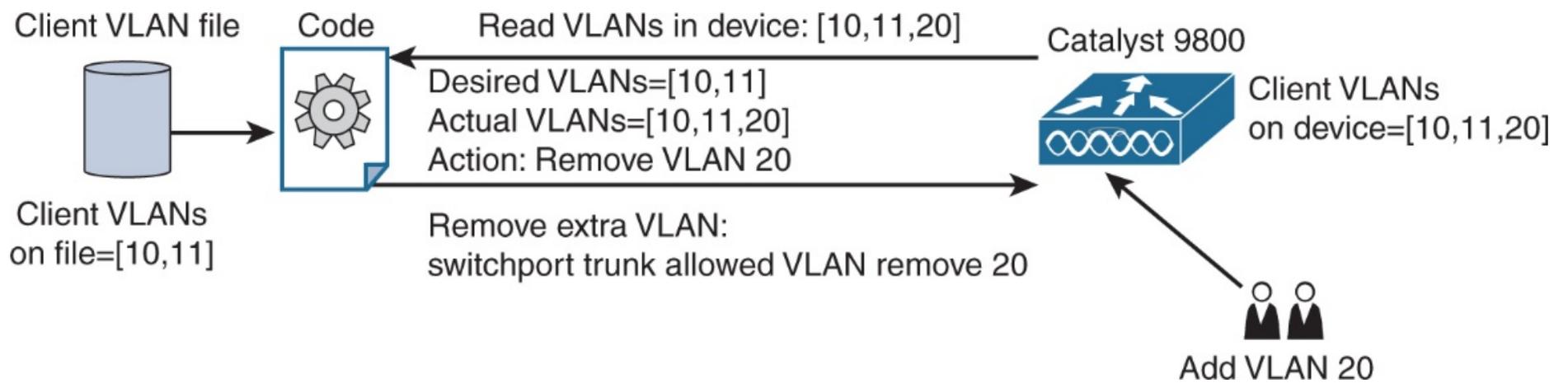


Figure 12-8 Automatic correction using declarative models

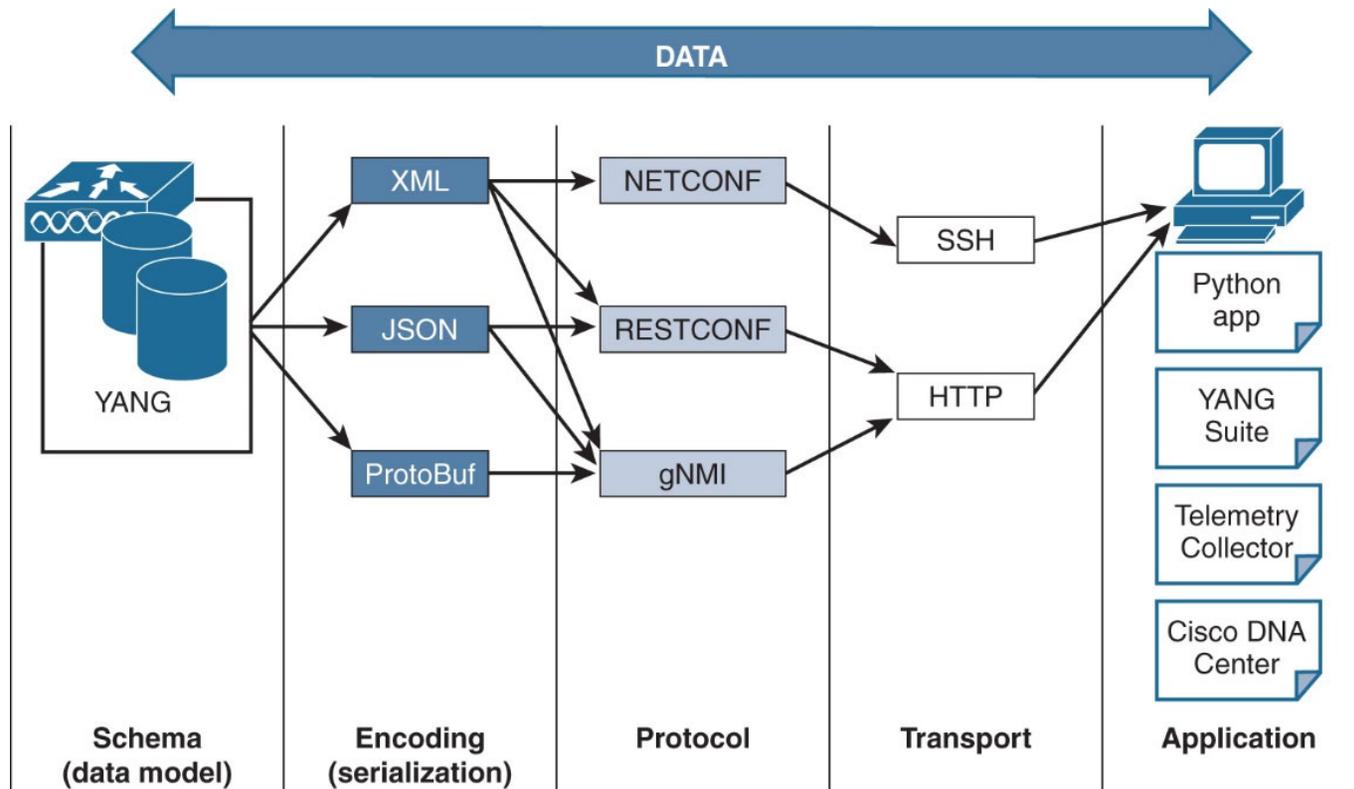


Figure 12-9 Protocols, encoding, and transport

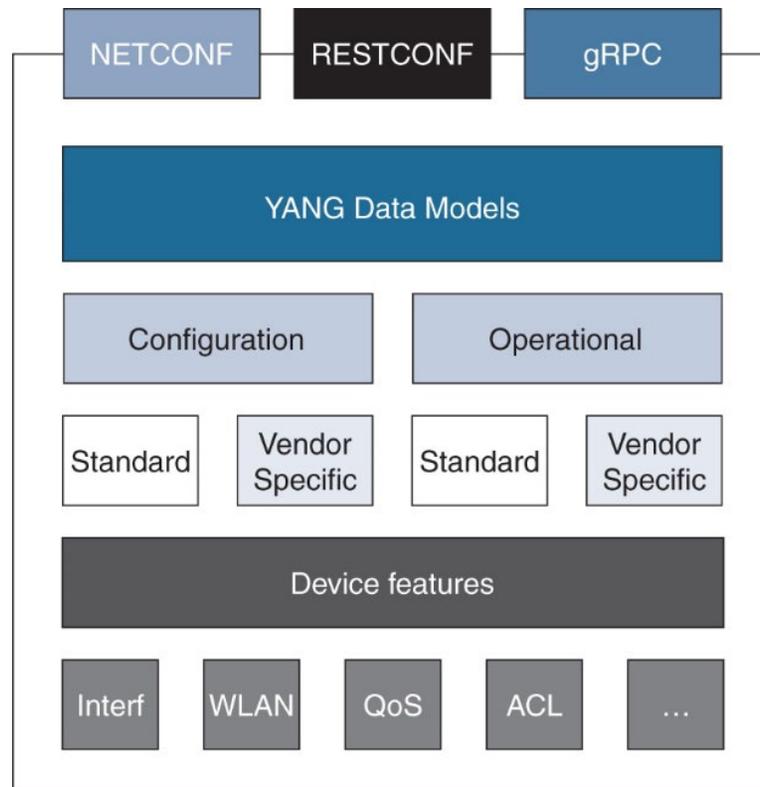


Figure 12-10 Data model and protocol hierarchy

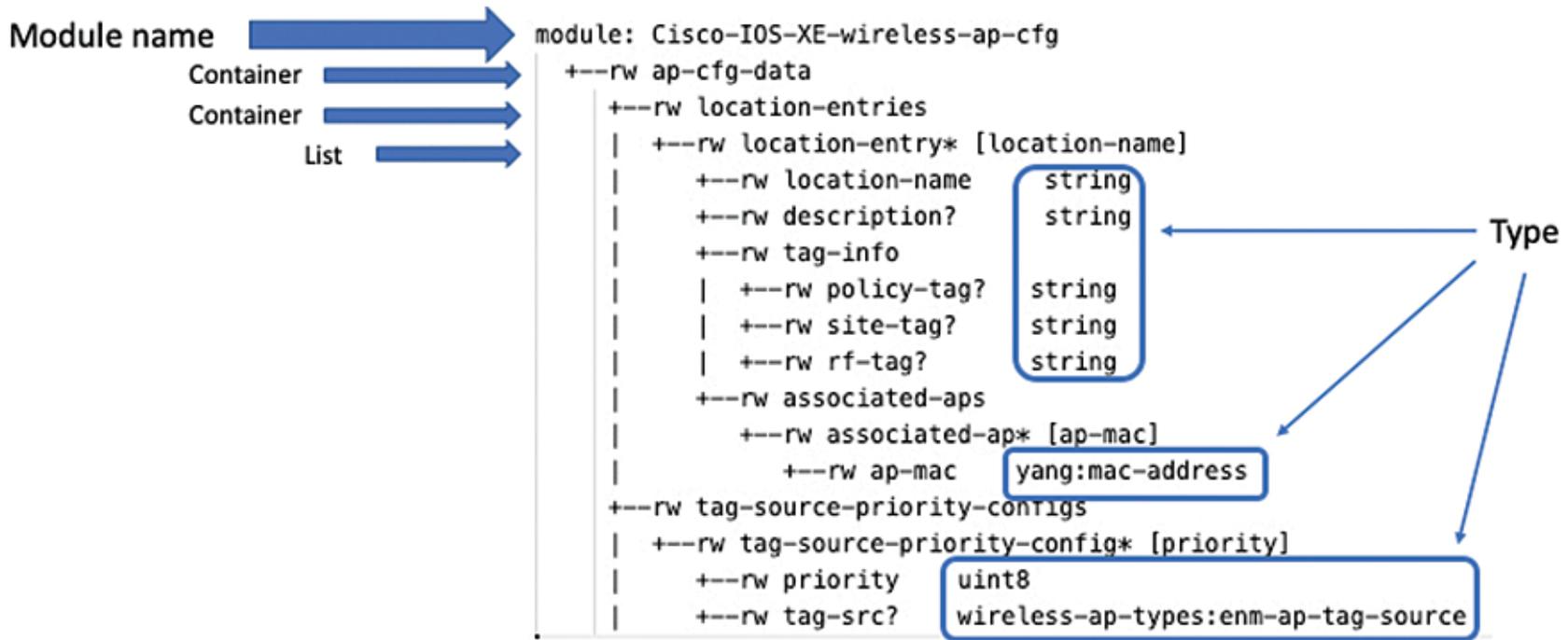


Figure 12-11 YANG module structure

```
Capabilities | <capabilities>
              | <capability>urn:ietf:params:netconf:base:1.0</capability>
              | <capability>urn:ietf:params:netconf:capability:writable-running:1.0</capability>
              | <capability>urn:ietf:params:netconf:capability:rollback-on-error:1.0</capability>
              | <capability>urn:ietf:params:netconf:capability:notification:1.0</capability>
              | <capability>urn:ietf:params:netconf:capability:yang-library:1.0?revision=2016-06-21</capability>
YANG modules | <capability>http://cisco.com/ns/cisco-xe-deviation?module=cisco-xe-deviation;revision=2016-08-10</capability>
              | <capability>http://cisco.com/ns/cisco-xe-routing?module=cisco-xe-unicast-routing;revision=2015-09-11</capability>
              | ...
              | </capabilities>
```

Figure 12-12 NETCONF capabilities

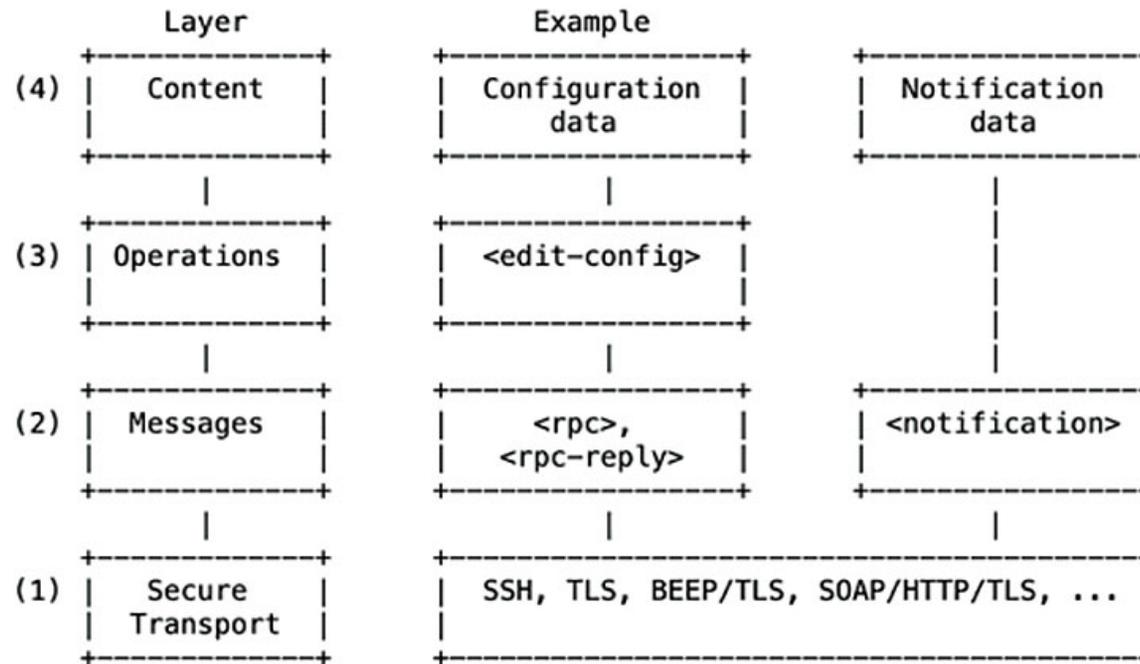


Figure 12-13 NETCONF layers

YANG Suite / YANG module repositories / repo1

Manage YANG module files and repositories

admin

Select a YANG module repository repo1

New repository Clone this repository Delete this repository

YANG modules in repository

Select all Select none Delete selected

Filter

Cisco-IOS-XE-wireless-ap-cfg @ 2021-03-01

Add modules to repository

Upload NETCONF SCP Git

Select device profile vlwc

Check device connectivity Get schema list

wireless

- Cisco-IOS-XE-wireless-access-point-cfg-rpc @ 2021-03-01
- Cisco-IOS-XE-wireless-access-point-cmd-rpc @ 2021-03-01
- Cisco-IOS-XE-wireless-access-point-oper @ 2021-03-01
- Cisco-IOS-XE-wireless-ap-cfg @ 2021-03-01
- Cisco-IOS-XE-wireless-ap-global-oper @ 2021-03-01
- Cisco-IOS-XE-wireless-ap-types @ 2021-03-01
- Cisco-IOS-XE-wireless-apf-cfg @ 2021-03-01
- Cisco-IOS-XE-wireless-awips-oper @ 2020-11-01
- Cisco-IOS-XE-wireless-ble-ltx-oper @ 2020-07-01
- Cisco-IOS-XE-wireless-ble-mgmt-cmd-rpc @ 2020-07-01

Select all Select none

Download selected schemas

Repository status

It appears that the modules currently in this repository depend on the following missing modules.

Please add the missing dependencies or else YANG sets using this repository may be incomplete or invalid.

- Cisco-IOS-XE-wireless-ap-types @ unknown
- cisco-semver @ unknown
- ietf-yang-types @ unknown

Missing YANG dependencies

Figure 12-14 Missing dependencies in a YANG Suite repository

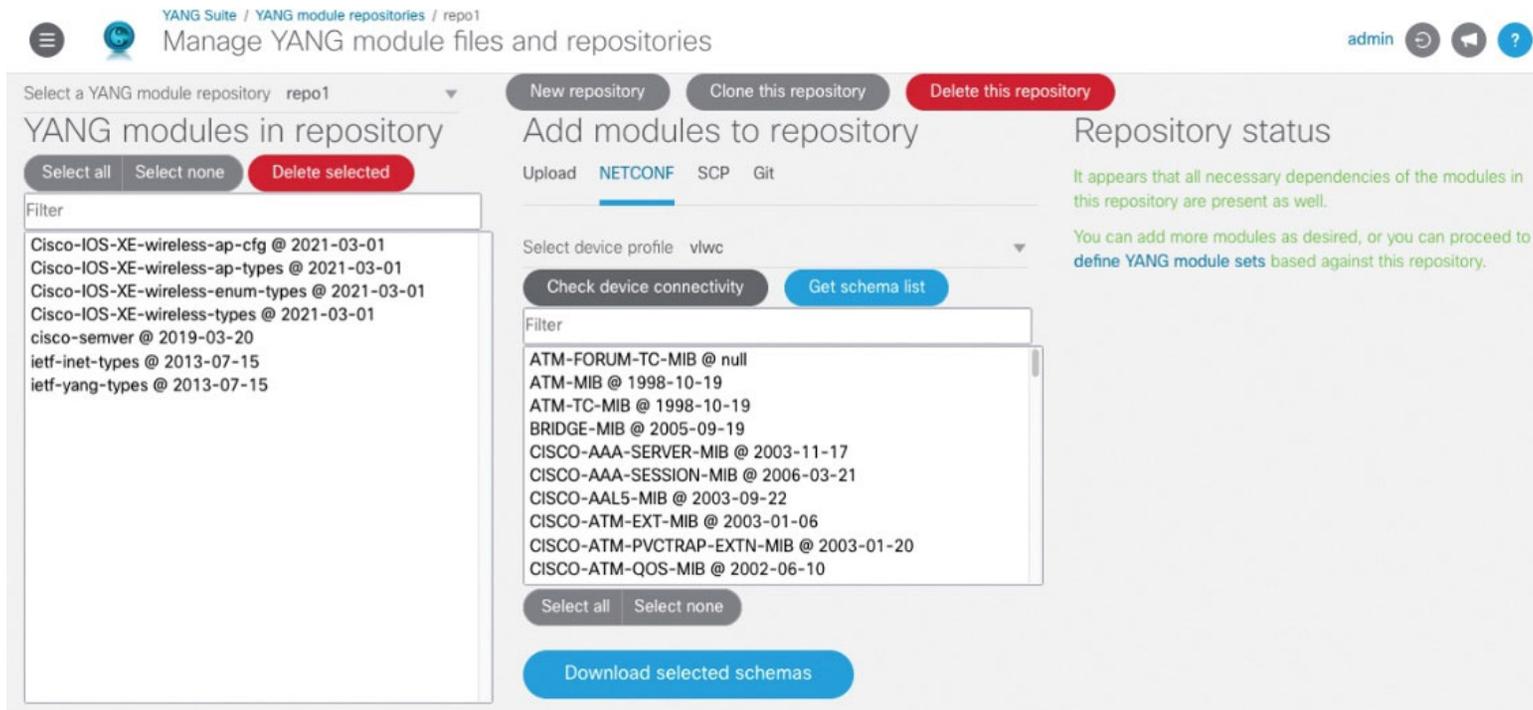


Figure 12-15 YANG Suite repository ready to be used

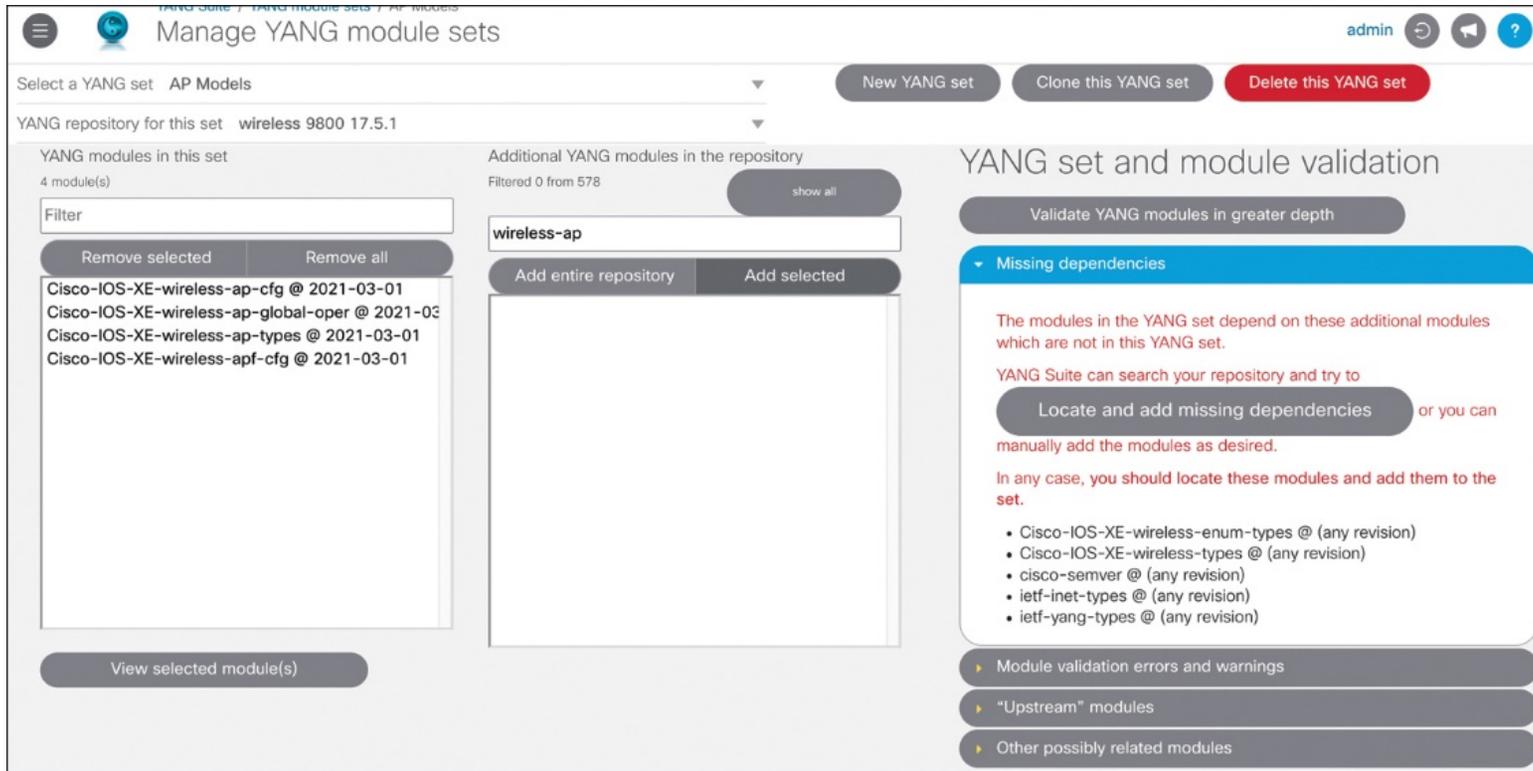


Figure 12-16 YANG Suite displaying missing dependencies

YANG Suite / Exploring YANG / YANG set "AP Models" / Modules

admin

Explore YANG Models

Select a YANG set: AP Models | Select YANG module(s): Cisco-IOS-XE-wireless-ap-cfg x | Load module(s)

Icon legend | Search XPath(s) | Search nodes | Expand all nodes | Display schema nodes only | Display all nodes

Cisco-IOS-XE-wireless-ap-cfg

- ap-cfg-data
 - location-entries
 - tag-source-priority-configs
 - ap-filter-configs
 - ap-filter-priority-cfg-entries
 - ap-rule-priority-cfg-entries
 - ap-tags
 - ap-tag
 - ap-mac
 - policy-tag
 - site-tag
 - rf-tag

Node Properties

Name	ap-tags
Nodetype	container
Description	Configuration of AP tags
Module	Cisco-IOS-XE-wireless-ap-cfg
Revision	2021-03-01
Xpath	/ap-cfg-data/ap-tags
Prefix	wireless-ap-cfg
Namespace	http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-ap-cfg
Access	read-write
Operations	<ul style="list-style-type: none"> "edit-config" "get-config" "get"
Schema Node Id	/ap-cfg-data/ap-tags

Reference URL:
<https://tools.ietf.org/html/rfc6020#section-7.5>
 7.5. The container Statement

The "container" statement is used to define an interior data node in the schema tree. It takes one argument, which is an identifier, followed by a block of substatements that holds detailed container information.

A container node does not have a value, but it has a list of child nodes in the data tree. The child nodes are defined in the container's substatements.

Bjorklund Standards Track [Page 51]

Figure 12-17 Exploring YANG models

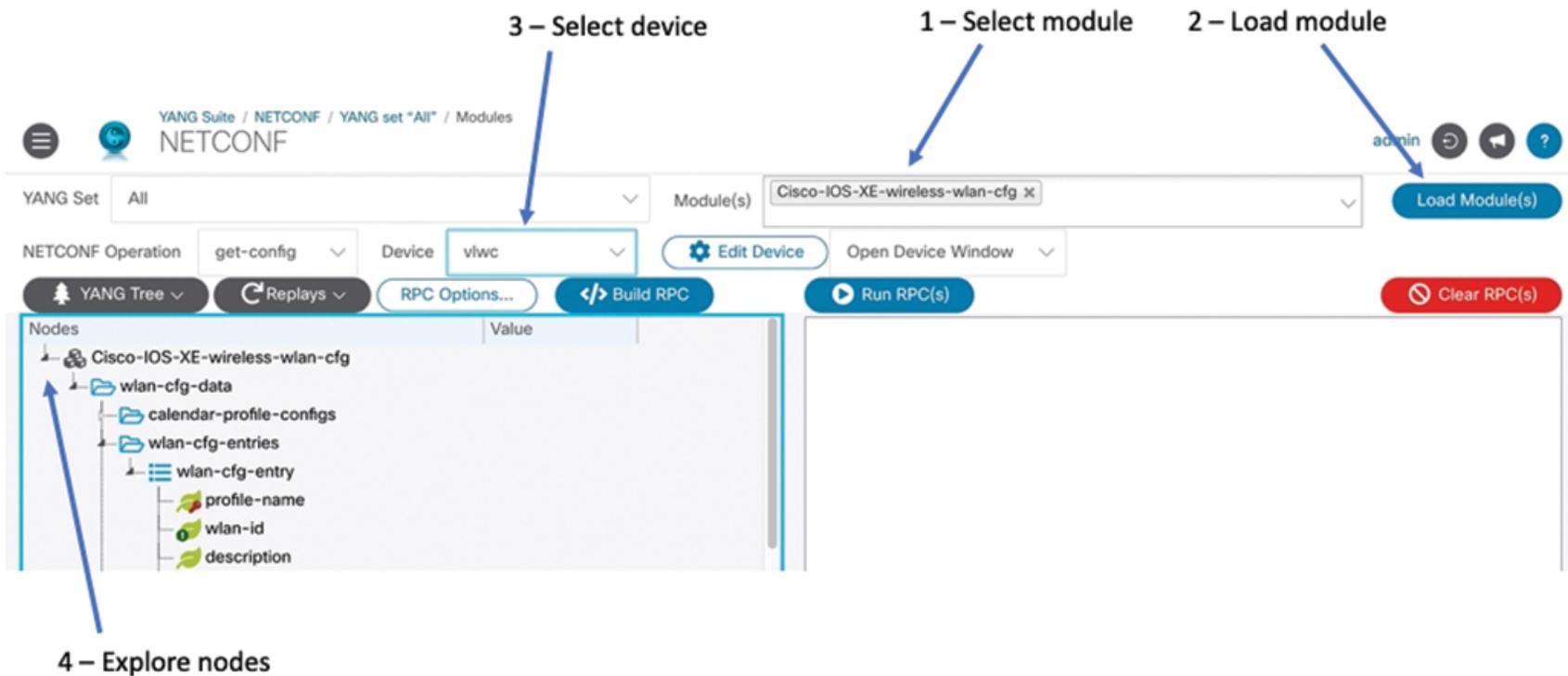


Figure 12-18 Exploring data in YANG Suite

YANG Set: All | Module(s): Cisco-IOS-XE-wireless-wlan-cfg x | Load Module(s)

NETCONF Operation: get-config | Device: vlwc | Edit Device | Open Device Window

Buttons: YANG Tree | Replays | RPC Options... | Build RPC | Run RPC(s) | Clear RPC(s)

Nodes

Nodes	Value
Cisco-IOS-XE-wireless-wlan-cfg	
wlan-cfg-data	
calendar-profile-configs	
wlan-cfg-entries	<input checked="" type="checkbox"/>
wlan-cfg-entry	
wlan-policies	
policy-list-entries	
wireless-aaa-policy-configs	
guest-lan-configs	
guest-lan-maps	

```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
  <get-config>
    <source>
      <running/>
    </source>
    <filter>
      <wlan-cfg-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-wlan-cfg">
        <wlan-cfg-entries/>
      </wlan-cfg-data>
    </filter>
  </get-config>
</rpc>
```

Figure 12-19 Building RPCs in YANG Suite

```
1 → <nc:rpc xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="...">
2 → <nc:get-config>
   <nc:source>
3 → <nc:running/>
   </nc:source>
   <nc:filter>
4 → <wlan-cfg-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-wlan-cfg">
5 → <wlan-cfg-entries/>
   </wlan-cfg-data>
   </nc:filter>
   </nc:get-config>
</nc:rpc>
```

Figure 12-20 NETCONF RPC request

```

1 → <rpc-reply message-id="..." xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0">
    <data>
2 → <wlan-cfg-data xmlns="http://cisco.com/ns/yang/Cisco-IOX-XE-wireless-wlan-cfg">
3 → <wlan-cfg-entries>
4 → <wlan-cfg-entry>
    <profile-name>test_wlan_1</profile-name>
    <wlan-id>1</wlan-id>
    <wep-key-index>1</wep-key-index>
    <multicast-buffer-value>0</multicast-buffer-value>
    <apf-vap-id-data>
    <ssid>test_wlan_1</ssid>
    </apf-vap-id-data>
    </wlan-cfg-entry>
5 → <wlan-cfg-entry>
    <profile-name>test_wlan_2</profile-name>
    <wlan-id>2</wlan-id>
    <wep-key-index>1</wep-key-index>
    <multicast-buffer-value>0</multicast-buffer-value>
    <apf-vap-id-data>
    <ssid>test_wlan_2</ssid>
    <wlan-status>true</wlan-status>
    </apf-vap-id-data>
    </wlan-cfg-entry>
    </wlan-cfg-entries>
    </wlan-cfg-data>
    </data>
</rpc-reply>

```

Figure 12-21 NETCONF RPC reply

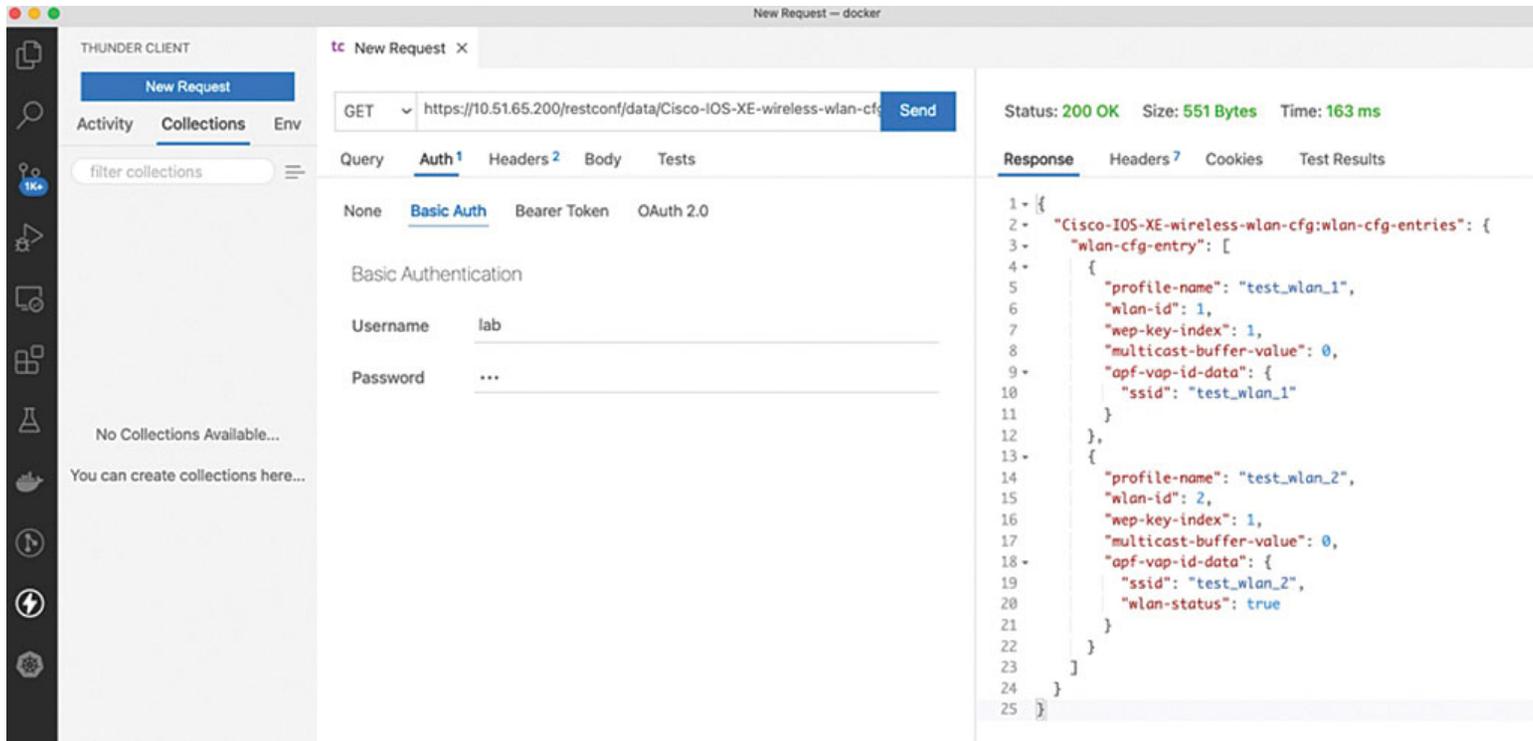


Figure 12-22 Thunder plug-in for Visual Studio Code

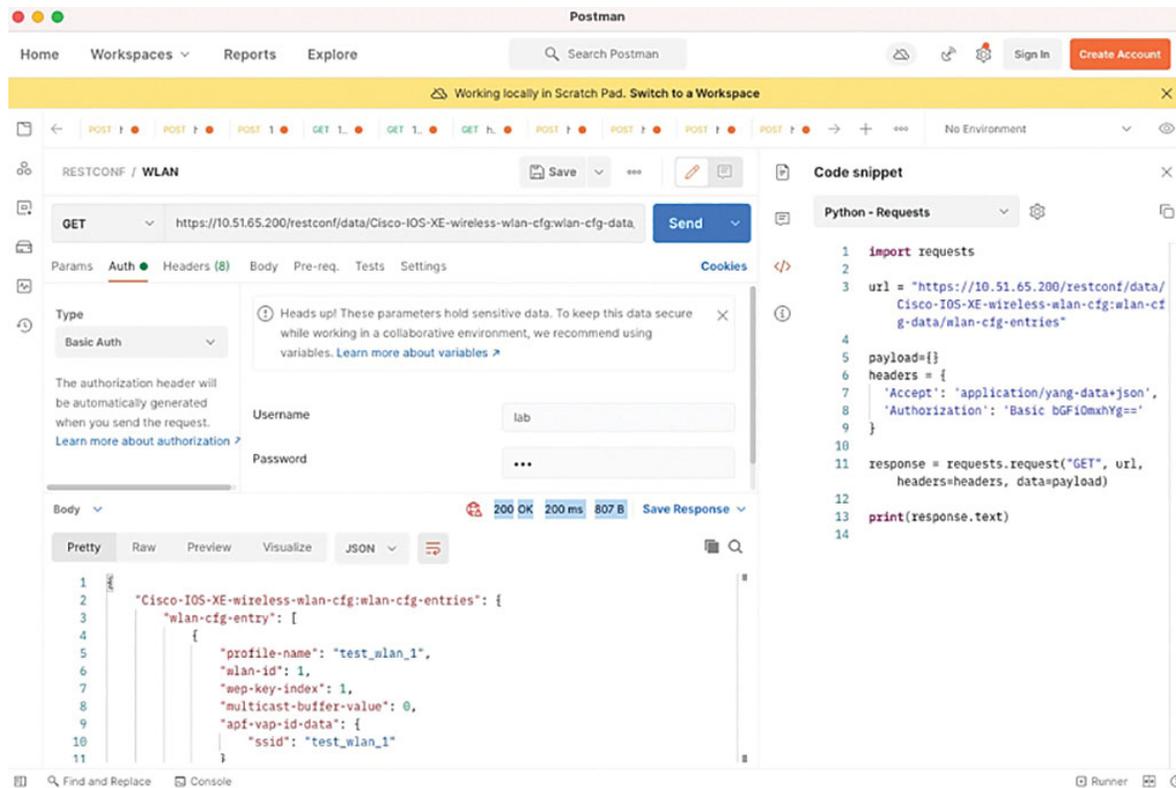


Figure 12-23 Postman

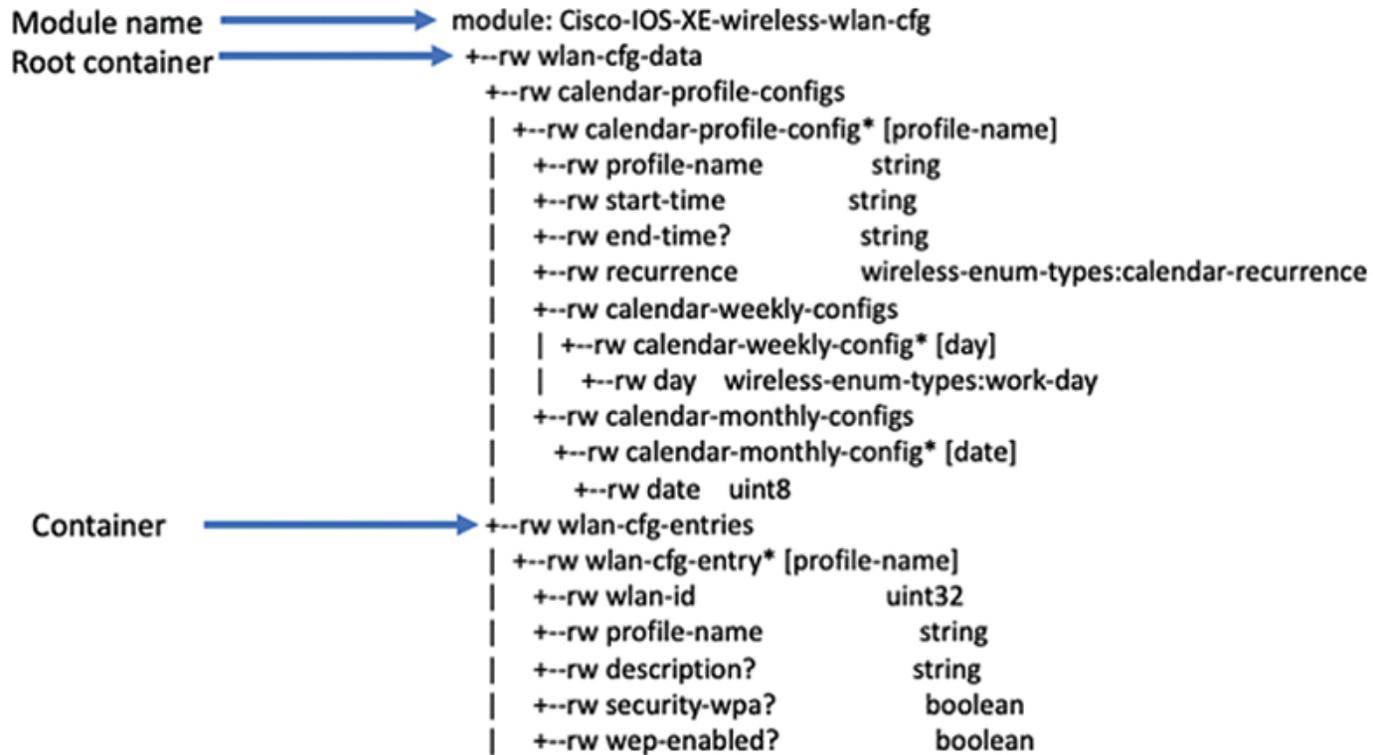


Figure 12-24 WLAN YANG Model

/restconf/data/Cisco-IOS-XE-wireless-wlan-cfg:wlan-cfg-data/wlan-cfg-entries

root resource	YANG Module	root container	container
---------------	-------------	----------------	-----------

Figure 12-25 Constructing URI from YANG data model

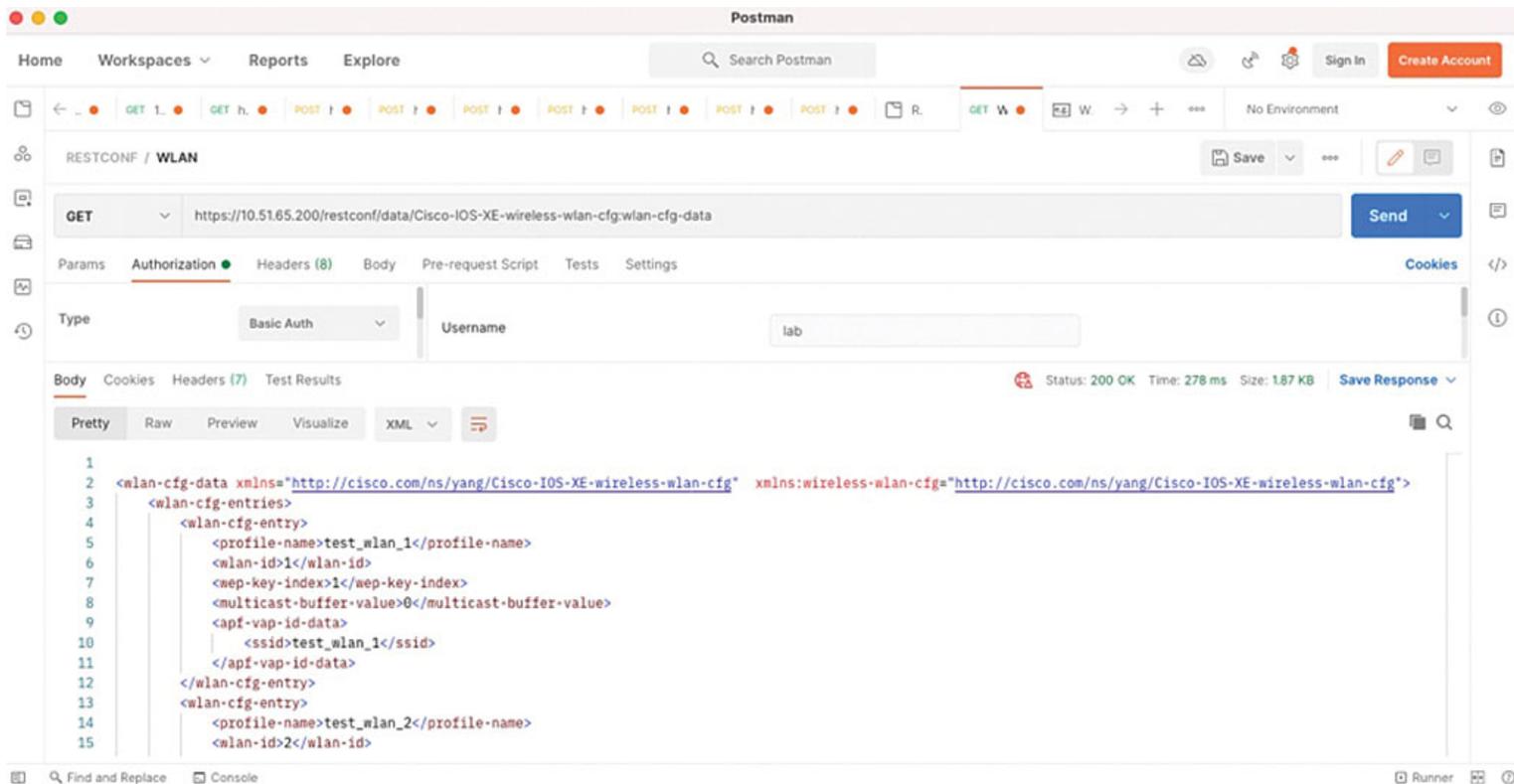


Figure 12-26 Using Postman to retrieve a list of WLANs

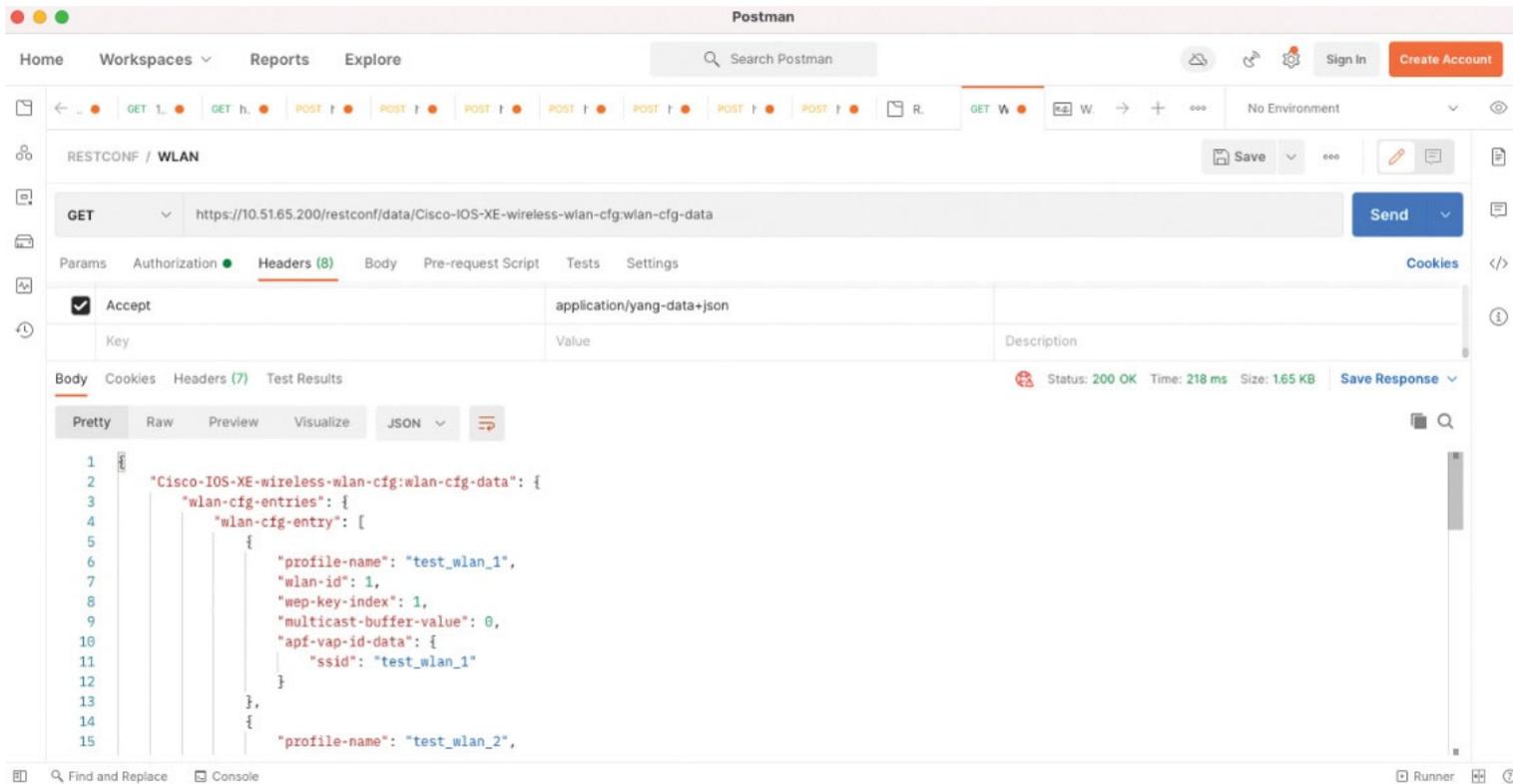


Figure 12-27 Requesting JSON data in Postman

YANG Suite / Exploring YANG / YANG set "WLAN" / Modules

Explore YANG Models

admin

Select a YANG set: WLAN | Select YANG module(s): Cisco-IOS-XE-wireless-wlan-cfg x | Load module(s)

Icon legend | Search XPath | Search nodes | Expand all nodes

Display schema nodes only | Display all nodes

Cisco-IOS-XE-wireless-wlan-cfg

- wlan-cfg-data
 - calendar-profile-configs
 - wlan-cfg-entries
 - wlan-cfg-entry** ← List
 - profile-name ← Key
 - wlan-id
 - description
 - security-wpa
 - wep-enabled
 - webauth-enabled
 - cond-web-redirect
 - splash-web-redirect
 - dot11-auth-type

Name	wlan-cfg-entry
Nodetype	list
Description	List of WLAN config parameters
Module	Cisco-IOS-XE-wireless-wlan-cfg
Revision	2021-03-01
Xpath	/wlan-cfg-data/wlan-cfg-entries/wlan-cfg-entry
Prefix	wireless-wlan-cfg
Namespace	http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-wlan-cfg
Keys	<ul style="list-style-type: none"> "profile-name"
Access	read-write
Operations	<ul style="list-style-type: none"> "edit-config" "get-config" "get"

Figure 12-28 List and key in the WLAN config entry model

/restconf/data/Cisco-IOS-XE-wireless-wlan-cfg:wlan-cfg-data/wlan-cfg-entries/wlan-cfg-entry=test_wlan_1

root resource	YANG Module	root container	container	list	search key
---------------	-------------	----------------	-----------	------	------------

Figure 12-29 Constructing searches in RESTCONF

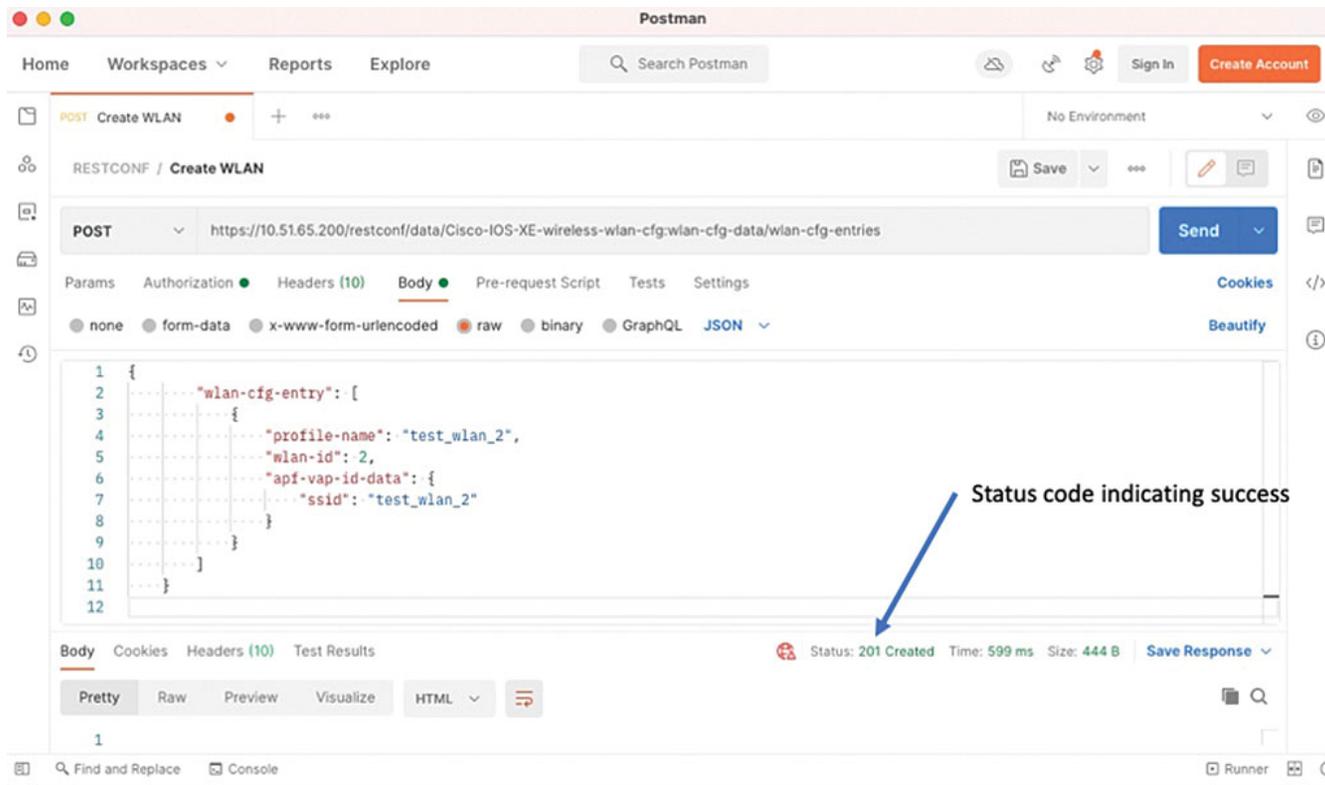


Figure 12-30 Adding a new WLAN using Postman

Params	Authorization ●	Headers (10)	Body ●	Pre-request Script	Tests	Settings
<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/> Content-Length ⓘ				<calculated when request is sent>
<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/> Host ⓘ				<calculated when request is sent>
<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/> User-Agent ⓘ				PostmanRuntime/7.28.0
<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/> Accept ⓘ				*/*
<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/> Accept-Encoding ⓘ				gzip, deflate, br
<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/> Connection ⓘ				keep-alive
<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/> Content-Type ⓘ				application/yang-data+json

 **New header**

Figure 12-31 Content-type header

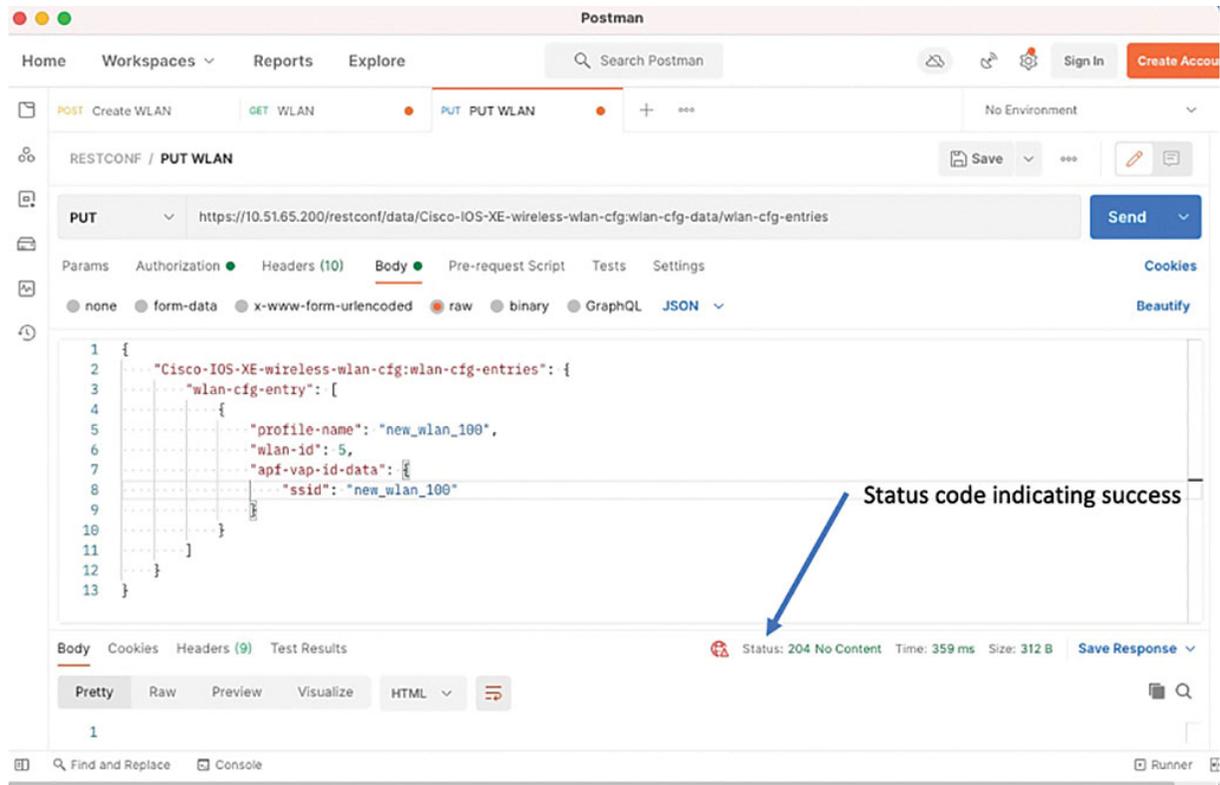


Figure 12-32 Replacing WLAN configuration using Postman

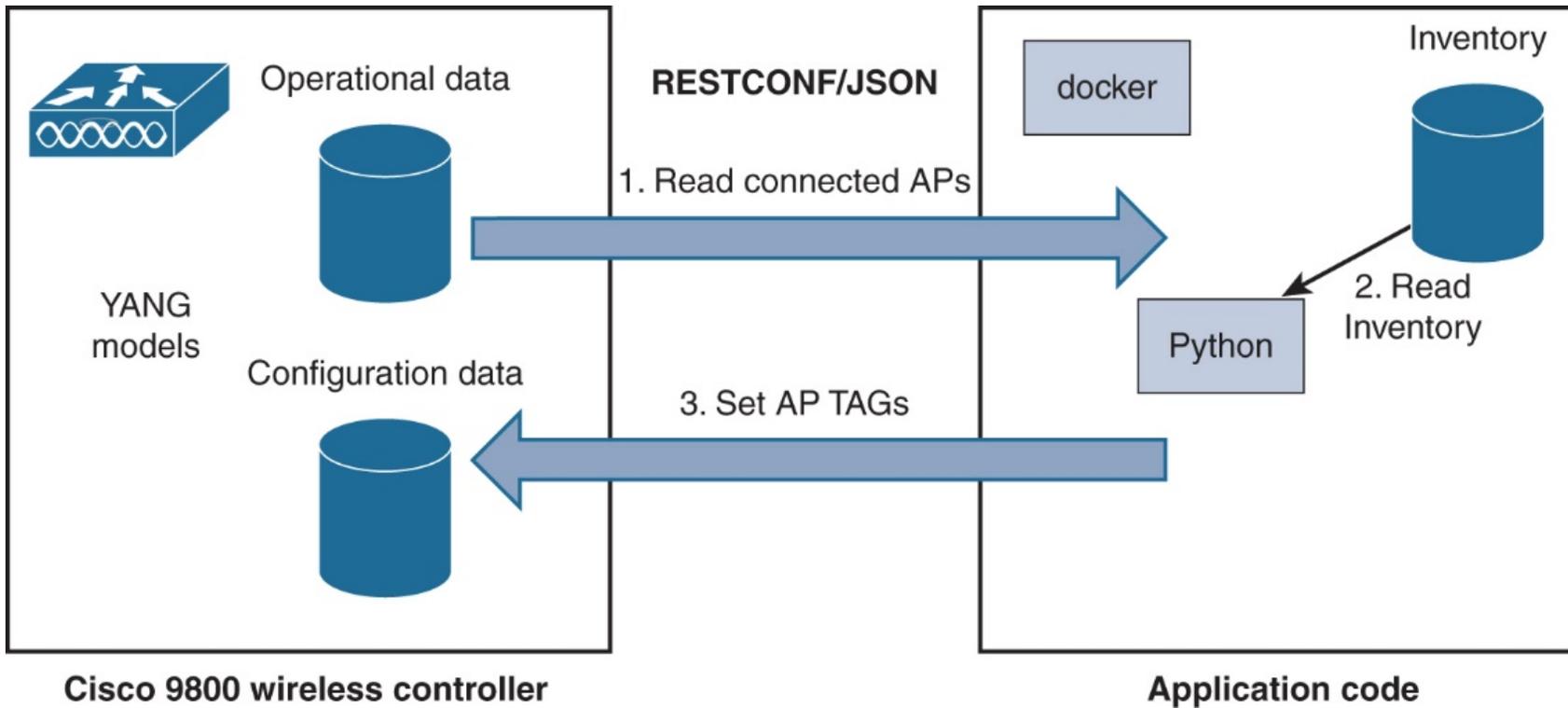


Figure 12-33 Python application to assign a tag based on the AP serial number



Figure 12-34 Inventory file

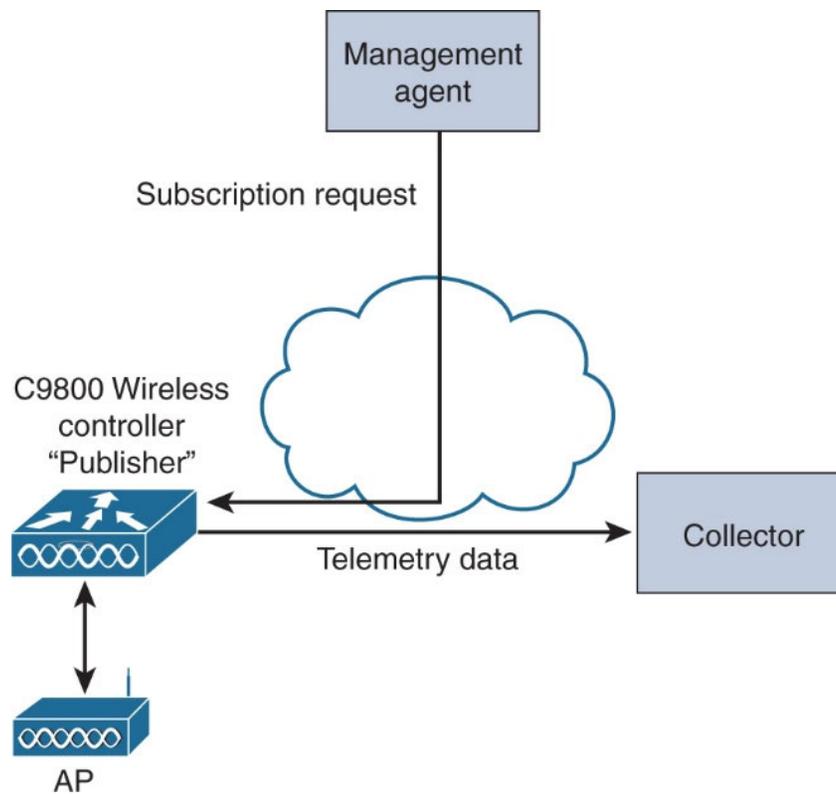


Figure 13-1 Roles in model-driven telemetry

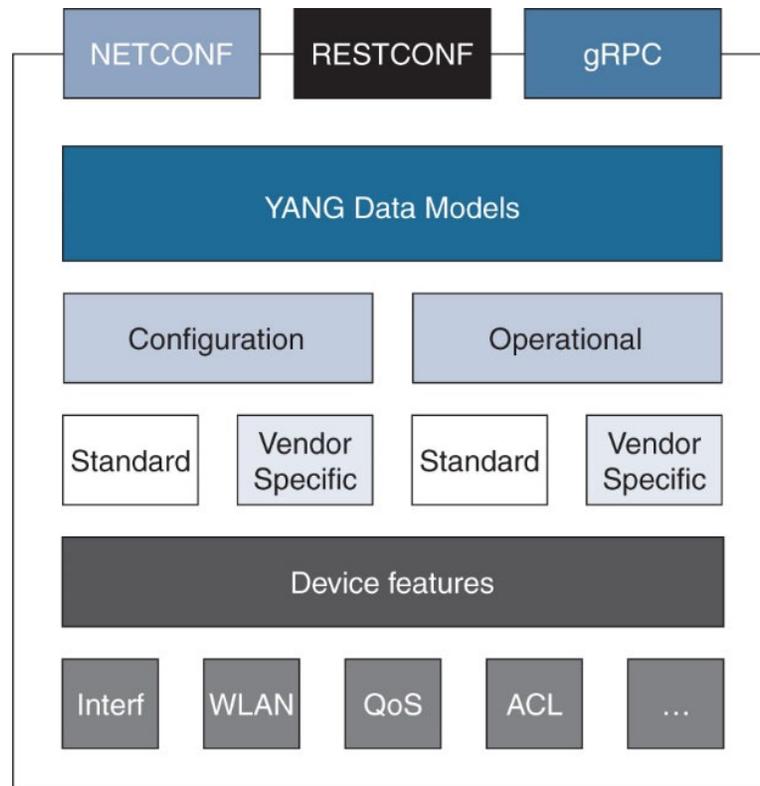


Figure 13-2 Configuration and operational YANG data models

```
202 container ap-global-oper-data {
203     config false; ← Indicates this is an operational model
204     description
205         "Root container for AP operational data aggregated across wireless processes";
206     container ap-img-predownload-stats {
207         presence "ap-img-predownload-stats";
208         description
209             "AP image predownload stats";
210         uses wireless-ap-global-oper:global-ap-stats;
211     }
212     list ap-join-stats {
213         key "wtp-mac";
214         description
215             "AP join statistics";
216         uses wireless-ap-global-oper:st-empltd-ap-stats-info;
217     }
218 }
219 }
```

Figure 13-3 Identifying an operational YANG model

YANG Suite / Exploring YANG / YANG set "wlc-default-yangset" / Modules

Explore YANG Models

admin   

Select a YANG set: wlc-default-yangset Select YANG module(s): ietf-interfaces

Display schema nodes only Display all nodes

ietf-interfaces

- interface-type
- interface-ref
- interface-state-ref
- interfaces**
- interfaces-state

Node Properties	
Name	interfaces
Nodetype	container
Description	Interface configuration parameters.
Module	ietf-interfaces
Revision	2014-05-08
Xpath	/interfaces
Prefix	if
Namespace	urn:ietf:params:xml:ns:yang:ietf-interfaces
Access	read-write
Operations	<ul style="list-style-type: none"> "edit-config" "get-config" "get"
Schema Node Id	/interfaces

Figure 13-4 Configuration container for interfaces

YANG Suite / Exploring YANG / YANG set "wlc-default-yangset" / Modules

Explore YANG Models

admin

Select a YANG set: wlc-default-yangset

Select YANG module(s): ietf-interfaces x

Load module(s)

Icon legend | Search XPath | Search nodes | Expand all nodes

Display schema nodes only
 Display all nodes

ietf-interfaces

- interface-type
- interface-ref
- interface-state-ref
- interfaces
- interfaces-state**

Node Properties

Name	interfaces-state
Nodetype	container
Description	Data nodes for the operational state of interfaces.
Module	ietf-interfaces
Revision	2014-05-08
Xpath	/interfaces-state
Prefix	if
Namespace	urn:ietf:params:xml:ns:yang:ietf-interfaces
Access	read-only
Operations	• "get"
Schema Node Id	/interfaces-state

Figure 13-5 Operational container for interfaces-state

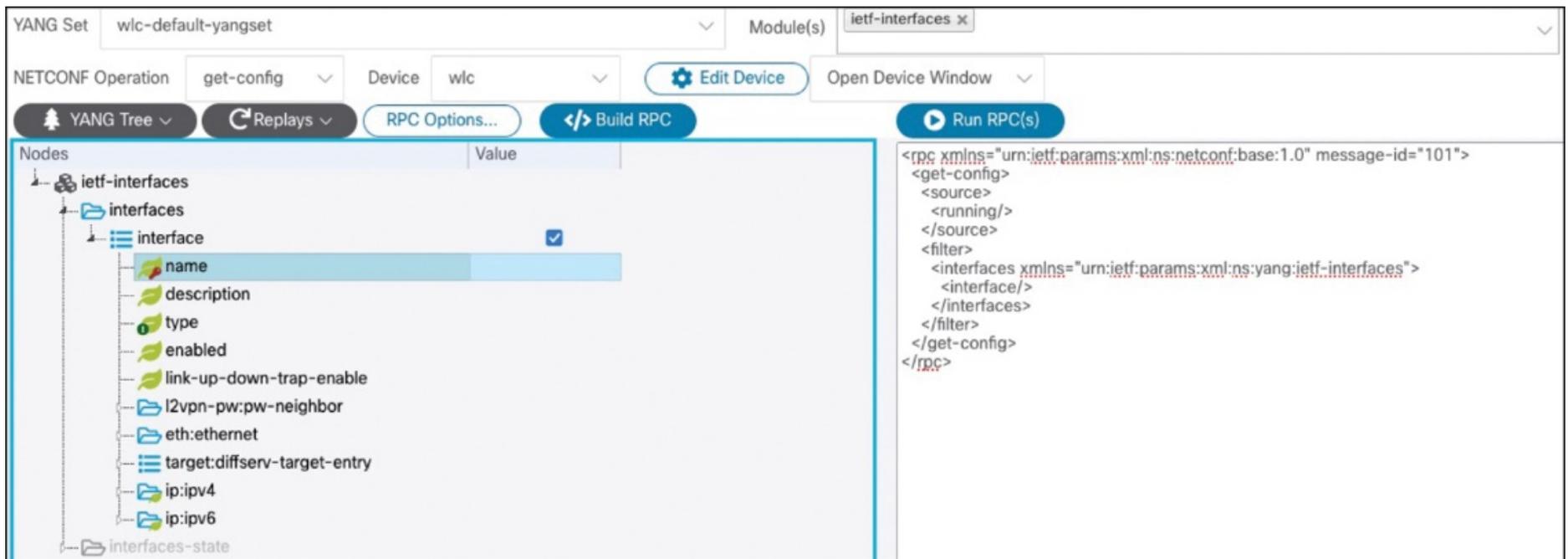


Figure 13-6 RPC to read configured interfaces using NETCONF

```
get-config operation > <rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
  <get-config>
    <source>
      <running/>
    </source>
    <filter>
      <interfaces xmlns="urn:ietf:params:xml:ns:yang:ietf-interfaces">
        <interface/>
      </interfaces>
    </filter>
  </get-config>
</rpc>
```

Figure 13-7 NETCONF query RPC to get interface list

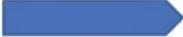
```
GET operation  <rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
  <get>
    <filter>
      interfaces-state container  <interfaces-state xmlns="urn:ietf:params:xml:ns:yang:ietf-interfaces">
        <interface>
          <name/>
          <oper-status/>
        </interface>
      </interfaces-state>
    </filter>
  </get>
</rpc>
```

Figure 13-8 NETCONF RPC to read the interfaces operational state

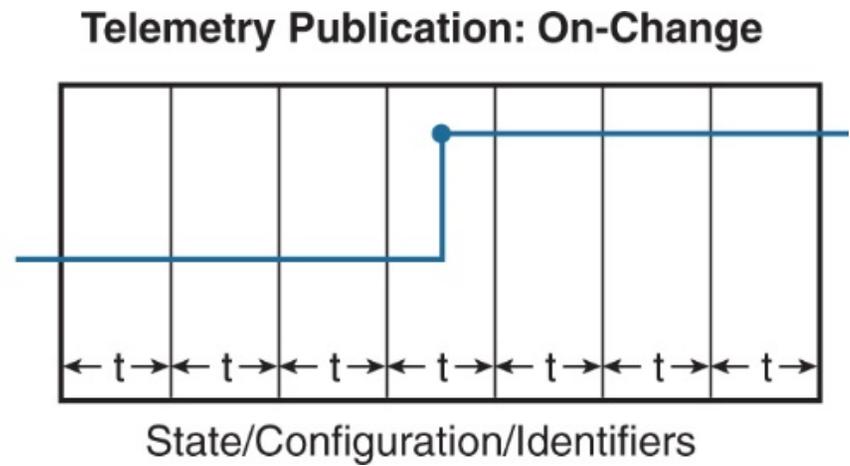
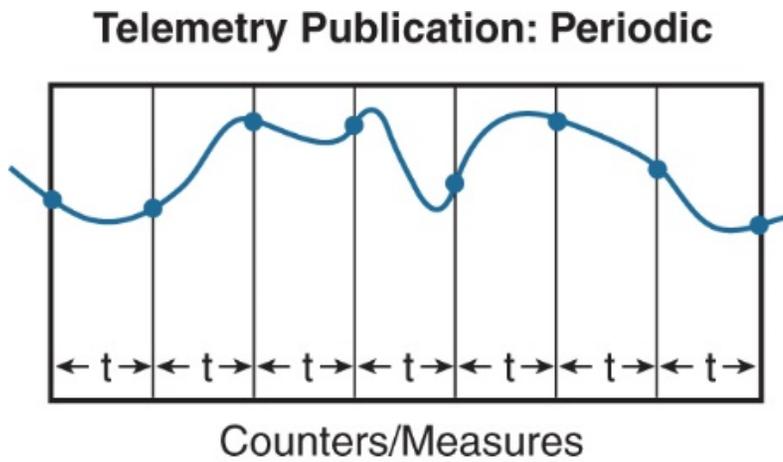


Figure 13-9 Periodic versus on-change publications

```
1 module Cisco-IOS-XE-wireless-ap-global-oper {
2   yang-version 1;
3   namespace "http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-ap-global-oper";
4   prefix wireless-ap-global-oper;
5
6   import ietf-yang-types {
7     prefix yang;
8   }
9   import cisco-semver {
10    prefix cisco-semver;
11  }
12
13  organization
14    "Cisco Systems, Inc.";
```

Module prefix 

Figure 13-10 YANG module prefix in the YANG file

Select a YANG set: wlc-default-yangset | Select YANG module(s): Cisco-IOS-XE-wireless-ap-global-oper x | Load module(s)

Icon legend | Search XPath(s) | Search nodes | Expand all nodes | Display schema nodes only | Display all nodes

Node Properties

Name	ap-name
Nodetype	leaf
Datatype	string
Description	Name of the AP
Module	Cisco-IOS-XE-wireless-ap-global-oper
Revision	2021-07-01
Xpath	/ap-global-oper-data/ap-join-stats/ap-join-info/ap-name
Prefix	wireless-ap-global-oper
Namespace	http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-ap-global-oper
Access	read-only
Operations	• "get"
Schema Node Id	/ap-global-oper-data/ap-join-stats/ap-join-info/ap-name

Module prefix →

Figure 13-11 YANG module prefix as shown in YANG Suite

Select a YANG set: wlc-default-yangset | Select YANG module(s): Cisco-IOS-XE-wireless-ap-global-oper x | Load module(s)

Icon legend | Search XPath(s) | Search nodes | Expand all nodes | Display schema nodes only | Display all nodes

Cisco-IOS-XE-wireless-ap-global-oper

- ap-global-oper-data
 - ap-img-predownload-stats
 - ap-join-stats
 - wtp-mac
 - ap-join-info
 - ap-ip-addr
 - ap-ethernet-mac
 - ap-name** (highlighted)
 - is-joined
 - last-error-type
 - ap-disconnect-reason

Element XPath →

Node Properties	
Name	ap-name
Nodetype	leaf
Datatype	string
Description	Name of the AP
Module	Cisco-IOS-XE-wireless-ap-global-oper
Revision	2021-07-01
XPath	/ap-global-oper-data/ap-join-stats/ap-join-info/ap-name
Prefix	wireless-ap-global-oper
Namespace	http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-ap-global-oper
Access	read-only
Operations	• "get"
Schema Node Id	/ap-global-oper-data/ap-join-stats/ap-join-info/ap-name

Figure 13-12 Element XPath as shown in YANG Suite

/wireless-ap-global-oper:ap-global-oper-data/ap-join-stats/ap-join-info/ap-name

Module prefix Node XPATH

Figure 13-13 Composing a full XPath from the information in YANG Suite

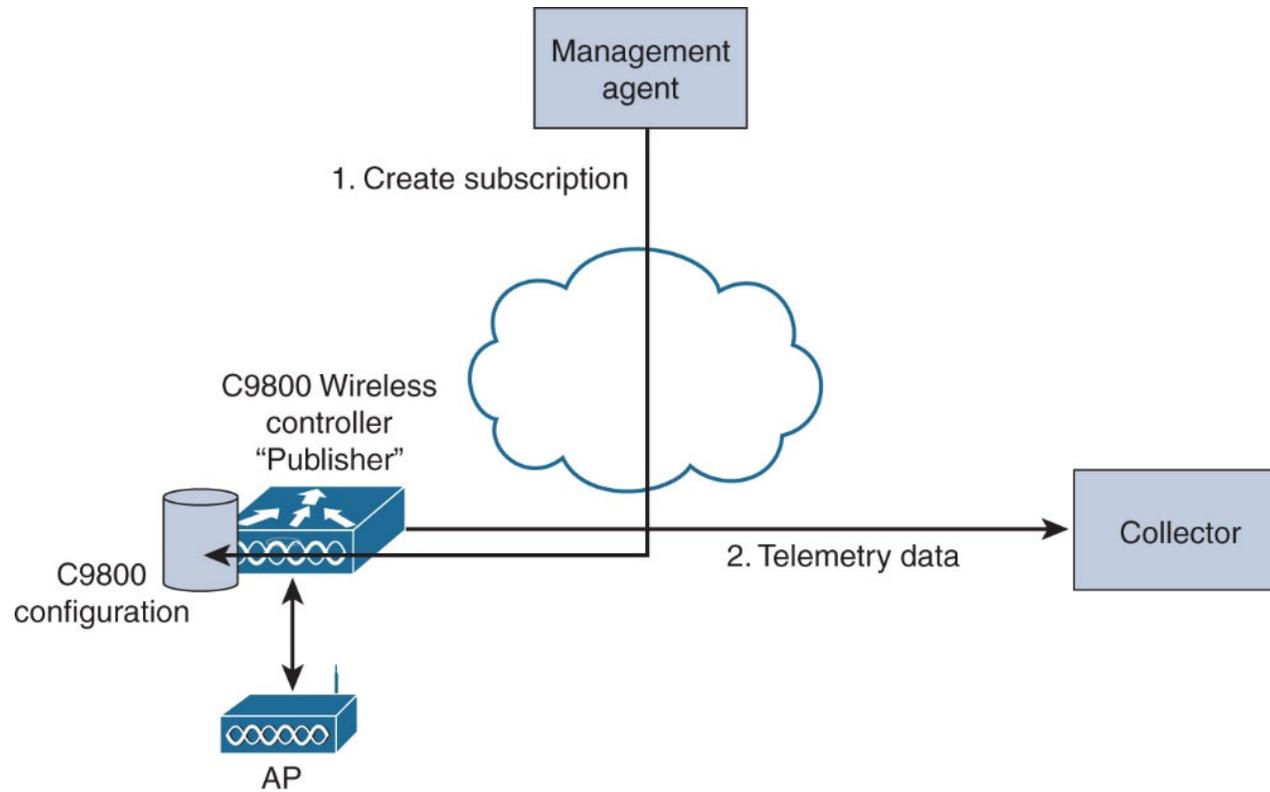


Figure 13-14 Flow for dial-out telemetry subscriptions

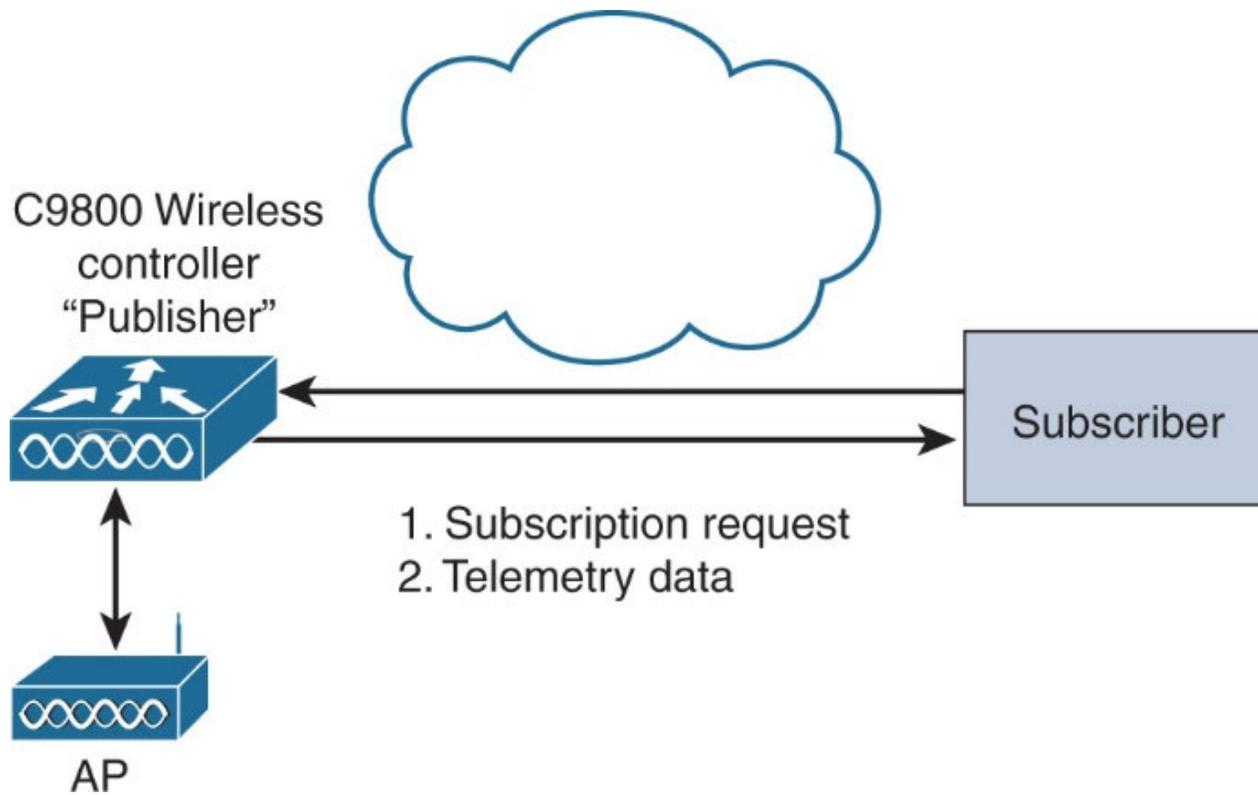


Figure 13-15 Flow for dial-in telemetry subscriptions

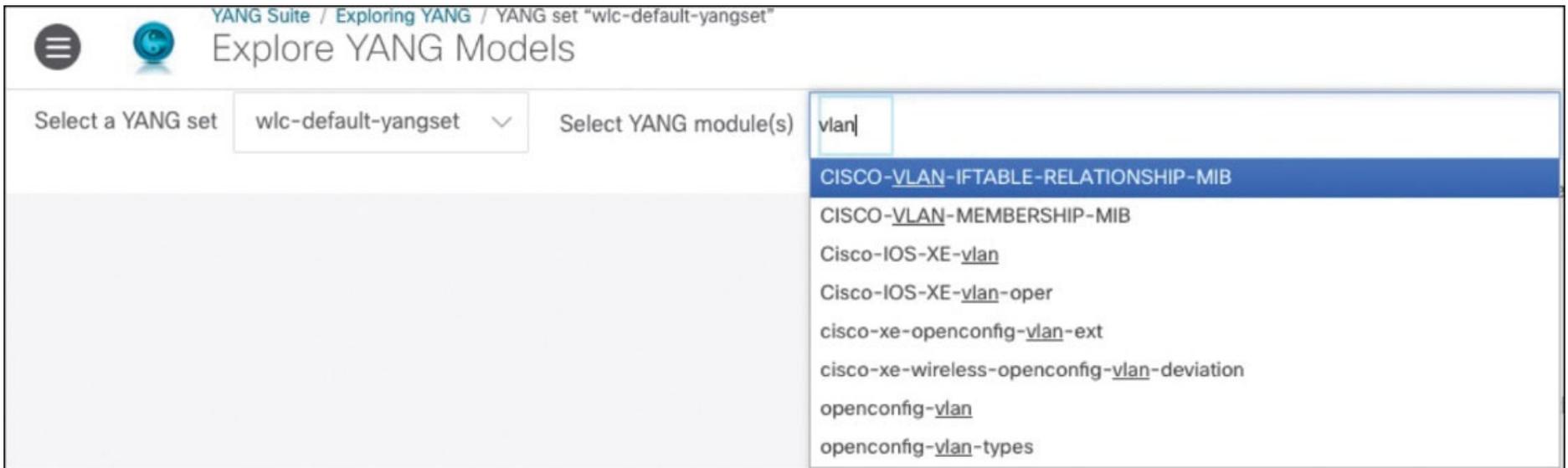


Figure 13-17 Searching models in YANG Suite

The screenshot shows the YANG Suite interface with the following components:

- Header:** "Explore YANG Models" with a user profile "admin" and navigation icons.
- Filters:** "Select a YANG set" (wlc-default-yangset) and "Select YANG module(s)" (Cisco-IOS-XE-vlan-oper).
- Actions:** "Load module(s)", "Icon legend", "Search XPath(s)", "Search nodes", and "Expand all nodes".
- Display Options:** "Display schema nodes only" (selected) and "Display all nodes".
- Tree View:** A tree structure showing the hierarchy: Cisco-IOS-XE-vlan-oper > vlans > vlan. The 'vlan' node is selected, showing its children: id, name, status, ports (with sub-nodes interface and subinterface), and vlan-interfaces (with sub-nodes interface and subinterface).
- Node Properties Table:**

Name	vlan
Nodetype	list
Description	List of VLANs, keyed by id
Module	Cisco-IOS-XE-vlan-oper
Revision	2019-05-01
Xpath	/vlans/vlan
Prefix	vlan-ios-xe-oper
Namespace	http://cisco.com/ns/yang/Cisco-IOS-XE-vlan-oper
Keys	• "id"
Access	read-only
Operations	• "get"
Schema Node Id	/vlans/vlan

Figure 13-18 Displaying details of YANG models using YANG Suite

```
4  rpc = """
5  <establish-subscription xmlns="urn:ietf:params:xml:ns:yang:ietf-event-notifications"
6  | xmlns:yp="urn:ietf:params:xml:ns:yang:ietf-yang-push">
7  |   <stream>yp:yang-push</stream>
8  |   <yp:xpath-filter>
9  |     /vlan-ios-xe-oper:vlangs/vlan
10 |   </yp:xpath-filter>
11 |   <yp:dampening-period>0</yp:dampening-period>
12 </establish-subscription>
13 """
```

Figure 13-19 Python code with the subscription NETCONF RPC

```
3  version: '3'
4  services:
5    yangsuite:
6      image: yangsuite:latest
7      build:
8        context: ./yangsuite
9      env_file:
10     - ./yangsuite/setup.env
11     command: /yangsuite/migrate_and_start.sh
12     ports:
13     - "50052:50052"
14     - "50051:50051"
15     - "9339:9339"
16     - "57344:57344"
17     - "57345:57345"
18     - "443:443"
```

Figure 13-20 Ports exposed in a docker-compose file

YANG Suite / gRPC Telemetry

admin

Listen at IP address 127.0.0.1 Listen at port 57344

Stop telemetry receiver Clear output

```

Node          : C9800-telemetry
Subscription  : 2
Path          : Cisco-IOS-XE-wireless-ap-global-oper:ap-global-oper-data/ap-join-stats/ap-join-info

Key           : /wtp-mac           : cc:16:7e:30:59:00

/ap-ip-addr   : 192.168.30.136
/ap-ethernet-mac : 58:ac:78:de:8d:0e
/ap-name      : AP58AC-78DE-8D0E
/is-joined    : true
/last-error-type : ap-con-failure-run
/ap-disconnect-reason : DTLS close alert from peer

Node
Subscription
Path
...-ap-global-oper:wireless-ap-global-oper:ap-global-oper-data/ap-join-stats/ap-join-info/ap-name

Node          : C9800-telemetry
Subscription  : 2
Path          : Cisco-IOS-XE-wireless-ap-global-oper:ap-global-oper-data/ap-join-stats/ap-join-info

Key           : /wtp-mac           : cc:16:7e:30:59:00

/ap-ip-addr   : 192.168.30.136
/ap-ethernet-mac : 58:ac:78:de:8d:0e
/ap-name      : AP58AC-78DE-8D0E
/is-joined    : true
/last-error-type : ap-con-failure-run
/ap-disconnect-reason : DTLS close alert from peer

```

YANG Suite
Server started on 172.18.0.2 port 57344

Figure 13-21 YANG Suite receiving gRPC dial-out telemetry

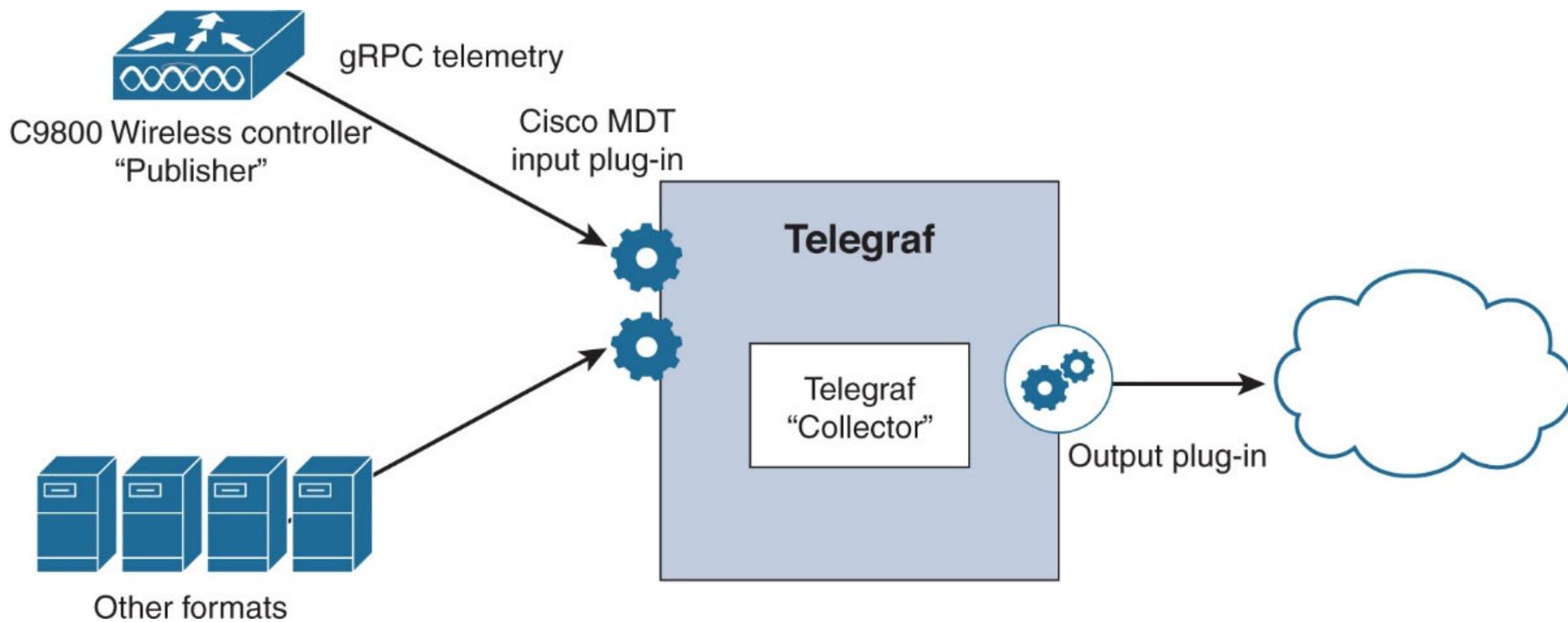


Figure 13-22 Telegraf serving as an aggregator for telemetry data

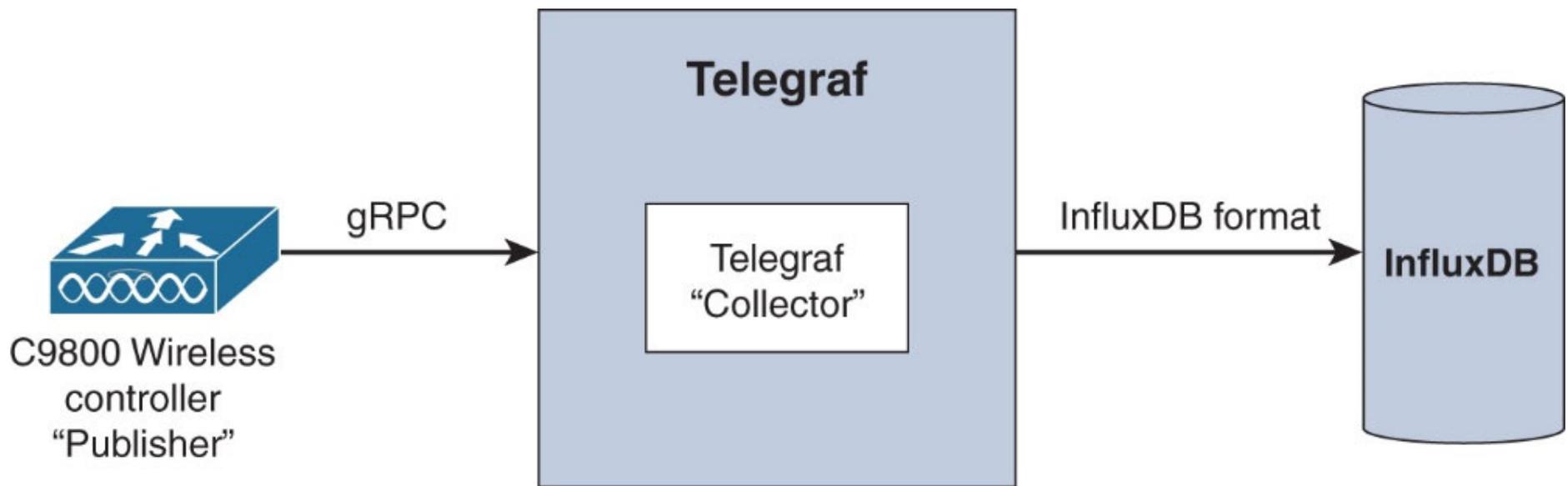


Figure 13-23 Sending data to InfluxDB

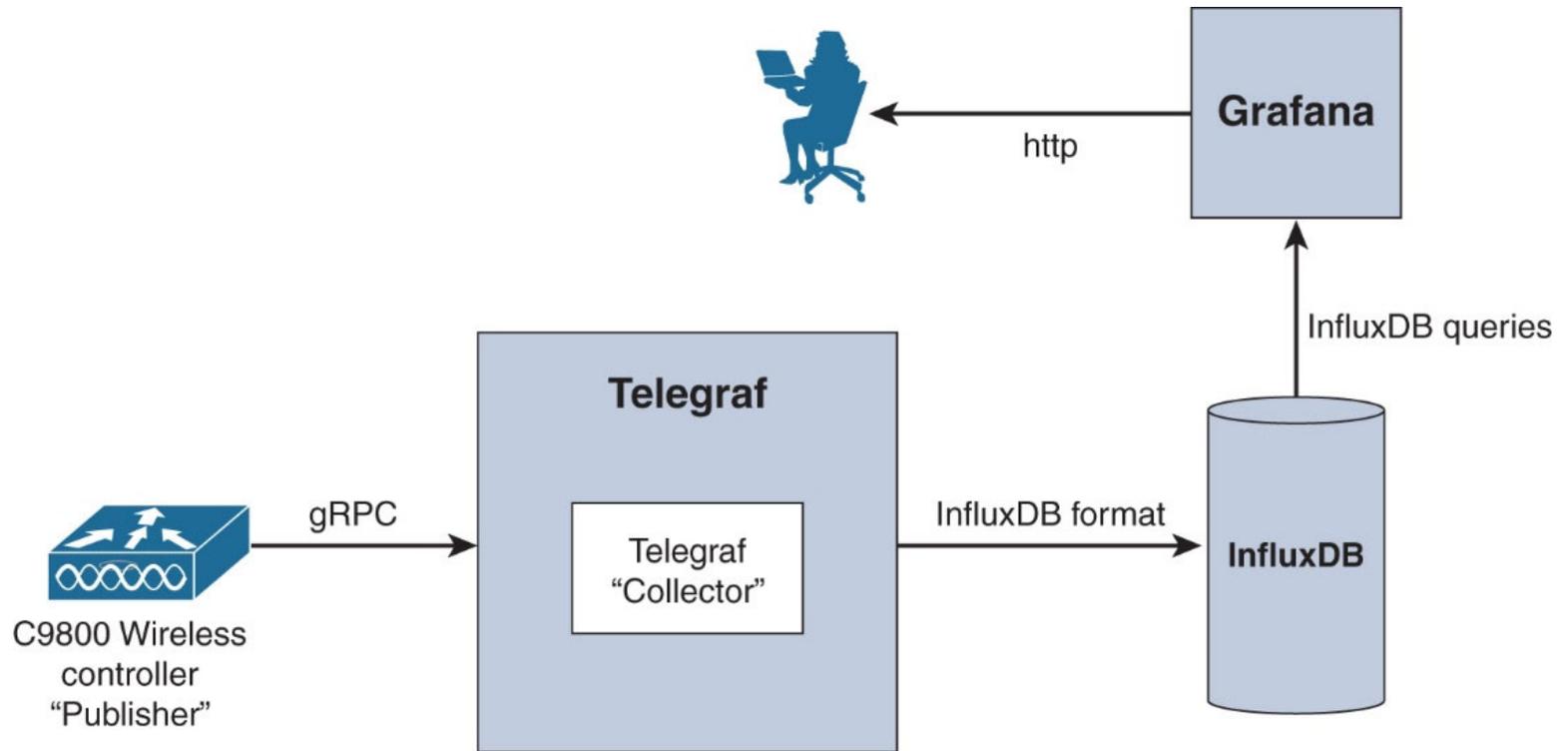


Figure 13-24 Grafana receiving data from InfluxDB

Select a YANG set: wlc-default-yangset

Select YANG module(s): Cisco-IOS-XE-wireless-client-global-oper x
Cisco-IOS-XE-wireless-client-oper x

Load module(s)

Icon legend Search XPaths Search nodes Expand all nodes

Display schema nodes only Display all nodes

Node Properties

Name	client-live-stats
Nodetype	container
Description	Snapshot of statistics of current state of wireless clients
Module	Cisco-IOS-XE-wireless-client-global-oper
Revision	2021-07-01
Xpath	/client-global-oper-data/client-live-stats
Prefix	wireless-client-global-oper
Namespace	http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-client-global-oper
Presence	true
Access	read-only
Operations	• "get"

Figure 13-25 Identifying prefix and XPath using YANG Suite

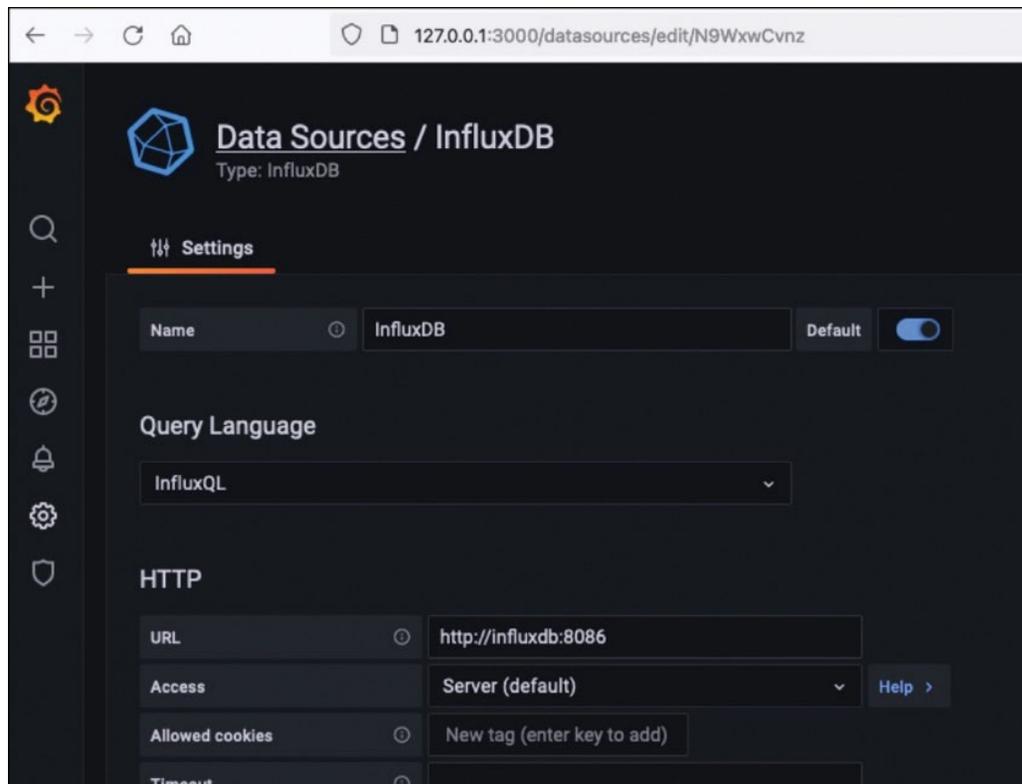


Figure 13-26 Configuring the database connection in Grafana

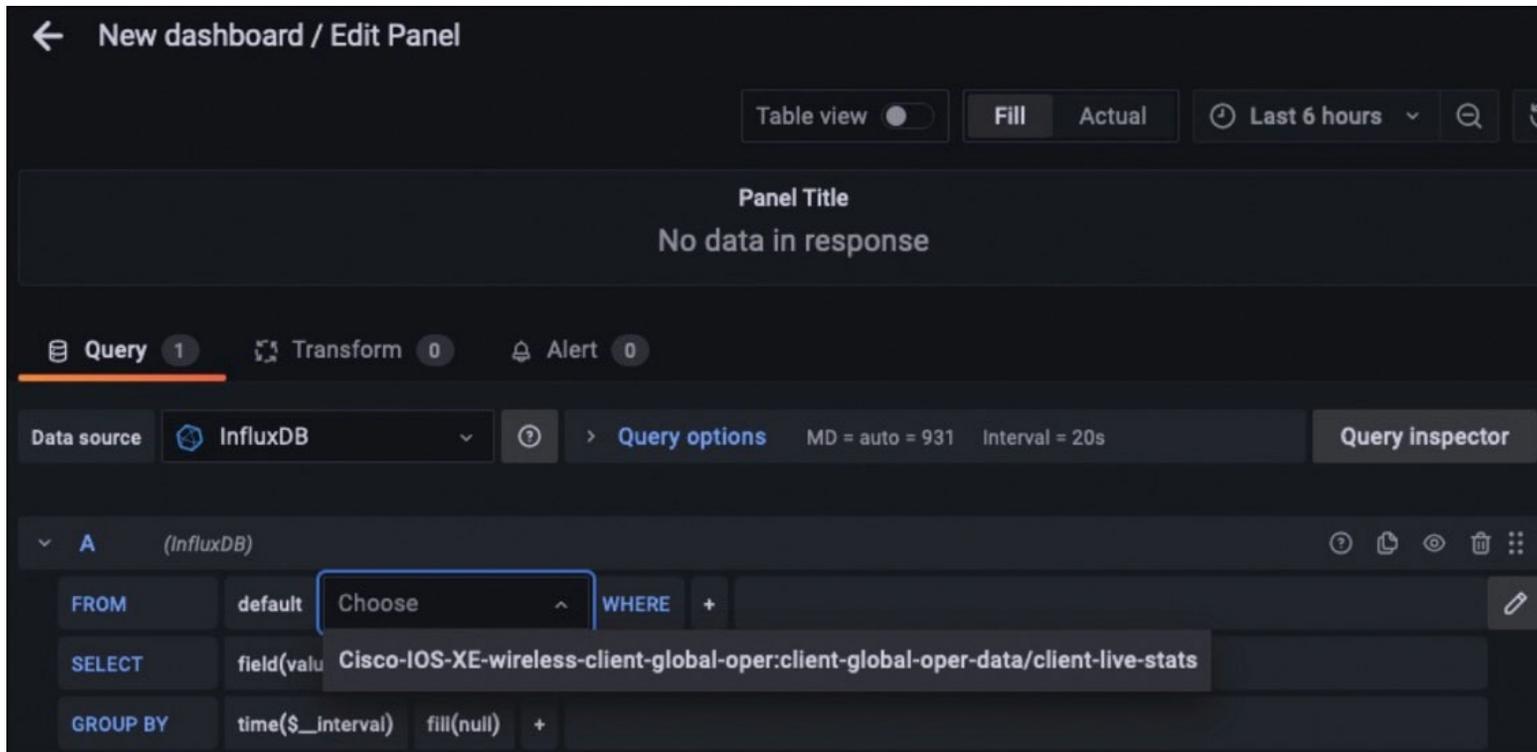


Figure 13-27 Displaying available measurements in Grafana

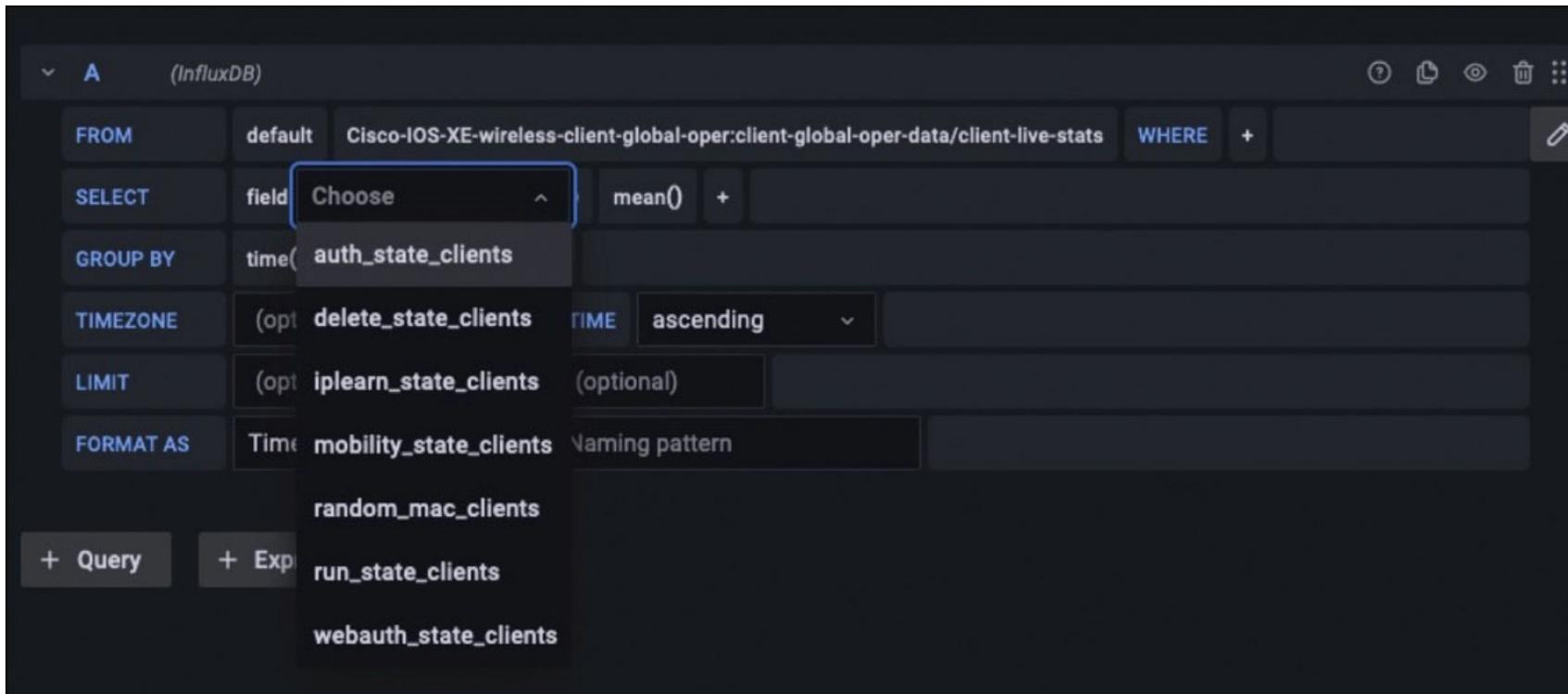


Figure 13-28 Displaying available metrics in Grafana

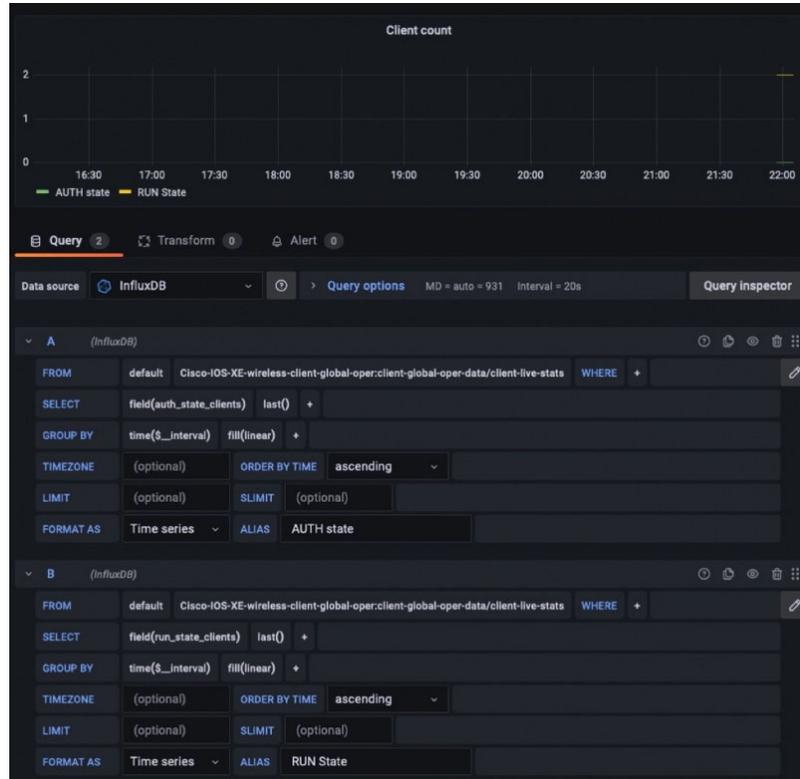


Figure 13-29 Grafana configuration

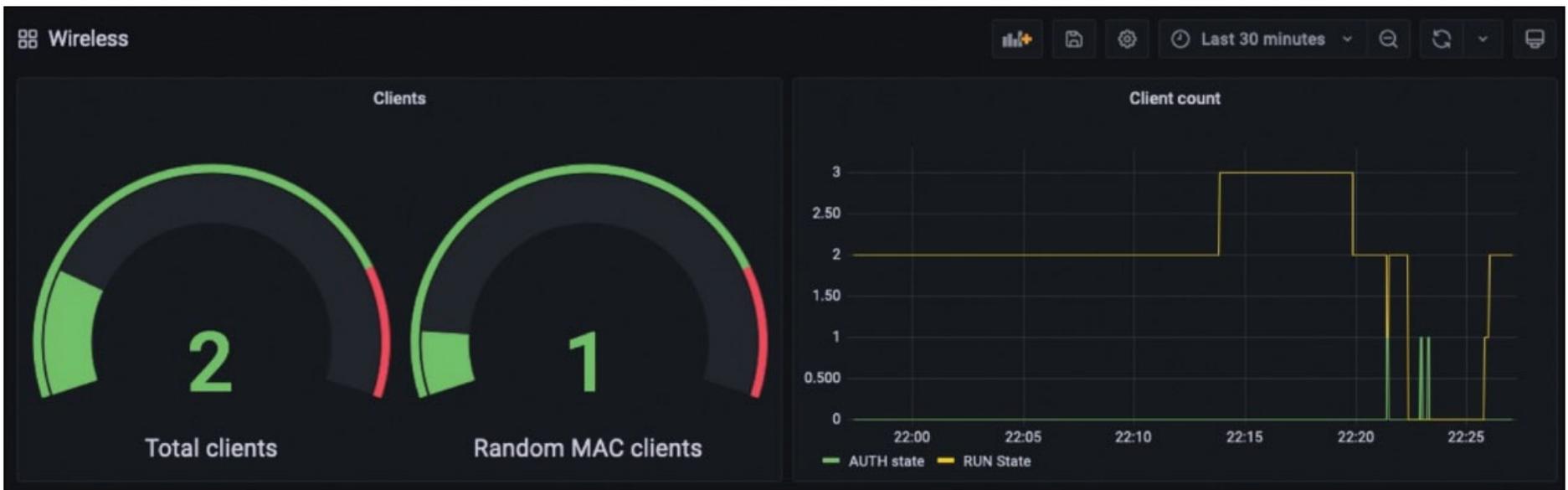


Figure 13-30 Final Grafana dashboard

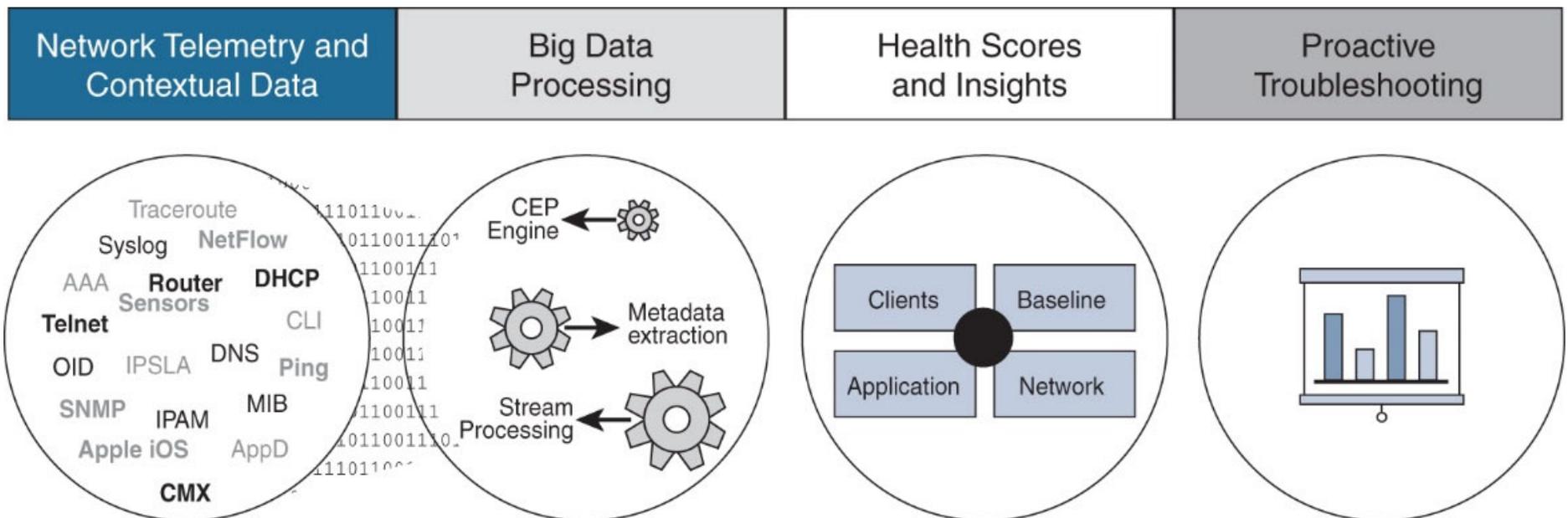


Figure 14-1 The principles of Cisco DNA Center telemetry and data processing flows

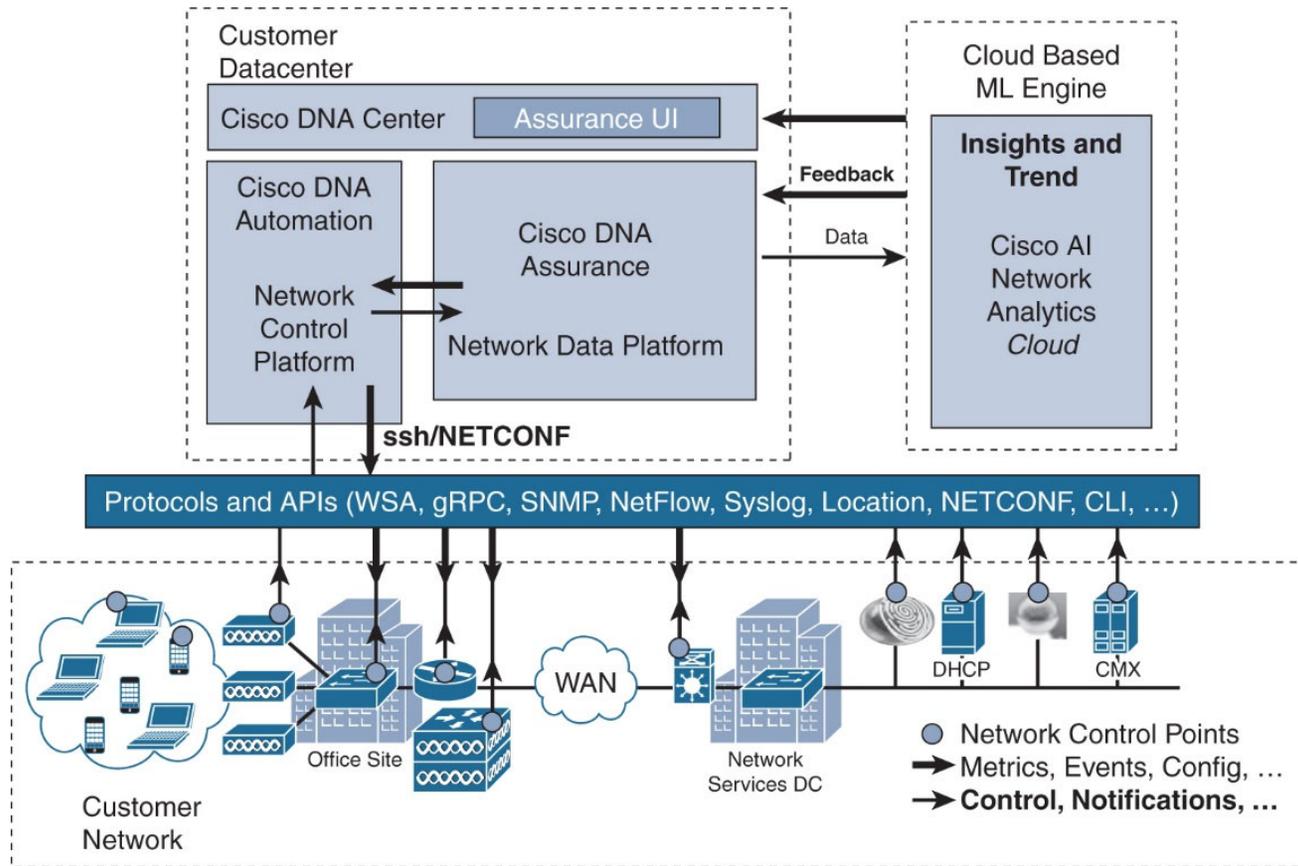


Figure 14-2 Cisco DNA Center Assurance architecture

DEVICES (5)
 FOCUS: **Inventory** ▾

Filter | ● Add Device Tag Device Actions ▾ ⓘ | Take a Tour

As of: 1:30 PM [Export](#) [Refresh](#)

Image Version is *17.6* ✕

<input type="checkbox"/>	Device Name	IP Address	Device Family ▾	Reachability ⓘ	Manageability ⓘ	Health Score	Site	Image Version	Uptime	Last Updated	Resync Interval ⓘ
<input type="checkbox"/>	9120AXE-A ⓘ	10.48.39.39	Unified AP	🔴 Unreachable	🟢 Managed	NA	Assign	17.6.1.13	2 days 10 hrs	a day ago	N/A
<input type="checkbox"/>	1832I-E ⓘ	10.48.39.180	Unified AP	🔴 Unreachable	🟢 Managed	NA	Assign	17.6.1.13	2 days 1 hr	a day ago	N/A
<input type="checkbox"/>	RazanAP9130-1 ⓘ	10.48.70.61	Unified AP	🟢 Reachable	🟢 Managed	NA	Assign	17.6.1.13	1 day 16 hrs	a day ago	N/A
<input type="checkbox"/>	Razan9130AP-2 ⓘ	10.48.70.62	Unified AP	🟢 Reachable	🟢 Managed	NA	Assign	17.6.1.13	1 day 14 hrs	a day ago	N/A
<input type="checkbox"/>	9800-17-6-1 ⓘ	10.48.39.206	Wireless Controller	🟢 Reachable	🟢 Managed	10	.../RitinBuilding/Ritinfloor	17.6.1	2 days 14 hrs	a day ago	24:00:00

Figure 14-3 Cisco DNA Center inventory page

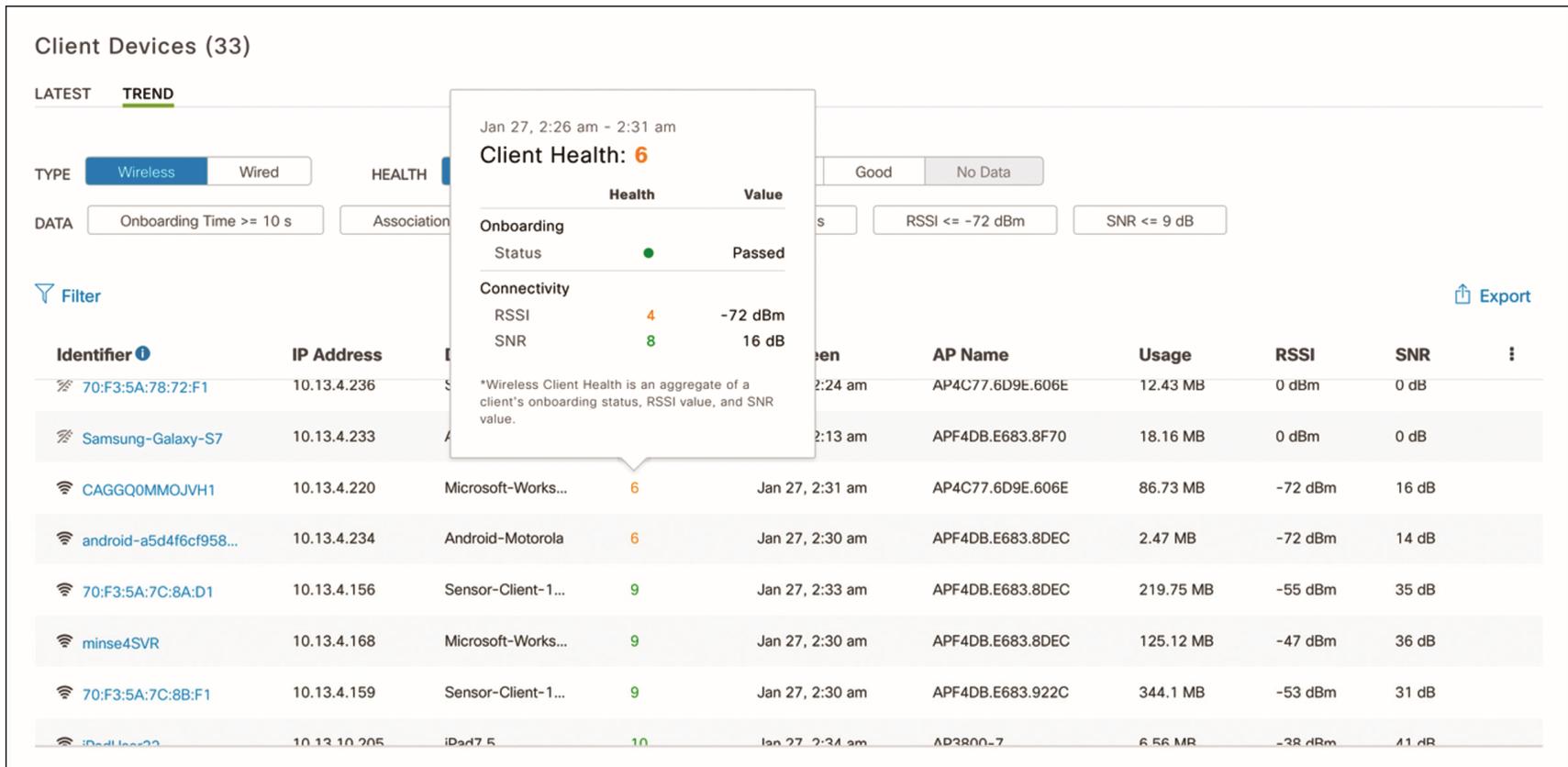


Figure 14-4 Cisco DNA Center client devices list Assurance page

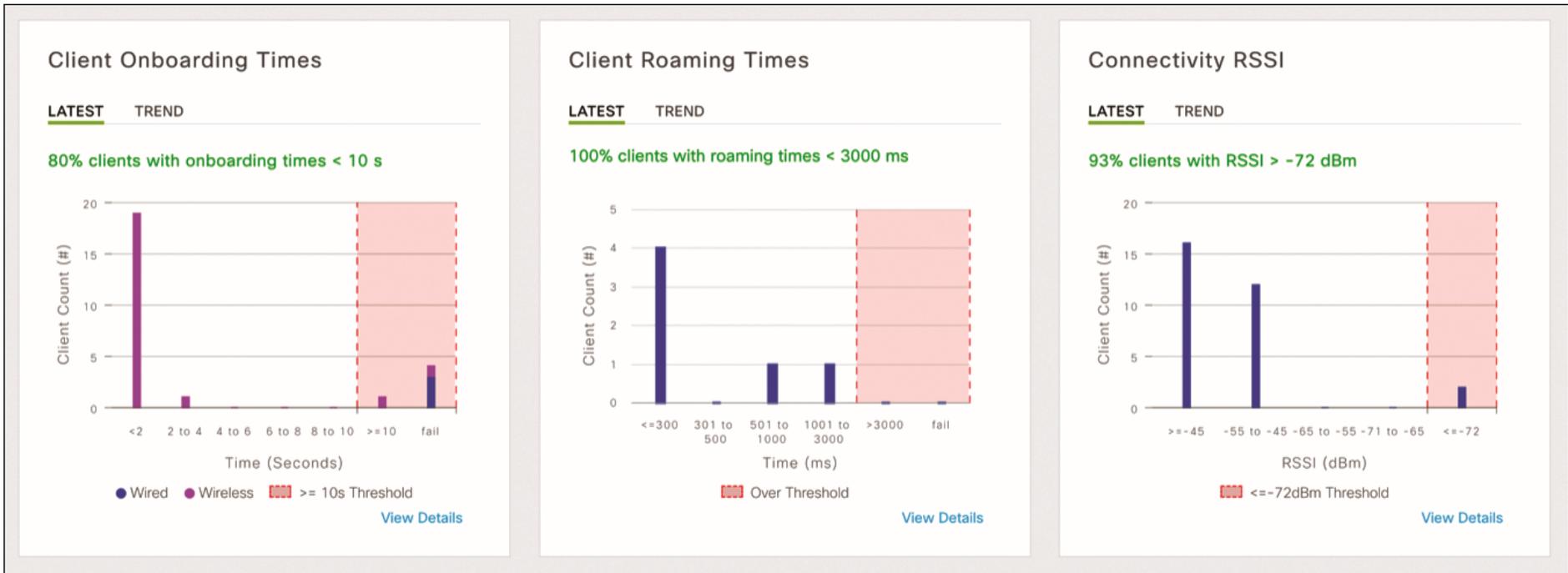


Figure 14-5 Roaming and onboarding times

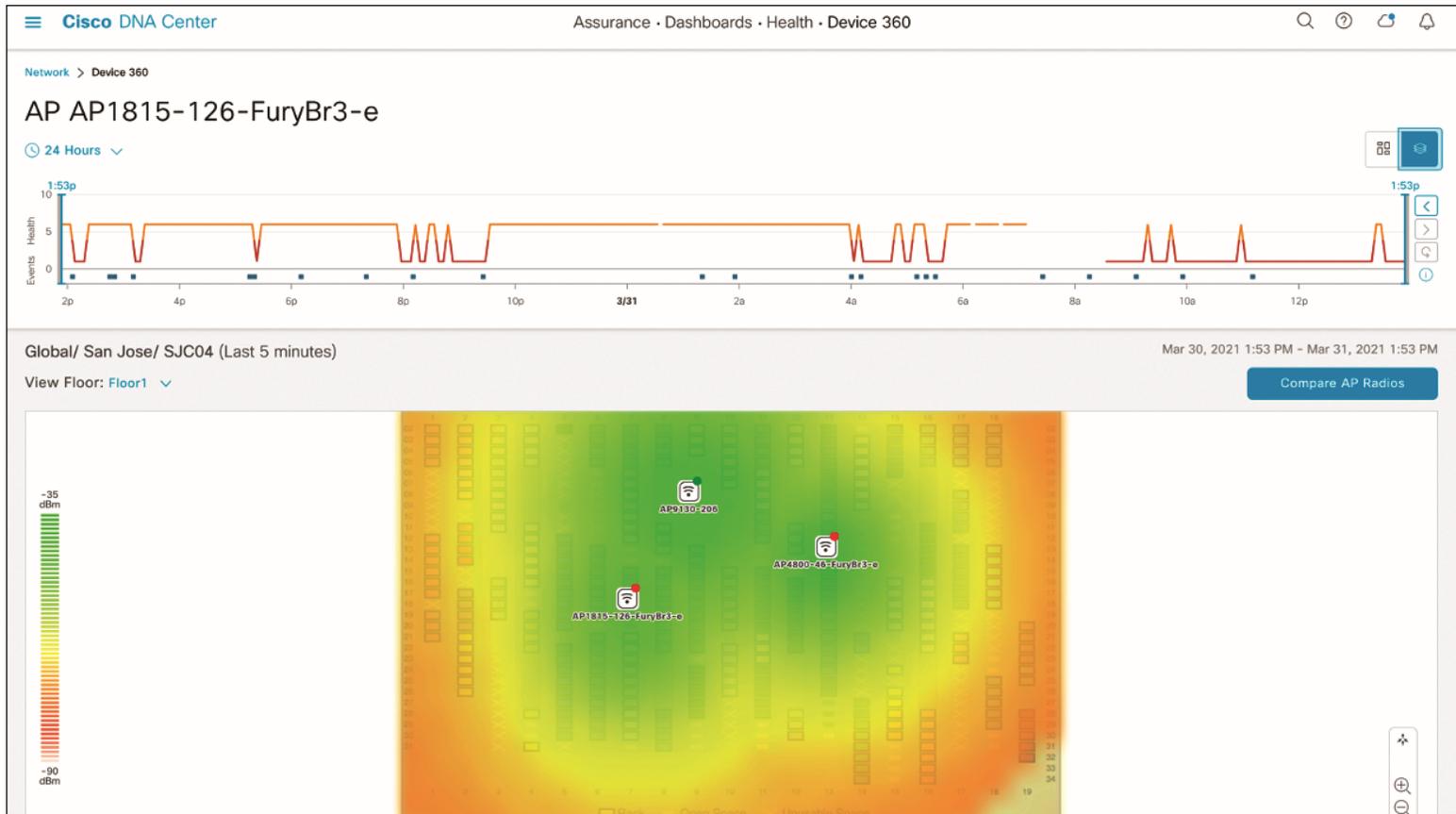


Figure 14-6 AP 360 page

Cisco DNA Center Assurance · Dashboards · Health · Device 360

Network > Device 360
View Floor: Floor1

Access Point Radios

Search Table

Device Name	Radio	Band	Model	IP Address	Radio Mode	Operational Status	Client Count	Channel information
AP1815-126-FuryBr3-e	1	5.0 GHz	AIR-AP1815I-H-K9	10.79.59.126	Local	●	0	44,48
AP1815-126-FuryBr3-e	0	2.4 GHz	AIR-AP1815I-H-K9	10.79.59.126	Local	●	0	6
AP4800-46-FuryBr3-e	1	5.0 GHz	AIR-AP4800-H-K9	10.79.46.199	Local	●	0	149,153,157,161
AP4800-46-FuryBr3-e	2	2.4 GHz	AIR-AP4800-H-K9	10.79.46.199	Monitor	●	--	--
AP4800-46-FuryBr3-e	0	5.0 GHz	AIR-AP4800-H-K9	10.79.46.199	Local	●	0	
AP9130-206	1	5.0 GHz	C9130AXI-H	10.74.14.206	Local	●	0	36,40

8 Records Show Records: 25 1 - 8

AP Radio Comparison (3/5 Selected)

AP1815-126-FuryBr3-e AP4800-46-FuryBr3-e AP9130-206

Radio: 1 (5.0 GHz)

IP Address: 10.79.59.126

Model: AIR-AP1815I-H-K9

Uptime: 2 days, 2 hours, 38 minutes

Connected to WLC: FuryBr3-eWLC-17.5-182

Floor: Floor1

Radio: 1 (5.0 GHz)

IP Address: 10.79.46.199

Model: AIR-AP4800-H-K9

Uptime: 5 days, 12 hours, 28 minutes

Connected to WLC: FuryBr3-eWLC-17.5-182

Floor: Floor1

[View AP 360](#)

Radio: 1 (5.0 GHz)

IP Address: 10.74.14.206

Model: C9130AXI-H

Uptime: 16 days, 12 hours, 49 minutes

Connected to WLC: FreeAgent-eWLC-17.4-179

Floor: Floor1

[View AP 360](#)

Figure 14-7 AP radios comparison screen

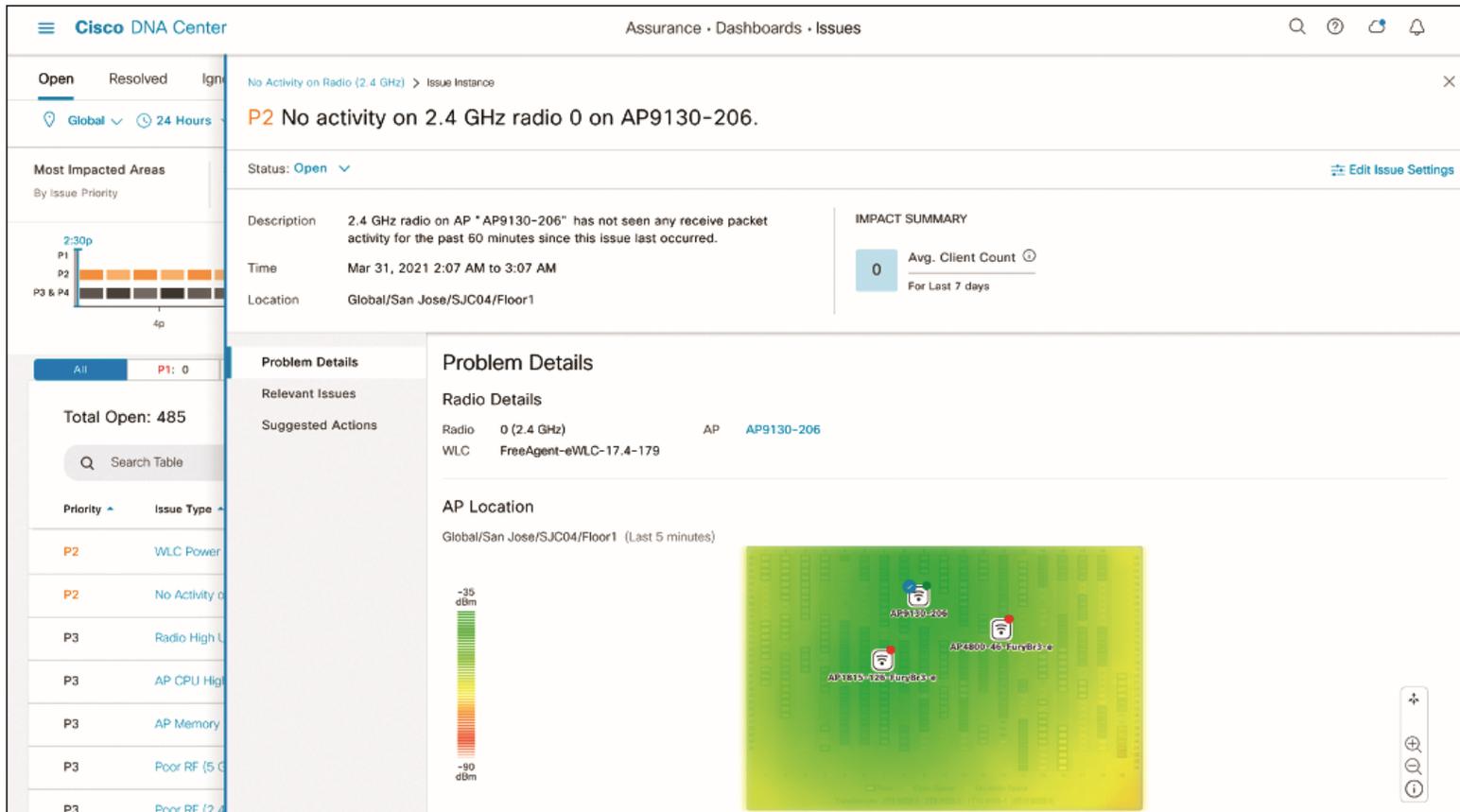


Figure 14-8 Issues dashboard

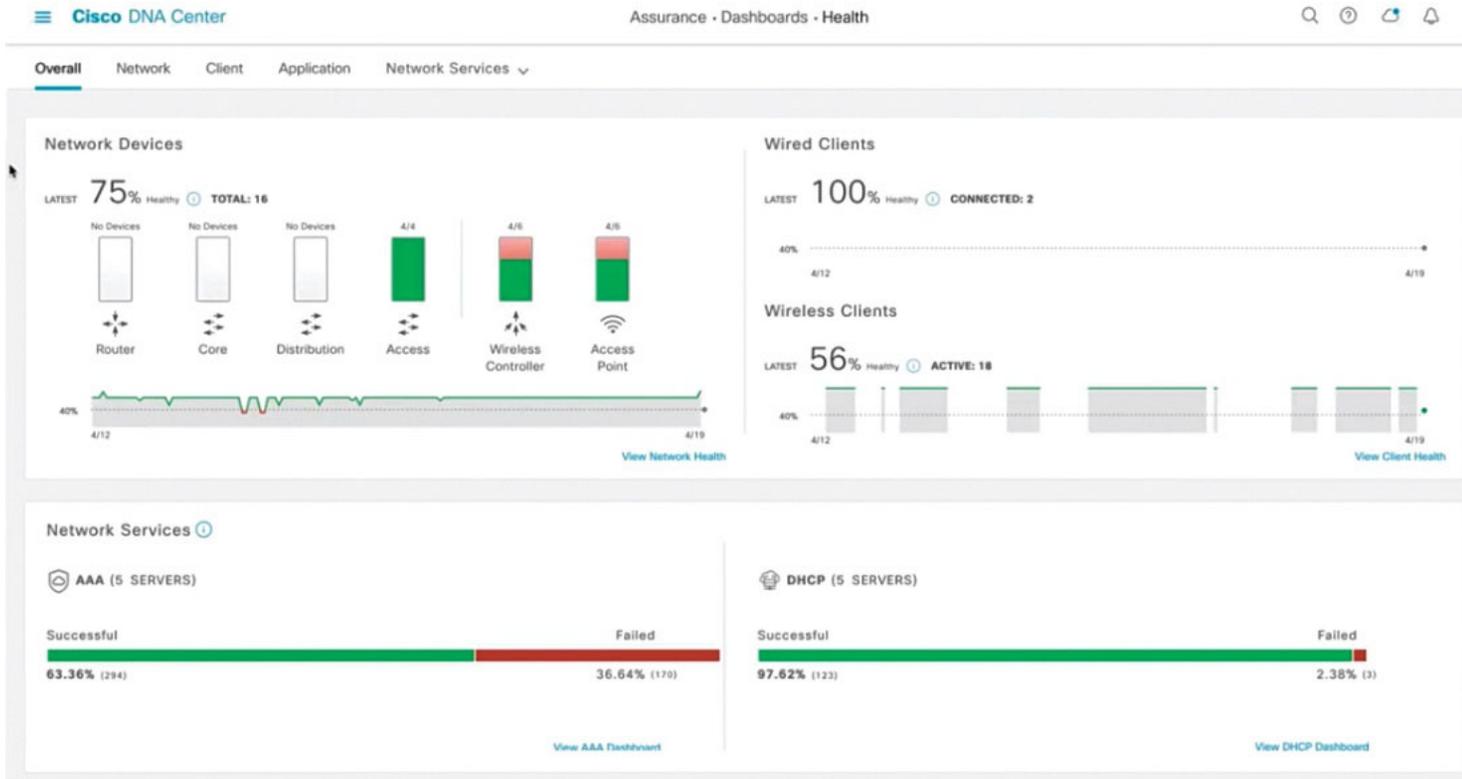


Figure 14-9 Assurance overview health dashboard

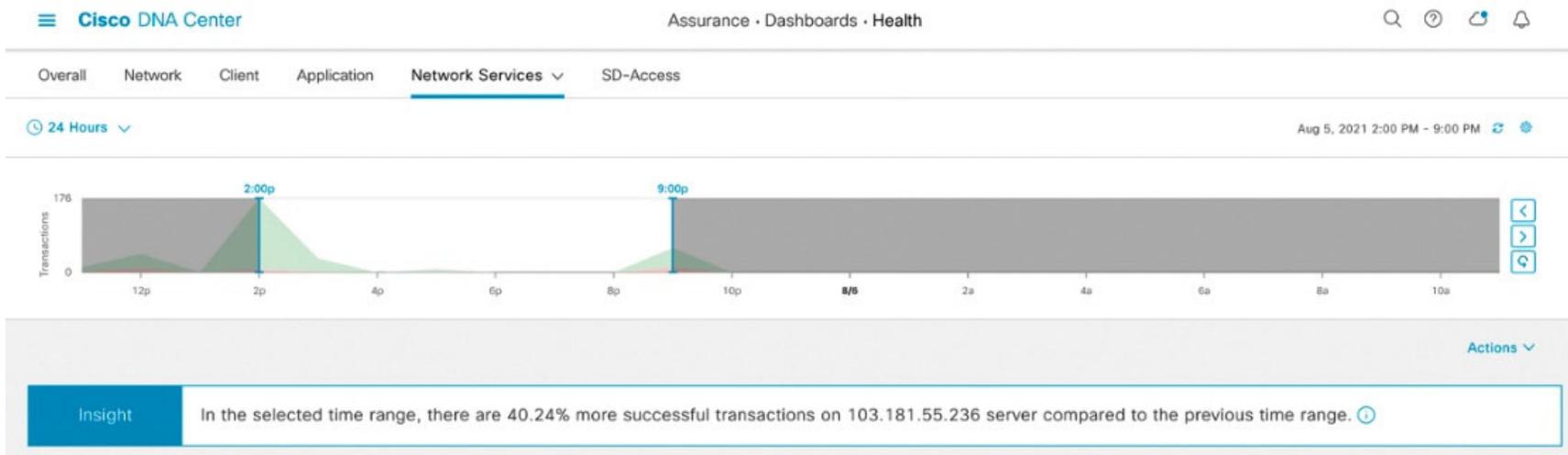


Figure 14-10 Network services health timeline

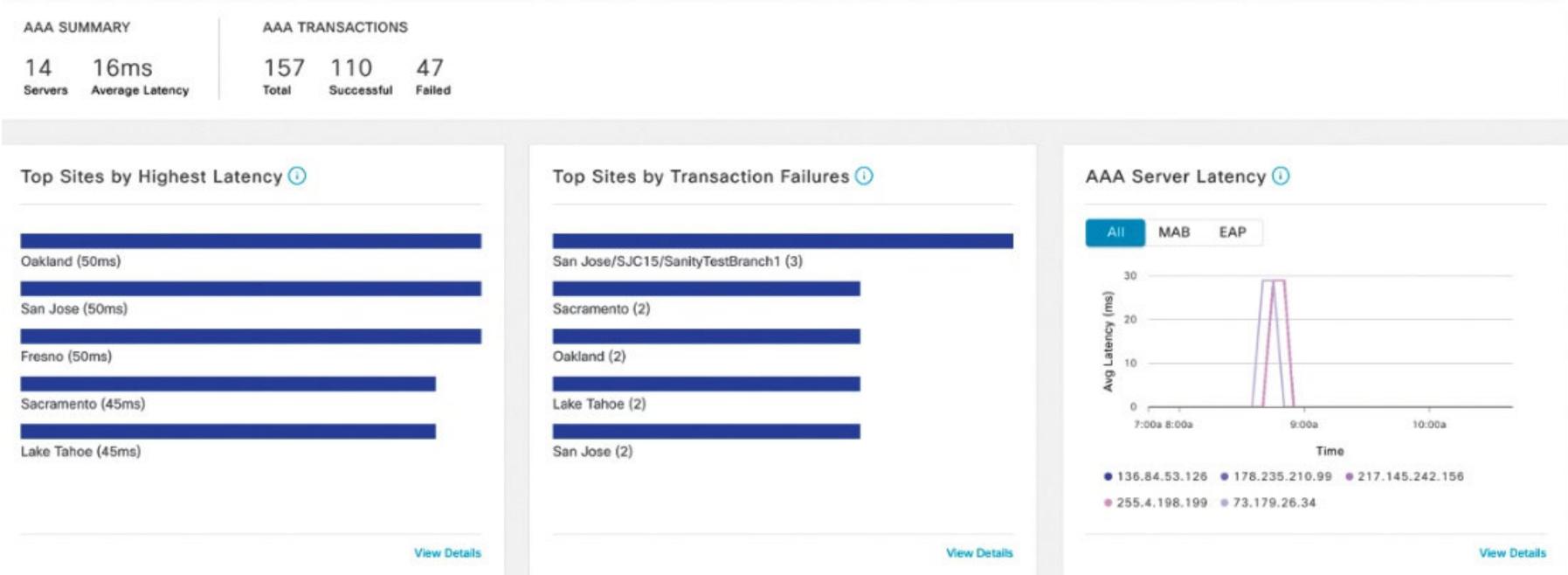


Figure 14-11 Top AAA sites sorted

From *Understanding and Troubleshooting Cisco Catalyst 9800 Series Wireless Controller* by Simone Arena, Francisco Sedano Crippa, Nicolas Darchis and Sudha Katgeri(9780137492329) Cisco Press Copyright© 2023 Cisco Systems, Inc. All rights reserved

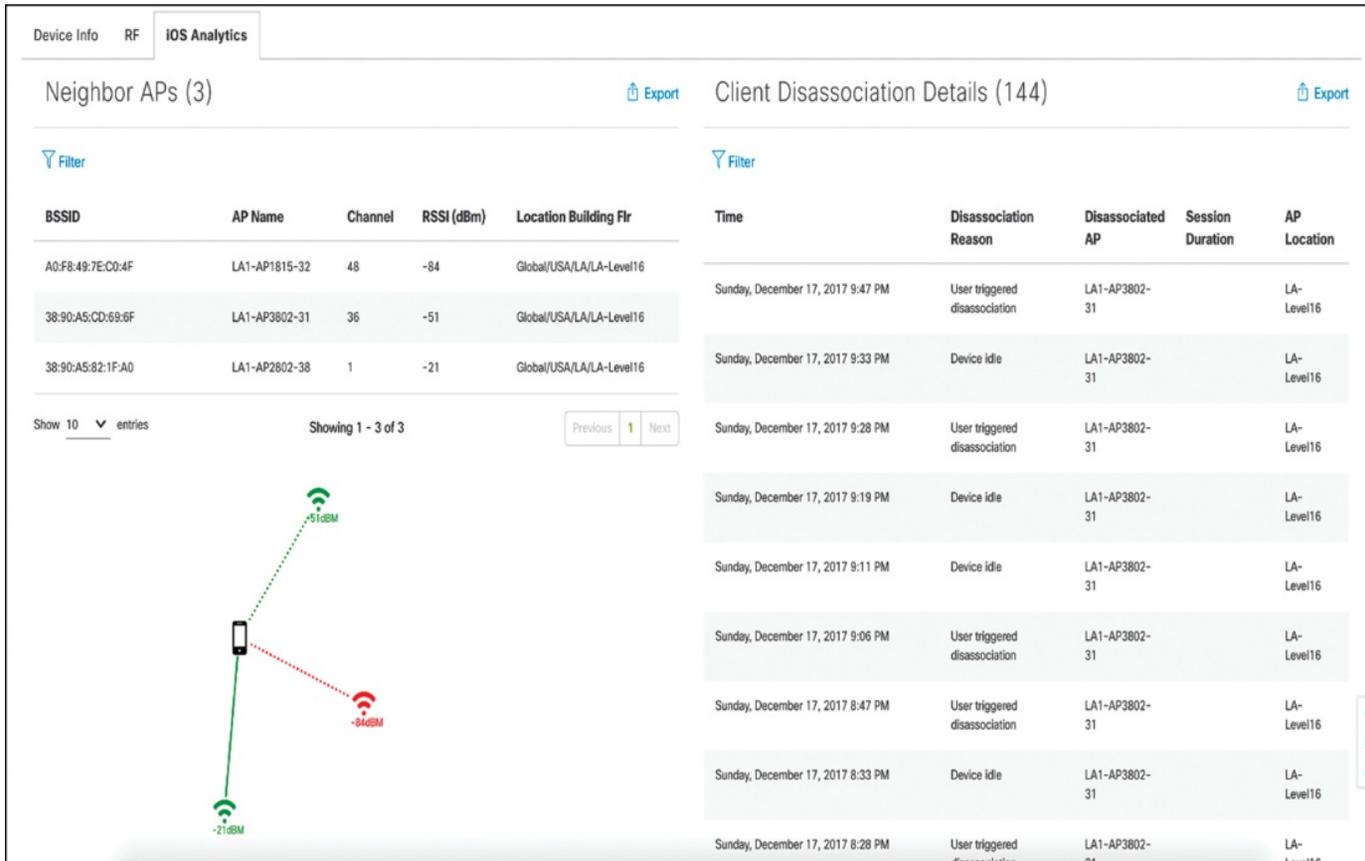


Figure 14-12 The IOS Analytics tab showing the insights received from an iPhone device

Edit WLAN ✕

Per AP Radio Per WLAN <input style="width: 80px;" type="text" value="200"/>	Prediction Optimization <input type="checkbox"/>				
11v BSS Transition Support					
BSS Transition <input checked="" type="checkbox"/>	Neighbor List <input checked="" type="checkbox"/>				
Dual Neighbor List <input type="checkbox"/>	Dual Band Neighbor List <input type="checkbox"/>				
BSS Max Idle Service <input checked="" type="checkbox"/>	DTIM Period (in beacon intervals)				
BSS Max Idle Protected <input type="checkbox"/>	5 GHz Band (1-255) <input style="width: 80px;" type="text" value="1"/>				
Directed Multicast Service <input checked="" type="checkbox"/>	2.4 GHz Band (1-255) <input style="width: 80px;" type="text" value="1"/>				
<i>Configuration of '11v BSS Disassociation Imminent' is supported from Command Line Interface (CLI) only</i>					
11ax					
Enable 11ax ⓘ <input checked="" type="checkbox"/>	<div style="background-color: #f0f0f0; padding: 5px;">Device Analytics</div> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 5px;">Advertise Support <input checked="" type="checkbox"/></td> </tr> <tr> <td style="padding: 5px;">Advertise PC Analytics Support ⓘ <input checked="" type="checkbox"/></td> </tr> <tr> <td style="padding: 5px;">Share Data with Client <input type="checkbox"/></td> </tr> </table>		Advertise Support <input checked="" type="checkbox"/>	Advertise PC Analytics Support ⓘ <input checked="" type="checkbox"/>	Share Data with Client <input type="checkbox"/>
Advertise Support <input checked="" type="checkbox"/>					
Advertise PC Analytics Support ⓘ <input checked="" type="checkbox"/>					
Share Data with Client <input type="checkbox"/>					

Figure 14-13 Advanced WLAN settings page, allowing you to enable Device Analytics on the C9800

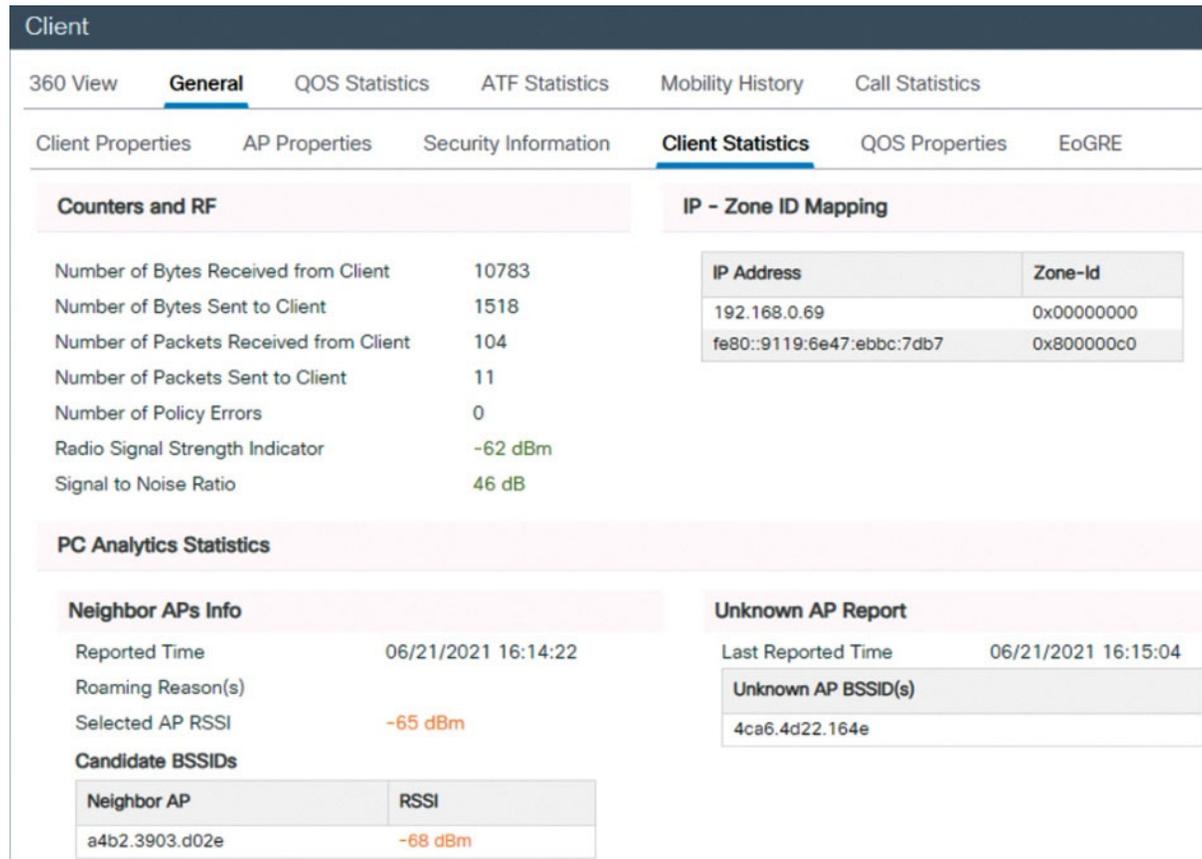


Figure 14-14 C9800 Client statistics monitoring page

Client

360 View **General** QOS Statistics ATF Statistics Mobility History Call Statistics

Client Properties AP Properties Security Information Client Statistics QOS Properties EoGRE

Cellular Capability N/A
 Regular ASR support DISABLED
 Confidence Level 40
 Day Zero Classification Dell Inc.
Software Version 99.00.63.01
 Device Vendor Intel
Power Type AC Powered
Hardware Model AX200 160MHz

Mobility

Move Count 0
 Role Local
 Roam Type None
 Complete Timestamp 07/16/2021 12:57:37 IST

Device Classification

Device Name INTEL CORPORATE
 Protocol Map 0x000401 (OUI, DOT11)
Device OS Windows 10
 Device Protocol DOT11

AP Name	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type	Role
Roam_2_471C	Intel	5	WLAN	Run	11ax(5)		Dell Inc. Latitude 7480	Local

Figure 14-15 C9800 Client general properties

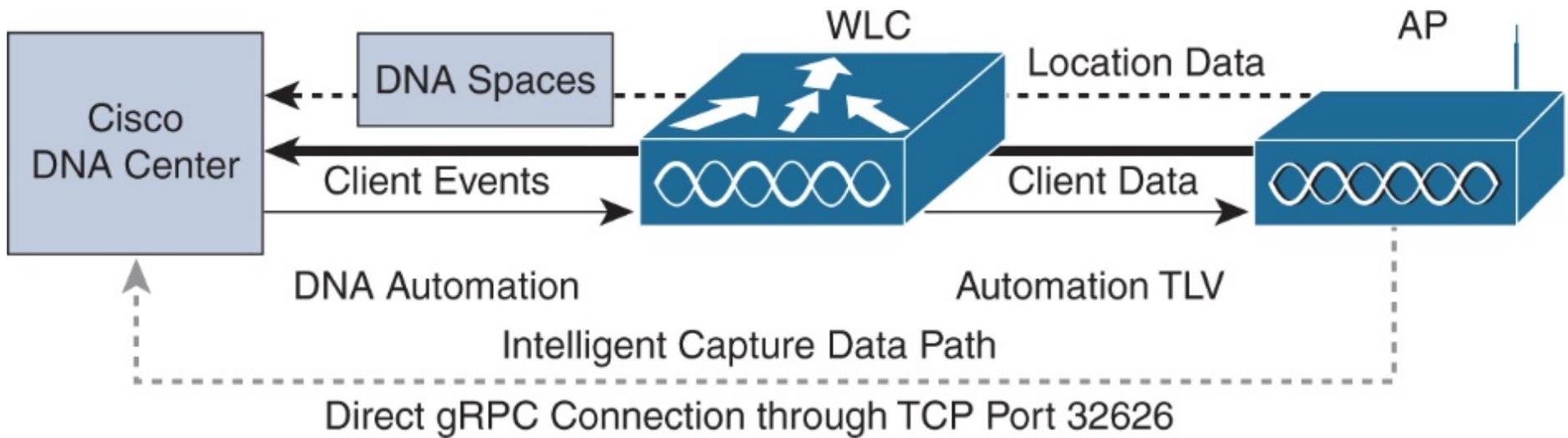


Figure 14-16 Intelligent Capture workflow

Client Schedule Capture

Client Data Packet Capture

Access Point

Access Point

AP Stats Capture ⓘ

Anomaly Capture ⓘ

None - disable all APs

Specific - select specific APs and enable

Global - all capable APs are enabled



Globally Enabled

All the APs are globally enabled for AP Statistics.

Figure 14-17 Intelligent Capture access point configuration page

Intelligent Capture: Grace.Smith

Run Data Packet Capture | Download | Start Live Capture



Onboarding Events

Nov 15, 2020

Time	Duration
Authentication Start	2:07:23 pm
DHCP	2:07:23 pm
Broadcast Rekey	2:02:23 pm < 1 ms
Client Deauthenticated	2:02:23 pm
KeyExchange	2:02:23 pm
Broadcast Rekey	2:02:23 pm
Delete	1:57:23 pm < 1 ms
Onboarding	1:52:23 pm < 1 ms
Run	1:52:23 pm
DHCP	1:52:23 pm
DHCP	1:52:23 pm
Mobility	1:52:23 pm
KeyExchange	1:52:23 pm

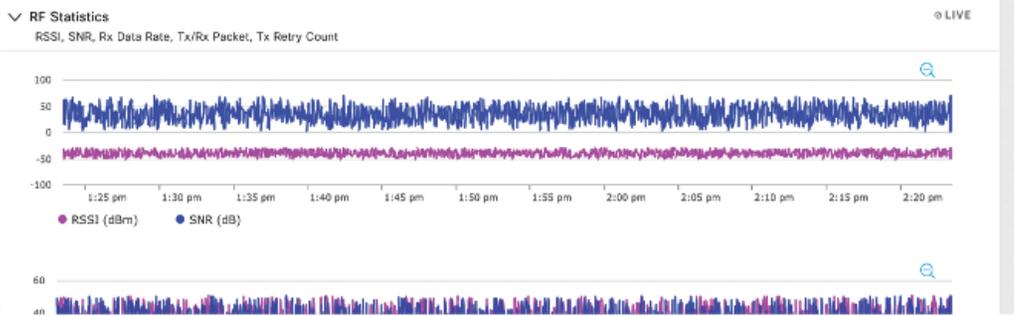


Figure 14-18 Intelligent Capture client 360 health page

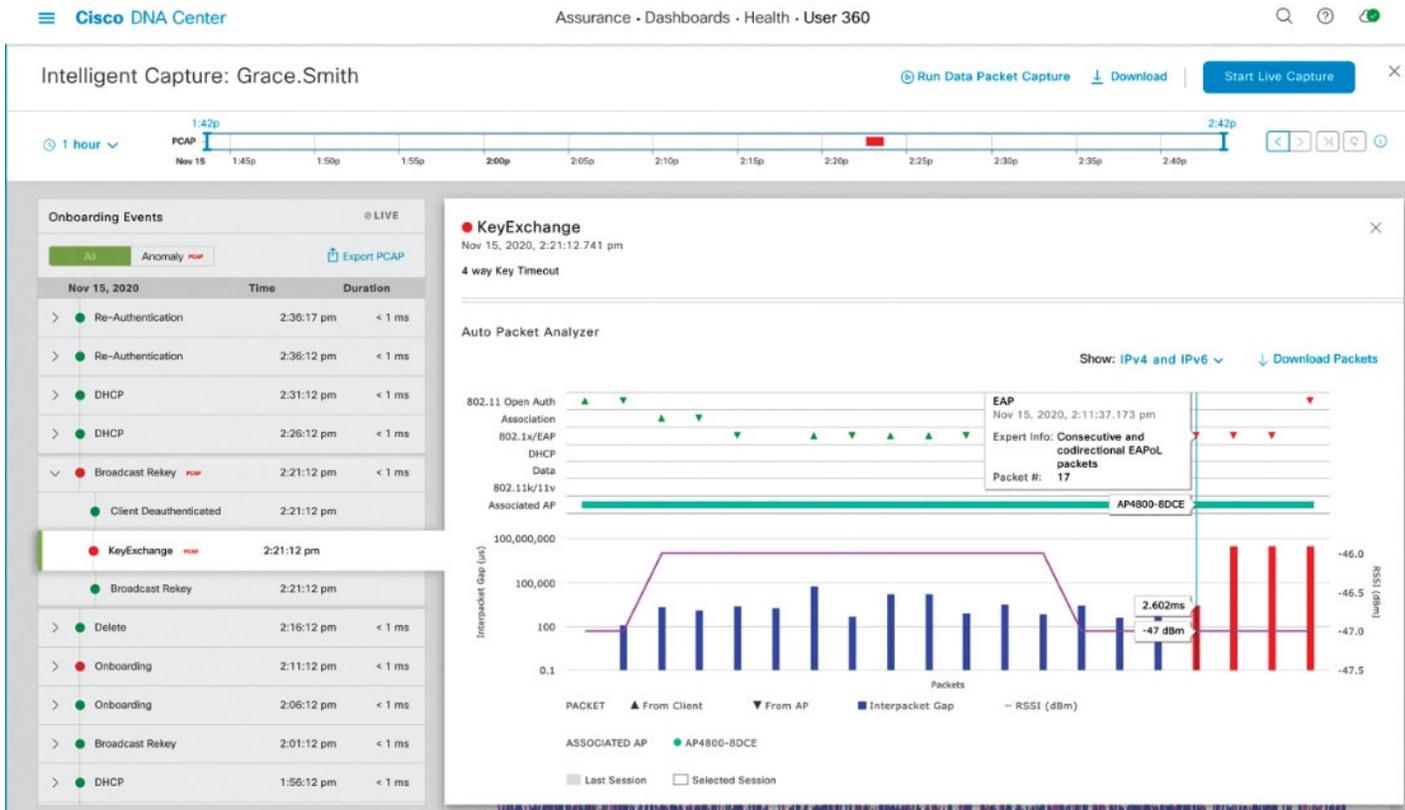
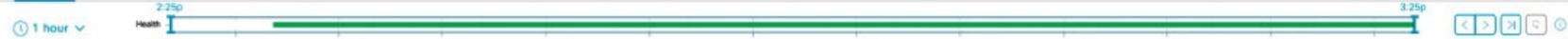


Figure 14-19 The packet analyzer from the onboarding events list

Intelligent Capture: Assurance_9130_2 Global / San Jose / SJC14 / Floor 1

Device Model: C9130AXI-B IP Address: 10.70.18.241 Software Version: 17.4.1.6 Mode: local Uptime: 33 days 21 hr 47 min Connected to WLC: c9800-40-TMEDNAC

RF Statistics Spectrum Analysis



Radio Mode: Local Channel: 44

Radio 1 (5 GHz) RF Statistics is enabled

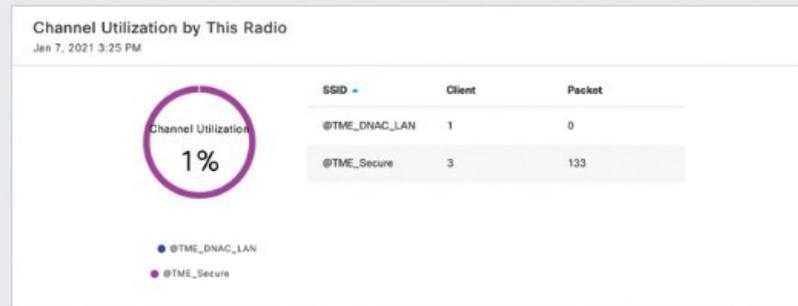
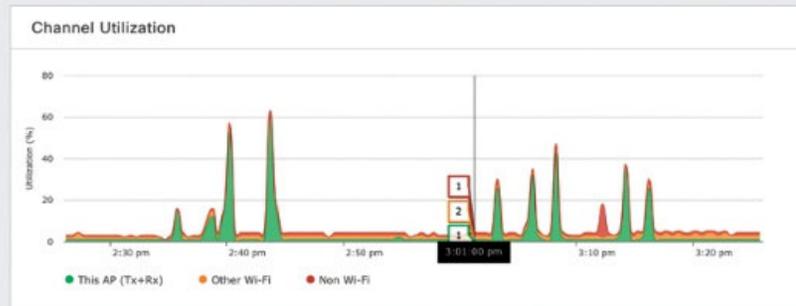
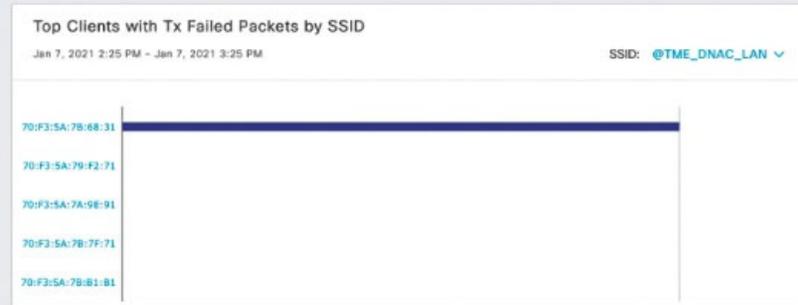
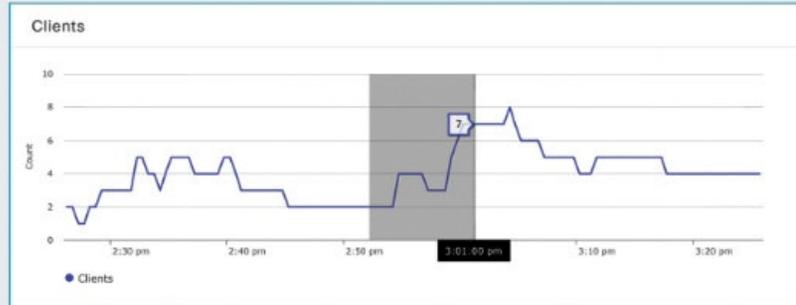


Figure 14-20 The AP health Intelligent Capture page



Figure 14-21 The 1800S sensor

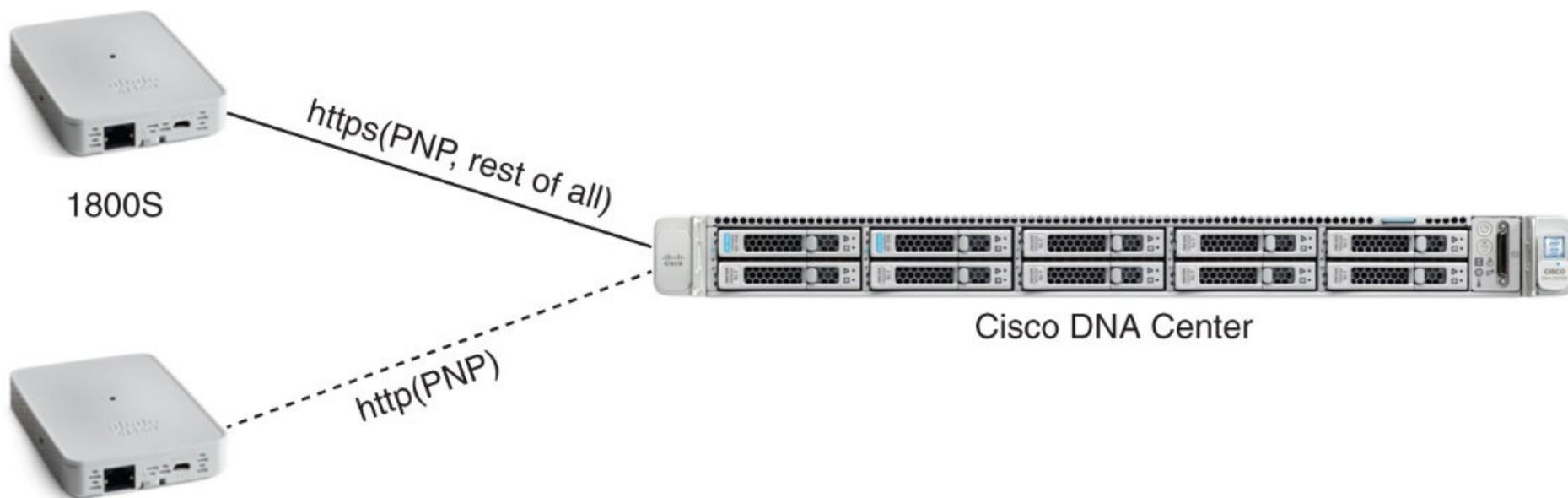


Figure 14-22 1800S protocol workflow overview

Wired Sensor

Actions ▾

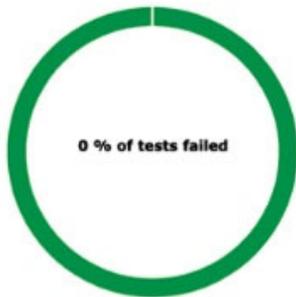
🕒 3 Hours ▾



Location: All Sites

Show

Test Summary



0
Failed Tests

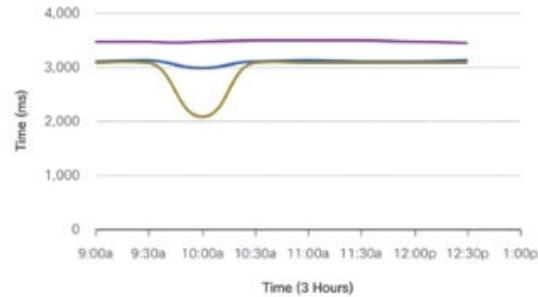
0
Slow Tests

896
Passed Tests

DHCP

100% Success of 224 Tests

Top Impacted Site: --



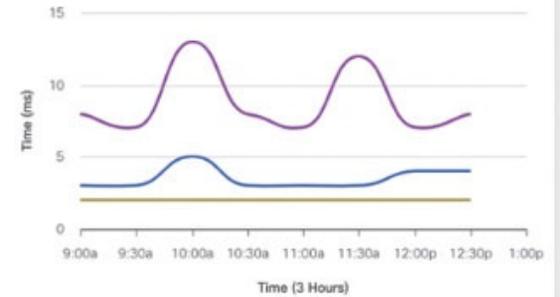
● Average ● Top ● Bottom --- Slow Threshold

No Global Issues

DNS

100% Success of 224 Tests

Top Impacted Site: --



● Average ● Top ● Bottom --- Slow Threshold

No Global Issues

Figure 14-23 Cisco 1800S test suite dashboard

Test Results

 Filter

 Find

Test Name ▲	Location	Vlan	Test Types	Test Results
wired_sensor		vlan11	Onboarding Test DHCP Test DNS Test	

Showing 1 of 1

Figure 14-24 Cisco 1800S test result timeline

All Devices > deadbeef-1.dna.local

deadbeef-1.dna.local [Run Commands](#) [View 360](#) Last updated: 11:12 AM [Refresh](#)

ASSURANCE DEADBEEF

● Reachable | ● Managed | IP Address: 192.168.0.101 | Device Model: Cisco Catalyst 9200L Switch Stack | Role: ACCESS | Uptime: 33 days 12 hrs | Site: Global/Deadbeef/Area-1/Building-1

DETAILS

- Interfaces
- Ethernet Ports
- VLANs
- Hardware & Software
- Configuration**
- Power
- Fans

COMPLIANCE

Building configuration...

Current configuration : 28541 bytes

```
!
! Last configuration change at 18:49:27 UTC Wed Sep 16 2020 by netadmin!
! NVRAM config last updated at 18:49:35 UTC Wed Sep 16 2020 by netadmin!
!
version 17.3
service timestamps debug datetime msec
service timestamps log datetime msec show-timezone year
service password-encryption
service call-home
no platform punt-keepalive disable-kernel-core
!
```

Figure 15-1 The Export CLI Output allows you to export the configuration of a device

 Cisco Catalyst 9800-L Wireless Controller 17.6.1
 Welcome *admin*

Administration > **Software Management**

Search Menu Items

- Dashboard
- Monitoring >
- Configuration >
- Administration >
- Licensing
- Troubleshooting

Walk Me Through >

Software Upgrade

<p>Software Maintenance Upgrade (SMU)</p> <p>AP Service Package (APSP)</p> <p>AP Device Package (APDP)</p>	<p>Upgrade Mode <input type="text" value="INSTALL"/></p> <p>One-Shot Install Upgrade <input type="checkbox"/></p> <p>Transport Type <input type="text" value="My Desktop"/></p> <p>File System <input type="text" value="bootflash"/> Free Space: 18271.05 MB</p> <p>Source File Path* <input type="text" value="Select File"/></p>	<p>Current Mode (until next reload): INSTALL</p> <p>Manage</p> <p>Remove Inactive Files</p> <p>Rollback</p>
--	---	---

Download & Install
Save Configuration & Activate

Figure 15-3 The Catalyst 9800 upgrade page

Troubleshooting > Syslog

Syslog Web Server Logs License logs

Number of latest Syslog entries to display* [View](#) [Manage Syslog Servers](#)

[Clear](#) [Download](#) [Refresh](#) [Scroll to Bottom](#)

hostname/domain name
*Mar 19 12:10:35.620: %CRYPTO_ENGINE-4-CSDL_COMPLIANCE_RSA_WEAK_KEYS: RSA keypair CISCO_IDEVID_SUDI_LEGACY is in violation of Cisco security compliance guidelines and will be rejected by future releases.
*Mar 19 08:29:59.781: %RIF_MGR_FSM-6-GW_REACHABLE_ACTIVE: Chassis 1 R0/0: rif_mgr: Gateway reachable from Active
*Mar 19 04:17:23.781: %RIF_MGR_FSM-6-GW_REACHABLE_ACTIVE: Chassis 1 R0/0: rif_mgr: Gateway reachable from Active
*Mar 18 23:28:24.991: %WEBSERVER-5-SESS_TIMEOUT: Chassis 1 Session timeout from host 192.168.1.67 by user 'katgeri' using crypto cipher 'ECDHE-RSA-AES128-GCM-SHA256'
*Mar 18 20:00:21.952: %WEBSERVER-5-LOGIN_PASSED: Chassis 1 Login Successful from host 192.168.1.67 by user 'katgeri' using crypto cipher 'ECDHE-RSA-AES128-GCM-SHA256'
*Mar 18 20:00:21.951: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: katgeri] [Source: 192.168.1.5] [localport: 21111] at 20:00:21 Central Fri Mar 18 2022
*Mar 18 19:58:37.275: %SYS-5-CONFIG_I: Configured from console by katgeri on vty0 (192.168.1.67)
*Mar 18 19:58:02.104: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully encrypted private config file
*Mar 18 19:57:54.729: %SYS-5-CONFIG_I: Configured from console by katgeri on vty0 (192.168.1.67)
*Mar 18 19:57:46.597: %LINK-3-UPDOWN: Interface Loopback0, changed state to up
*Mar 18 19:57:46.596: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
*Mar 18 19:57:39.569: %SYS-5-CONFIG_I: Configured from console by katgeri on vty0 (192.168.1.67)
*Mar 18 19:57:32.997: %WEBSERVER-5-SESS_LOGOUT: Chassis 1 Successfully logged out from host 192.168.1.67 by user 'katgeri' using crypto cipher 'ECDHE-RSA-AES128-GCM-SHA256'

Figure 16-1 Troubleshooting Dashboard (Syslog)

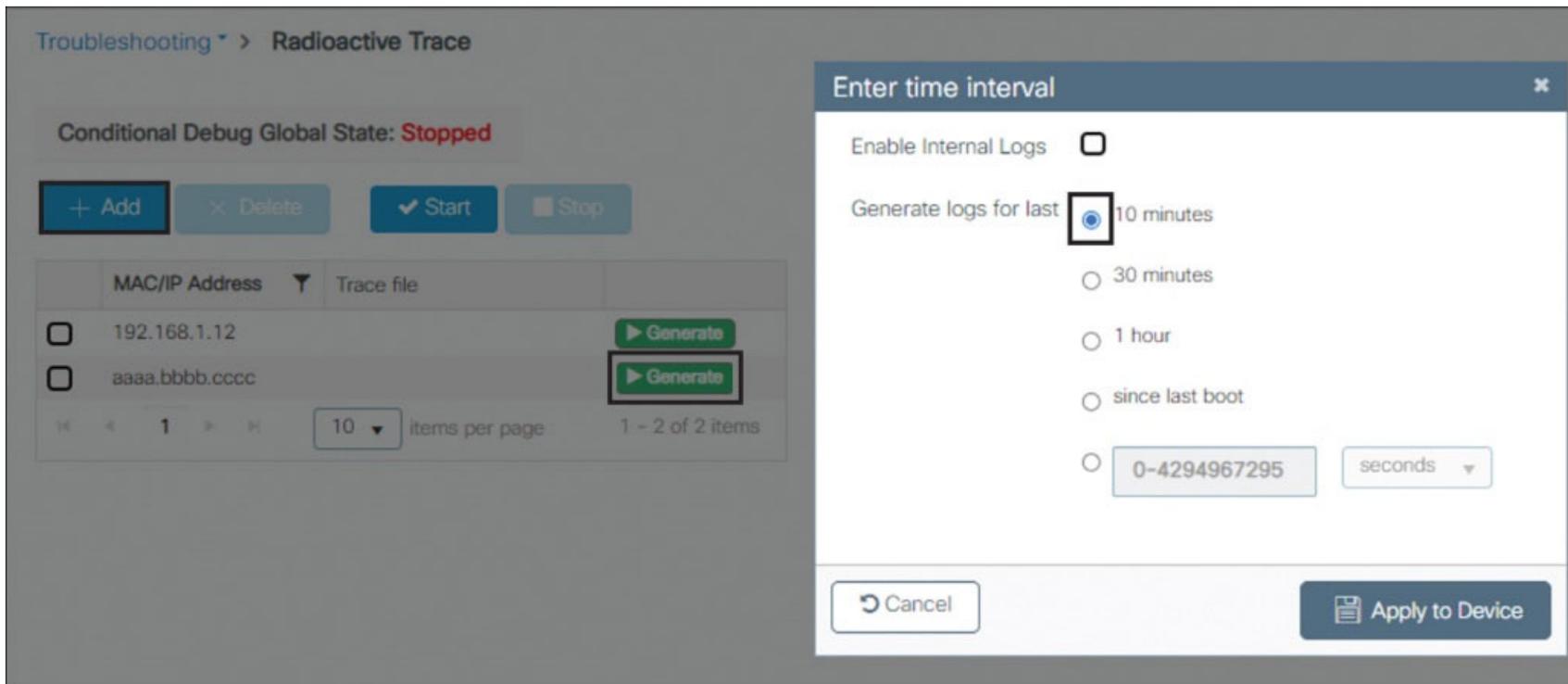


Figure 16-2 Collecting always-on traces for a client MAC from the C9800 GUI

Troubleshooting > Packet Capture

+ Add × Delete

	Capture Name	Interface	Monitor Control Plane	Buffer Size	Filter by	Limit	Status	Action
<input type="checkbox"/>	MYCAP	TwoGigabitEthernet0/0/2	Yes	0%	acl	0 secs	Inactive	▶ Start

◀ 1 ▶ 10 items per page 1 - 1 of 1 items

Figure 16-3 Selecting the AP MAC address for conditional tracing from APs listed under Monitoring

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

× Delete 

Selected 0 out of 1 Clients

<input type="checkbox"/>	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	SSID	WLAN ID	Client Type	State
<input type="checkbox"/>	9233.17c6.561e 	10.150.1.12	fe80::9033:17ff:fec6:561e	9120	11renable	2	WLAN	Run

10 items per page 1 - 1 of 1 clients

Figure 16-4 Selecting the client MAC address for conditional tracing from the client listed under Monitoring

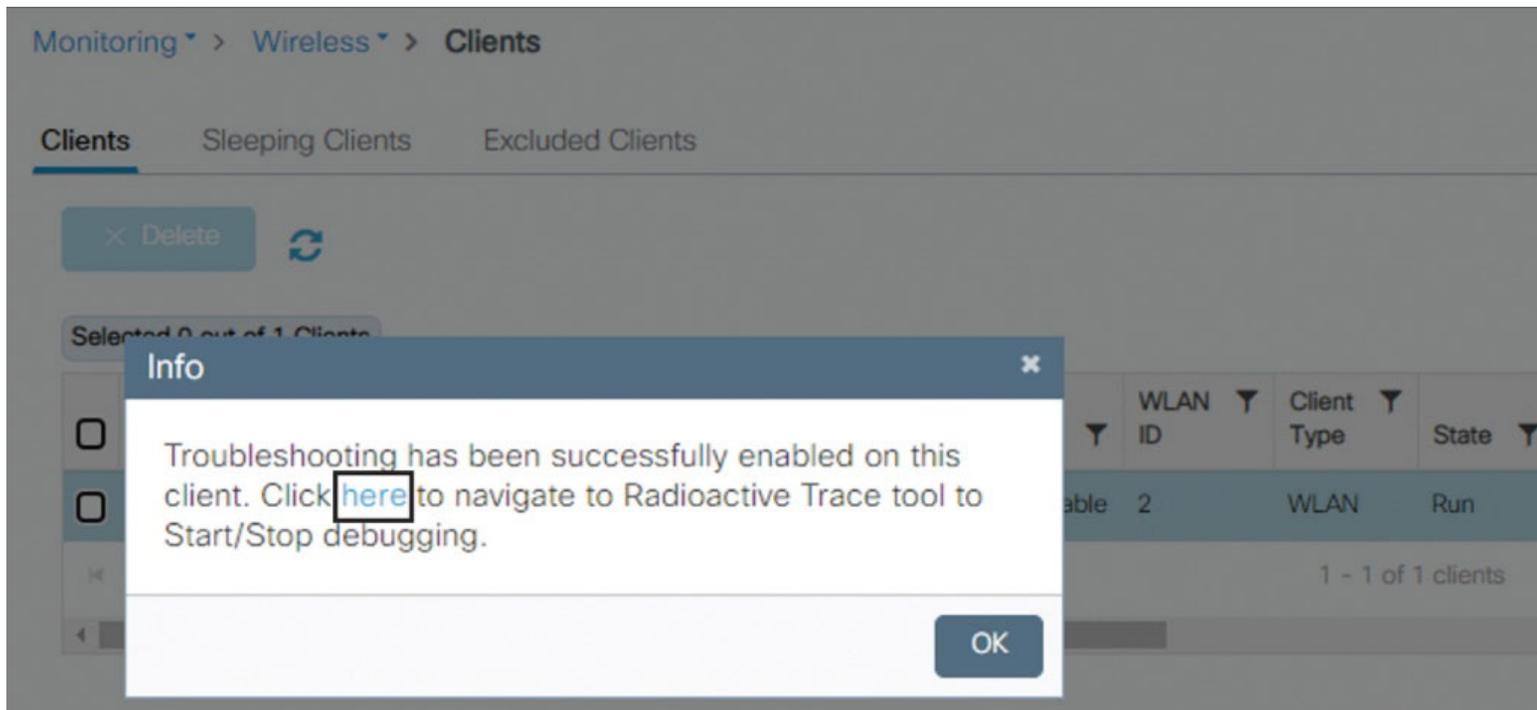


Figure 16-5 Direct navigation of the C9800 GUI from Monitoring to Troubleshooting

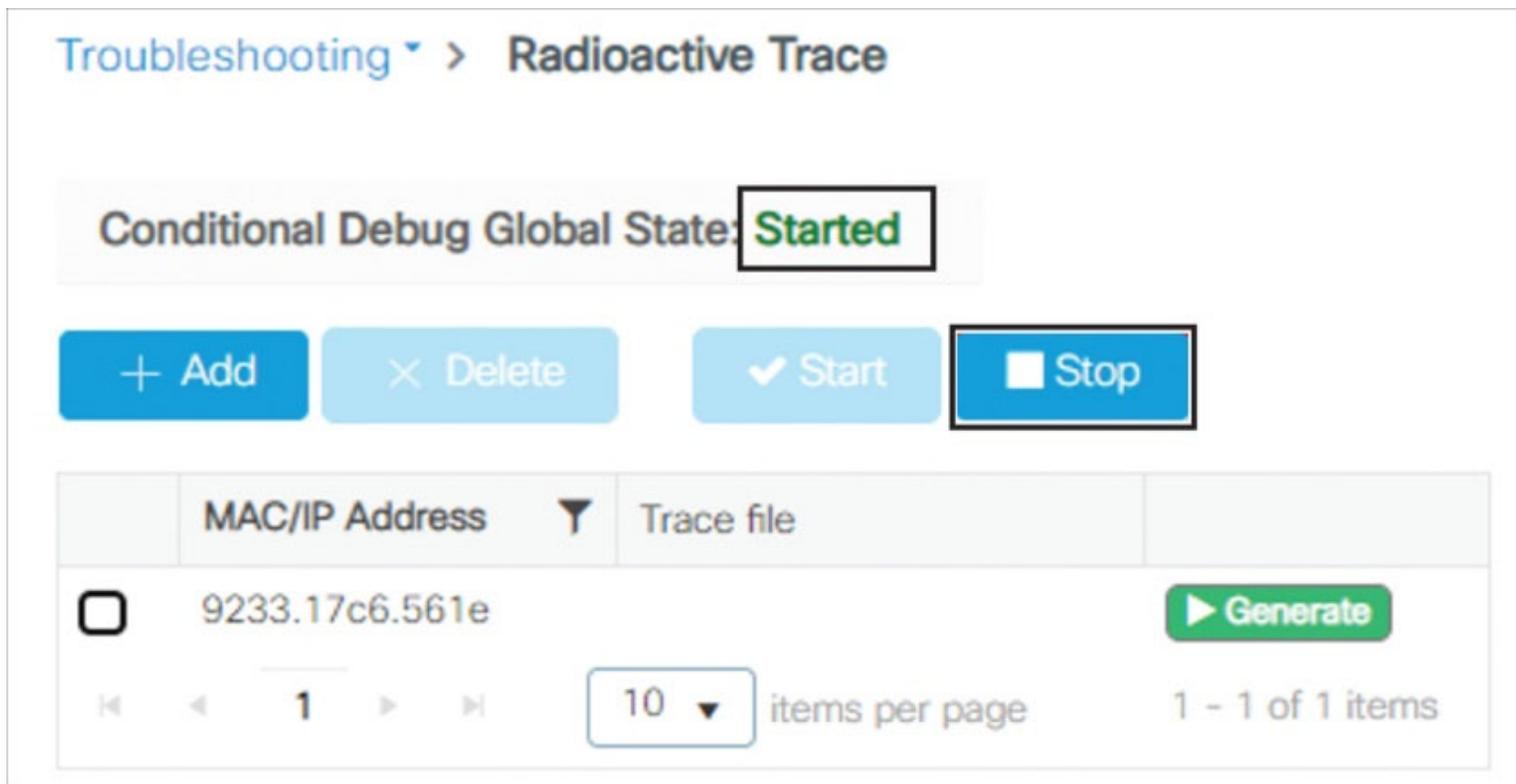


Figure 16-6 Starting a radioactive trace on the C9800 GUI

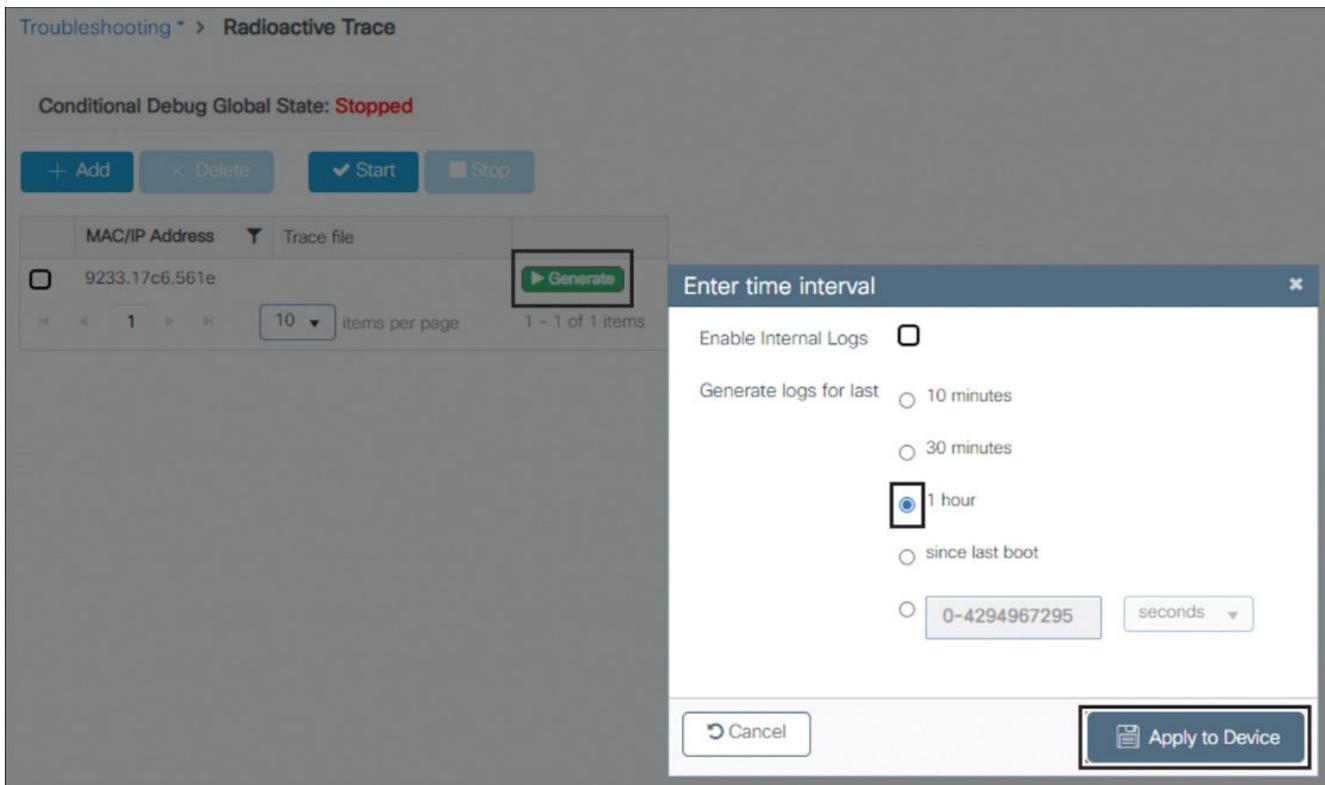


Figure 16-7 Collecting customer-use radioactive traces from the C9800 GUI

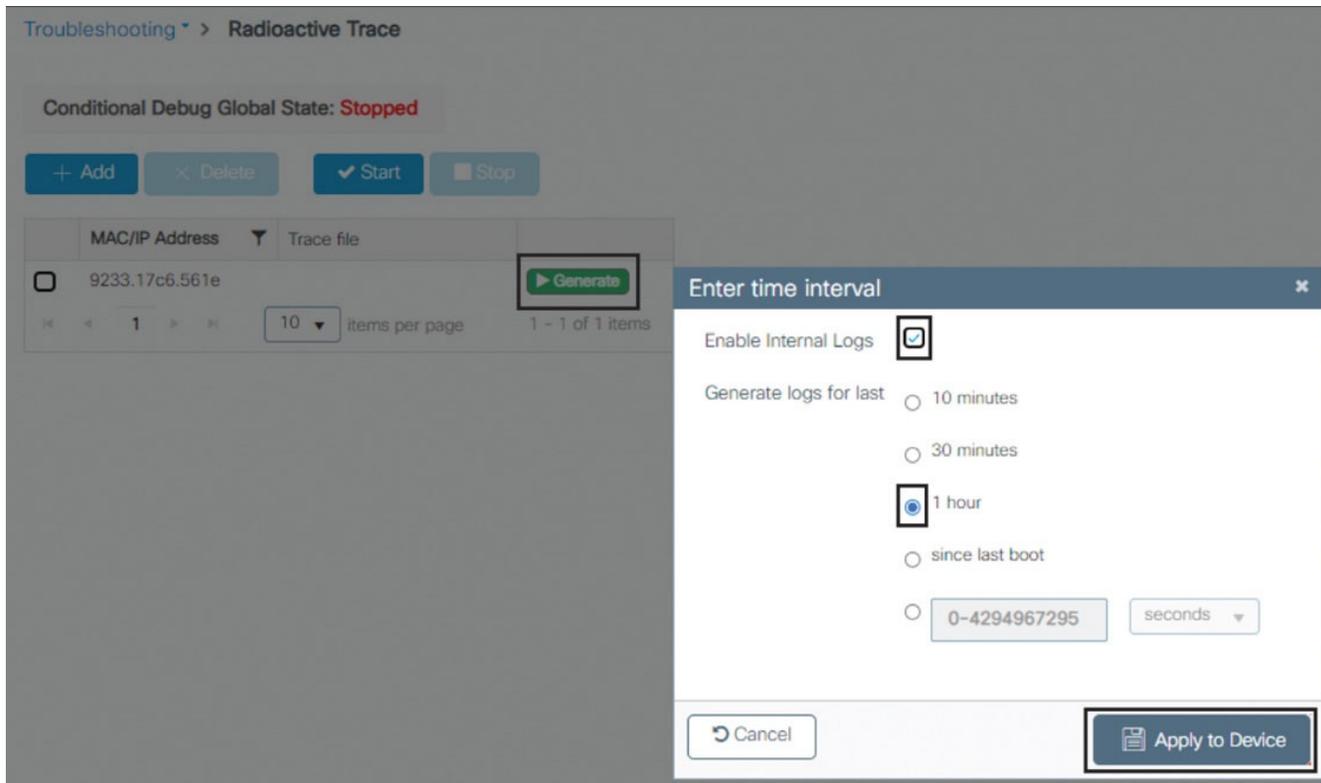


Figure 16-8 Collecting internal radioactive traces from the C9800 GUI

```

C9800#show platform software punt-policer | include Punt|Cause|--|EPC
Per Punt-Cause Policer Configuration and Packet Counters
Punt  Description  Config Rate(pps)  Conform Packets  Dropped Packets  Config Burst(pkts)  Config Alert
Cause          Normal  High  Normal  High  Normal  High  Normal  High  Normal  High
-----
75    EPC          8738  1000    0      0     0      0     8738  1000  Off    Off

```

Figure 16-9 Viewing the default EPC punt policer

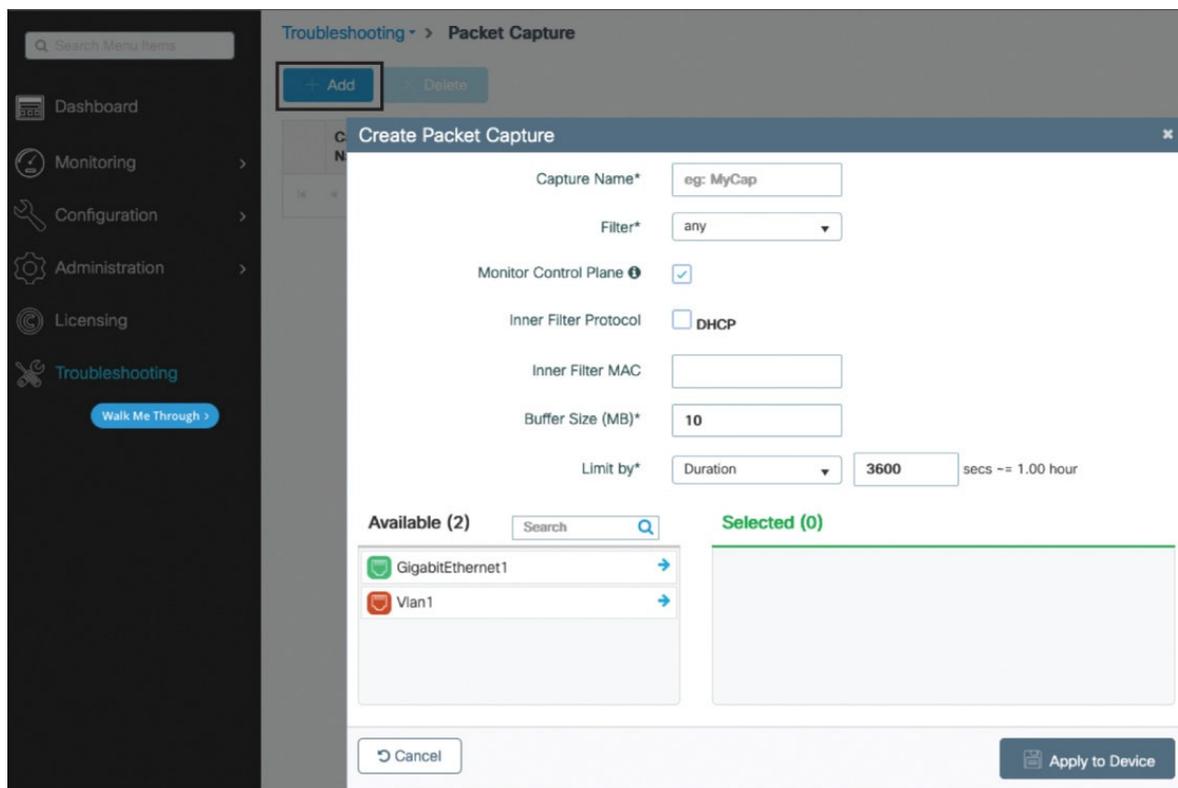


Figure 16-10 Enabling EPC on the C9800 Troubleshooting dashboard

22	2022-03-15	04:29:50.301971	10.5.1.11	192.168.1.5	191 Application Data
23	2022-03-15	04:29:52.336972	10.5.1.11	192.168.1.5	479 Application Data
24	2022-03-15	04:29:52.337979	192.168.1.5	10.5.1.11	411 Application Data
25	2022-03-15	04:29:52.337979	192.168.1.5	10.5.1.11	587 Application Data
26	2022-03-15	04:29:52.340970	10.5.1.11	192.168.1.5	143 Application Data
27	2022-03-15	04:29:52.342969	192.168.1.5	10.5.1.11	155 Application Data
28	2022-03-15	04:29:52.378978	10.5.1.11	192.168.1.5	175 Application Data
29	2022-03-15	04:29:52.446967	10.5.1.11	192.168.1.5	159 Application Data
30	2022-03-15	04:29:52.446967	192.168.1.5	10.5.1.11	155 Application Data
31	2022-03-15	04:29:52.446967	192.168.1.5	10.5.1.11	155 Application Data
32	2022-03-15	04:29:52.452964	10.5.1.11	192.168.1.5	303 Application Data
33	2022-03-15	04:29:52.494969	10.5.1.11	192.168.1.5	223 Application Data

encrypted

Figure 16-11 EPC showing only encrypted packets with data DTLS without control plane monitoring

80	2022-03-15 04:37:43.681956	92:33:17:c6:56:1e	Cisco_23:c6:4b	419 Association Request, SN=1105, FN=0, Flags=....., SSID=11renable
90	2022-03-15 04:37:43.723961	92:33:17:c6:56:1e	Cisco_23:c6:4b	107 Response, Identity
96	2022-03-15 04:37:43.826953	92:33:17:c6:56:1e	Cisco_23:c6:4b	233 Client Hello
102	2022-03-15 04:37:43.968944	92:33:17:c6:56:1e	Cisco_23:c6:4b	102 Response, Protected EAP (EAP-PEAP)
106	2022-03-15 04:37:43.984934	92:33:17:c6:56:1e	Cisco_23:c6:4b	228 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
110	2022-03-15 04:37:43.989939	92:33:17:c6:56:1e	Cisco_23:c6:4b	102 Response, Protected EAP (EAP-PEAP)
114	2022-03-15 04:37:43.995935	92:33:17:c6:56:1e	Cisco_23:c6:4b	142 Application Data
118	2022-03-15 04:37:44.000000	92:33:17:c6:56:1e	Cisco_23:c6:4b	144 Application Data
122	2022-03-15 04:37:44.004989	92:33:17:c6:56:1e	Cisco_23:c6:4b	142 Application Data
128	2022-03-15 04:37:44.021986	92:33:17:c6:56:1e	Cisco_23:c6:4b	334 Key (Message 2 of 4)
132	2022-03-15 04:37:44.036985	92:33:17:c6:56:1e	Cisco_23:c6:4b	191 Key (Message 4 of 4)
136	2022-03-15 04:37:44.037992	92:33:17:c6:56:1e	Cisco_23:c6:4b	96 Action, SN=1363, FN=0, Flags=....., SSID=11renable


```

> Frame 106: 228 bytes on wire (1824 bits), 228 bytes captured (1824 bits)
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 10.5.1.11, Dst: 192.168.1.5
> User Datagram Protocol, Src Port: 5248, Dst Port: 5247
> Control And Provisioning of Wireless Access Points - Data
> IEEE 802.11 QoS Data, Flags: .....T
> Logical-Link Control
> 802.1X Authentication
> Extensible Authentication Protocol

```

Figure 16-12 EPC showing decrypted packets even with data DTLS enabled with control plane monitoring

Troubleshooting > Packet Capture

+ Add × Delete

	Capture Name	Interface	Monitor Control Plane	Buffer Size	Filter by	Limit	Status	Action
<input type="checkbox"/>	MYCAP	TwoGigabitEthernet0/0/2	Yes	0%	acl	0 secs	Inactive	▶ Start

◀ 1 ▶ 10 items per page 1 - 1 of 1 items

Figure 16-13 Starting EPC on the C9800 Troubleshooting dashboard

Troubleshooting > Packet Capture

+ Add × Delete

	Capture Name	Interface	Monitor Control Plane	Buffer Size	Filter by	Limit	Status	Action
<input type="checkbox"/>	MYCAP	TwoGigabitEthernet0/0/2	Yes	2%	acl	0 secs	Active	Stop

10 items per page 1 - 1 of 1 items

Figure 16-14 Monitoring progress and stopping EPC capture on the C9800 Troubleshooting dashboard

Troubleshooting > Core Dump and System Report

Core Dump

[Delete](#)

	Date & Time	Size (Bytes)	Name	Download
<input type="checkbox"/>	29 Jan 2022 21:31:26	12602510	bootflash/core/9800L_1_RP_0_wncd_21425_20220129-213122-Central.core.gz	Download

1 - 1 of 1 items

System Report

[Delete](#)

	Date & Time	Size (Bytes)	Name	Download
<input type="checkbox"/>	31 Aug 2021 07:32:17	11769973	bootflash/core/9800L_1_RP_0-system-report_20210831-073206-Central.tar.gz	Download
<input type="checkbox"/>	28 Jun 2021 22:11:56	1900648	bootflash/core/sudha-9800L-2_2_RP_0-system-report_20210628-221155-UTC.tar.gz	Download

Figure 16-15 Core Dump and System Report web page that shows the WNCd core and two older system reports

Troubleshooting > Debug Bundle

Name of the debug bundle

debugBundle_C9800-L



Create a compressed package with required information such as CLI outputs, logs, etc. for reporting and debugging the issues

Enter the CLIs of which output needs to be packaged. Maximum 5 CLIs are allowed.

Enter the CLIs of which output needs to be packaged

View

Add



show tech wireless



Web Server log

Core File

Radioactive Trace log

Create Debug Bundle

Figure 16-16 Troubleshooting the dashboard—Debug Bundle

Troubleshooting > Ping and Traceroute

Destination*

8.8.8.8

Source

GigabitEthernet1

Ping

Traceroute

Source (Device)



GigabitEthernet1

Destination



8.8.8.8



```
#ping ip 8.8.8.8 source GigabitEthernet1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 172.31.9.80
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

Figure 16-17 Troubleshooting the dashboard—Ping and Trace Route

Administration ▾ > Command Line Interface

Exec Configure Run Command Clear Copy Export

```
show ip int bri
```

Control+X: Clear | Control+M: Switch Mode | Control+Return(↵): Execute Command | Control+Y: Copy | Control+Shift+E: Export | Shift+Up Arrow(↑)/Down Arrow(↓): Lookup History

```
Thu Jan 27 2022 09:38:14 GMT+0100 (Central European Standard Time)
=====
#show ip int bri
Interface      IP-Address   OK? Method Status      Protocol
GigabitEthernet1  172.31.9.80 YES DHCP    up          up
Vlan1          unassigned  YES NVRAM   administratively down down
```

Figure 16-19 Command-line interface on the C9800 GUI

Administration > Management > File Manager

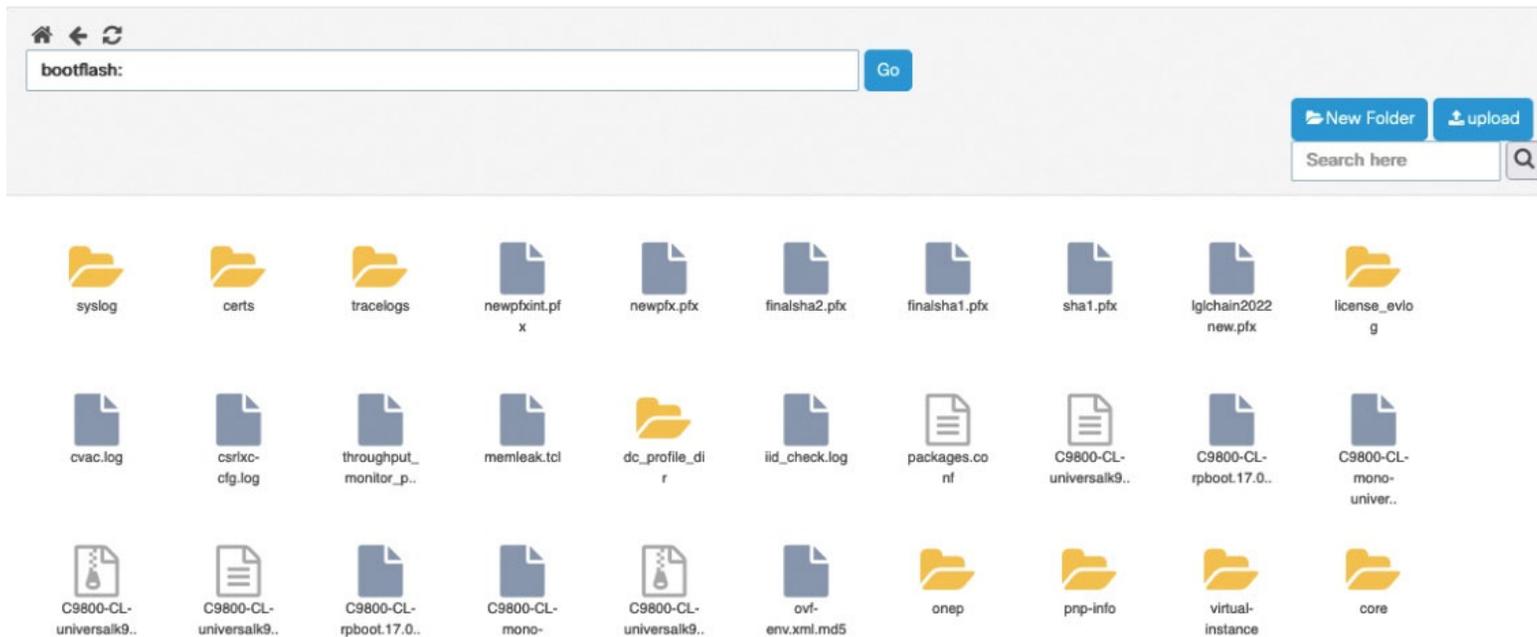


Figure 16-20 File Manager on the C9800 GUI

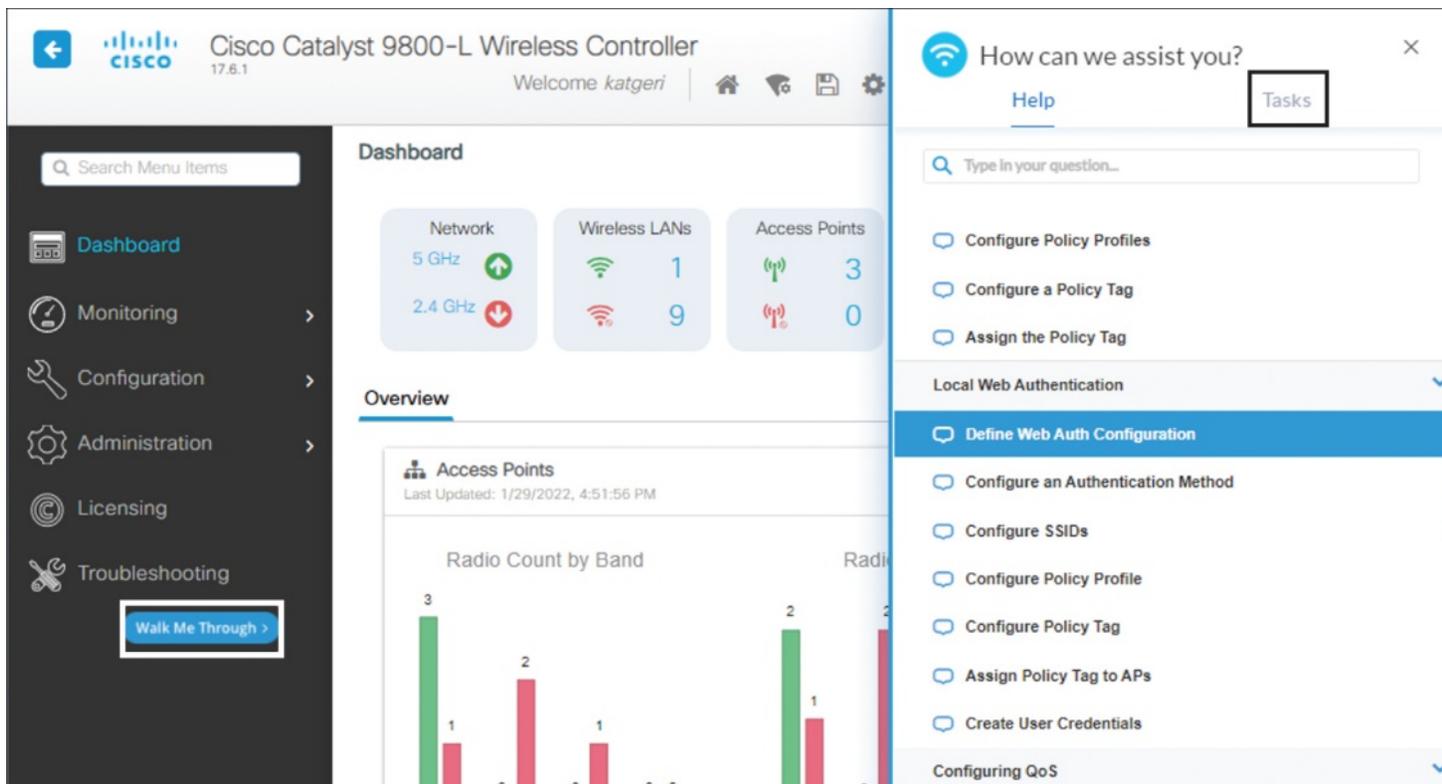


Figure 16-21 Configuration-guided workflow via Walk-me integration on the C9800 GUI

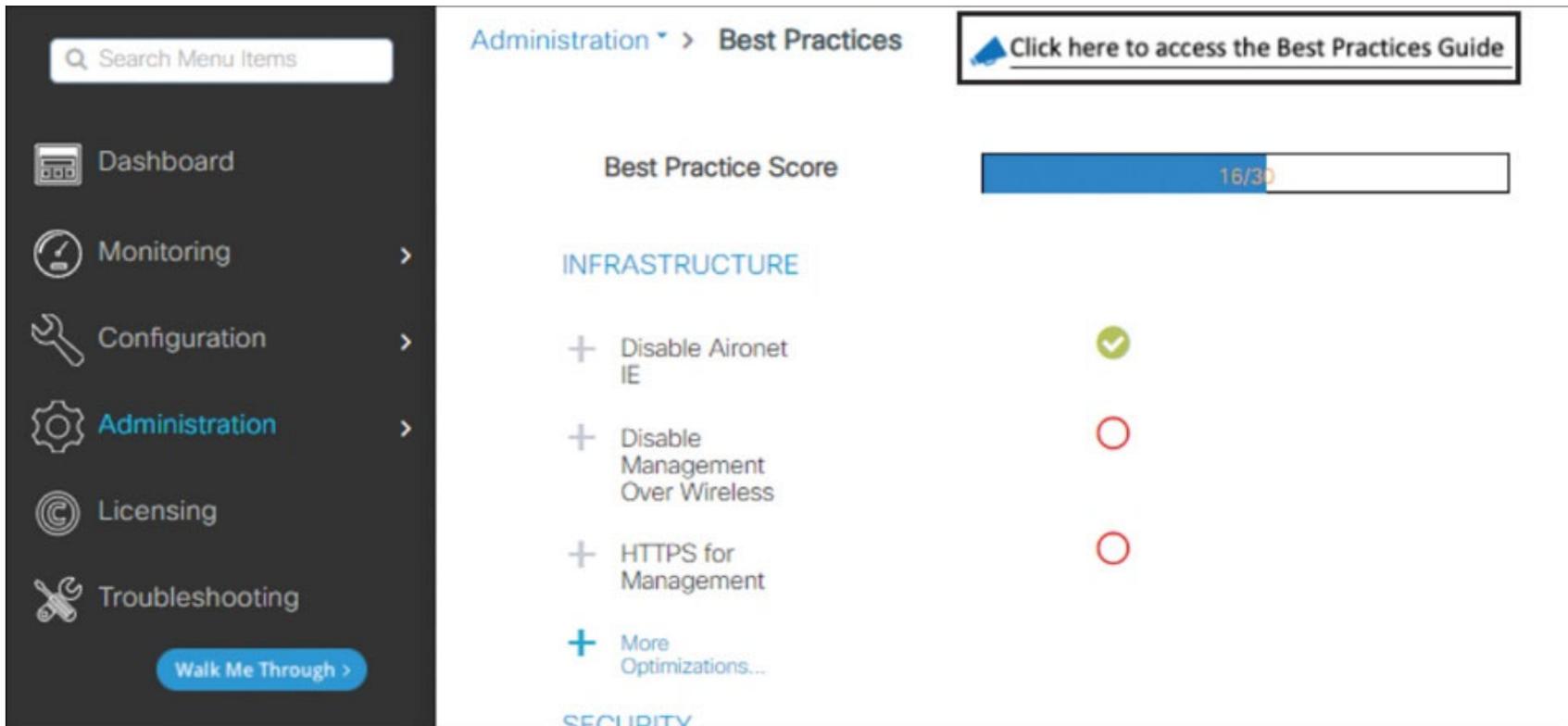


Figure 16-22 Best practices linked to the C9800 GUI via Walk-me integration

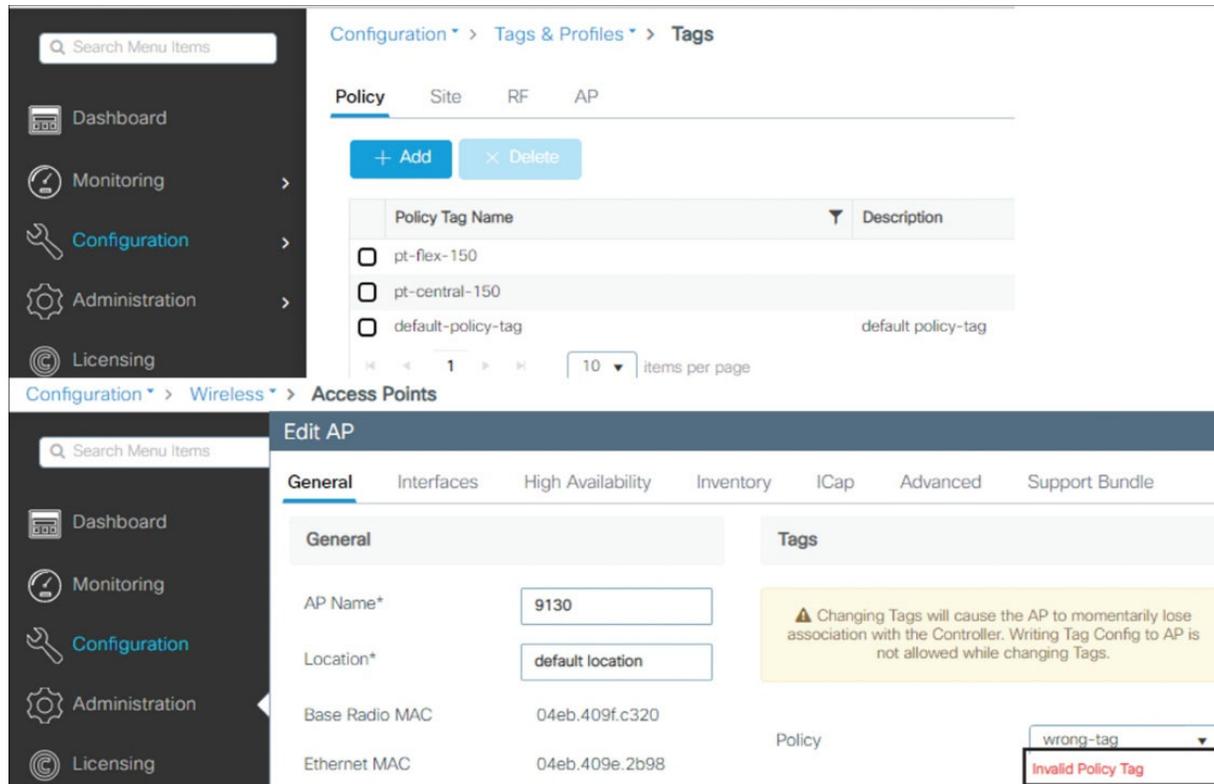


Figure 16-23 C9800 GUI preventing misconfiguration via configuration validation

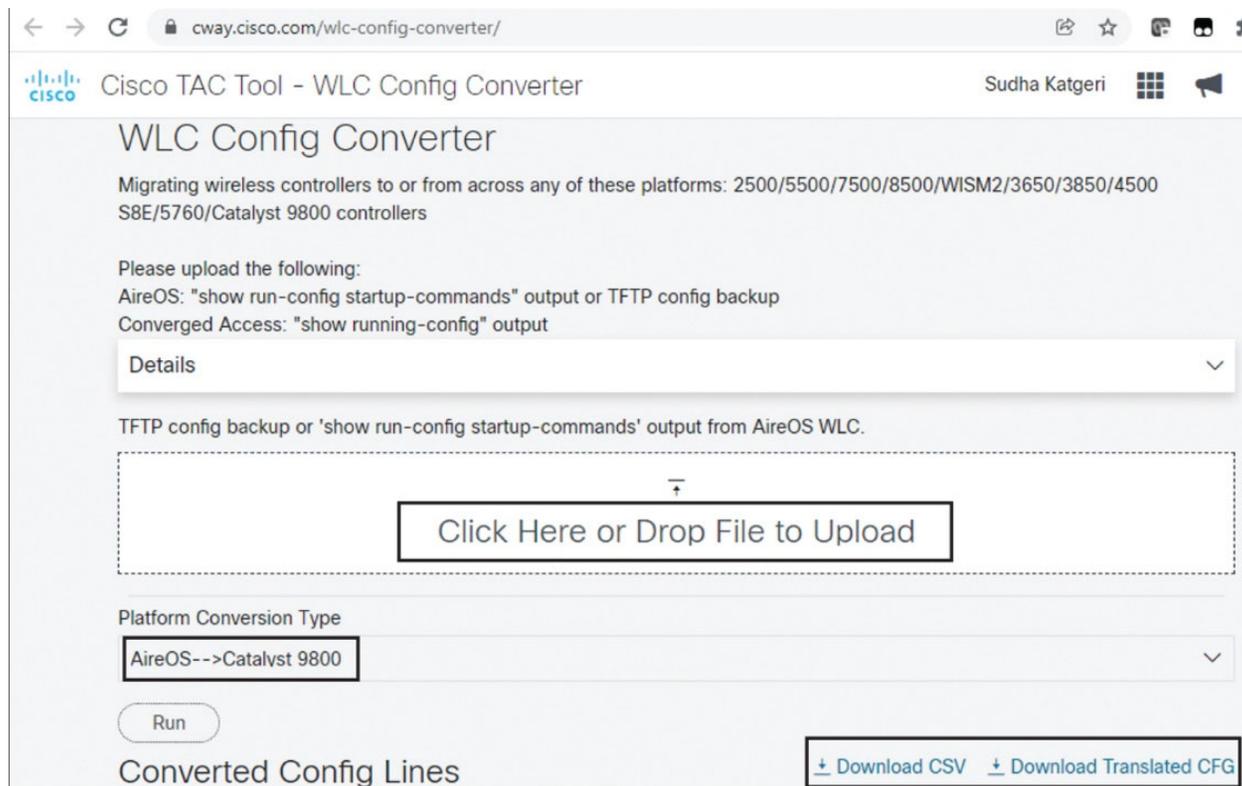


Figure 16-24 Wireless Config Converter on cisco.com

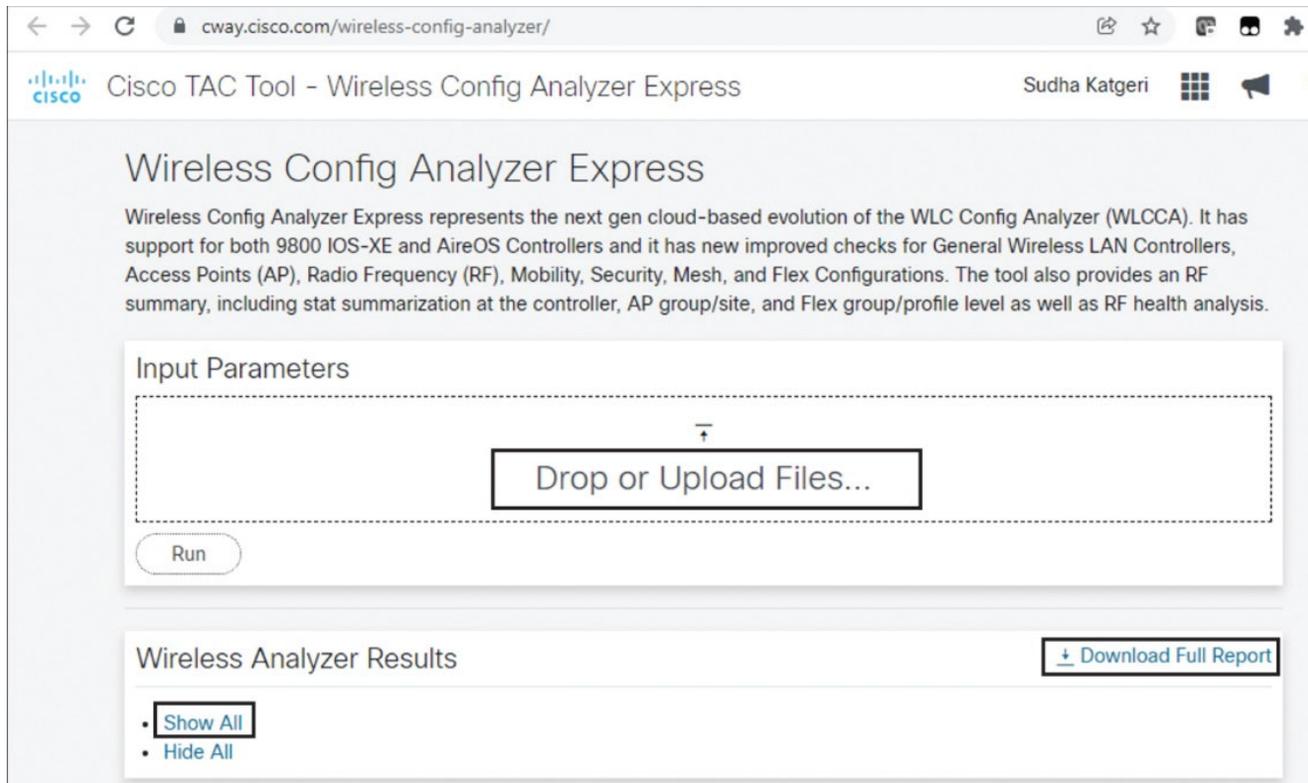


Figure 16-25 Wireless Config Analyzer Express on cisco.com

Cisco TAC Tool - Wireless Debug Analyzer

Nicolas Darchis

Select a client MAC Address and connection to see logs. [Download CSV](#)

Connection 1 of 13

Show Time
 Show Task
 Show Translated
 Show Original
 Show Prior First Connection
 Show All

Time	Task	Translated
2022/01/26 19:13:41.129	client-orch-sm	Client made a new Association to an AP/BSSID: BSSID [REDACTED], WLAN [REDACTED] Slot 0 AP [REDACTED] APA [REDACTED]
2022/01/26 19:13:41.130	dot11	Association success for client, assigned AID is: 1
2022/01/26 19:13:41.130	client-orch-sm	Client started layer 2 authentication (either dot1X or PSK)
2022/01/26 19:13:41.135	client-keymgmt	Sent M1 for EAPOL 4-Way Handshake
2022/01/26 19:13:41.148	client-keymgmt	Received and validated M2 for EAPOL 4-Way Handshake
2022/01/26 19:13:41.148	client-keymgmt	Sent M3 for EAPOL 4-Way Handshake
2022/01/26 19:13:41.155	client-keymgmt	Received and validated M4 for EAPOL 4-Way Handshake
2022/01/26 19:13:41.155	client-keymgmt	Negotiated the following encryption mechanism: AKM:PSK Cipher:CCMP WPA Version: WPA2
2022/01/26 19:13:41.155	client-auth	Client successfully completed Pre-shared Key authentication. Assigned VLAN: 5
2022/01/26 19:13:41.155	client-orch-sm	Client passed layer 2 authentication
2022/01/26 19:13:41.155	client-orch-state	Starting Mobility Anchor discovery for client
2022/01/26 19:13:41.156	avc-afc	AVC is enabled for the client session
2022/01/26 19:13:41.157	client-orch-state	Entering IP learn state
2022/01/26 19:13:41.842	auth-mgr-feat_dsensor	Not performing DHCP profiling as it is not enabled
2022/01/26 19:13:41.842	sisf-packet	Sending DHCP Discover to: 255.255.255.255 on vlan 5 through gateway 0.0.0.0

Figure 16-26 Wireless Debug Analyzer on cisco.com

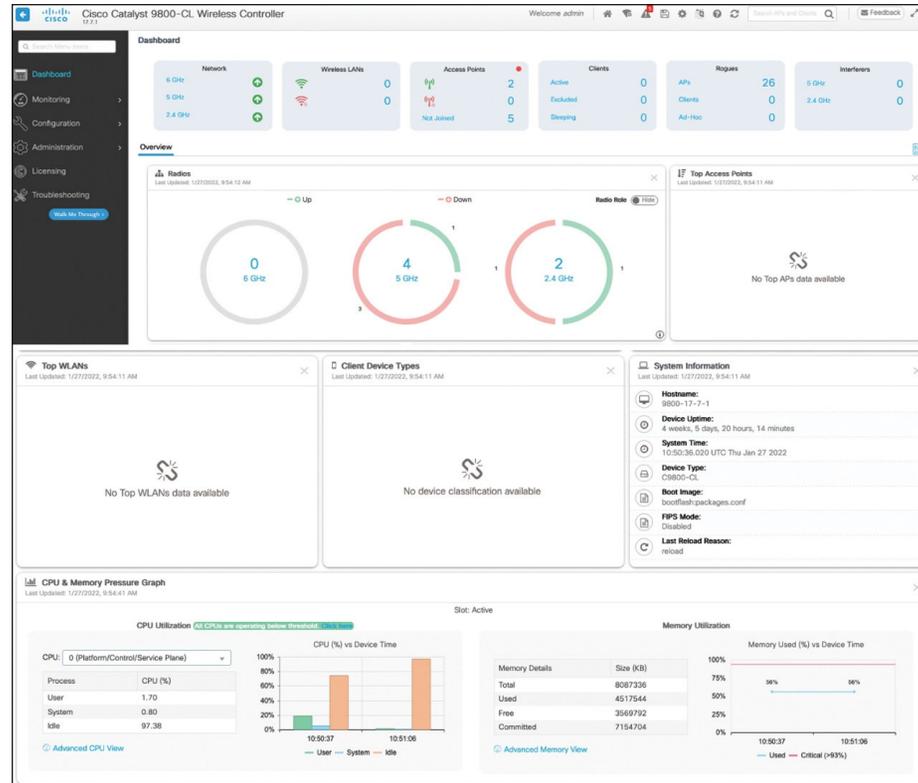


Figure 16-27 Dashboard on the C9800 GUI in IOS-XE 17.7.1

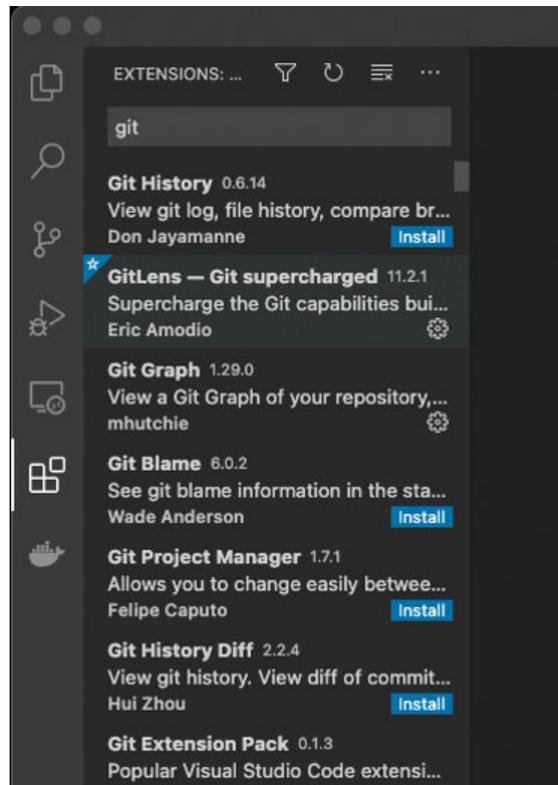


Figure A-1 Git plug-ins for Visual Studio Code

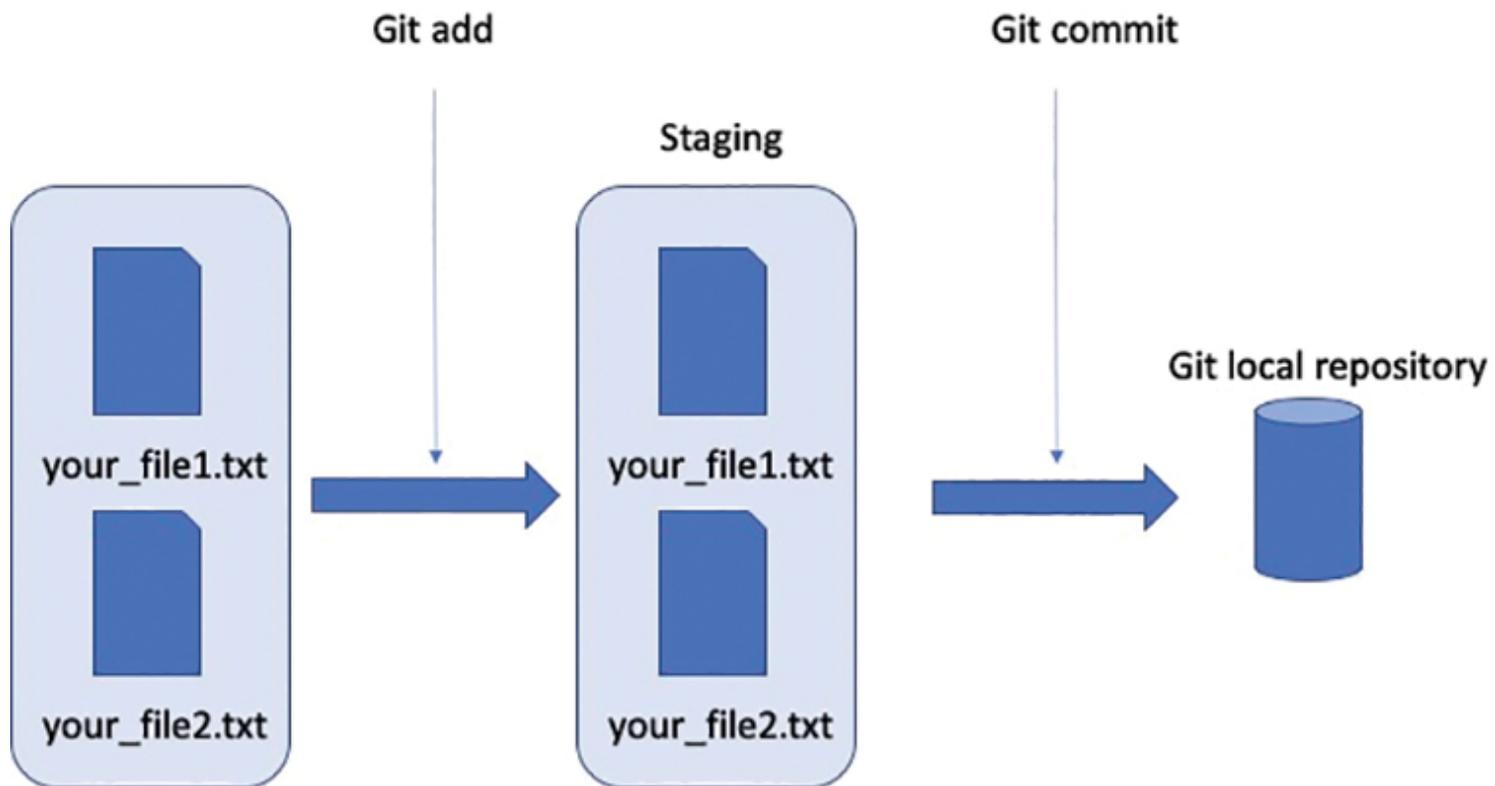


Figure A-2 Git workflow

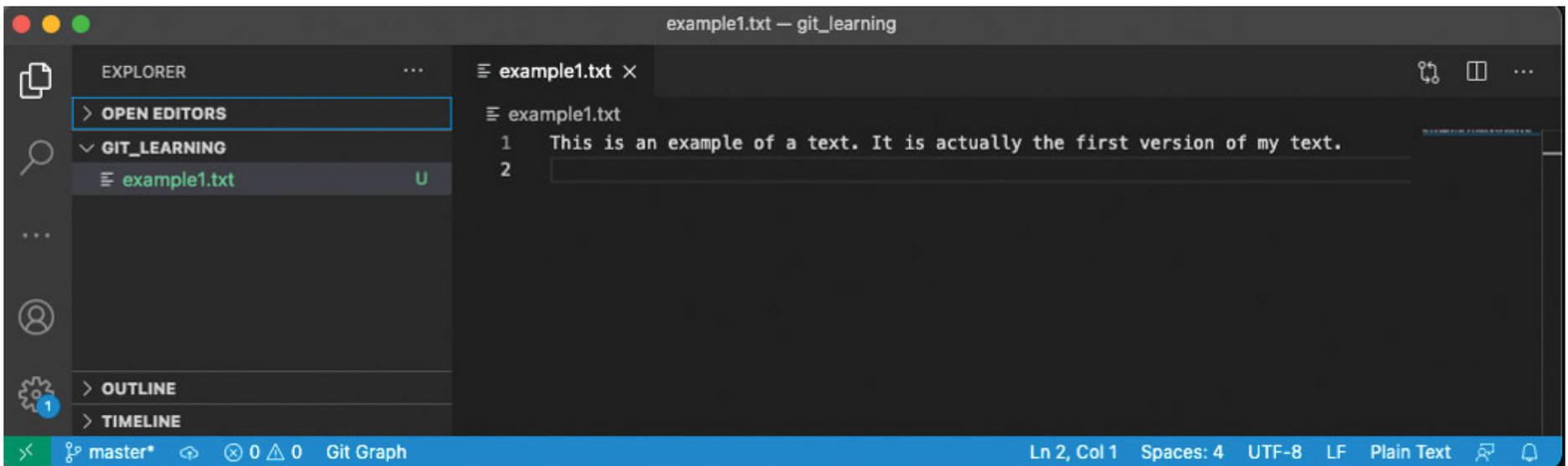


Figure A-3 Creating first file

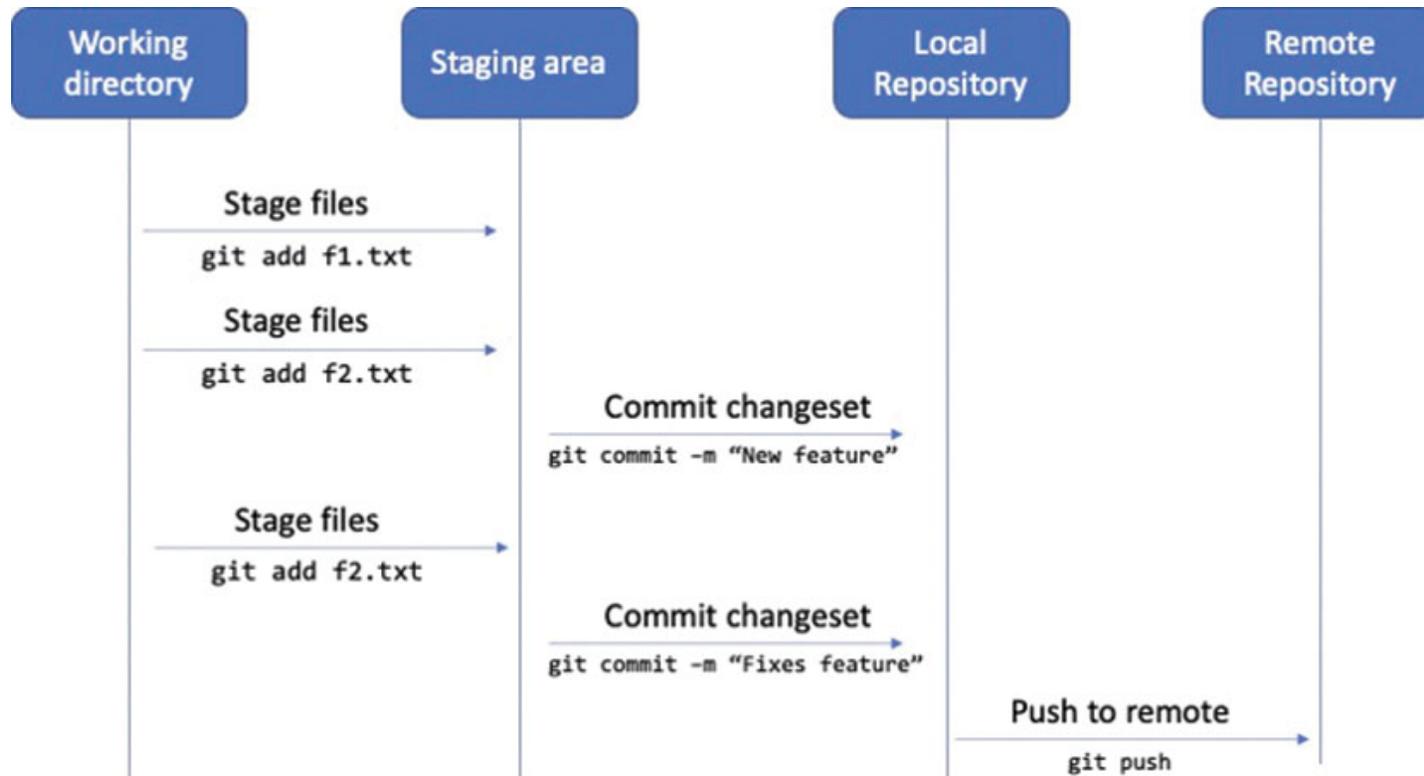


Figure A-4 Commit process in Git

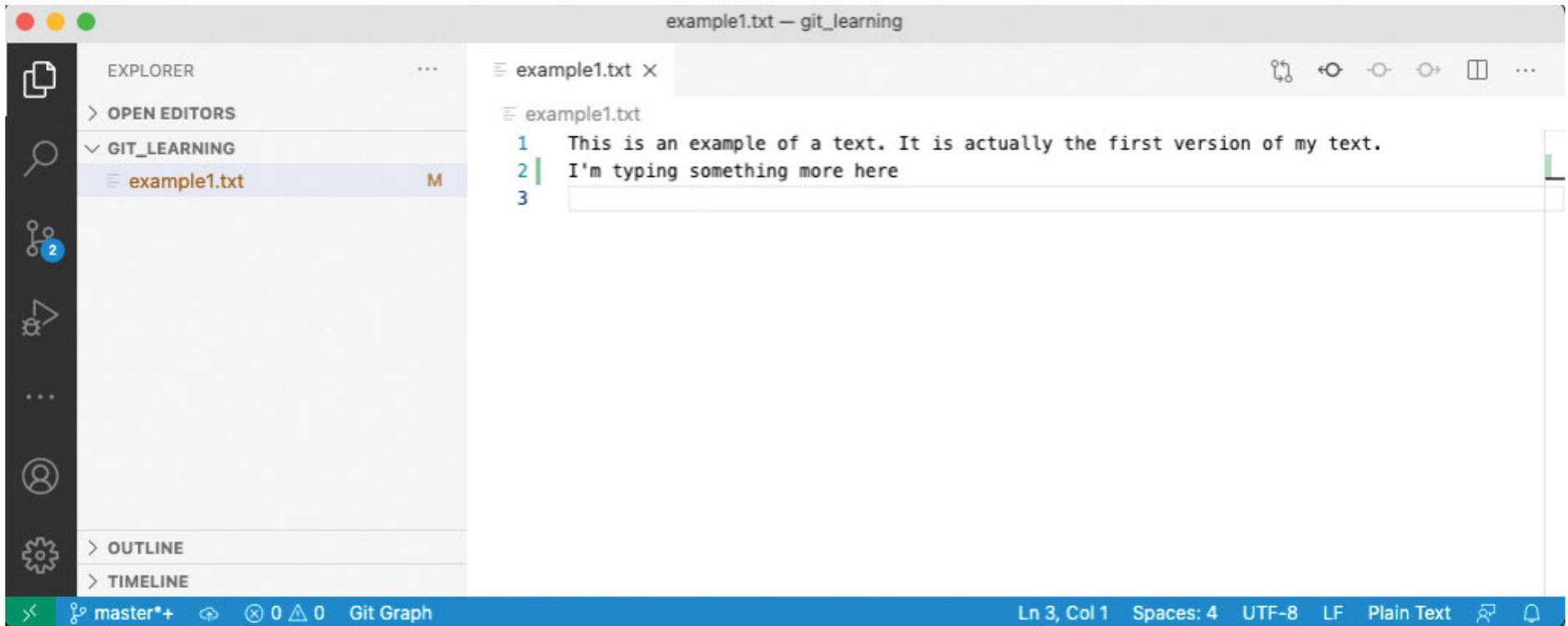


Figure A-5 Updating the first file

```
fsedano@Franciscos-Mac-mini git_learning %  
fsedano@Franciscos-Mac-mini git_learning % git status  
On branch master  
  
No commits yet  
  
Changes to be committed:  
  (use "git rm --cached <file>..." to unstage)  
    new file:   example1.txt  
  
Changes not staged for commit:  
  (use "git add <file>..." to update what will be committed)  
  (use "git restore <file>..." to discard changes in working directory)  
    modified:   example1.txt  
  
fsedano@Franciscos-Mac-mini git_learning %
```

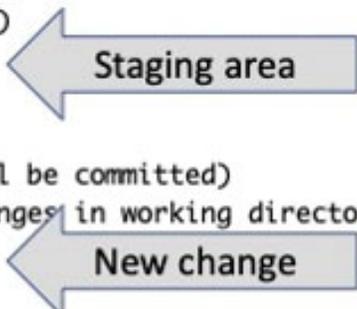
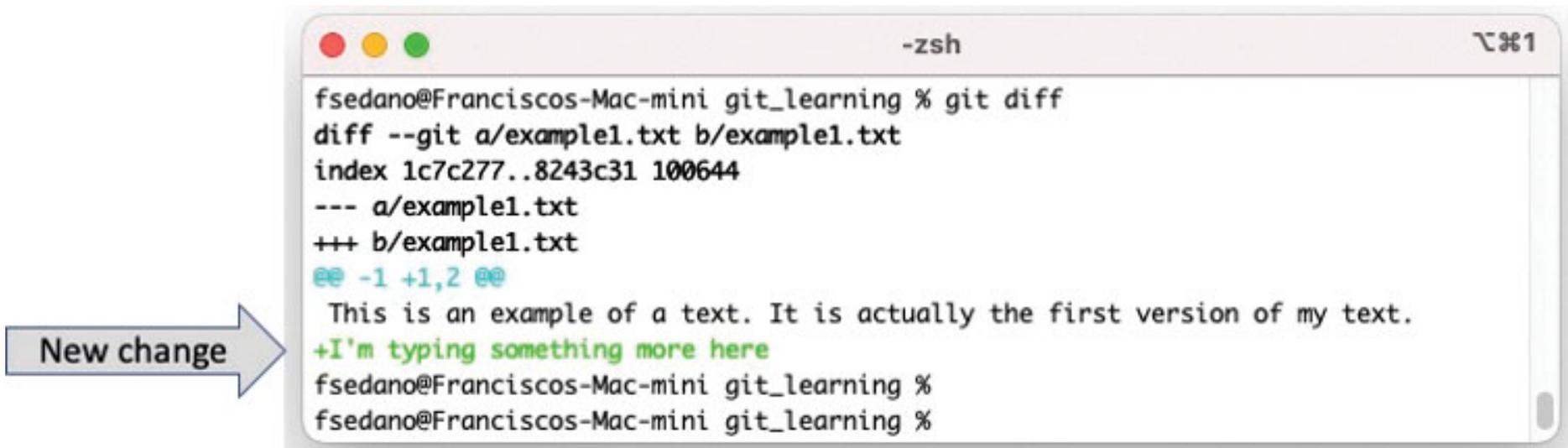
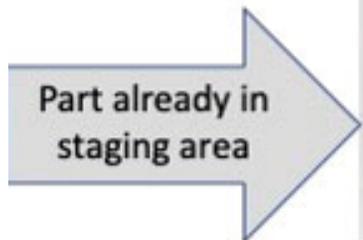


Figure A-6 Git detecting changed files



```
fshedano@Franciscos-Mac-mini git_learning % git diff
diff --git a/example1.txt b/example1.txt
index 1c7c277..8243c31 100644
--- a/example1.txt
+++ b/example1.txt
@@ -1,2 @@
 This is an example of a text. It is actually the first version of my text.
+I'm typing something more here
fshedano@Franciscos-Mac-mini git_learning %
fshedano@Franciscos-Mac-mini git_learning %
```

Figure A-7 Diff between two file versions

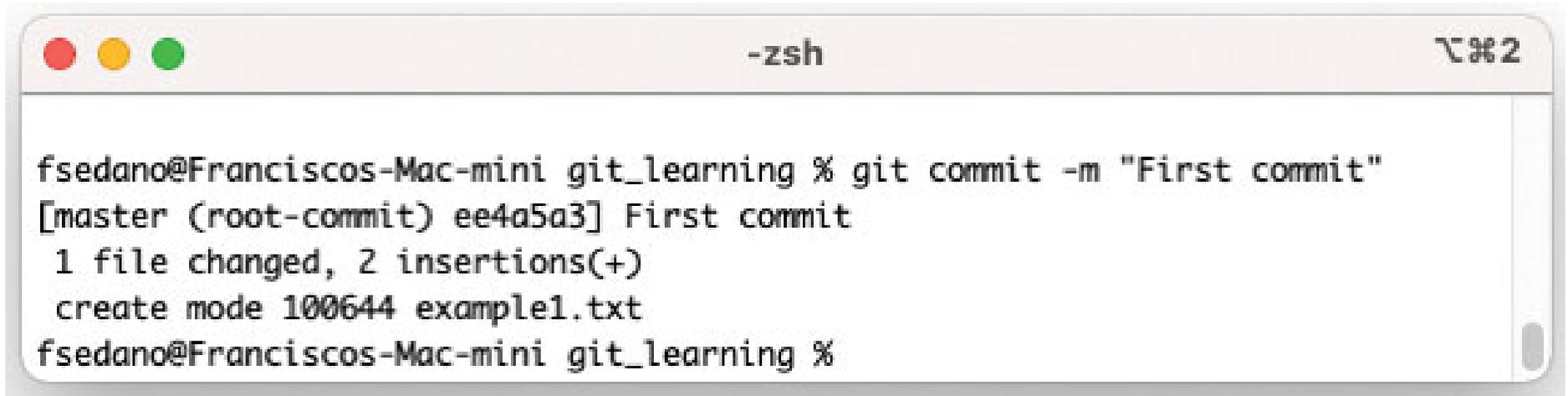


```

fshedano@Franciscos-Mac-mini git_learning % git diff --staged
diff --git a/example1.txt b/example1.txt
new file mode 100644
index 0000000..1c7c277
--- /dev/null
+++ b/example1.txt
@@ -0,0 +1 @@
+This is an example of a text. It is actually the first version of my text.
fshedano@Franciscos-Mac-mini git_learning %
fshedano@Franciscos-Mac-mini git_learning % _

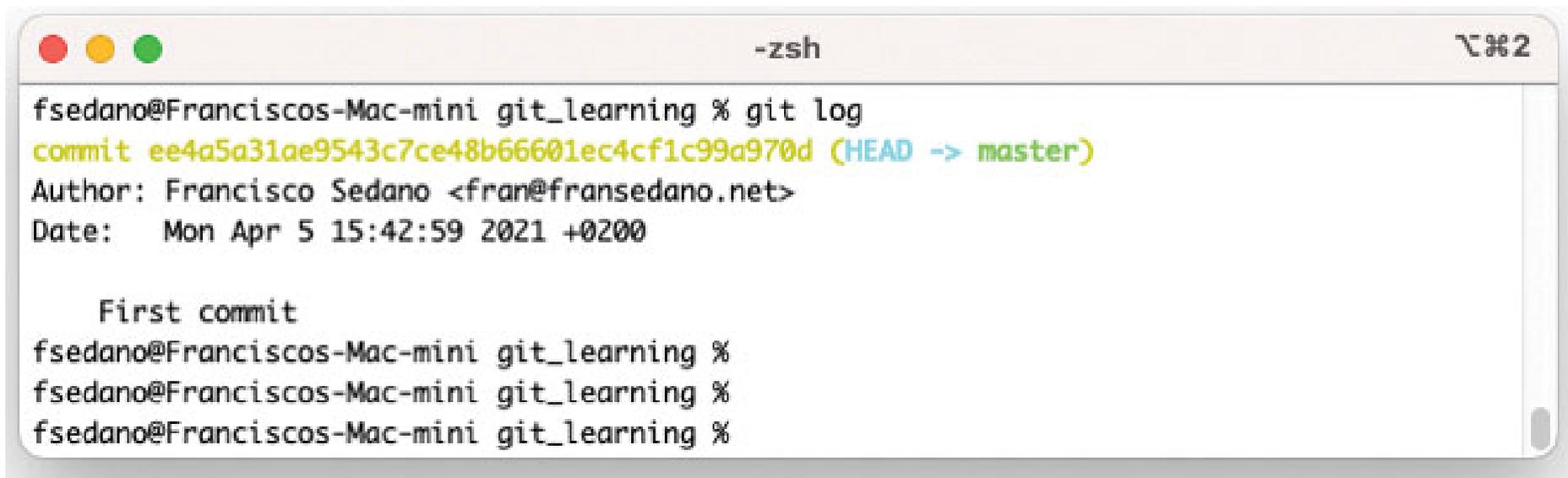
```

Figure A-8 Git displaying staged files

A terminal window titled "-zsh" with standard macOS window controls (red, yellow, green buttons) and a zoom icon in the top right. The terminal text shows a user named "fsedano" at a "Franciscos-Mac-mini" in a "git_learning" directory. They execute the command "git commit -m 'First commit'". The output shows the commit is successful on the "master" branch with hash "ee4a5a3", indicating "1 file changed, 2 insertions(+)" and the creation of "example1.txt" with mode "100644". The prompt returns to "fsedano@Franciscos-Mac-mini git_learning %".

```
fsedano@Franciscos-Mac-mini git_learning % git commit -m "First commit"
[master (root-commit) ee4a5a3] First commit
1 file changed, 2 insertions(+)
create mode 100644 example1.txt
fsedano@Franciscos-Mac-mini git_learning %
```

Figure A-9 Committing changes

A terminal window titled "-zsh" with a window control bar (red, yellow, green buttons) and a zoom icon. The terminal shows the output of a "git log" command. The output includes a commit hash, author information, date, and a commit message. The terminal prompt is "fsedano@Franciscos-Mac-mini git_learning %".

```
fsedano@Franciscos-Mac-mini git_learning % git log
commit ee4a5a31ae9543c7ce48b66601ec4cf1c99a970d (HEAD -> master)
Author: Francisco Sedano <fran@fransedano.net>
Date:   Mon Apr 5 15:42:59 2021 +0200

    First commit
fsedano@Franciscos-Mac-mini git_learning %
fsedano@Franciscos-Mac-mini git_learning %
fsedano@Franciscos-Mac-mini git_learning %
```

Figure A-10 Examining Git repository changes

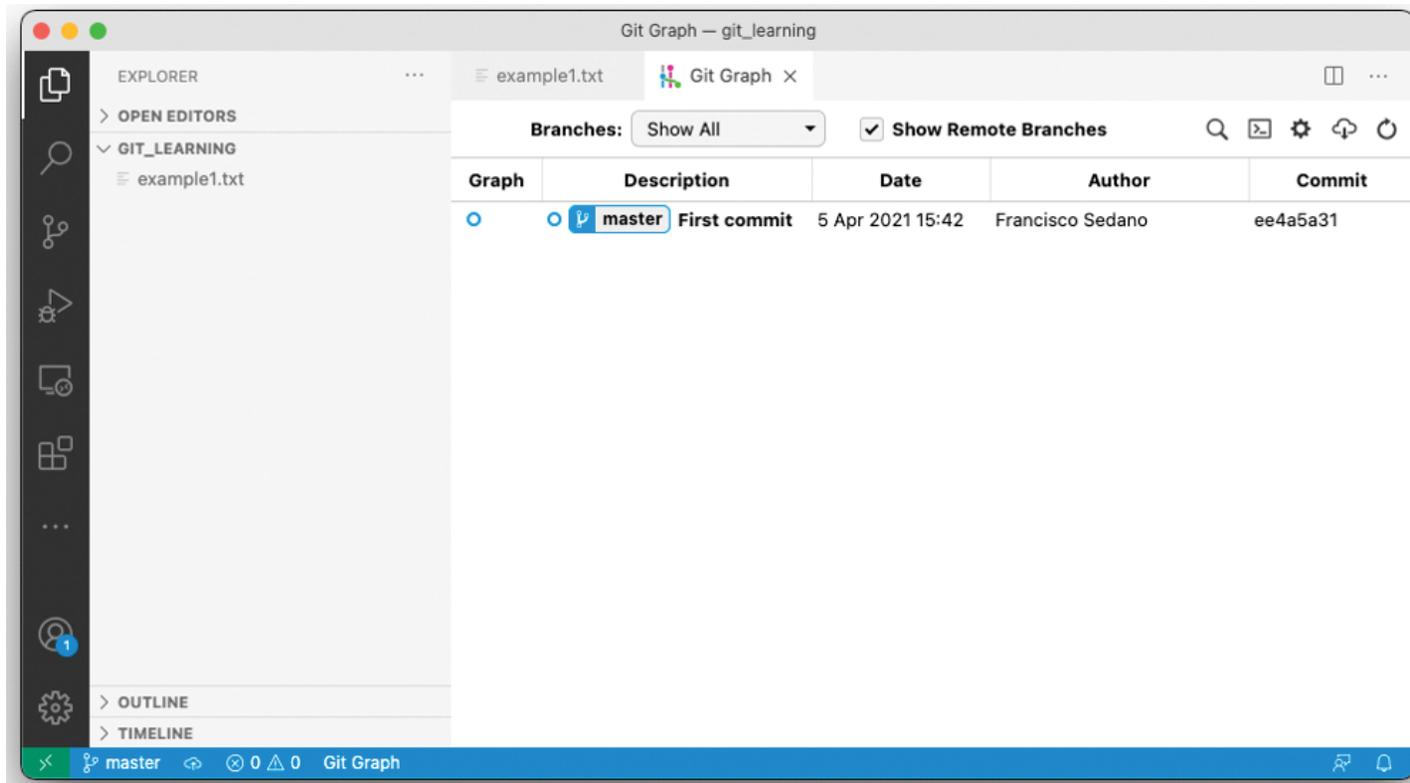


Figure A-11 Viewing repository activity

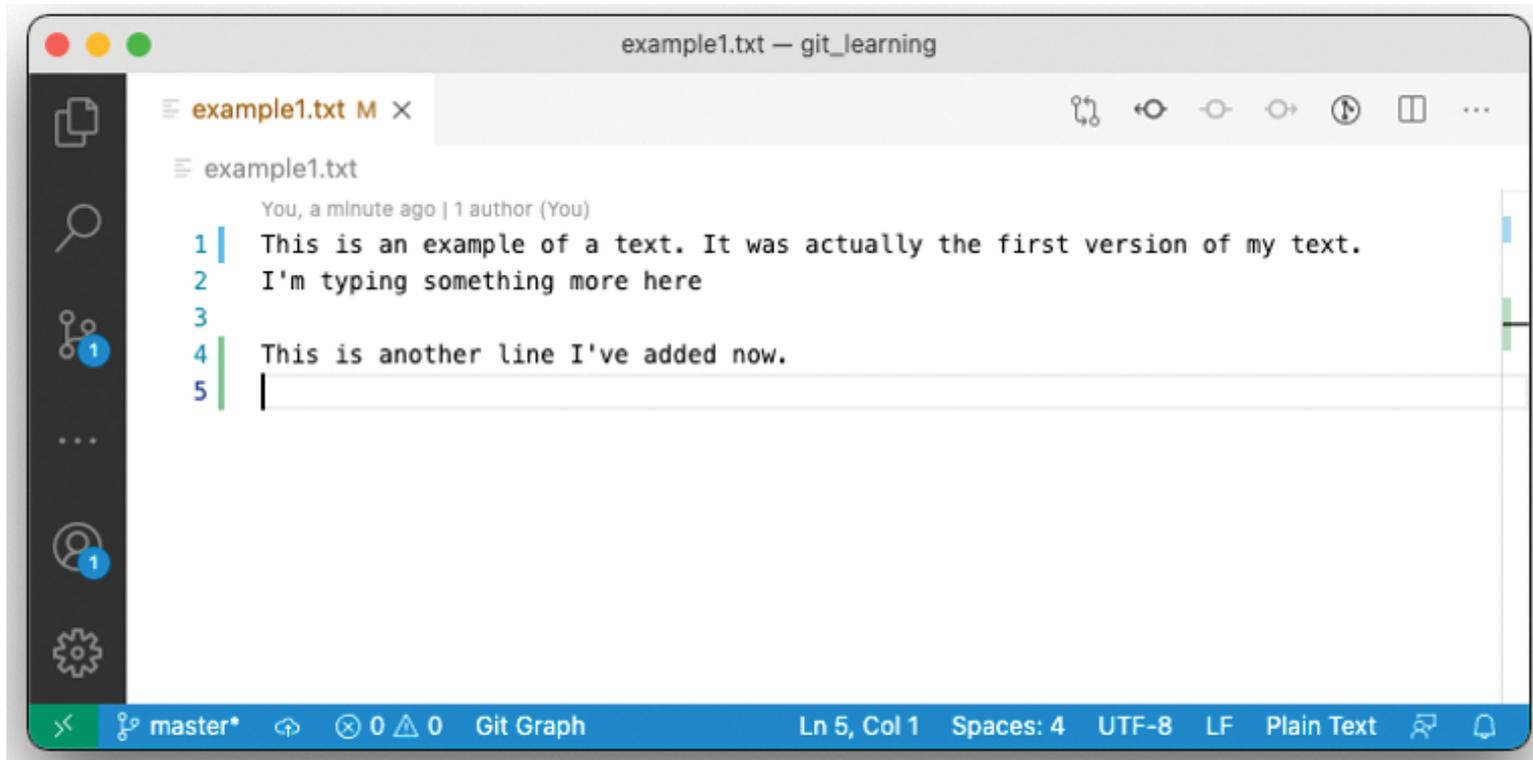
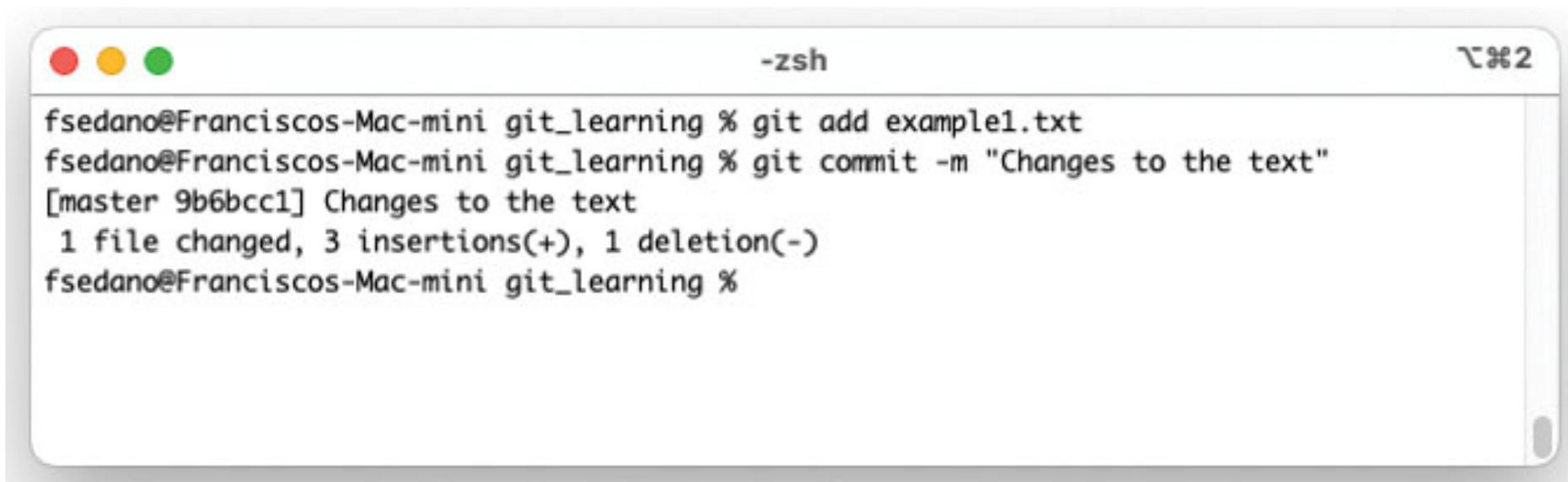
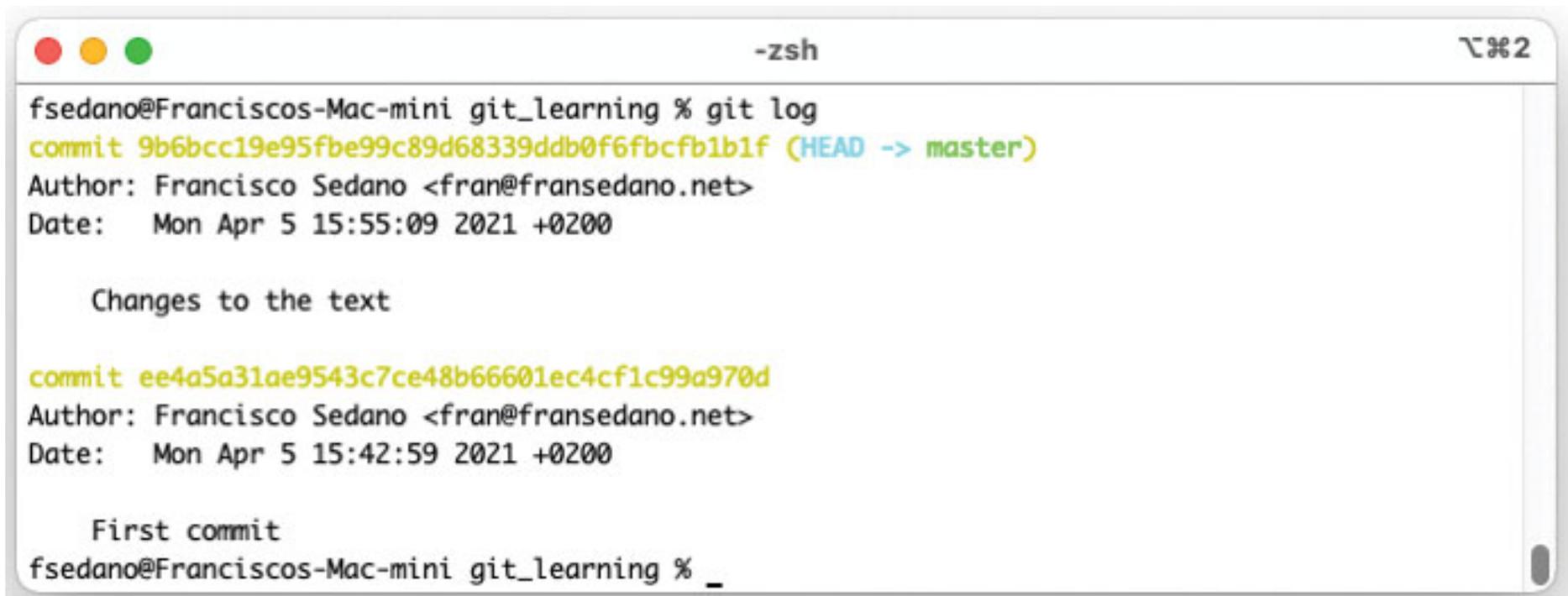


Figure A-12 Marks in Visual Studio Code

A terminal window titled "-zsh" with standard macOS window controls (red, yellow, green buttons) and a zoom icon in the top right corner. The terminal text shows a user named 'fsedano' on a 'Franciscos-Mac-mini' in a 'git_learning' directory. They execute 'git add example1.txt', followed by 'git commit -m "Changes to the text"'. The output shows the commit is successful on the 'master' branch with hash '9b6bcc1', and reports that 1 file changed with 3 insertions and 1 deletion.

```
fsedano@Franciscos-Mac-mini git_learning % git add example1.txt
fsedano@Franciscos-Mac-mini git_learning % git commit -m "Changes to the text"
[master 9b6bcc1] Changes to the text
1 file changed, 3 insertions(+), 1 deletion(-)
fsedano@Franciscos-Mac-mini git_learning %
```

Figure A-13 Committing changes

A terminal window titled "-zsh" with a window control bar (red, yellow, green buttons) and a zoom icon. The terminal shows the output of the "git log" command. The output lists two commits. The first commit is the most recent, with a yellow commit hash, a blue "(HEAD -> master)" label, and a description "Changes to the text". The second commit is older, with a yellow commit hash and a description "First commit". The prompt "fsedano@Franciscos-Mac-mini git_learning %" is visible at the top and bottom of the terminal.

```
fsedano@Franciscos-Mac-mini git_learning % git log
commit 9b6bcc19e95f9c89d68339ddb0f6fbcfb1b1f (HEAD -> master)
Author: Francisco Sedano <fran@fransedano.net>
Date:   Mon Apr 5 15:55:09 2021 +0200

    Changes to the text

commit ee4a5a31ae9543c7ce48b66601ec4cf1c99a970d
Author: Francisco Sedano <fran@fransedano.net>
Date:   Mon Apr 5 15:42:59 2021 +0200

    First commit
fsedano@Franciscos-Mac-mini git_learning % _
```

Figure A-14 Viewing commit history with git log

```
fsedano@Franciscos-Mac-mini git_learning % git show 9b6bcc19e95f9c89d68339ddb0f6fbcfb1b1f
commit 9b6bcc19e95f9c89d68339ddb0f6fbcfb1b1f (HEAD -> master)
Author: Francisco Sedano <fran@fransedano.net>
Date: Mon Apr 5 15:55:09 2021 +0200

    Changes to the text

diff --git a/example1.txt b/example1.txt
index 8243c31..393ffb0 100644
--- a/example1.txt
+++ b/example1.txt
@@ -1,2 +1,4 @@
-This is an example of a text. It is actually the first version of my text.
+This is an example of a text. It was actually the first version of my text.
 I'm typing something more here
+
+This is another line I've added now.
fsedano@Franciscos-Mac-mini git_learning %
fsedano@Franciscos-Mac-mini git_learning %
```

Figure A-15 Displaying changes in a commit using the command line

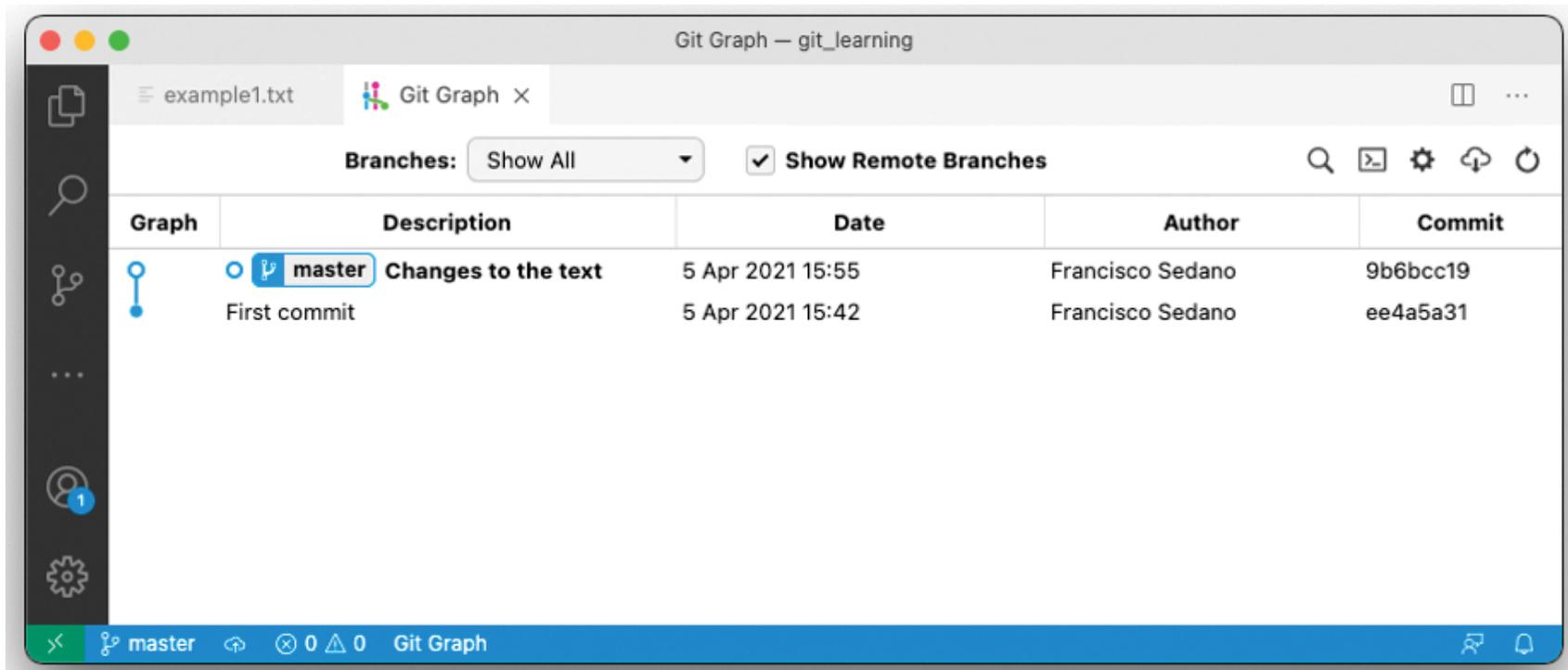


Figure A-16 Displaying commits using Visual Studio Code

The image shows the GitHub account settings page for Francisco Sedano. The left sidebar contains a list of settings: Account settings, Profile, Account, Appearance (marked as 'New'), Account security, Billing & plans, Security log, Security & analysis, Emails, Notifications, SSH and GPG keys, Repositories, Packages, Codespaces, Organizations, Saved replies, and Applications. A grey arrow points from the text 'Add your SSH key here' to the 'SSH and GPG keys' option. The main content area is titled 'Public profile' and includes fields for Name (Francisco Sedano), Public email (fran@fransedano.net), Bio (Tell us a little bit about yourself), URL (www.fransedano.net), Twitter username, and Company (cisco). A profile picture of Francisco Sedano is also visible.

Figure A-17 Adding SSH keys to GitHub

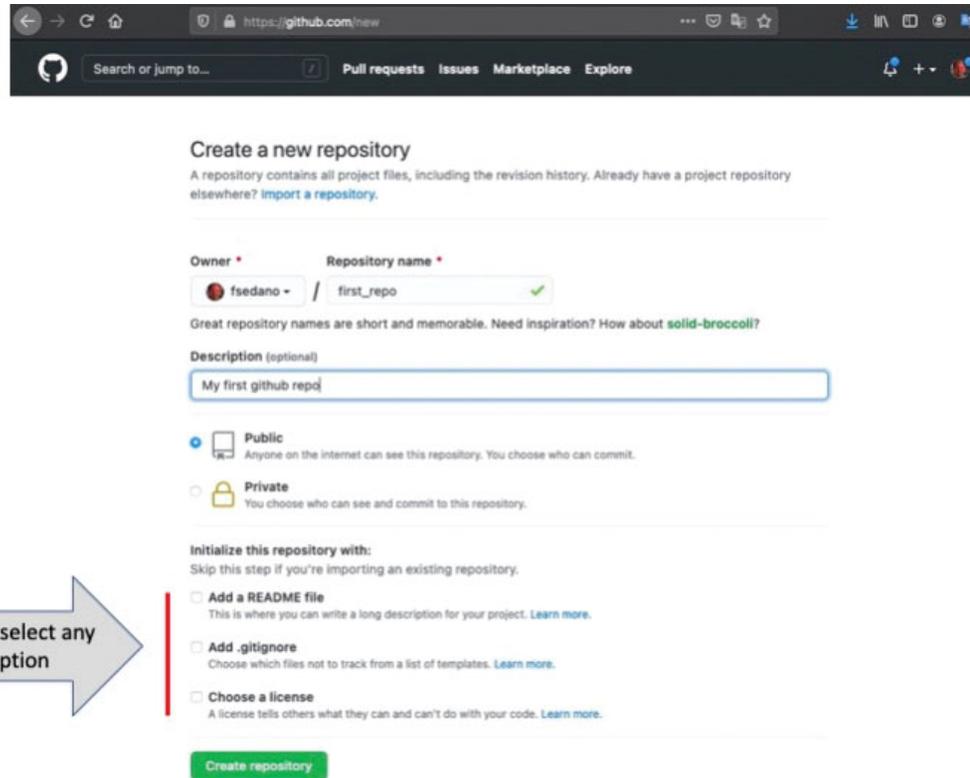


Figure A-18 Creating a new repository in GitHub

fsedano / first_repo

Unwatch 1 Star 0

Code Issues Pull requests Actions Projects Wiki Security Insights Settings

Quick setup — if you've done this kind of thing before

Set up in Desktop or **HTTPS** SSH git@github.com:fsedano/first_repo.git

Get started by [creating a new file](#) or [uploading an existing file](#). We recommend every repository include a [README](#), [LICENSE](#), and [.gitignore](#).

...or create a new repository on the command line

```
echo "# first_repo" >> README.md
git init
git add README.md
git commit -m "first commit"
git branch -M master
git remote add origin git@github.com:fsedano/first_repo.git
git push -u origin master
```

...or push an existing repository from the command line

```
git remote add origin git@github.com:fsedano/first_repo.git
git branch -M master
git push -u origin master
```

...or import code from another repository

You can initialize this repository with code from a Subversion, Mercurial, or TFS project.

Import code

ProTip! Use the URL for this page when adding GitHub as a remote.

Figure A-19 New repository in GitHub

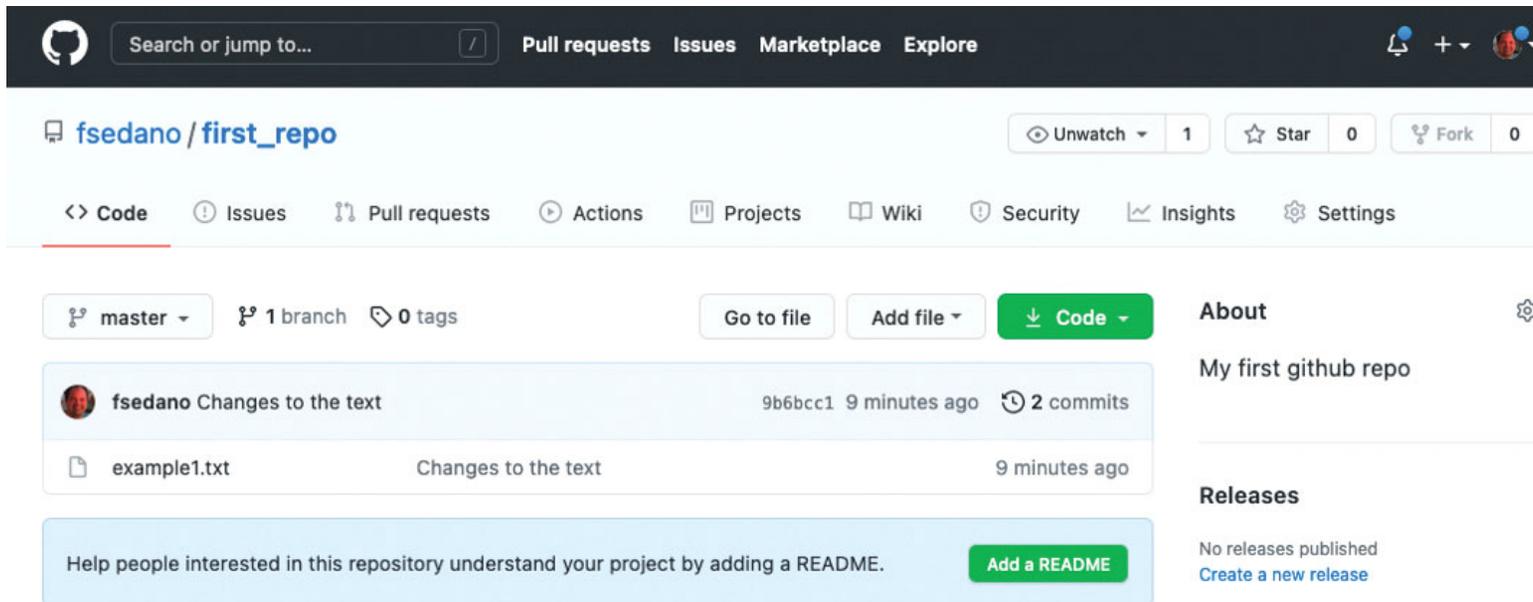


Figure A-20 Repository after the first commit

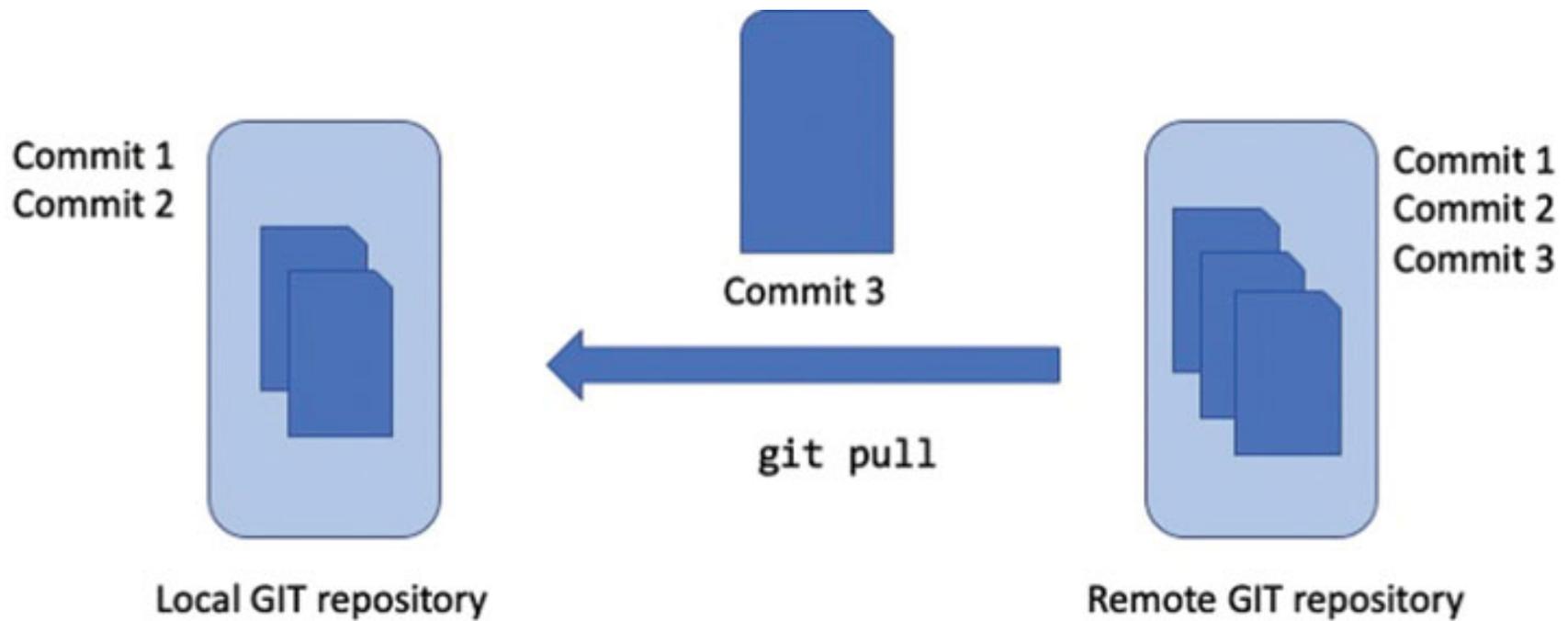


Figure A-21 Pulling from remote repositories

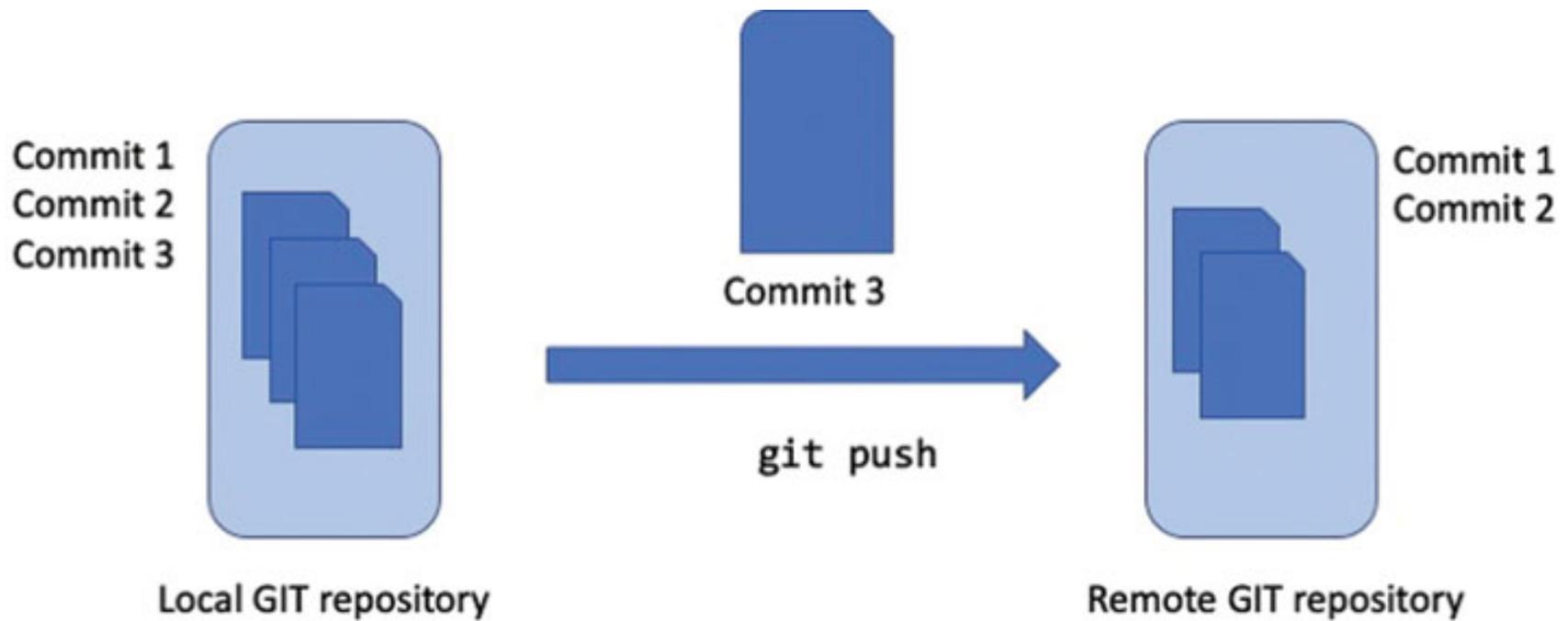
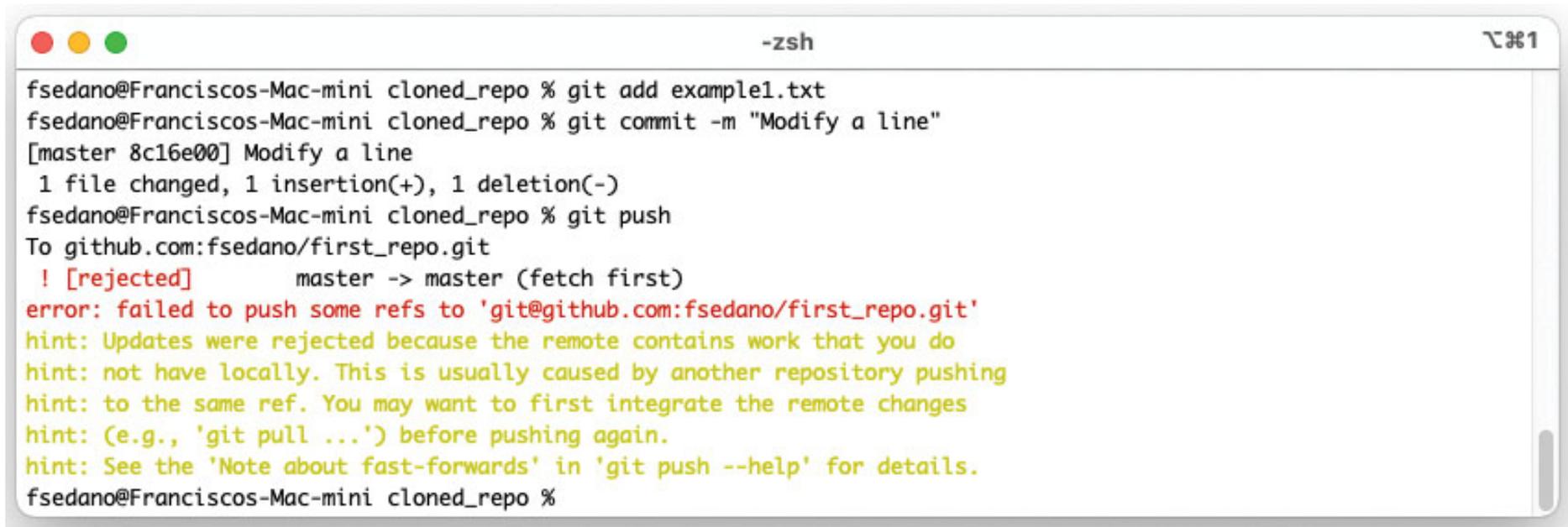
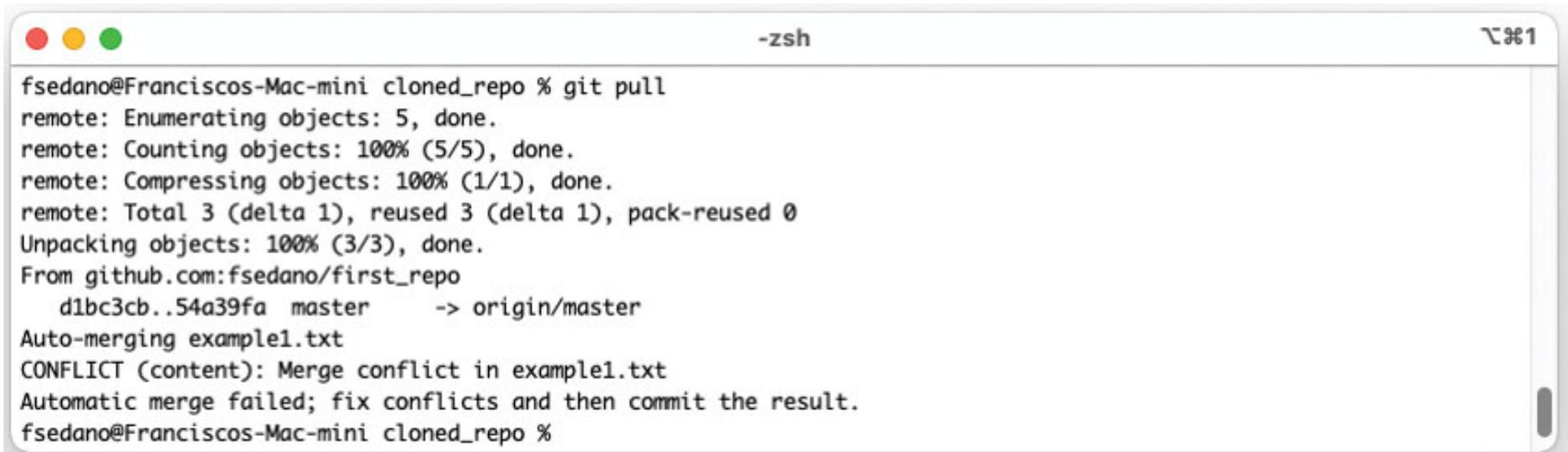


Figure A-22 Pushing to remote repositories

A terminal window titled "-zsh" with a window control bar (red, yellow, green buttons) and a zoom icon. The terminal shows a user named "fsedano" on a "Franciscos-Mac-mini" in a "cloned_repo" directory. They run "git add example1.txt", "git commit -m 'Modify a line'", and "git push". The push fails with a "rejected" error because the remote repository has newer changes. The error message is: "error: failed to push some refs to 'git@github.com:fsedano/first_repo.git'". A yellow hint explains: "Updates were rejected because the remote contains work that you do not have locally. This is usually caused by another repository pushing to the same ref. You may want to first integrate the remote changes (e.g., 'git pull ...') before pushing again. See the 'Note about fast-forwards' in 'git push --help' for details." The prompt returns to "fsedano@Franciscos-Mac-mini cloned_repo %".

```
fsedano@Franciscos-Mac-mini cloned_repo % git add example1.txt
fsedano@Franciscos-Mac-mini cloned_repo % git commit -m "Modify a line"
[master 8c16e00] Modify a line
 1 file changed, 1 insertion(+), 1 deletion(-)
fsedano@Franciscos-Mac-mini cloned_repo % git push
To github.com:fsedano/first_repo.git
 ! [rejected]        master -> master (fetch first)
error: failed to push some refs to 'git@github.com:fsedano/first_repo.git'
hint: Updates were rejected because the remote contains work that you do
hint: not have locally. This is usually caused by another repository pushing
hint: to the same ref. You may want to first integrate the remote changes
hint: (e.g., 'git pull ...') before pushing again.
hint: See the 'Note about fast-forwards' in 'git push --help' for details.
fsedano@Franciscos-Mac-mini cloned_repo %
```

Figure A-23 Git message if the local repository lags behind a remote one

A terminal window titled "-zsh" with a window control bar (red, yellow, green buttons) and a zoom icon. The terminal output shows a successful git pull from a remote repository, but it fails at the merge stage due to a conflict in the file "example1.txt". The conflict message is "CONFLICT (content): Merge conflict in example1.txt" and the instruction is "Automatic merge failed; fix conflicts and then commit the result." The prompt returns to "fsedano@Franciscos-Mac-mini cloned_repo %".

```
fsedano@Franciscos-Mac-mini cloned_repo % git pull
remote: Enumerating objects: 5, done.
remote: Counting objects: 100% (5/5), done.
remote: Compressing objects: 100% (1/1), done.
remote: Total 3 (delta 1), reused 3 (delta 1), pack-reused 0
Unpacking objects: 100% (3/3), done.
From github.com:fsedano/first_repo
   d1bc3cb..54a39fa master    -> origin/master
Auto-merging example1.txt
CONFLICT (content): Merge conflict in example1.txt
Automatic merge failed; fix conflicts and then commit the result.
fsedano@Franciscos-Mac-mini cloned_repo %
```

Figure A-24 Git conflicts

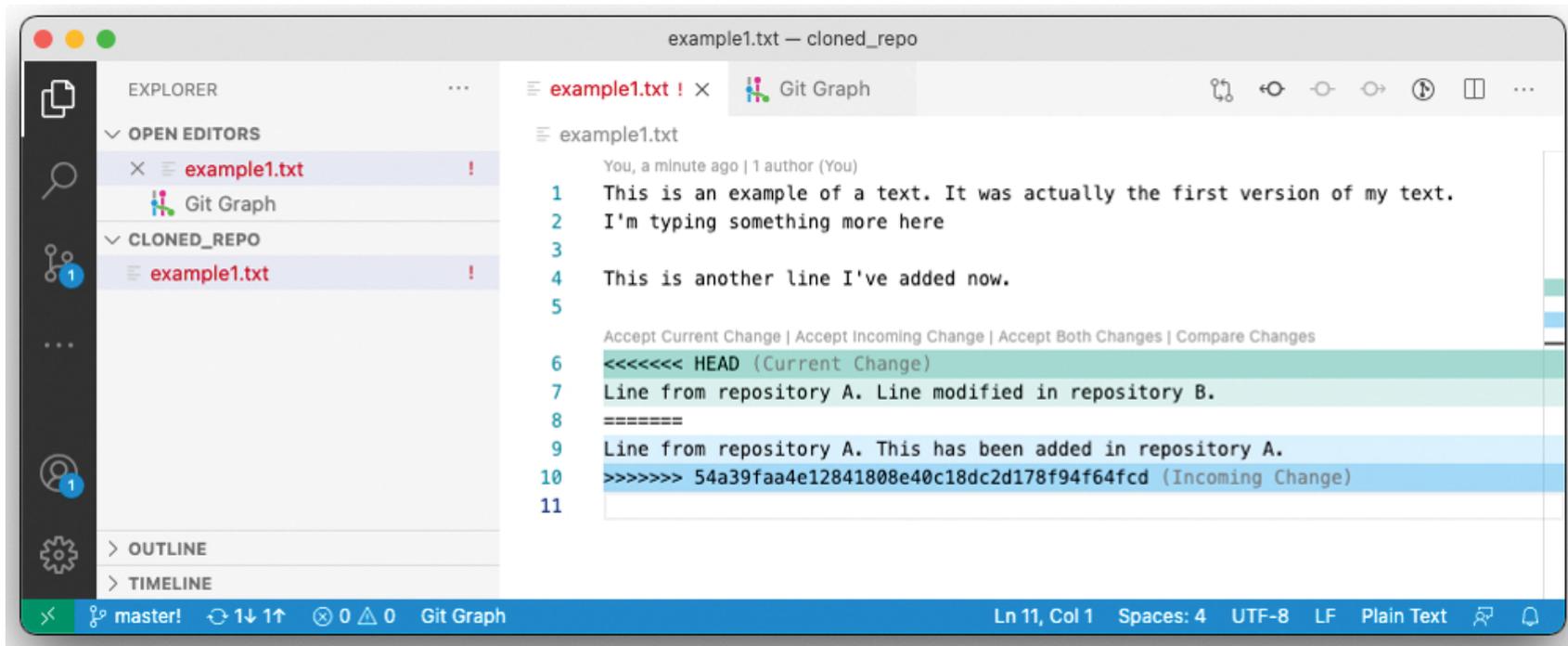
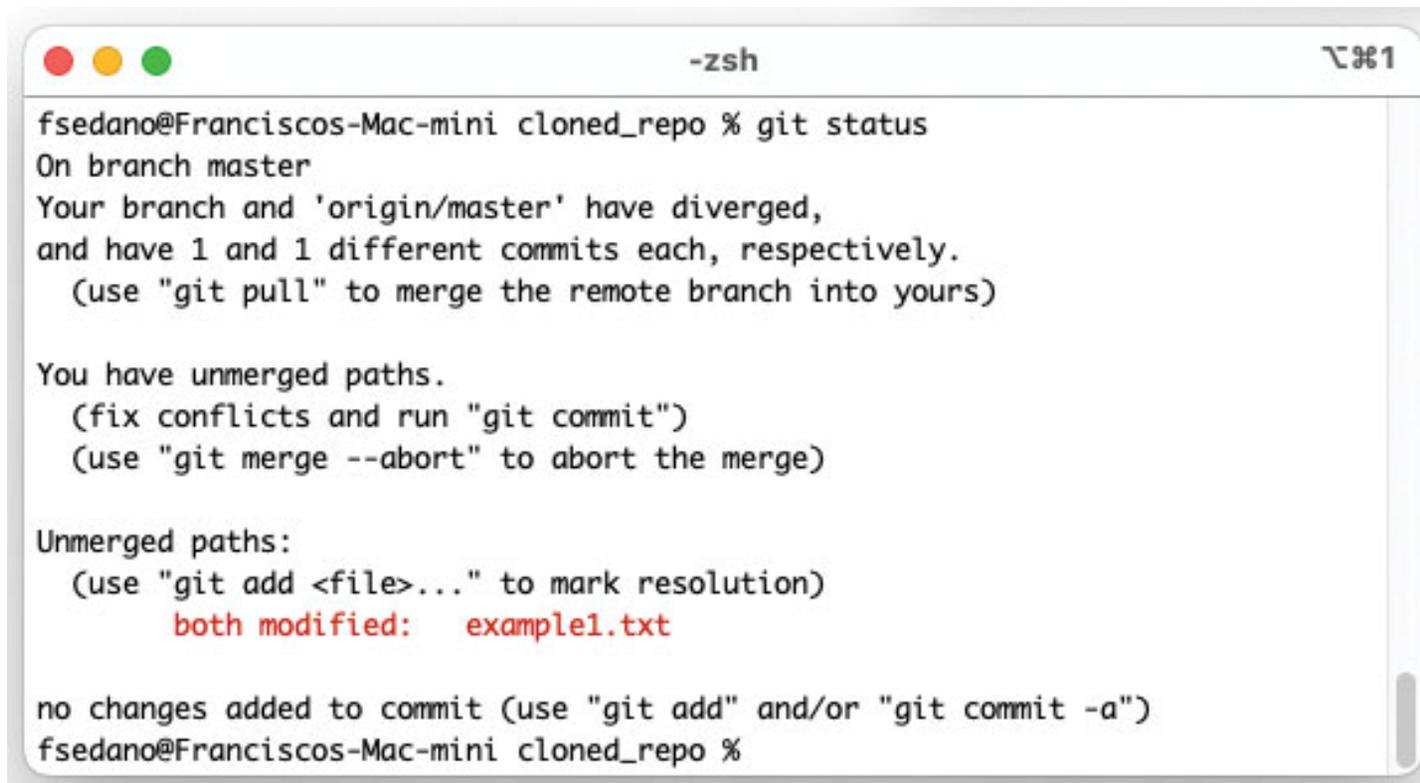


Figure A-25 Solving Git conflicts



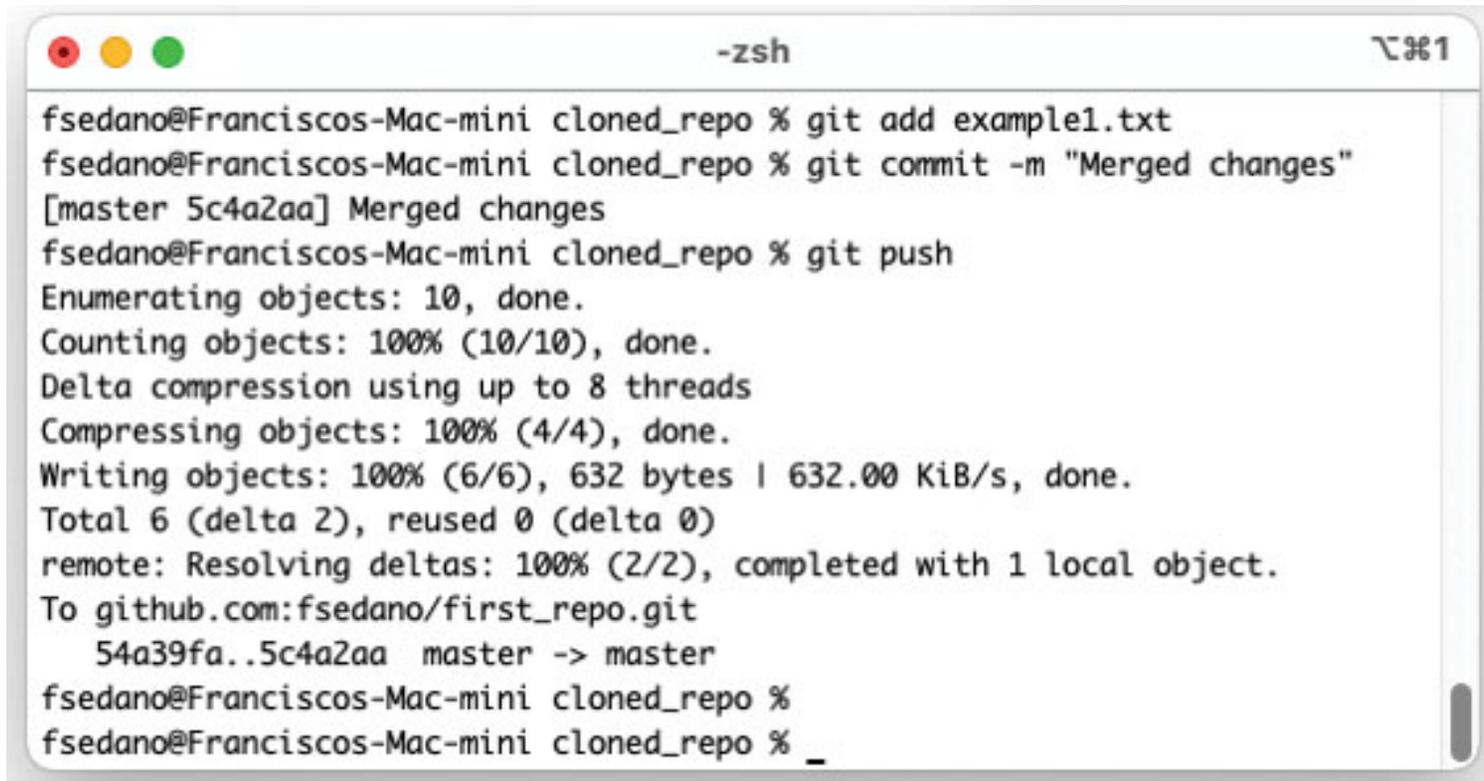
```
fshedano@Franciscos-Mac-mini cloned_repo % git status
On branch master
Your branch and 'origin/master' have diverged,
and have 1 and 1 different commits each, respectively.
  (use "git pull" to merge the remote branch into yours)

You have unmerged paths.
  (fix conflicts and run "git commit")
  (use "git merge --abort" to abort the merge)

Unmerged paths:
  (use "git add <file>..." to mark resolution)
    both modified:   example1.txt

no changes added to commit (use "git add" and/or "git commit -a")
fshedano@Franciscos-Mac-mini cloned_repo %
```

Figure A-26 Solving Git conflicts

A terminal window titled "-zsh" with a window control bar (red, yellow, green buttons) and a zoom icon. The terminal shows the following commands and output:

```
fshedano@Franciscos-Mac-mini cloned_repo % git add example1.txt
fshedano@Franciscos-Mac-mini cloned_repo % git commit -m "Merged changes"
[master 5c4a2aa] Merged changes
fshedano@Franciscos-Mac-mini cloned_repo % git push
Enumerating objects: 10, done.
Counting objects: 100% (10/10), done.
Delta compression using up to 8 threads
Compressing objects: 100% (4/4), done.
Writing objects: 100% (6/6), 632 bytes | 632.00 KiB/s, done.
Total 6 (delta 2), reused 0 (delta 0)
remote: Resolving deltas: 100% (2/2), completed with 1 local object.
To github.com:fshedano/first_repo.git
   54a39fa..5c4a2aa  master -> master
fshedano@Franciscos-Mac-mini cloned_repo %
fshedano@Franciscos-Mac-mini cloned_repo % _
```

Figure A-27 Git conflict solved

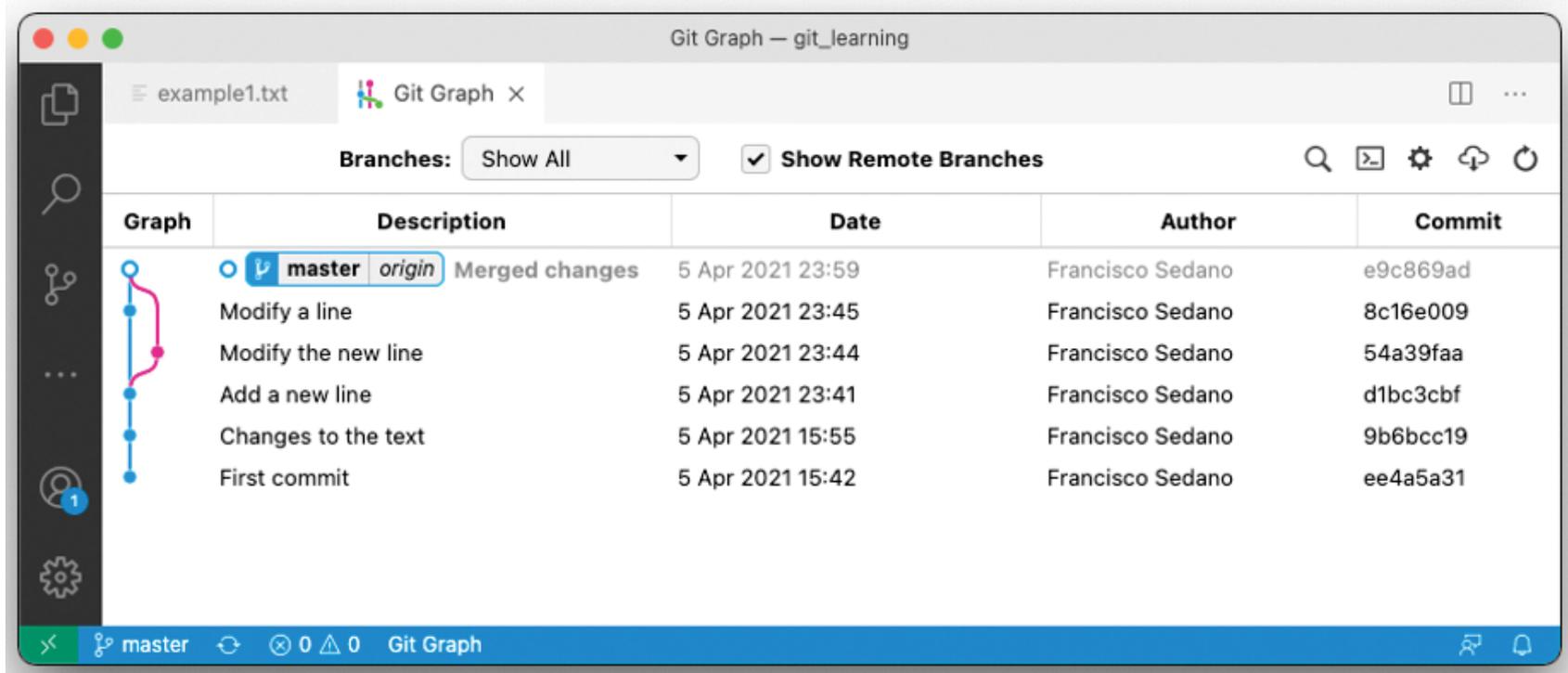


Figure A-28 Git history flow

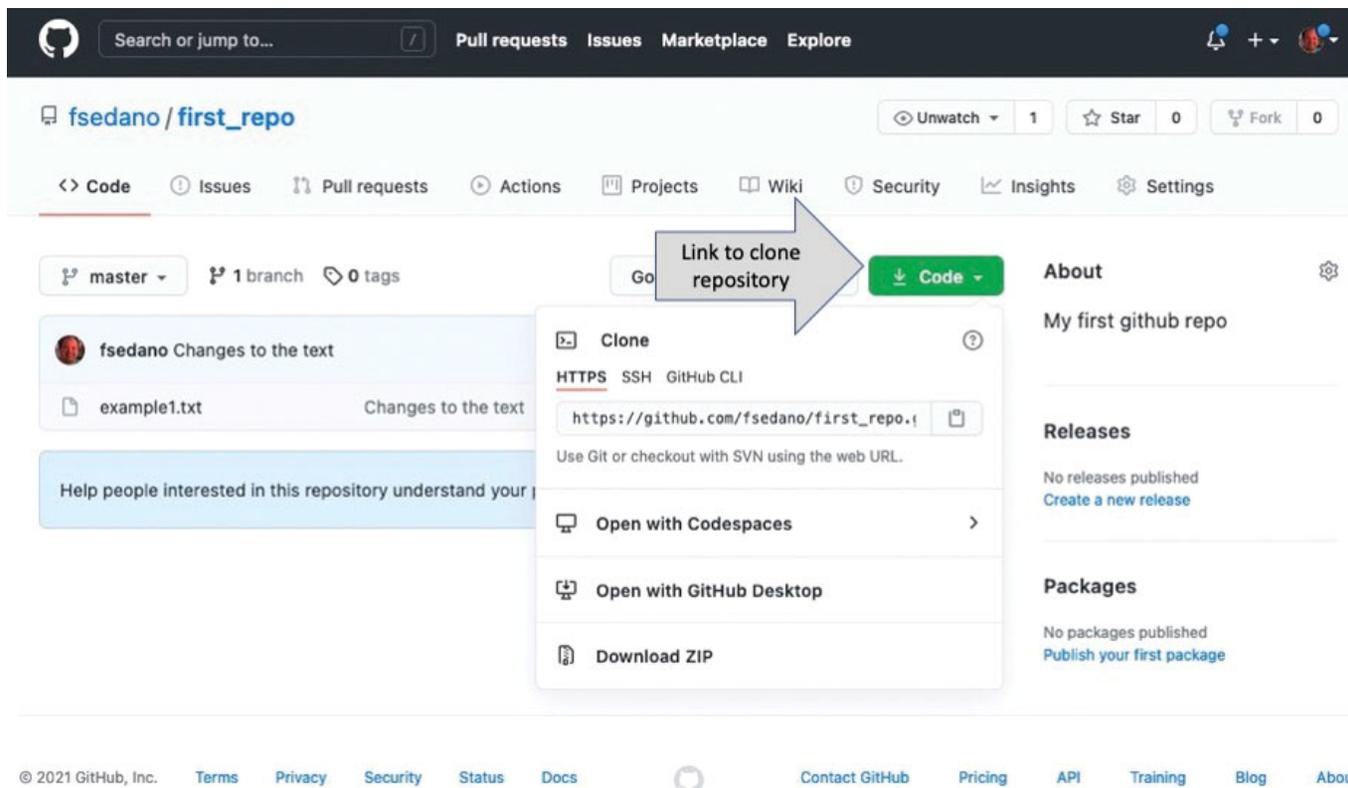


Figure A-29 Sharing repositories using GitHub

Create a new repository

A repository contains all project files, including the revision history. Already have a project repository elsewhere? [Import a repository](#).

Repository template

Start your repository with a template repository's contents.

No template ▾

Owner ▾

 fsedano ▾

Repository name ▾

new_repo ✓

Great repository names are short and memorable. Need inspiration? How about [super-fiesta?](#)

Description (optional)



Public

Anyone on the Internet can see this repository. You choose who can commit.



Private

You choose who can see and commit to this repository.

Visibility options

Figure A-30 Cloning Git repositories

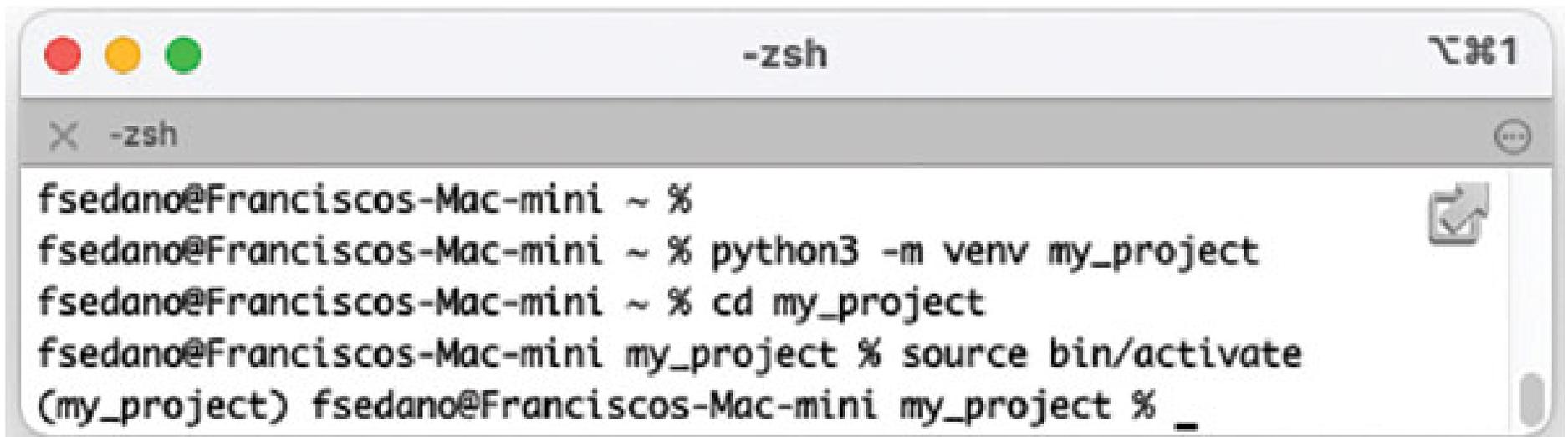
```
fsedano@Franciscos-Mac-mini ~ % git clone https://github.com/fsedano/first_repo.git
Cloning into 'first_repo'...
remote: Enumerating objects: 6, done.
remote: Counting objects: 100% (6/6), done.
remote: Compressing objects: 100% (4/4), done.
remote: Total 6 (delta 0), reused 6 (delta 0), pack-reused 0
Unpacking objects: 100% (6/6), done.
fsedano@Franciscos-Mac-mini ~ % cd first_repo
fsedano@Franciscos-Mac-mini first_repo % ls
example1.txt
fsedano@Franciscos-Mac-mini first_repo % git log
commit 9b6bcc19e95f9c89d68339ddb0f6fbcfb1bf (HEAD -> master, origin/master, origin/HEAD)
Author: Francisco Sedano <fran@fransedano.net>
Date: Mon Apr 5 15:55:09 2021 +0200

    Changes to the text

commit ee4a5a31ae9543c7ce48b66601ec4cf1c99a970d
Author: Francisco Sedano <fran@fransedano.net>
Date: Mon Apr 5 15:42:59 2021 +0200

    First commit
fsedano@Franciscos-Mac-mini first_repo %
```

Figure A-31 Choosing repository visibility at creation time

A screenshot of a macOS terminal window titled "-zsh". The window shows a series of commands being executed to create a Python virtual environment. The prompt changes from the user's home directory to the "my_project" directory, and the prompt itself changes to "(my_project)".

```
fshedano@Franciscos-Mac-mini ~ %  
fshedano@Franciscos-Mac-mini ~ % python3 -m venv my_project  
fshedano@Franciscos-Mac-mini ~ % cd my_project  
fshedano@Franciscos-Mac-mini my_project % source bin/activate  
(my_project) fshedano@Franciscos-Mac-mini my_project % _
```

Figure A-32 Creating a Python virtual environment

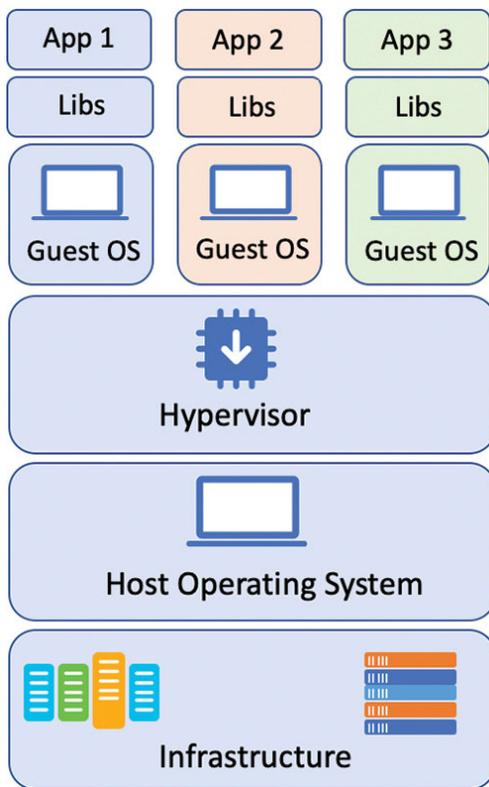


Figure A-33 Hypervisor architecture

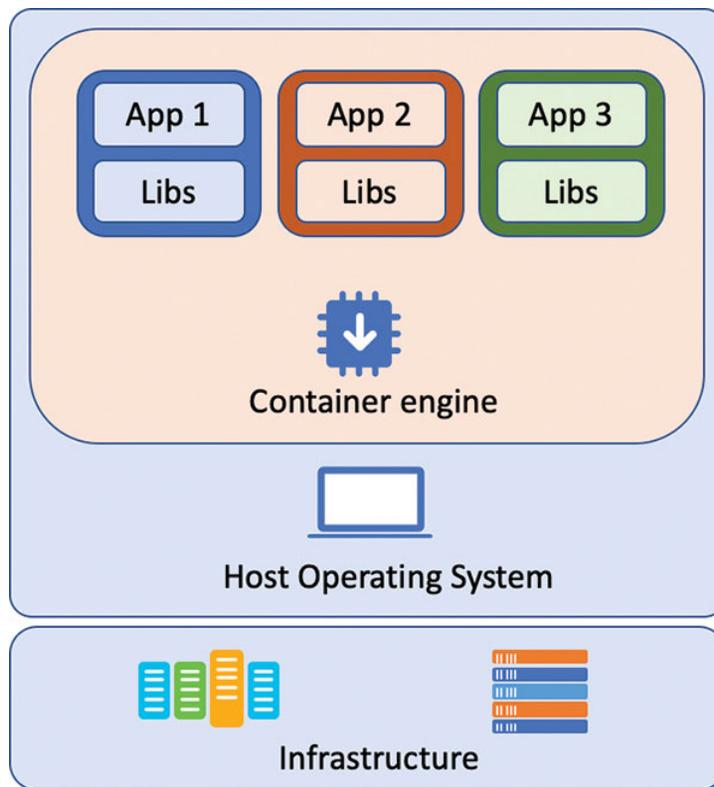


Figure A-34 Container architecture

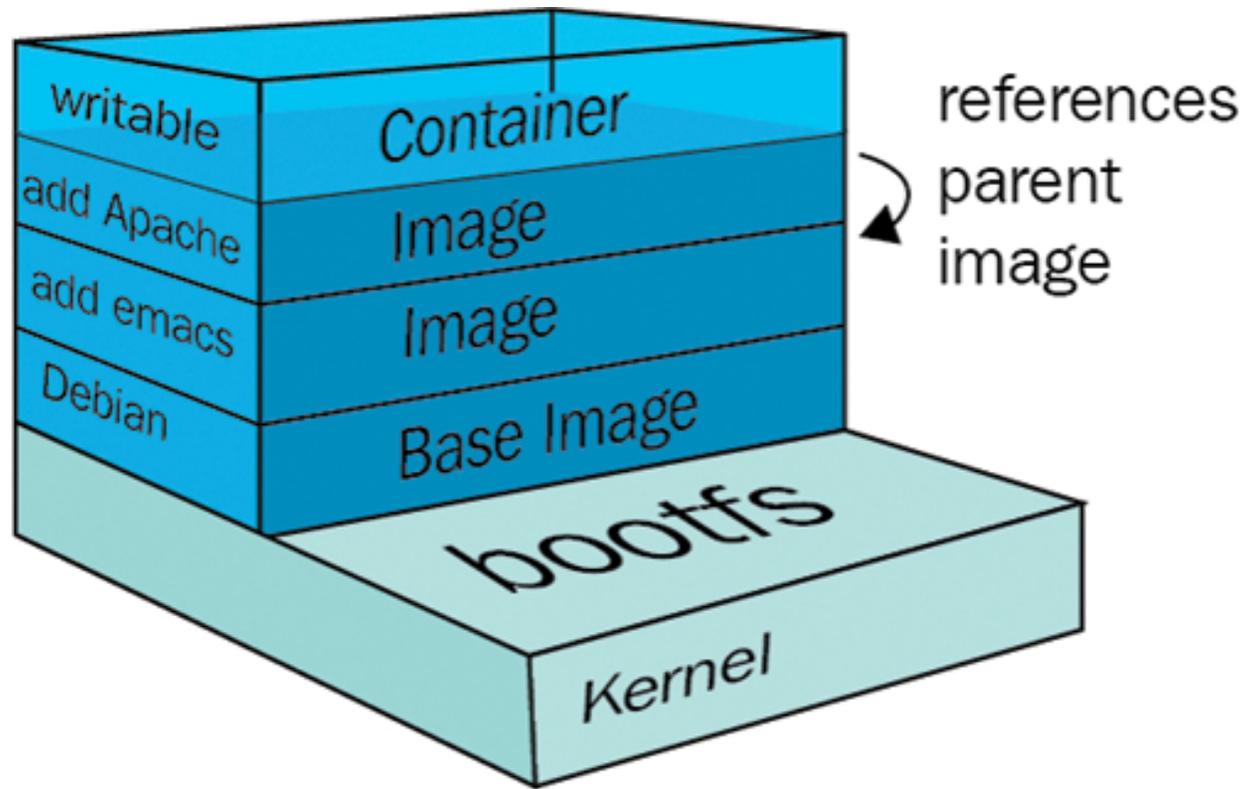


Figure A-35 Layers in a container image

```
apt-get update && apt-get install -y python3
2bec8cbaddb0
Base layer: Ubuntu:18.04
1715a469e5df
```

```
RUN apt-get update && apt-get install -y python3
FROM ubuntu:18.04
```

Figure A-36 Layers created by a Dockerfile

```
root@53a12151910e: /app

fsedano@Franciscos-Mac-mini book-docker %
fsedano@Franciscos-Mac-mini book-docker % docker-compose up -d
Docker Compose is now in the Docker CLI, try `docker compose up`

Creating network "book-docker_default" with the default driver
Creating book-docker_adminer_1 ... done
Creating book-docker_app_1_1 ... done
Creating book-docker_db_1 ... done
█

fsedano@Franciscos-Mac-mini book-docker % docker-compose ps
      Name                                Command                                State                Ports
-----
book-docker_adminer_1  entrypoint.sh docker-php-e ...      Up                   0.0.0.0:9000->8080/tcp
book-docker_app_1_1    /bin/bash                               Exit 0
book-docker_db_1       docker-entrypoint.sh mysqld           Up                   3306/tcp
fsedano@Franciscos-Mac-mini book-docker % _
```

Figure A-37 Checking container status by using docker-compose