CISCO IOS-XE Wireless EFT User Manual

Contents [hide

IOS-XE Wireless EFT

Product Information: IOS-XE 17.11.1 Wireless EFT Guide

The Cisco Enterprise Wireless solutions are designed to provide resilient and secure wireless networking with adaptive and insightful intelligence. The solutions are built on Cisco Digital Network Architecture, making them ready for the growing user expectations, IoT devices, and cloud-driven applications. The Cisco Catalyst 9800 Series Wireless Controllers based on IOS-XE were introduced in 2018 and have since undergone constant innovation, new platform introductions, feature enhancements, and feature parity additions, making them the best in enterprise-class in the market.

Compatibility Matrix

The compatibility matrix for IOS-XE 17.11.1 Wireless EFT Guide is available in the user manual.

Features to Test

The features to test include:

- Efficient AP image download through TCP

Providing Feedback and Requesting Support

If you encounter any issues or have additional comments or feedback during the EFT program, you can provide your feedback to the TME team. If you find issues or have additional comments or feedback after the EFT program concludes, you can still provide your feedback to the TME team.

Product Usage Instructions: IOS-XE 17.11.1 Wireless EFT Guide

Network Topology

The network topology depends on your specific setup and requirements. Refer to the user manual for more information.

Pre-Requisites

Test Setup

Before conducting the tests, ensure that you have:

- Cisco Catalyst 9800 Series Wireless Controllers

- Cisco Catalyst 9100 Access Points
- Test devices

Upgrade Paths

The upgrade paths are available in the user manual.

Efficient AP Image Download through TCP Feature Overview

Feature Description

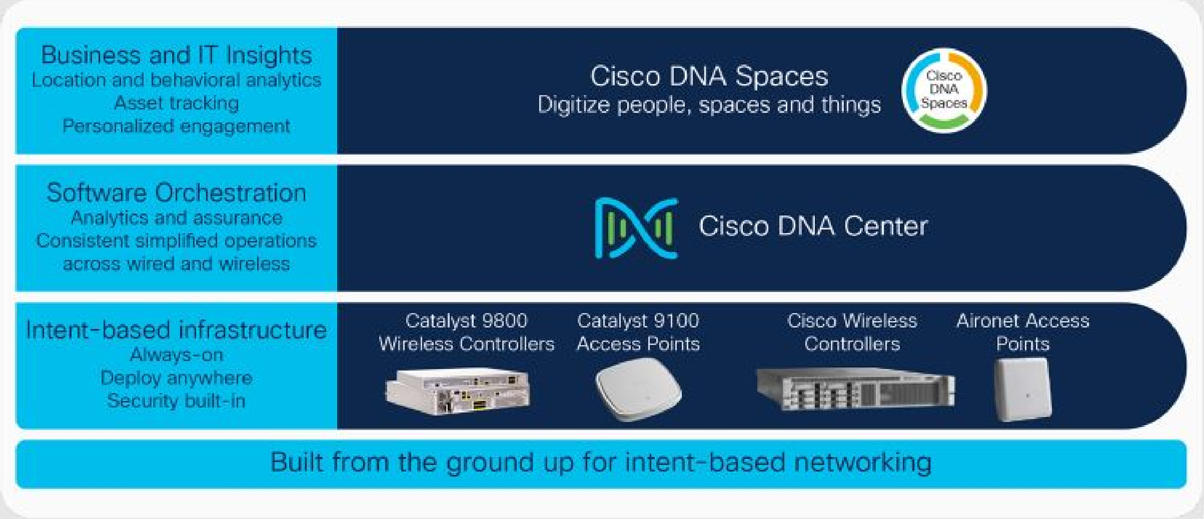
The efficient AP image download through TCP feature allows for faster and more reliable AP image downloads through the use of TCP.

Feature Usage

To use the efficient AP image download through TCP feature, follow the instructions in the user manual.

Introduction

Cisco Enterprise Wireless solutions are resilient, have integrated security, and employ adaptive and insightful intelligence providing useful insight into your network. With intent-based networking built on Cisco Digital Network Architecture, Cisco Enterprise Wireless solutions go beyond the latest Wi-Fi 6 and WiFi 6E (802.11ax) standards and are ready for the growing user expectations, IoT devices, and next-gen cloud-driven applications.


Business and IT Insights
Location and behavioral analytics
Asset tracking
Personalized engagement
Cisco DNA Spaces
Digitize people, spaces and things
Cisco DNA Spaces
Software Orchestration
Analytics and assurance
Consistent simplified operations across wired and wireless
Cisco DNA Center
Intent-based infrastructure
Always-on
Deploy anywhere
Security built-in
Catalyst 9800 Wireless Controllers
Catalyst 9100 Access Points
Cisco Wireless Controllers
Aironet Access Points
Built from the ground up for intent-based networking

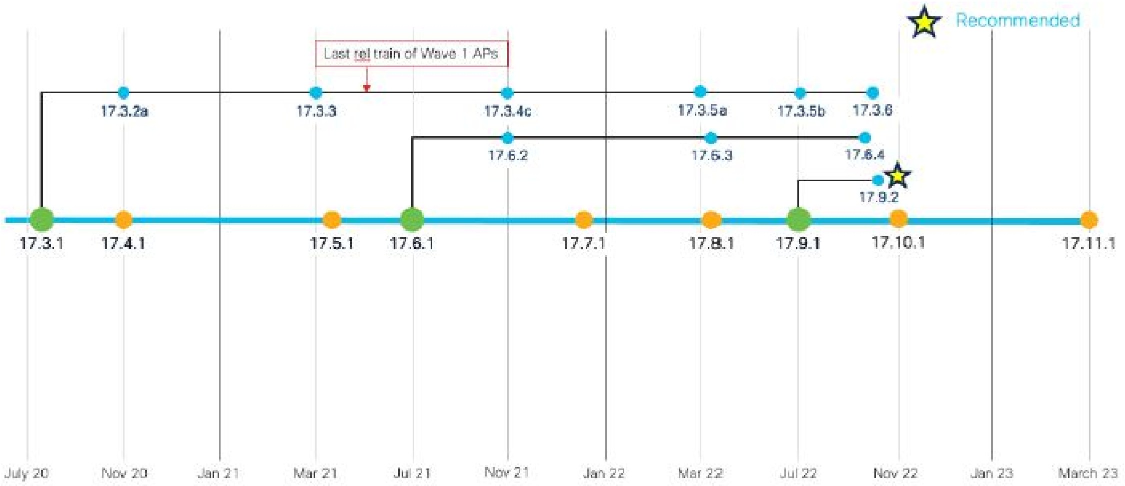
IOS-XE 17.11.1 Wireless EFT Guide

Cisco Catalyst 9800 Series Wireless Controllers: The Catalyst controllers streamline the best of RF excellence with open, programmable Cisco IOS® XE benefits, meaning you no longer have two operating systems to manage. These modular, reliable, and highly secure controllers are flexible enough to deploy anywhere– including your choice of cloud.

Cisco Catalyst® 9100 Access Points: Going beyond the Wi-Fi 6 and 6E standard, the Cisco Catalyst 9100 access points provide integrated security, resiliency, and operational flexibility, as well as increased network intelligence. These access points extend Cisco's intent-based network and scale to the growing demands of the Internet of Things (IoT) while fully supporting the latest innovations and newest technologies, making them perfect for organizations of all sizes.

To get a complete overview and learn more about Cisco Enterprise Wireless Products and Solutions, please visit the following page: https://www.cisco.com/c/en/us/products/wireless/index.html – ~resources

Cisco Catalyst 9800 Series Wireless Controllers based on IOS-XE was introduced to the market in the end of 2018 with IOS-XE Release 16.10.1. There have been constant innovations, new platform introductions, feature enhancements, and feature parity additions over the last couple of years to make Cisco Catalyst 9800 Series Wireless Controllers and Cisco Catalyst 9100 Access Points, the best in enterprise-class in the market.



This document provides a feature overview, configuration, and test scenarios for a few selected wireless features based on customer interest, for an early field trial of IOS-XE Release 17.11.1. We are pleased to welcome you to the EFT for the IOS-XE Wireless Software Release 17.11.1. Cisco recognizes and appreciates the time and effort that will be evaluating the features in this software release and hopes that you will find it meets your expectations. This software and accompanying documentation are being provided to you under the non-disclosure agreement between you, your organization, and Cisco. Please do not discuss this project and its features outside of the discussions on Cisco Beta-related mailing lists. This software is pre-release software and as such should never be used in a commercial operating environment or with mission-critical data. We recommend that you install this software on a test network/system initially and then move to production testing as you are more comfortable with it. Please use the software as you would normally in your day-to-day tasks and report any problems that you find.

Providing Feedback and requesting support

Details on providing feedback are given below. Also, note that throughout the project we may ask for feedback on specific areas of the software. Your feedback is vital to Cisco Systems in providing you with the features and utility that you require to realize your individual mission. This EFT represents an opportunity to see if this addresses your needs and to provide input regarding its suitability. The EFT program start dates and timelines have been communicated to you under a separate communication by the EFT administrator. During the EFT period, at least one EFT software refresh will be available during the EFT phase. In order to include as many fixes as possible in this refresh release; you and your staff are encouraged to test this software and provide feedback as early in the program as is possible. There will be a cut-off at which point we will freeze development in order to test and release the update image. The update will contain important fixes and all participants are recommended to upgrade once the EFT refresh software is available. If you find issues or have additional comments or feedback after the EFT program concludes we still, as always welcome your feedback!

For us to track found issues, provide comments, or ask questions you can submit your query to: polariswireless-beta@cisco.com

Catalyst 9800 IOS XE 17.11.1 Software EFT Images: The below location can be used to pull the latest EFT Images:

Catalyst 9800 platforms:

- **Catalyst 9800-CL Wireless Controller for Cloud –**
  https://software.cisco.com/download/beta/1572566934

- **Catalyst 9800-80 Wireless Controller –** https://software.cisco.com/download/beta/1536549615
- **Catalyst 9800-L Wireless Controller –** https://software.cisco.com/download/beta/1597144509
- **Catalyst 9800-40 Wireless Controller –** https://software.cisco.com/download/beta/1388071271

EWC (Embedded Wireless Controller on AP):

- **Catalyst 9130AXI Access Point –** https://software.cisco.com/download/beta/773616253
- **Catalyst 9120AXI Access Point –** https://software.cisco.com/download/beta/792652702
- **Catalyst 9117AXI Access Point –** https://software.cisco.com/download/beta/811480614
- **Catalyst 9115AXI Access Point –** https://software.cisco.com/download/beta/811599778

Again, thank you for your time an effort in helping Cisco to meet your needs. We value this relationship and look forward to your comments and continued support. Please do not hesitate to contact us if you have any questions now, or at any point during the EFT.
Wireless Features Targeted for EFT (Early Field Trial) in IOS-XE Release 17.11.1:

Simplicity:

- C9800 Jumbo Frame Support for Radius/AAA packets
- Enhancement in client steering during Rolling AP Upgrade
- Efficient AP image download through TCP
- Intelligently disable 2.4 GHz radios
- **Usability:** AAA CLI request
- RPC for Syslog Configuration

Security:

- Improvements to Built-in Captive Portal
- Multi Authentication Combination of 802.1x w/AAA Override (Dynamic Vlan Assignment) and LWA (consent) on C9800
- A location-Capable attribute in the Access-Request messages as part of RFC5580
- C9800 optimization of client exclusion time with WPA3 SAE

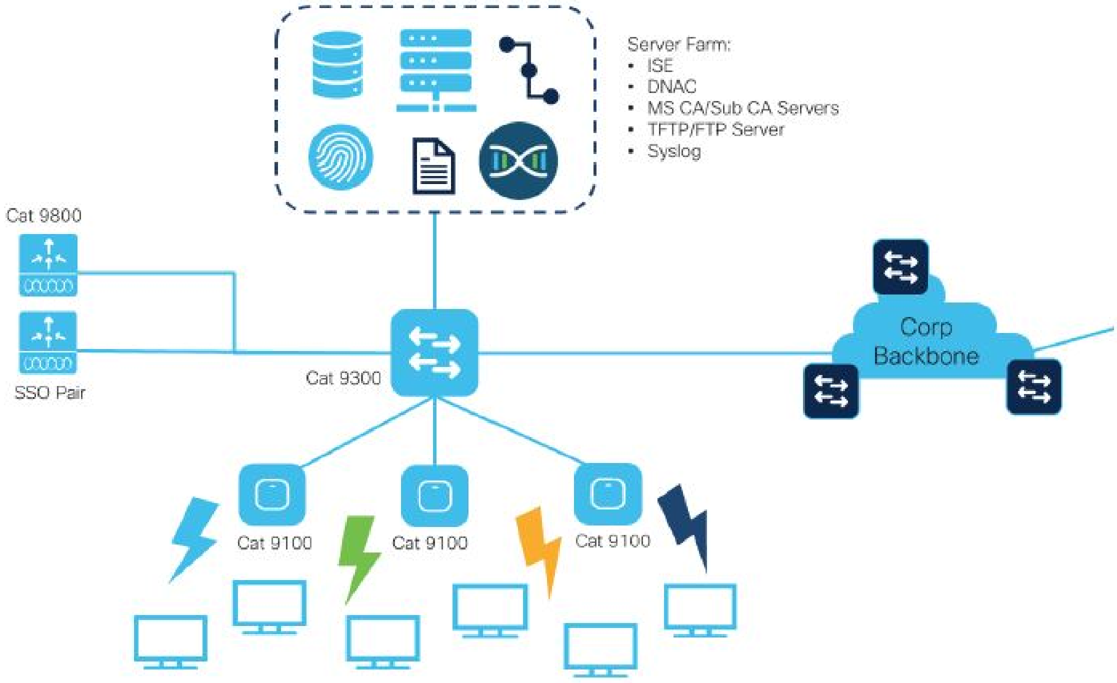
Connectivity:

- Mesh: Background Scanning
- Zero Wait DFS: Support on C9136

Sustainability:

- Unable to query OIDs from CISCO-LWAPP-AP-MIB on 9800- Migration halted
- SNMP OIDs – Phase 2

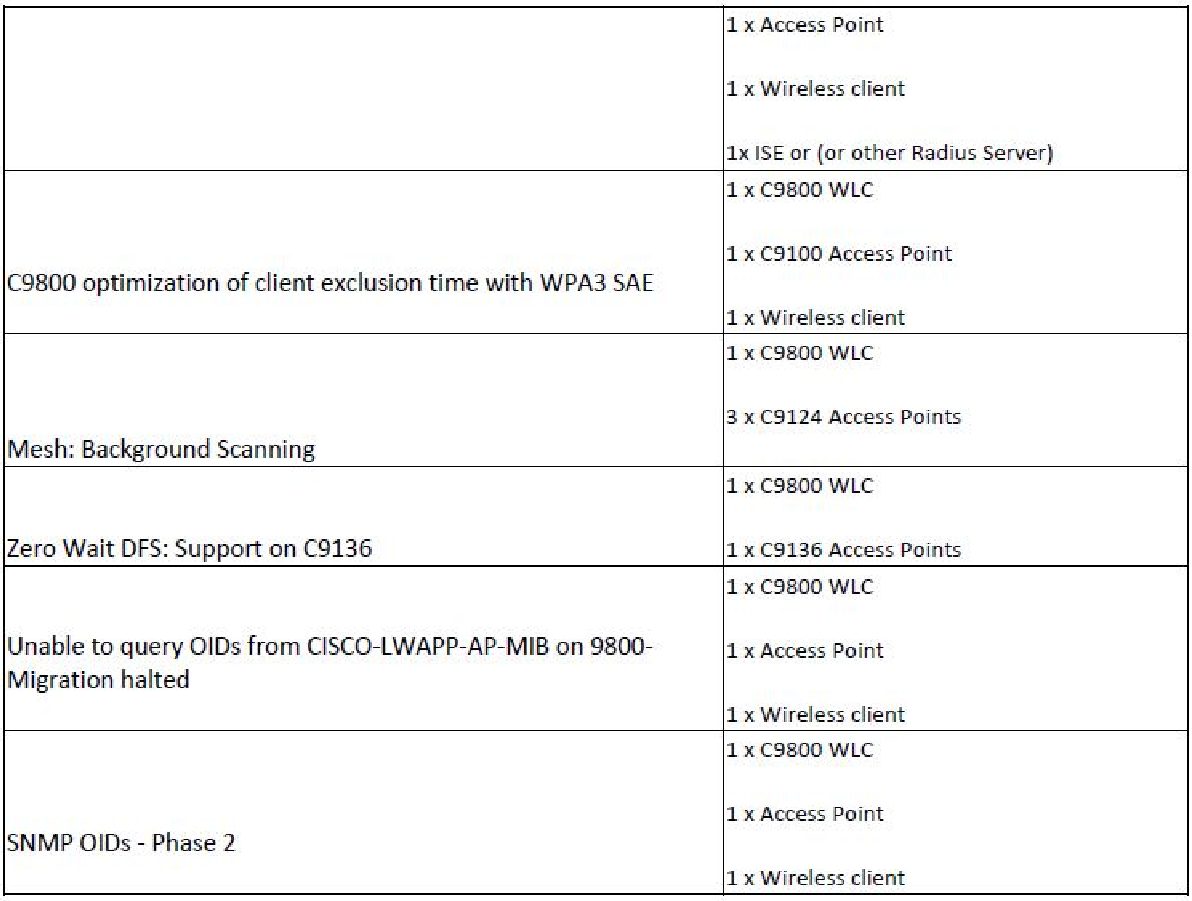
Network Topology



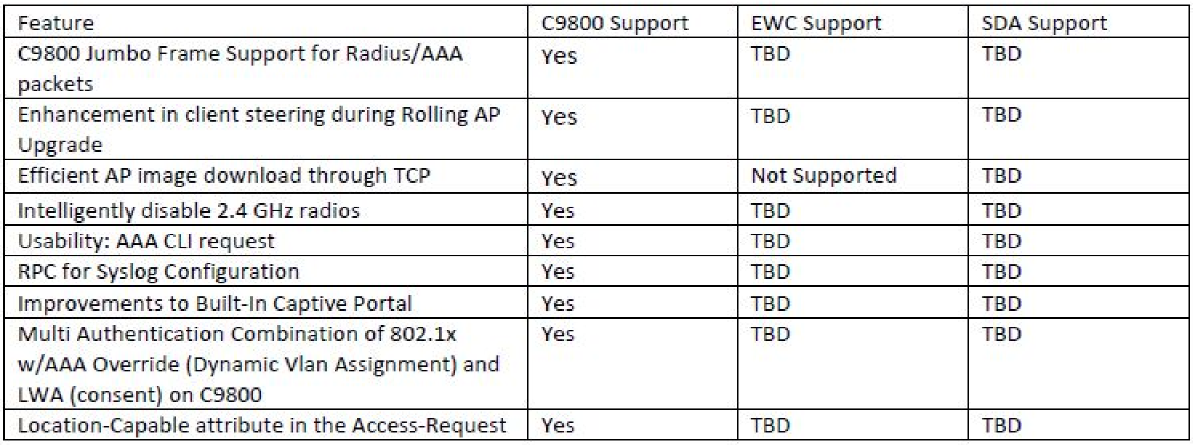
Pre-requisites

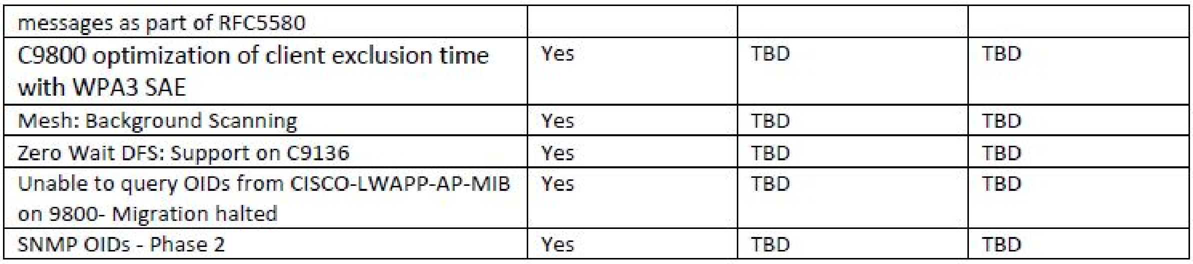
Test Setup

Feature	Mandatory Equipment
C9800 Jumbo Frame Support for Radius/AAA packets	1 x C9800-80 WLC 1 x ISE (or other Radius Server that supports the MTU) (1*Access Point and 1*client for verification on Auth traffic)
Enhancement in client steering during Rolling AP Upgrade	2 x C9800 WLC 3 x C9100 Access Point 1 x Wireless client
Efficient AP image download through TCP	1 x C9800 WLC 1 x Access Point
Intelligently disable 2.4 GHz radios	1 x C9800 WLC 1 x C9100 Access Point 1 x Wireless client
Usability: AAA CLI request	1 x C9800 WLC 1 x Access Point 1 x Wireless Client 1 x ISE (or other Radius Server)
RPC for Syslog Configuration	1 x C9800 WLC 1 x Syslog Server
Improvements to Built-In Captive Portal	1 x C9800 WLC 1 x Access Point 1 x Wireless client
Multi Authentication Combination of 802.1x w/AAA Override (Dynamic Vlan Assignment) and LWA (consent) on C9800	1 x C9800 WLC 1 x Access Point 1 x Wireless client
Location-Capable attribute in the Access-Request messages as part of RFC5580	1 x C9800 WLC



	1 x Access Point 1 x Wireless client 1x ISE or (or other Radius Server)
C9800 optimization of client exclusion time with WPA3 SAE	1 x C9800 WLC 1 x C9100 Access Point 1 x Wireless client
Mesh: Background Scanning	1 x C9800 WLC 3 x C9124 Access Points
Zero Wait DFS: Support on C9136	1 x C9800 WLC 1 x C9136 Access Points
Unable to query OIDs from CISCO-LWAPP-AP-MIB on 9800-Migration halted	1 x C9800 WLC 1 x Access Point 1 x Wireless client
SNMP OIDs - Phase 2	1 x C9800 WLC 1 x Access Point 1 x Wireless client





Feature	C9800 Support	EWC Support	SDA Support
C9800 Jumbo Frame Support for Radius/AAA packets	Yes	TBD	TBD
Enhancement in client steering during Rolling AP Upgrade	Yes	TBD	TBD
Efficient AP image download through TCP	Yes	Not Supported	TBD
Intelligently disable 2.4 GHz radios	Yes	TBD	TBD
Usability: AAA CLI request	Yes	TBD	TBD
RPC for Syslog Configuration	Yes	TBD	TBD
Improvements to Built-In Captive Portal	Yes	TBD	TBD
Multi Authentication Combination of 802.1x w/AAA Override (Dynamic Vlan Assignment) and LWA (consent) on C9800	Yes	TBD	TBD
Location-Capable attribute in the Access-Request messages as part of RFC5580	Yes	TBD	TBD
C9800 optimization of client exclusion time with WPA3 SAE	Yes	TBD	TBD
Mesh: Background Scanning	Yes	TBD	TBD
Zero Wait DFS: Support on C9136	Yes	TBD	TBD
Unable to query OIDs from CISCO-LWAPP-AP-MIB on 9800- Migration halted	Yes	TBD	TBD
SNMP OIDs - Phase 2	Yes	TBD	TBD

Upgrade Paths

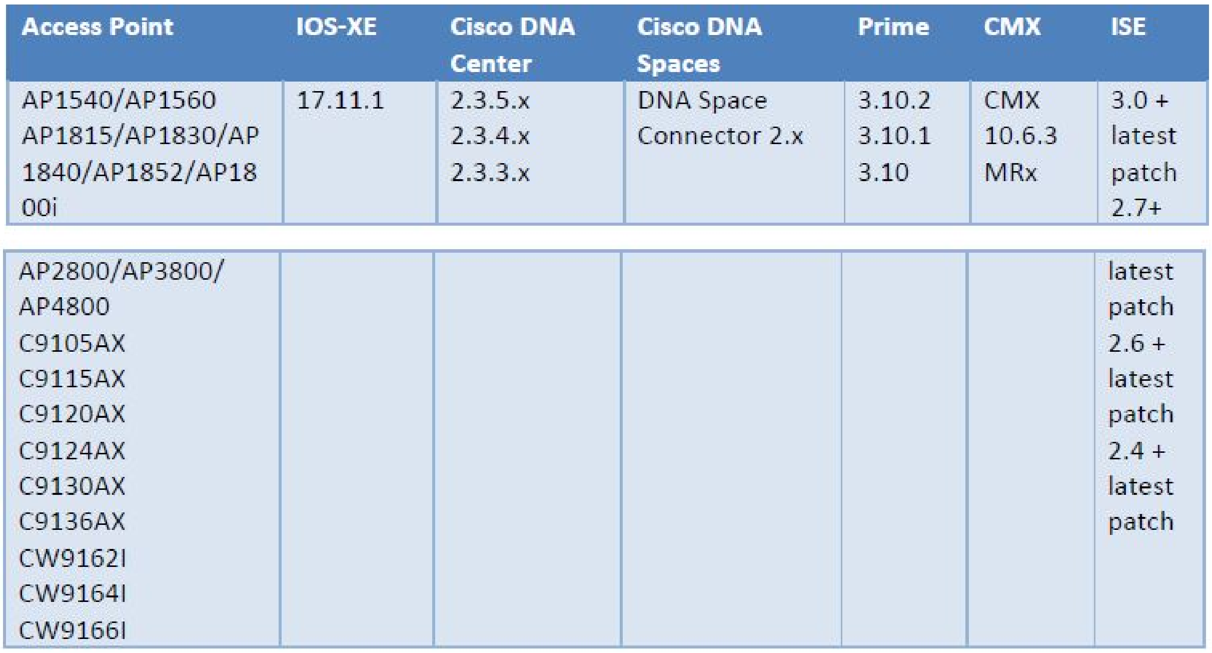
For the purpose of this EFT program, Cisco recommends following the below upgrade path

- 17.3.6 -> 17.11.1 EFT Image (Cisco qualified)
- 17.6.4 -> 17.11.1 EFT Image (Cisco qualified)

- 17.10.1 -> 17.11.1 EFT Image (Cisco qualified)

Note: If the customers have C9130 running 17.3.x, to successfully upgrade to 17.11, please upgrade to 17.6.x first.
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-3/release-notes/rn-17-39800.html#Cisco_Concept.dita_9d1727be-e4ff-48e0-bbfd-cdb60f7b4054

Compatibility Matrix



Access Point	IOS-XE	Cisco DNA Center	Cisco DNA Spaces	Prime	CMX	ISE
AP1540/AP1560 AP1815/AP1830/AP1840/AP1852/AP1800i	17.11.1	2.3.5.x 2.3.4.x 2.3.3.x	DNA Space Connector 2.x	3.10.2 3.10.1 3.10	CMX 10.6.3 MRx	3.0 + latest patch 2.7+
AP2800/AP3800/ AP4800 C9105AX C9115AX C9120AX C9124AX C9130AX C9136AX CW9162I CW9164I CW9166I						latest patch 2.6 + latest patch 2.4 + latest patch

Features to Test

C9800 Jumbo Frame Support for Radius/AAA packets

Feature Overview:

In all the Polaris releases (till date), by default the radius packet Fragmentation is done at 1396 bytes in the intermediate layer. Which means “interface IP MTU configuration” is not honored. This leads to the below issues like Fragmentation size is fixed and Jumbo Frames are not supported. By adding this feature, the interface IP MTU configuration will be honored. Which would cover all the possible customer use cases with consistent behavior on outgoing RADIUS packets. With the new design, the RADIUS packet gets fragmented at the interface IP MTU configured value. The user has to configure the required IP MTU value under the interface config and in order to use the configured IP MTU value for the RADIUS transaction user has to configure the interface name under the corresponding RADIUS group.

Pre-Requisite:

- This feature will be supported on all platforms from the 17.11.1 version. · Jumbo packet support is available on ISE 3.1 version onwards

Configuration:

Interface configuration: interface <Interface Name> no switchport mtu 5000 -> setup the Max MTU Range ip address x.x.x.x x.x.x.x ip mtu <bytes> -> setup the IP MTU

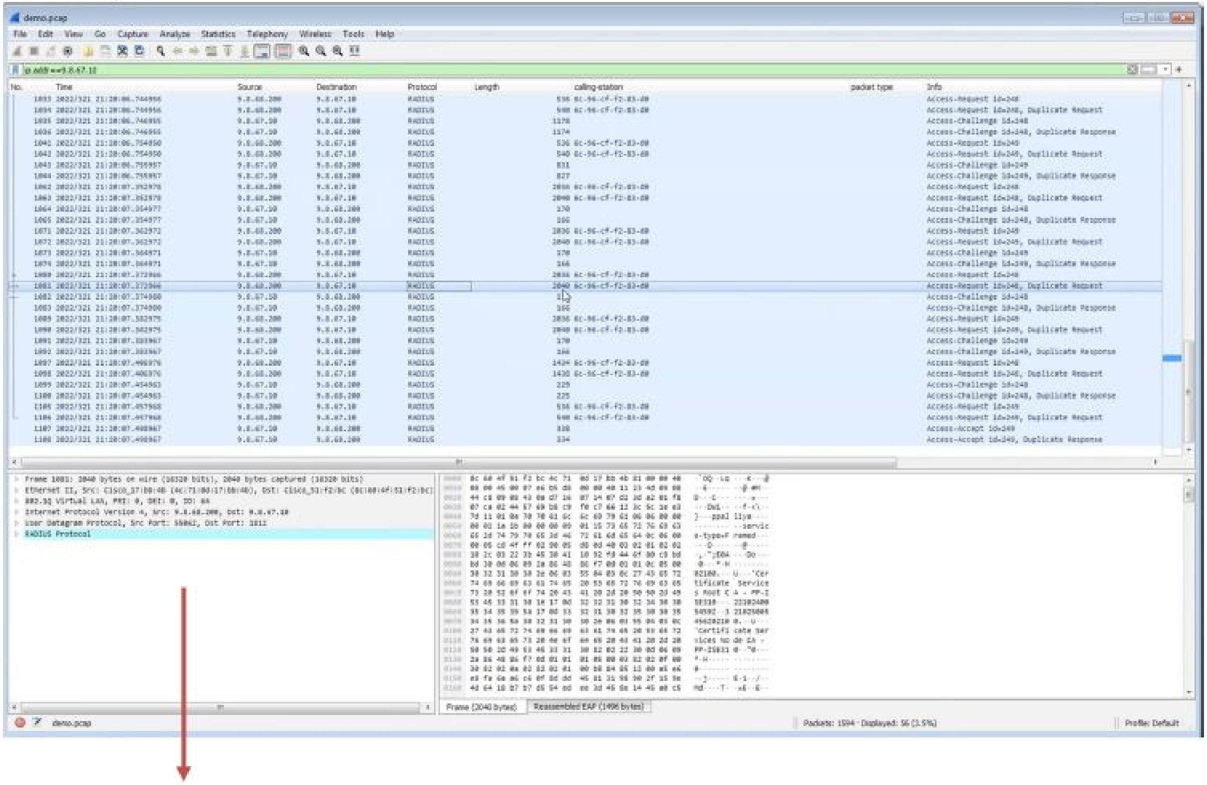
Radius Configuration on controller: aaa group server radius RADIUS_GROUP server name radius_server1 ip radius source-interface <Interface Name>

ISE Configuration interface <Interface Name> ip mtu <bytes>

Note: If IP MTU is changed on ISE, please expect a network service restart for ISE.

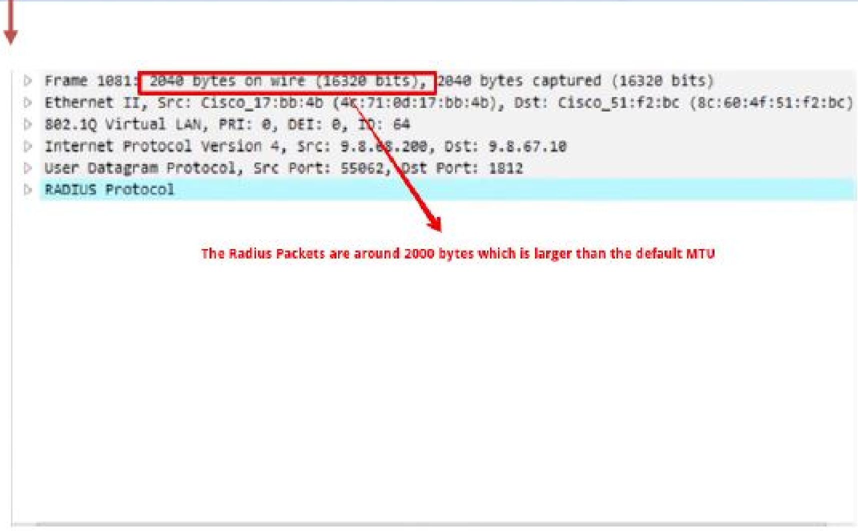
Verification

Packet capture on Radius Packets:



demo.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr==9.8.67.10

No.   Time                      Source       Destination  Protocol  Length  calling-station        packet type  Info
1033  2022/321 21:28:06.744956  9.8.68.200   9.8.67.10    RADIUS            536 8c-96-cf-f2-83-d0               Access-Request id=248
1034  2022/321 21:28:06.744956  9.8.68.200   9.8.67.10    RADIUS            540 8c-96-cf-f2-83-d0               Access-Request id=248, Duplicate Request
1035  2022/321 21:28:06.746955  9.8.67.10    9.8.68.200   RADIUS           1178                                 Access-Challenge id=248
1036  2022/321 21:28:06.746955  9.8.67.10    9.8.68.200   RADIUS           1174                                 Access-Challenge id=248, Duplicate Response
1041  2022/321 21:28:06.754850  9.8.68.200   9.8.67.10    RADIUS            536 8c-96-cf-f2-83-d0               Access-Request id=249
1042  2022/321 21:28:06.754850  9.8.68.200   9.8.67.10    RADIUS            540 8c-96-cf-f2-83-d0               Access-Request id=249, Duplicate Request
1043  2022/321 21:28:06.755957  9.8.67.10    9.8.68.200   RADIUS            831                                 Access-Challenge id=249
1044  2022/321 21:28:06.755957  9.8.67.10    9.8.68.200   RADIUS            827                                 Access-Challenge id=249, Duplicate Response
1062  2022/321 21:28:07.352976  9.8.68.200   9.8.67.10    RADIUS           2036 8c-96-cf-f2-83-d0               Access-Request id=248
1063  2022/321 21:28:07.352976  9.8.68.200   9.8.67.10    RADIUS           2040 8c-96-cf-f2-83-d0               Access-Request id=248, Duplicate Request
1064  2022/321 21:28:07.354977  9.8.67.10    9.8.68.200   RADIUS            170                                 Access-Challenge id=248
1065  2022/321 21:28:07.354977  9.8.67.10    9.8.68.200   RADIUS            166                                 Access-Challenge id=248, Duplicate Response
1071  2022/321 21:28:07.362972  9.8.68.200   9.8.67.10    RADIUS           2036 8c-96-cf-f2-83-d0               Access-Request id=249
1072  2022/321 21:28:07.362972  9.8.68.200   9.8.67.10    RADIUS           2040 8c-96-cf-f2-83-d0               Access-Request id=249, Duplicate Request
1073  2022/321 21:28:07.364971  9.8.67.10    9.8.68.200   RADIUS            170                                 Access-Challenge id=249
1074  2022/321 21:28:07.364971  9.8.67.10    9.8.68.200   RADIUS            166                                 Access-Challenge id=249, Duplicate Response
1080  2022/321 21:28:07.372966  9.8.68.200   9.8.67.10    RADIUS           2036 8c-96-cf-f2-83-d0               Access-Request id=248
1081  2022/321 21:28:07.372966  9.8.68.200   9.8.67.10    RADIUS           2040 8c-96-cf-f2-83-d0               Access-Request id=248, Duplicate Request
1082  2022/321 21:28:07.374900  9.8.67.10    9.8.68.200   RADIUS            1                                   Access-Challenge id=248
1083  2022/321 21:28:07.374900  9.8.67.10    9.8.68.200   RADIUS            166                                 Access-Challenge id=248, Duplicate Response
1089  2022/321 21:28:07.382975  9.8.68.200   9.8.67.10    RADIUS           2036 8c-96-cf-f2-83-d0               Access-Request id=249
1090  2022/321 21:28:07.382975  9.8.68.200   9.8.67.10    RADIUS           2040 8c-96-cf-f2-83-d0               Access-Request id=249, Duplicate Request
1091  2022/321 21:28:07.383967  9.8.67.10    9.8.68.200   RADIUS            170                                 Access-Challenge id=249
1092  2022/321 21:28:07.383967  9.8.67.10    9.8.68.200   RADIUS            166                                 Access-Challenge id=249, Duplicate Response
1097  2022/321 21:28:07.406976  9.8.68.200   9.8.67.10    RADIUS           1434 8c-96-cf-f2-83-d0               Access-Request id=248
1098  2022/321 21:28:07.406976  9.8.68.200   9.8.67.10    RADIUS           1438 8c-96-cf-f2-83-d0               Access-Request id=248, Duplicate Request
1099  2022/321 21:28:07.454963  9.8.67.10    9.8.68.200   RADIUS            229                                 Access-Challenge id=248
1100  2022/321 21:28:07.454963  9.8.67.10    9.8.68.200   RADIUS            225                                 Access-Challenge id=248, Duplicate Response
1105  2022/321 21:28:07.497968  9.8.68.200   9.8.67.10    RADIUS            536 8c-96-cf-f2-83-d0               Access-Request id=249
1106  2022/321 21:28:07.497968  9.8.68.200   9.8.67.10    RADIUS            540 8c-96-cf-f2-83-d0               Access-Request id=249, Duplicate Request
1107  2022/321 21:28:07.498967  9.8.67.10    9.8.68.200   RADIUS            338                                 Access-Accept id=249
1108  2022/321 21:28:07.498967  9.8.67.10    9.8.68.200   RADIUS            334                                 Access-Accept id=249, Duplicate Response

> Frame 1081: 2040 bytes on wire (16320 bits), 2040 bytes captured (16320 bits)
> Ethernet II, Src: Cisco_17:bb:4b (4c:71:0d:17:bb:4b), Dst: Cisco_51:f2:bc (8c:60:4f:51:f2:bc)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 64
> Internet Protocol Version 4, Src: 9.8.68.200, Dst: 9.8.67.10
> User Datagram Protocol, Src Port: 55062, Dst Port: 1812
> RADIUS Protocol

Frame (2040 bytes)   Reassembled EAP (1496 bytes)
demo.pcap            Packets: 1594 · Displayed: 56 (3.5%)            Profile: Default
```



```
> Frame 1081: 2040 bytes on wire (16320 bits), 2040 bytes captured (16320 bits)
> Ethernet II, Src: Cisco_17:bb:4b (4c:71:0d:17:bb:4b), Dst: Cisco_51:f2:bc (8c:60:4f:51:f2:bc)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 64
> Internet Protocol Version 4, Src: 9.8.68.200, Dst: 9.8.67.10
> User Datagram Protocol, Src Port: 55062, Dst Port: 1812
> RADIUS Protocol
```

The Radius Packets are around 2000 bytes which is larger than the default MTU

Enhancement in client steering during Rolling AP Upgrade

Feature Overview:

During software upgrades, the Rolling AP Upgrade allows there to be minimal network connectivity downtime. This is because when an AP goes to reload with the new image, the surrounding APs will be up to serve clients. When an AP is selected to reload, the clients currently connected to it need to roam to a different AP. To do this, the AP will no longer respond to client join requests, and it will send 802.11v BSS transition management frames to all the clients supporting 802.11v. This will notify them the AP is going to reload and to roam to a new AP. For clients that do not support 802.11v or do not roam, the controller will de-authenticate all the clients connected to the AP.

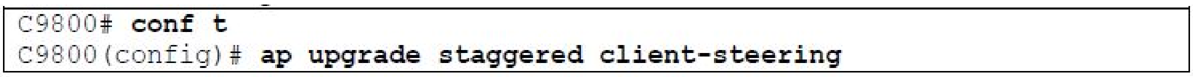
For more information on Rolling AP Upgrade, please check this link:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-6/configguide/b_wl_17_6_cg/m_hitless_upgrade.html

Pre-Requisite:

- Cisco Catalyst 9800 Wireless LAN Controller running IOS XE 17.11.1

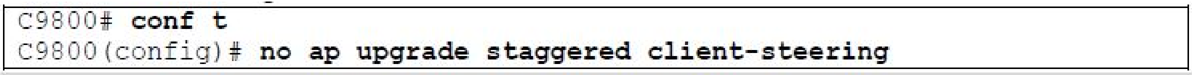
Configuration & Verification:

- **To enable client steering:** C9800# conf t C9800(config)# ap upgrade staggered client-steering



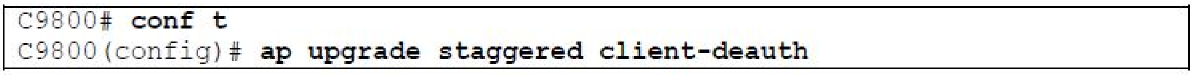
```
C9800# conf t
C9800(config)# ap upgrade staggered client-steering
```

- **To disable client steering:** C9800# conf t C9800(config)# no ap upgrade staggered client-steering



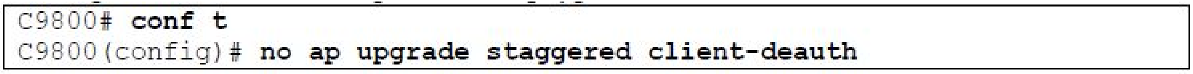
```
C9800# conf t
C9800(config)# no ap upgrade staggered client-steering
```

- **To configure de-authenticating clients during upgrade before the AP reloads:** C9800# conf t C9800(config)# ap upgrade staggered client-deauth



```
C9800# conf t
C9800(config)# ap upgrade staggered client-deauth
```

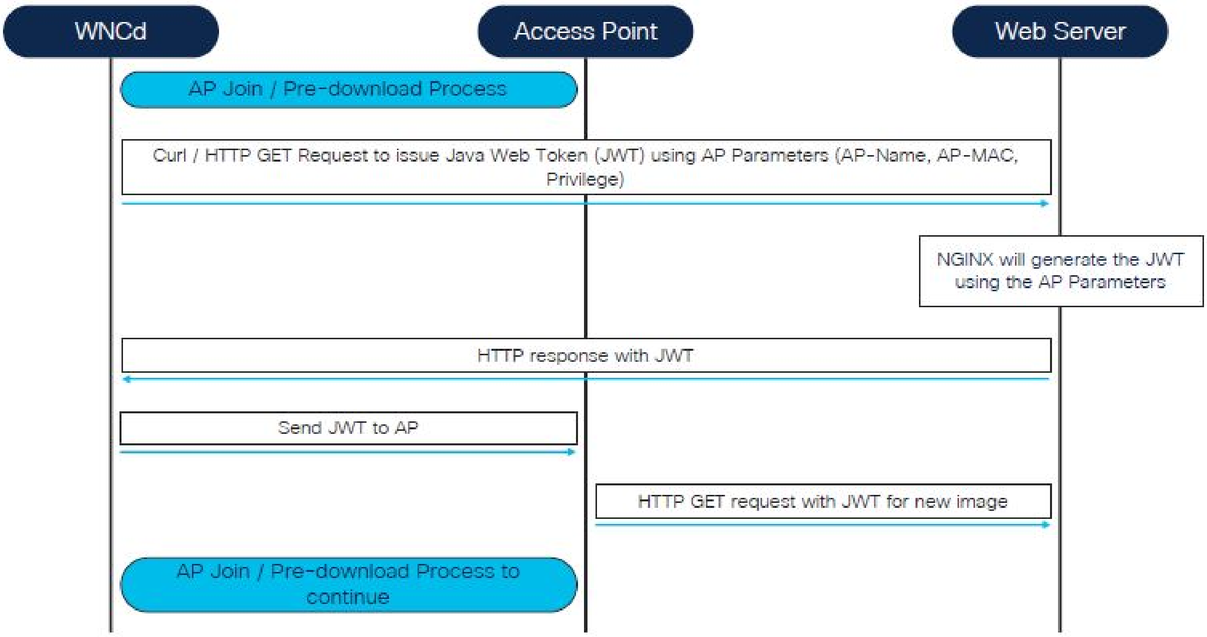
- **To configure not de-authenticating clients during upgrade before the AP reloads:** C9800# conf t C9800(config)# no ap upgrade staggered client-deauth



```
C9800# conf t
C9800(config)# no ap upgrade staggered client-deauth
```

Efficient AP image download through TCP

Feature Overview:
Prior to IOS XE 17.11.1, the AP image download during software upgrades utilized the CAPWAP control tunnel. However, the CAPWAP control tunnel is often occupied as it is used for many other purposes. Also, the image download time is limited by the CAPWAP window size. There is also a heavy load on the C9800 as the AP image downloads cause the WNCD processes to heavily utilize the CPU. With IOS XE 17.11.1, AP image downloads move out of the CAPWAP control tunnel and into the out-of-band data plane, allowing the image downloads to happen over HTTPS. By moving the download process to HTTPS, the load on the WNCd processes is reduced and frees the CAPWAP control path. Furthermore, by utilizing HTTPS and TCP, the image downloads are faster and more flexible as the link type and speed can be specified. If the HTTPS download fails, there is seamless fallback to the CAPWAP control tunnel. By default, the image upgrade will leverage port 8443 in order to avoid impact on the WebUI and telemetry streams on the C9800. This can be changed to fit the deployment. **The mechanism for AP image download is as follows:**


WNCd
Access Point
Web Server
AP Join / Pre-download Process
Curl / HTTP GET Request to issue Java Web Token (JWT) using AP Parameters (AP-Name, AP-MAC, Privilege)
NGINX will generate the JWT using the AP Parameters
HTTP response with JWT
Send JWT to AP
HTTP GET request with JWT for new image
AP Join / Pre-download Process to continue

Pre-Requisite:

Configuration & Verification:

To enable AP upgrade to use HTTPS: C9800# conf t C9800(config)# ap upgrade method https

```
C9800# conf t
C9800(config)# ap upgrade method https
```

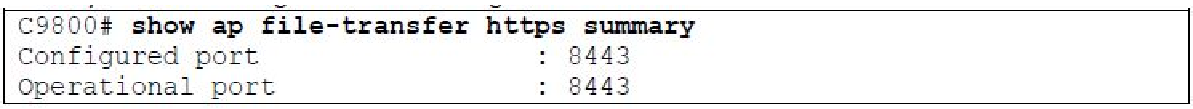
To configure the AP file transfer port: C9800# conf t C9800(config)# ap file-transfer https port <port_number> **Note:** If left unconfigured, the C9800 will use port 8443.

```
C9800# conf t
C9800(config)# ap file-transfer https port <port_number>
```

To verify that the AP image download is using HTTPS: C9800# show ap upgrade method HTTPS: Enabled>

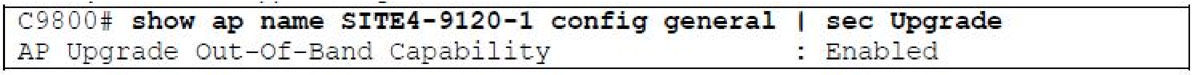
```
C9800# show ap upgrade method
AP upgrade method HTTPS : Enabled>
```

To verify that the AP image download is using HTTPS: C9800# show ap file-transfer https summary



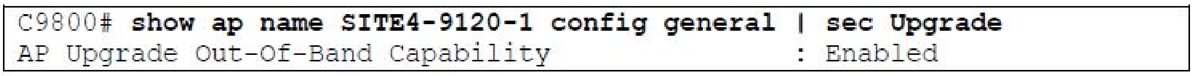
```
C9800# show ap file-transfer https summary
Configured port                   : 8443
Operational port                  : 8443
```

To verify that the AP supports image download over HTTPS: C9800# show ap name SITE4-9120-1 config general | sec Upgrade



```
C9800# show ap name SITE4-9120-1 config general | sec Upgrade
AP Upgrade Out-Of-Band Capability                  : Enabled
```

To verify that the AP image download over HTTPS: C9800# show ap name SITE4-9120-1 config general | sec Upgrade AP Upgrade Out-Of-Band Capability



```
C9800# show ap name SITE4-9120-1 config general | sec Upgrade
AP Upgrade Out-Of-Band Capability                  : Enabled
```

Intelligently disable 2.4 GHz radios

Feature Overview:

- **FRA** Flexible Radio Assignment
- **XOR** Dual-Band Radios
- **RRM** Radio Resource Management

To provide a configurable option to move redundant dual band XOR radios in the network to monitor role only. Current IOS-XE implementation, FRA moves redundant dual-band (XOR 2.4GHz/5GHz) radios to either 5GHz client serving or Monitor function. There is no choice but to select a particular option based on the deployment. This feature will allow customers to configure and choose as per their requirements. FRA evaluates 2.4GHz coverage only and determines if overlapping coverage is creating interference. If detected, the feature will move dual-band (XOR 2.4/5GHz) radio to either a 5GHz Client serving or Monitor role. As per the current implementation, there is no option to choose. This feature implements a configuration option in the 2.4GHz RF profile to select the radio to move to monitor-only mode. As part of this feature, the customer will have a configurable option to select the redundant dualband (XOR 2.4/5GHz) radios in the network to operate in a monitor role. Currently, there is no option to choose an FRA that will move radios to either 5GHz client serving or monitor. With this option, customers can choose based on their deployment.

Pre-Requisite:

- Cisco Catalyst 9800 Wireless LAN Controller running IOS XE 17.11.1
- APs: C9115, C9120, C9130, C9136, CW9164, CW9166, CW9162

Configuration & Verification:

Default-RF-Profile [Global Config]:
wlc(config)#ap dot11 24ghz fra action ? monitor Configures FRA action as monitor

GHz RF-Profile
mdc-prod-wc2(config)#ap dot11 24ghz rf-profile madhu-rf-profile-24 mdc-prod-wc2(config-rf-profile)#fra action ? monitor Configures FRA action as monitor

WebUI Configuration [1/2] Navigate: Configuration > Radio Configuration > RRM > FRA > 2.4/ 5GHz Flexible Radio > FRA Action

WebUI Configuration [2/2] Navigate: Configuration > Tags & Profiles > RF/Radio > Advanced > FRA Action **Select:** Update and Apply to Device

Show Commands

mdc-prod-wc2#sh ap fra

- **FRA State:** Enabled
- **FRA Freeze:** Disabled
- **FRA Operation State**: Up
- **FRA Sensitivity:** higher (85%)
- **FRA Interval:** 1 Hour(s)
- **Service Priority:** Coverage
- **Client Aware FRA:** Enabled
- **Client Select:** 25%
- **Client Reset:** 5%

- **FRA Action:** 2.4GHz/Monitor
- **Last Run:** 3069 seconds ago

Show CLI [2/2]

mdc-prod-wc2#sh ap rf-profile <rf-profile name> detail | sec FRA

- **Client Aware FRA:** Disabled
- **FRA Action:** 2.4GHz/Monitor

mdc-prod-wc2#sh ap name AP7872.5DED.CB74 config slot 0 | sec Attribute Attributes for Slot 0

- **Radio Type:** 802.11n – 2.4/5 GHz
- **Radio Mode:** Monitor
- **Radio Role:** Monitor
- **Assignment Method:** Auto
- **Monitor Mode Reason:** Automatically Switched by FRA

Usability: AAA CLI request

Feature Overview:
To increase the user readability on the show command for the AAA server, a new CLI “show aaa server brief” is introduced which will show all the necessary details in tabular format. **And the column includes the following information:**

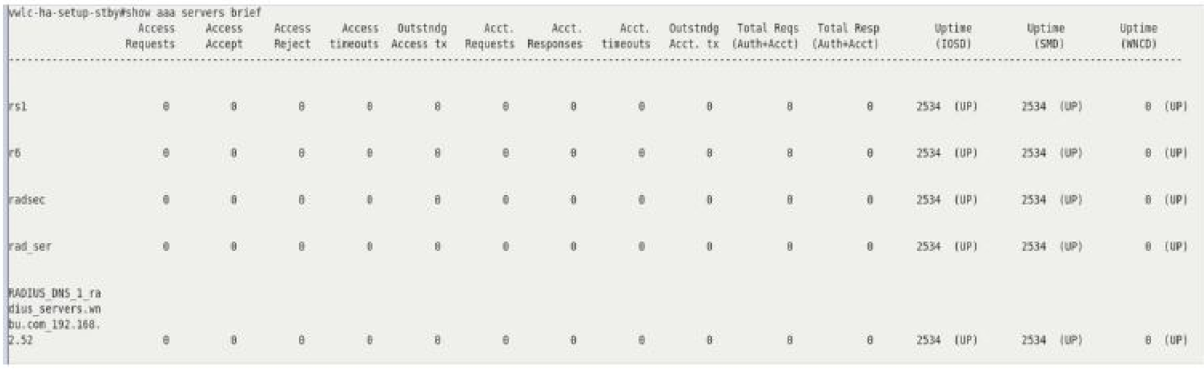
- Access Requests
- Access-Accept
- Access-Reject
- Access Timeouts
- Outstanding Access Transactions
- Uptime
- Accounting Requests
- Accounting response
- Accounting Timeouts
- Outstanding Accounting Transactions
- Total Requests (Auth+Acct)
- Total Responses(Auth+Acct)

Pre-Requisite:
Cisco Catalyst 9800 Wireless LAN Controller running IOS XE 17.11.1

Configuration & Verification:

Configuration:
No configuration needed.

Verification:
show aaa server brief



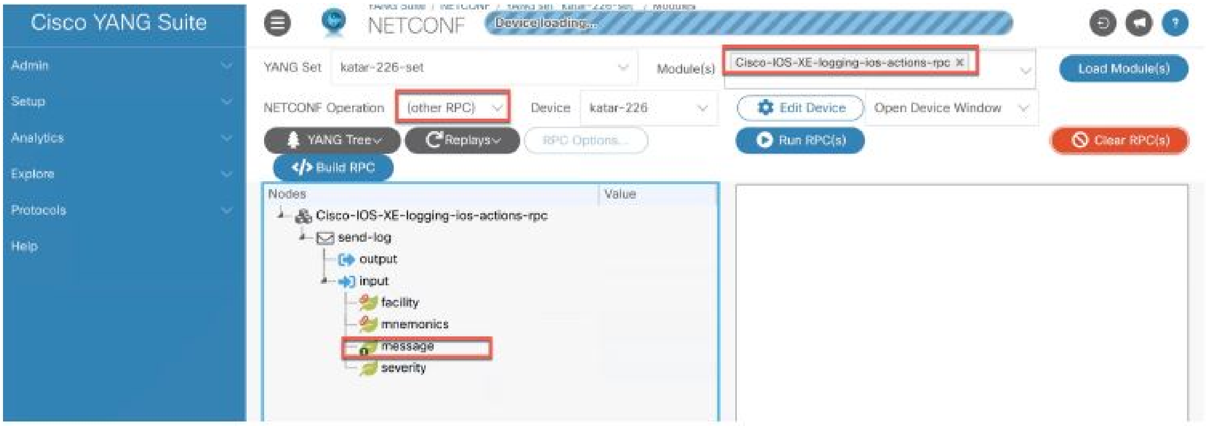
```
wlc-ha-setup-stby#show aaa servers brief
                     Access    Access    Access    Access  Outstndg     Acct.     Acct.     Acct.  Outstndg  Total Reqs  Total Resp       Uptime        Uptime        Uptime
                   Requests    Accept    Reject  timeouts Access tx  Requests Responses  timeouts Acct. tx (Auth+Acct) (Auth+Acct)       (IOSD)         (SMD)        (WNCD)
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------


rs1                       0         0         0         0         0         0         0         0         0           0           0   2534  (UP)    2534  (UP)       0  (UP)

r6                        0         0         0         0         0         0         0         0         0           0           0   2534  (UP)    2534  (UP)       0  (UP)

radsec                    0         0         0         0         0         0         0         0         0           0           0   2534  (UP)    2534  (UP)       0  (UP)

rad_ser                   0         0         0         0         0         0         0         0         0           0           0   2534  (UP)    2534  (UP)       0  (UP)

RADIUS_DNS_1_ra
dius_servers.wn
bu.com_192.168.
2.52                      0         0         0         0         0         0         0         0         0           0           0   2534  (UP)    2534  (UP)       0  (UP)
```

RPC for Syslog Configuration

Feature Overview:
This feature enhancement provides yang RPC support for CLI `send log’ such that they can send the syslog message to device. Basically, IOS-XE exec CLI send log, sends the specified logs to the syslog server. It helps to validate both syslog server and device to send and receive syslogs, now this can be achieved through the yang programable interface.

Pre-Requisite:
Cisco Catalyst 9800 Wireless LAN Controller running IOS XE 17.11.1 Yang RPC support of this CLI `send log ‘will provide a mechanism to push the syslog message to device. In turn, the device will send this message to a configured Syslog server. The Netconf-yang and restconf should be configured on the C9800 C9800#show running-config | in rest restconf C9800#show running-config | in net conf net conf-yang

Generally, the `send log’ is configured from CLI but in 17.11 we can send it through the programable interface as shown below



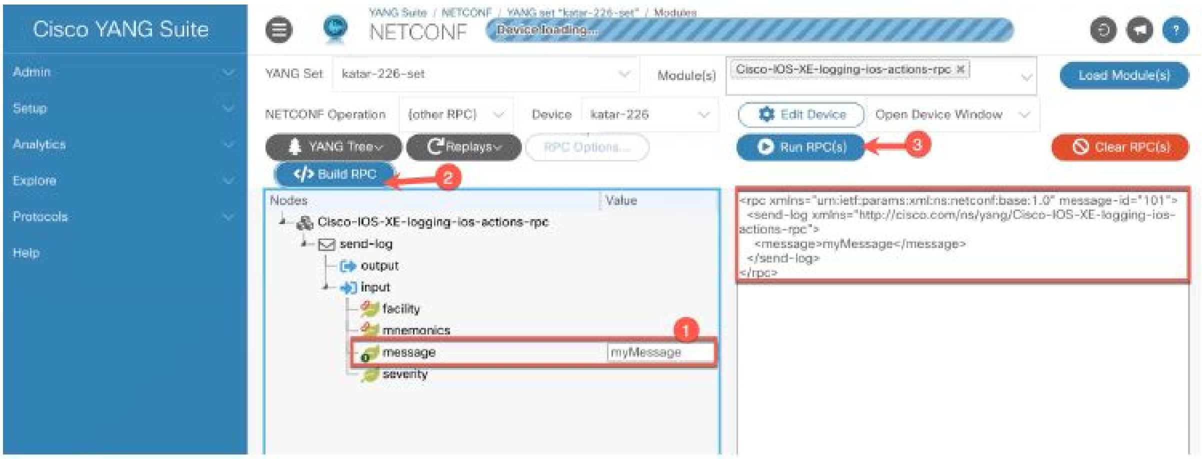
YANG Set: katar-226-set

Module(s): Cisco-IOS-XE-logging-ios-actions-rpc

NETCONF Operation: (other RPC)

Device: katar-226

There should not be any empty message



YANG Set: katar-226-set

Module(s): Cisco-IOS-XE-logging-ios-actions-rpc

NETCONF Operation: (other RPC)

Device: katar-226

Nodes	Value
Cisco-IOS-XE-logging-ios-actions-rpc	
send-log	
output	
input	
facility	
mnemonics	
message	myMessage
severity	

```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
  <send-log xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-logging-ios-
actions-rpc">
    <message>myMessage</message>
  </send-log>
</rpc>
```

On WLC we see the message is printed in the log message.

The following are the restrictions on the inputs:

- The string in the log message should be in plain text format.
- An empty log message is not allowed.
- Special characters are allowed in log messages, mnemonics, and facilities.
- No space is allowed in the Facility name and Mnemonics, unlike the log message.
- **There are 3 ways for inputs:**
  1. Only log message (In this case log message will be sent with default severity, facility, and mnemonics).
  2. Severity along with log message (In this case log-message will be sent with default facility and mnemonics)
  3. All 4 options log message, severity, facility, and mnemonics.
- Below is the list of default values:
  1. Severity 7
  2. Facility “SYS”
  3. Mnemonics “USERLOG_DEBUG”

Improvements to Built-in Captive Portal

Feature Overview:
International customers across varying legal entities must comply with all local laws. A legal requirement that is becoming more apparent is the inclusion of local languages in all operations. Within current implementations of IOS-XE, the login portal banner text section is limited of around 200 chars. Additionally, the software does not allow for the input of special chars such as “ö” or “à”. Within 17.11.1, the banner text CLI input limit will be enhanced to accommodate up to 400 chars. Furthermore, both banner text and banner title strings displayed in the HTML login page will now be able to support special characters such as “ö” or “à” etc. Since the multi-line banner is supported via CLI, it is possible to configure via YANG as well. If the input string provided exceeds the maximum limit, an error message will be thrown indicating the same, and the config will be rejected. The Webauth login portal banner comprises of two parts.

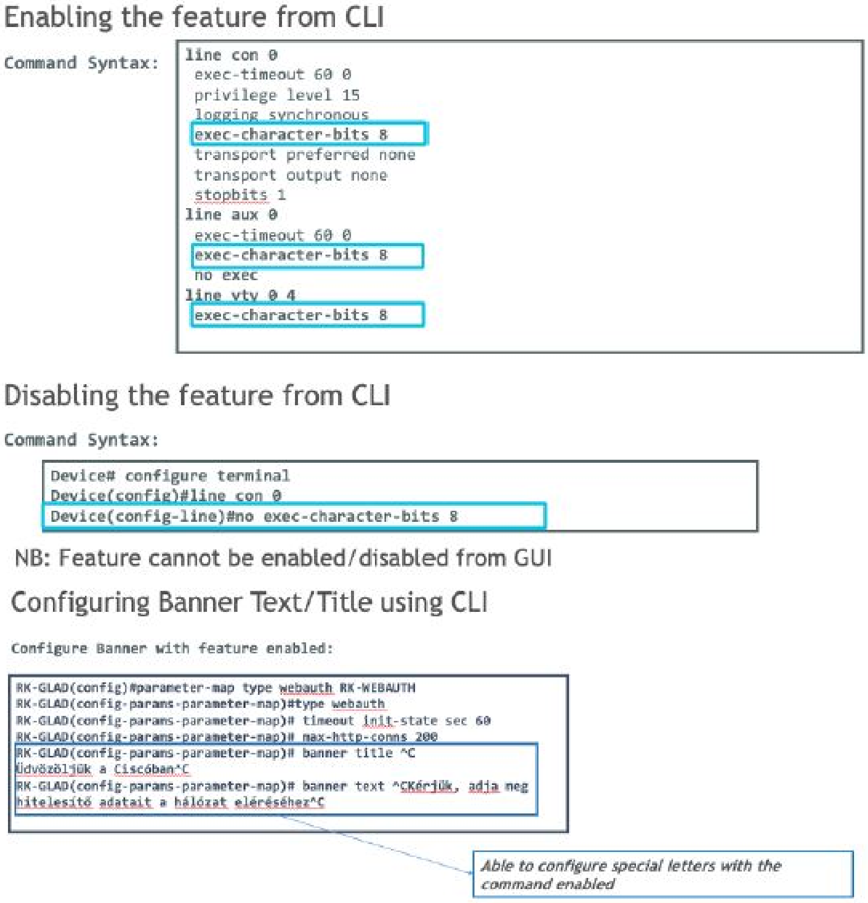
1. **Banner title** This can be customized using banner title <> CLI under web auth parameter map. The default title string is “Welcome to the Cisco Web-Authentication network.”
2. **Banner text** This can be customized using banner text <> CLI under web auth parameter map. The default text string is “Cisco is pleased to provide web-authentication infrastructure for your network. Please login.”

Limitations:

1. No WebUI support for this feature.
2. Parser has a limitation of 254 characters per line (including the CLI keywords). Hence, user will need to keep this in account while providing the input

Pre-Requisite:

- Cisco Catalyst 9800 Wireless LAN Controller running IOS XE 17.11.1
- Users must have knowledge of Local Web-Auth, Banner text and banner title.



Enabling the feature from CLI

Command Syntax:

```
line con 0
 exec-timeout 60 0
 privilege level 15
 logging synchronous
 exec-character-bits 8
 transport preferred none
 transport output none
 stopbits 1
line aux 0
 exec-timeout 60 0
 exec-character-bits 8
 no exec
line vty 0 4
 exec-character-bits 8
```

Disabling the feature from CLI

Command Syntax:

```
Device# configure terminal
Device(config)#line con 0
Device(config-line)#no exec-character-bits 8
```

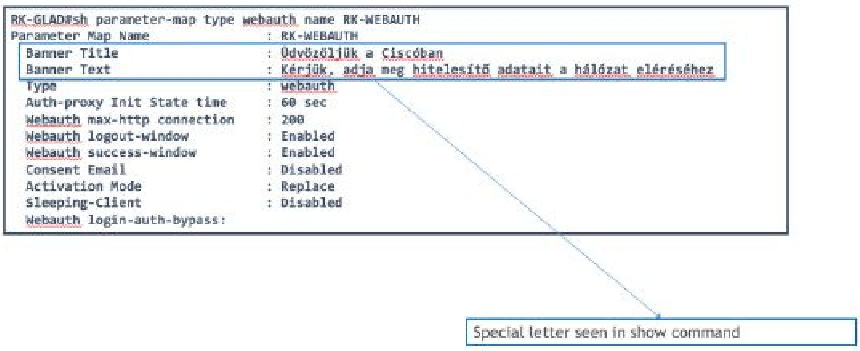
NB: Feature cannot be enabled/disabled from GUI

Configuring Banner Text/Title using CLI

Configure Banner with feature enabled:

```
RK-GLAD(config)#parameter-map type webauth RK-WEBAUTH
RK-GLAD(config-params-parameter-map)#type webauth
RK-GLAD(config-params-parameter-map)# timeout init-state sec 60
RK-GLAD(config-params-parameter-map)# max-http-conns 200
RK-GLAD(config-params-parameter-map)# banner title ^C
Üdvözöljük a Ciscóban^C
RK-GLAD(config-params-parameter-map)# banner text ^CKérjük, adja meg
hitelesitő adatait a hálózat eléréséhez^C
```

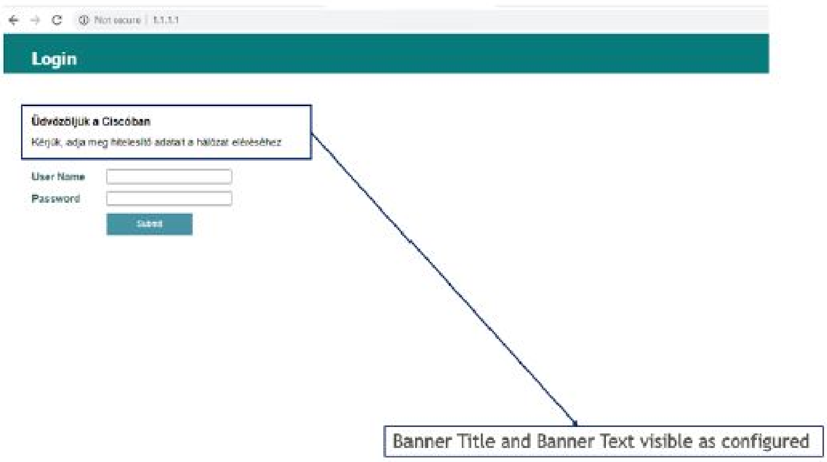
Able to configure special letters with the command enabled



```
RK-GLAD#sh parameter-map type webauth name RK-WEBAUTH
Parameter Map Name               : RK-WEBAUTH
  Banner Title                   : Üdvözöljük a Ciscóban
  Banner Text                    : Kérjük, adja meg hitelesítő adatait a hálózat eléréséhez
  Type                           : webauth
  Auth-proxy Init State time     : 60 sec
  Webauth max-http connection    : 200
  Webauth logout-window          : Enabled
  Webauth success-window         : Enabled
  Consent Email                  : Disabled
  Activation Mode                : Replace
  Sleeping-Client                : Disabled
  Webauth login-auth-bypass:
```

Special letter seen in show command

Web Auth Page as seen on Client



Üdvözöljük a Ciscóban

Kérjük, adja meg hitelesítő adatait a hálózat eléréséhez

Banner Title and Banner Text visible as configured

Troubleshooting:

Below IOS debug can be enabled to see if there was any problem in banner config. debug ip admission all On binos side, we can enable wncd all module verbose logs and collect the traces. RA internal logs can also be collected for client-related debugging. Below command outputs should also be collected. show parameter-map type webauth name <> test platform software database get sm_exec_context/tbl_webauth_parammap;name=<name of parameter map> sh platform software process database wncd ch ac R0 details SM_CONFIG_DB “table tbl_webauth_parammap” content

Multi Authentication Combination of 802.1x w/AAA Override (Dynamic Vlan Assignment) and LWA (consent) on C9800

Feature Overview:

In a university setup, clients authenticate using 802.1X. As part of 802.1X authentication, AAA server pushes the policies to be applied for the client. VLAN is one attribute which is pushed from AAA server. Since dot1x is secure and happens without any user intervention, the end users are not aware of which network they are connected to. This could lead to problems if the clients connect to university Wifi and the users post inappropriate posts or visit inappropriate sites.

To circumvent this problem, the university has configured for WebAuth authentication post 802.1X. Web-Consent is used as part of WebAuth to inform the end users that they are connected to the University Wifi. However, as part of Web-Consent, since, no AAA policy is applied, the previously applied AAA policy gets removed. This results in VLAN change and leads to client disconnection. This cycle continues and the client doesn’t get network access.

To fix this problem, CLI is introduced. If this CLI is configured, then the policy applied via Consent would be merged with the policy applied for 802.1X/MAB.

Pre-Requisite:

- Cisco Catalyst 9800 Wireless LAN Controller running IOS XE 17.11.1
- Users must have knowledge on Multi Auth concepts, LWA(Consent), AAA override.

Enabling the Feature from CLI: Device# configure terminal Device(config)#parameter-map type web auth LWA_consent Device(config-params-parameter-map)#type consent Device(config-params-parameter-map)#consent activation-mode merge
Disabling the Feature from CLI: Device# configure terminal Device(config)#parameter-map type web auth LWA_consent Device(config-params-parameter-map)#no consent activation-mode merge

Show command with the feature enabled from CLI: JD_9800-L_1#sh parameter-map type web auth name LWA_consent

- **Parameter Map Name:** LWA_consent
- Banner Title: Consent Title
- Banner Text: Please accept the consent
- Type: consent
- Auth-proxy Init State time: 300 sec
- Webauth max-http connection: 200
- Webauth logout-window: Enabled
- Webauth success-window: Enabled
- Consent Email: Disabled
- Activation Mode:
- Sleeping-Client: Merge
- Webauth login-auth-bypass: Disabled

policy applied via Consent would be merged with the policy applied for 802.1X/MAB.

Show command with feature disabled from CLI:|
JD_9800-L_1#sh parameter-map type webauth name LWA_consent

- Parameter Map Name: LWA_consent
- Consent Email: Disabled
- Activation Mode: Replace

policy applied via Consent would not be merged with the policy applied for 802.1X/MAB.

Limitations:

- No WebUI support for this feature.
- No SNMP support. Only Yang support would be added for this feature.
- When “activation-mode merge” is not configured on the WebAuth parameter map, then the default activation mode is REPLACE-ALL. This means that user-profile for consent would replace all previously applied user-profile policies.

Location-Capable attribute in the Access-Request messages as part of RFC5580 Feature Overview:
The RFC 5580 location attributes convey location-related information for authentication and accounting exchanges. The location information is useful in several scenarios. Wireless networks are deployed in public places, such as shopping malls, airports, hotels, and coffee shops by a diverse set of operators, such as wireless internet service providers (WISPs), cellular network operators, and fixed broadband networks. In all these scenarios, the network may need to know the user location to enable location-aware authorization, billing, or services. Please refer to the IOS-XE 17.9 config guide for configuring RFC 5508 location attributes

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-9/configguide/b_wl_17_9_cg/m_rfc-5580-loc-att-on-the-controller.html#Cisco_Reference.dita_aed3a65e9f99-4d8b-bddb-a6c4e9c3fe54

RFC 5580 mentions three location delivery methods for location information to AAA server, as mentioned below:

1. Location delivery based on Out-of-Band agreement
2. Location delivery based on Initial request
3. Location delivery based on Mid-Session request

In IOS-XE 17.11 release we are enhancing this feature by adding the location-capable attribute in the access request to the out-of-band agreement.

Pre-Requisite:

1. Cisco Catalyst 9800 Wireless LAN Controller running IOS XE 17.11.1
2. Users must have knowledge of AAA and 802.1x

Configuration & Verification:
The location-Capable attribute is sent as part of access requests only in case of method 2 (Location delivery based on Initial request) which is initial-request-based, but we are providing the support for this attribute in out-of-band which is (Location delivery based on Out-of-Band agreement) To enable this attribute following command needs to be configured on C9800. Currently, its only supported from CLI C9800(config)#radius-server attribute wireless location delivery outof-band include-location-capable

C9800 optimization of client exclusion time with WPA3 SAE Feature Overview:
The SAE client exclusion mechanism is designed to protect the system from using computational resources on processing invalid authentication requests from malicious users. If a client fails SAE authentication multiple times (up to 5), the C9800 will exclude the client for an exclusion time frame (default 60 sec). During this exclusion time, all authentication requests from this client are dropped. In local mode, SAE authentication is processed on WLC which counts the number of authentication failures and adds client into the exclusion list when the count reaches a predefined threshold. The client will be allowed to connect again after the exclusion timeout. The timeout value is configurable to allow flexibility in enforcing client exclusion. Prior to IOS XE 17.11.1, SAE exclusion implementation starts the exclusion process at client cleanup time after authentication failure. It takes a couple of more message exchanges between C9800 and client to reach the cleanup state. As the client may back off before sending the next message, SAE commit, after authentication failure, the time lapse varies between the failure and the start of exclusion. We can optimize the flow by starting the exclusion process right at the authentication failure (SAE confirm message mismatch) time. This avoids the delay and excludes client sooner.

Pre-Requisite:

- Cisco Catalyst 9800 Wireless LAN Controller running IOS XE 17.11.1 · This feature is for Local Mode deployments only.

Configuration & Verification:
The optimization for WPA3 SAE client exclusion takes places in the background, and no extra configuration needs to be done.
To verify the client exclusions:

- C9800# show wireless exclusionlist
- client mac-address f2f8.4a03.a0e8 detail

- Client State : Excluded
- Client MAC Address : f2f8.4a03.a0e8
- Client IPv4 Address: N/A
- Client IPv6 Address: N/A
- Client Username: N/A
- Exclusion Reason : SAE authentication failure
- Authentication Method : None
- Protocol: N/A
- AP MAC Address : 0c75.bdb1.3f20
- AP Name: AP0C75.BDB1.EDA8
- AP slot : 0
- Wireless LAN Id : 7
- Wireless LAN Name:
- VLAN Id : 0

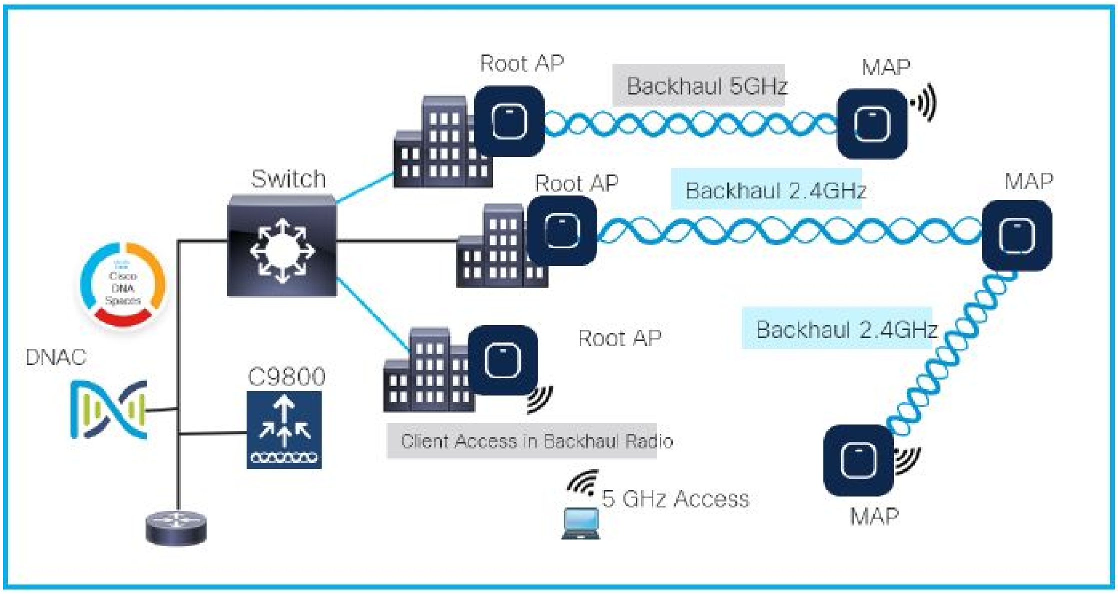
Mesh: Background Scanning Feature Overview:
Cisco Mesh access points (MAP) are interconnected over wireless links in a spanning tree like topology. A MAP connected to the network via ethernet uplink is designated as the root MAP aka RAP. AWPP protocol is used to maintain the tree and form the tree. When a MAP comes up, it tries to look for another MAP (parent) to join to reach the gateway eventually via a RAP. The same happens when a MAP loose connectivity with its existing parent. This procedure is known as mesh tree convergence. This document aims to improve the convergence procedure to make is faster and robust. A MAP in search its parent uplink undergoes following procedures:

1. Parent loss detection (if connected already)
2. Scan (passive) for a new parent across all / subset of regulatory domain channels
3. Seek (request/response) on newfound parent on scanned/operable channels
4. Evaluate and choose the best neighbor
5. Select the neighbor as potential parent and authenticate via selected parent to WLC
6. Retain / Renew IP and
7. Restart CAPWAP to join back the WLC

This procedure today could take from tens of seconds to a minute. We plan to implement the following to improve it: Mesh Background Scanning and auto parent selection are mechanisms used by a MAP to find and connect faster to a better potential parent across channels and always maintain its uplink with a best parent.

Pre-Requisite:
C9800 running in latest EFT IOS-XE image with Mesh network Up and running.

Topology:



Configuration & Verification:
To enable Background Scanning: In Mesh Profile (wireless profile mesh default-mesh-profile), enable the background scanning(background-scanning)
Verification: Check the background scanning in show wireless profile mesh detailed <mesh profile

Configure: C9800-CL-AWS(config)#wireless profile mesh <profile_name> C9800-CL-AWS(config-wireless-mesh-profile)#background-scanning

Verify: C9800-CL-AWS#show wireless profile mesh detailed <profile_name>

- **Mesh Profile Name:** <profile_name>
- **Description:** custom mesh profile
- **Bridge Group Name:** custom_bgn_name
- **Background Scan:** ENABLED

1. Enable background scanning and verify functionality works as expected on C9124 MAP.
    1. Enable background scanning and verify functionality works as expected on C9124 MAP.
    2. Verify mesh network is UP and running stable.
    3. Enable background scanning.
    4. On C9124 MAP verify that feature is enabled and functioning.

       Use:

        - show mesh stats
        - show mesh history recent
        - show mesh adjacency all
        - show mesh convergence
        - show mesh res
        - show mesh bags can config backhaul
        - show mesh bags can config slot 1
        - show mesh bags can channels backhaul
        - show mesh bags can channels slot 1
        - show mesh bags can status backhaul

        - show mesh bags can status slot 1
        - show mesh bags can schedule backhaul
        - show mesh bags can schedule slot 1
    5. Verify that MAP UT is aware of the full channel list on which mesh peers from the same BNG operate, i.e. it is receiving complete information during RES provisioning.
    6. Verify MAP UT is able to establish full adjacencies with radio neighbors that belong to the same BGN.
    7. Verify MAP UT will not create adjacencies with radio neighbors that are not members of the same BGN
2. Verify impact on client traffic when background scanning is enabled on C9124
    1. C9124 MAP is operating on a 5GHz backhaul channel.
    2. Wireless clients are connected to 2.4GHz client serving radio and generating constant traffic.
    3. Enable background scanning.
    4. Verify that background scanning has no impact on the client's traffic.

Zero Wait DFS: Support on C9136 Feature Overview:

- The U-Nii-2 and U-Nii-2C(e) bands also known as the "DFS Channels" (Dynamic Frequency Assignment) require a 60 second (or more) Channel Availability Check (CAC) before being used by Wi-Fi to ensure no radar is in operation.
- Zero Wait DFS allows for using the AP's resources to perform a preemptive CAC before a channel change is initiated, eliminating the 60-600 second delay experienced on a channel change to any DFS channel

Prior to 17.8 IOS-XE release, DFS CAC has been performed on demand as a precursor to assuming WiFi operations on a channel. This behavior is required to verify that there is no operating radar on the channel we will assume. Once accessed, scanning must continue during channel operation and be immediately abandoned if Radar is detected. When RRM assigns a channel, it assigns the "best" channel available in the current DCA run. There is also a second-best channel assigned at the time which is labeled as a future channel. In the event of a radar detection on the current DFS channel, the Future channel would be scanned and then used. This "Mini DCA" run ensured that the succession channel was already a good choice based on the channel adjacencies. If that future channel happened to be a DFS required channel, then the AP would scan 60 seconds (or 600 seconds if ETSI TDWR Channels 120, 124, 128) and then assume beaconing again on the new channel. The Zero Wait DFS feature was introduced originally in IOS-XE 17.9 for ETSI and FCC Catalyst C9130 AP. The IOS-XE 17.11 release adds support for the Catalyst C9136 AP's. Zero Wait DFS is heavily dependent on local regulatory bodies rules, and as such there are differences in the methods used, but minimal difference to the outcomes experienced.

ETSI Regulatory:
The concept of Pre-CAC is supported. In ETSI, once a channel has been cleared by CAC it can be considered cleared by the AP and used without additional CAC indefinitely until the AP is restarted.

- This allows the AP to scan as few or as many channels as we wish to hold for future use
- If AP needs to use a future channel, it may do so without performing CAC
- If Radar is detected on the serving channel, AP can move to a Pre-CAC Channel and broadcast immediately.

This feature effectively removes the 10-minute (600 second) penalty for using a TDWR channel (120,124,128) in ETSI.

FCC Regulatory:
FCC approach differs in that there is not provision for Pre-CAC. In FCC a channel is only valid as long as a receiver is listening to it and providing CAC data. This rule means that we can still CAC a future channel choice, but it must be continuously CAC'd if we are to assume it radar free and begin immediate operations. DCA already

calculates the “second best” channel in any channel assignment as of the time of the DCA run. With the second-best channel we have a valid, If slightly less optimal, channel already selected that won’t conflict with the rest of the APs to be used in the event of a Radar detection. This channel can be continuously CAC’d and in this way maintain readiness for immediate operations by the AP at any time. The Catalyst C9130 and C9136 radio chipsets have 3 DFS scanning engines. Running in Tri-Radio mode will demand that two of these engines be engaged if two DFS channels are assigned. However, the 3rd goes unused and can be dedicated to scan the future channel(s).

- This allows the AP to continuously scan a future channel (determined by DCA)
- If AP needs to use a future channel, it may do so without performing CAC
- If Radar is detected on the serving channel, AP can move to the future Channel and broadcast immediately.

NOTE: Future channel CAC is performed continuously without impact to serving radio operations for zero client impact.

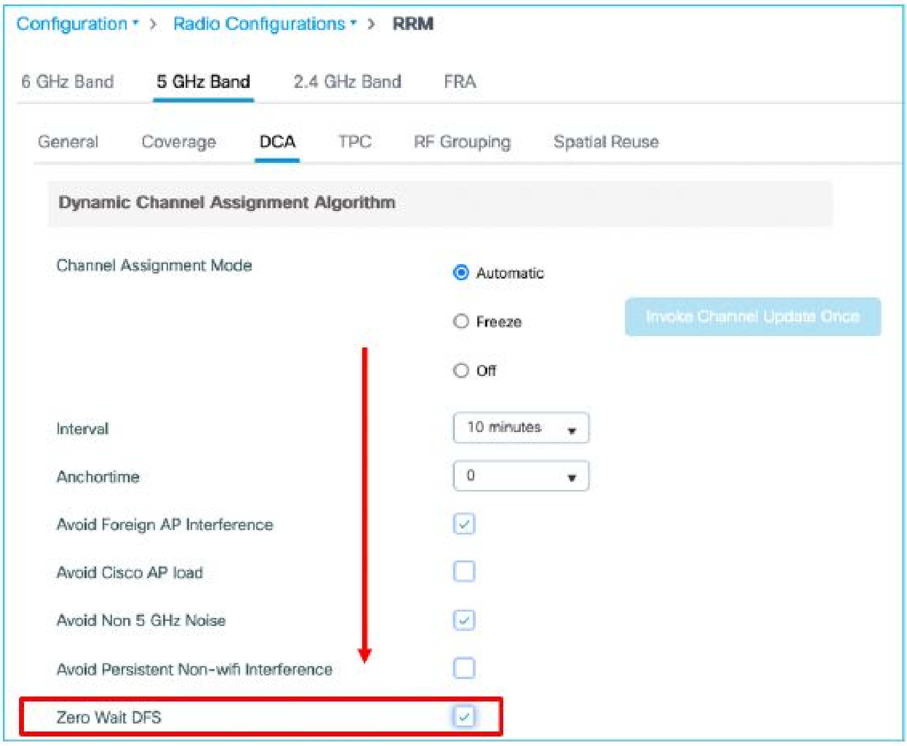
Dual 5 GHz Considerations:
Pre-CAC covers all channels and scenarios for the ETSI region. Rolling CAC for FCC presents a couple of possible scenarios. In FCC we can continuously CAC only one future channel. If both 5 GHz interfaces are assigned DFS channels, then only one can have a fully CAC’d and ready future channel. In the event that we do have two interfaces with DFS channels assigned, the second best channel for each must still maintain 100 MHz separation from the other interfaces channel at all times. In many cases this will end up in a different band all together. In cases where both Future channels are DFS as well, then the interface with the highest number of clients will get the priority for rolling CAC. If the other interface detects radar -its channel change will have to perform a normal CAC (60 seconds) before assuming operations.
Pre-Requisite:

1. C9136I or C9130 -B or -E AP’s
2. C9800 Controller running the 17.11.1 EFT code
3. Console access to the controller

Testing this feature is straight forward. All states can be shown presently in CLI show commands. Configuration can be achieved at the GUI or CLI levels.

Configuration & Verification:
Zero Wait DFS can be enabled at the global level for all AP’s on the WLC or through an RF profile to manage a subset of APs. There is no configuration options for this feature.

To enable Zero Wait DFS on the GUI: On the controller GUI – select Configuration=>RRM=>5 GHz Band=> DCA and choose Zero Wait DFS option, check the box to enable at the global level.



Dynamic Channel Assignment Algorithm

Channel Assignment Mode: ● Automatic ○ Freeze ○ Off

Interval: 10 minutes

Anchortime: 0

Avoid Foreign AP Interference ☑

Avoid Cisco AP load □

Avoid Non 5 GHz Noise ☑

Avoid Persistent Non-wifi Interference □

Zero Wait DFS ☑

To enable Globally from the CLI: C9800-L_17_11(config)#AP dot11 5ghz rrm channel zero-wait-dfs

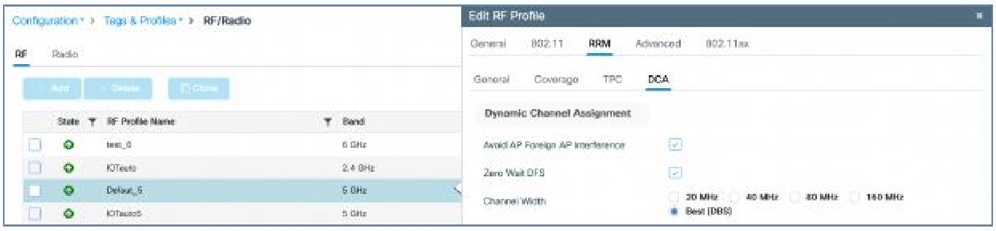
To disable, use the no command: C9800-L_17_11(config)#no AP dot11 5ghz rrm channel zero-waitdfs

In all cases to verify that the feature is globally enabled, use the following show command to determine the current global state for Zero Wait DFS:
C9800-L_17_11#sh ap dot11 5ghz channel | i Zero

- **Zero Wait DFS:** Enabled

NOTE: Enabling Zero Wait DFS will only affect APs that it is supported on, presently just the Catalyst C9130AX AP's. Other APs that are not supported will not be affected by the configuration option.

Enable Zero Wait DFS selectively through an RF Profile:
Zero Wait DFS can also be selectively applied through an RF -Profile allowing granular selection of a subset of APs for which this setting will apply.
There is no prerequisite for enabling at the global level:
From the GUI, navigate from the main menu to: Configuration=> Tags & Profiles => RF/Radio Select the 5 GHz RF Profile to modify or create a new one and select RRM/DCA and check Zero Wait DFS check box.



	State	RF Profile Name	Band
□	●	test_6	6 GHz
□	●	IOTests	2.4 GHz
□	●	Default_5	5 GHz
□	●	IOTests5	5 GHz

Dynamic Channel Assignment

Avoid AP Foreign AP Interference ☑

Zero Wait DFS ☑

Channel Width: ○ 20 MHz ○ 40 MHz ○ 80 MHz ○ 160 MHz ● Best (DBS)

To enable Zero Wait DFS in an RF Profile from the CLI:

- C9800-L_17_11(config)#ap dot11 5ghz rf-profile <profile name>
- C9800-L_17_11(config-rf-profile)#channel zero-wait-dfs
- C9800-L_17_11(config-rf-profile)#no channel zero-wait-dfs

To verify the state of Zero Wait DFS for an individual AP, use the following show commands:

C9800-L_17_11#sh ap name C9130i_9f.6e.a0 config slot 1 | s Zero

- Zero Wait DFS Parameters
  - Zero Wait DFS Capable: Yes
  - CAC Domain: FCC
  - Zero Wait DFS Enabled: Enabled
  - DFS Channel Inclusion list: 60,64,104
- DFS Channel Exclusion list: 52,56,100,108,112,116,120,124,128,132,136,140,144
- Pre-CAC Status: NA (this is FCC so there is no Pre-CAC capability)
- Reserved Channel CAC Status : In Progress (indicates that off channel scanning is being run)
- Reserved Channel: 108
- Reserved Channel Width: 40 M

The Example above is for an FCC AP below is the example for ETSI

AIRV_VWLC2#sh ap name AP1416.9D28.0CC4 config slot 1 | s Zero

- Zero Wait DFS Parameters
  - Zero Wait DFS Capable: Yes
  - CAC Domain: ETSI
  - Zero Wait DFS Enabled: Enabled
  - DFS Channel Inclusion list: 52,132
  - DFS Channel Exclusion list: 56,60,64,100,104,108,112,116,136,140
  - Pre-CAC Status: In progress (ETSI
- **Pre-CAC, running)**
  - **Reserved Channel CAC Status:** In Progress (indicates that off-channel scanning is being run)
  - Reserved Channel: 100
  - Reserved Channel Width: 20 MHz

Testcases:

In order to test Zero Wait DFS, follow the steps below.

Note: It is important to match the suggested configuration as the test radar command on the AP only operates on a 20 MHz channel, using this against an AP with wider channels can get unpredictable results.

To test either FCC or ETSI

1. 1. Configure the AP for a single slot 5 GHz. Either turn off tri-band mode (operate as 8×8) or disable the slot 2 radio.
2. 2. Ensure that Zero Wait DFS is configured and that a reserve channel has been selected
   1. C9800-L_17_11#sh ap name <AP-Name> config slot 1 | s Zero Zero Wait DFS Parameters
      - Zero Wait DFS Capable CAC Domain: Yes : FCC

- Zero Wait DFS Enabled: Enabled
- DFS Channel Inclusion list DFS Channel Exclusion list: 52,60 : 56,64,100,104,108,112,116,120,124,128,132,136,140,144
- Pre-CAC Status Reserved Channel CAC Status: NA : Complete
- Reserved Channel Reserved Channel Width: 60 : 20 MHz

3. 3. On the AP CLI execute the Test Spectrum Radar command test spectrum radar signal dot11Radio 1 center-frequency <MHz> bandwidth 20 The Center Frequency of the 20 MHz channel assignment needs to be entered in MHz. for channel 52, this value is 5260 MHz, channel bandwidth should be set to 20 MHz.
4. 4. Once the radar signal is triggered the AP should resume operations on the "reserve" channel immediately, without the usual 60 second CAC delay.
    1. C9800-L_17_11#sh ap name C9130i_9f.6e.a0 config slot 1 | s Zero
        1. Zero Wait DFS Parameters Zero Wait DFS Capable CAC Domain: Yes : FCC
        2. Zero Wait DFS Enabled: Enabled
        3. DFS Channel Inclusion list: 60 New
    2. Operating channel the former reserve channel
        1. DFS Channel Exclusion list: 52,56,64,100,104,108,112,116,120,124,128,132,136,140,144
        2. Pre-CAC Status: NA
        3. Reserved Channel CAC Status: In
    3. Progress CAC is in progress for the new Reserve Channel
        1. Reserved Channel: 56
    4. Channel 56 will be the new reserve channel
        1. Reserved Channel Width: 20 MHz

Unable to query OIDs from CISCO-LWAPP-AP-MIB on 9800Migration halted Feature Overview:
This is a AireOS parity Feature. Few AP MIB OIDs are missing in C9800 WLCs. This feature is to add support of those missing OIDs.

Pre-Requisite:
No specific pre-requisite needed. SNMP should be enabled in the C9800.

Configuration & Verification:

1. Bring up a C9800 with the latest validated EFT image provided through EFT program.
2. Connect an access point to this C9800
3. Create a WLAN and connect a client to this WLAN
4. Configure the SNMP communities(read/write)
5. Make sure the C9800 is responding to the SNMP queries
6. Validate the following latest introduced OIDs (walk/get/get next/set)
    1. cLApSlotWlanStats
    2. cLApRadioWlanInfoEntry
    3. cLApActiveClientCount
    4. cLApAssociatedClientCount
    5. cLApMemoryCurrentUsage
    6. cLApMemoryAverageUsage
    7. cLApCpuCurrentUsage

8. cLApCpuAverageUsage
9. cLApGlobalAPConnectCount
10. clsSysApConnectCount
11. cLApWlanStatsAssocClientNum
12. cLApWlanStatsOnlineUserNum

SNMP OIDs – Phase 2 Feature Overview:
This feature is to cater customer request to support few SNMP variables which are useful for 9800 deployments.

Following are the new OID additions:

- bsnDot11EssNumberOfMobileStations
- bsnDot11EssNumApsUp
- bsnDot11EssNumApsDown
- bsnAPOperationStatus
- cLApUpTime
- bsnGlobalDot11SystemMobileStations
- cLApGlobalAPConnectCount

Pre-Requisite:

- Cisco Catalyst 9800 Wireless LAN Controller running IOS XE 17.11.1
- SNMP manager should be enabled
- Private or Public SNMP community should be configured

Configuration & Verification:
Start with verifying if SNMP manager is enabled and communities are added on the Cisco Catalyst 9800 controller.

- sri-dao#sh run | i
- snmp snmp-server group v3_ro_users v3 priv read preview
- snmp-server group v3_rw_users v3 priv write preview
- snmp-server view preview is included
- snmp-server community public RO
- snmp-server community private RW
- snmp-server community test RW
- snmp-server trap-source Vlan8
- snmp-server packet size 5000
- snmp-server enable traps
- snmp authentication link down linkup coldstart warm start
- snmp-server enables traps wireless wireless_mobility
- snmp-server enable traps config
- snmp-server enables traps rf
- snmp-server host 10.104.174.58 public
- SNMP-server host 9.2.14.175 public

- SNMP-server host 9.5.11.19 public
- SNMP-server manager
  - field phy_ ht_cfg.cfg_data. snmp_freq_string
  - field radio_oper_data.phy_ht_cfg.cfg_data. snmp_freq_string
  - field radio_oper_data.phy_ht_cfg.cf8_data. snmp_ freq_string

OID Verification on Cisco Catalyst 9800 Controller:
Use these commands on 9800 CLI

SNMP Response: reqid 25, errstat 17, erridx 1 cLApGlobalAPConnectCount.0 = 4

Documents / Resources

 IOS-XE 17.11.1 Wireless EFT Guide TME Team	CISCO IOS-XE Wireless EFT [pdf] User Manual IOS-XE Wireless EFT, IOS-XE Wireless EFT, Wireless EFT, EFT, IOS-XE

References

- Software Download - Cisco Systems
- Software Download - Cisco Systems
- Software Download - Cisco Systems
- Software Download - Cisco Systems
- Software Download - Cisco Systems
- Software Download - Cisco Systems
- Software Download - Cisco Systems
- Software Download - Cisco Systems
- Wireless Network, Wi-Fi Networking, and Mobility Solutions - Cisco