



Oil and Gas Refinery WLAN MESH

Implementation Guide

August 2020



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS DESCRIBED IN THIS DOCUMENT ARE SUBJECT TO CHANGE WITHOUT NOTICE. THIS DOCUMENT IS PROVIDED “AS IS.”

ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS, IMPLIED, OR STATUTORY INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, PUNITIVE, EXEMPLARY, OR INCIDENTAL DAMAGES UNDER ANY THEORY OF LIABILITY, INCLUDING WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OF OR INABILITY TO USE THIS DOCUMENT, EVEN IF CISCO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

©2020 CISCO SYSTEMS, INC. ALL RIGHTS RESERVED



Contents

Deployment Models	2
Greenfield Deployment	2
Brownfield Deployment	3
Detailed Configurations of Components	5
Network Flow	5
DHCP Flow for the APs	5
Configuring Switches	7
Wired Network QoS Configuration	11
ISE Configuration—802.1x EAP-FAST Authentication	16
Network Management with Prime Infrastructure and Connected Mobile Experience (CMX) 23	
Guidelines for Preparing Image Files for Use Within Wireless Site Maps	24
Creating a Wireless site map	25
Adding Devices to Prime Infrastructure	27
View Mesh Access Point Configurations Using Wireless Site Maps	30
Integration with CMX	30
Quality of Service (QoS)	32
Detailed Configuration of the Deployment Models	38
Greenfield Deployment Model	38
Configuring HA SSO	38
Configuring Mesh Profile	41
WLAN Configuration	43
AP Join Policy Configuration	46
Policy Profile Creation	48
Tags Configuration	49
NTP Configuration	51
MESH Backhaul Security (MAC Filter)	53
Changing an AP Role	54
Verifying Mesh	54
Ethernet Bridging Configuration	55
WLC 802.1x AAA Server Configuration	58
Brownfield Deployment Model	60
AireOS (8.5) to AireOS (8.10) Deployment	60
AireOS (8.5) to Catalyst 9800 (17.1.1s) Deployment	85

Use Cases	89
Remote Access	89
Emerson WiHart for condition-based monitoring	89
Video Surveillance	91
Location Services and Asset Tracking	91
Troubleshooting	92
Appendix A: Integrating Emerson 1410S Gateway with IW6300	94
Configuring Power Over Ethernet Out Functionality	95



Oil and Gas Refinery WLAN MESH Implementation Guide

The designs described in this Oil & Gas Refinery (O&G) WLAN MESH Implementation Guide have been conceived and validated to address oil & gas field and refinery plant stringent requirements. In the environment where heavy metal infrastructures, high temperatures, extreme moisture, and potential explosive materials are consistently present. A typical O&G field and refinery plant can employ environmental sensors, asset tags, personnel tracking RFID tags, and equipment and process monitoring devices, enabling operators to predict maintenance, optimize workflow, meet CAPEX and OPEX requirements, and successfully operate the facility 24x7x365.

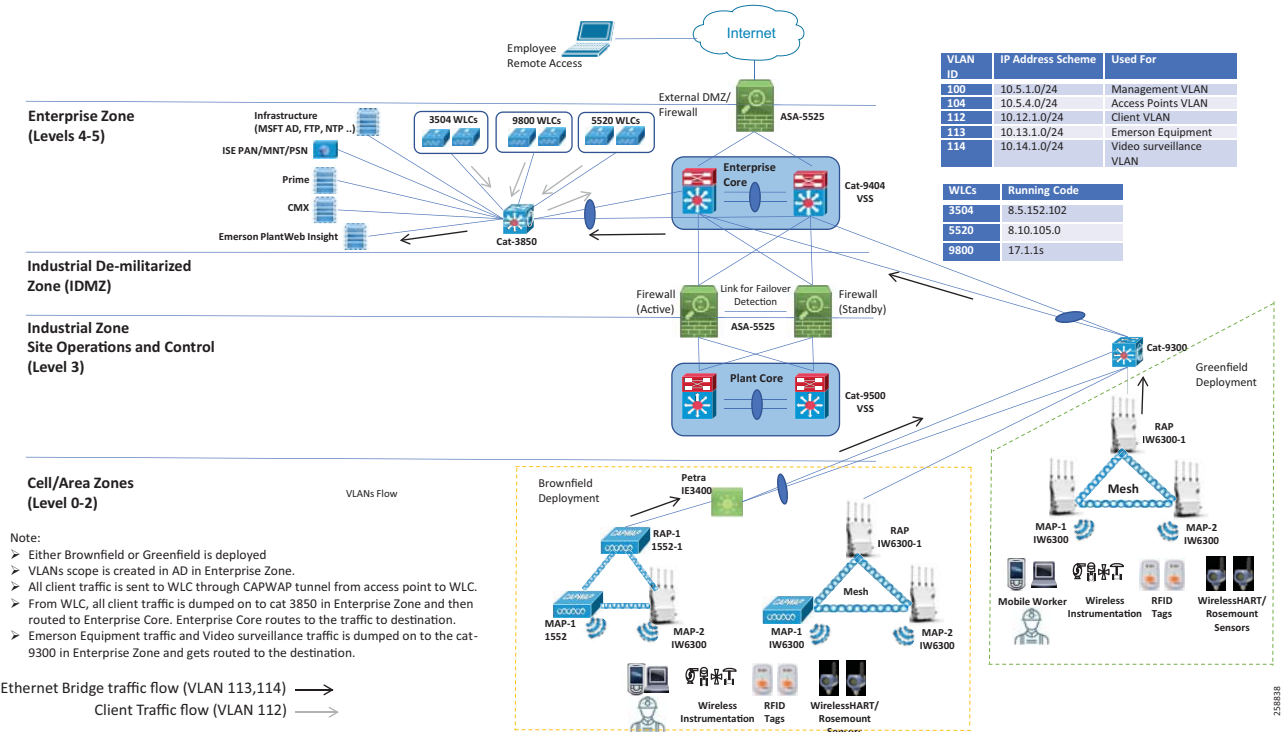
The Cisco Hazloc certified class 1 WLAN MESH network solution consists of the following components as shown in [Figure 1](#), including:

- Industrial heavy duty 1552/IW6300 lightweight Access Points (APs)
- Catalyst Access Switches (C3850, C9300, C9400)
- Industrial Ethernet Switches (IE3300, IE3400, IE3500)
- Cisco Connected Mobile Experiences (CMX) or Cisco Mobility Service Engine (MSE)
- Cisco Prime Collaboration (PI)
- Identity Services Engine (ISE)
- Active Directory and External DHCP Server
- AireOS wireless controllers in SSO running 8.5.152.102

Note: Contact the Cisco Technical Assistance Center (TAC) or send an email to wnbu-escalation@cisco.com to receive the Cisco AireOS 8.5 IRCM image based on the 8.5 Maintenance Release software.

- AireOS Wireless controllers in SSO running 8.10.105
- Cisco Catalyst 9800 Series Wireless Controllers in SSO running 17.1.1s
- Emerson Hazardous Area Equipment

Figure 1 Oil and Gas Refinery WLAN MESH End-to-End Validation Topology



Deployment Models

Historically, O&G field and refinery customers have deployed WLAN MESH mainly with 1552 Access points. Many new features and improvements have been integrated into the CAPWAP IW6300; O&G operators can plan transition to seamlessly replace 1552 Access points with IW6300 LAP using this Cisco Validated Design (CVD).

A successful transition must meet the following requirements:

- No interruption to daily operation
- In-transition coexistence of 1552 & IW6300; after-transition environment using only IW6300
- Infrastructure operation support for third-party equipment: Emerson Rosemount WiHART, and others.
- Continue to meet performance Key Performance Indicators (KPIs) throughout the transition

The focus of this document is:

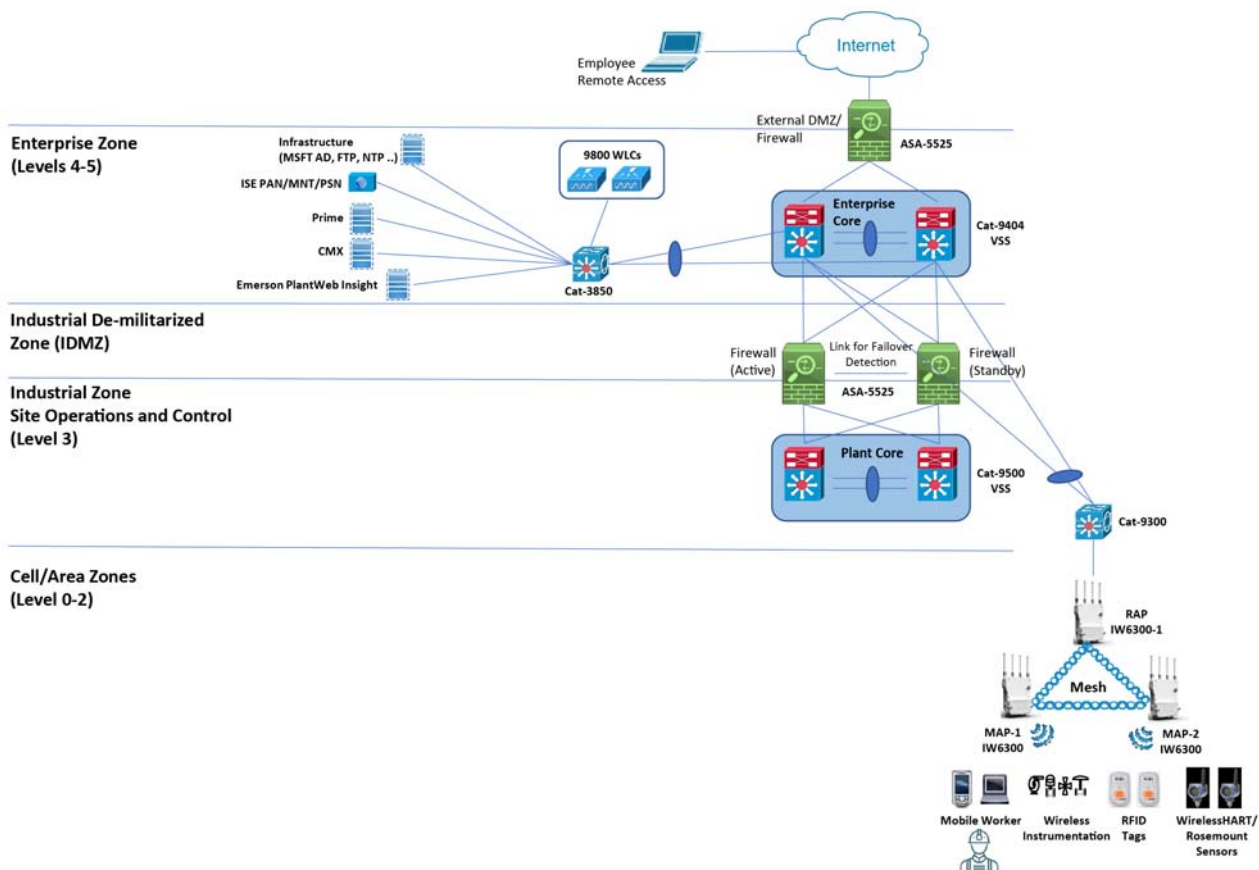
- Deploying a new wireless network in O&G fields and refineries with IW6300 access points (Greenfield Deployment).
- Expanding an existing 1552 Access points network with the new IW6300 (Brownfield Deployment).

Greenfield Deployment

For Greenfield scenarios, using Cisco Catalyst 9800 WLCs with the Cisco IW6300 Heavy Duty Access Points in a Mesh deployment is recommended. Multiple Root Access Points (RAPs) can be used for redundancy.

For Emerson Sensor and video surveillance use cases, the Emerson Gateways or the IP cameras directly connected to the IW6300 Mesh Access points (MAPs) are recommended. More details about the Greenfield deployment are given in a later section.

Figure 2 Greenfield Deployment



Brownfield Deployment

The Brownfield deployment model shows expanding the existing network with Cisco IW6300 Heavy Duty Access Points or replacing the existing 1552 Access Points (APs) with the new Cisco IW6300 APs. The eventual goal is to phase out all 1552 Access points with IW6300 Access points.

This deployment model uses two pairs of controllers running different code versions. Existing 1552 APs network is compatible with the AireOS controllers running 8.5 code. The IW6300 is compatible with the Cisco Catalyst 9800 WLCs or the AireOS controllers running 8.10 code.

The following two Brownfield deployment models have been validated for this design:

- 3504 wireless controllers running IRCM 8.5 code and 5520 wireless controllers running 8.10 code
- 3504 wireless controllers running IRCM 8.5 code and Cisco Catalyst 9800 Series Wireless Controller running 17.1.1s

Deployment Models

Figure 3 Brownfield Deployment with WLC3504 and Cat9800

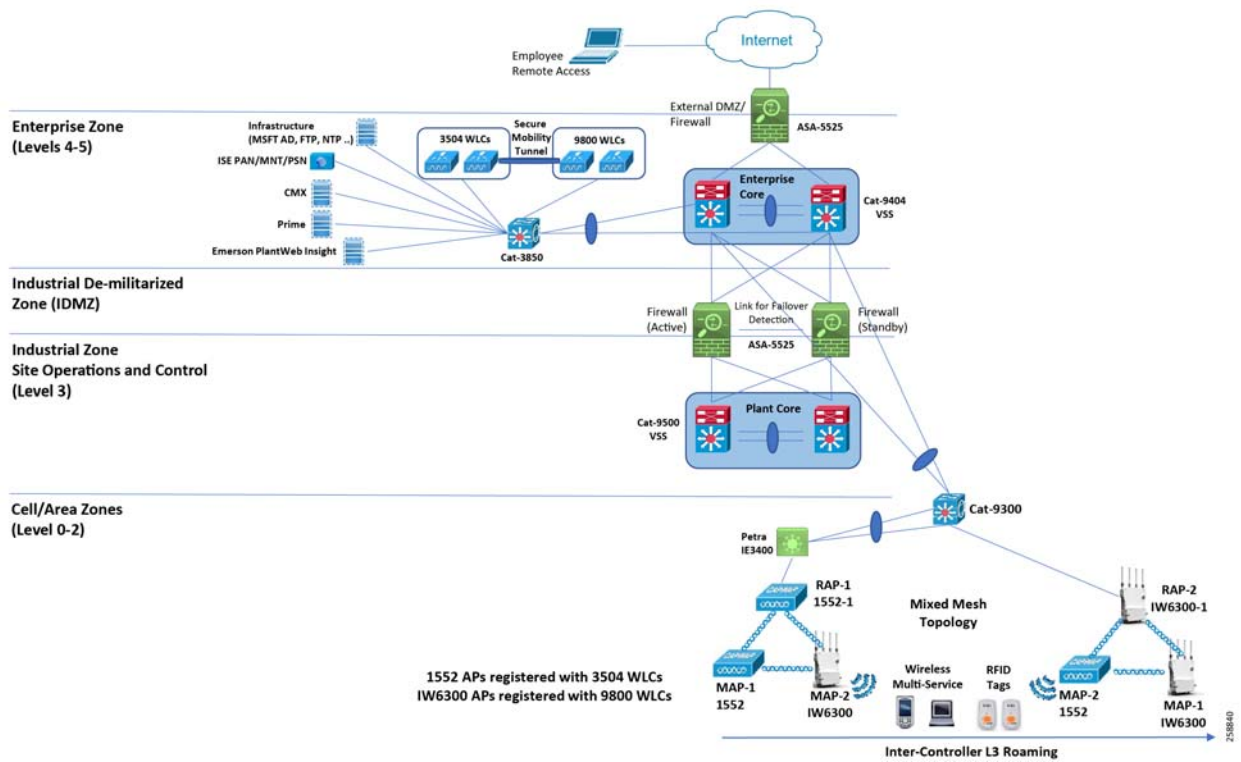
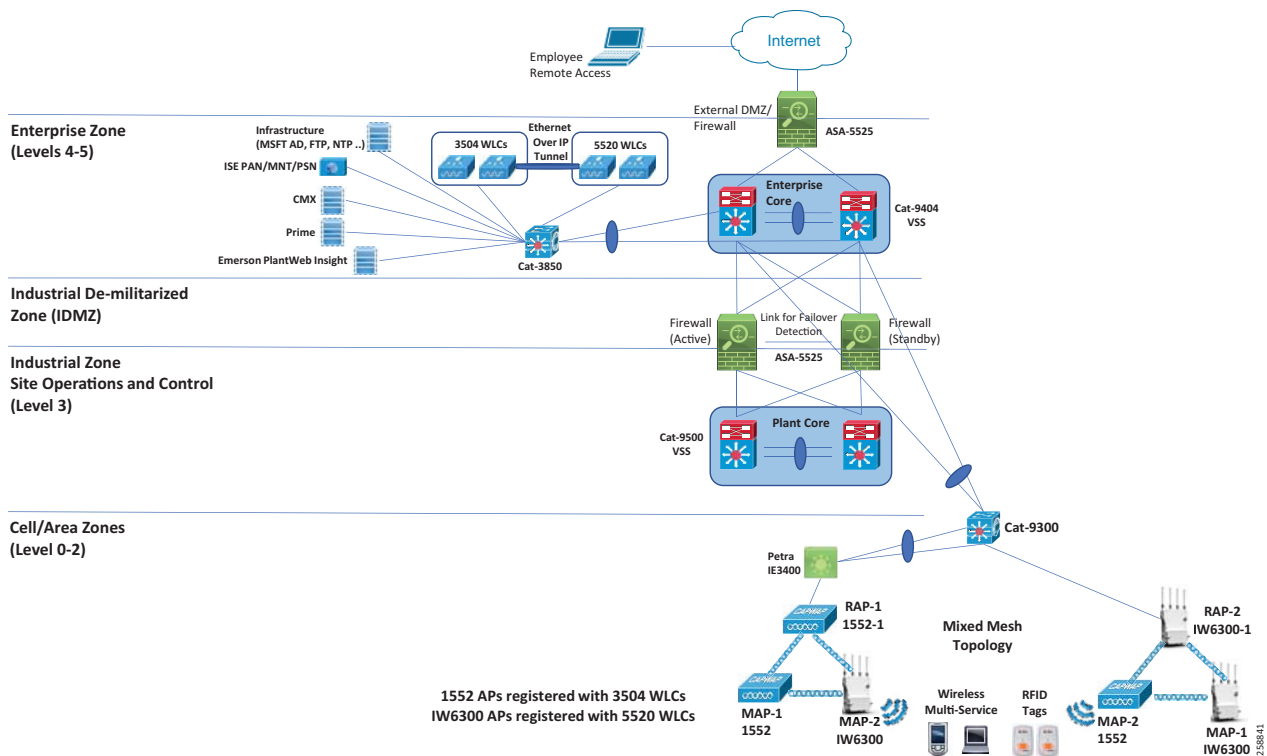


Figure 4 Brownfield Deployment with WLC3504 and WLC5520



Detailed Configurations of Components

Network Flow

The VLANs in [Table 1](#) were used in the testbed; refer to the topology in [Figure 4](#) for details.

Table 1 VLANs Used in the Testbed

VLAN ID	IP Address Scheme	Used For
100	10.5.1.0/24	Management VLAN
104	10.5.4.0/24	Access Points VLAN
112	10.12.1.0/24	Client VLAN
113	10.13.1.0/24	Emerson Equipment
114	10.14.1.0/24	Video surveillances VLAN

DHCP Flow for the APs

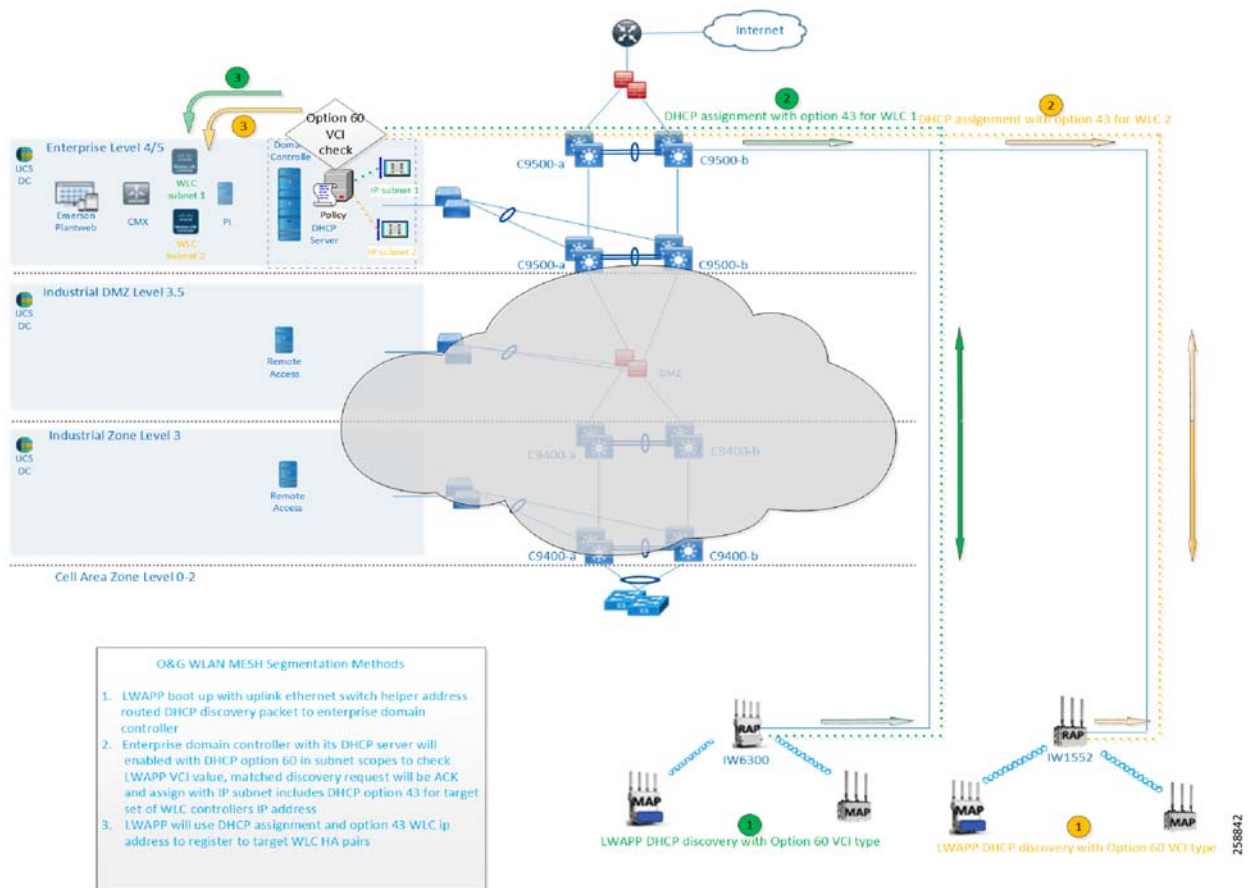
Two Dynamic Host Configuration Protocol (DHCP) options enable the WLAN MESH Network on the APs during the registration process to pass the Virtual Channel Identifier (VCI) using different methods. The options are:

- DHCP Option 43

Detailed Configurations of Components

- DHCP Option 60
- The DHCP option 43 defines vendor-specific information using Type-Length-Value (TLV) pairs to inform LAP with the Wireless LAN Controller (WLC) IP address.
- DHCP Option 60 – When the DHCP Server in the local domain controller is enabled with the VCI, Option 60 DHCP identifier service, the operation is:
 - a. Each LLAP boots up with the IP helper address on access switch interface configuration, and sends a discovery message to the DHCP server.
 - b. The DHCP server scope filter parses LAP VCI information and forwards it to the appropriate DHCP scope.
 - c. The DHCP scope is assigned to the correct IP subnet, which is reflected on the WLC HA pair management interface.

Figure 5 Mesh Segmentation with DHCP Option 43 and 60



Configuring Switches

Cisco C9400

The Cisco C9400 switch is located at the O&G enterprise network layer. It serves as a connection switch between the enterprise data center Layer 2 and Layer 3 edge network device. To set up the C9400 switch:

1. Enable privileged EXEC mode and enter your password when prompted.

```
Device> enable
```

2. Enter global configuration mode.

```
Device#configure terminal
```

3. Create a VLAN.

```
vlan <id>  
name <vlan name>
```

For example:

```
IA-Ent-9404(config)#vlan 112  
IA-Ent-9404(config-vlan)#name client-vlan
```

4. Create a VLAN interface.

```
int vlan <id>  
ip address <ipaddress><subnetmask>
```

For example:

```
IA-Ent-9404(config)#int vlan 112  
IA-Ent-9404(config-if)#ip address 10.12.1.1 255.255.255.0
```

5. Create a channel group.

```
int <name>  
channel-group <port channel id> mode active
```

For example:

```
IA-Ent-9404(config)#int Giga-bitEthernet1/1/0/1  
IA-Ent-9404(config-if)#channel-group 100 mode active  
Creating a port-channel interface Port-channel 100
```

6. Create a port channel interface.

```
interface Port-channel <id>  
switchport mode trunk  
switchport trunk allowed vlan id <vlan id>
```

For example:

```
IA-Ent-9404(config)# interface Port-channel 100  
IA-Ent-9404(config-if)#switchport mode trunk  
IA-Ent-9404(config-if)#switchport trunk allowed vlan 100,112
```

7. Configure EIGRP routing.

```
router eigrp <id>  
network <network><subnet>
```

Detailed Configurations of Components

```
passive-interface default
no passive-interface <interface-Name/Vlan id>
eigrp router-id <ip address>
```

Cisco C9300

The C9300 switch is located at the O&G industrial network layer. It serves as a distribution network feeder switch for the MESH WLAN network infrastructure. To set up the C9300 switch:

1. Enable privileged EXEC mode and enter your password when prompted.

```
Device> enable
```

2. Enter global configuration mode.

```
Device#configure terminal
```

3. Create a VLAN.

```
vlan <id>
name <vlan name>
```

For example:

```
IA-OG-C9300(config)#vlan 104
IA-OG-C9300(config-vlan)#name VLAN0104
```

4. Create a VLAN interface.

```
IA-OG-C9300(config)#int vlan <id>
IA-OG-C9300(config-if)#ip address <ip address of the switch><subnet mask>
```

For example:

```
IA-OG-C9300(config)#int vlan 104
IA-OG-C9300(config-if)#ip address 10.5.4.1 255.255.255.0
IA-OG-C9300(config-if)#ip helper-address 10.5.1.20
```

5. Configure this port as a trunk port. This port is connected to a Wireless LAN Controller.

```
description connected 3504-wlc-1
switchport trunk allowed vlan <ids>
switchport mode trunk
```

For example:

```
IA-OG-C9300(config)#interface TenGigabitEthernet1/0/42
IA-OG-C9300(config-if)# switchport trunk allowed vlan 100,112
IA-OG-C9300(config-if)# switchport mode trunk
```

6. Create a channel group.

```
int <name>
channel-group <port channel id> mode active
```

For example:

```
IA-OG-C9300(config)#int TwoGigabitEthernet1/0/2
IA-OG-C9300(config-if)#channel-group 101 mode active
Creating a port-channel interface Port-channel 101
```

7. Configure interfaces in the port channel.

```
interface Port-channel <id>
```

Detailed Configurations of Components

```
switchport mode trunk
switchport trunk allowed vlan id <vlan id>
```

For example:

```
IA-OG-C9300(config)# inter-face Port-channel 101
IA-OG-C9300(config-if)#switchport mode trunk
IA-OG-C9300(config-if)#switchport trunk native vlan 101
IA-OG-C9300(config-if)#switchport trunk allowed vlan 101
```

8. Configure EIGRP routing.

```
router eigrp <id>
network <network><subnet>
passive-interface default
no passive-interface <interface-Name/Vlan id>
eigrp router-id <ip address>
```

9. Configure this port as trunk port. This port is connected to the Root Access Point.

```
interface <name>
description connected to root ap
switchport mode trunk
switchport trunk native vlan <id>
switchport trunk allowed vlan <ids>
```

For example:

```
IA-OG-C9300(config)# inter-face interface TwoGigabitEther-net1/0/5
IA-OG-C9300(config-if)#description Connected to Duplo RTP-06-1FL-6300R01
IA-OG-C9300(config-if)#switchport mode trunk
IA-OG-C9300(config-if)#switchport trunk native vlan 104
IA-OG-C9300(config-if)#switchport trunk allowed vlan 104,113
```

Cisco C3850

The C3850 switch is located at the O&G enterprise network layer. It serves as an enterprise data center access switch for hosting the Wireless LAN Controller, AD domain controller, ISE, the remote access network server, and so on. To setup the C3850 switch:

1. Enable privileged EXEC mode and enter your password when prompted.

```
Device> enable
```

2. Enter global configuration mode.

```
Device#configure terminal
```

3. Create a VLAN.

```
vlan <id>
name <vlan name>
```

For example:

```
IA-OG-C3850(config)#vlan 112
IA-OG-C3850(config-vlan)#name client-vlan
```

4. Create a VLAN interface.

```
Int vlan <id>
Ip address <ipad-dress><subnetmask>
```

Detailed Configurations of Components

For example:

```
IA-OG-C3850(config)#int vlan 112
IA-OG-C3850(config-if)#ip address 10.12.1.1 255.255.255.0
```

5. Configure this port as a trunk port. This port is connected to Wireless LAN Controller.

```
interface <name>
description connected 3504-wlc-1
switchport trunk allowed vlan <ids>
switchport mode trunk
```

For example:

```
IA-OG-C3850(config)#interface TenGigabitEthernet1/0/42
IA-OG-C3850(config-if)# switchport trunk allowed vlan 100,112
IA-OG-C3850(config-if)# switchport mode trunk
```

6. Create a channel group.

```
int <name>
channel-group <port channel id> mode active
```

For example:

```
IA-OG-C3850(config)#int TenGigabitEthernet1/0/47
IA-OG-C3850(config-if)# chan-nel-group 100 mode active
Creating a port-channel interface Port-channel 100
```

7. Configuring the port channel also configures interfaces in the port channel.

```
interface Port-channel <id>
switchport mode trunk
switchport trunk allowed vlan id <vlan id>
```

For example:

```
IA-OG-C3850(config)# interface Port-channel 100
IA-OG-C3850(config-if)#switchport mode trunk
IA-OG-C3850(config-if)#switchport trunk allowed vlan 100
```

Cisco IE3400

The IE3400 is at the O&G industrial network layer. It serves as a distribution network device for the MESH WLAN network infrastructure. Configure the IE3400 following the steps below.

1. Enable privileged EXEC mode and enter your password when prompted.

```
Device> enable
```

2. Enter the global configuration mode.

```
Device#configure terminal
```

3. Create a VLAN.

```
vlan <id>
Name <vlan name>
```

For example:

```
IA-OG-IE3400(config)#vlan 104
IA-OG-IE3400(config-vlan)#name VLAN0104
```

Detailed Configurations of Components

4. Create a channel group.

```
int <name>
channel-group <port channel id> mode active
```

For example:

```
IA-OG-IE3400(config)#int Gi-gabitEthernet1/4
IA-OG-IE3400(config-if)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1
```

5. Create a port channel interface.

```
interface Port-channel <id>
switchport mode trunk
switchport trunk allowed vlan id <vlan id>
```

For example:

```
IA-OG-IE3400(config)# inter-face Port-channel 1
IA-OG-IE3400(config-if)#switchport mode trunk
IA-OG-IE3400(config-if)#switchport trunk native vlan 104
IA-OG-IE3400(config-if)#switchport trunk allowed vlan 104,113
```

6. Configure this port as trunk port. This port is connected to a Root Access Point.

```
interface <name>
switchport trunk native vlan <id>
switchport trunk allowed vlan <ids>
switchport mode trunk
```

For example:

```
IA-OG-IE3400(config)# inter-face interface TwoGigabitEther-net1/0/5
IA-OG-IE3400(config-if)#switchport mode trunk
IA-OG-IE3400(config-if)#switchport trunk native vlan 104
IA-OG-IE3400(config-if)#switchport trunk allowed vlan 104,113
```

Wired Network QoS Configuration

Cisco C9300

The C9300 is also used as a network segmentation switch. To setup the C9300 as a segmentation switch:

```
!
!
access-list 101 permit udp any eq 2222 any dscp 55
access-list 102 permit udp any eq 2222 any dscp 47
access-list 103 permit udp any eq 2222 any dscp 43
access-list 104 permit udp any eq 2222 any
access-list 105 permit udp any eq 44818 any
access-list 105 permit tcp any eq 44818 any
access-list 106 permit udp any eq 319 any
access-list 107 permit udp any eq 320 any
!
policy-map CIP-PTP-Traffic
class CIP-Implicit_dscp_55
set qos-group 1
class CIP-Implicit_dscp_47
set qos-group 1
class CIP-Implicit_dscp_43
```

Detailed Configurations of Components

```
    set qos-group 1
class CIP-Implicit_dscp_any
    set qos-group 2
class CIP-Other
    set qos-group 2
class 1588-PTP-Event
    set qos-group 0
class 1588-PTP-General
    set qos-group 1
!
policy-map PTP-Event-Priority
class qos-group-0
    priority level 1
class qos-group-1
    bandwidth remaining percent 40
class qos-group-2
    bandwidth remaining percent 40
class class-default
    bandwidth remaining percent 20
!
class-map match-any 1588-PTP-General
    match access-group 107
class-map match-any 1588-PTP-Event
    match access-group 106
class-map match-any CIP-Other
    match access-group 105
class-map match-any CIP-Implicit_dscp_any
    match access-group 104
class-map match-any CIP-Implicit_dscp_43
    match access-group 103
class-map match-any CIP-Implicit_dscp_47
    match access-group 102
class-map match-any CIP-Implicit_dscp_55
    match access-group 101
!
class-map match-any qos-group-2
    match qos-group 2
class-map match-any qos-group-1
    match qos-group 1
class-map match-any qos-group-0
    match qos-group 0
!
interface TwoGigabitEthernet1/0/1
description Connect to IA-Ent-9404 GigabitEthernet1/1/0/2
switchport trunk native vlan 101
switchport trunk allowed vlan 101
switchport mode trunk
channel-group 101 mode active
service-policy output PTP-Event-Priority
!
interface TwoGigabitEthernet1/0/2
description Connect to IA-Ent-9404 GigabitEthernet2/1/0/2
switchport trunk native vlan 101
switchport trunk allowed vlan 101
switchport mode trunk
channel-group 101 mode active
service-policy output PTP-Event-Priority
!
interface TwoGigabitEthernet1/0/3
description Connected to IE-3400
switchport trunk native vlan 104
switchport trunk allowed vlan 104,113,150
switchport mode trunk
channel-group 102 mode active
service-policy output PTP-Event-Priority
```


Detailed Configurations of Components

```

!
interface TwoGigabitEthernet1/0/4
description Connected to IE-3400
switchport trunk native vlan 104
switchport trunk allowed vlan 104,113,150
switchport mode trunk
channel-group 102 mode active
service-policy output PTP-Event-Priority
!
interface TwoGigabitEthernet1/0/5
description Connected to Duplo RTP-06-1FL-6300R01
switchport trunk native vlan 104
switchport trunk allowed vlan 104,113,150
switchport mode trunk
service-policy input CIP-PTP-Traffic
service-policy output PTP-Event-Priority
!
interface TwoGigabitEthernet1/0/6
description Connected to Duplo RTP-06-1FL-6300R02
switchport trunk native vlan 104
switchport trunk allowed vlan 104,113,150
switchport mode trunk
service-policy input CIP-PTP-Traffic
service-policy output PTP-Event-Priority
!

```

Cisco C3850

The C3850 is also used as a enterprise data center layer 2 access network switch. To setup the C3850 for this usage:

```

!
access-list 101 permit udp any eq 2222 any dscp 55
access-list 102 permit udp any eq 2222 any dscp 47
access-list 103 permit udp any eq 2222 any dscp 43
access-list 104 permit udp any eq 2222 any
access-list 105 permit udp any eq 44818 any
access-list 105 permit tcp any eq 44818 any
access-list 106 permit udp any eq 319 any
access-list 107 permit udp any eq 320 any
!
policy-map CIP-PTP-Traffic
class CIP-Implicit_dscp_55
set qos-group 1
class CIP-Implicit_dscp_47
set qos-group 1
class CIP-Implicit_dscp_43
set qos-group 1
class CIP-Implicit_dscp_any
set qos-group 2
class CIP-Other
set qos-group 2
class 1588-PTP-Event
set qos-group 0
class 1588-PTP-General
set qos-group 1
!
policy-map PTP-Event-Priority
class qos-group-0
priority level 1
class qos-group-1
bandwidth remaining percent 40
class qos-group-2

```

Detailed Configurations of Components

```
    bandwidth remaining percent 40
class class-default
    bandwidth remaining percent 20
!
class-map match-any 1588-PTP-General
    match access-group 107
class-map match-any 1588-PTP-Event
    match access-group 106
class-map match-any CIP-Other
    match access-group 105
class-map match-any CIP-Implicit_dscp_any
    match access-group 104
class-map match-any CIP-Implicit_dscp_43
    match access-group 103
class-map match-any CIP-Implicit_dscp_47
    match access-group 102
class-map match-any CIP-Implicit_dscp_55
    match access-group 101
!
class-map match-any qos-group-2
    match qos-group 2
class-map match-any qos-group-1
    match qos-group 1
class-map match-any qos-group-0
    match qos-group 0
!
interface GigabitEthernet1/0/1
    description Connected to IA-Ent-9404 Gig 1/1/0/1
    switchport trunk native vlan 100
    switchport trunk allowed vlan 100,111,112
    switchport mode trunk
    channel-group 100 mode active
    service-policy output PTP-Event-Priority
!
interface GigabitEthernet1/0/2
    description Connected to IA-Ent-9404 Gig 2/1/0/1
    switchport trunk native vlan 100
    switchport trunk allowed vlan 100,111,112
    switchport mode trunk
    channel-group 100 mode active
    service-policy output PTP-Event-Priority
!
interface TenGigabitEthernet1/0/41
    description connected 3504-wlc-10.5.1.54
    switchport trunk allowed vlan 12,100,112
    switchport mode trunk
    service-policy output PTP-Event-Priority
!
interface TenGigabitEthernet1/0/42
    description connected 3504-wlc-10.5.1.53
    switchport trunk allowed vlan 100,112
    switchport mode trunk
    service-policy output PTP-Event-Priority
!
interface TenGigabitEthernet1/0/43
    description connect to 5520-wlc2-up-.55 (old)
    switchport trunk allowed vlan 100,112
    switchport mode trunk
    service-policy output PTP-Event-Priority
!
interface TenGigabitEthernet1/0/44
    description connect to 5520-wlc2-up-.55 (old)
    switchport trunk allowed vlan 100,112
    switchport mode trunk
    service-policy output PTP-Event-Priority
```

Detailed Configurations of Components

```

!
interface TenGigabitEthernet1/0/45
  description connect to 9800-wlc-1-top
  switchport trunk native vlan 100
  switchport trunk allowed vlan 11,100,111,112
  switchport mode trunk
  shutdown
  service-policy output PTP-Event-Priority
!
interface TenGigabitEthernet1/0/46
  description connect to 9800-wlc-2-bottom
  switchport trunk native vlan 100
  switchport trunk allowed vlan 11,100,111,112
  switchport mode trunk
  shutdown
  service-policy output PTP-Event-Priority
!

```

Cisco IE3400

Use the IE3400 as an industrial cell area zone distribution switch. To setup the IE3400:

```

!
access-list 101 permit udp any eq 2222 any dscp 55
access-list 102 permit udp any eq 2222 any dscp 47
access-list 103 permit udp any eq 2222 any dscp 43
access-list 104 permit udp any eq 2222 any
access-list 105 permit udp any eq 44818 any
access-list 105 permit tcp any eq 44818 any
access-list 106 permit udp any eq 319 any
access-list 107 permit udp any eq 320 any
!
policy-map CIP-PTP-Traffic
  class CIP-Implicit_dscp_55
    set ip dscp 55
  class CIP-Implicit_dscp_47
    set ip dscp 47
  class CIP-Implicit_dscp_43
    set ip dscp 43
  class CIP-Implicit_dscp_any
    set ip dscp 31
  class CIP-Other
    set ip dscp 27
  class 1588-PTP-Event
    set ip dscp 59
  class 1588-PTP-General
    set ip dscp 47
!
policy-map PTP-Event-Priority
  class class-0
    priority
  class class-1
    bandwidth remaining percent 40
  class class-2
    bandwidth remaining percent 20
  class class-default
    bandwidth remaining percent 40
!
class-map match-all 1588-PTP-General
  match access-group 107
class-map match-all 1588-PTP-Event
  match access-group 106
class-map match-all CIP-Other

```

Detailed Configurations of Components

```
match access-group 105
class-map match-all CIP-Implicit_dscp_any
match access-group 104
class-map match-all CIP-Implicit_dscp_43
match access-group 103
class-map match-all CIP-Implicit_dscp_47
match access-group 102
class-map match-all CIP-Implicit_dscp_55
match access-group 101
!
class-map match-all class-2
match ip dscp ef
class-map match-all class-1
match ip dscp 47
class-map match-all class-0
match ip dscp 59
!
interface GigabitEthernet1/3
description Connected to IA-OG-C9300
switchport trunk native vlan 104
switchport trunk allowed vlan 104,113,150
switchport mode trunk
channel-group 1 mode active
service-policy output PTP-Event-Priority
!
interface GigabitEthernet1/4
description Connected to IA-OG-C9300
switchport trunk native vlan 104
switchport trunk allowed vlan 104,113,150
switchport mode trunk
channel-group 1 mode active
service-policy output PTP-Event-Priority
!
interface GigabitEthernet1/5
description Connected to 1552-1
switchport trunk native vlan 104
switchport trunk allowed vlan 104,113,150
switchport mode trunk
service-policy input CIP-PTP-Traffic
service-policy output PTP-Event-Priority
!
```

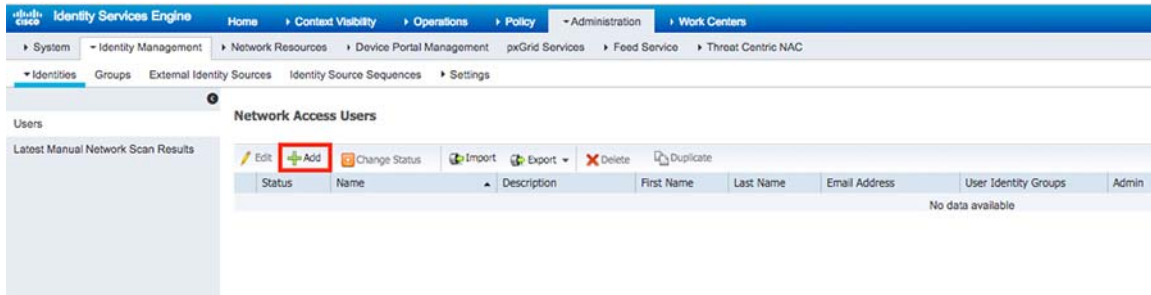
ISE Configuration—802.1x EAP-FAST Authentication

This section explains how to configure the Identity Services Engine (ISE) as the external RADIUS server to authenticate the wireless client using 802.1x Extensible Authentication Protocol (EAP) and Flexible Authentication via Secure Tunneling (FAST) authentication (EAP-FAST).

Create a User Database to Authenticate EAP-FAST Clients

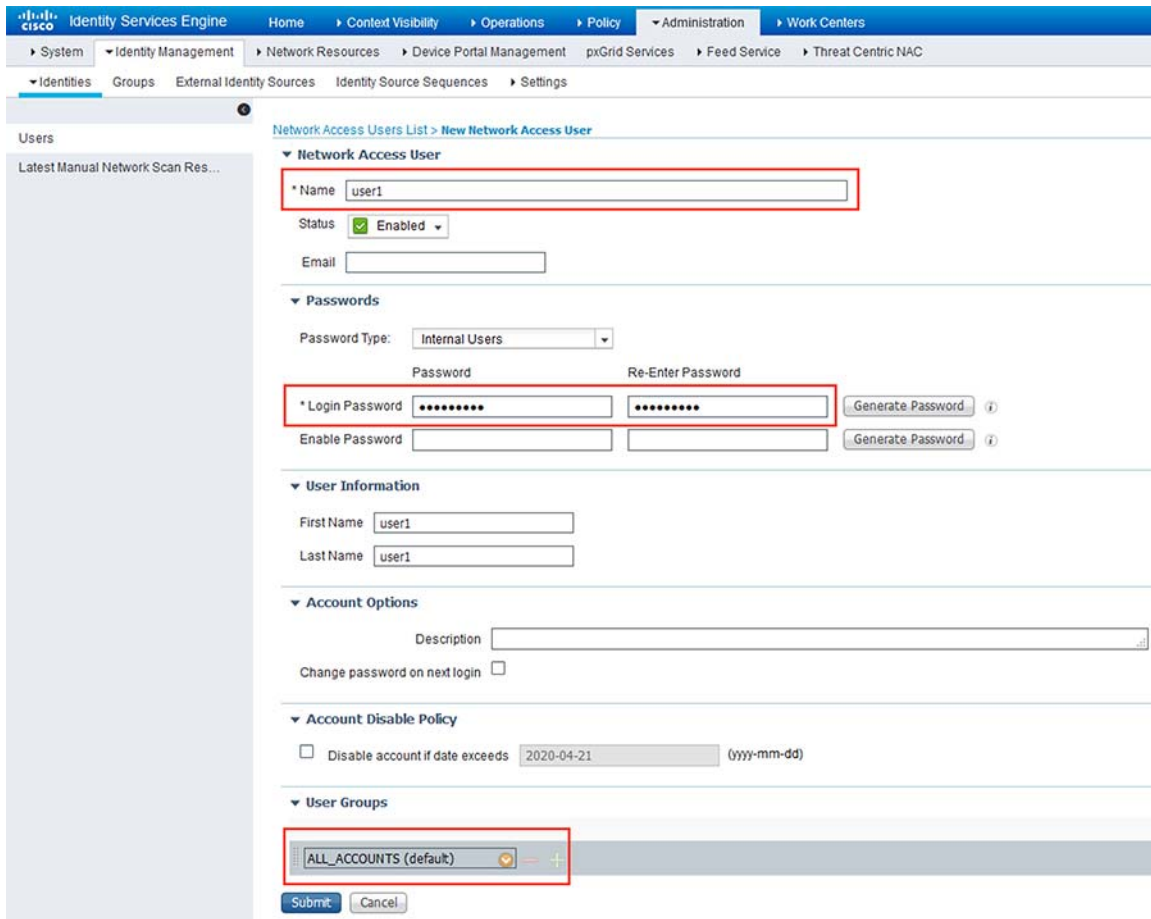
1. Using the ISE interface, navigate to **Administration > Identity Management > Users** and then click **Add**. See [Figure 6](#) below.

Figure 6 Adding a Network Access User to ISE

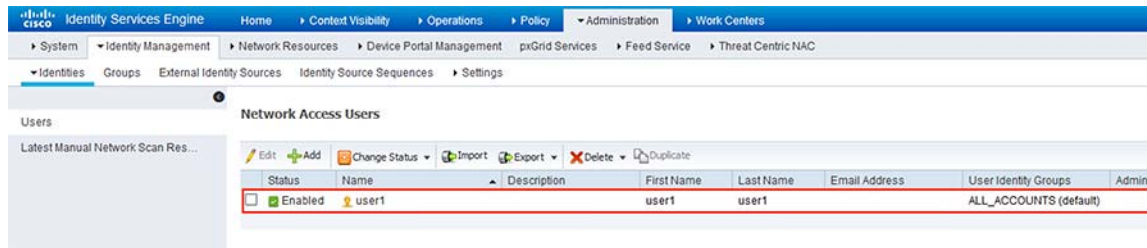


2. As shown in Figure 7 enter information to create a new user: **Name** and **Login password**, and select **User group** from the drop-down list. You can enter optional information for the user account.
3. Click **Submit**.

Figure 7 Adding Network Access User to ISE



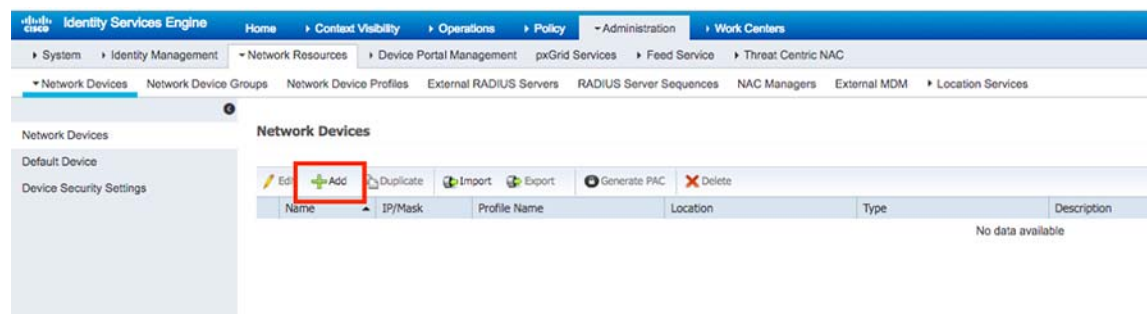
The user is created. See Figure 8 below.

Figure 8 Network Access User Added to ISE

Add the WLC as AAA Client to the ISE Server

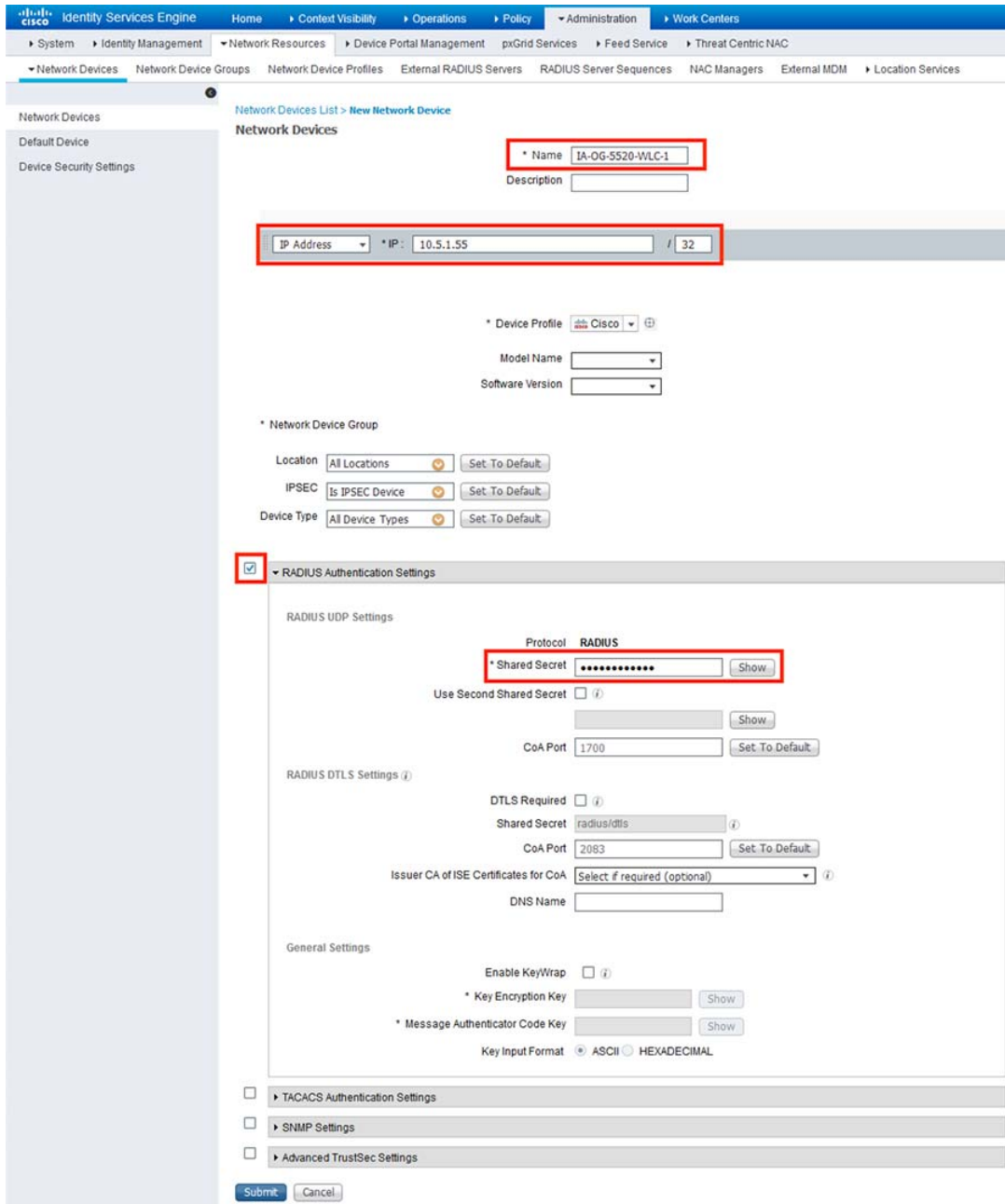
Complete these steps to define the controller as an Authentication, Authorization, Accounting (AAA) client on the Cisco Access Control Server (ACS):

1. Navigate to **Administration > Network Resources > Network Devices** and then click **Add**. See [Figure 9](#).

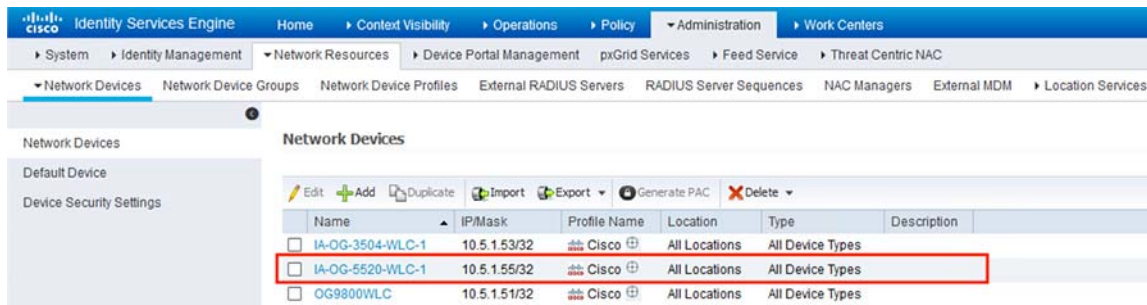
Figure 9 Adding WLC to Network Devices on ISE - Step 1

2. As shown in [Figure 10](#) enter the required information for the device you are adding: **Name** and **IP address**, and configure the same shared secret password as was configured on the WLC on the **Shared Secret** form. You can enter optional information for the device such as location, group, etc.
3. Click **Submit**.

Figure 10 Adding WLC to Network Devices on ISE - Step 2

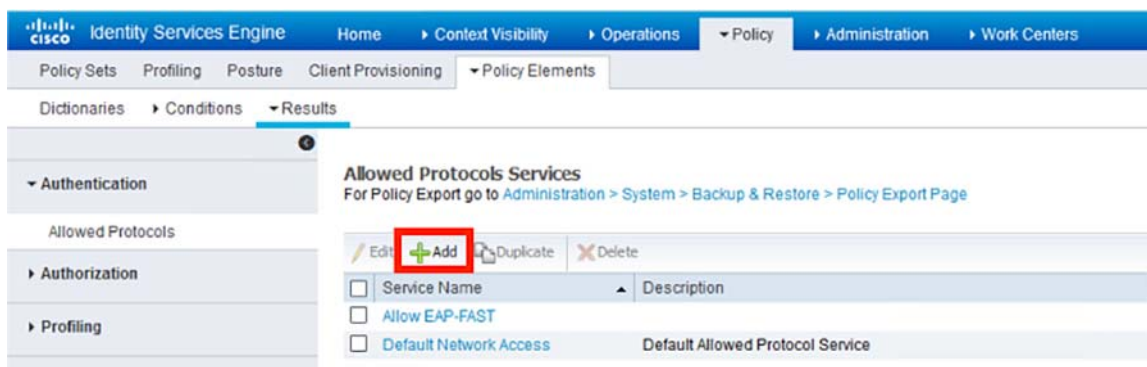


As shown in Figure 11 the device is added to the ISE Network Access Device list (NAD).

Figure 11 WLC Added to Network Devices on ISE

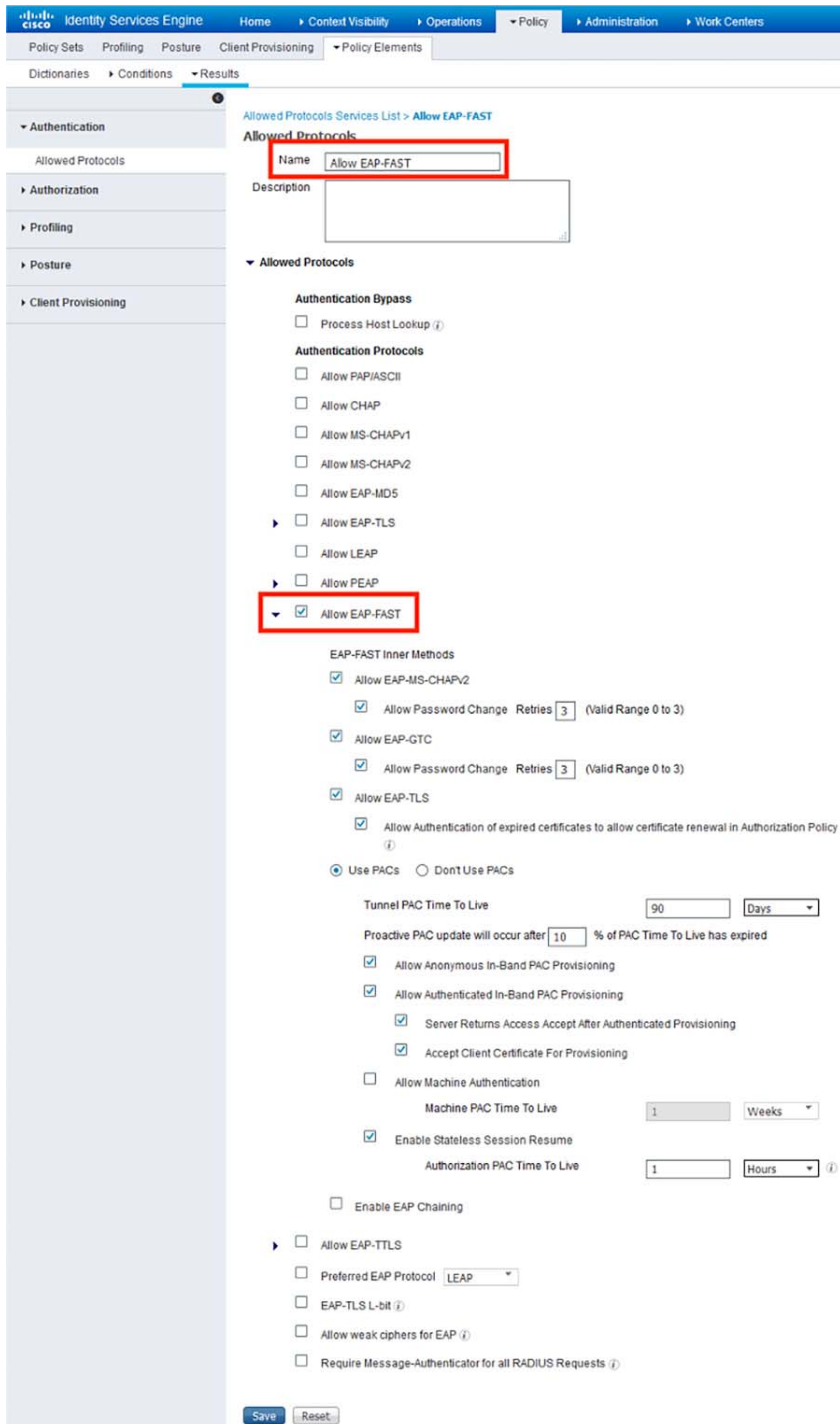
Configure Allowed Protocols Services

- Using the ISE interface, navigate to **Policy > Policy Elements > Results** and then click **Add** as shown in [Figure 12](#).

Figure 12 Adding Allowed Protocols Service on ISE

- Enter **Name** and **Allowed Protocols**, and then click **Save**. In this example we chose to use EAP-FAST, but different authentication methods can also be used, depending on your security requirements. See [Figure 13](#).

Figure 13 Adding Allowed Protocols on ISE

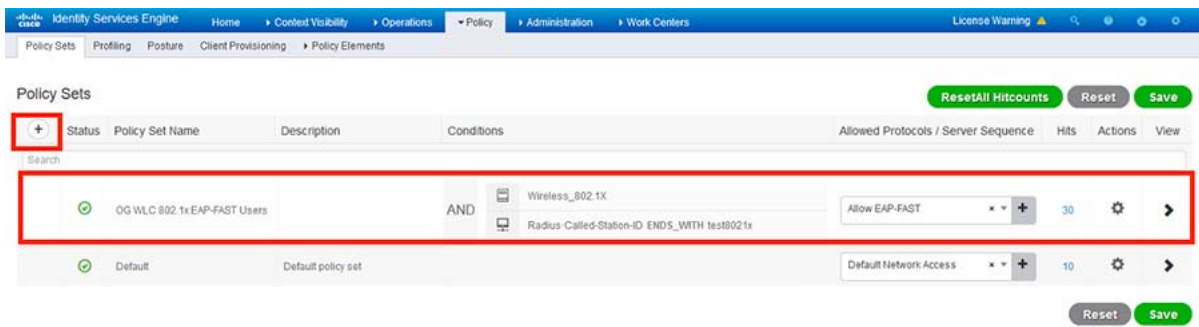


Configure Policy Sets on the ISE Server

1. Using the ISE interface, navigate to **Policy > Policy Sets** and click the + (plus) icon.

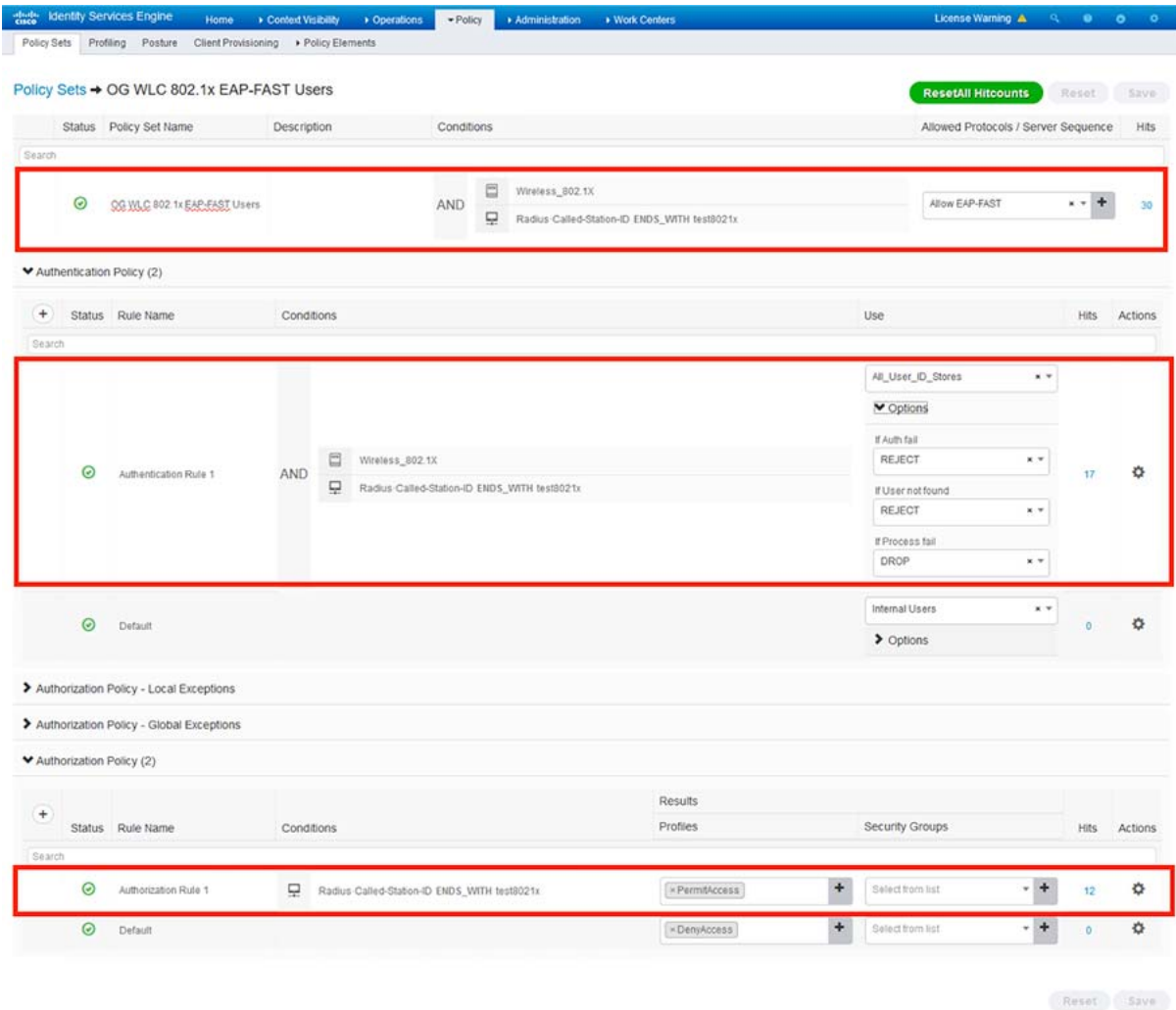
Detailed Configurations of Components

2. Fill in the required form for the policy set you want to add: **Policy Set Name** and **Conditions**, and then select **Allowed Protocols/Server Sequence** from the drop-down list. See [Figure 14](#).
3. Click **Save**. By default, the WLC sends a Called-Station-ID ending with the SSID name for authentication. The SSID name in this example is *test802.1x*.

Figure 14 Adding Policy Sets on ISE

4. Enter **Rule Name**, **Conditions**, **Use**, and **Profiles**, and then click **Save**. See [Figure 15](#) below.

Figure 15 Authentication and Authorization Policies Added on ISE



Network Management with Prime Infrastructure and Connected Mobile Experience (CMX)

Prime Infrastructure provides a single integrated solution for comprehensive lifecycle management of the wired or wireless access, campus, and branch networks, and rich visibility into end-user connectivity and application performance assurance issues. Tightly coupling client awareness with application performance visibility and network control, Prime Infrastructure helps ensure uncompromised end-user quality of experience. Within the Oil & Gas Refinery, implementing a network management system to encompass network status and health in a single pane of glass view is highly recommended.

Cisco's Prime infrastructure coupled with Connected Mobility eXperience (CMX) provides an administrator a real time visual view into the wireless network with its next generation wireless site maps from release 3.2 and beyond. In the following sections the critical components needed for optimal wireless mesh monitoring are discussed.

Note: This guide does not describe the installation and granular tuning of Prime infrastructure. For implementation details, see the *Prime Infrastructure End User Guide*.

Detailed Configurations of Components

To view and monitor the mesh network, add a site map of the coverage area to Prime infrastructure. Site maps have a predetermined hierarchy described below:

- Campuses are the highest level in the map hierarchy. A campus represents a single business location or site. A campus includes at least one building, with one or more floor areas, and many outside areas.
- Buildings represent single structures within a campus representing organization-related floor-area maps. You can add as many buildings you want to a single campus map. A building can have one or more floors and outside areas associated with it. You can only add buildings to a campus map.
- Floor areas are within the building which comprises cubicles, walled offices, wiring closets, and so on. You can only add floor areas to building maps. You can add up to 100 floors to each building map that you create.
- Basement levels are similar to floor areas, except they are numbered in reverse order from floor areas. You can only add basements to buildings. You can add up to 100 basement levels to each building map you create, in addition to the 100 above-ground floor areas.
- Outside areas are the exterior locations. Although they are typically associated with buildings, outside areas must be added directly to campus maps, at the same level as buildings. You can add as many outside areas to a campus map as you want.

Cisco Prime Infrastructure comes with two campus maps:

- System Campus—This is the default campus map. If you create a new building, floor, basement, or outside area, but do not create it as part of your campus map, these subordinate maps are automatically created as children of the System Campus map.
- Unassigned—This is the default map for all network endpoints and hosts that you have not assigned to any other map, including the System Campus.

Guidelines for Preparing Image Files for Use Within Wireless Site Maps

- To create maps, you can use any graphics application that saves raster image file formats such as: PNG, JPEG, or GIF.
- For floor and outdoor area maps, Cisco Prime Infrastructure allows bitmap images such as PNG, JPEG, GIF, and CAD vector formats (DXF and DWG).
- The dimension of the site map image must be larger than the combined dimension of all buildings and outside areas that you plan to add to the campus map.
- Map image files can be any size. Cisco Prime Infrastructure imports the original image to its database at a full definition. Elements are automatically resized to fit the workspace when displayed.
- Decide the horizontal and vertical dimensions of the site in either feet or meters before importing. You must specify these dimensions during import.
- You can change the default map measurement units to meters if you plan to enter campus, building, floor, or outside area dimension in meters.
- After you have created the maps, you can assign network elements to them. You can do this manually by selecting individual devices and assigning them to campuses, buildings, floors, and outside areas as needed. For wireless access points and access controllers, you can add them to your maps automatically by using your organization naming hierarchy for access points or wireless access controllers.

To create site maps for mesh networks, add elements in the following order:

- Campus map
- Outdoor area map
- Buildings

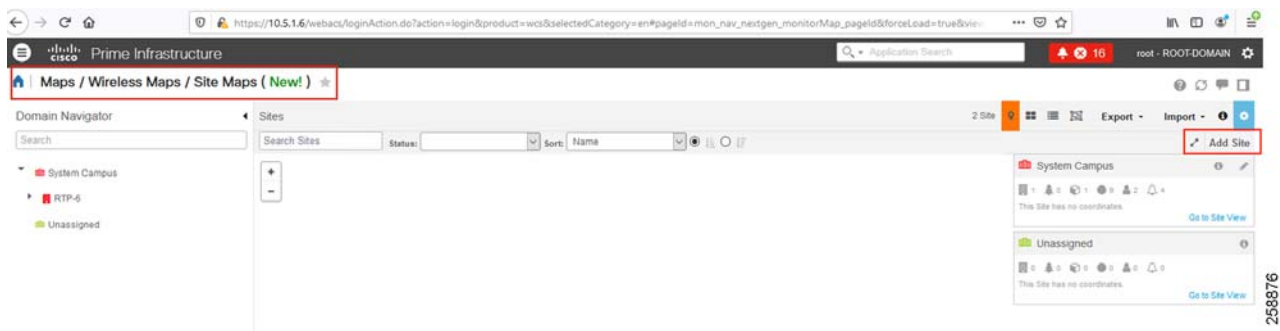
- Mesh access points

Creating a Wireless site map

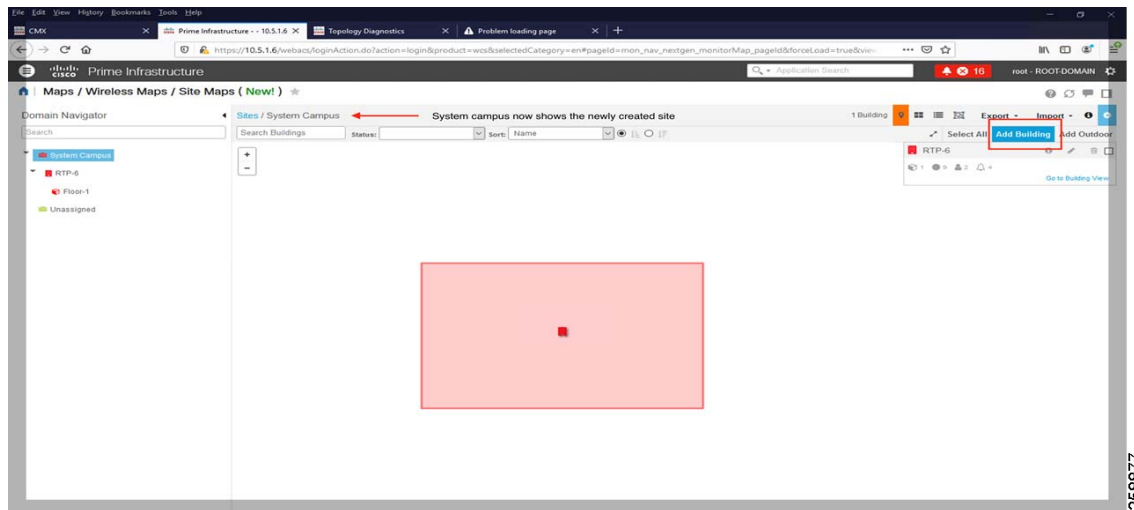
To create your Wireless site map, follow the steps below.

1. From the Cisco Prime Infrastructure interface, choose **Maps > Wireless Maps > Site Maps (New)**.
2. The available site panels are displayed in the right pane. Use the **Domain Navigator** to navigate to your selected site map, and highlight it.
3. Click **Add Site** in the upper right corner of the Sites page. See [Figure 16](#). The New Site window displays; all fields with a yellow background are mandatory.
4. Enter a name for your site in the **Site Name** text box. The site name can contain up to 32 characters.
5. Enter the email address in the **Contact** text box. The contact details can contain up to 32 characters.
6. Select the parent location group from the **Parent Location Group** drop-down list.
7. Upload your site map by double-clicking the filename, or dragging it to the upload box.
8. Enter the civic location details in the **Civic Location** text box. The Longitude and Latitude text boxes are automatically updated when you enter valid civic location details.
9. Enter the actual dimension of the site in the **Width** and **Length** text boxes.
10. Click **Save**.

Figure 16 Prime Infrastructure Add Site



After the Site has been created, enter building parameters. See [Figure 17](#) below.

Figure 17 Prime Infrastructure Add Building to site

Alternatively, you can import a map archive using the method below.

1. Choose **Maps > Wireless Maps > Site Maps (New)** to navigate to this page.
2. Using the Domain Navigator, navigate to the site map you want to import. Available site maps display in the right pane.
3. From the Import drop-down list, choose **Map Archive**.

The Import Map Archive wizard opens.

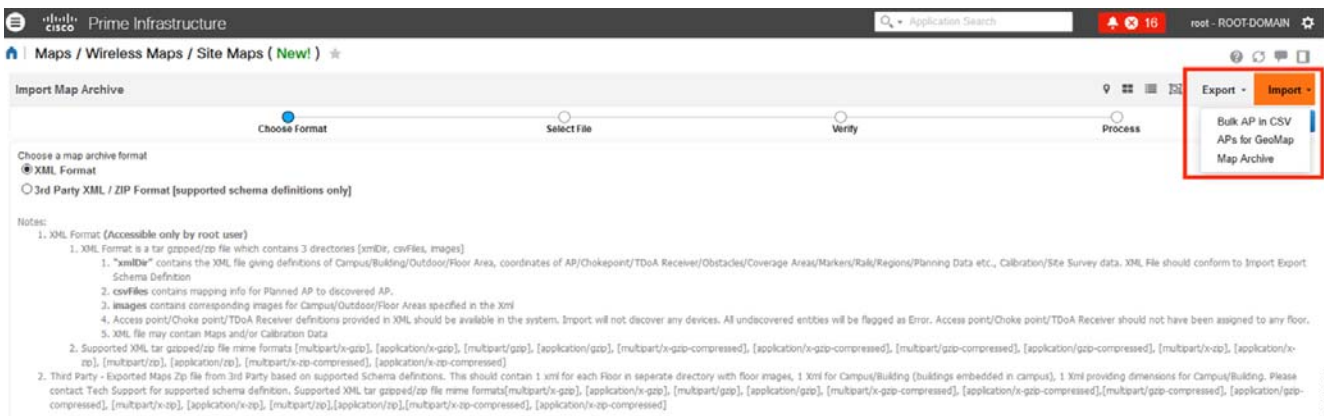
4. On the Choose Format page (see [Figure 18](#)), you can choose either of the following map format types:
 - XML Format
 - Third-Party XML/Zip
5. On the Select File page, click to select file or drag it to the appropriate box for Upload. You can import either zip or tar format files. You can also download a sample template.
6. Click **Verify**. After the validation is complete, the result appears which contains information about map path, message, status, and overwrite information.
7. Click **Process**. The map import process starts.

The Summary table shows the Map Path, Message, and Status information. A green dot in the Status column represents a successful import to the database. A red dot indicates that there was an error while importing the map.

8. From the Show drop-down list, choose **All** or **Quick Filter** to search using the Map Path and Message.
9. After the import process is successful, click **Done**.

The imported maps appear in the Domain Navigator left sidebar menu on the Site Maps page.

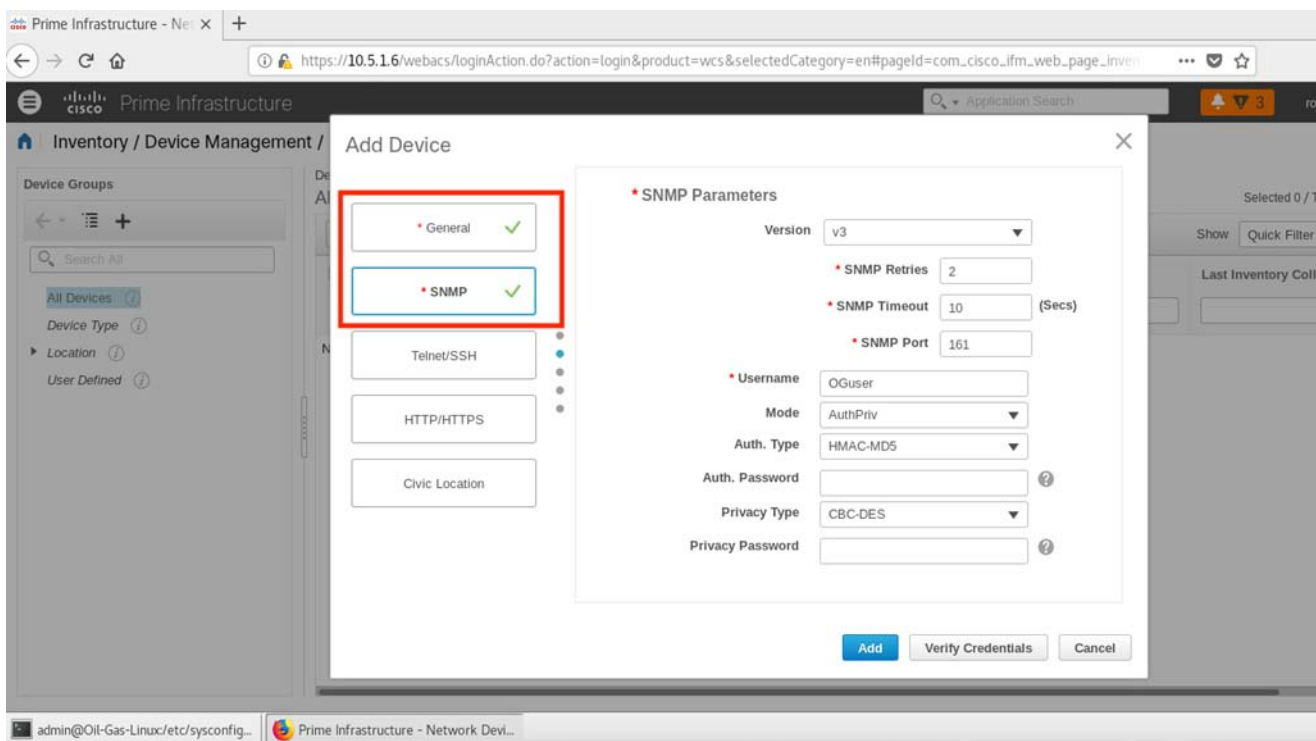
Figure 18 Prime Infrastructure Import Map



Adding Devices to Prime Infrastructure

Prime Infrastructure can manage and collect metrics on the network devices after they are inventoried into the server database with Hostname or IP address, and SNMP v3. After you enter device parameters, (see Figure 19) Prime Infrastructure will verify the same information and attempt to add the device.

Figure 19 Prime Infrastructure Add Device SNMP parameters



For the SNMP configuration on the Catalyst 9800, refer to *Managing Catalyst 9800 Wireless Controller Series with Prime Infrastructure using SNMP v3 and NetCONF* at:

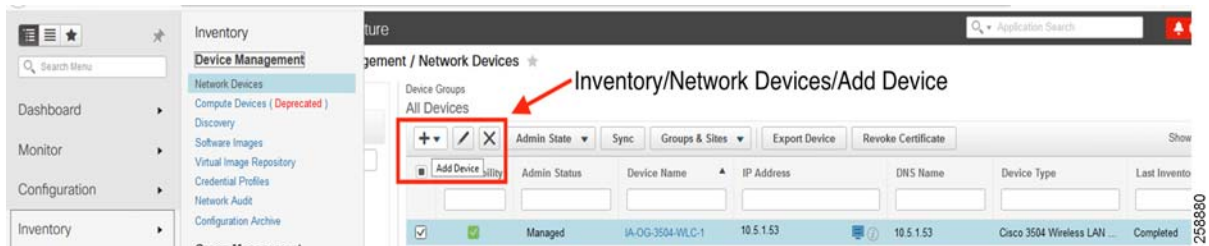
<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/214286-managing-catalyst-9800-wireless-controll.html>

For SNMP configuration on the AireOS controller, refer to the *SNMP Configuration in:*

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/wireless_intrusion_detection_system.html#id_16872

After a few minutes the WLC will be discovered and synchronized with Prime infrastructure.

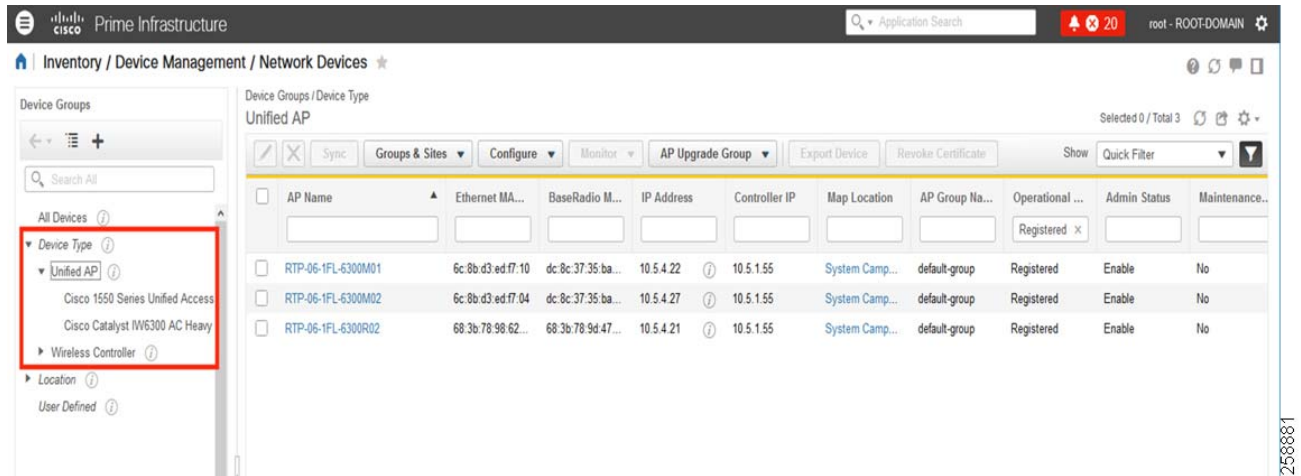
Figure 20 Prime Infrastructure Add Devices with SNMP discovery



After the controller is inventoried, Prime infrastructure will obtain a copy of the running configuration, controller version, associated clients, access points, and various analytical data using SNMP.

When the wireless LAN controller is added to Prime Inventory, the associated APs are automatically added into Prime infrastructure and can be seen as device type Unified AP within the Device Group. See [Figure 21](#).

Figure 21 Prime Infrastructure Discovered Access Points



After device inventory is complete, and synchronization with Wireless LAN Controllers is done, access points can be added to the site map for RF signal approximation.

Prime Infrastructure computes the heat map for the entire site which displays the relative intensity of the RF signals on the coverage area, as shown in [Figure 22](#). This does not take into account the attenuation of various building materials, nor does it display the effects of RF bouncing off of obstructions.

Figure 22 Prime Infrastructure Add Devices into Site Map

To add APs to your site maps, complete the instructions below.

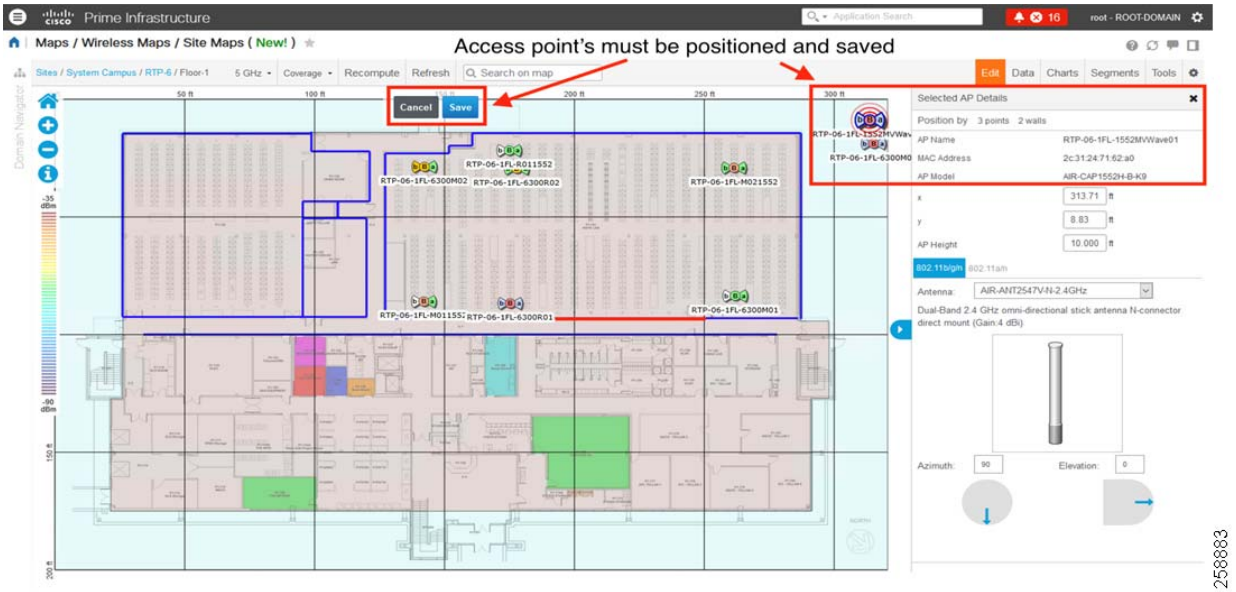
1. Using the Prime Infrastructure interface, choose **Maps > Site Maps (New)**.
2. From the Domain Navigator left sidebar menu, select the applicable floor to open the floor view page.
3. Click **Edit** at the upper right corner of the page.
4. In the Floor Elements panel, next to Access Points, click **Add**.

All the access points that are not assigned to any floors appear in the list.

- a. In the Add APs page, select check box(es) of the access points that you want to add to the floor area and click **Add Selected**.
 - b. To add all access points, click **Select All** and click **Add Selected**.
 - c. To directly assign access points to the floor area, click + (plus sign).
 - d. You can search for access points using the search option available. Use the Quick Filter and search using the AP name, MAC address, Model, or Controller. The search is case-insensitive. The search result appears in the table. Click + (plus sign) to add them to the floor area.
5. Assign access points to the floor area, then close the Add APs window.
 6. Click **Save** as shown in [Figure 23](#).

Each access point that you added to the floor map appears on the right side of the map. You need to position them correctly. When you have completed placing and adjusting the AP into position, the heatmap is generated based on the new position.

Figure 23 Prime Infrastructure Save Site Map

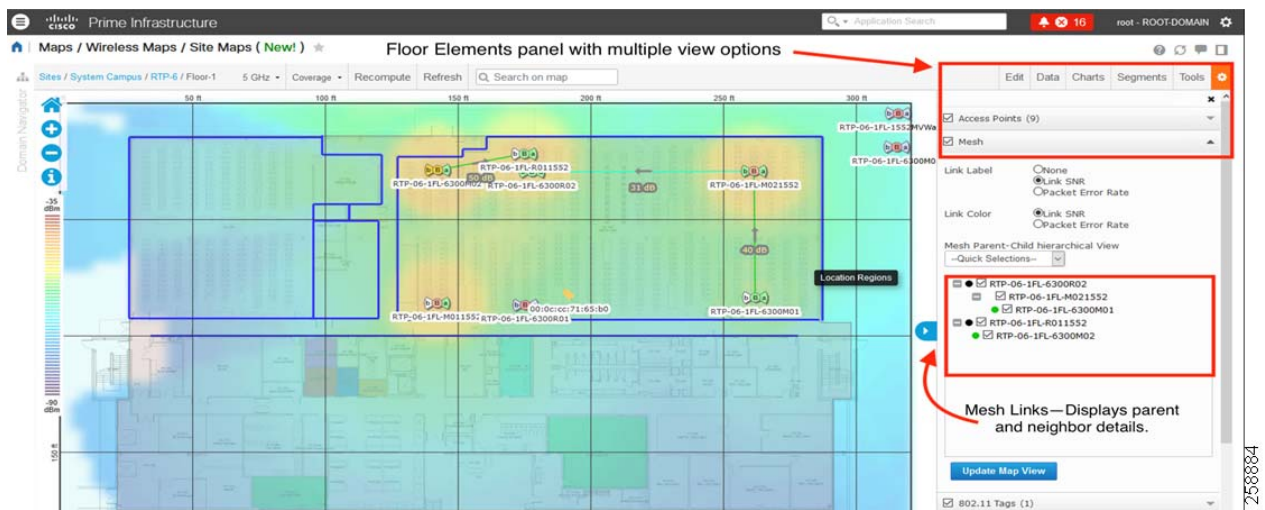


View Mesh Access Point Configurations Using Wireless Site Maps

You can view details about the mesh APs. Hover your cursor over any device icon in a map to view details about that device. Double-click the AP that you want to view detailed configuration info. See [Figure 24](#) below.

In Prime Infrastructure, you can change the view of your maps, and see information about parent or neighbor maps.

Figure 24 Prime Infrastructure Retrieve Network Device Configuration



Integration with CMX

Cisco Connected Mobile eXperiences (CMX) is a smart Wi-Fi solution that uses the Cisco wireless infrastructure to provide location services and analytics for mobile devices. If location services are required, then it is recommended you incorporate the Cisco Connected Mobility Experience (CMX) platform. Prime Infrastructure integrates with CMX to provide a visual and accurate representation of client activity in real time and in playback mode.

Detailed Configurations of Components

Note: Location validation was not tested in this release. For location testing, consult with Cisco CX or a certified vendor such as Accenture.

To add CMX to your Prime Infrastructure:

1. On the Prime Infrastructure interface, navigate to **Services > Mobility Services > Connected Mobile Experiences**.
Alternately, navigate to **Services > Mobility Services > Mobility Service Engine** and click **Manage CMX**.
2. Click **Add**.
3. Enter the following details: IP, device name, CMX username (gui), CMX password (gui)
4. Click **Save**.

To Edit or Delete any device in CMX:

- Using the Prime Infrastructure interface, choose **Services > Mobility Services > Connected Mobile Experiences**. Select the device and then click **OK**.

To import the site maps into CMX:

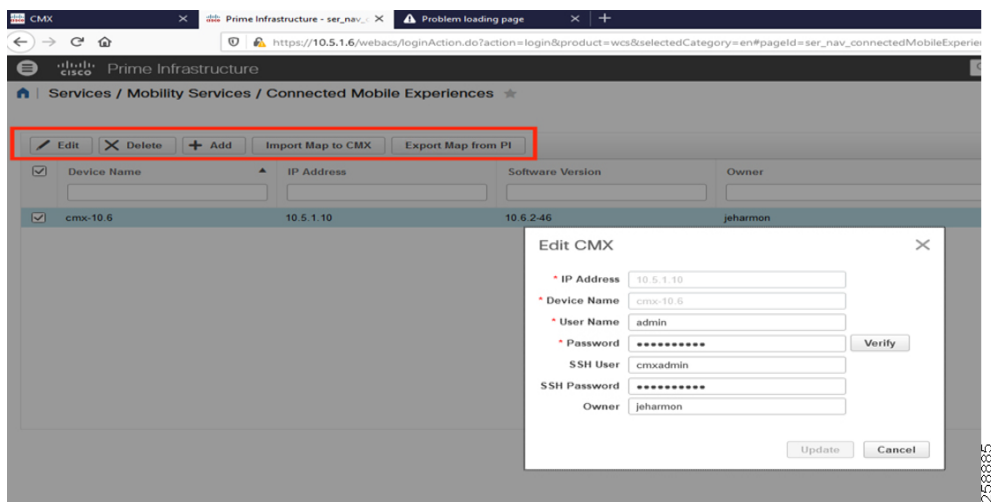
1. Using the Prime Infrastructure interface, choose **Services > Mobility Services > Connected Mobile Experiences**. Select a CMX and then click **Import Map to CMX**.

Note: Maps are not visible when CMX is in Presence mode; switch to Location mode to see maps.

2. Choose a map and then click **Import Map to CMX**.

Note: You can also add map files to Prime Infrastructure with the **Export Map from PI** button in the List CMX page.

Figure 25 Prime Infrastructure Import CMX



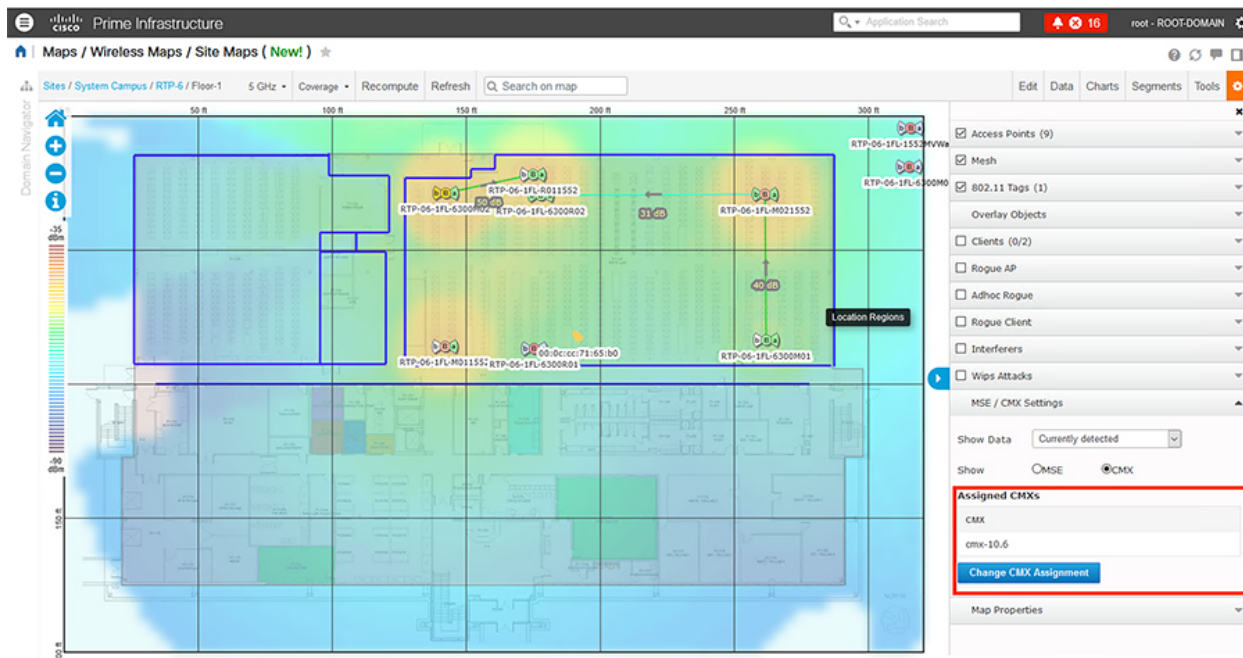
After CMX has been added to the Prime Infrastructure server, the maps can now be integrated with CMX. To integrate maps:

1. Click **CMX** radio button and then click **Change CMX Assignment**.
2. In the assigned CMX table, select the node to which the maps have to be synchronized and then click **Synchronize**.
3. Click **Cancel** to discard any changes to the assignment.

- After CMX has been synchronized with Prime Infrastructure, site maps will display the positions of RFID Tags, Rogue clients, APs, and clients (associated and non-associated).

Note: Changes to maps in Prime Infrastructure are not automatically synchronized with CMX; maps have to be re-imported to CMX to retrieve updated information.

Figure 26 Prime Infrastructure and CMX Assignment



For more advanced configuration tasks in Prime Infrastructure and CMX, see the following user guides:

- Cisco Prime Infrastructure 3.7 User Guide**
https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-7/user/guide/bk_CiscoPrimeInfrastructure_3_7_0_User_Guide/bk_CiscoPrimeInfrastructure_3_7_0_User_Guide_chapter_010100.html
- Cisco CMX Configuration Guide, Release 10.6.0 and Later**
https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-6/cmxcfg/b_cg_cmx106/getting_started_with_cisco_cmx.html#concept_48D1D73677E9492D9D2BA51EE81AD2AE

Quality of Service (QoS)

Quality of Service (QoS) ensures underlying network infrastructure, classifies and polices network flows to guarantee mission critical network traffic flow is expedited, while offering best effort service to less important network traffic.

A good QoS design and implementation can be evaluated with the following metrics:

- Loss**—Measured by number of packets not received as compared with total packets transmitted; network availability measurement. Traffic loss in a wired and wireless network is incurred by network congestion and wireless client contention to access designated wireless channel.
- Latency (Delay)**—Measured by amount of time it takes for a packet to reach a receiving client. Network delay is a critical metric for a control and process environment. Automation device monitoring control logic modules constantly send / receive IO/SAFETY information for continuous operation. Excessive latency will trigger customer plant instability.

Detailed Configurations of Components

- Jitter—Measured by the difference in the end-to-end delay between transmit and receiving packets. Jitter also named as delay variation. It is a critical measurement for network service synchronization.

O&G WLAN MESH network QoS includes both wired and wireless networks. Wired network QoS design and implementation details are referenced in the Switching section in this document. Wireless QoS configuration profiles can choose Platinum support based on the customer service requirements.

The QoS implementation on wireless LANs differs from QoS implementations on wired networks in the following ways:

- Wireless LANs do not classify packets.

Packets prioritization is based on differentiated services code point (DSCP) value, client type, or the priority value in the 802.1q or 802.1p tag.
- Wireless LANs do not match packets using ACL.

Modular Quality of Service (MQC) class-map used for matching classes.
- Wireless LANs do not construct internal DSCP values.

IP DSCP, precedence, or protocol values are assigned to Layer 2 COS values.
- Wireless LANs use Enhanced Distributed Coordination Function (EDCF)-like queuing on egress radio port.
- Wireless LANs do only FIFO queuing on the Ethernet egress port.
- Wireless LANs support only 802.1Q/P tagged packets.

You can reference these Cisco QoS documents when designing a new QoS model to fit customer premise specific requirements:

- Quality of Service (QoS) Configuration Guide, Cisco IOS XE Everest 16.6.x (Catalyst 9400 Switches)
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9400/software/release/16-6/configuration_guide/qos/b_166_qos_9400_cg/b_166_qos_9400_cg_chapter_01.html
- Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2SR
https://www.cisco.com/c/en/us/td/docs/ios/qos/configuration/guide/12_2sr/qos_12_2sr_book.html

The following figures show the O&G WLAN MESH WLC QoS configuration details.

Figure 27 WLC3504 WLAN QoS Configuration

The screenshot shows the Cisco WLC3504 configuration interface for the 'OG-SSID-1' WLAN. The 'QoS' tab is selected, and the 'Quality of Service (QoS)' dropdown is set to 'Platinum (voice)'. Below this, there are several configuration options: 'Application Visibility' (checkbox), 'AVC Profile' (none), 'Flex AVC Profile' (none), 'Netflow Monitor' (none), and 'Fastlane' (Disable). There are also sections for 'Override Per-User Bandwidth Contracts (kbps)' and 'Override Per-SSID Bandwidth Contracts (kbps)', both with input fields for DownStream and UpStream rates.

WLANs > Edit 'OG-SSID-1'

QoS

Quality of Service (QoS) Platinum (voice)

Application Visibility Enabled

AVC Profile none

Flex AVC Profile none

Netflow Monitor none

Fastlane Disable

Override Per-User Bandwidth Contracts (kbps)

	DownStream	UpStream
Average Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Average Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>

Override Per-SSID Bandwidth Contracts (kbps)

	DownStream	UpStream
--	------------	----------

Figure 28 WLC3504 QoS Profile Configuration

The screenshot displays the Cisco WLC3504 configuration interface for editing a QoS profile. The main content area is titled 'Edit QoS Profile' and contains the following configuration details:

- QoS Profile Name:** platinum
- Description:** For Voice Applications
- Per-User Bandwidth Contracts (kbps) *:**

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0
- Per-SSID Bandwidth Contracts (kbps) *:**

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0
- WLAN QoS Parameters:**
 - Maximum Priority: voice
 - Unicast Default Priority: voice
 - Multicast Default Priority: voice
- Wired QoS Protocol (highlighted in red):**
 - Protocol Type: 802.1p
 - 802.1p Tag: 5

Foot Notes:
 1. Override Bandwidth Contracts parameters are specific to per Radio of AP. The value zero (0) indicates the feature is disabled.

Figure 29 WLC3504 QoS MAP Configuration

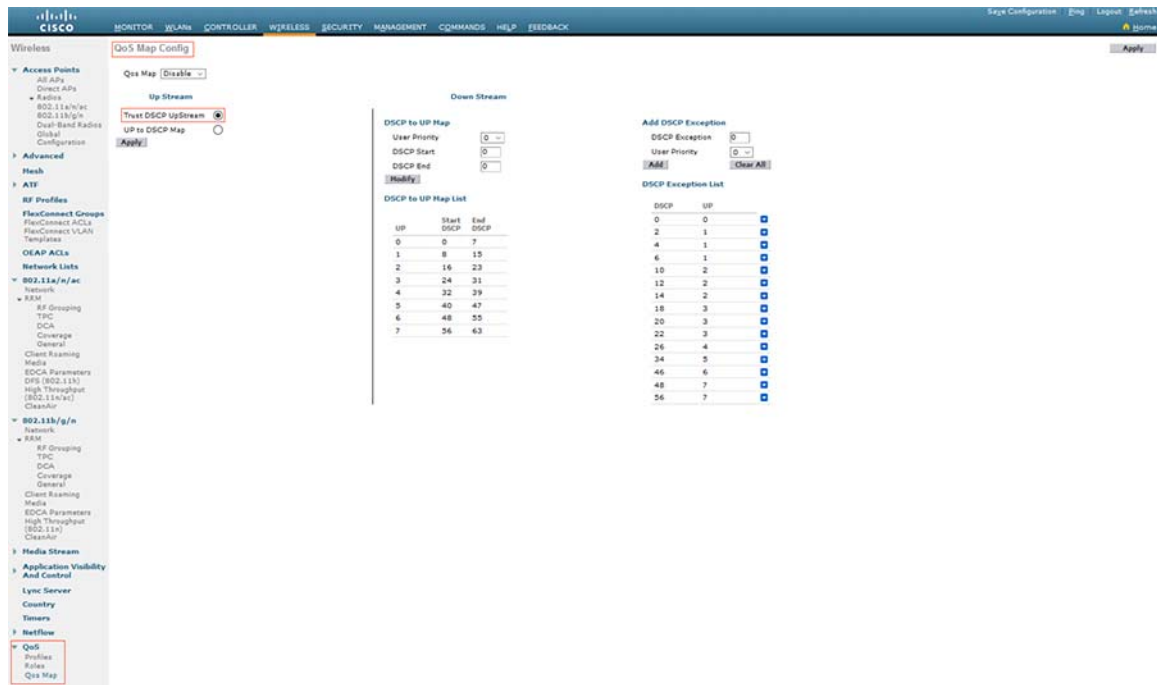


Figure 30 WLC5520 WLAN QoS Configuration

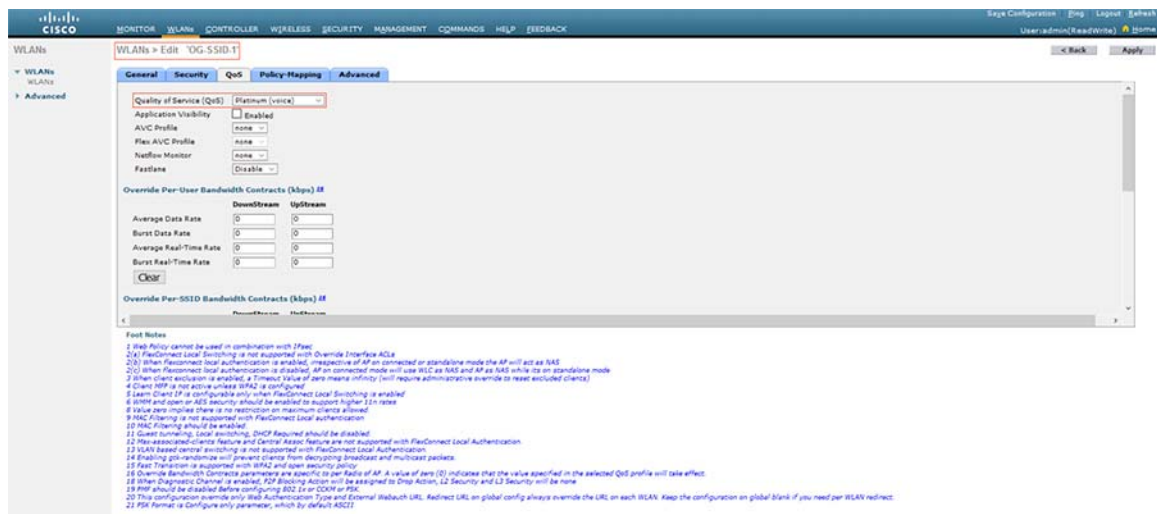


Figure 31 WLC5520 QoS Profile Configuration

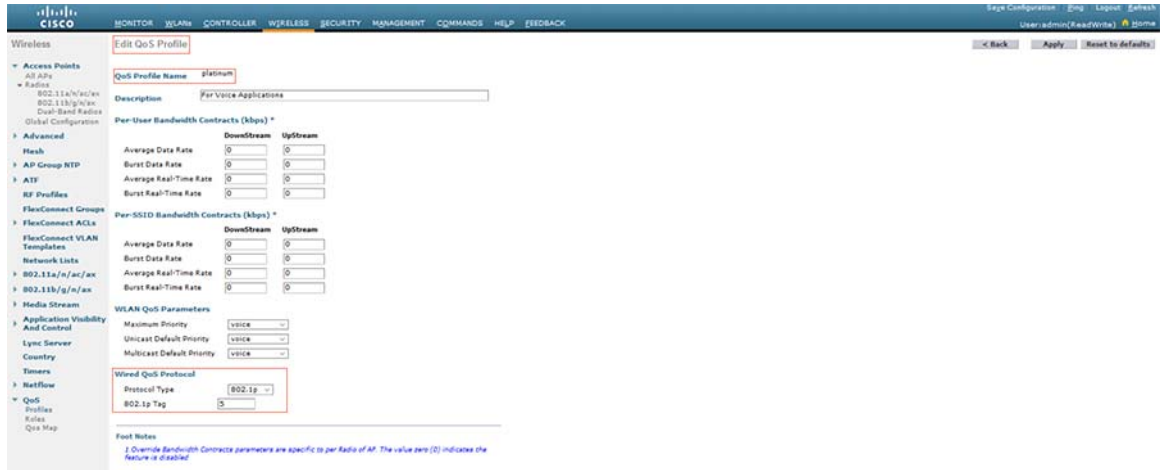


Figure 32 WLC5520 WLAN QoS MAP Configuration

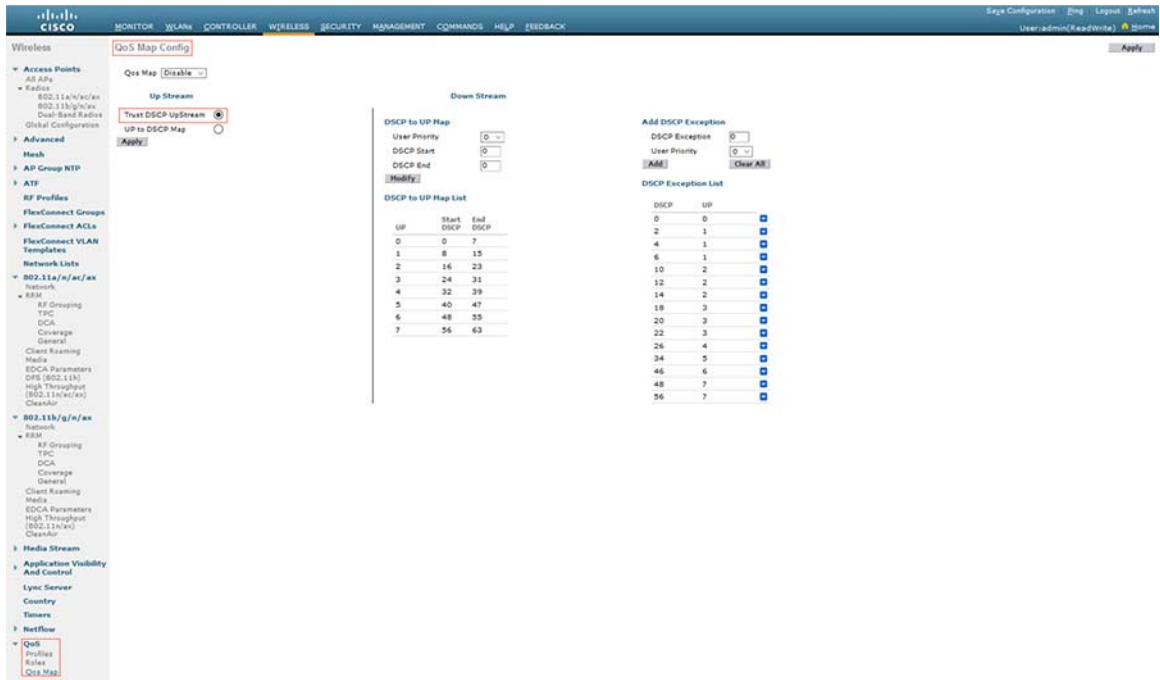


Figure 33 Cat 9800 WLAN QoS Configuration

2568859

Detailed Configuration of the Deployment Models

Greenfield Deployment Model

Recommended equipment for greenfield deployments are:

- Cisco Catalyst 9800 series wireless LAN controllers (Cat 9800 WLC) in High Availability

Cisco Catalyst 9800 controllers come in three models:

- Cisco Catalyst 9800-80
- Cisco Catalyst 9800-40
- Cisco Catalyst 9800-L

The Cisco Catalyst 9800-40 was used in validation.

- Cisco IW6300 Heavy Duty Access Points

Configuring HA SSO

When configuring High Availability SSO on Cat 9800s, consider:

- High availability between controllers reduces the downtime in live networks. When the Active wireless LAN controller goes down, the stand-by controller takes its place with minimum downtime.
- The Catalyst 9800 Wireless Controller supports the stateful switchover (SSO) of access points and clients. The two controllers in High Availability SSO maintain the mirror copy of AP and client databases. This prevents APs in the Discovery state and clients from disconnecting when the Active wireless controller fails. The Standby wireless controller takes over as the Active wireless controller.

Detailed Configuration of the Deployment Models

- A physical connection has to be maintained between the WLCs that are in HA SSO. There are dedicated RJ-45 RP ports or Gigabit SFP Redundancy Pairing (RP) ports on the chassis of the Cat 9800 that can be used for this purpose. WLCs need to be connected back to back either using RP ports or the Gigabit SFP RP ports.

Note:

- The SFP Gigabit Ethernet port takes precedence if they are connected at same time.
- HA between RJ-45 and SFP Gigabit RP ports is not supported.
- Only Cisco supported SFPs (GLC-LH-SMD and GLC-SX-MMD) are supported for RP port.
- When the HA link is up through RJ-45, SFPs on HA port should not be inserted even if there is no link between them. As it is a physical level detection, this would cause the HA to go down as precedence is given to SFP.

Configuring HA SSO between two 9800 WLCs using the GUI:

1. To configure HA SSO go to **Administration > Device > Redundancy**.
2. Enable the redundancy configuration and select Redundancy pairing type **RP**.
3. Assign the IP address and subnet mask and the peer IP. The Peer IP address and local IP address should be in the same subnet.
4. On the active controller, set the priority value to be higher than the standby controller. The controller with higher priority is made active in **active-active** election.
5. If the priority value is set to equal, the active controller is elected based on the lowest MAC address, shortest start-up time.

Note: Assign the highest priority to the controller you prefer to be active. This ensures that the controller is re-elected as active controller if re-election occurs.

For more details, see the Cisco Catalyst 9800 Wireless Controller High Availability SSO Deployment Guide https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/b_c9800_wireless_controller_ha_sso_dg.html

Figure 34 Redundancy Configuration on active Catalyst 9800

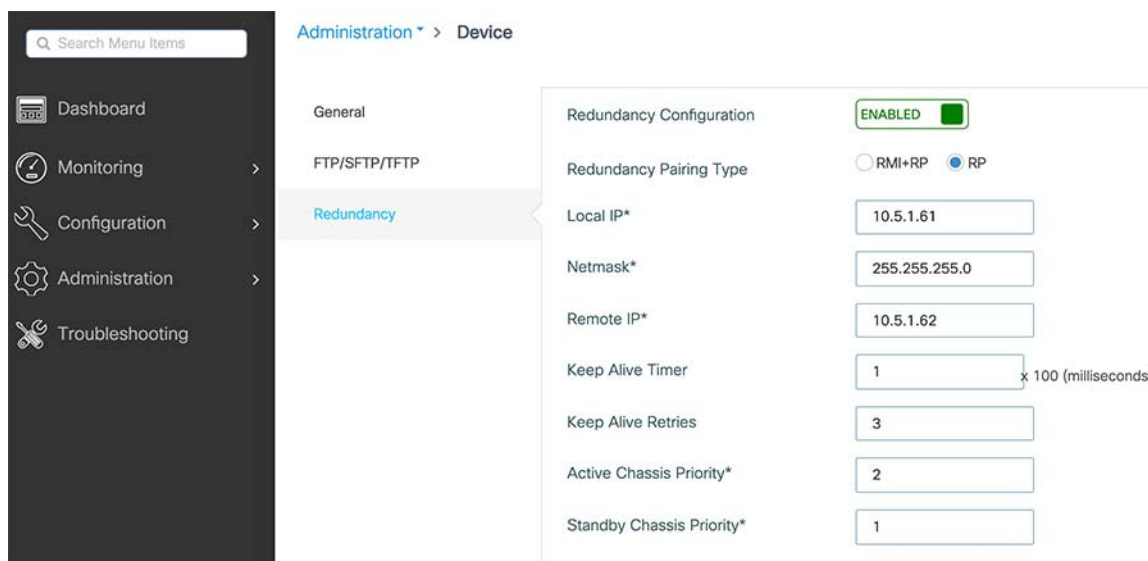


Figure 35 Redundancy Configuration on Stand-by Catalyst 9800

Administration > Device

General

FTP/SFTP/TFTP

Redundancy

Redundancy Configuration **ENABLED**

Redundancy Pairing Type RMI+RP RP

Local IP* 10.5.1.62

Netmask* 255.255.255.0

Remote IP* 10.5.1.61

Keep Alive Timer 1 x 100 (milliseconds)

Keep Alive Retries 5

Active Chassis Priority* 1

Standby Chassis Priority* 2

Verifying HA SSO Configuration:

You can check the redundancy on the active controller through the Web Interface and through the CLI.

To check the redundancy through CLI from the active controller:

```
WLC#show chassis
Chassis/Stack Mac Address : d4e8.80b2.d740 - Local Mac Address
Mac persistency wait time: Indefinite
Local Redundancy Port Type: Twisted Pair

Chassis#   Role    Mac Address      Priority  H/W   Current State      IP
-----
*1         Active  d4e8.80b2.d740   2        V02   Ready      10.5.1.61
2         Standby d4e8.80b2.d080   1        V02   Ready      10.5.1.62

WLC#show redundancy
Redundant System Information :
-----
    Available system uptime = 2 days, 18 minutes
Switchovers system experienced = 0
    Standby failures = 0
    Last switchover reason = none

    Hardware Mode = Duplex
Configured Redundancy Mode = sso
Operating Redundancy Mode = sso
Maintenance Mode = Disabled
Communications = Up

Current Processor Information :
-----
    Active Location = slot 1
    Current Software state = ACTIVE
    Uptime in current state = 2 days, 18 minutes
    Image Version = Cisco IOS Software [Amsterdam], C9800 Software (C9800_IOSXE-K9),
Version 17.1.1s, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Sat 15-Feb-20 20:00 by mcpre
    BOOT = bootflash:packages.conf,1;
    CONFIG_FILE =
```

Detailed Configuration of the Deployment Models

```

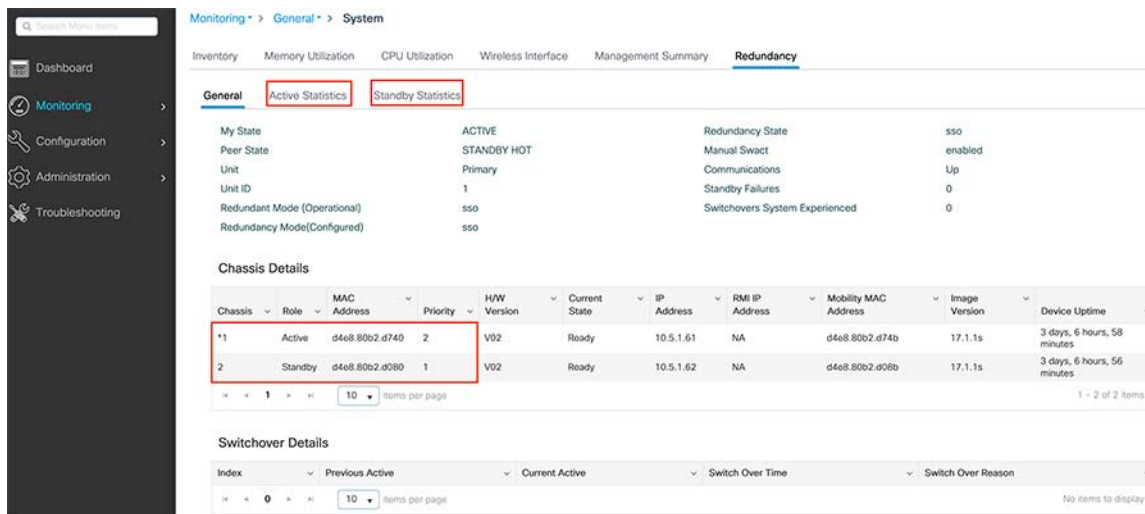
Configuration register = 0x2102
Recovery mode = Not Applicable

Peer Processor Information :
-----
Standby Location = slot 2
Current Software state = STANDBY HOT
Uptime in current state = 2 days, 16 minutes
Image Version = Cisco IOS Software [Amsterdam], C9800 Software (C9800_IOSXE-K9),
Version 17.1.1s, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Sat 15-Feb-20 20:00 by mcpre
BOOT = bootflash:packages.conf,1;
CONFIG_FILE =
Configuration register = 0x2102
    
```

Monitor HA Status from GUI:

To monitor the redundancy status from the Web interface of the active and stand-by controllers go to **Monitoring > General > system -> redundancy**. Refer to [Figure 36](#).

Figure 36 Monitor Redundancy Configuration



Note: Only the active controller is accessible through the GUI and CLI.

Configuring Mesh Profile

Mesh networking employs Cisco Aironet outdoor mesh access points and indoor mesh access points along with Cisco Wireless Controller and Cisco Prime Infrastructure to provide scalability, central management, and mobility between indoor and outdoor deployments. Control and Provisioning of Wireless Access Points (CAPWAP) protocol manages the connection of mesh access points to the network.

In the new configuration model, the controller has a default mesh profile. This profile is mapped to the default AP-join profile, which is in turn mapped to a site tag. If you are creating a named mesh profile, ensure that these mappings are put in place and the corresponding AP is added to the corresponding site-tag. To configure Mesh profile:

1. Navigate to **Configuration > Wireless > Mesh**.

Detailed Configuration of the Deployment Models

- Under the Global Config Tab, configure common parameters that are used across multiple mesh profiles and general mesh settings. To restrict mesh access points from moving out of network and joining other mesh networks enable PSK Provisioning under security. See [Figure 37](#) below.

Figure 37 Mesh Global Configuration

Configuration > Wireless > Mesh

Global Config Profiles

General

Ethernet Bridging Allow BPOU

Subset Channel Sync

Backhaul

Extended UNII B Domain Channels

RRM

Security

PSK Provisioning

Default PSK

Alarm

Max Hop Count

Recommended Max Children for MAP

Recommended Max Children for RAP

Parent Change Count

Low Link SNR (dB)

High Link SNR (dB)

Association Count

Apply

- Under the Profile tab, you can add a new mesh profile.
- For faster mesh convergence select the Convergence Method as Very Fast and enable background scanning and channel change notification.
- Mesh background scanning improves convergence time and reliability and stability of parent selection. With the help of the Background Scanning feature, a MAP can find and connect with a better potential parent across channels and maintain its uplink with the appropriate parent all the time.

Figure 38 Creating a Mesh Profile

Configuration > Wireless > Edit Mesh Profile

Global Config Profiles

+ Add - Delete

Number of Profiles : 3

Name

MeshProfile1

MeshProfile2

default-mesh-profile

10

General Advanced

Name* MeshProfile1

Description MeshProfile1

Range (Root AP to Mesh AP) 12000

Multicast Mode In-Out

IDS (Rogue/Signature Detection)

Convergence Method Very Fast

Background Scanning

Channel Change Notification

LSC

Backhaul amsdu

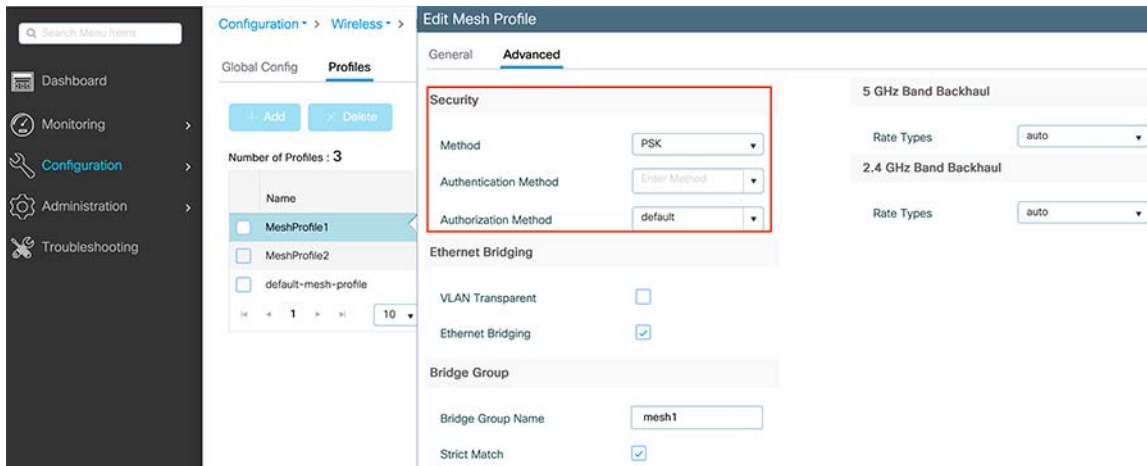
Backhaul Client Access

Battery State for an AP

Full sector DFS status

- Use the PSK key provisioning feature to enable PSK functionality from the controller which helps make a controlled mesh deployment and enhance MAPs security beyond the default. Under the Advanced tab, specify the security method for the mesh access points. In this document, the validation is done with PSK.

Figure 39 PSK Configuration in a Mesh Profile



WLAN Configuration

This feature enables you to control WLANs for lightweight access points. Each WLAN has a separate WLAN ID, a separate profile name, and a WLAN SSID. You can configure WLANs with different SSIDs or with the same SSID. An SSID identifies the specific wireless network that you want the device to access.

To configure WLAN through the GUI:

1. Navigate to **Configuration > Tags & Profiles > WLANs**, and click **Add**.
2. Under the General tab, enter the Profile Name (WLAN name).
3. By default, WLAN ID is automatically generated. You can change the WLAN ID to any number between 1-4096.
4. To enable the WLAN, toggle the Status button to **Enabled**.
5. On the Security tab, select the authentication method used for the client access.
6. For faster client transition enable Fast Transition on the Security tab. The client roaming can be either over the air or over the distributed system.

Figure 40 General Tab Configuration of WLAN

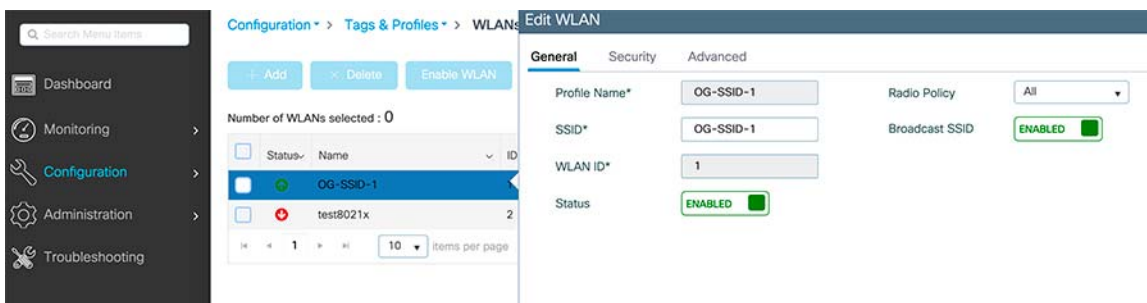


Figure 41 Example of PSK Security Configuration for Client Access

Edit WLAN

General **Security** Advanced

Layer2 **Layer3** AAA

Layer 2 Security Mode Fast Transition

MAC Filtering Over the DS

Protected Management Frame

PMF Reassociation Timeout

WPA Parameters

WPA Policy

WPA2 Policy

WPA2 Encryption AES(CCMP128)

CCMP256

GCMP128

GCMP256

Auth Key Mgmt 802.1x

PSK

CCKM

FT + 802.1x

FT + PSK

802.1x-SHA256

PSK-SHA256

PSK Format

PSK Type

Pre-Shared Key*

MPSK Configuration

MPSK

Figure 42 Advanced Tab Configuration on WLAN

Edit WLAN

General
Security
Advanced

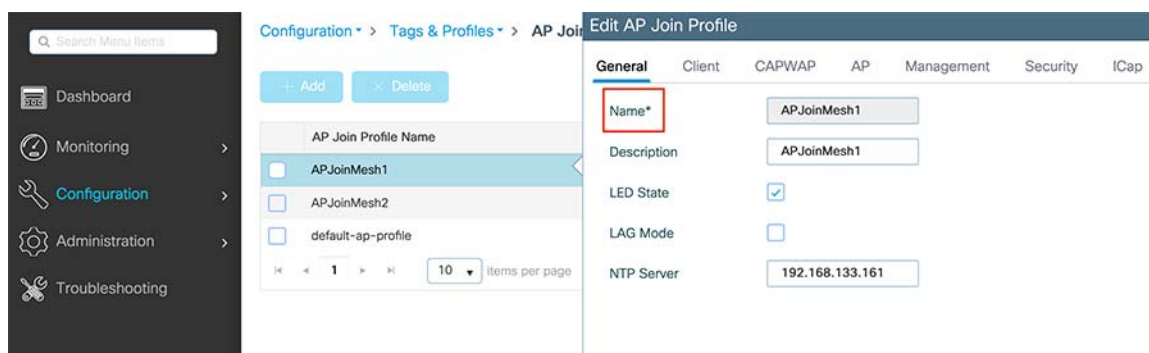
<p>Coverage Hole Detection <input checked="" type="checkbox"/></p> <p>Aironet IE <input checked="" type="checkbox"/></p> <p>P2P Blocking Action Disabled</p> <p>Multicast Buffer DISABLED</p> <p>Media Stream Multicast-direct <input type="checkbox"/></p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">Max Client Connections</div> <p>Per WLAN 0</p> <p>Per AP Per WLAN 0</p> <p>Per AP Radio Per WLAN 200</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">11v BSS Transition Support</div> <p>BSS Transition <input checked="" type="checkbox"/></p> <p>Disassociation Imminent(0 to 3000 TBTT) 200</p> <p>Optimized Roaming Disassociation Timer(0 to 40 TBTT) 40</p> <p>BSS Max Idle Service <input checked="" type="checkbox"/></p> <p>BSS Max Idle Protected <input type="checkbox"/></p> <p>Directed Multicast Service <input checked="" type="checkbox"/></p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">11ax</div> <p>Downlink OFDMA <input checked="" type="checkbox"/></p> <p>Uplink OFDMA <input checked="" type="checkbox"/></p> <p>Downlink MU-MIMO <input checked="" type="checkbox"/></p> <p>Uplink MU-MIMO <input checked="" type="checkbox"/></p> <p>BSS Target Wake Up Time <input checked="" type="checkbox"/></p>	<p>Universal Admin <input type="checkbox"/></p> <p>Load Balance <input type="checkbox"/></p> <p>Band Select <input type="checkbox"/></p> <p>IP Source Guard <input type="checkbox"/></p> <p>WMM Policy Allowed</p> <p>mDNS Mode Bridging</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">Off Channel Scanning Defer</div> <p>Defer Priority <input type="checkbox"/> 0 <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input checked="" type="checkbox"/> 4 <input checked="" type="checkbox"/> 5 <input checked="" type="checkbox"/> 6 <input type="checkbox"/> 7</p> <p>Scan Defer Time 100</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">Assisted Roaming (11k)</div> <p>Prediction Optimization <input type="checkbox"/></p> <p>Neighbor List <input checked="" type="checkbox"/></p> <p>Dual Band Neighbor List <input type="checkbox"/></p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">DTIM Period (in beacon intervals)</div> <p>5 GHz Band (1-255) 1</p> <p>2.4 GHz Band (1-255) 1</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">Device Analytics</div> <p>Advertise Support <input checked="" type="checkbox"/></p> <p>Share Data with Client <input type="checkbox"/></p>
--	---

AP Join Policy Configuration

The default AP join profile values have global AP parameters and the AP group parameters. The AP join profile contains the following parameters - CAPWAP IPv4/IPv6, UDP Lite, High Availability, retransmit configuration parameters, global AP failover, Hyperlocation configuration parameters, Telnet/SSH, 11u parameters, and so on.

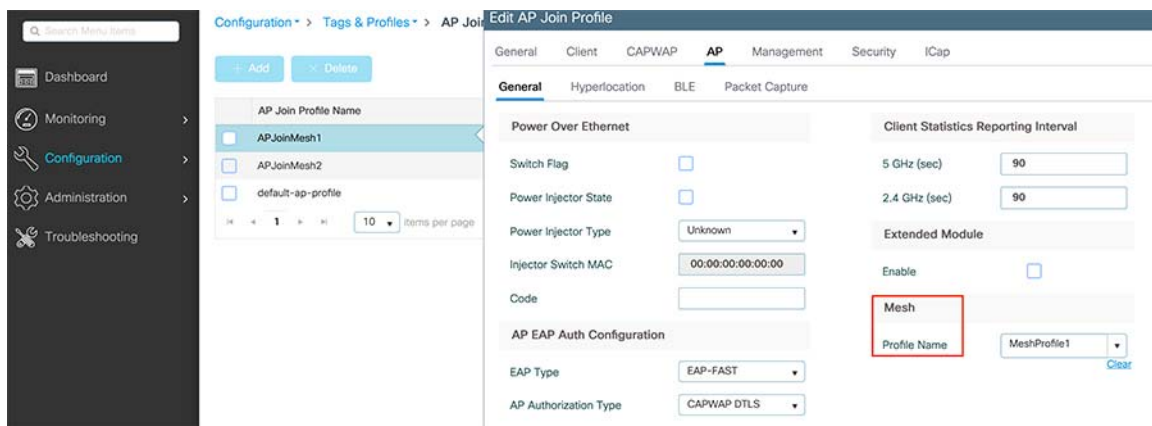
1. To configure a new AP Join policy, go to **Configuration > Tags & Profiles > AP Join**.
2. On AP Join Profile, click **Add**.
3. On the Creating AP Join Profile General tab, enter a name and description for the AP Join Profile and then click **Apply to the device**.

Figure 43 Creating AP Join Profile



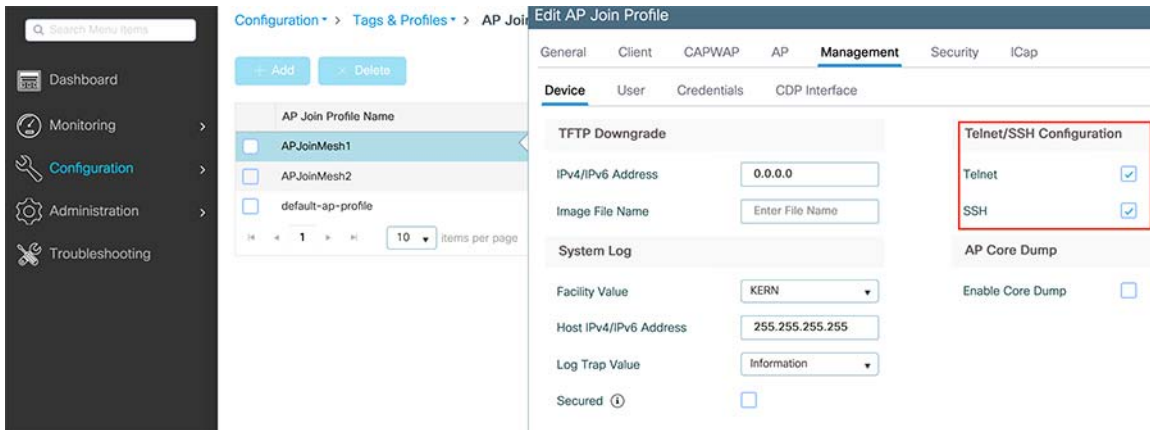
4. Click on the created AP join policy and then go to the AP tab. In the General pane select the Mesh profile that was created in [Configuring Mesh Profile](#).

Figure 44 Associating Mesh Profile to AP Join Policy



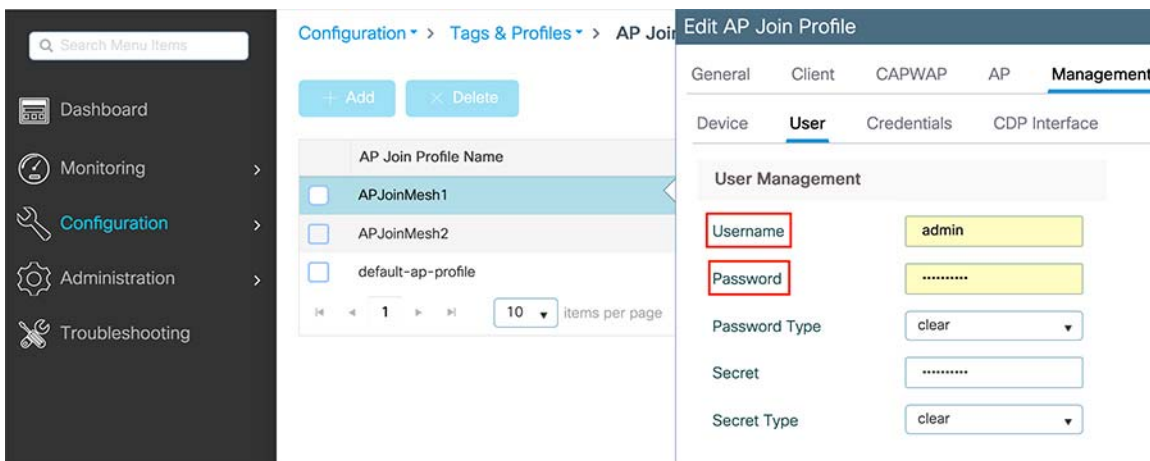
5. On the Management tab:
 - a. In Device tab, enable SSH/Telnet for the access point that joins this profile.

Figure 45 Enabling Telnet/SSH in AP Join Profile



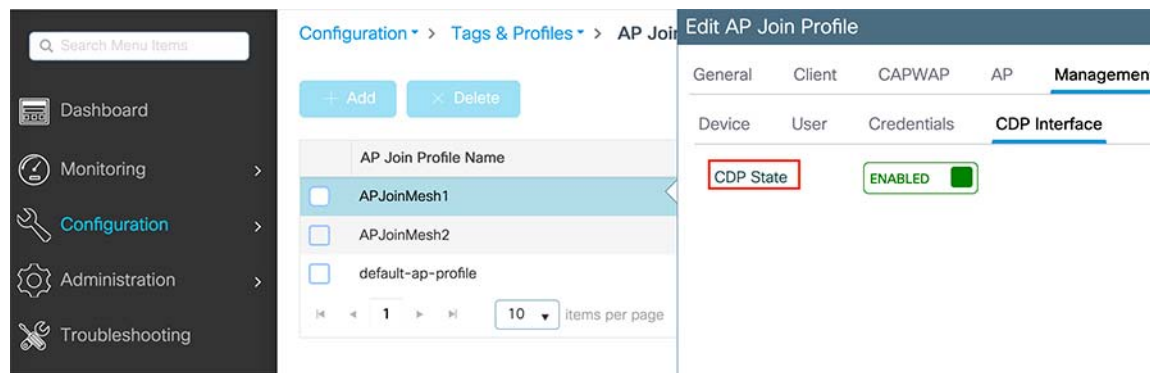
b. On the User tab, configure the username and password for all the access points that join this profile.

Figure 46 Credentials for APs in AP Join Profile



c. On the CDP Interface tab, enable CDP state to enable CDP on the access points.

Figure 47 Enabling CDP in AP Join Profile



6. Click **Update & Apply to Device** to save all the configurations to the AP join profile.

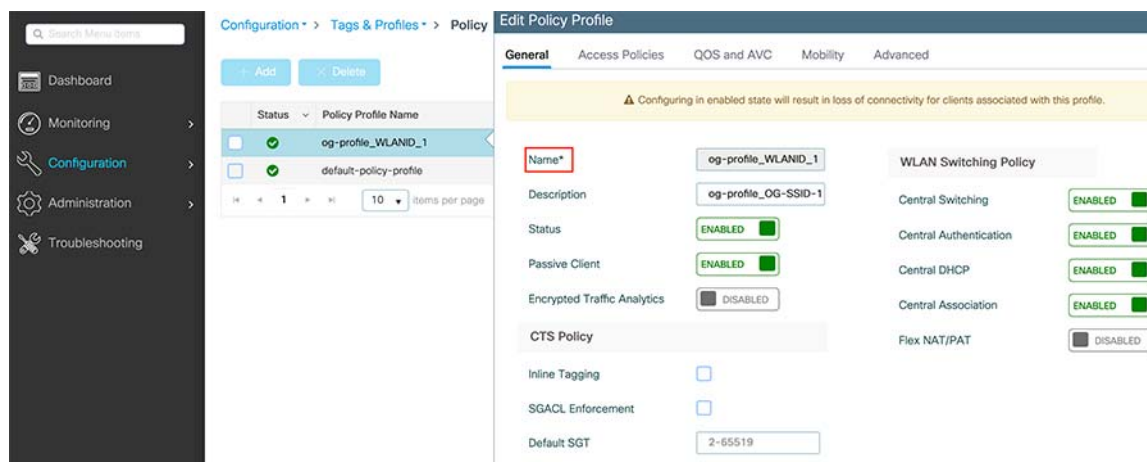
Policy Profile Creation

The policy profile defines the network policies and the switching policies for a client with the exception of QoS which constitute the AP policies as well. Policy profile is a reusable entity across tags.

The WLAN Profile and Policy Profile are both part a Policy Tag and define the characteristics and policy definitions of a set of WLANs.

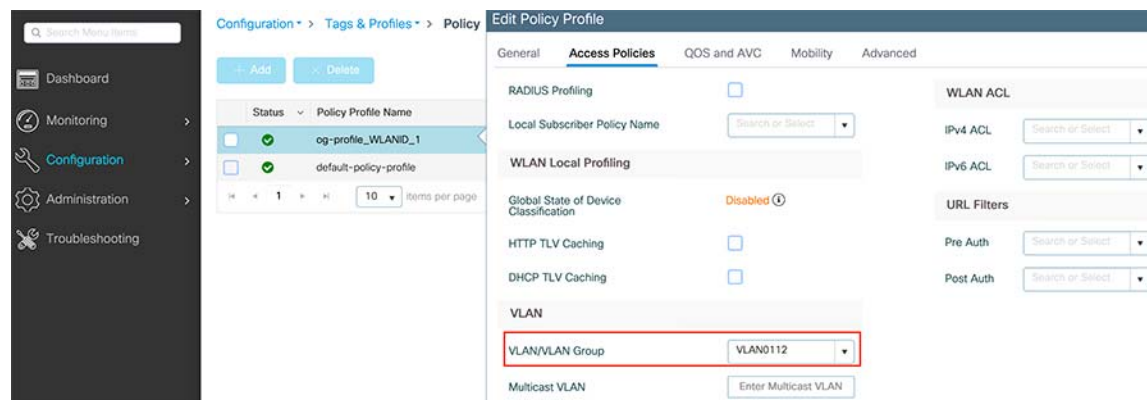
1. To configure the Policy profile, go to **Configuration > Tags & Profiles > Policy** and click **Add** on the Policy page.
2. On the General tab, enter the name, description of the policy profile, and enable passive client.
3. By default all the central switching, central authentication, central DHCP, and central association are enabled.

Figure 48 Creating Policy Profile

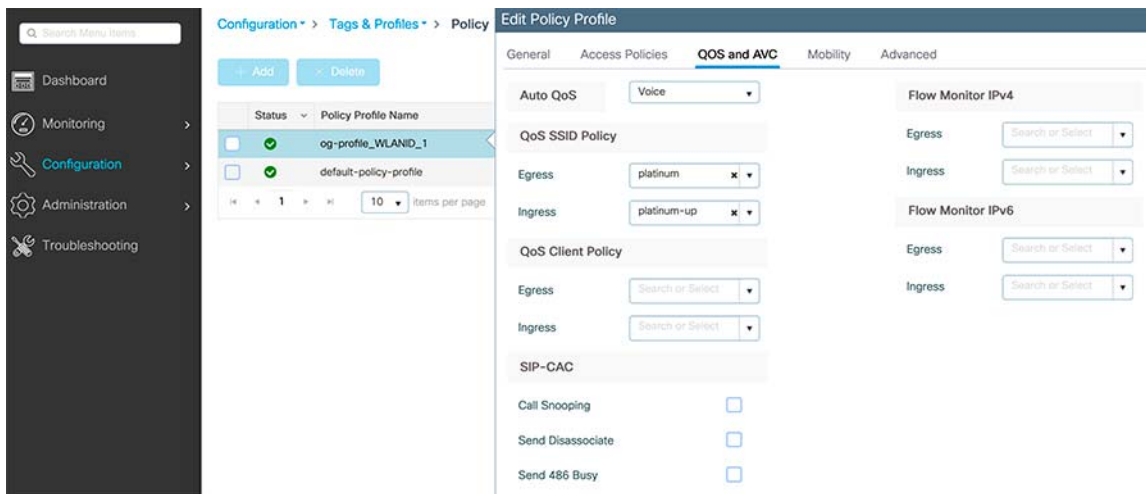


4. On the Access Policies tab, assign the VLAN to the wireless policy profile. When the client connects to the SSID, client gets assigned IP address from the VLAN subnet.

Figure 49 Assigning VLAN to the Policy Profile



5. In QoS and AVC tab, specify QoS SSID Policy as **platinum**.

Figure 50 QoS Configuration in Policy Profile

Tags Configuration

A Policy Tag property is defined by the policies associated to it. A property is inherited from an associated client/AP.

To associate a Policy Tag property to a client AP:

The policy tag is the mapping of the WLAN profile to the Policy profile.

1. To configure policy tag, go to **Configuration > Tags & Profiles > Tags > Policy** and click **Add** in the policy page.
2. Enter a name and description of the Policy tag.
3. Click **Add** in WLAN Policy, and then on that same screen, select the WLAN profile and the Policy profile. This creates the mapping between the WLAN Configuration and Policy Profile. Click the check mark to create the association.

Figure 51 WLAN and Policy Profiles Mapping

Name*

Description

✓ WLAN-POLICY Maps: 2

WLAN Profile	Policy Profile
<input type="checkbox"/> OG-SSID-1	og-profile_WLANID_1
<input type="checkbox"/> test8021x	og-profile_WLANID_1

◀ 1 ▶ 10 items per page 1 - 2 of 2 items

Map WLAN and Policy

WLAN Profile* Policy Profile*

Site Tag

The site tag defines the properties of a site and contains the AP join profile.

1. To configure site tag, go to **Configuration > Tags & Profiles > Tags > Site** and click **Add** to add a new site tag.
2. Enter the name, description, and select the AP join profile that is created in AP join policy Configuration step.
3. Click **Apply to Device**.

Figure 52 Creating Site Tag

Add Site Tag

Name*

Description

AP Join Profile

Control Plane Name

Enable Local Site

RF Tag

The RF tag contains the IEEE 802.11a and IEEE 802.11b RF profiles. The default RF tag contains the global configuration.

1. In this deployment we used global configuration for the RF tag. You can create a new RF Tag by following steps.
2. To Create an RF Tag, go to **Configuration > Tags & Profiles > Tags > RF** and then click **Add**.
3. Enter the name and description of the RF tag.
4. Select global config for 5GHz Band RF Profile and 2.4 GHz Band RF Profile and then click **Apply to Device**.

Figure 53 Creating RF Tag

Name*	og-profile
Description	RF-profile
5 GHz Band RF Profile	Global Config
2.4 GHz Band RF Profile	Global Config

Cancel Apply to Device

NTP Configuration

Network Time Protocol (NTP) is very important for several features. It is mandatory to use NTP synchronization on the Cisco Catalyst 9800 Series Wireless Controller if you use any of these features: Location, SNMP v3, access point authentication, or MFP. The controller supports synchronization with NTP.

1. To configure an NTP server, go to **Administration > Time** and click **Add** on the NTP window.
2. Enter the Hostname or the IP address of the NTP server.
3. By enabling **prefer**, you make sure that the controller reaches this peer first to synchronize first.
4. Cat 9800 can synchronize time whether through VRF or through the interface. You can select either one based on your network configuration. In this document we validated using VRF.
5. After adding the information click **Apply to Device**.

Figure 54 Adding NTP Server

Create NTP Server
✕

Host Name*

Prefer

VRF

VRF Name

Source Address

↶ Cancel

📄
Apply to Device

Verifying Status of NTP Configuration

1. The configuration page shows the Status of the NTP configuration whether the peer is reachable or not.

Figure 55 Verifying NTP Status

NTP Server Details

+ Add
✕ Delete
↻ Refresh NTP Table

	Host Name	Status	VRF Name	Source Address
<input type="checkbox"/>	192.168.133.161	Peer (reachable)	Mgmt-intf	None
<input type="checkbox"/>	192.168.133.171	Candidate (reachable)	Mgmt-intf	None

⏪ 1 ⏩
10 items per page
1 - 2 of 2 items

2. To check the status on the CLI:

```
WLC#show ntp status
Clock is synchronized, stratum 2, reference is 192.168.133.161
nominal freq is 250.0000 Hz, actual freq is 249.9980 Hz, precision is 2**10
ntp uptime is 78621800 (1/100 of seconds), resolution is 4016
reference time is E2025FA9.13B645D8 (10:32:57.077 Eastern Thu Feb 27 2020)
clock offset is 1.4934 msec, root delay is 1.54 msec
root dispersion is 59.14 msec, peer dispersion is 1.12 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000008012 s/s
system poll interval is 1024, last update was 3738 sec ago.
```

3. To check the NTP associations association through CLI:

```
WLC#show ntp associations
address      ref clock      st  when  poll reach  delay  offset  disp
*~192.168.133.161 .MRS.         1   554  1024  377  0.628  1.493  1.129
+~192.168.133.171 .MRS.         1   357  1024  377  0.452  1.575  1.052
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

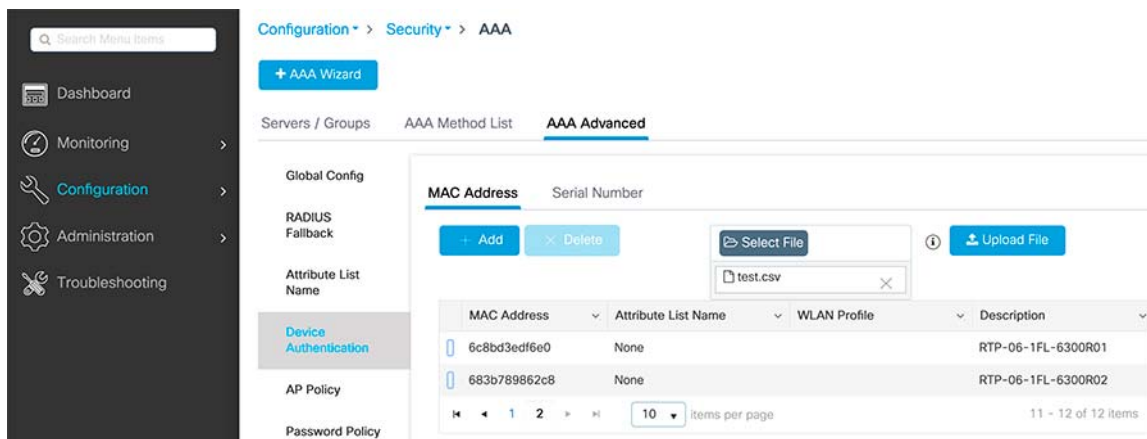

MESH Backhaul Security (MAC Filter)

Before installing your access points, MAC address of all the mesh access points i.e., the MAC address provided at the back of access point must be added to the controller. The controller responds only to those CAPWAP requests from MAPs that are available in its authorization list.

MAC filtering for bridge-mode APs are enabled by default on the controller. Therefore, only the MAC address needs to be configured.

1. To add MAC address to the Controller, go to **Configuration -> Security -> AAA -> AAA Advanced -> Device Authentication**.
2. You can manually add MAC address of access points one-by-one or you can add all the details of the Access Points through a CSV File.
3. To add an access point click **Add**.
4. Enter the MAC Address, description, and WLAN Profile Name of the access point.

Figure 56 MAC Address Configuration to the CAT 9800



5. To add access points through a CSV file should have MAC Address, Attribute List Name, Description, and WLAN Profile Name. MAC Address column is mandatory.
6. Under device authentication tab, select the file that needs to be uploaded and click **Upload File**. You will see a preview of data that is being added.

Figure 57 Example of CSV File for Adding MAC Addresses

dc8c3735ba00		AP in Site 1	Profile Name
dc8c3735ba01		AP in Site 2	Profile Name
dc8c3735ba02		AP in Site 3	Profile Name
dc8c3735ba03		AP in Site 4	Profile Name
dc8c3735ba04		AP in Site 5	Profile Name
dc8c3735ba05		AP in Site 6	Profile Name
dc8c3735ba06		AP in Site 7	Profile Name

Changing an AP Role

In this deployment all the access points need to be in Bridge mode. If the AP is in different mode other than bridge mode, you can change the mode of the AP after it is registered with WLC.

1. To change the access point form GUI, go to **Configuration > Access Points**.
2. Select the access point from the list to change its mode.
3. Under General tab, change the mode of access to bridge.

By default, all the bridge mode Access points join the controller in mesh access point role. After access point got registered in the WLC, the access point role can be changed to RAP, or MAP form the WLC GUI or CLI.

4. To change the access point from GUI, go to the **Configuration > Access points**.
5. Select the access point from the list to change its role.
6. Go to the **Mesh** tab, change the role under General to Mesh/Root based on the requirement.

Figure 58 AP Role as Root

The screenshot displays the WLC GUI configuration for an AP. On the left, a sidebar contains navigation options: Dashboard, Monitoring, Configuration (selected), Administration, and Troubleshooting. The main content area is titled 'Configuration > Wireless > Access Point' and shows a table of 'All Access Points' with 5 total APs. The first AP, 'RTP-06-1FL-6300R02', is selected. Below the table are sections for '5 GHz Radios', '2.4 GHz Radios', 'Dual-Band Radios', and 'Country'. The right-hand side of the screen shows the 'Edit AP' configuration page, with the 'Mesh' tab selected. Under the 'General' section, the 'Role' dropdown menu is highlighted with a red box and set to 'Root'. Other settings include 'Block Child', 'Daisy Chaining', 'Daisy Chaining strict-RAP', 'Preferred Parent MAC' (0000.0000.0000), 'VLAN Trunking Native' (checked, 104), 'Ethernet Port Configuration' (Port: 0, Mode: trunk, Native VLAN ID*: 104, Allowed VLAN IDs: 113,112), 'Backhaul' (Backhaul Radio Type: 5ghz, Backhaul Slot ID: 1, Rate Types: auto), and 'Remove PSK'.

7. You can change the AP role from the controller CLI using the command:

```
ap name ap-name role {mesh-ap | root-ap}
```

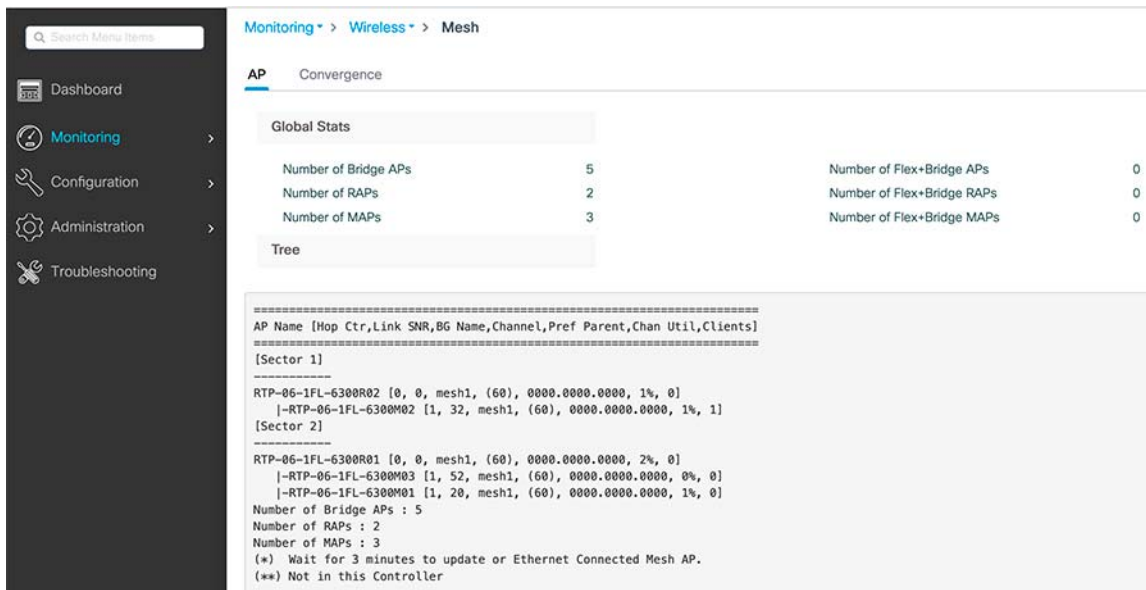
Note: There should be at least two RAPs in the network for resiliency and stability of the network.

Verifying Mesh

The mesh network that is formed can be verified from the WLC GUI or CLI. Prime Infrastructure can also be used to view the Mesh topology. For more details on Prime Infrastructure refer to the [Network Management with Prime Infrastructure and Connected Mobile Experience \(CMX\)](#), page 23 in this document.

1. To view the Mesh formed from the controller GUI, go to **Monitoring > Wireless > Mesh**. See [Figure 59](#) below.

Figure 59 Monitor Wireless Mesh from WLC



2. You can also view the formed Mesh from the controller CLI using the command:

```
WLC#show wireless mesh ap tree
```

Ethernet Bridging Configuration

Ethernet bridging allows multiple remote wired networks to connect to each other using the Ethernet port of the MAPs. For ethernet bridging to work, every MAP and RAP in the path must have Ethernet bridging enabled along the path. By default, for security reasons the ethernet port on the MAPs are disabled.

For Mesh deployments with VLAN support for Ethernet bridging, the secondary Ethernet interfaces on MAPs are assigned a VLAN individually.

Ethernet bridging should be enabled for the following scenarios in our deployment:

- Integration of Emerson Sensors
- Video Surveillance

For detail description of Integration of Emerson Sensors and Video Surveillance, see the use cases section in this document.

1. To configure Ethernet bridging, go to **Configuration > Wireless > Mesh > Profiles**.
2. Click the **already created Mesh profile** and go to the Advanced tab.
3. Enable **Ethernet bridging** and then click **Update & Apply to Device**.
4. Go to **Configuration > Access Points**.

RAP Configuration

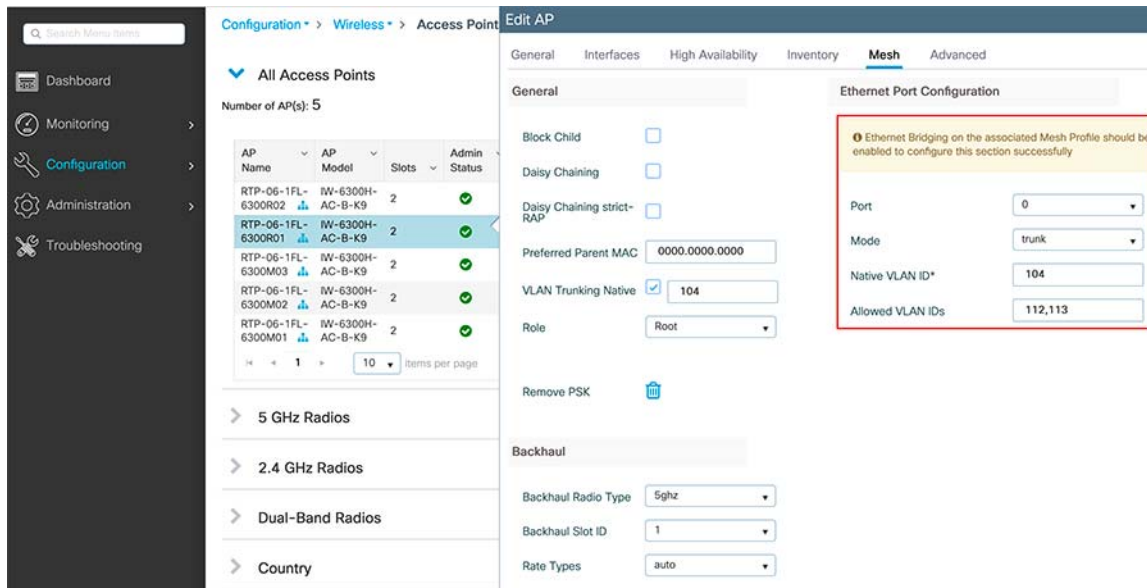
1. Select **RAP** and go to the Mesh tab to enable **VLAN Trunking Native** and add the access point native VLAN.

Figure 60 Enabling Ethernet Bridge on Mesh Profile

The screenshot shows the 'Edit Mesh Profile' configuration interface. The 'Advanced' tab is selected. The 'Ethernet Bridging' section is highlighted with a red box, showing the 'Ethernet Bridging' checkbox checked. Other sections include 'Security' (Method: PSK, Authentication Method: Enter Method, Authorization Method: default), '5 GHz Band Backhaul' (Rate Types: auto), '2.4 GHz Band Backhaul' (Rate Types: auto), and 'Bridge Group' (Bridge Group Name: mesh1, Strict Match: checked). At the bottom, there are 'Cancel' and 'Update & Apply to Device' buttons.

2. Under the Mesh tab, configure the port that is connected to switch as trunk port with native VLAN as AP's VLAN and allowed VLANs should be the VLANs that are planned to use Ethernet bridging.
3. For example in this deployment model, Emerson Sensors are on VLAN 113, IP Cameras are on VLAN 114 and Access points are on VLAN 104. So, native VLAN should be VLAN 104, and allowed VLANs need to be VLAN 113 and VLAN 114.

Figure 61 Ethernet Bridge Configuration on RAP



MAP Configuration

1. Select the MAP from the access points list under Configuration -> Access Points.
2. Under mesh tab, configure the port where equipment to connected as access port.

Note:

- Ensure that Ethernet bridging is enabled for every parent mesh AP taking the path from the mesh AP to the controller.
- Unified VLAN database across all the MAPs (If desired VLANs not in all MAPs, then in the event of a failure within the mesh network it is possible to break the bridging feature if a MAP in the new path to the RAP does not support a particular VLAN)
- The switchport where RAP is connected on the switch needs to be configured as trunk port. The trunk port and wired switch trunk port setting must be match to each other.
- MAPs using Ethernet bridging VLAN transparency to perform Ethernet bridging when extending the Layer 2 network which assumes that all traffic is destined to and from the same VLAN with no 802.1 tagging. To allow multiple VLAN bridging/tagging, you must disable VLAN transparency
- When Ethernet bridging enabled:
 - The wireless clients Traffic flow is unchanged. (The wireless client packets are sent using LAP/CAPWAP data, which is sent through the encrypted backhaul to the controller. The controller then bridges that traffic to the wired network.)
 - The bridged wired client traffic flow, however, is bridged directly into the backhaul toward the RAP. The RAP then bridges the traffic directly onto the wired network. The wired bridged traffic is not sent back to the controller.

WLC 802.1x AAA Server Configuration

Configuring the Radius Server, Authentication Method List, and applying the Method List on a WLAN will allow ISE to handle AAA services.

1. Declare a RADIUS server. Navigate to **Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > +Add**.

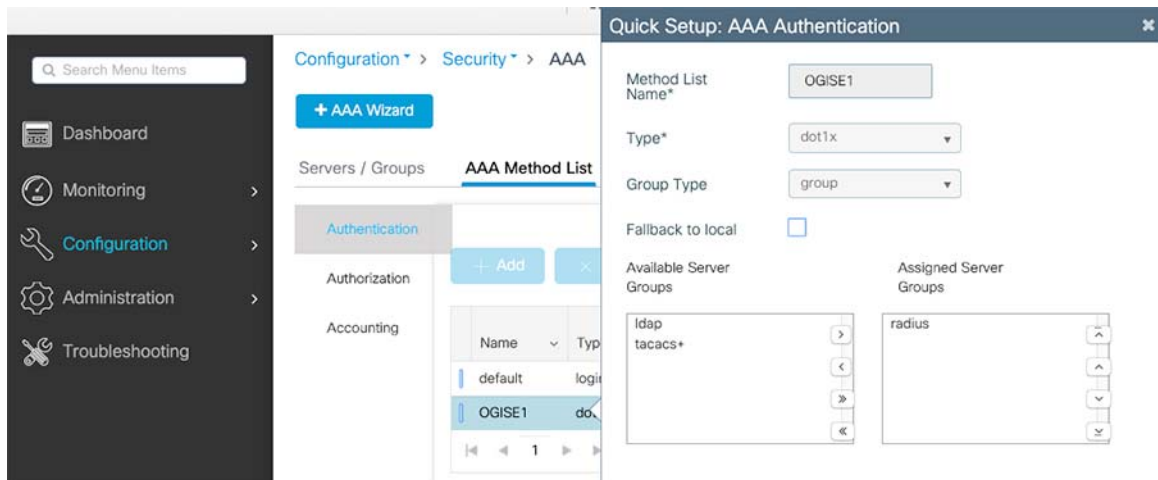
Figure 62 Radius Server Configuration

The screenshot displays the Cisco ISE configuration interface for editing a RADIUS server. The breadcrumb navigation is **Configuration > Security > AAA**. The left sidebar shows the **Configuration** menu selected. The main area shows the **Servers / Groups** section with a table containing one entry named **OGISE**. The right panel shows the configuration details for the **OGISE** server.

Name*	OGISE
Server Address*	10.5.1.19
PAC Key	<input type="checkbox"/>
Key Type	0
Key*
Confirm Key*
Auth Port	1812
Acct Port	1813
Server Timeout (seconds)	1-1000
Retry Count	0-100
Support for CoA	ENABLED <input checked="" type="checkbox"/>

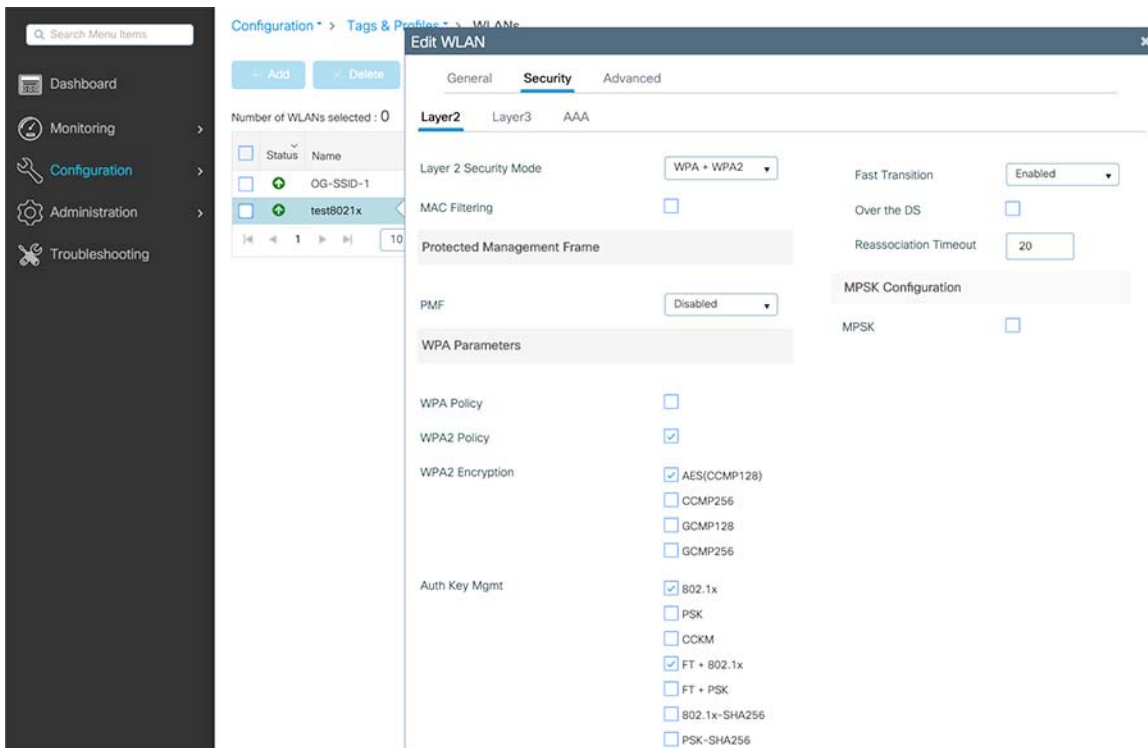
2. Create an Authentication Method List. Navigate to **Configuration > Security > AAA > AAA Method List > Authentication > +Add**.

Figure 63 Authentication Method List

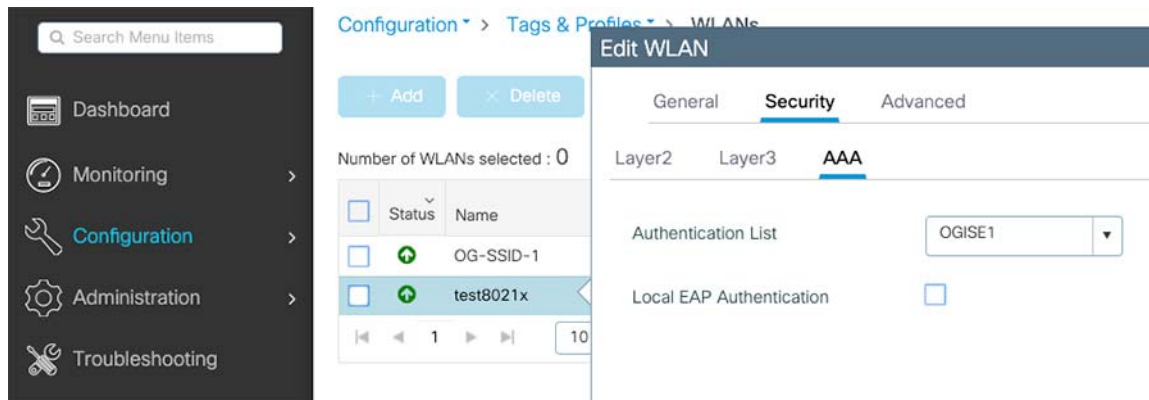


3. Apply 802.1x Config to WLAN. Navigate to **Configuration > Tags & Profiles > WLANs > Select the desired WLAN > Security > Layer 2**.

Figure 64 WLAN 802.1x Configuration



4. Apply Authentication Method List to 802.1x WLAN. Navigate to **Configuration > Tags & Profiles > WLANs > Select the desired WLAN > Security > AAA > Authentication List**.

Figure 65 WLAN Authentication Method List Configuration

For a detailed implementation guide, refer to:

Configure 802.1x Authentication on Catalyst 9800 Wireless Controller Series

<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213919-configure-802-1x-authentication-on-catal.html>

Brownfield Deployment Model

WLC configuration follows Cisco Wireless MESH Networking design guide (Mobility 8.5 Design Guide) with the exception of the following for O&G outdoor deployment:

AireOS (8.5) to AireOS (8.10) Deployment

Configuring HA SSO on 3504 or 5520

WLC3504 and WLC5520 is enabled with high availability between its peer controllers to reduce downtime, which reply on each of the HA primary and backup WLC to keep a mirror copy of AP and the client database. HA is enabled by inter-connecting the Primary and back WLC dedicated redundant ports. Detailed Cisco WLC controller for 3504 and 5520 High Availability (SSO) deployment can be refer to *High Availability (SSO) Deployment Guide*. The following is the detailed example for O&G brownfield deployment configuration.

Figure 66 3504 WLC Controller Redundancy Management Interface Configuration

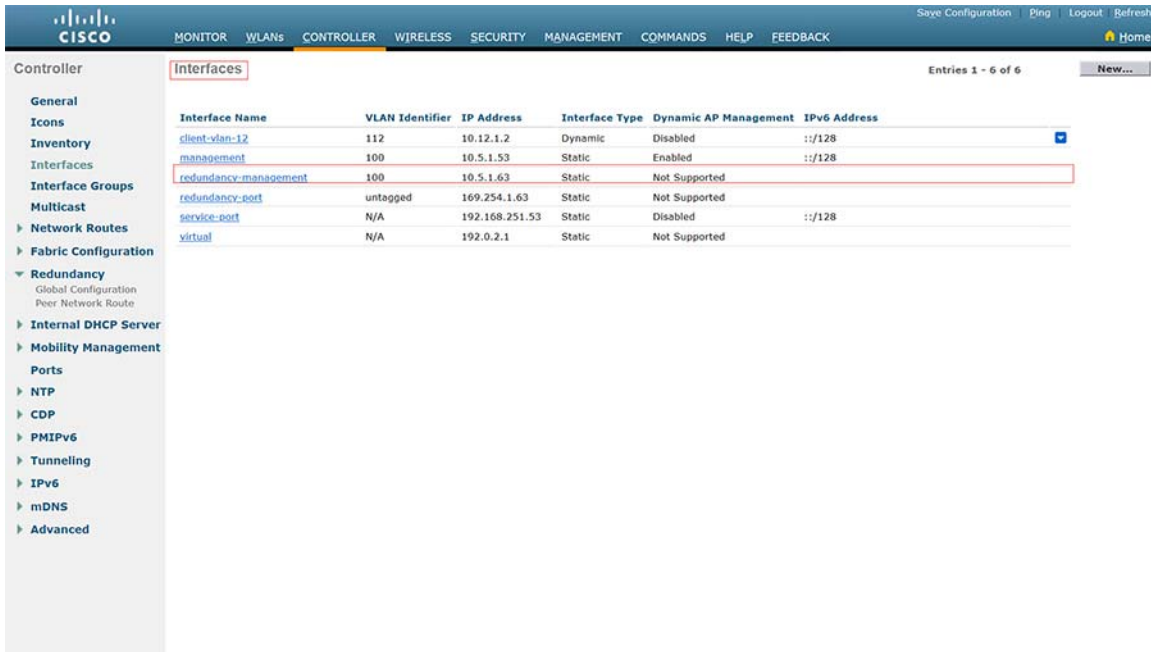


Figure 67 3504 WLC Controller Redundancy Global Configuration

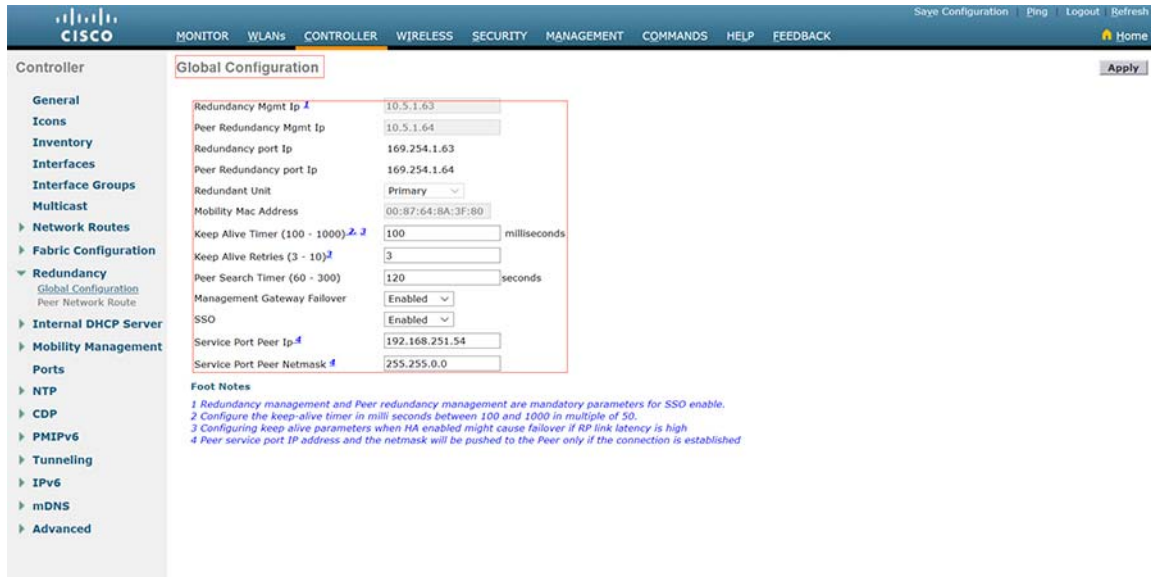


Figure 68 5520 WLC Controller Redundancy Management Interface Configuration

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
client-vlan-112	112	10.12.1.3	Dynamic	Disabled	:::128
management	100	10.5.1.55	Static	Enabled	:::128
redundancy-management	100	10.5.1.65	Static	Not Supported	
redundancy-port	untagged	169.254.1.65	Static	Not Supported	
service-port	N/A	192.168.251.55	Static	Disabled	:::128
virtual	N/A	192.0.2.1	Static	Not Supported	

Figure 69 5520 WLC Controller Redundancy Global Configuration

Redundancy Mgmt Ip: 10.5.1.65

Peer Redundancy Mgmt Ip: 10.5.1.66

Redundancy port Ip: 169.254.1.65

Peer Redundancy port Ip: 169.254.1.66

Redundant Unit: Primary

Mobility Mac Address: 6C:AB:05:88:44:09

Keep Alive Timer (100 - 1000): 100 milliseconds

Keep Alive Retries (3 - 10): 3

Peer Search Timer (60 - 300): 120 seconds

Management Gateway Fallover: Enabled

Link encryption: Disabled

SSO: Enabled

Service Port Peer Ip: 192.168.251.56

Service Port Peer Netmask: 255.255.0.0

Foot Notes

1 Redundancy management and Peer redundancy management are mandatory parameters for SSO enable.
 2 Configure the keep-alive timer in milli seconds between 100 and 1000 in multiple of 50.
 3 Configuring keep alive parameters when HA enabled might cause fallover if RP link latency is high
 4 Peer service port IP address and the netmask will be pushed to the Peer only if the connection is established

Verifying HA SSO Configuration

3504:

```
(Cisco Controller) >show sysinfo
```

```
Manufacturer's Name..... Cisco Systems Inc.
Product Name..... Cisco Controller
Product Version..... 8.5.152.102
RTOS Version..... 8.5.152.102
```

Detailed Configuration of the Deployment Models

```

Bootloader Version..... 8.5.103.0
Emergency Image Version..... 8.5.103.0

OUI File Last Update Time..... N/A
Build Type..... DATA + WPS

System Name..... IA-OG-3504-WLC-1
System Location.....
System Contact.....
System ObjectID..... 1.3.6.1.4.1.9.1.2427
Redundancy Mode..... SSO
IP Address..... 10.5.1.53
IPv6 Address..... ::
Last Reset..... Soft reset due to RST_SOFT_RST write
System Up Time..... 86 days 3 hrs 15 mins 51 secs
System Timezone Location..... (GMT -5:00) Eastern Time (US and Canada)
System Stats Realtime Interval..... 5

System Stats Normal Interval..... 180

Configured Country..... US - United States
Operating Environment..... Commercial (10 to 35 C)
Internal Temp Alarm Limits..... -10 to 80 C
Internal Temperature..... +60 C
Mgig Temp Alarm Limits..... -10 to 78 C
Mgig Temperature..... +50 C
External Temp Alarm Limits..... -10 to 71 C
External Temperature..... +46 C
Fan Status..... OK
Fan Speed Mode..... Disable

State of 802.11b Network..... Disabled
State of 802.11a Network..... Enabled
Number of WLANs..... 2
Number of Active Clients..... 0

OUI Classification Failure Count..... 5

Memory Current Usage..... 36
Memory Average Usage..... 36
CPU Current Usage..... 0

CPU Average Usage..... 0

Flash Type..... Compact Flash Card
Flash Size..... 1073741824

Burned-in MAC Address..... 00:87:64:8A:3F:80
Maximum number of APs supported..... 150
System Nas-Id.....
WLC MIC Certificate Types..... SHA1/SHA2
Licensing Type..... RTU
    
```

```

(Cisco Controller) >show redundancy summary
    Redundancy Mode = SSO ENABLED
        Local State = ACTIVE
        Peer State = STANDBY HOT
            Unit = Primary
            Unit ID = 00:87:64:8A:3F:80
    Redundancy State = SSO
        Mobility MAC = 00:87:64:8A:3F:80
        Redundancy Port = UP
        BulkSync Status = Complete
    
```

Detailed Configuration of the Deployment Models

Average Redundancy Peer Reachability Latency = 162 Micro Seconds
 Average Management Gateway Reachability Latency = 747 Micro Seconds

5520:

(Cisco Controller) >show sysinfo

```

Manufacturer's Name..... Cisco Systems Inc.
Product Name..... Cisco Controller
Product Version..... 8.10.105.0
RTOS Version..... 8.10.105.0
Bootloader Version..... 8.3.15.177
Emergency Image Version..... 8.3.143.0

OUI File Last Update Time..... Tue Feb 06 10:44:07 UTC 2018

Build Type..... DATA + WPS

System Name..... IA-OG-5520-WLC-1
System Location.....
System Contact.....
System ObjectID..... 1.3.6.1.4.1.9.1.2170
Redundancy Mode..... SSO
IP Address..... 10.5.1.55
IPv6 Address..... ::
System Up Time..... 73 days 7 hrs 12 mins 7 secs
System Timezone Location..... (GMT -5:00) Eastern Time (US and Canada)
System Stats Realtime Interval..... 5

System Stats Normal Interval..... 180

Configured Country..... US - United States
Operating Environment..... Commercial (10 to 35 C)
Internal Temp Alarm Limits..... 10 to 38 C
Internal Temperature..... +22 C
Fan Status..... OK

State of 802.11b Network..... Enabled
State of 802.11a Network..... Enabled
Number of WLANs..... 2
Number of Active Clients..... 2

OUI Classification Failure Count..... 21

Memory Current Usage..... 11
Memory Average Usage..... 11
CPU Current Usage..... 0
CPU Average Usage..... 0

Flash Type..... Compact Flash Card
Flash Size..... 1073741824

Burned-in MAC Address..... 6C:AB:05:88:44:09
Power Supply 1..... Present, OK
Power Supply 2..... Absent/Failed
Maximum number of APs supported..... 1500
System Nas-Id.....
WLC MIC Certificate Types..... SHA1/SHA2
Licensing Type..... RTU

```

```

(Cisco Controller) >show redundancy summary
Redundancy Mode = SSO ENABLED
Local State = ACTIVE
Peer State = STANDBY HOT

```

Detailed Configuration of the Deployment Models

```
Unit = Primary
Unit ID = 6C:AB:05:88:44:09
Redundancy State = SSO
Mobility MAC = 6C:AB:05:88:44:09
Redundancy Port = UP
BulkSync Status = Complete
Link Encryption = DISABLED
Average Redundancy Peer Reachability Latency = 264 Micro Seconds
Average Management Gateway Reachability Latency = 693 Micro Seconds
```

Mesh Configurations

General MESH WLAN employs outdoor mesh access points (APs: 1552 and IW6300 mesh APs) along with the Cisco Wireless LAN Controller (WLC), and Cisco Prime Infrastructure to provide scalable, central management and mobility for O&G customers. The Control and Provisioning of Wireless Access Points (CAPWAP) protocol manages the connection of the mesh APs to the network.

The following is the WLC configuration on 3504 and 5520 controllers, where, 5Ghz radio will act as down link backhaul, 2.4Ghz radio will be used for client access, convergence mode will be configured with "VERYFAST" with Channel Change Notification (CCN) and background Scanning enabled for fast convergence.

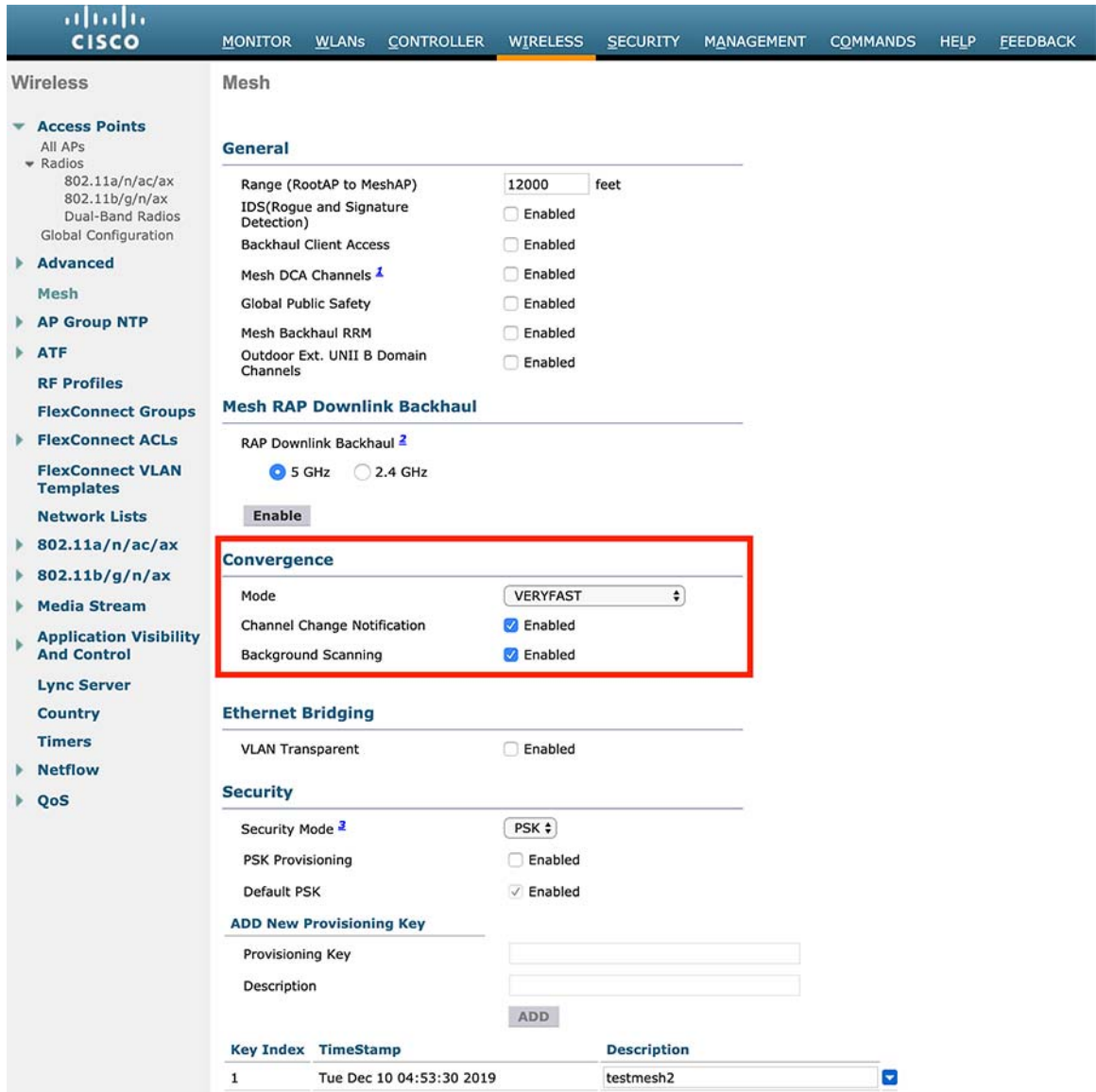
Figure 70 WLC3504 Mesh Configuration

The screenshot displays the Cisco WLC3504 Mesh Configuration interface. The left sidebar shows the navigation menu with 'Wireless' selected. The main content area is divided into several sections:

- General:**
 - Range (RootAP to MeshAP): 12000 feet
 - IDS(Rogue and Signature Detection): Enabled
 - Backhaul Client Access: Enabled
 - Mesh DCA Channels: Enabled
 - Global Public Safety: Enabled
 - Mesh Backhaul RRM: Enabled
 - Outdoor Ext. UNII B Domain Channels: Enabled
- Mesh RAP Downlink Backhaul:**
 - RAP Downlink Backhaul: 5 GHz 2.4 GHz
 - Enable button
- Convergence (highlighted in red):**
 - Mode: VERYFAST (dropdown)
 - Channel Change Notification: Enabled
 - Background Scanning: Enabled
- Ethernet Bridging:**
 - VLAN Transparent: Enabled
- Security:**
 - Security Mode: PSK (dropdown)
 - PSK Provisioning: Enabled
 - Default PSK: Enabled
- ADD New Provisioning Key:**
 - Provisioning Key:
 - Description:
 - ADD button
- Table:**

Key Index	TimeStamp	Description
1	Wed Nov 13 12:29:03 2019	testmesh2

Figure 71 WLC5520 Mesh Configuration



Configuration Steps

3504 and 5520

1. For configuring MESH go to Wireless tab, select each AP > MESH.
2. Assign AP Role, Bridge Group Name, select Strict Matching BGN (optional), VLAN, Native VLAN, and Mesh backhaul as shown below.
3. Repeat these steps for each AP.

Detailed Configuration of the Deployment Models

Figure 72 1552 RAP MESH Configuration

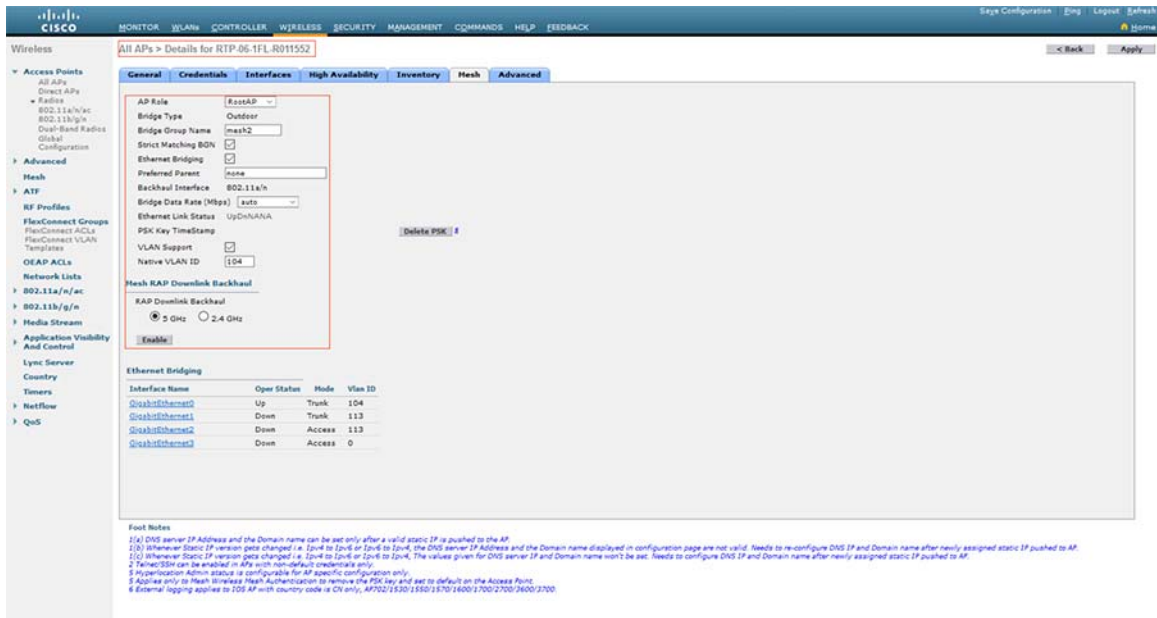


Figure 73 1552 MAP MESH Configuration

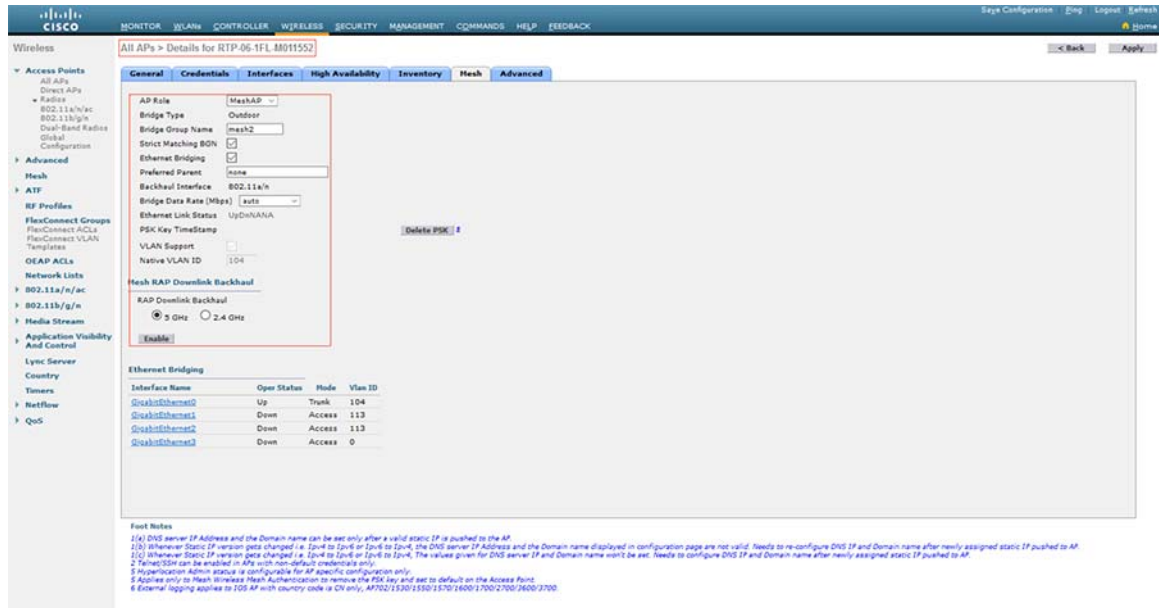


Figure 74 6300 RAP MESH Configuration

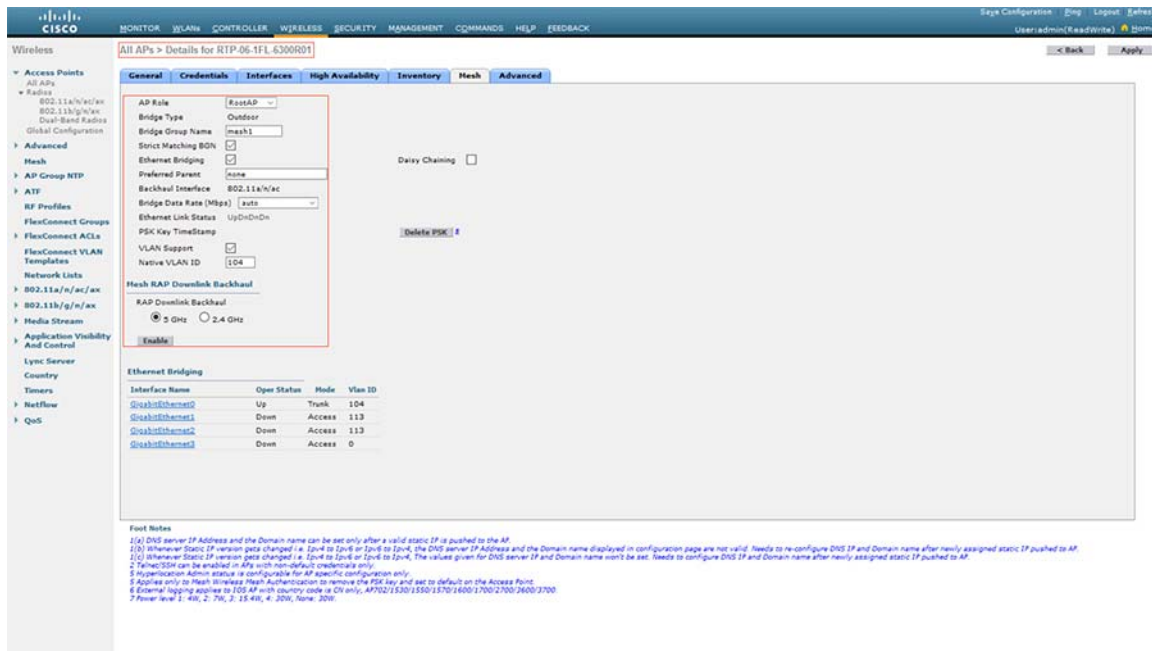
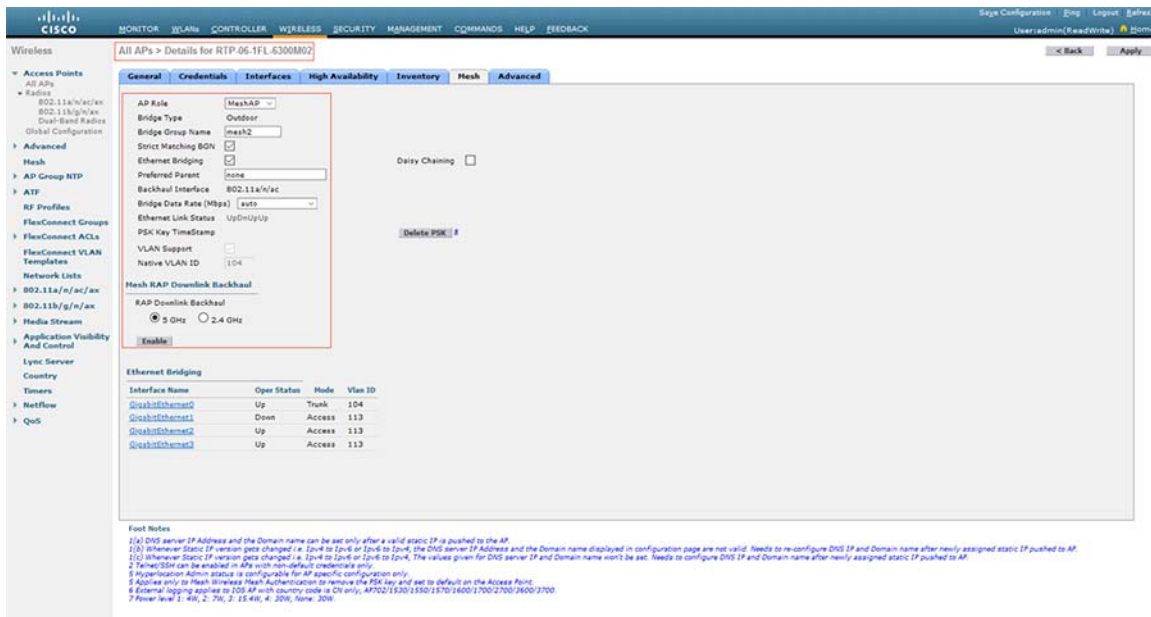


Figure 75 6300 MAP MESH Configuration



Note: Each MESH AP has default PSK key configured when ship out from factory, it is a customer's preference to rekey them to enforce MESH infrastructure segmentation and security. When proceeding with new MESH key re-configuration, follow MAP-RAP sequences to prevent MAP AP connection loss.

Detailed Configuration of the Deployment Models

MESH Backhaul Security (MAC Filter)

Before installing your access points, both controllers must be configured with radio MAC address for all mesh access points that are planning to use in the mesh network to the filter list.

A controller only responds to discovery requests from outdoor radios that appear in its authorization list. MAC filtering is enabled by default on the controller, so only the MAC addresses need to be configured.

MAC addresses of the mesh access point can be added to MAC filter list of the WLC using either the GUI or the CLI.

Both controllers AireOS need to have same mac address list under Mac filter tab for 1552 and IW6300 to co-exist in the network.

Figure 76 3504 MAC Filter Configuration

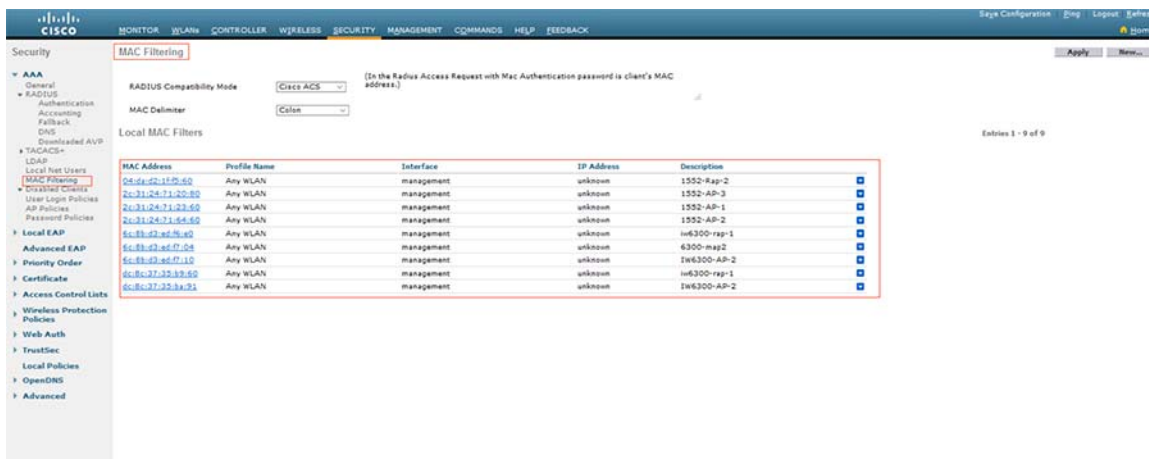
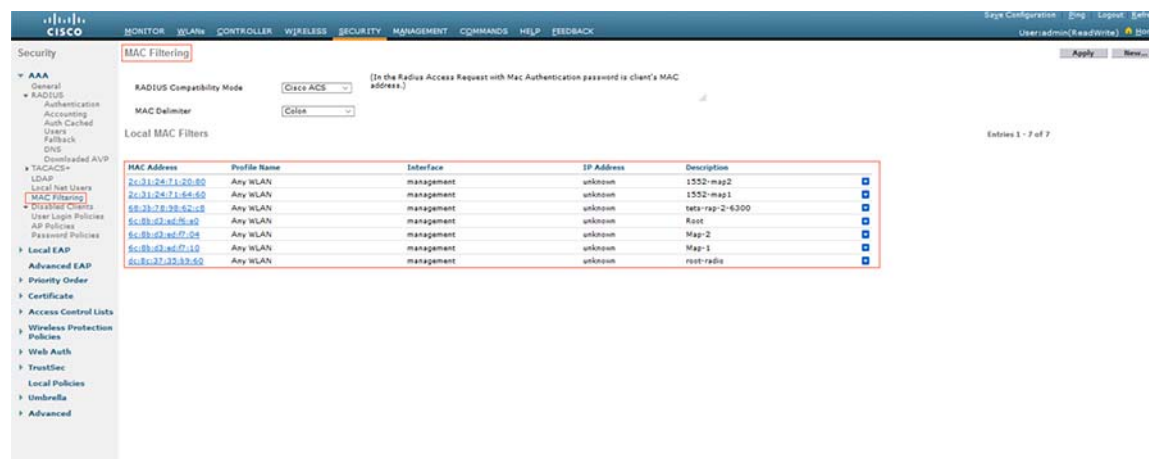


Figure 77 5520 MAC Filter Configuration



WLAN Configurations

O&G MESH WLAN infrastructure deployment follows [Cisco Wireless MESH Design & Deployment Guide, Release 8.6](#) with the following snapshots to show a detailed deployment examples for controller and WLAN respectively.

3504

Figure 78 3504 WLC Controller Interface Configuration

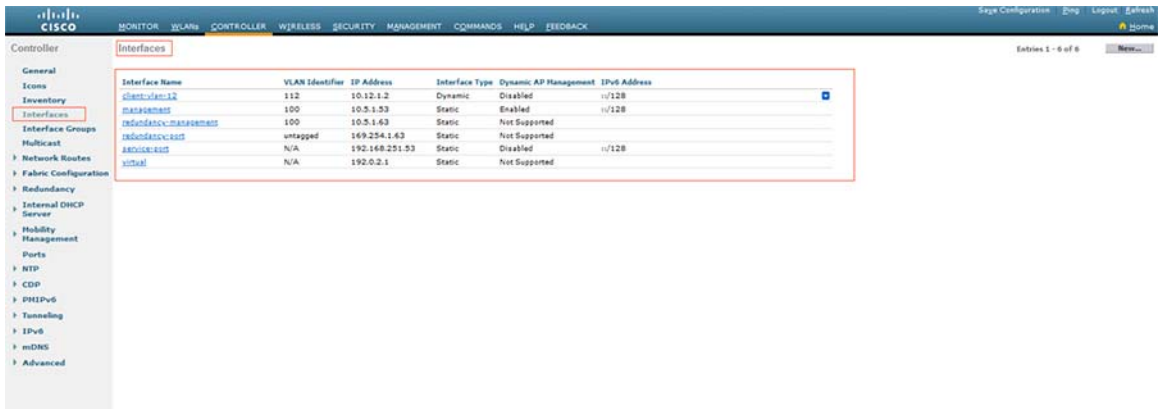


Figure 79 3504 WLC Controller Management Interface Configuration



Figure 80 3504 WLC Controller Dynamic Interface Configuration

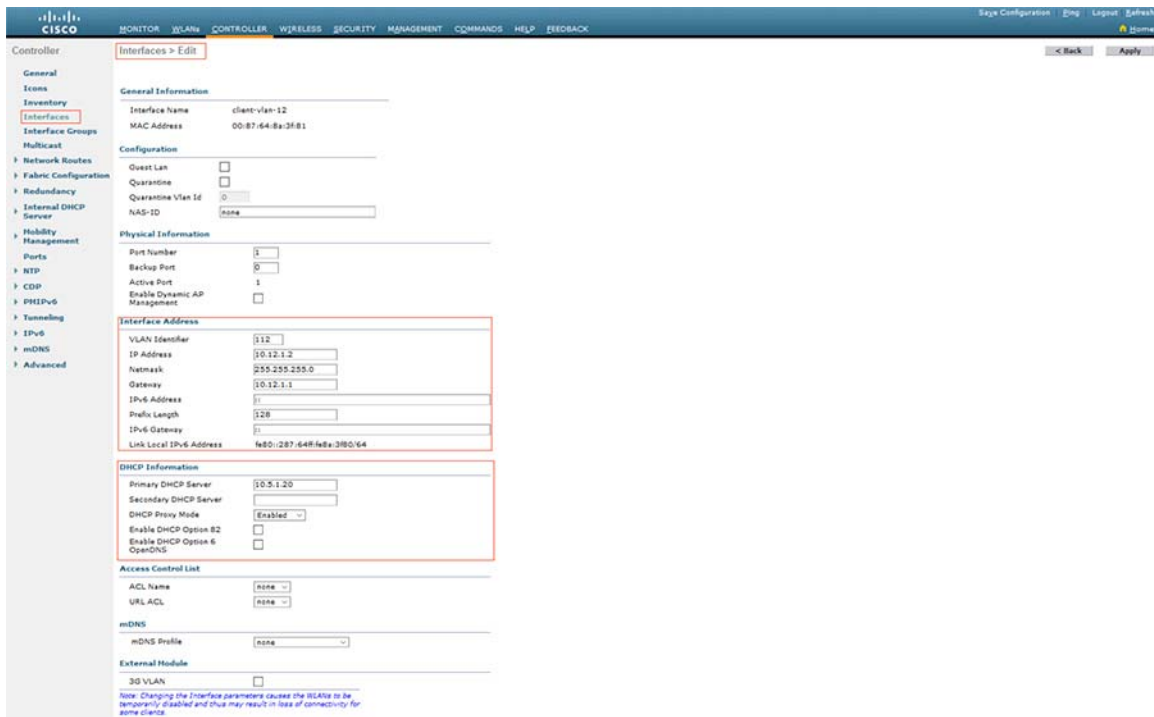


Figure 81 3504 WLAN Configuration

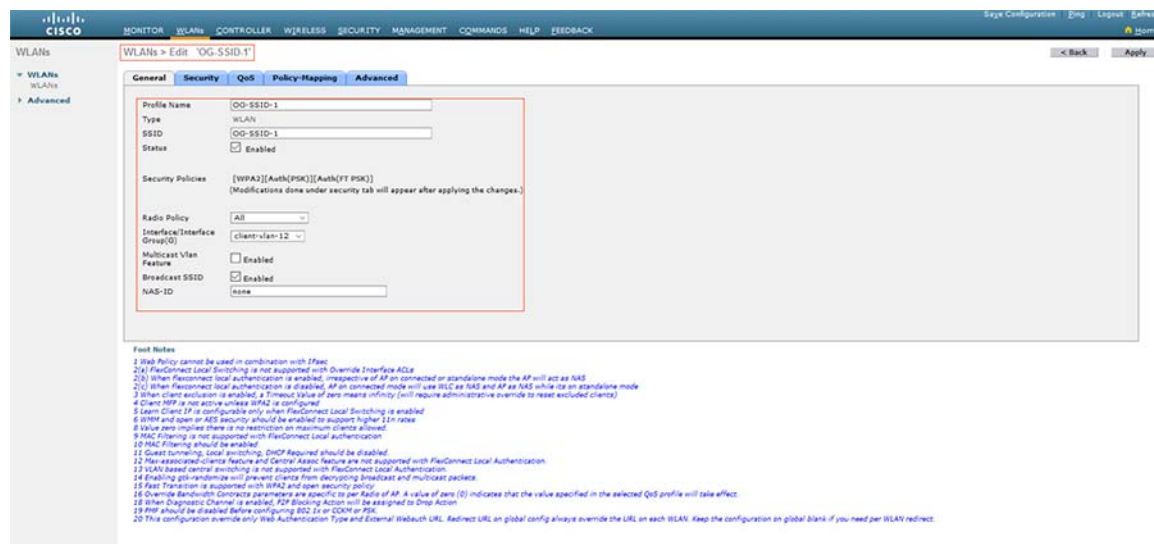
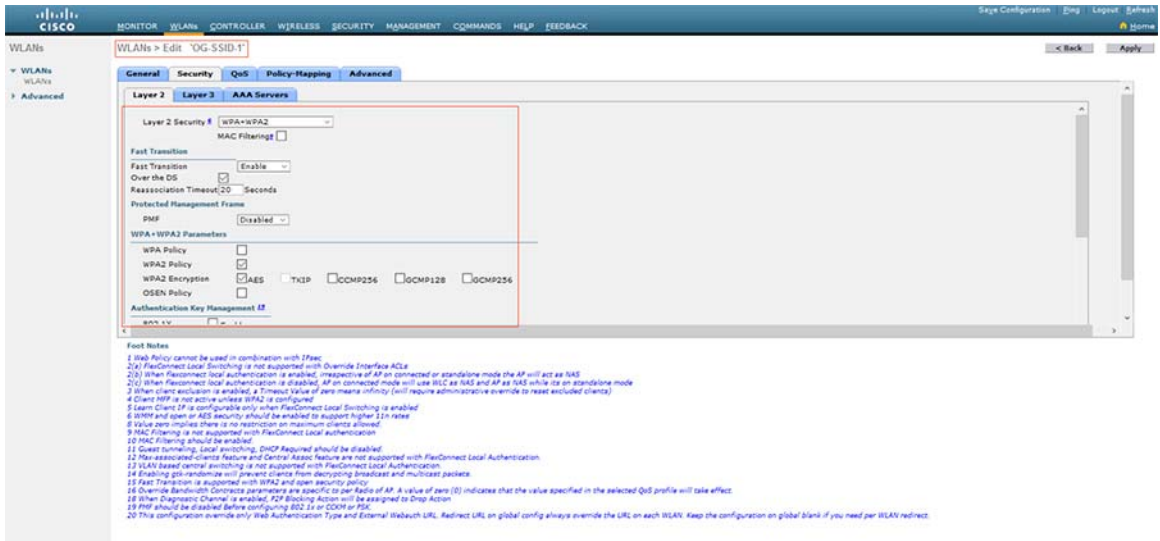
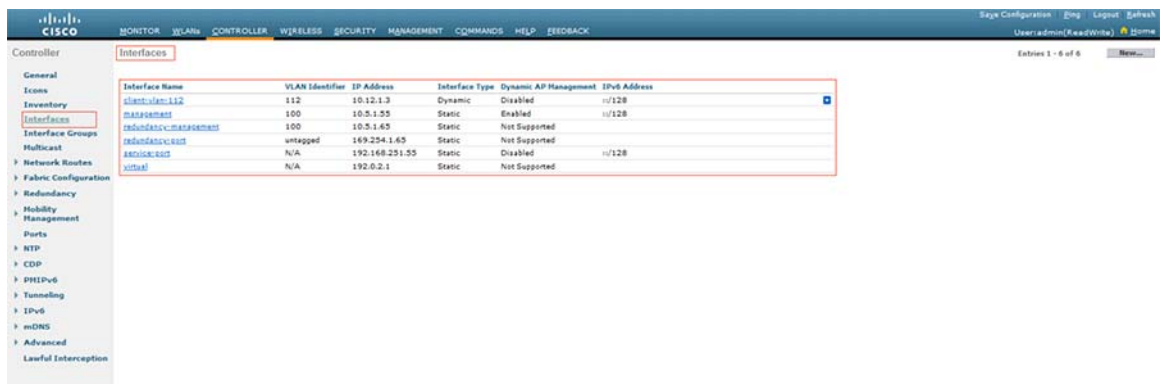


Figure 82 3504 WLAN Security Configuration



5520

Figure 83 5520 WLC Controller Interface Configuration



Detailed Configuration of the Deployment Models

Figure 84 5520 WLC Controller Management Interface Configuration

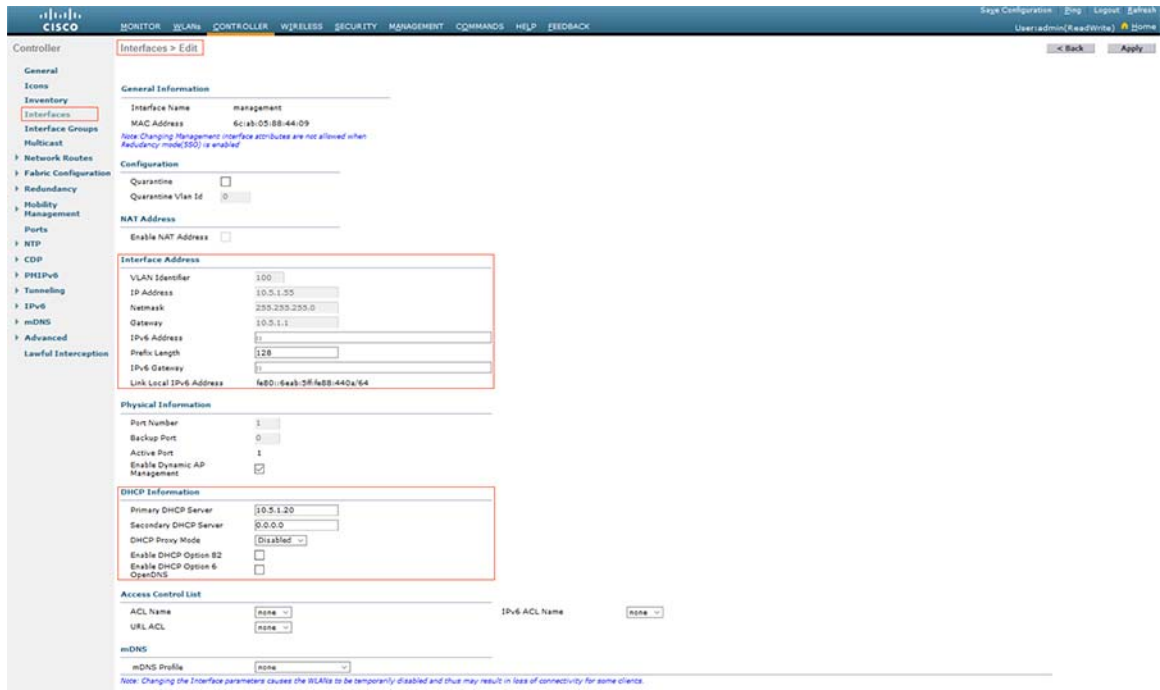
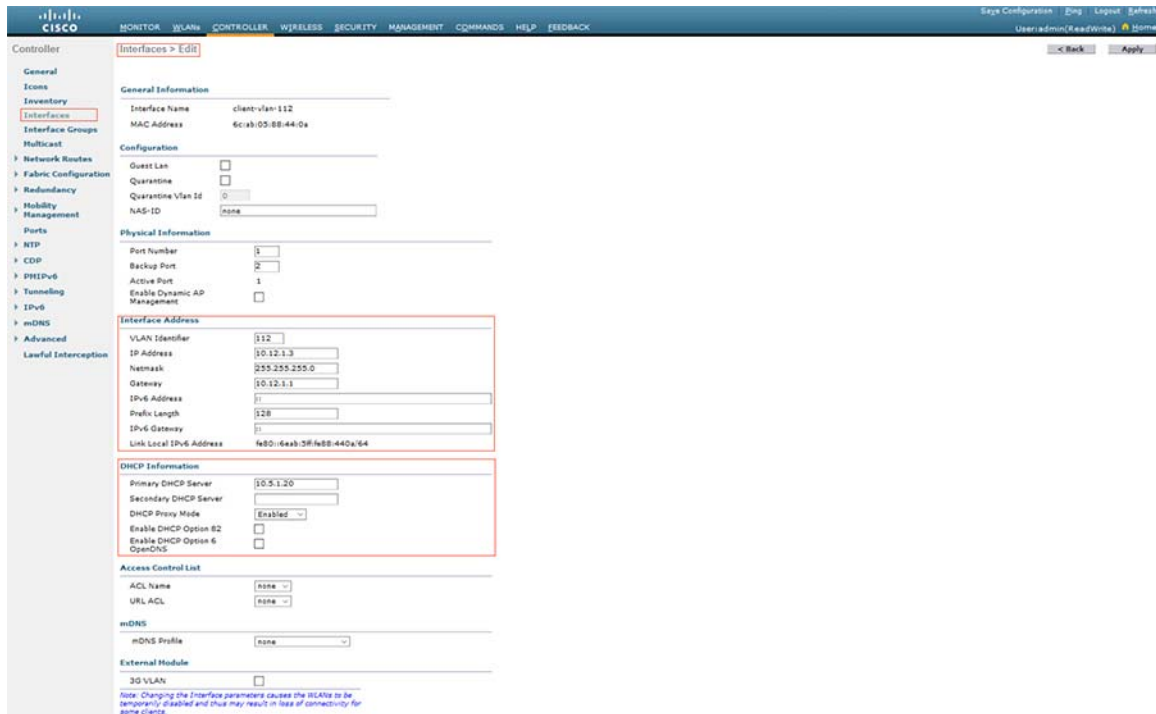


Figure 85 5520 WLC Controller Dynamic Interface Configuration



Detailed Configuration of the Deployment Models

Figure 86 5520 WLAN Configuration

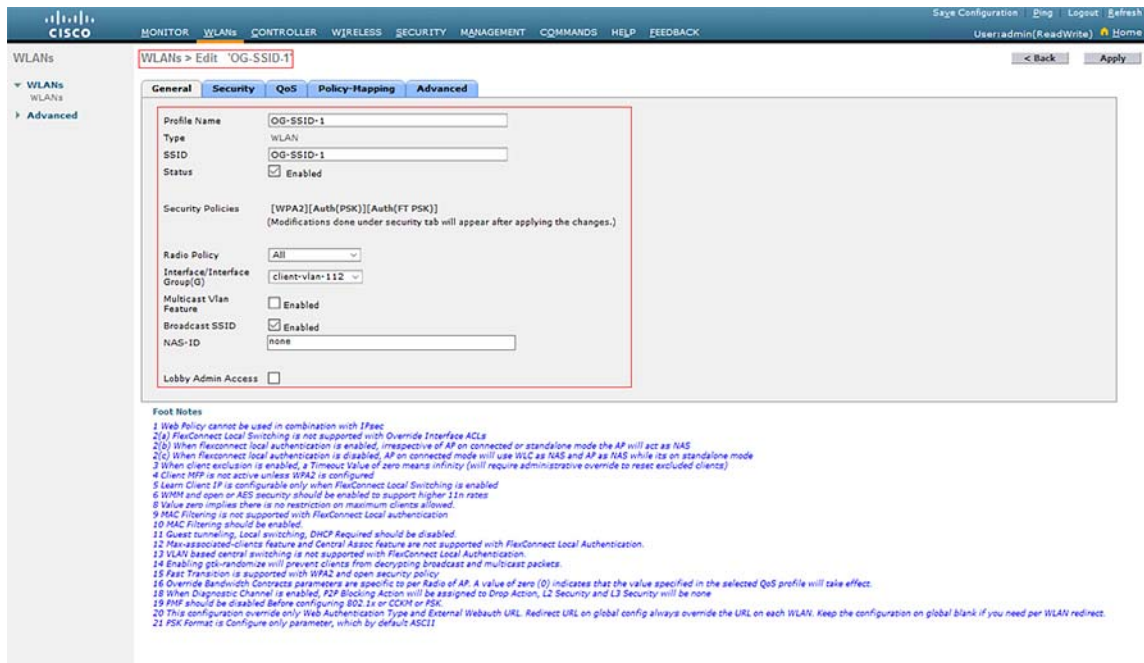
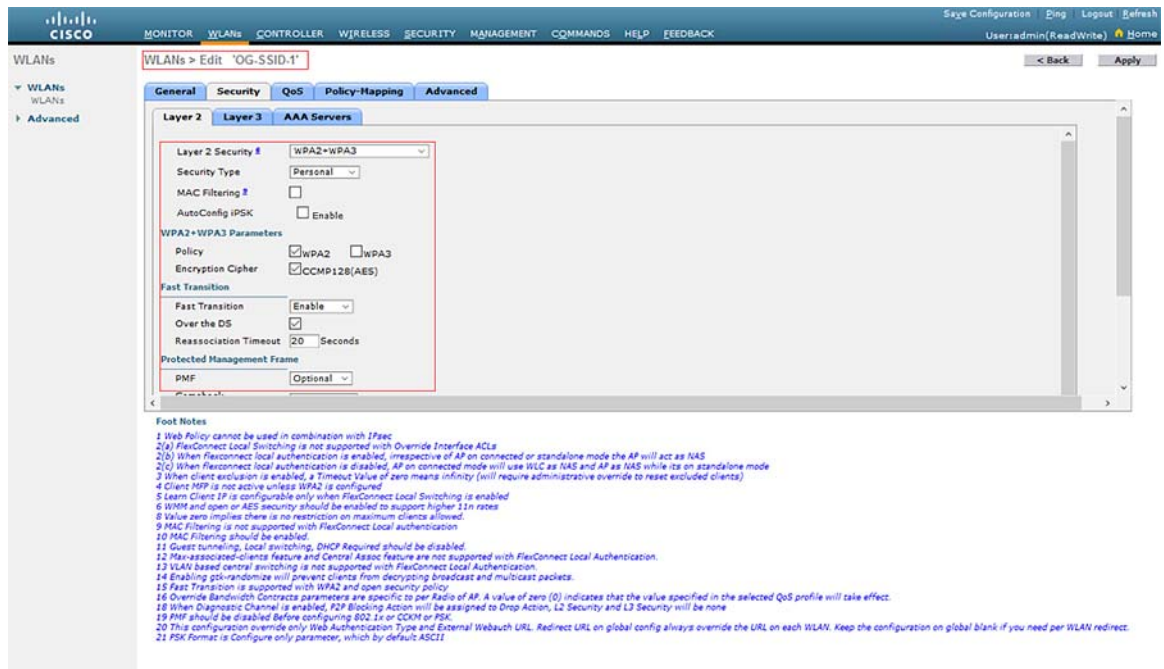


Figure 87 5520 WLAN Security Configuration



Mobility Group

A mobility group is a set of controllers, identified by the same mobility group name that defines the realm of seamless roaming for wireless clients. By creating a mobility group, you can enable multiple WLCs in a network to dynamically share essential client, AP, and RF information as well as forward data traffic when inter-controller or inter-subnet roaming occurs.

Inter-Release Controller Mobility (IRCM) supports seamless mobility and services across different wireless LAN controllers that runs on different software and controllers.

AireOS wireless controller uses EoIP tunnels for mobility. Support for CAPWAP-based encrypted mobility (Secure Mobility) on AireOS wireless controller was introduced on AireOS special IRCM image based on the 8.5 Maintenance Release software.

Figure 88 WLC3504 Mobility Group Configuration

The screenshot shows the Cisco WLC3504 configuration interface. The 'Static Mobility Group Members' page is active, displaying a table of mobility group members. The table has columns for MAC Address, IP Address (IPv4/IPv6), Group Name, Multicast IP, Status, Hash Key, Secure Mobility, and Data Encryption. Three entries are listed, with the first two highlighted in red.

MAC Address	IP Address (IPv4/IPv6)	Group Name	Multicast IP	Status	Hash Key	Secure Mobility	Data Encryption
00:07:64:8a:3f:80	10.5.1.53	default	0.0.0.0	Up	none	NA	NA
6c:ah:05:88:44:09	10.5.1.55	default	0.0.0.0	Up	none	Disabled	NA
d4:e8:80:b2:d7:4b	10.5.1.51	default	0.0.0.0	Control and Data Path Down	none	Enabled	Disabled

Figure 89 WLC5520 Mobility Group Configuration

The screenshot shows the Cisco WLC5520 configuration interface. The 'Static Mobility Group Members' page is active, displaying a table of mobility group members. The table has columns for MAC Address, IP Address (IPv4/IPv6), Group Name, Multicast IP, Status, Hash Key, Secure Mobility, Data Encryption, and High Cipher. Three entries are listed, with the first two highlighted in red.

MAC Address	IP Address (IPv4/IPv6)	Group Name	Multicast IP	Status	Hash Key	Secure Mobility	Data Encryption	High Cipher
6c:ah:05:88:44:09	10.5.1.55	default	0.0.0.0	Up	none	NA	NA	NA
00:07:64:8a:3f:80	10.5.1.53	default	0.0.0.0	Up	none	Disabled	NA	NA
d4:e8:80:b2:d7:4b	10.5.1.51	default	0.0.0.0	Control and Data Path Down	none	Enabled	Enabled	Disabled

The Mobility Group Configurations can be verified with the following show commands:

3504

Detailed Configuration of the Deployment Models

```
(Cisco Controller) >show mobility summary

Mobility Protocol Port..... 16666
Default Mobility Domain..... default
Multicast Mode ..... Disabled
Mobility Domain ID for 802.11r..... 0xac34
Mobility Keepalive Interval..... 10
Mobility Keepalive Count..... 3
Mobility Group Members Configured..... 3
Mobility Control Message DSCP Value..... 0
```

```
Controllers configured in the Mobility Group
  MAC Address      IP Address      Status      Group Name
Multicast IP
  00:87:64:8a:3f:80  10.5.1.53      Up          default
  0.0.0.0
  6c:ab:05:88:44:09  10.5.1.55      Up          default
  0.0.0.0
```

5520

```
(Cisco Controller) >show mobility summary

Mobility Protocol Port..... 16666
Default Mobility Domain..... default
Multicast Mode ..... Disabled
DTLS Mode ..... Disabled
Mobility Domain ID for 802.11r..... 0xac34
Mobility Keepalive Interval..... 10
Mobility Keepalive Count..... 3
Mobility Group Members Configured..... 3
Mobility Control Message DSCP Value..... 0
```

```
Controllers configured in the Mobility Group
  MAC Address      IP Address      Status      Group Name
Multicast IP
  00:87:64:8a:3f:80  10.5.1.53      Up          default
  0.0.0.0
  6c:ab:05:88:44:09  10.5.1.55      Up          default
  0.0.0.0
```

Ethernet Bridging

Ethernet bridging allows multiple remote wired networks to connect to each other using the Ethernet port of the MAPs. A common use for Ethernet bridging is for video cameras on mesh APs. For ethernet bridging to work, every MAP and RAP in the path must have Ethernet bridging enabled along the path, where, every MAP in the mesh path back to the RAP and including the RAP must support bridging the same VLANs as the MAP with the wired connection.

Ethernet bridging should be enabled for the following scenarios:

- Integration of Emerson Sensors
- Video Surveillance

For detail description on Integration of Video Surveillance, refer to the use cases in this document.

3504

Figure 90 1552 MAP Ethernet Bridging Configuration

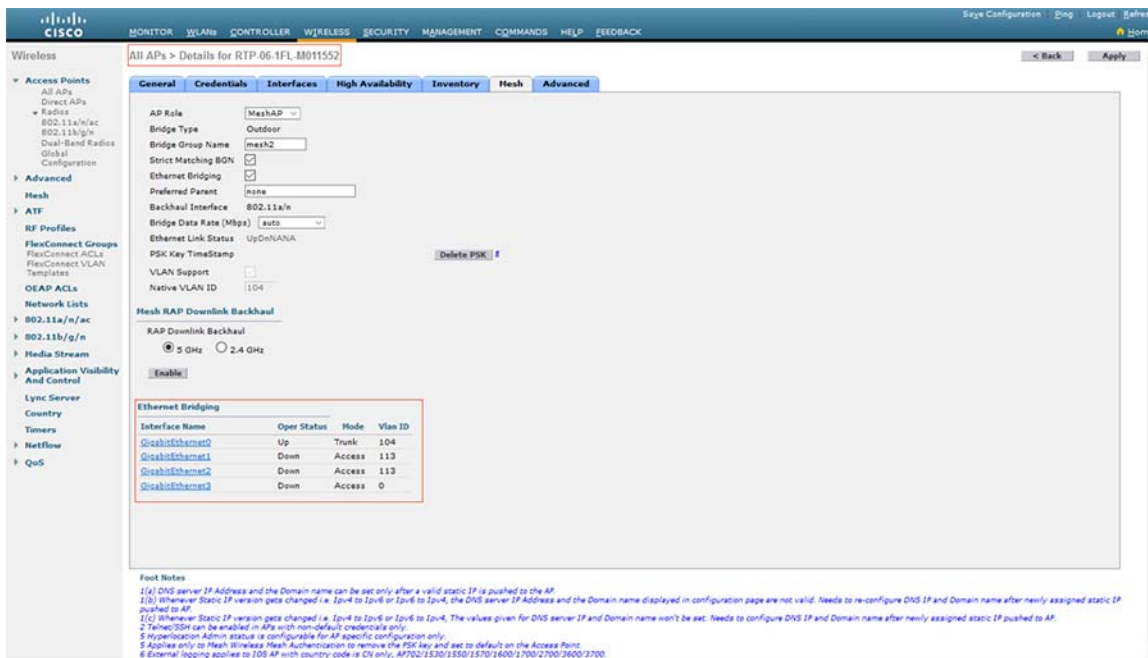


Figure 91 1552 RAP Ethernet Bridging Configuration

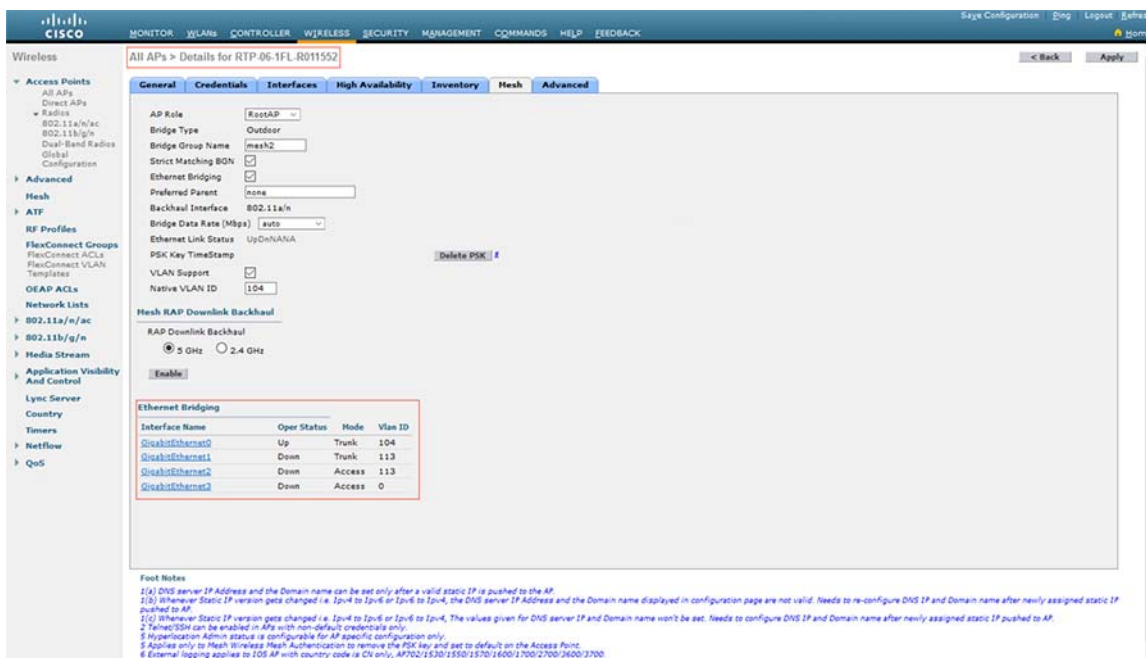
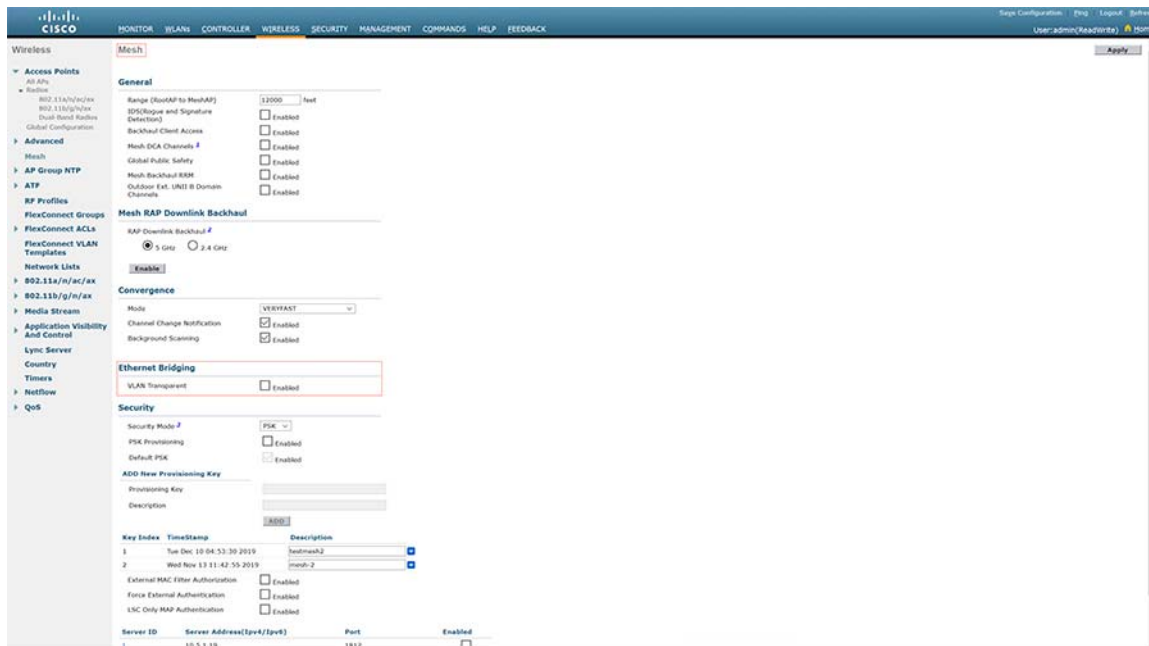


Figure 92 3504 Wireless MESH Disable VLAN Transparency



5520

Figure 93 6300 MAP Ethernet bridging Configuration on 5520

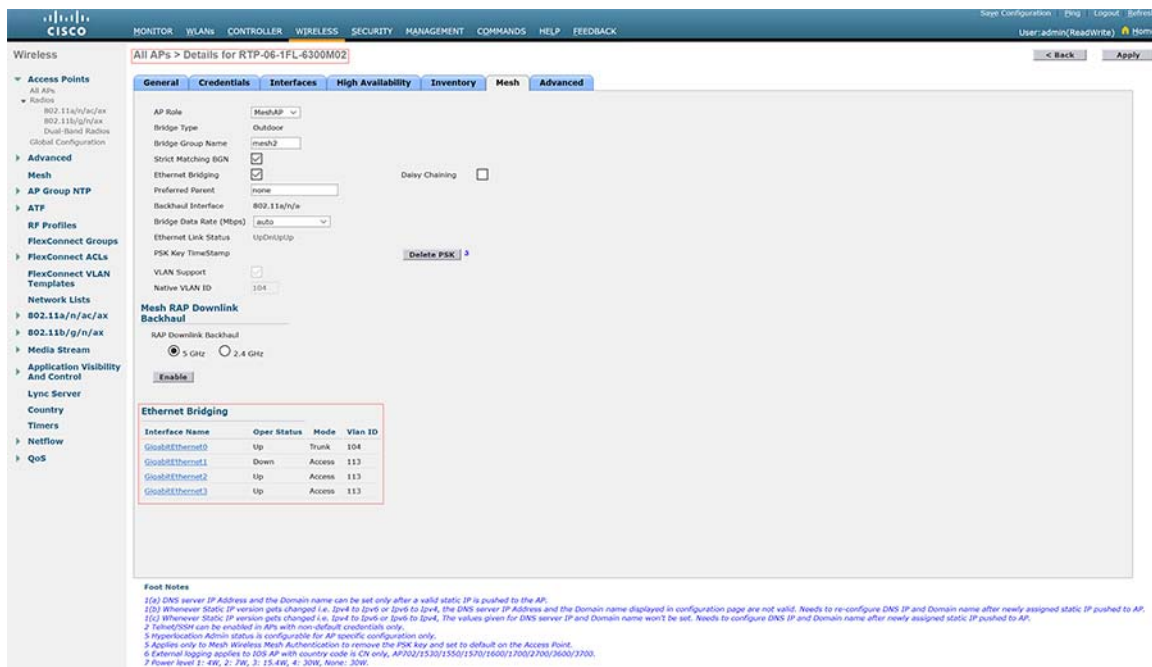


Figure 94 6300 RAP Ethernet Bridging Configuration on 5520

The screenshot shows the Cisco Wireless LAN Controller configuration interface for AP RTP-06-1FL-6300R01. The 'Mesh' tab is selected, and the 'Ethernet Bridging' section is expanded. The configuration includes:

- AP Role: RootAP
- Bridge Type: Outdoor
- Bridge Group Name: mesh1
- Strict Matching BGN:
- Ethernet Bridging: (Daisy Chaining:)
- Preferred Parent: none
- Backhaul Interface: 802.11a/n/y
- Bridge Data Rate (BDR): auto
- Ethernet Link Status: Up/On/On
- PSK Key TimeStamp: Delete PSK
- VLAN Support:
- Native VLAN ID: 104
- Mesh RAP Downlink Backhaul: 5 GHz (selected), 2.4 GHz
- Enable button for Mesh RAP Downlink Backhaul.

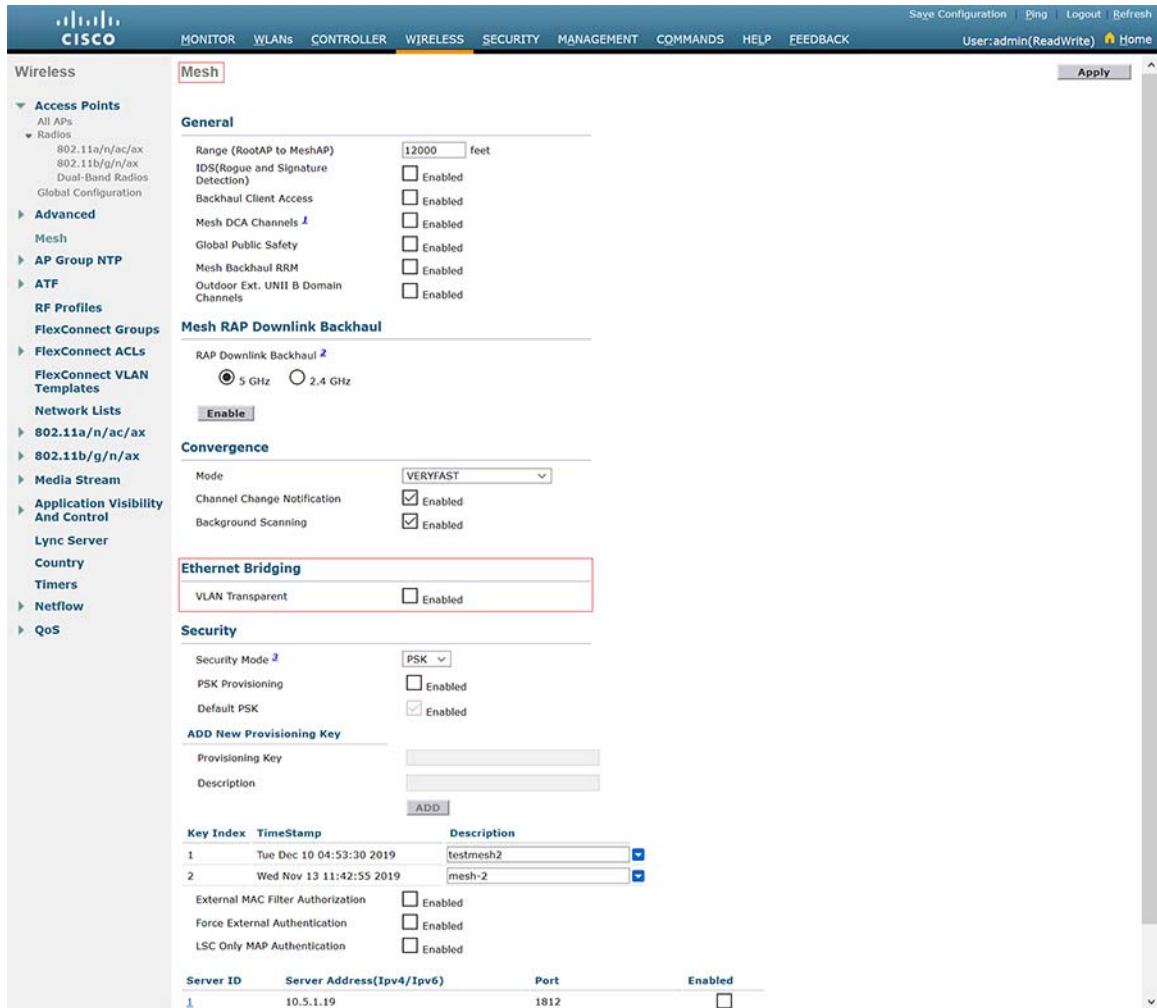
The 'Ethernet Bridging' table is highlighted with a red box:

Interface Name	Oper Status	Mode	Vlan ID
GigabitEthernet0	Up	Trunk	104
GigabitEthernet1	Down	Access	113
GigabitEthernet2	Down	Access	113
GigabitEthernet3	Down	Access	0

Foot Notes:

- [1] DNS server IP Address and the Domain name can be set only after a valid static IP is pushed to the AP.
- [2] Whenever Static IP version gets changed i.e. ipv4 to ipv6 or ipv6 to ipv4, the DNS server IP Address and the Domain name displayed in configuration page are not valid. Needs to re-configure DNS IP and Domain name after newly assigned static IP pushed to AP.
- [3] Whenever Static IP version gets changed i.e. ipv4 to ipv6 or ipv6 to ipv4, the values given for DNS server IP and Domain name won't be set. Needs to configure DNS IP and Domain name after newly assigned static IP pushed to AP.
- [4] Tunnel/VPN can be enabled in APs with non-default credentials only.
- [5] Replication Admin status is configurable for AP-specific configurations only.
- [6] Applies only to Mesh Wireless Mesh Authentication to remove the PSK key and set to default on the Access Point.
- [7] External logging applies to 5520 AP with country code is CN only. AP350/1530/1550/1570/1600/1700/2700/2600/3700.
- [8] Power level 1: 4W, 2: 7W, 3: 15.4W, 4: 30W, Name: 30W.

Figure 95 5520 Wireless MESH Disable VLAN Transparency



BGN

Brownfield mixed mesh deployment requires several technologies to be enabled to register and manage 1552 LAP clusters and IW6300 LAP clusters. This includes: Bridge Group Name (BGN) and DHCP option 43 and option 60 described previously.

BGN provides a logical grouping mechanism for preventing two mesh networks on the same channel to communicate with each other, where, 1552 RAPs and IW6300 RAPs hosts two clusters of MESH network and services. It is highly recommended to use BGN group to segment them to enable predictable mesh WLAN formation.

BGN grouping can be enabled with “Strict” BGN group matching which will have the following effects, customer can (optionally) enable this feature based on their specific requirement in the field:

- Scan 10 times to find the matched BGN parent.
- After 10 scans, if no parent with matched BGN is identified, then connect to the non-matched BGN.
- After 15 minutes, break the connection and scan again.

Detailed Configuration of the Deployment Models

Given the separate BGN groups segmenting between 1552 RAP extended cluster with IW6300 RAP extended cluster, each 1552 LAP family AP and IW6300 LAP family AP is actually registered and managed separately by different sets of WLC HA pairs because of features compatibility, between these WLC pairs, mobility group tunnel is implemented to sync up clients and MESH AP database, to facilitate clients across WLC Layer 3 roaming.

Two types of extended MESH clusters segmented by unique BGN are described below:

- 6300 as RAP scenario—Where 6300 MAPs and 1552 MAPs will be configured with, for example, BGN of “mesh1” in the following examples.
- 1552 as RAP scenario—Where 6300 MAPs and 1552 MAPs will be configured with, for example, BGN of “mesh2” in the following examples.

Note: In the BGN configuration, consider the following conditions:

- If BGN is mismatched, the AP will join a mesh network of another BGN, but after 15 minutes, the AP will drop AWPP and scan for its own BGN link. BGN mismatch will incur instability; adds a higher AWPP priority on BGN group does not strand AP with misconfigured BGN.
- If you want to change the BGN of the APs after the RAP is deployed at its remote site, configure the BGN parameter first on the MAP and then on the RAP. If the RAP is configured first, it causes serious connectivity issues since the MAP goes to default mode because its parent (RAP) is configured with a different bridge group name.
- For configurations with multiple RAPs, make sure that all RAPs have the same BGN to allow failover from one RAP to another. Conversely, for configurations where separate sectors are required, make sure that each RAP and associated MAPs have separate BGNs.

Note: A general Mesh Deployment recommendation includes:

- Placing Access Points where the desired parent will have the highest link SNR.
- Setting Bridge Group Names (BGN).
- Configuring a Preferred Parent.
- Configuring at least two RAPs with same BGN but on different channel to provide redundancy.

Figure 96 6300 RAP Bridge Group Name Configuration

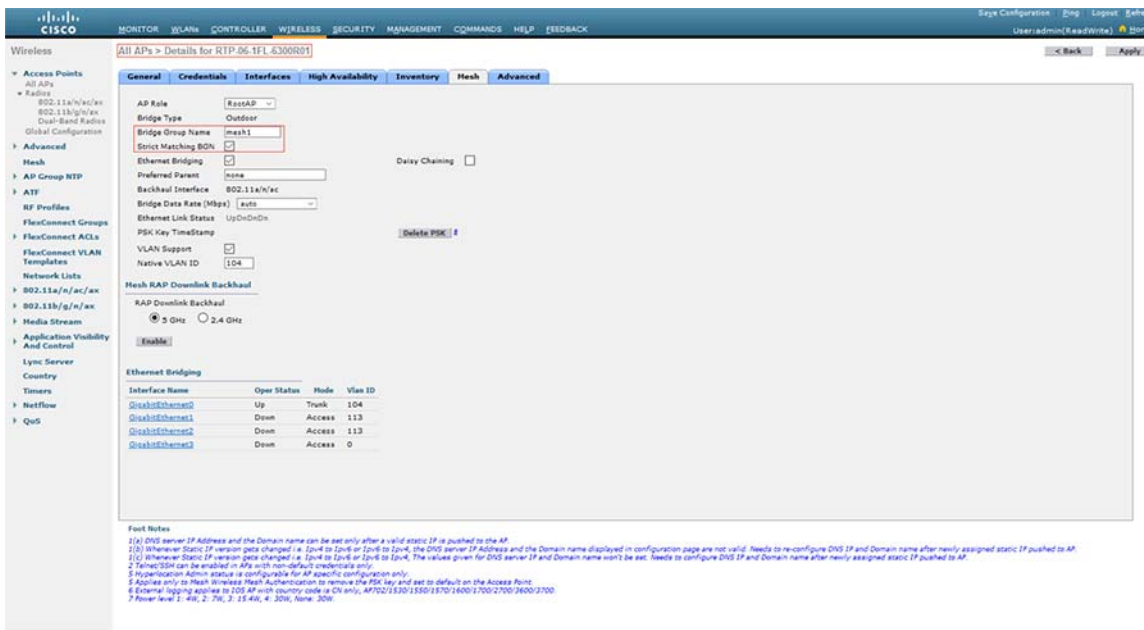


Figure 97 6300 MAP Bridge Group Name Configuration

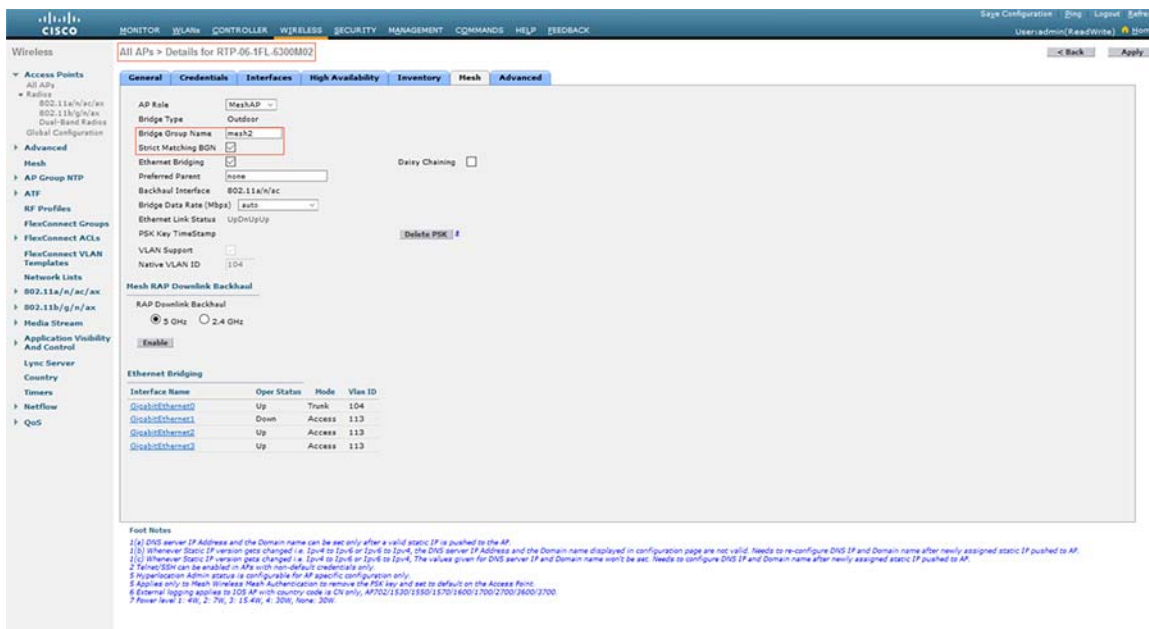


Figure 98 1552 RAP Bridge Group Name Configuration

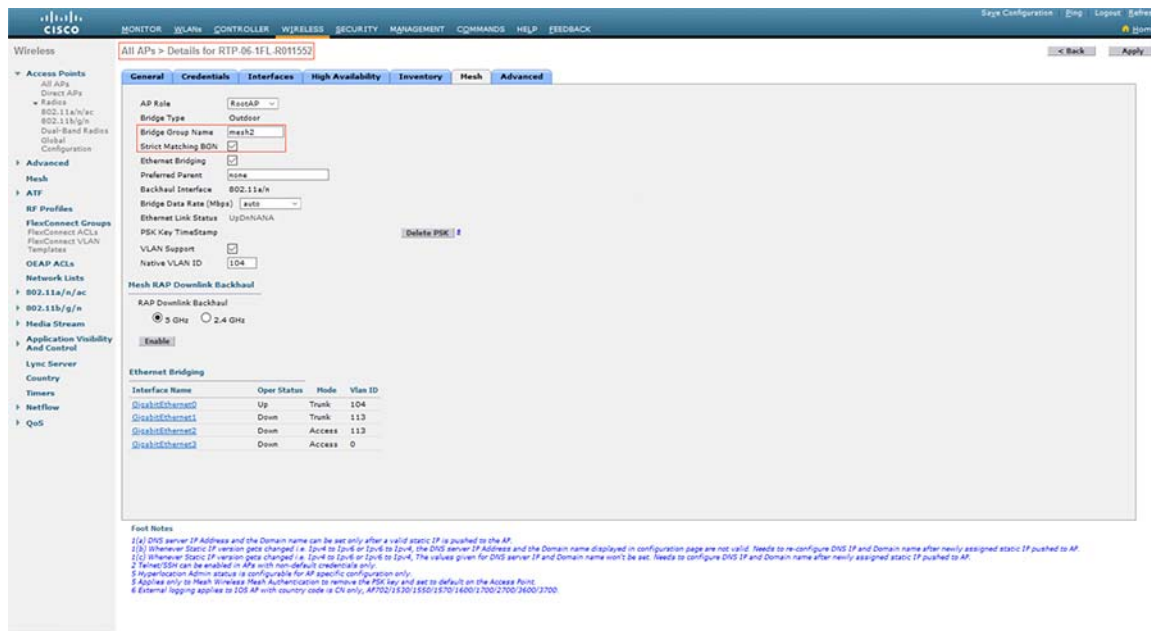
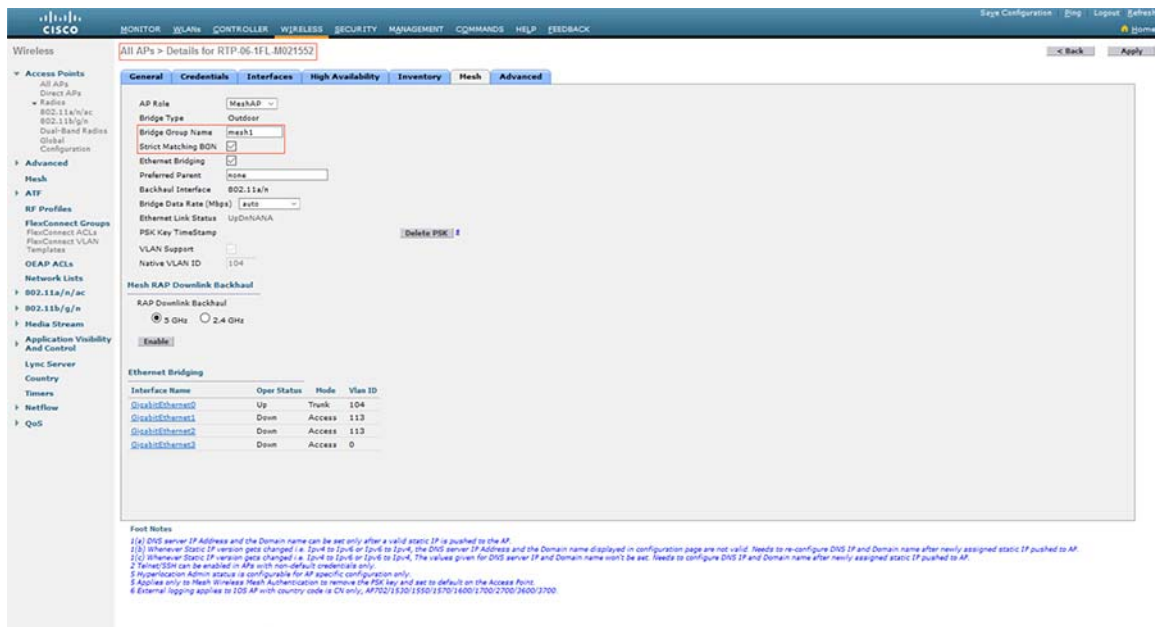


Figure 99 1552 MAP Bridge Group Name Configuration



AireOS (8.5) to Catalyst 9800 (17.1.1s) Deployment

Configuring HA SSO

For 3504 HA SSO Configuration please refer to above Configuring HA SSO on 3504 or 5520.

For catalyst 9800 HA SSO Configuration please refer to Configuring HA SSO in Greenfield Deployment.

Mesh Configurations

For 3504 Mesh Configurations please refer to the above section and for Catalyst 9800 please refer to the Configuring Mesh Profile in Greenfield Section.

MESH Backhaul Security (MAC Filter)

For 8.5 IRCM code refer to above section and for Cat 9800 refer to greenfield section.

Note: Both controllers AireOS and Catalyst 9800 need to have same mac address list under Mac filter tab for 1552 and IW6300 to co-exist in the network.

WLAN Configurations

For 3504 WLAN Configurations please refer to the above section and for Catalyst 9800 please refer to the WLAN Configuration in Greenfield Section.

For Catalyst 9800 configure the AP Join policy, Policy profile, Site Tag and RF Tag. Refer to Greenfield Deployment for the detailed steps to configure Catalyst 9800.

Mobility Group

Cisco IOS-XE wireless controller uses CAPWAP based tunnels for mobility. The mobility control channel will be encrypted, and the mobility data channel can be optionally encrypted. This is termed as Secure Mobility.

For more information about IRCM between Cisco IOS XE releases for Cisco Catalyst 9800 Series Wireless Controllers and Cisco Wireless Release for AireOS Controllers, see the [Cisco Catalyst 9800 Wireless Controller-AireOS IRCM Deployment Guide](#).

Note: AireOS of WLC3504 mobility configuration must enable the “secure mobility” option to establish secure mobility tunnel with the Cat9800 IOS-XE wireless controller.

Figure 100 Catalyst 9800 Mobility Group Configuration

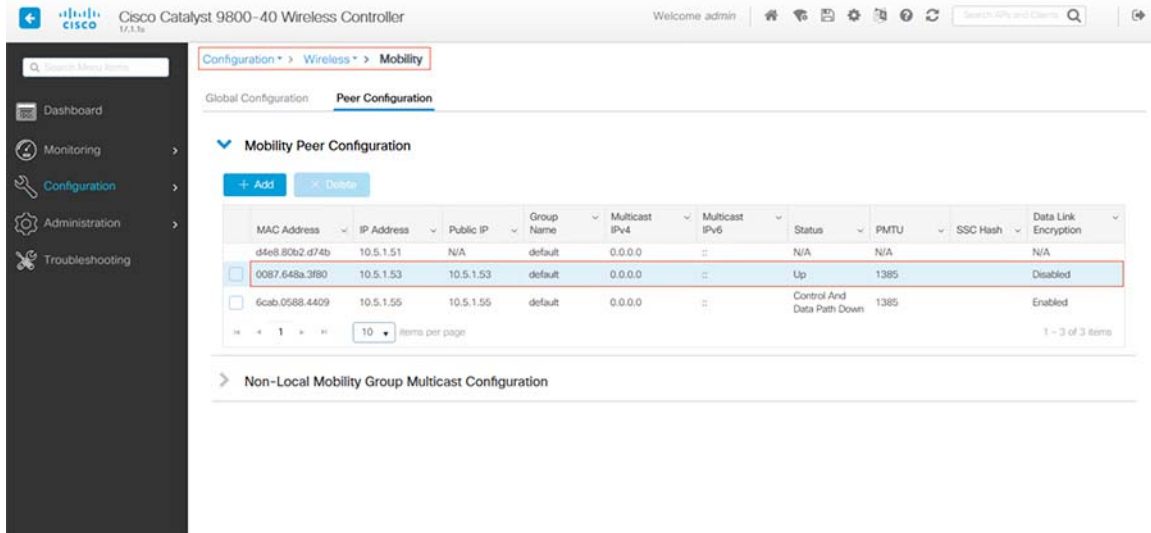
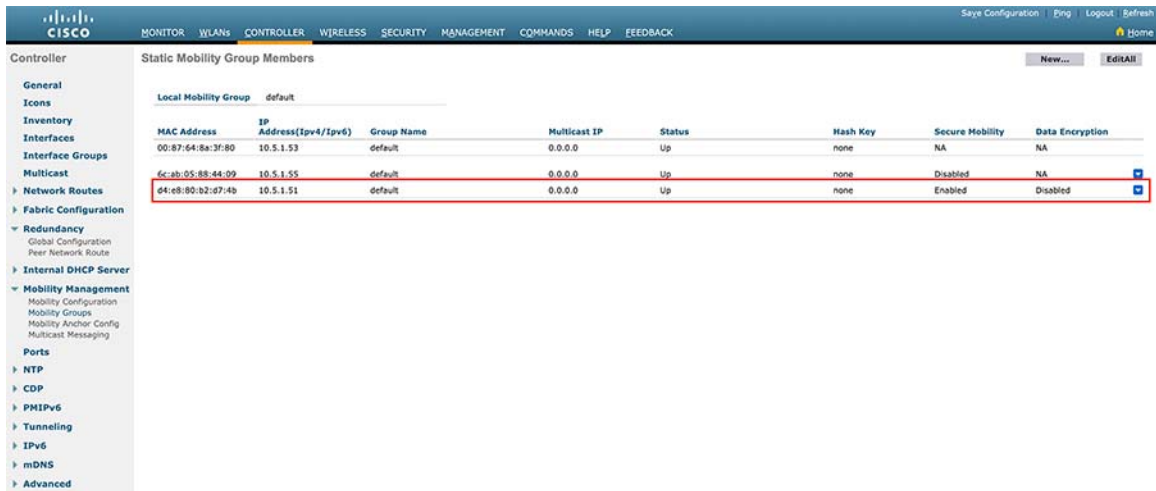


Figure 101 3504 WLC Mobility Group Configuration



Show Commands:

(Cisco Controller) >show mobility summary

```

Mobility Protocol Port..... 16666
Default Mobility Domain..... default
Multicast Mode ..... Disabled
Mobility Domain ID for 802.11r..... 0xac34
Mobility Keepalive Interval..... 10
Mobility Keepalive Count..... 3
Mobility Group Members Configured..... 3
Mobility Control Message DSCP Value..... 0
    
```

```

Controllers configured in the Mobility Group
MAC Address      IP Address      Status      Group Name
Multicast IP
00:87:64:8a:3f:80 10.5.1.53      Up          default
0.0.0.0
    
```

Detailed Configuration of the Deployment Models

```
d4:e8:80:b2:d7:4b 10.5.1.51          default
0.0.0.0                               Up
```

17.1.1s:

```
WLC#show wireless mobility summary
Mobility Summary
```

```
Wireless Management VLAN: 100
Wireless Management IP Address: 10.5.1.51
Wireless Management IPv6 Address:
Mobility Control Message DSCP Value: 48
Mobility Keepalive Interval/Count: 10/3
Mobility Group Name: default
Mobility Multicast Ipv4 address: 0.0.0.0
Mobility Multicast Ipv6 address: ::
Mobility MAC Address: d4e8.80b2.d74b
Mobility Domain Identifier: 0x34ac
```

Controllers configured in the Mobility Domain:

IP Group Name	Multicast IPv4	Public Ip Multicast IPv6	MAC Address Status
PMTU			

10.5.1.51		N/A	d4e8.80b2.d74b
default	0.0.0.0	::	N/A
N/A			
10.5.1.53		10.5.1.53	0087.648a.3f80
default	0.0.0.0	::	Up
1385			

Ethernet Bridging

Ethernet bridging configuration of WLC3504 and Cat9800 share the same configuration and can be referred to above brownfield and greenfield deployment sections for details.

Figure 102 6300 MAP Ethernet Bridging Configuration

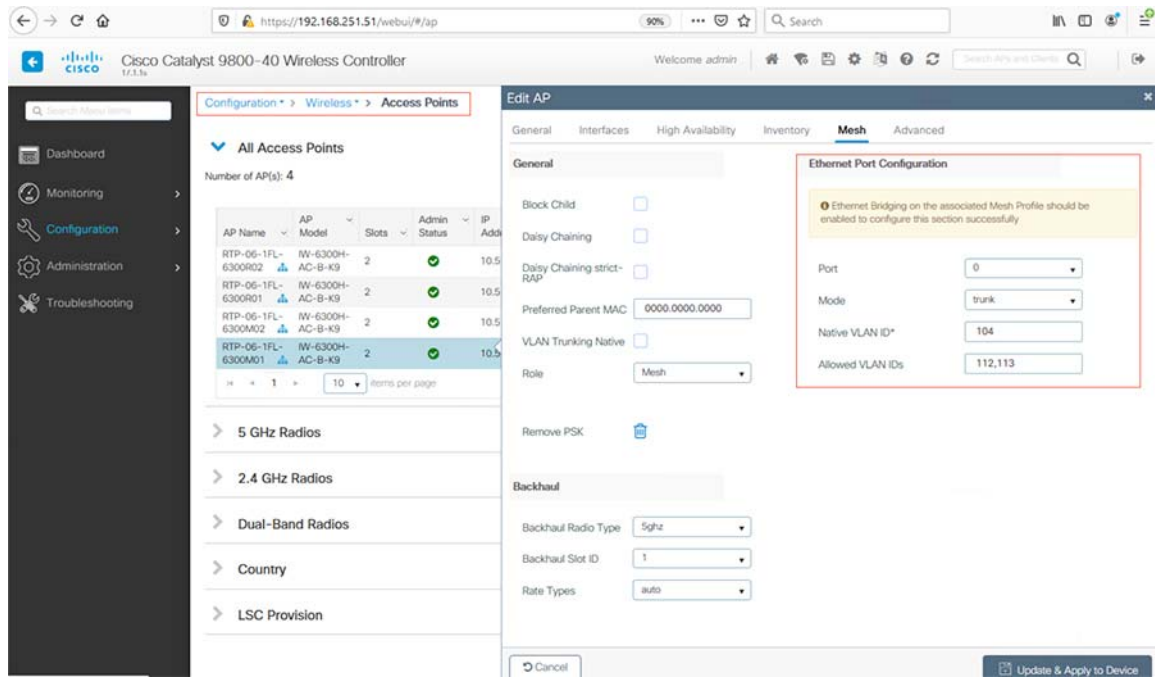
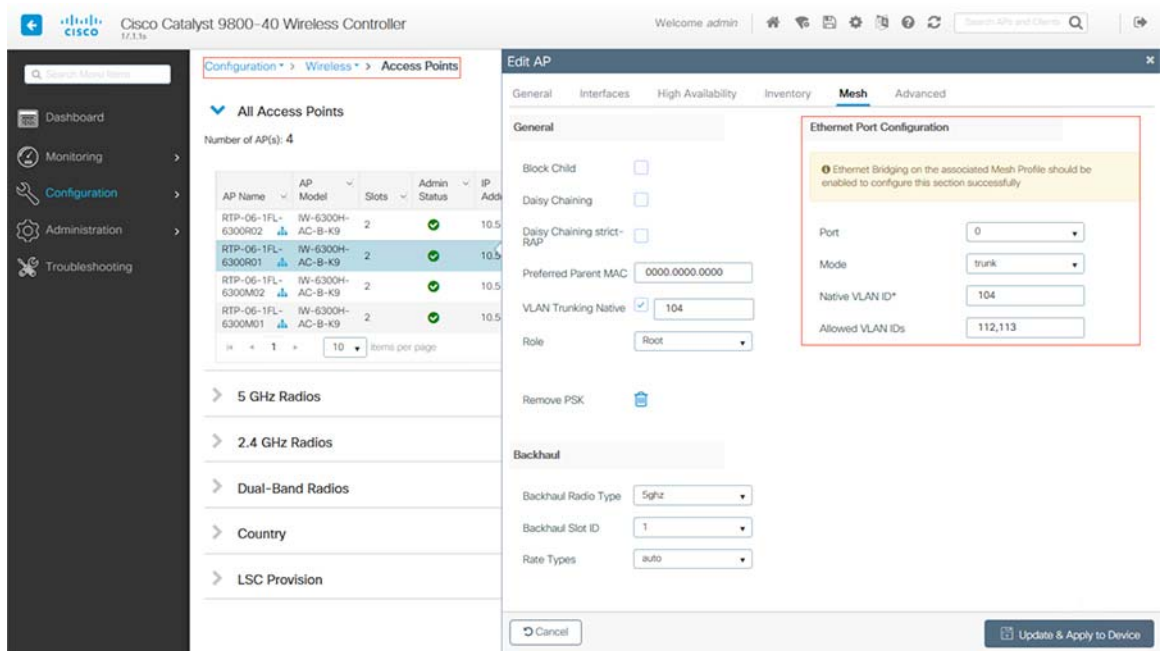


Figure 103 6300 RAP Ethernet Bridging Configuration



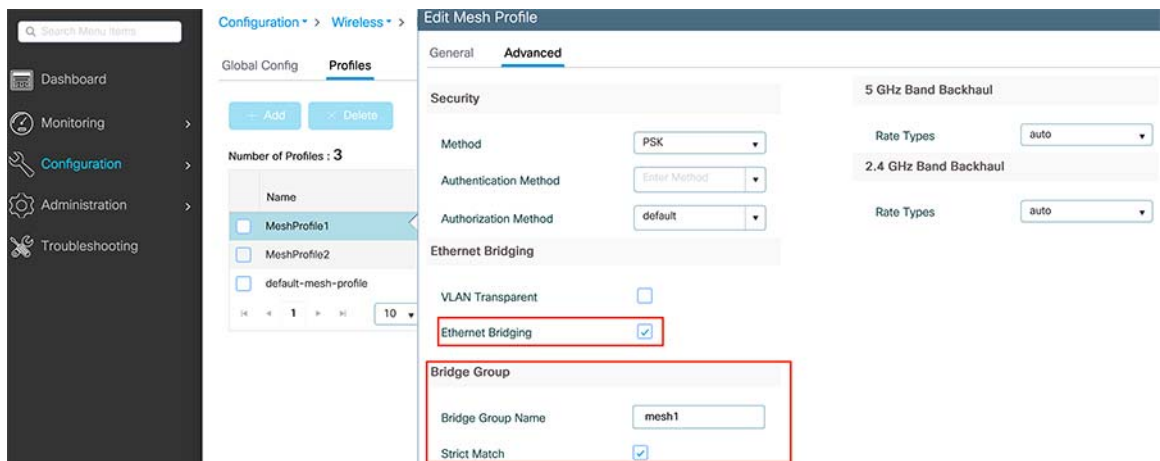
Use Cases

BGN

Refer to above section to configure BGN on MAPs and RAPs connected to 3504 WLC. In Cisco Catalyst 9800 Series Wireless Controller, the BGN is configured on the mesh profile. Whenever a MAP joins the controller, the controller pushes the BGN that is configured on the mesh profile to the AP.

Specify the Bridge Group Name under Advanced tab of the specific Mesh profile. To create a mesh profile on catalyst 9800, refer to Configuring Mesh Profile in Greenfield Deployment.

Figure 104 BGN Configuration for Mesh profile on Catalyst 9800



Use Cases

Remote Access

Remote access enabling O&G refinery personnel to access onsite resources over public broadband network, this is achieved by utilizing Cisco ASA security appliance (and industrial de-militarized zone security appliance depending on each customer’s own network design and requirements) to allow this remote access traffic to pass through ASA security appliance, remote access control is typically to use a remote desktop as shown in the above figure as below:

- Remote user access via enterprise ASA establish session to Industrial Demilitarized Zone (IDMZ)
- Remote user access IDMZRDG server with industrial zone IACS SGT default policy
- Remote user use IDMZ RDG Server to access industrial RDG server via IDMZ ASA
- Remote user use IDMZ RDG server to access industrial RDG server
- Remote user uses Industrial RDG server to access industrial floor IACS devices

Emerson WiHart for condition-based monitoring

Emerson is partnering with Cisco to introduce a next-generation industrial wireless networking solution that fundamentally transforms data management to improve plant productivity, reliability and safety.

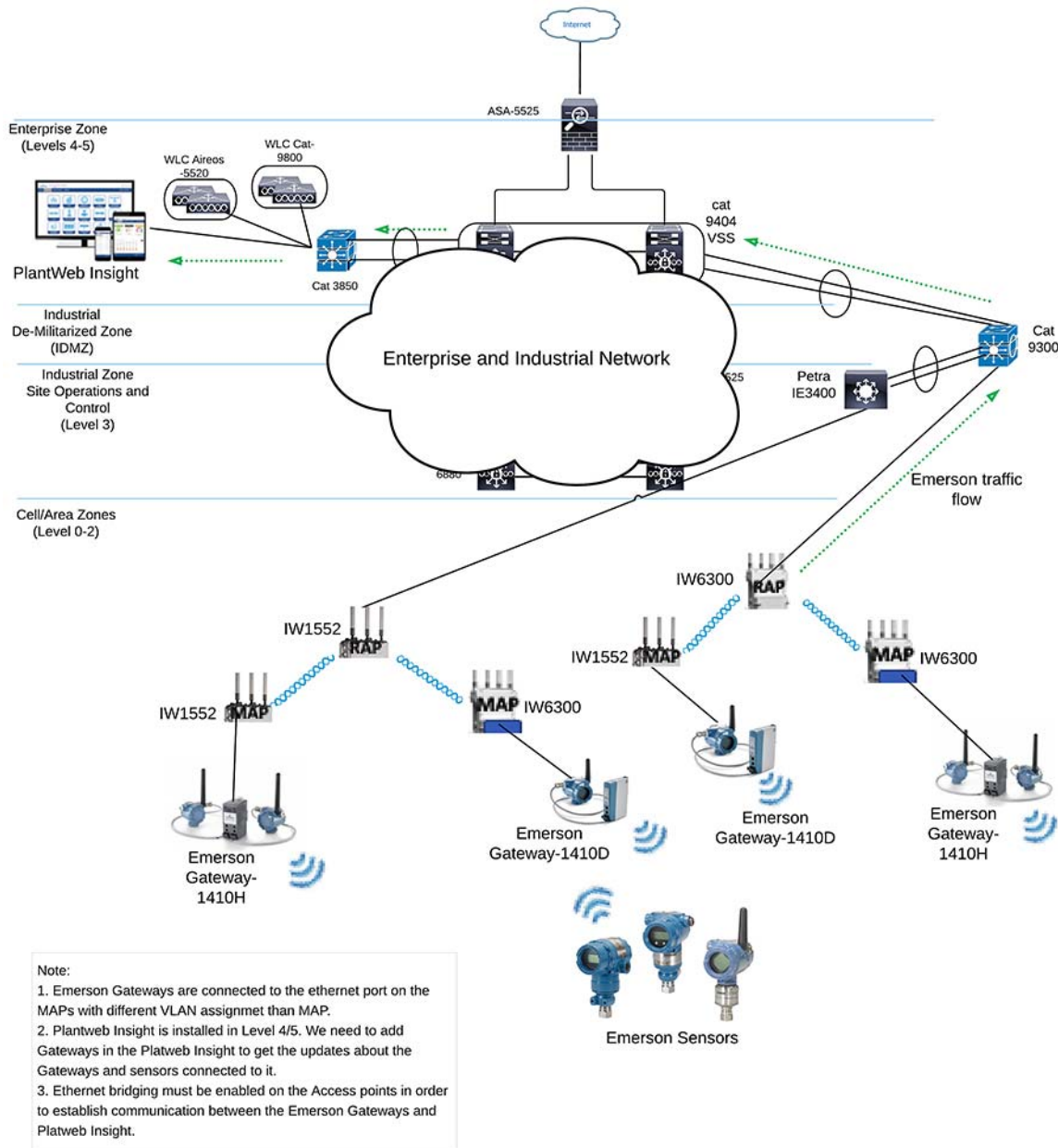
Use Cases

Emerson Gateways are connected to the MAPs in the topology. Emerson sensors communicate with the Gateways using WirelessHART protocol. Please refer to the Design Guide for more details on Emerson/WiHART.

Among different kinds of Emerson gateways, this guide uses 1410D, 1410H, and 1410S. Emerson WiHart sensors send data to gateways and in turn gateways send all the data to Emerson’s data analytic platform called Emerson PlantWeb Insight. For detailed instructions on integrating Emerson 1410S Gateway with IW6300 Access Point refer to [Appendix A: Integrating Emerson 1410S Gateway with IW6300, page 94](#).

[Emerson PlantWeb Insight](#) is the data analytics platform that provides better visibility into the health of your facility key assets. In our deployment, PlantWeb Insight is installed in Enterprise level 4/5 which is a visualization platform where the data from the Emerson sensors connected to Emerson Gateways and health of the Emerson Gateways can be seen.

Figure 105 Emerson Sensors Integration



Video Surveillance

Physical security solutions provide broad capabilities for video surveillance, IP cameras, electronic physical access control, incident response and notifications, and personnel safety. For the video surveillance use-case, IP cameras can be attached to the PoE out port of the Mesh APs. With this option bridged traffic from the Map is forwarded upstream to the RAP where it is then switched locally.

For improved throughput and high-resolution camera feeds one can also disable the 2.4GHz client access radio on that particular MAP so that only video traffic is carried over the back-haul link and it does not have to contend with any other Wi-Fi Client Traffic. In this design, the video stream will be ethernet bridged and dropped off at the RAP ethernet link. Any QoS markings from the video camera equipment will be preserved. It is recommended to segment the video stream traffic onto a separate VLAN from the Wi-Fi client traffic. For Brownfield & Greenfield deployment please reference the previous Ethernet bridging configuration sections of this document.

Location Services and Asset Tracking

This solution uses the Cisco Connected Mobile Experiences (CMX) product to provide location services. CMX uses existing wireless infrastructure to calculate the location of the Wi-Fi devices and interferers such as BLE Beacons, microwave ovens, RFID tag, and etc. CMX uses RSSI triangulation from three nearby APs to locate connected and unconnected Wi-Fi devices, interferers, and active RFID tags. Location can range from 5 to 7 meters for RFID tags 90% of the time. Location for Wi-Fi clients is within 10 meters 90% of the time. The following figure depicts an Aero scout RFID tag located and detected within Prime infrastructure.

Note: Location was not thoroughly tested in this design, it is highly recommended to consult with Customer Experience (CX) and verified Vendor (such as Accenture) if location design and validation is needed in the network.

Figure 106 Asset tracking on Prime Infrastructure

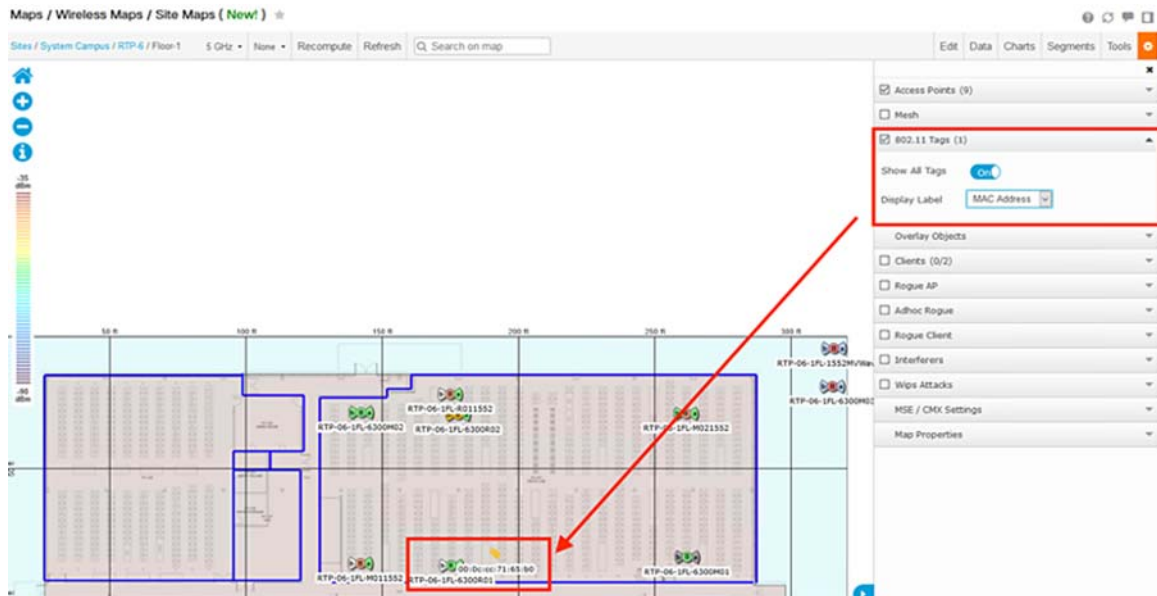
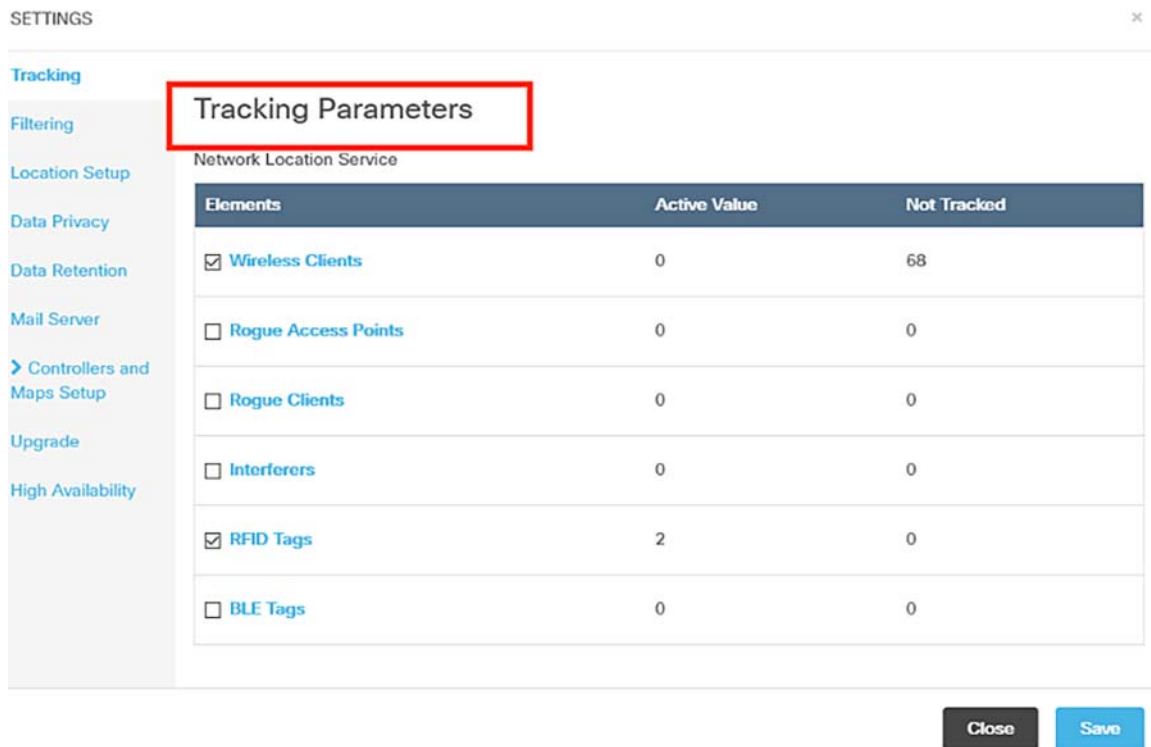


Figure 107 is a snapshot of tracking parameters within CMX; these settings can be tuned to your network requirements.

Figure 107 Tracking Parameters



SETTINGS

Tracking

Filtering

Location Setup

Data Privacy

Data Retention

Mail Server

Controllers and Maps Setup

Upgrade

High Availability

Tracking Parameters

Network Location Service

Elements	Active Value	Not Tracked
<input checked="" type="checkbox"/> Wireless Clients	0	68
<input type="checkbox"/> Rogue Access Points	0	0
<input type="checkbox"/> Rogue Clients	0	0
<input type="checkbox"/> Interferers	0	0
<input checked="" type="checkbox"/> RFID Tags	2	0
<input type="checkbox"/> BLE Tags	0	0

Close Save

Troubleshooting

Debug Command:

- For general AP join issues (1552 RAP & 1552 MAP):

```
deb mesh error
deb mesh convergence
deb mesh link

show mesh config
show mesh backhaul
show mesh status
show capwap client rcb
```

- For general AP join issues (6300 RAP & 6300 MAP):

```
deb capwap client events
deb mesh convergence
deb mesh link

show mesh config
show mesh backhaul
show mesh status
show capwap client rcb
```

- For AP join security related issues (1552 RAP & 1552 MAP):

- WLC:

Troubleshooting

```
Debug client
Debug dot1x all enable
Debug aaa all enable
```

– MAP:

```
Deb mesh convergence
Debug mesh security error
Debug mesh security event
Debug dot1x
```

■ For AP join security related issues (6300 RAP & 6300 MAP):

– WLC:

```
Debug dot1x all
Debug aaa authentication
Debug aaa authorization
Debug aaa accounting

Show ap status
Show wireless mesh ap summary
Show ap dot11 5ghz summary
Show wireless mesh ap tree
Show ap name <?AP name?> mesh neighbor
Show mesh adjacency parent
Show mesh adjacency all
```

– MAP:

```
Debug mesh convergence
Debug mesh security
Debug dot1x
```

Appendix A: Integrating Emerson 1410S Gateway with IW6300

This Appendix chapter covers the integration of an Emerson 1410S Gateway with a Cisco IW6300 AP with respect to:

1. Powering-up the Cisco IW6300 AP to supply enough power for the IW6300 along with the POE-out ports.
2. Connecting the Emerson 781S Smart Antenna to the Emerson 1410S Gateway.
3. Powering-up the Emerson 1410S Gateway using POE from the Cisco IW6300.

The Emerson 1410S Gateways is mounted on to the IW6300. The 1410S gateway can be powered on by using Power Over Ethernet from IW6300. There are two Ethernet LAN ports capable of supplying PoE power in IW6300. There are certain restrictions for the PoE Out to be enabled on these ports.

The IW6300 access point can be powered by one of these methods:

1. Power over Ethernet by power injector AIR-PWRINJ-60RGD1= and AIR-PWRINJ-60RGD2=
2. AC or DC power
 - IW-6300H-AC-x-K9: 85-264V~ maximum, marked 100-240V~, 50-60Hz, 1.3A
 - IW-6300H-DC-x-K9: 44 to 57Vdc, 1.2A
 - IW-6300H-DCW-x-K9: 10.8 to 36Vdc, 5.9A

Notes:

- Power injector AIR-PWRINJ-60RGDx= is not certified for installation within hazardous locations environments.
- The PoE output on IW6300 will be disabled when PoE (IEEE 802.3at, UPoE) or power injector is the power source for IW6300. But the PoE Out data link can still be active.
- The PoE output on IW6300 will be enabled when AC, DC or DCW is the input power source of IW6300.

By default, Power over ethernet is enabled on the IW6300 when the input power source is AC, DC, or DCW. The Power Over Ethernet would be disabled when PoE (IEEE 802.3at, UPoE) or power injector is the power source.

The following table shows the access point POE out port power allocation on IW6300. Power manager holds 35.3 Watts when power source is AC, DC, or DCW.

Table 2 PoE Out Options for IW6300

Power Input Type	POE OUT 1 (POE PSE)	POE OUT 2 (POE PSE)	POE OUT 1 (10/100/1000 Traffic)	POE OUT2 (10/100/1000 Traffic)
PoE+ 802.3at	No	No	Yes	Yes
UPoE/Power Injector	No	No	Yes	Yes
DC/DCW	PoE+ capable	PoE+ capable	Yes	Yes
AC	PoE+ capable	PoE+ capable	Yes	Yes

Notes:

DC/DCW Power Input:

- Maximum of 35.3W shared between the two PoE out ports.
- If one port supports PoE+ (30 W), then the other ports have no PoE.
- Two ports support PoE (15.4 W) at the same time.

AC Power Input:

- Maximum of 20W shared between the two PoE out ports
- Either of the ports support PoE (15.4W) but not at the same time

Table 3 PoE-Out Port Power Allocation

	PoE Port 1	PoE Port 2
PSE: 35.3W (including 4.5W USB)	Disconnected	Class 0/1/2/3/4
	Class 1	Class 0/1/2/3/4
	Class 2	Class 0/1/2/3
	Class 0/3	Class 0/1/2/3
	Class 4	Class 1
	Class 0/1/2/3/4	Disconnected

The power levels on the two PoE out interfaces on IW6300 are in range of None to 4. The following table shows the mapping between power level and power capacity.

Table 4 Power Level and Power Capacity Mapping

Power Level	Max PoE Class	Max Power from PSE	Usage
None	4	30W	Default
1	1	4W	Optional
2	2	7W	Optional
3	0/3	15.4W	Optional
4	4	30W	Optional

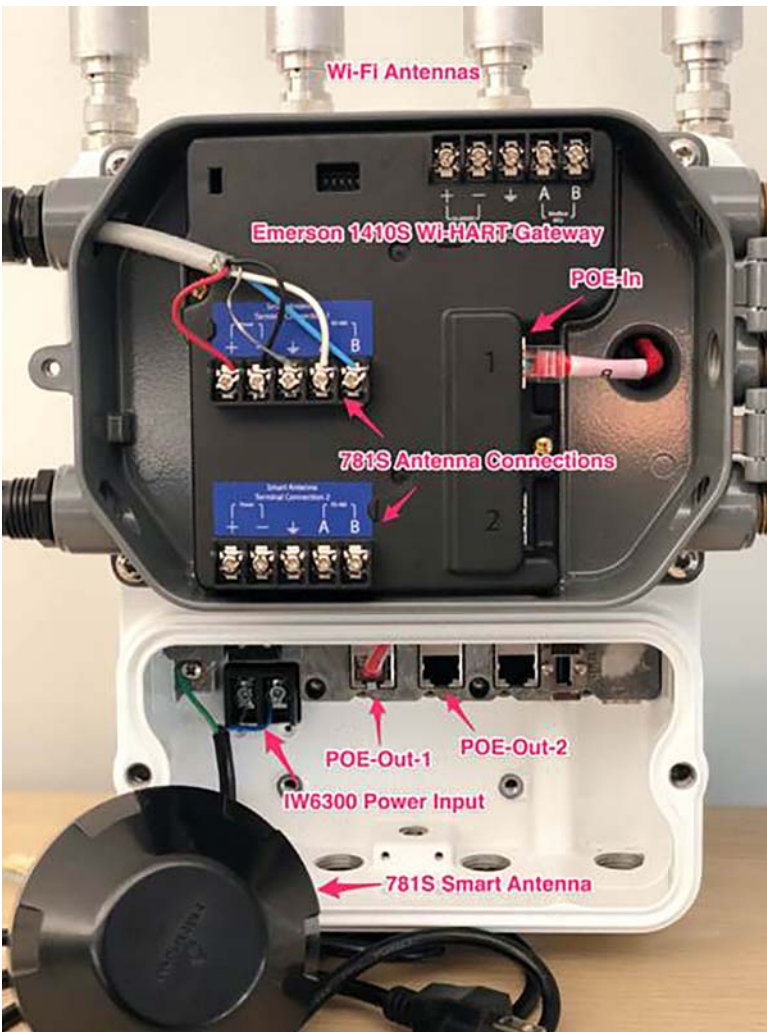
For more details on powering procedures of IW6300 refer to [Powering the IW6300 Access point](#).

Configuring Power Over Ethernet Out Functionality

The Power over Ethernet can be configured for all the Access points globally or else can be done per access point. The total available PoE power is 35.3W when the input power source is DC, DCW, or AC. In this document the 1410S is powered on from PoE Out Port 1 on IW6300. The power level of 2 (7W) is sufficient to power on the 1410S.

The following figure shows Emerson 1410S is mounted onto IW6300H. For more details on 1410S installation refer to [quick-start guide Emerson wireless 1410s gateway](#).

Figure 108 Emerson 1410S with 781S Smart Antenna embedded on IW6300

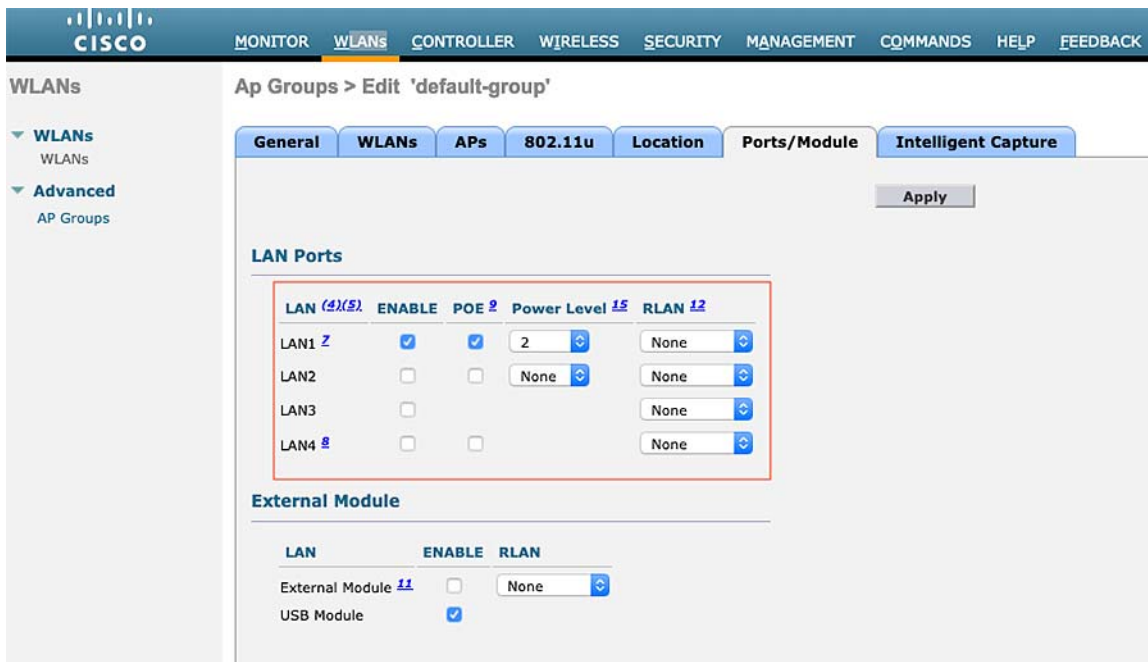


To configure PoE globally on specific set of access points the Controller GUI:

For AireOS Controller:

1. Navigate to WLANs > Advanced > AP Group, select the AP group
2. Under Ports/Module > Lan ports, enable the LAN interfaces, POE and power level.

Figure 109 LAN Port Configuration on AP Group on AireOS Controller



For Catalyst 9800 Wireless Controller:

- Remote LAN feature helps to configure the PoE functionality on the Access points that join the specific policy.

Configuring RLAN:

- To configure Remote LAN navigate to **Configuration > Wireless > Remote LAN**
- Select Add to create a new RLAN Profile.
- Enter the Profile Name, RLAN ID and toggle the status to enabled.
- Leave everything else to default values and hit Apply to device button to create the RLAN Profile.
- Go to RLAN Policy tab and create a RLAN Policy by clicking Add button.
- Enter the Policy Name and toggle the status to Enabled.
- Check in the PoE box to enable PoE on the Access points that join the profile, adjust the power level to meet the requirements and click Update & Apply to Device.
- RLAN-Policy have to be mapped to policy tag for Access points to be configured with the PoE out functionality.

Figure 110 Creating RLAN Profile

Add RLAN Profile
✕

General
Security

Profile Name*	<input type="text" value="poeout"/>
RLAN ID*	<input type="text" value="1"/>
Status	ENABLED <input checked="" type="checkbox"/>
Client Association Limit	<input type="text" value="0"/>
mDNS Mode	<input style="border: none; border-bottom: 1px solid #ccc; width: 100%;" type="text" value="Bridging"/>

↶ Cancel

📄
Apply to Device

Figure 111 Creating RLAN Policy

Add RLAN Policy
✕

General
Access Policies
Advanced

⚠️ Configuring in enabled state will result in loss of connectivity for clients associated with this policy.

Policy Name*	<input type="text" value="poeout"/>	RLAN Switching Policy	
Description	<input type="text" value="Enter Description"/>	Central Switching	ENABLED <input checked="" type="checkbox"/>
Status	ENABLED <input checked="" type="checkbox"/>	Central DHCP	<input type="checkbox"/> DISABLED
PoE	<input checked="" type="checkbox"/>		
Power Level	<input style="border: none; border-bottom: 1px solid #ccc; width: 100%;" type="text" value="2"/>		

↶ Cancel

📄
Apply to Device

Mapping RLAN Policy to Policy tag:

1. To map RLAN-policy to the policy tag go to **Configuration > Tags & Profiles > Policy** and select the policy tag that is created under the Tags Configuration section in Greenfield deployment Model under Detailed Configuration of Deployment Models.
2. Add the RLAN-policy by clicking the **Add** button.
3. Port ID specifies the Ethernet port of the access point on which PoE functionality needs to be configured.
4. From the drop down select the RLAN Profile, RLAN Policy profile that is created in Configuring RLAN and click **Update & Apply to Device**.

Figure 112 Mapping RLAN Policy to Policy Tag

Edit Policy Tag
✕

Name*

Description

▼ WLAN-POLICY Maps: 2

+ Add
✕ Delete

	WLAN Profile	Policy Profile
<input type="checkbox"/>	OG-SSID-1	og-profile_WLANID_1
<input type="checkbox"/>	test8021x	og-profile_WLANID_1

10 items per page
1 - 2 of 2 items

▼ RLAN-POLICY Maps: 0

+ Add
✕ Delete

Port ID	RLAN Profile	RLAN Policy Profile
No items to display		

Map RLAN and Policy

Port ID*

RLAN Profile* RLAN Policy Profile*

✕
✓

↶ Cancel

📄 Update & Apply to Device

Enabling LAN port on Access point:

1. The LAN port on the Access Point needs to be enabled.
2. To enable LAN port on the access point, go to **Configuration > Access Points**.
3. Select the specific access point and then under Interfaces > LAN port settings check in the status to enable the LAN port.
4. The LAN port of the Access point can also be enabled through Catalyst 9800 CLI.
5. WLC# ap name <ap name> lan port-id lan <port id> {disable | enable}

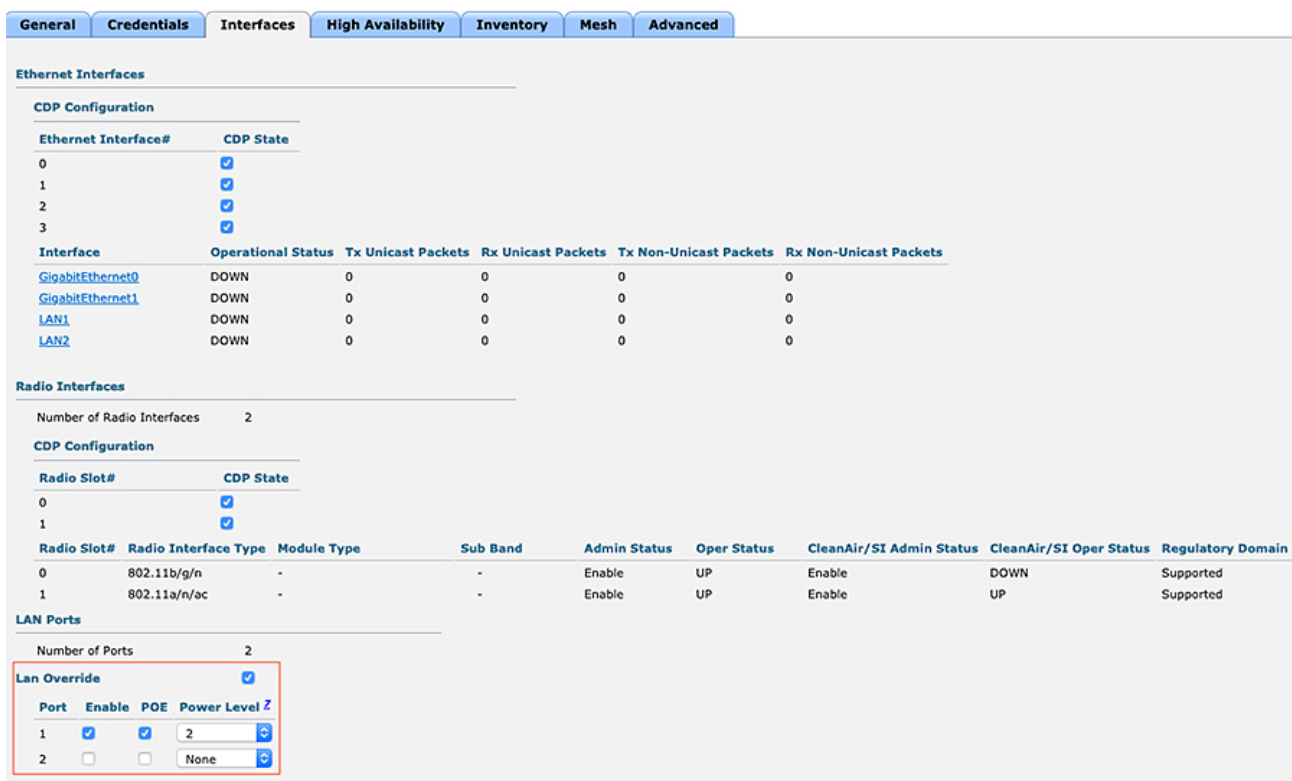
For more detailed steps on configuring Remote LAN and PoE Out refer to the [guide](#).

To configure PoE on a specific Access point:

For AireOS Controller:

1. Under Wireless, select the specific Access point.
2. Navigate to Interfaces tab, check the LAN Override box.
3. To enable the LAN ports, check the Enable box and for POE check the POE box.
4. The output power can be adjusted using the Power Level.

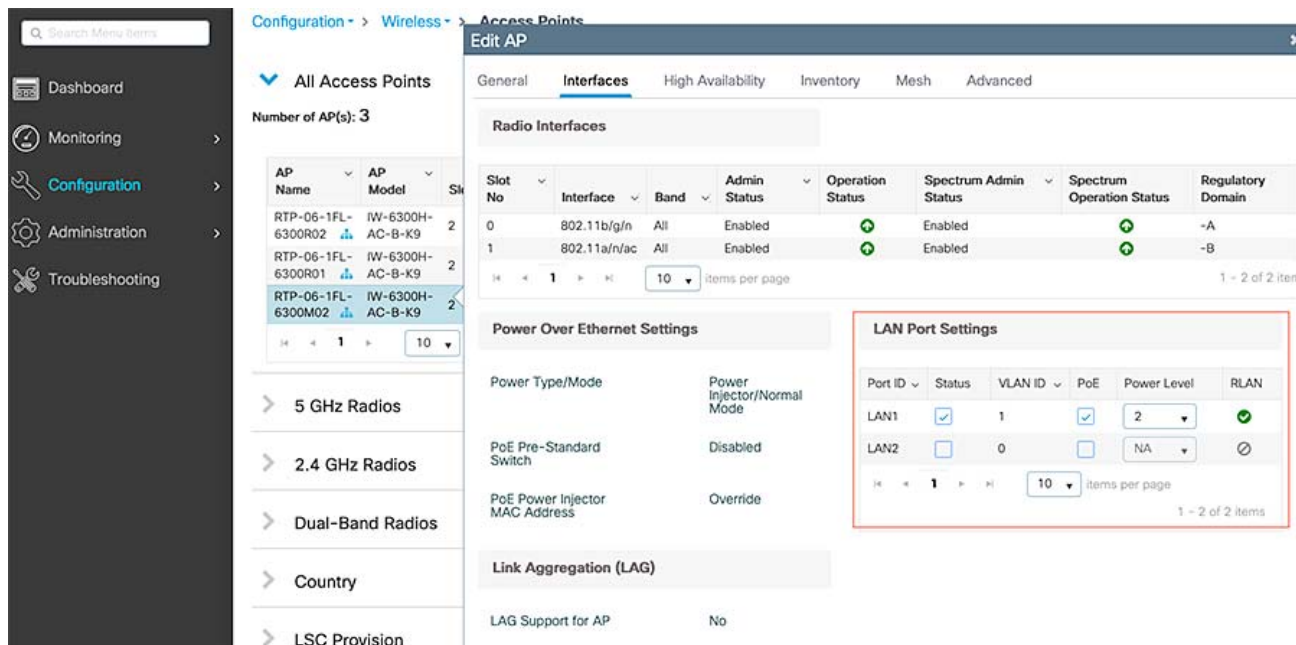
Figure 113 LAN Port Configuration on specific Access point on AireOS Controller



For Catalyst 9800 Controller:

1. Go to Configuration > Wireless > Access Points and select the specific access point.
2. Select the specific access point and then under Interfaces > LAN port settings check in the status and PoE to enable PoE on that specific interface of the access point.
3. Power output level can be adjusted using the Power Level drop down.

Figure 114 LAN Port Configuration on specific Access point on Catalyst 9800 Controller



To check the power status on the Access point:

From Controller CLI:

Catalyst 9800:

To check for specific access point from WLC:

```
WLC#show ap name RTP-06-1FL-6300M02 lan port summary
LAN Port status for AP RTP-06-1FL-6300M02
Port ID      status      vlanId      poe          power-level  RLAN
-----
LAN1         Enabled     1           Enabled      2            Enabled
LAN2         Disabled   0           Disabled     NA           Disabled
```

AireOS Controller:

To check the status on AP profile:

(Cisco Controller) >show wlan apgroups

```
Total Number of AP Groups..... 1

Site Name..... default-group
Site Description..... <none>
NAS-identifier..... none
Client Traffic QinQ Enable..... FALSE
DHCPv4 QinQ Enable..... FALSE
AP Operating Class..... Not-configured
Capwap Prefer Mode..... Not-configured
Antenna Monitoring - Status..... Disabled
CustomWeb Global Status..... Enabled
External Web Authentication URL..... <None>
Lan Fast Switching Status..... Disabled
```

Appendix A: Integrating Emerson 1410S Gateway with IW6300

```

RF Profile
-----
2.4 GHz band..... <none>
5 GHz band..... <none>

WLAN ID      Interface      Network Admission Control      Radio Policy
OpenDnsProfile

--More-- or (q)uit
-----
-----
1            client-vlan-112      Disabled                        None
None
2            client-vlan-112      Disabled                        None
None

*AP3600 with 802.11ac Module will only advertise first 8 WLANs on 5GHz radios.

NTP Server Index      Server IP      Auth
-----
-----
-----

```

```

Lan Port configs
-----

LAN      Status      POE      Power Level      RLAN
---      -
1        Enabled    Enabled   2                None
2        Disabled  Disabled  None             None
3        Disabled  Disabled  None             None
4        Disabled  Disabled  None             None

```

To check for specific access point from WLC:

```
(Cisco Controller) >show ap lan port-summary RTP-06-1FL-6300M02
```

LAN Port configuration for AP RTP-06-1FL-6300M02

```

Lan Override ..... Disabled
Port   Status   POE      Power Level
-----
LAN1   ENABLED  ENABLED   2
LAN2   DISABLED  DISABLED  None

```

(Cisco Controller) >

From Access point CLI:

```
RTP-06-1FL-6300M02#show power status
```

Device ID: 0xc4, Firmware Reversion:0x40, Bus:3, Address:0x24

Operating Mode: Semiauto

Available: 35.3 (w) Used:7.0 (w) Remaining:28.3 (w)

Interface	Admin	Oper	Power	Class Max	Config Power
POE-out 1	Up	ON	6.2	15.4	7.0
POE-out 2	Down	OFF	0.0	0.0	30.0

For more details on configuring Power Over Ethernet Out functionality refer to [Power Over Ethernet Configuration](#).

