



# Oil and Gas Refinery WLAN MESH

## Implementation Guide

April 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](http://www.cisco.com/go/offices).

©2020 CISCO SYSTEMS, INC. ALL RIGHTS RESERVED



# Contents

Deployment Models . . . . .	2
Greenfield Deployment . . . . .	2
Brownfield Deployment . . . . .	3
Detailed Component Configurations . . . . .	5
Network Flow . . . . .	5
DHCP Flow for the APs . . . . .	5
Configuring Switches . . . . .	6
Wired Network QoS Configuration . . . . .	11
Configure Allowed Protocols Services . . . . .	20
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 . . . . .	42
WLAN Configuration . . . . .	43
AP Join Policy Configuration . . . . .	47
Policy Profile Creation . . . . .	49
Tags Configuration . . . . .	50
NTP Configuration . . . . .	52
MESH Backhaul Security (MAC Filter) . . . . .	54
Changing an AP Role . . . . .	55
Verifying Mesh . . . . .	55
Ethernet Bridging Configuration . . . . .	56
WLC 802.1x AAA Server Configuration . . . . .	59
Brownfield Deployment Model . . . . .	61
MESH Backhaul Security (MAC Filter) . . . . .	68
WLAN Configuration . . . . .	69

---

HA SSO on 3504 HA Pair and 5520 HA Pair . . . . .	74
Ethernet Bridging . . . . .	79
Wireless MESH Disable VLAN Transparency . . . . .	82
WLC3504 Mobility Group Configuration . . . . .	84
MESH Backhaul Security (MAC Filter). . . . .	84
Ethernet Bridging . . . . .	84
Video Surveillance . . . . .	87
Location Services and Asset Tracking . . . . .	88
Troubleshooting . . . . .	88

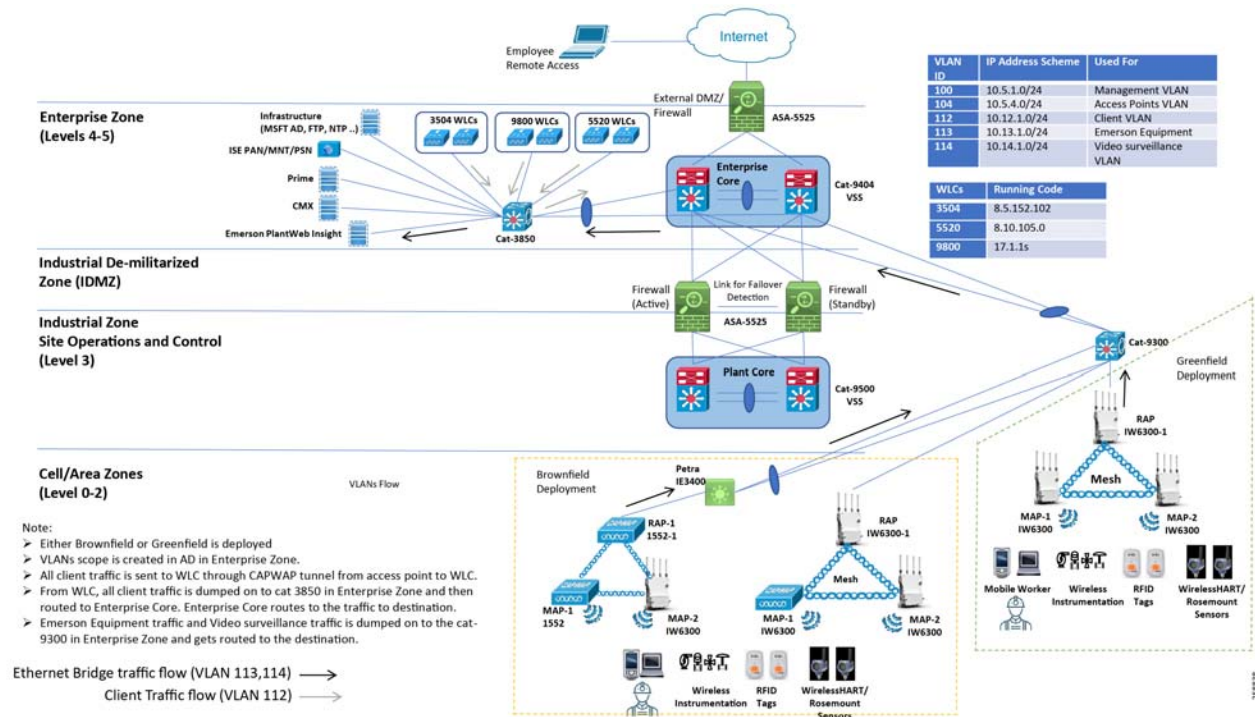


# Oil and Gas Refinery WLAN MESH Implementation Guide

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 IW1552H/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 8.5.105
- AireOS Wireless controllers in SSO running 8.10.0
- 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 IW1552H Access points. Many new features and improvements have been integrated into the CAPWAP IW6300; O&G operators can plan transition to seamlessly replace IW1552H 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 IW1552H & 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

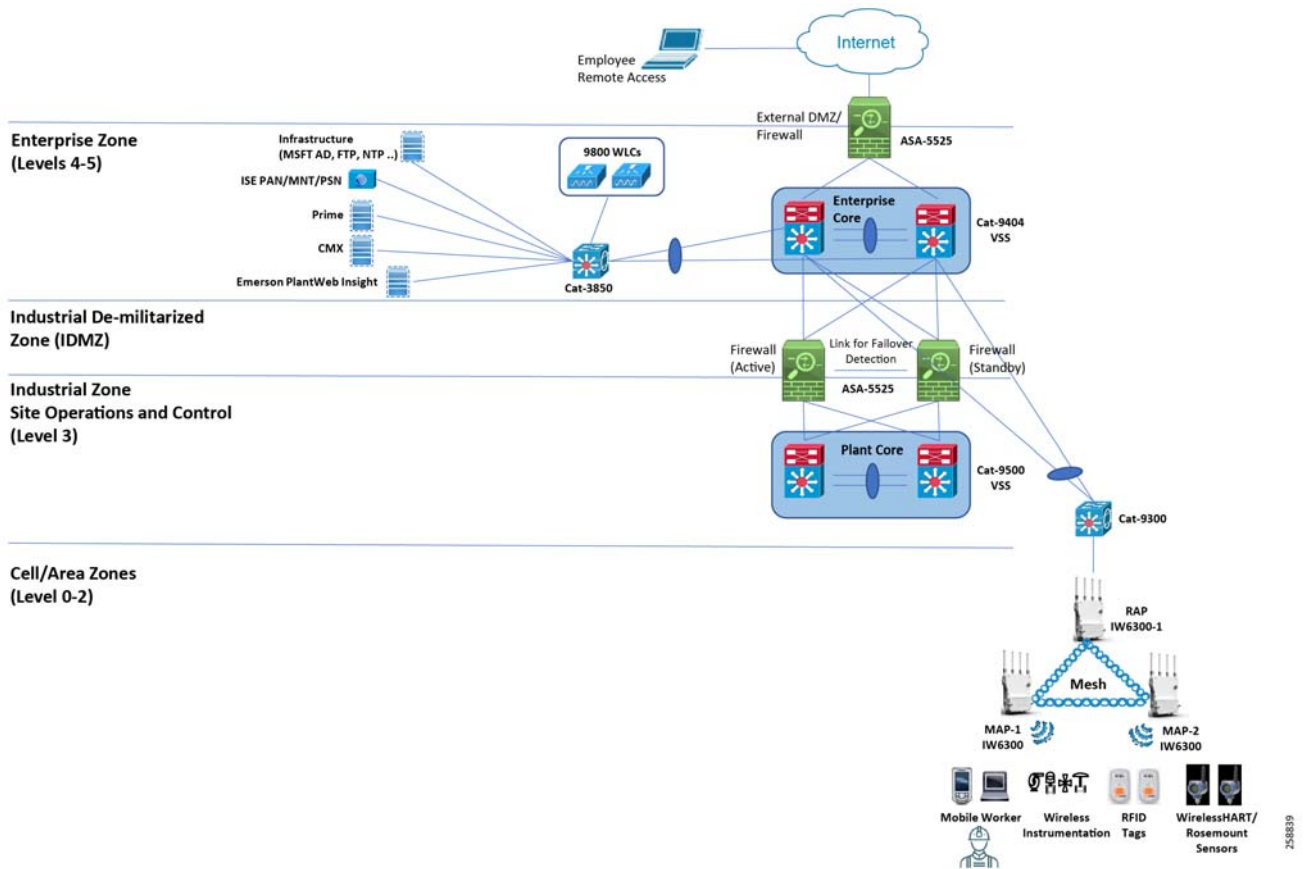
This focus of this document is:

- Deploying a new wireless network in O&G fields and refineries with IW6300 access points (Greenfield Deployment).
- Expanding an existing IW1552H 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

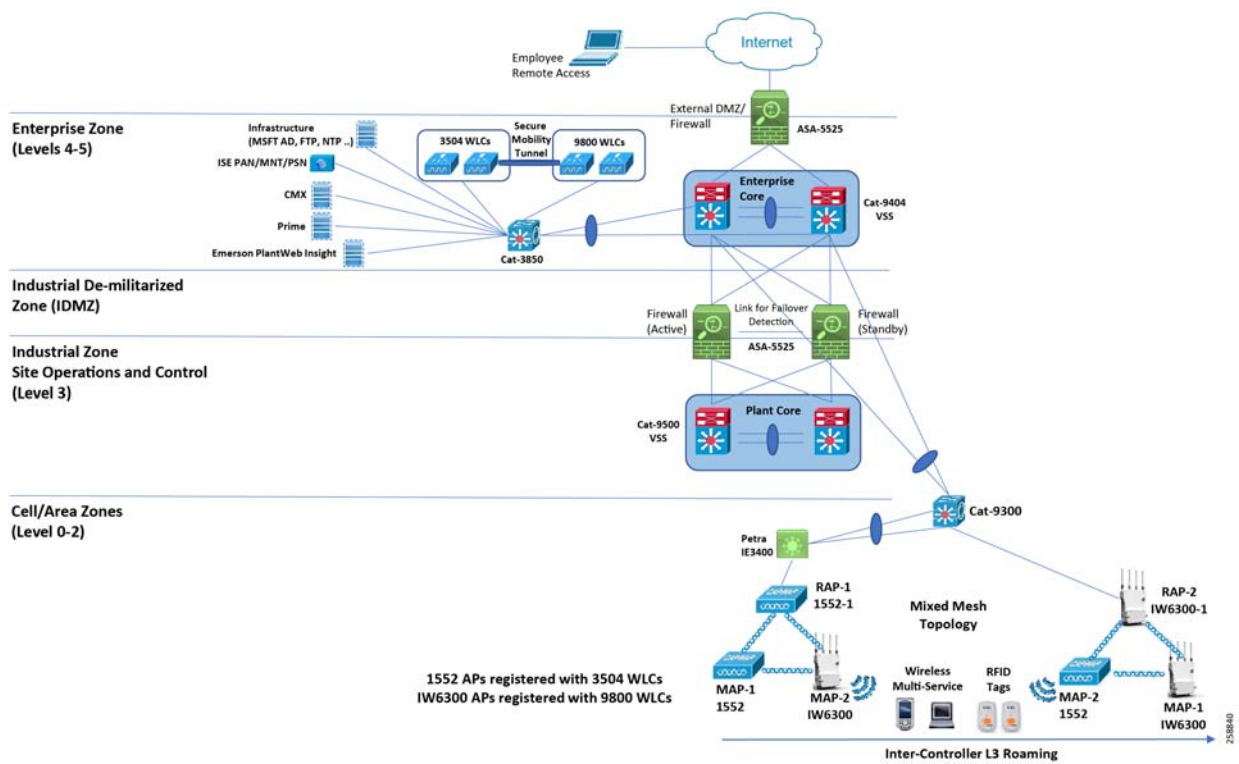
The Brownfield deployment model shows expanding the existing network with Cisco IW6300 Heavy Duty Access Points or replacing the existing IW1552H Access Points (APs) with the new Cisco IW6300 APs. The eventual goal is to phase out all IW1552H Access points with IW6300 Access points.

This deployment model uses two pairs of controllers running different code versions. Existing IW1552H 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.

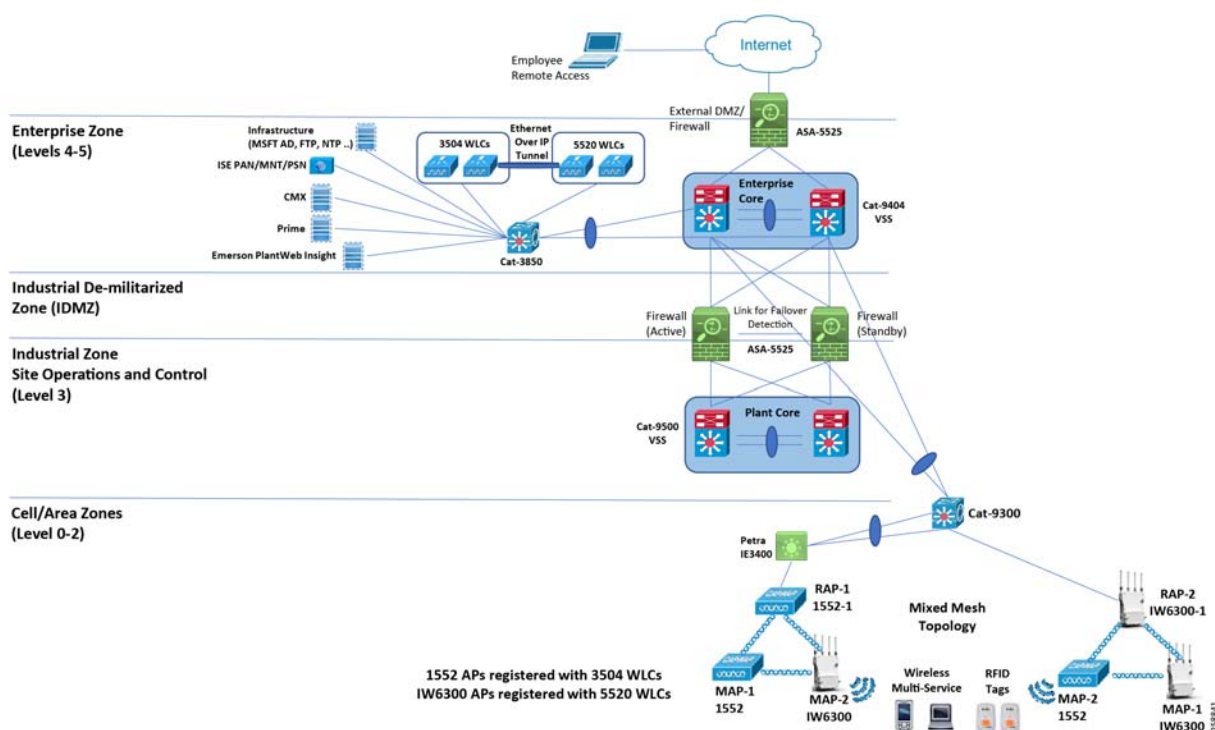
The following two Brownfield deployment models have been validated for this design:

- 3504 wireless controllers running IRCM 8.5 code and 5520 wireless controllers running 8.10
- 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 Component Configurations

### 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

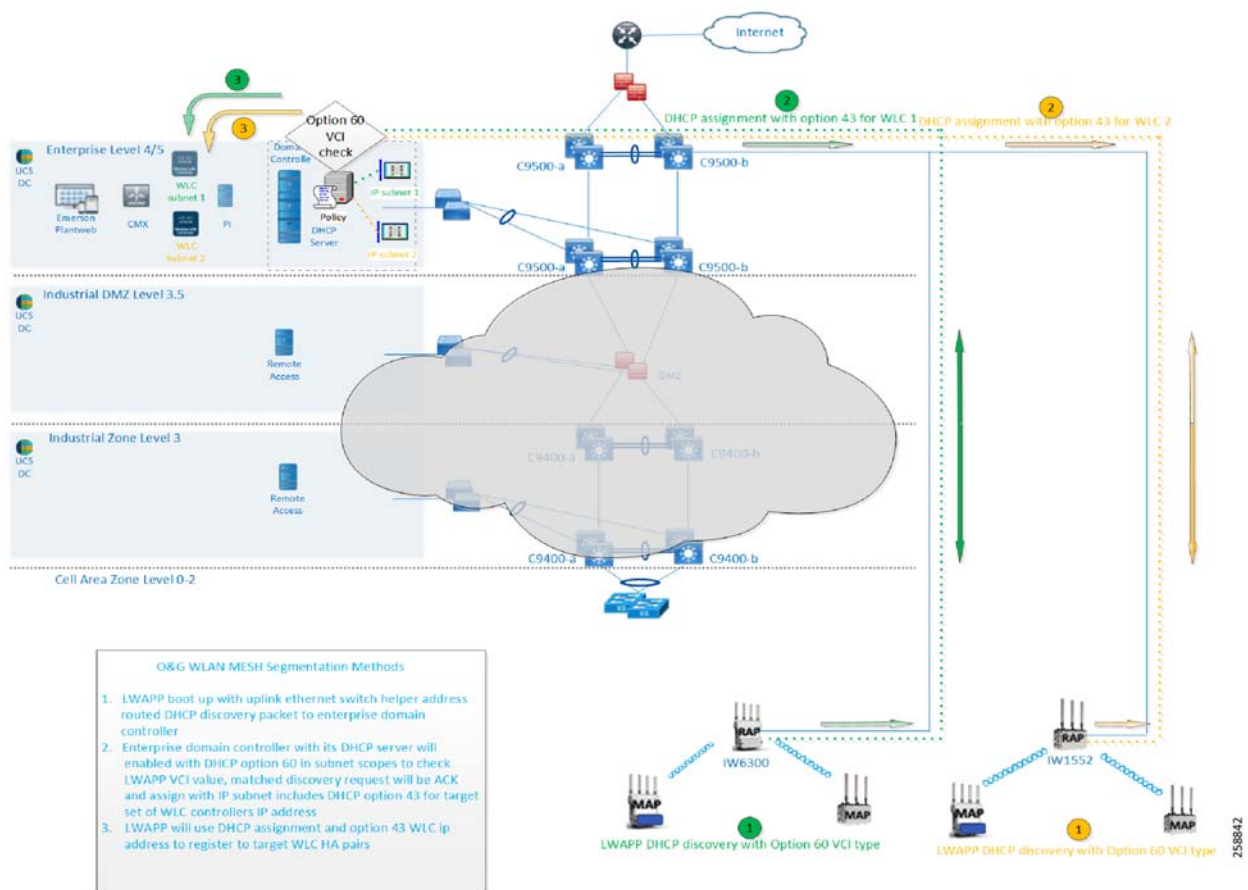
### DHCP Flow for the APs

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
- DHCP Option 60

## Deployment Models

- 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.

## Deployment Models

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

## Deployment Models

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

For example:

## Deployment Models

```
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>
```

For example:

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

## Deployment Models

### 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
```

### 4. Create a channel group.

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

## Deployment Models

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
set qos-group 1
class CIP-Implicit_dscp_any
set qos-group 2
class CIP-Other
set qos-group 2
```

## Deployment Models

```

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
!
interface TwoGigabitEthernet1/0/4
  description Connected to IE-3400
  switchport trunk native vlan 104
  switchport trunk allowed vlan 104,113,150

```



## Deployment Models

```
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
bandwidth remaining percent 40
class class-default
bandwidth remaining percent 20
!
class-map match-any 1588-PTP-General
```

## Deployment Models

```
    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
!
interface TenGigabitEthernet1/0/45
    description connect to 9800-wlc-1-top
    switchport trunk native vlan 100
    switchport trunk allowed vlan 11,100,111,112
```

## Deployment Models

```
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
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
```

## Deployment Models

```

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
!

```

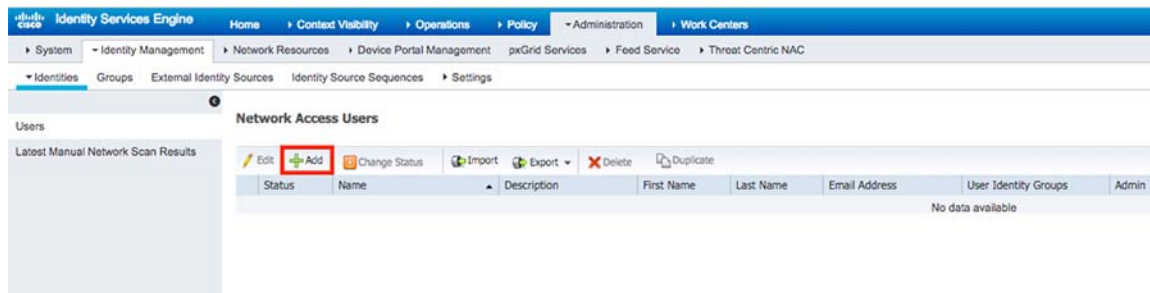
## ISE Configuration—802.1x EAP-FAST Authentication

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.

## Deployment Models

3. Click **Submit**.**Figure 7 Adding Network Access User to ISE**

The screenshot shows the 'New Network Access User' form in the Cisco ISE Administration console. The form is divided into several sections, each with a red box highlighting specific fields:

- Network Access User:** The 'Name' field is set to 'user1'.
- Passwords:** The 'Password Type' is set to 'Internal Users'. The 'Password' and 'Re-Enter Password' fields are both filled with asterisks.
- User Information:** The 'First Name' and 'Last Name' fields are both set to 'user1'.
- Account Options:** The 'Description' field is empty, and the 'Change password on next login' checkbox is unchecked.
- Account Disable Policy:** The 'Disable account if date exceeds' checkbox is unchecked, and the date field is set to '2020-04-21'.
- User Groups:** The 'User Groups' dropdown menu is set to 'ALL\_ACCOUNTS (default)'.

The 'Submit' button is located at the bottom of the form.

The user is created. See [Figure 8](#) below.

**Figure 8 Network Access User Added to ISE**

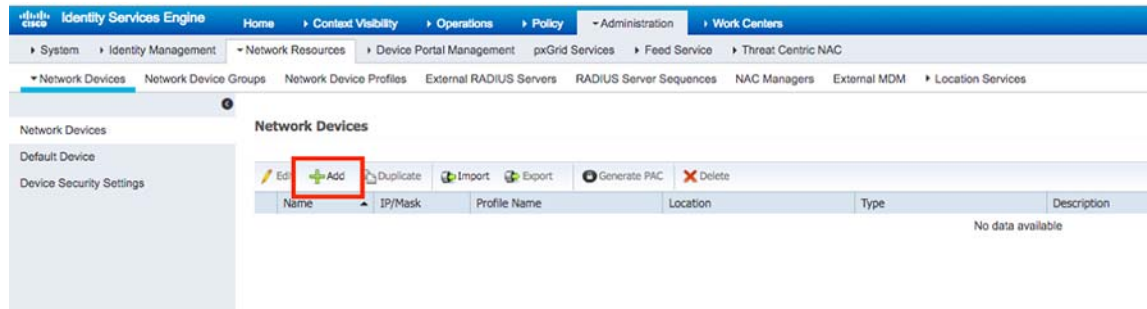
The screenshot shows the 'Network Access Users' table in the Cisco ISE Administration console. The table has a red box around the user entry, which is highlighted in blue. The table columns are: Status, Name, Description, First Name, Last Name, Email Address, User Identity Groups, and Admin.

Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
Enabled	user1		user1	user1		ALL_ACCOUNTS (default)	

**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**

The screenshot displays the Cisco ISE Administration console interface for adding a new network device. The breadcrumb trail indicates the path: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC > Network Devices > Network Device Groups > Network Device Profiles > External RADIUS Servers > RADIUS Server Sequences > NAC Managers > External MDM > Location Services.

The main configuration area is titled "Network Devices" and includes the following fields:

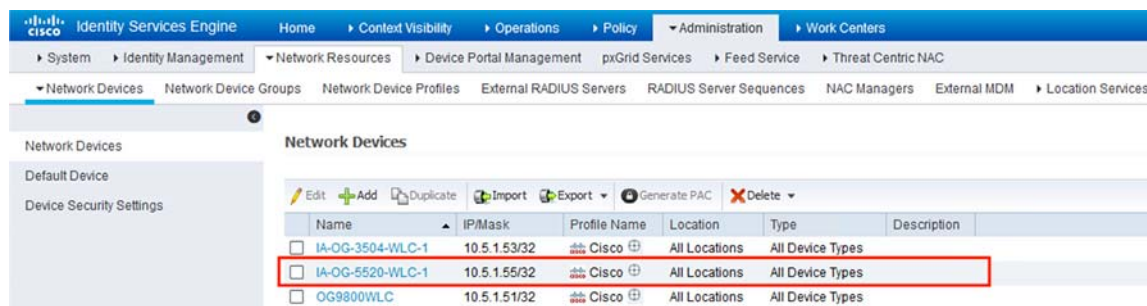
- Name:** IA-OG-5520-WLC-1
- Description:** (empty)
- IP Address:** 10.5.1.55 / 32
- Device Profile:** Cisco
- Model Name:** (empty)
- Software Version:** (empty)
- Network Device Group:**
  - Location:** All Locations (Set To Default)
  - IPSEC:** Is IPSEC Device (Set To Default)
  - Device Type:** All Device Types (Set To Default)

The **RADIUS Authentication Settings** section is expanded, showing the following configuration:

- Protocol:** RADIUS
- Shared Secret:** \*\*\*\*\* (Show)
- Use Second Shared Secret:** (No) (Show)
- CoA Port:** 1700 (Set To Default)
- RADIUS DTLS Settings:**
  - DTLS Required:** (No)
  - Shared Secret:** radius/dtls (Show)
  - CoA Port:** 2083 (Set To Default)
  - Issuer CA of ISE Certificates for CoA:** Select if required (optional)
  - DNS Name:** (empty)
- General Settings:**
  - Enable KeyWrap:** (No)
  - Key Encryption Key:** (empty) (Show)
  - Message Authenticator Code Key:** (empty) (Show)
  - Key Input Format:** ASCII (HEXADECIMAL)

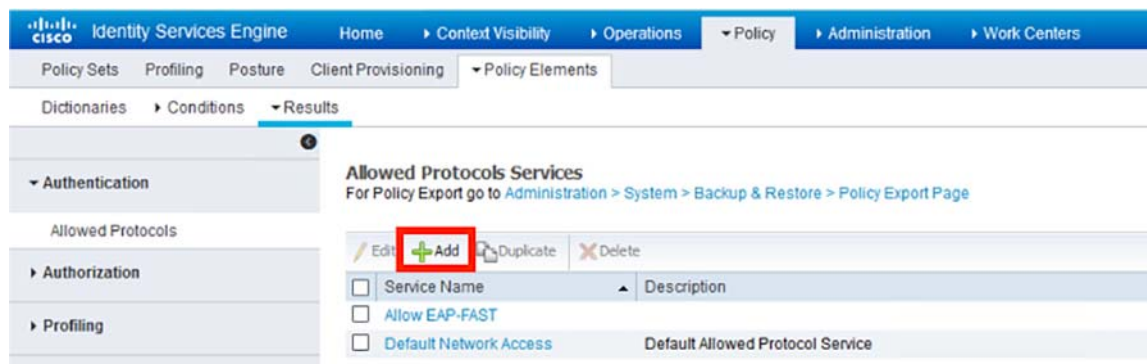
Below the RADIUS settings, there are three expandable sections: TACACS Authentication Settings, SNMP Settings, and Advanced TrustSec Settings, all currently collapsed.

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

1. 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**

2. 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**

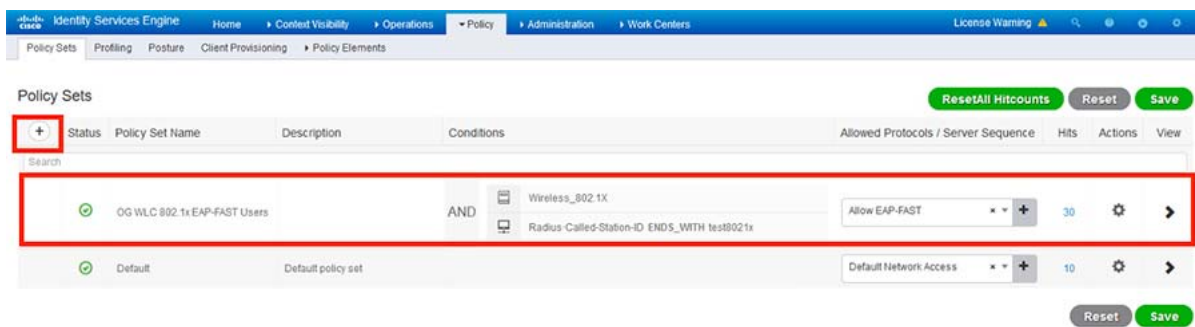
The screenshot shows the Cisco Identity Services Engine (ISE) interface. The left sidebar contains a navigation menu with the following items: Authentication, Authorization, Profiling, Posture, and Client Provisioning. The main content area is titled 'Allowed Protocols Services List > Allow EAP-FAST'. Below this title, there is a section for 'Allowed Protocols' with a 'Name' field set to 'Allow EAP-FAST' and a 'Description' field. Below the 'Allowed Protocols' section, there is a list of protocols with checkboxes. The 'Allow EAP-FAST' checkbox is checked. Below the 'Allow EAP-FAST' checkbox, there is a section for 'EAP-FAST Inner Methods' with several checkboxes: 'Allow EAP-MS-CHAPv2', 'Allow Password Change Retries 3 (Valid Range 0 to 3)', 'Allow EAP-GTC', 'Allow Password Change Retries 3 (Valid Range 0 to 3)', 'Allow EAP-TLS', and 'Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy'. Below this section, there is a radio button for 'Use PACs' which is selected. Below the 'Use PACs' radio button, there are several fields: 'Tunnel PAC Time To Live' (90 Days), 'Proactive PAC update will occur after 10 % of PAC Time To Live has expired', 'Allow Anonymous In-Band PAC Provisioning', 'Allow Authenticated In-Band PAC Provisioning', 'Server Returns Access Accept After Authenticated Provisioning', 'Accept Client Certificate For Provisioning', 'Allow Machine Authentication', 'Machine PAC Time To Live' (1 Weeks), 'Enable Stateless Session Resume', 'Authorization PAC Time To Live' (1 Hours), and 'Enable EAP Chaining'. Below the 'Enable EAP Chaining' checkbox, there is a section for 'Allow EAP-TTLS' with checkboxes for 'Preferred EAP Protocol' (LEAP), 'EAP-TLS L-bit', 'Allow weak ciphers for EAP', and 'Require Message-Authenticator for all RADIUS Requests'. At the bottom of the page, there are 'Save' and 'Reset' buttons.

**Configure Policy Sets on the ISE Server**

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

## Deployment Models

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**

The screenshot displays the Cisco ISE Policy Administration console. The top navigation bar includes links for Identity Services Engine, Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The main content area is titled 'Policy Sets → OG WLC 802.1x EAP-FAST Users'. It shows a table of Policy Sets with columns for Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, and Hits. A red box highlights the 'OG WLC 802.1x EAP-FAST Users' policy set, which has a status of 'Enabled' and 30 hits. Below this, the 'Authentication Policy (2)' section is shown, containing 'Authentication Rule 1' and 'Default'. 'Authentication Rule 1' is highlighted with a red box and shows conditions for 'Wireless\_802.1x' and 'Radius Called-Station-ID: ENDS\_WITH test8021x'. Its actions are 'All User ID Stores', 'Options', 'If Auth fail: REJECT', 'If User not found: REJECT', and 'If Process fail: DROP'. The 'Authorization Policy (2)' section is also shown, containing 'Authorization Rule 1' and 'Default'. 'Authorization Rule 1' is highlighted with a red box and shows conditions for 'Radius Called-Station-ID: ENDS\_WITH test8021x'. Its actions are 'PermitAccess' and 'DenyAccess'.

## 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*.

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:

## Deployment Models

- 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:

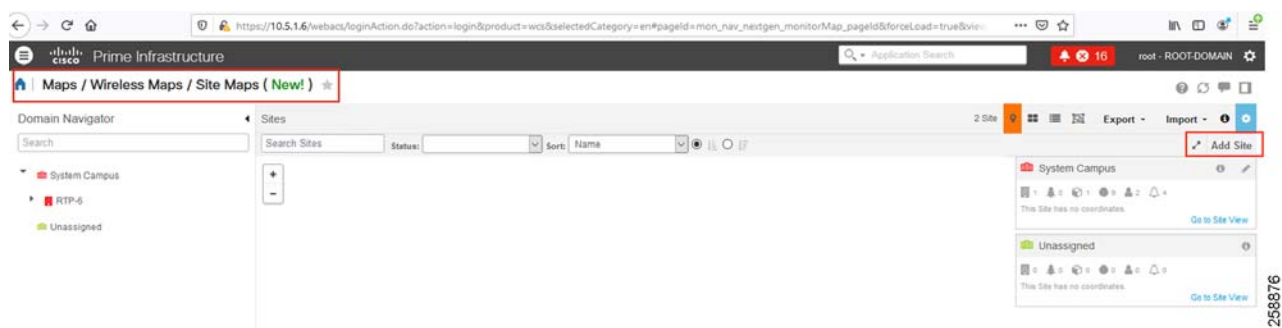
- Campus map
- Outdoor area map
- Buildings
- Mesh access points

## Creating a Wireless site map

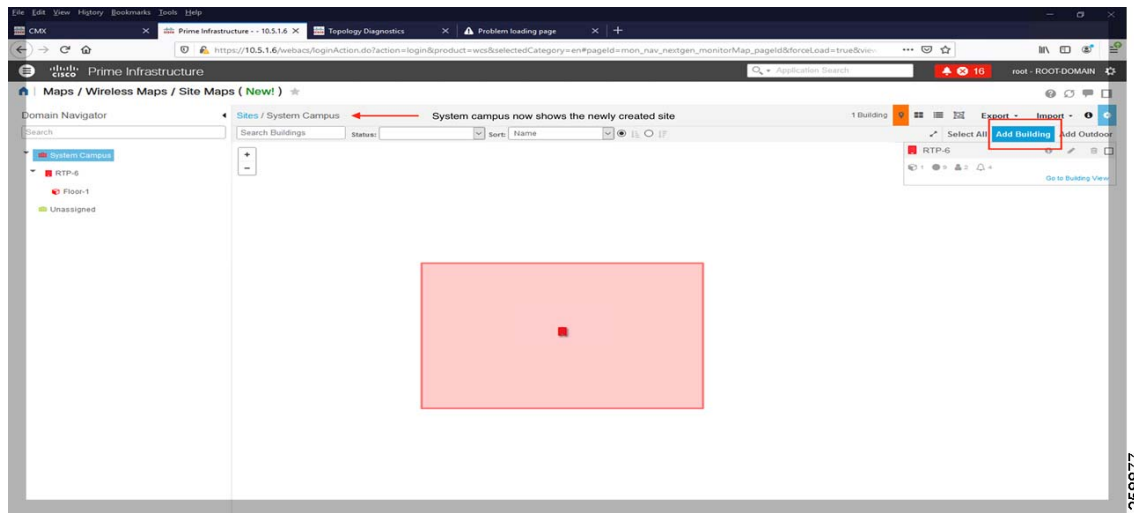
To create your Wireless site map, follow the steps below.

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**.

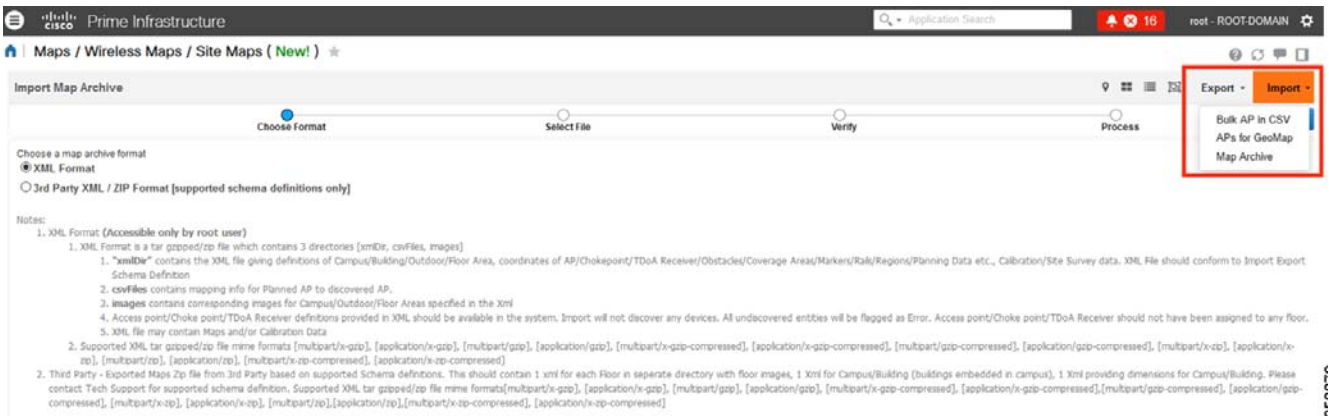
The Import Map Archive wizard opens.

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.

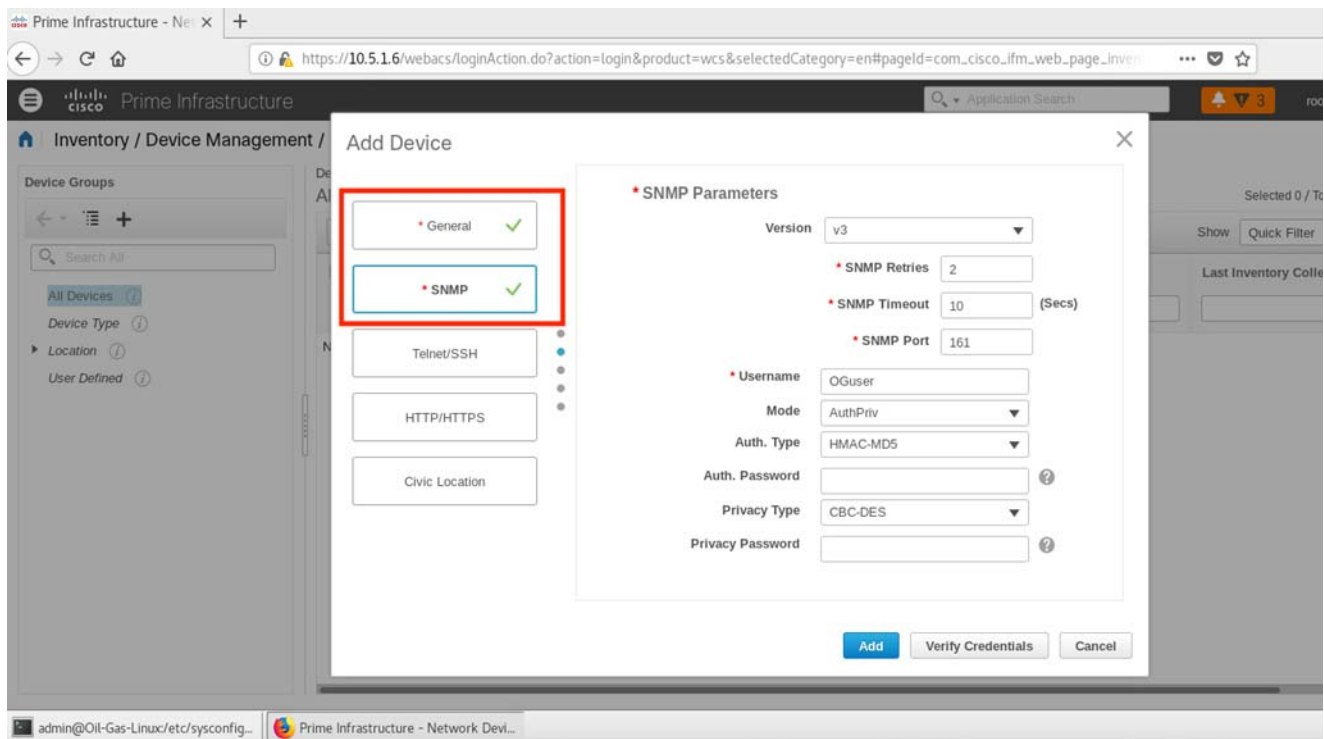
8. From the Show drop-down list, choose **All** or **Quick Filter** to search using the Map Path and Message.
9. After the import process is successful, click **Done**.

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**

## Deployment Models

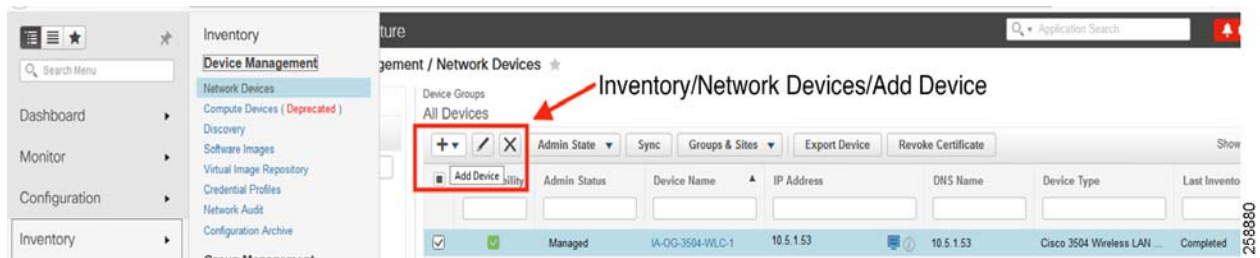
For the SNMP configuration on the Catalyst 9800, refer to *Managing Catalyst 9800 Wireless Controller Series with Prime Infrastructure using SNMP v3 and NetCONF* at:

<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 Brownfield Deployment*.

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

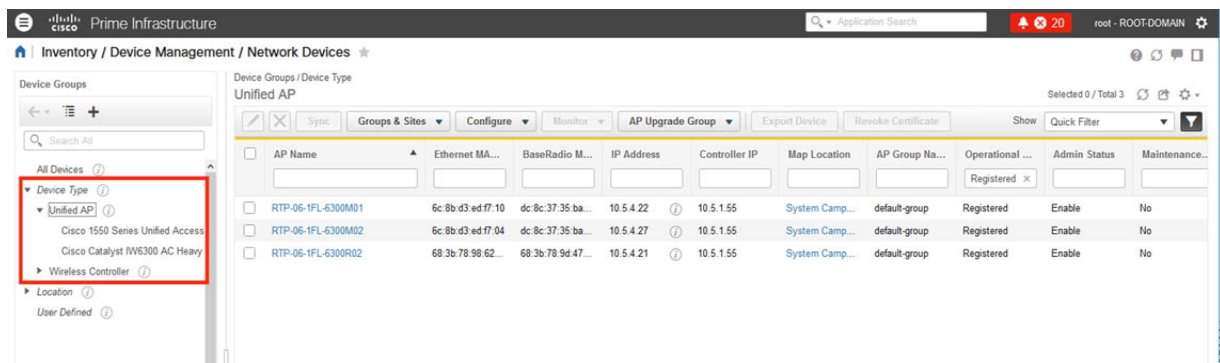
**Figure 20 Prime Infrastructure Add Devices with SNMP discovery**



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](#).

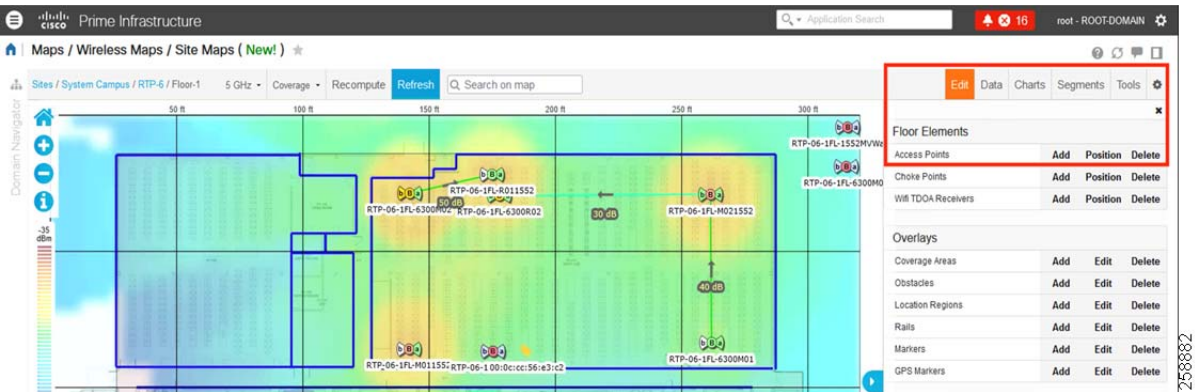
**Figure 21 Prime Infrastructure Network Devices Discovery Status**



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.

[illegible]

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

The screenshot shows the Cisco Prime Infrastructure interface. At the top, the navigation bar includes 'Cisco Prime Infrastructure', 'Maps / Wireless Maps / Site Maps (New!)', and a search bar. The main area displays a site map for 'RTP-6 / Floor-1' with a 5 GHz coverage area. The map shows a building footprint with various access points and mesh links. A red box highlights the 'Access Points (9)' and 'Mesh' options in the 'Tools' menu. Another red box highlights the 'Mesh Links' section in the 'Tools' menu, showing a list of mesh links with their parent and neighbor details. A red arrow points from the 'Tools' menu to the 'Mesh Links' section.

**Tools Menu:**

- Access Points (9)
- Mesh
- Link Label:
  - None
  - Link SNR
  - Packet Error Rate
- Link Color:
  - Link SNR
  - Packet Error Rate
- Mesh Parent-Child hierarchical View
  - Quick Selections
- Mesh Links:
  - RTP-06-1FL-6300R02
  - RTP-06-1FL-M021552
  - RTP-06-1FL-6300M01
  - RTP-06-1FL-R011552
  - RTP-06-1FL-6300M02

**Mesh Links—Displays parent and neighbor details.**

**Update Map View**

**802.11 Tags (1)**

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.

**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:

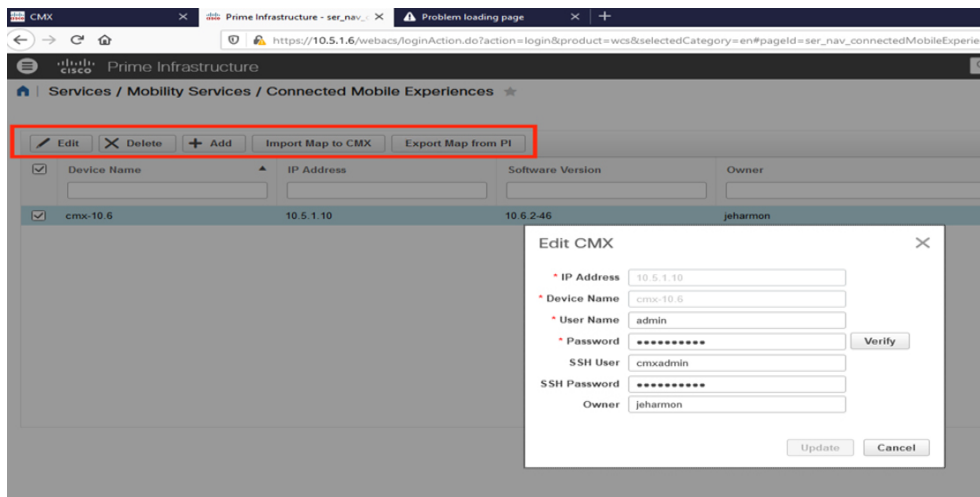
1. Using the Prime Infrastructure interface, choose **Services > Mobility Services > Connected Mobile Experiences**. Select a CMX and then click **Import Map to CMX**.

**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.

## Deployment Models

- 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 Import Status**

The screenshot displays the Cisco Prime Infrastructure web interface. The top navigation bar includes links for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar shows a tree view of configuration options, with 'SNMP' highlighted by a red rectangle. The main panel is titled 'SNMP V3 Users > New' and contains the following fields:

- User Profile Name: OGUser
- Access Mode: Read Only
- Authentication Protocol: HMAC-SHA
- Auth Password: (empty field)
- Confirm Auth Password: (empty field)
- Privacy Protocol: CFB-AES-128
- Priv Password: (empty field)
- Confirm Priv Password: (empty field)

Buttons for '< Back' and 'Apply' are located at the top right of the configuration area.

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](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/cmx\\_config/b\\_cg\\_cmx106/getting\\_started\\_with\\_cisco\\_cmx.html#concept\\_48D1D73677E9492D9D2BA51EE81AD2AE](https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-6/cmx_config/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.
- 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.

## Deployment Models

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.

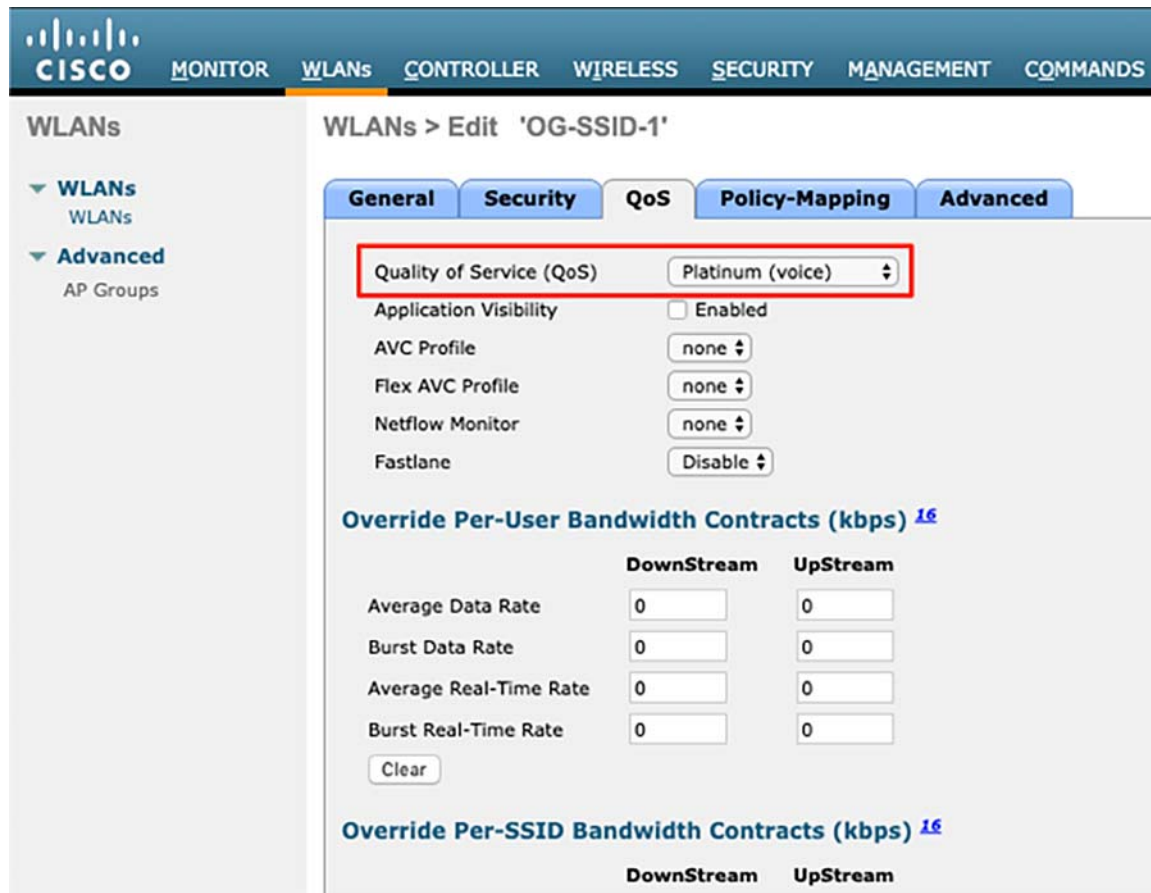
- Wireless LANs support only 802.1Q/P tagged packets.

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](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](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)'. The 'Application Visibility' checkbox is unchecked. The 'AVC Profile', 'Flex AVC Profile', and 'Netflow Monitor' are all set to 'none'. The 'Fastlane' option is set to 'Disable'. Below these settings, the 'Override Per-User Bandwidth Contracts (kbps)' section is visible, with a table for DownStream and UpStream rates. The 'Override Per-SSID Bandwidth Contracts (kbps)' section is also visible at the bottom.

**WLANs > Edit 'OG-SSID-1'**

**General Security QoS Policy-Mapping Advanced**

**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) <sup>16</sup>**

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

Clear

**Override Per-SSID Bandwidth Contracts (kbps) <sup>16</sup>**

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



Figure 28 WLC3504 QoS Profile Configuration

**Wireless**

**Access Points**

- All APs
- Radios
  - 802.11a/n/ac/ax
  - 802.11b/g/n/ax
  - Dual-Band Radios
  - Global Configuration

**Advanced**

- Mesh
- AP Group NTP
- ATF
- RF Profiles
- FlexConnect Groups
- FlexConnect ACLs
- FlexConnect VLAN Templates
- Network Lists
- 802.11a/n/ac/ax
- 802.11b/g/n/ax
- Media Stream
- Application Visibility And Control
- Lync Server
- Country
- Timers
- Netflow
- QoS**
  - Profiles
  - Roles
  - Qos Map

**Edit QoS Profile**

**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**

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

**QoS Map Config**

Qos Map: **Enable**

**Up Stream**

Trust DSCP UpStream: **+**

UP to DSCP Map: ☐

**Down Stream**

**DSCP to UP Map**

User Priority: 0  
DSCP Start: 0  
DSCP End: 0

**Add DSCP Exception**

DSCP Exception: 0  
User Priority: 0

**DSCP Exception List**

DSCP	UP
0	0
2	1
4	1
6	1
10	2
12	2
14	2
18	3
20	3
22	3
26	4
34	5
46	6
48	7
56	7

Figure 30 WLC5520 WLAN QoS Configuration

**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	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

**Override Per-SSID Bandwidth Contracts (Kbps)**

**Foot Notes**

1. Web Policy cannot be used in combination with 2Pass.
2. FlexConnect Local Switching is not supported with Override Interface ACLs.
3. When FlexConnect Local Authentication is enabled, irrespective of AP connected or standalone mode the AP will act as RADIUS.
4. When FlexConnect Local Authentication is disabled, AP in connected mode will use RADIUS as NAS and AP as NAS while in standalone mode.
5. When client exclusion is enabled, a Timeout value of zero means infinity (will require administrative override to re-add excluded clients).
6. Client WPA is not active unless WPA2 is configured.
7. Learn Client IP is configurable only when FlexConnect Local Switching is enabled.
8. When Client IP is configured, it should be enabled to support higher 11n rates.
9. Value zero implies there is no restriction on maximum clients allowed.
10. MAC Filtering is not supported with FlexConnect Local Authentication.
11. MAC Filtering should be enabled.
12. Guest Forwarding, Local Switching, DHCP Required should be disabled.
13. FlexConnect Local Authentication and Central Access feature are not supported with FlexConnect Local Authentication.
14. Enabling go-randomize will prevent clients from decrypting broadcast and multicast packets.
15. When Dynamic Channel is enabled, RRM Bandwidth Allocation will be assigned to this Action, L2 Security and L3 Security will be none.
16. Override Bandwidth Contracts parameters are specific to per Radio of AP. A value of zero (0) indicates that the value specified in the selected QoS profile will take effect.
17. When Dynamic Channel is enabled, RRM Bandwidth Allocation will be assigned to this Action, L2 Security and L3 Security will be none.
18. PSM should be disabled before configuring 802.11e or QoS or PSM.
19. This configuration overrides only local Authentication Type and External Webauth URL. Redirect URL on global config always override the URL on each WLAN. Keep the configuration on global blank if you need per WLAN redirect.
20. PSM format is Configure only parameter, which by default ASCII.



Deployment Models

Figure 31 WLC5520 QoS Profile Configuration

Figure 31 shows the Cisco WLC5520 QoS Profile Configuration page. The page displays the configuration for a QoS profile named "platinum". The configuration includes fields for the QoS Profile Name, Description, and various bandwidth contracts (Per-User and Per-SSID). The "Per-User Bandwidth Contracts (kbps)" section shows fields for Average Data Rate, Burst Data Rate, Average Real-Time Rate, and Burst Real-Time Rate, with tabs for DownStream and UpStream. The "Per-SSID Bandwidth Contracts (kbps)" section also shows similar fields. The "VLAN QoS Parameters" section includes fields for Maximum Priority, Unicast Default Priority, and Multicast Default Priority. The "Wired QoS Protocol" section shows fields for Protocol Type (802.1p) and 802.1p Tag (5). The "Foot Notes" section states: "1. Override bandwidth contracts parameters are specific to per radio of AP. The value zero (0) indicates the feature is disabled."

Figure 32 WLC5520 WLAN QoS MAP Configuration

Figure 32 shows the Cisco WLC5520 WLAN QoS MAP Configuration page. The page displays the configuration for a QoS Map named "Streamable". The configuration includes fields for the QoS Map, QoS Map Type, and various DSCP mappings. The "Up Stream" section shows fields for Trust DSCP Upstream and UP to DSCP Map. The "Down Stream" section shows fields for DSCP to UP Map, User Priority, DSCP Start, and DSCP End. The "DSCP to UP Map List" table shows a mapping of DSCP values to UP values. The "Add DSCP Exception" section shows fields for DSCP Exception, User Priority, and DSCP Start/End. The "DSCP Exception List" table shows a mapping of DSCP values to UP values.

UP	Start DSCP	End DSCP
0	0	7
1	8	15
2	16	23
3	24	31
4	32	39
5	40	47
6	48	55
7	56	63

DSCP	UP
0	0
2	1
4	1
6	1
10	2
12	2
14	2
18	3
20	3
22	3
26	4
34	5
46	6
48	7
56	7

**Figure 33 Cat9800 QoS Group Configuration**

## 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:

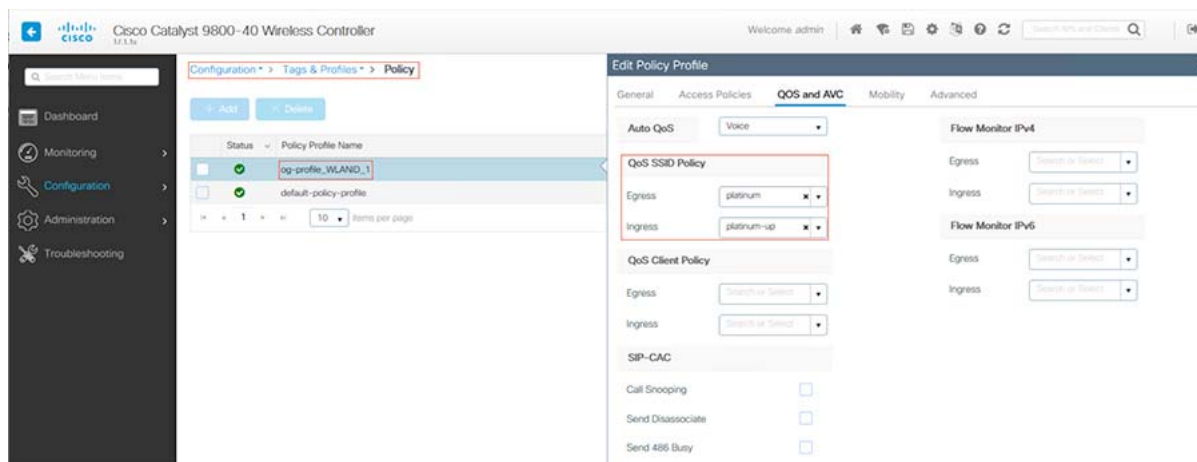
- High availability between controllers reduces the downtime in live networks. When the Active wireless LAN controller goes down, the stand-by controller takes its place with minimum downtime.
- The Catalyst 9800 Wireless Controller supports the stateful switchover (SSO) of access points and clients. 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.
- A physical connection has to be maintained between the WLCs that are in HA SSO. There are dedicated RJ-45 RP ports or Gigabit SPF 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 SPF 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.

## Detailed Configuration of the Deployment Models

- 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:**

- To configure HA SSO go to **Administration > Device > Redundancy**.
- Enable the redundancy configuration and select Redundancy pairing type **RP**.
- 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.
- 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.
- 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](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**

The screenshot shows the Catalyst 9800 Web Interface. The left sidebar contains a search bar and navigation links: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main content area is titled 'Administration > Device'. Under the 'Redundancy' tab, the 'Redundancy Configuration' section is expanded, showing a green 'ENABLED' status. The configuration parameters are as follows:

Parameter	Value
Redundancy Configuration	ENABLED
Redundancy Pairing Type	<input type="radio"/> RMI+RP <input checked="" type="radio"/> RP
Local IP*	10.5.1.61
Netmask*	255.255.255.0
Remote IP*	10.5.1.62
Keep Alive Timer	1 x 100 (milliseconds)
Keep Alive Retries	3
Active Chassis Priority*	2
Standby Chassis Priority*	1

**Figure 35 Redundancy Configuration on Stand-by Catalyst 9800**

The screenshot shows the Catalyst 9800 Web Interface for a stand-by device. The configuration parameters are as follows:

Parameter	Value
Redundancy Configuration	ENABLED
Redundancy Pairing Type	<input type="radio"/> RMI+RP <input checked="" type="radio"/> 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 Version	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

## Detailed Configuration of the Deployment Models

```
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 =
    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](#).

## Detailed Configuration of the Deployment Models

**Figure 36 Monitor Redundancy Configuration**

The screenshot displays the 'Monitoring > General > System' page, specifically the 'Redundancy' tab. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main content area has tabs for Inventory, Memory Utilization, CPU Utilization, Wireless Interface, Management Summary, and Redundancy. Under the Redundancy tab, there are three sub-tabs: General, Active Statistics, and Standby Statistics. The General sub-tab is active, showing a summary of the redundancy state. Below this, the 'Chassis Details' table lists two chassis: Chassis 1 (Active) and Chassis 2 (Standby). The 'Switchover Details' table is currently empty, showing 'No items to display'.

Chassis	Role	MAC Address	Priority	H/W Version	Current State	IP Address	RMI IP Address	Mobility MAC Address	Image Version	Device Uptime
1	Active	d4e8.80b2.d74d	2	V02	Ready	10.5.1.61	NA	d4e8.80b2.d74b	17.1.1s	3 days, 6 hours, 58 minutes
2	Standby	d4e8.80b2.d080	1	V02	Ready	10.5.1.62	NA	d4e8.80b2.d08b	17.1.1s	3 days, 6 hours, 56 minutes

**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**.
2. 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**

The screenshot displays the 'Configuration > Wireless > Mesh' page, specifically the 'Global Config' tab. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main content area has tabs for Global Config and Profiles. Under the Global Config tab, there are four sections: General, Backhaul, Security, and Alarm. The Alarm section is expanded, showing various parameters that can be configured. The 'Apply' button is visible in the top right corner.

Section	Parameter	Value
General	Ethernet Bridging Allow BPOU	<input type="checkbox"/>
	Subset Channel Sync	<input type="checkbox"/>
Backhaul	Extended UNI B Domain Channels	<input type="checkbox"/>
	RRM	<input type="checkbox"/>
Security	PSK Provisioning	<input type="checkbox"/>
	Default PSK	<input type="checkbox"/>
Alarm	Max Hop Count	4
	Recommended Max Children for MAP	10
	Recommended Max Children for RAP	20
	Parent Change Count	3
	Low Link SNR (dB)	12
	High Link SNR (dB)	60
Association Count	10	

3. Under the Profile tab, you can add a new mesh profile.

## Detailed Configuration of the Deployment Models

4. For faster mesh convergence select the Convergence Method as Very Fast and enable background scanning and channel change notification.
5. 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**

The screenshot shows the 'Edit Mesh Profile' configuration page. The 'General' tab is active, displaying various settings for the mesh profile. The 'Name' field is highlighted with a red box. The 'Convergence Method' is set to 'Very Fast', 'Background Scanning' is checked, and 'Channel Change Notification' is checked. The 'Advanced' tab is also visible, showing settings for Backhaul amsdu, Backhaul Client Access, Battery State for an AP, Full sector DFS status, and LSC.

6. 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**

The screenshot shows the 'Edit Mesh Profile' configuration page with the 'Advanced' tab selected. The 'Security' section is highlighted with a red box, showing the 'Method' set to 'PSK', 'Authentication Method' set to 'Enter Method', and 'Authorization Method' set to 'default'. The 'Ethernet Bridging' section is also visible, showing 'VLAN Transparent' checked and 'Ethernet Bridging' checked. The 'Bridge Group' section shows 'Bridge Group Name' set to 'mesh1' and 'Strict Match' checked.

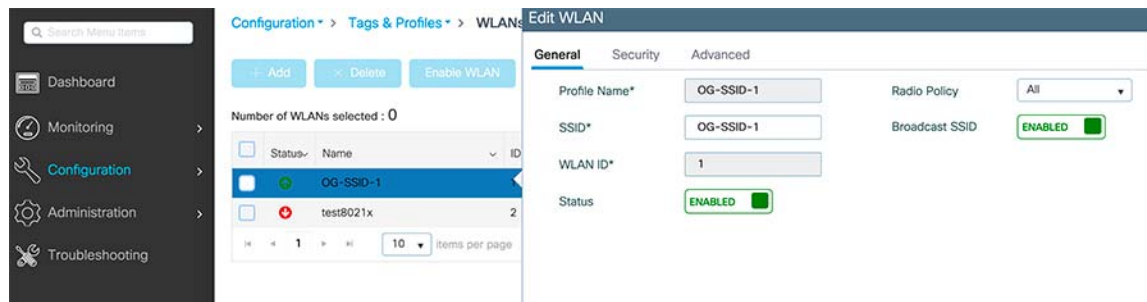
## WLAN Configuration

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

WPA + WPA2

Fast Transition

Enabled

MAC Filtering

☐

Over the DS

☒

Protected Management Frame

Reassociation Timeout

20

PMF

Disabled

MPSK Configuration

WPA Parameters

MPSK

☐

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

ASCII

PSK Type

Unencrypted

Pre-Shared Key\*

.....

**Figure 42 Advanced Tab Configuration on WLAN**

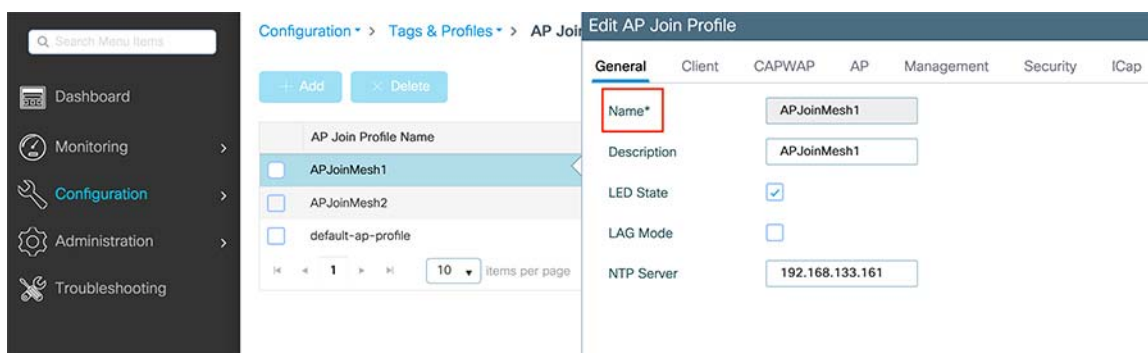
Edit WLAN			
General	Security	Advanced	
Coverage Hole Detection	<input checked="" type="checkbox"/>	Universal Admin	<input type="checkbox"/>
Aironet IE	<input checked="" type="checkbox"/>	Load Balance	<input type="checkbox"/>
P2P Blocking Action	Disabled	Band Select	<input type="checkbox"/>
Multicast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

## 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.

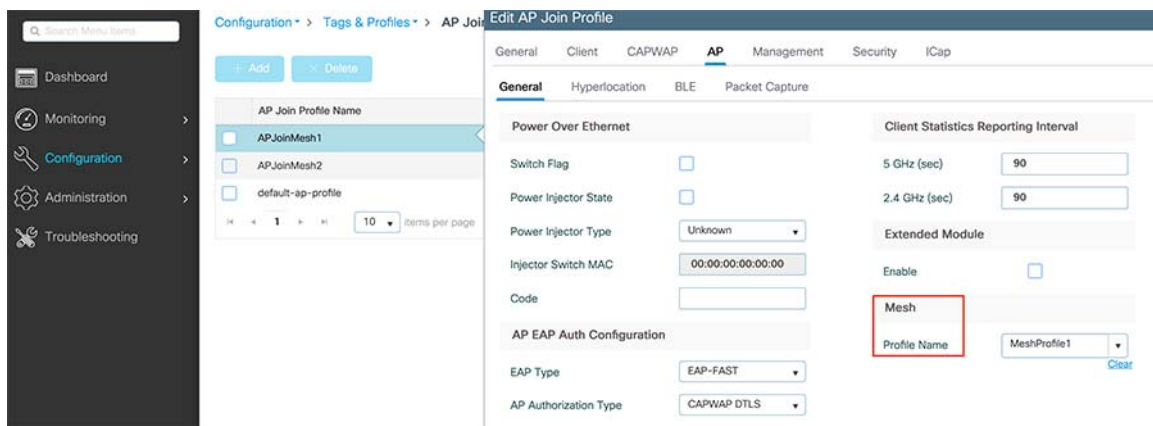
1. To configure a new AP Join policy, go to **Configuration > Tags & Profiles > AP Join**.
2. On AP Join Profile, click **Add**.
3. On the Creating AP Join Profile General tab, enter a name and description for the AP Join Profile and then click **Apply to the device**.

**Figure 43 Creating AP Join Profile**

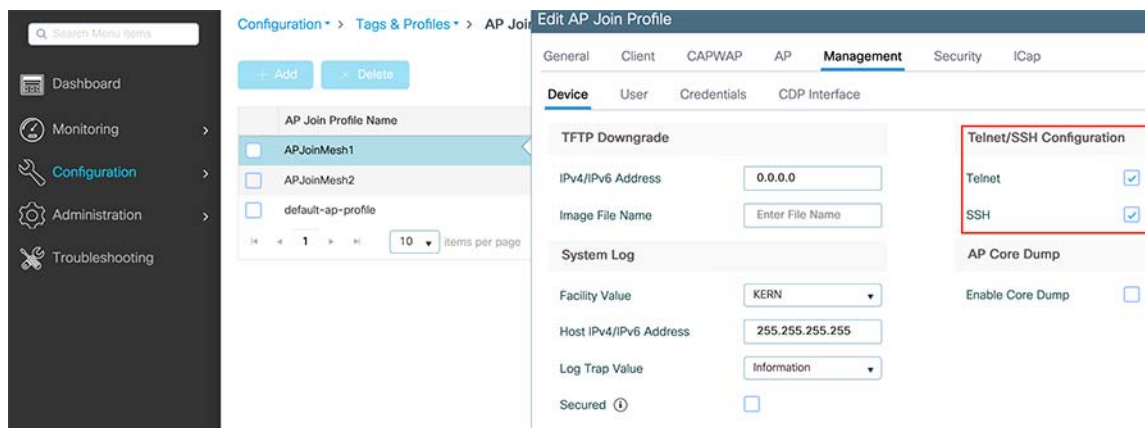


4. Click on the created AP join policy and then go to the AP tab. In the General pane select the Mesh profile that was created in [Configuring Mesh Profile](#).

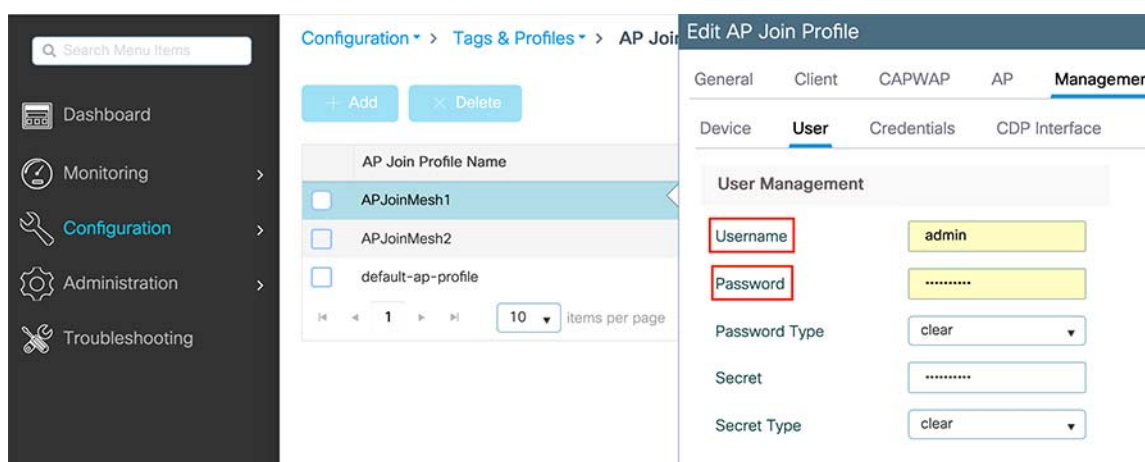
**Figure 44 Associating Mesh Profile to AP Join Policy**



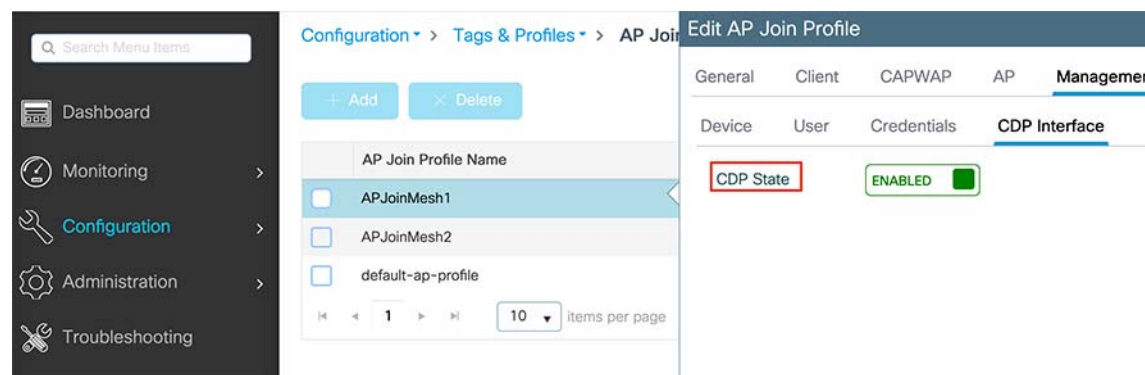
5. On the Management tab:
  - a. In Device tab, enable SSH/Telnet for the access point that joins this profile.

**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.

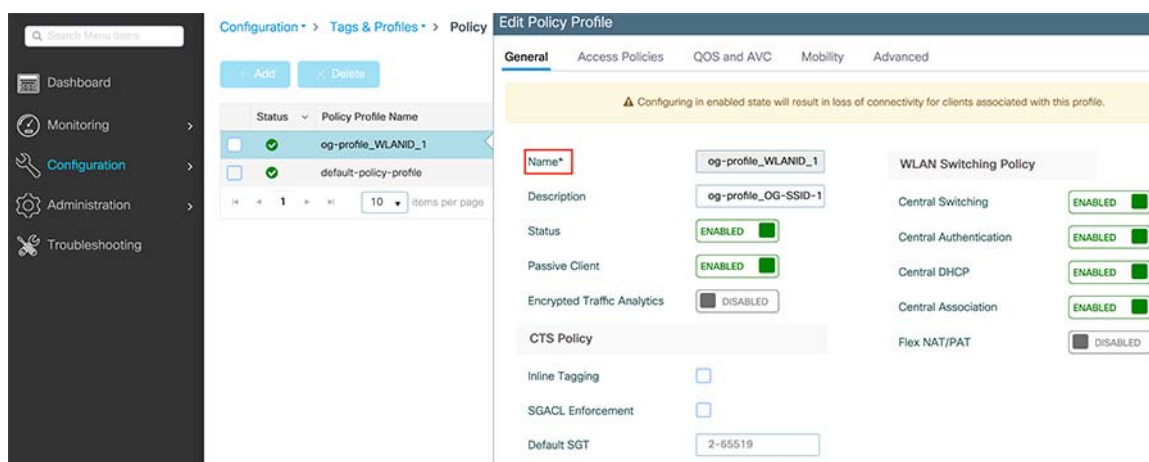
## Policy Profile Creation

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.

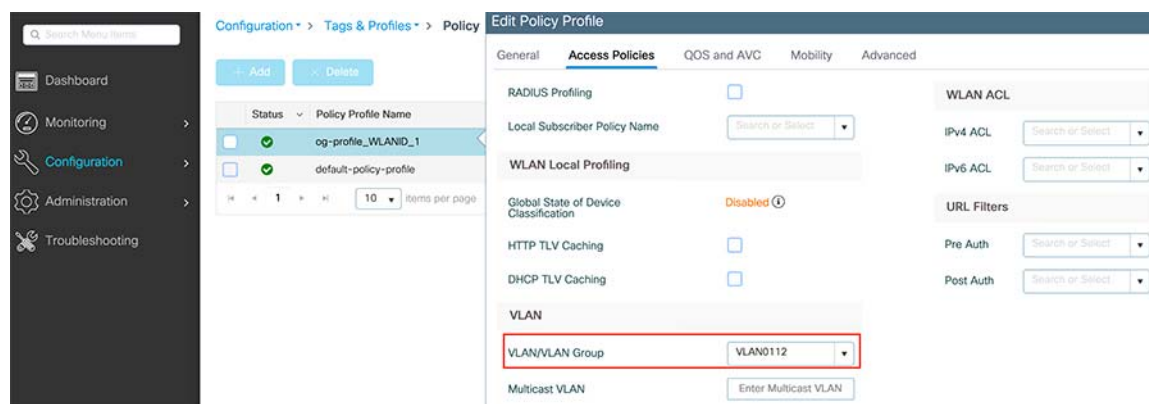
1. To configure the Policy profile, go to **Configuration > Tags & Profiles > Policy** and click **Add** on the Policy page.
2. On the General tab, enter the name, description of the policy profile, and enable passive client.
3. By default all the central switching, central authentication, central DHCP,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

og-profile

Description

Enter 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

◀ 1 ▶

10 items per page

1 - 2 of 2 items

Map WLAN and Policy

WLAN Profile\*

OG-SSID-1

Policy Profile\*

og-profile\_WLANID\_1

✕

✓

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\*

Site1

Description

local-site

AP Join Profile

APJoinMesh1

Control Plane Name

Enable Local Site

☒

Cancel

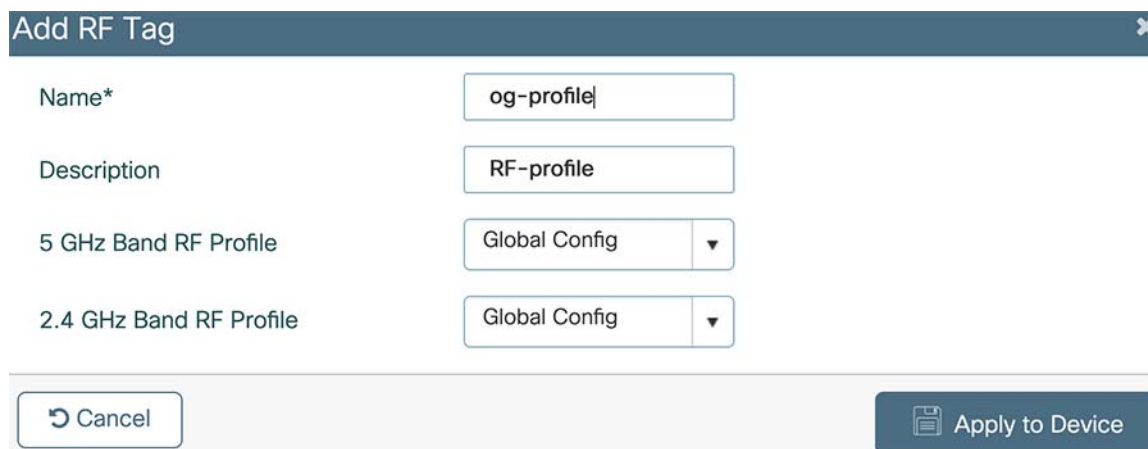
Apply to Device

## 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**



The screenshot shows a web-based configuration window titled "Add RF Tag". It contains the following fields and controls:

- Name\***: A text input field containing "og-profile".
- Description**: A text input field containing "RF-profile".
- 5 GHz Band RF Profile**: A dropdown menu with "Global Config" selected.
- 2.4 GHz Band RF Profile**: A dropdown menu with "Global Config" selected.
- Buttons**: A "Cancel" button on the left and an "Apply to Device" button on the right.

## 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\*

192.168.133.161

Prefer

☒

VRF

☒

VRF Name

Mgmt-intf

Source Address

None

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 - 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
```

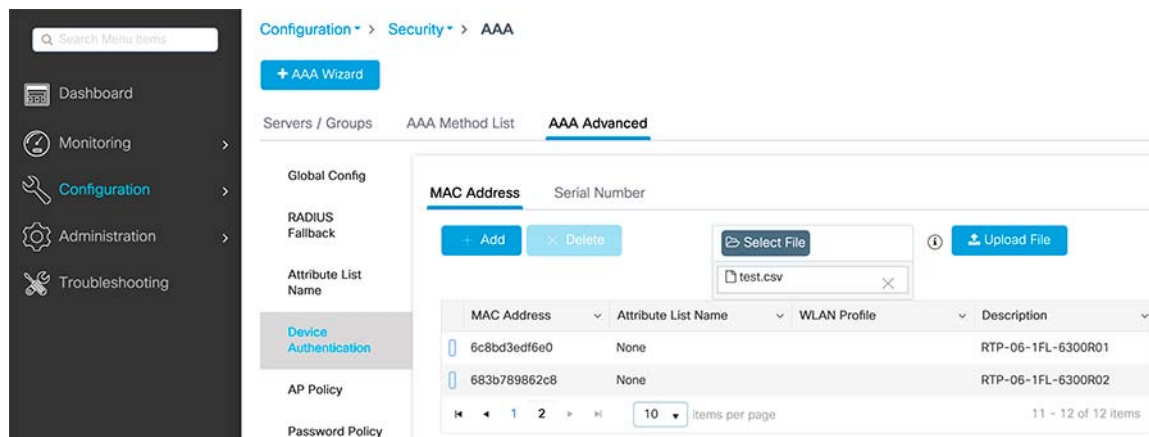
## MESH Backhaul Security (MAC Filter)

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

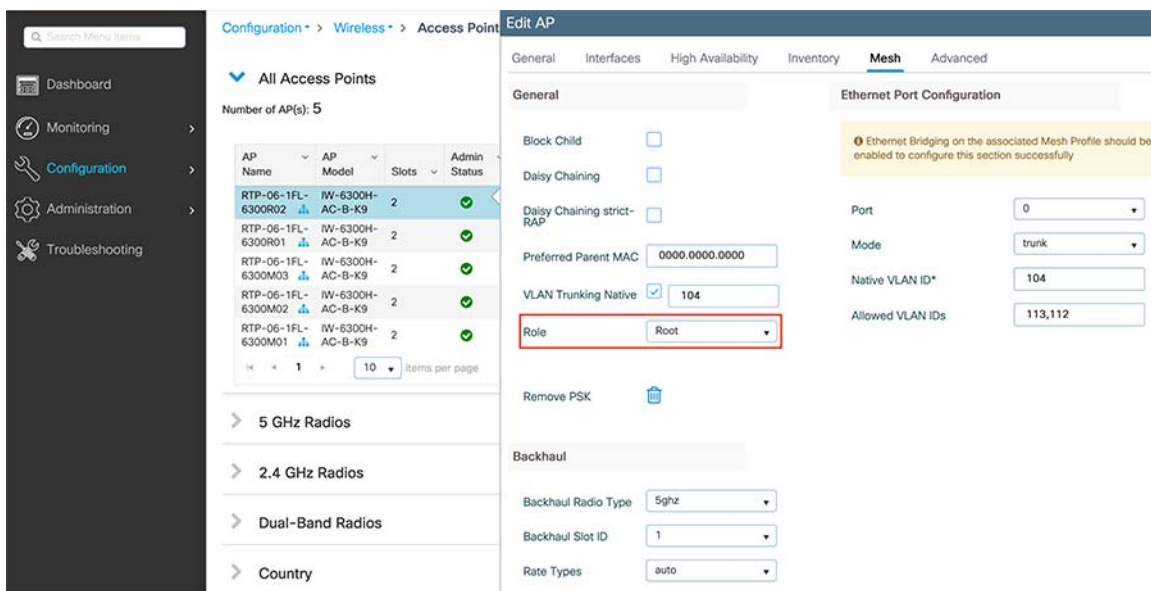
In this deployment all the access points need to be in Bridge mode. If the AP is in different mode other than bridge mode, you can change the mode of the AP after it is registered with WLC.

1. To change the access point from 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 from 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**



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**

The screenshot shows the WLC Monitoring > Wireless > Mesh page. The left sidebar contains navigation links: Dashboard, Monitoring (selected), Configuration, Administration, and Troubleshooting. The main content area is titled 'Monitoring > Wireless > Mesh' and has a sub-tab 'AP Convergence'. It displays 'Global Stats' with the following data:

Global Stats	Value
Number of Bridge APs	5
Number of RAPs	2
Number of MAPs	3
Number of Flex+Bridge APs	0
Number of Flex+Bridge RAPs	0
Number of Flex+Bridge MAPs	0

Below the stats is a 'Tree' view showing the mesh topology. The output is as follows:

```

=====
AP Name [Hop Ctr,Link SNR,BG Name,Channel,Prof Parent,Chan Util,Clients]
=====
[Sector 1]
-----
RTP-06-1FL-6300R02 [0, 0, mesh1, (60), 0000.0000.0000, 1%, 0]
[-RTP-06-1FL-6300M02 [1, 32, mesh1, (60), 0000.0000.0000, 1%, 1]
[Sector 2]
-----
RTP-06-1FL-6300R01 [0, 0, mesh1, (60), 0000.0000.0000, 2%, 0]
[-RTP-06-1FL-6300M03 [1, 52, mesh1, (60), 0000.0000.0000, 0%, 0]
[-RTP-06-1FL-6300M01 [1, 20, mesh1, (60), 0000.0000.0000, 1%, 0]
Number of Bridge APs : 5
Number of RAPs : 2
Number of MAPs : 3
(*) Wait for 3 minutes to update or Ethernet Connected Mesh AP.
(**) Not in this Controller

```

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**

**Edit Mesh Profile**

General **Advanced**

**Security**

Method: PSK

Authentication Method: Enter Method

Authorization Method: default

**Ethernet Bridging**

VLAN Transparent: ☐

**Ethernet Bridging**: ☒

**Bridge Group**

Bridge Group Name: mesh1

Strict Match: ☒

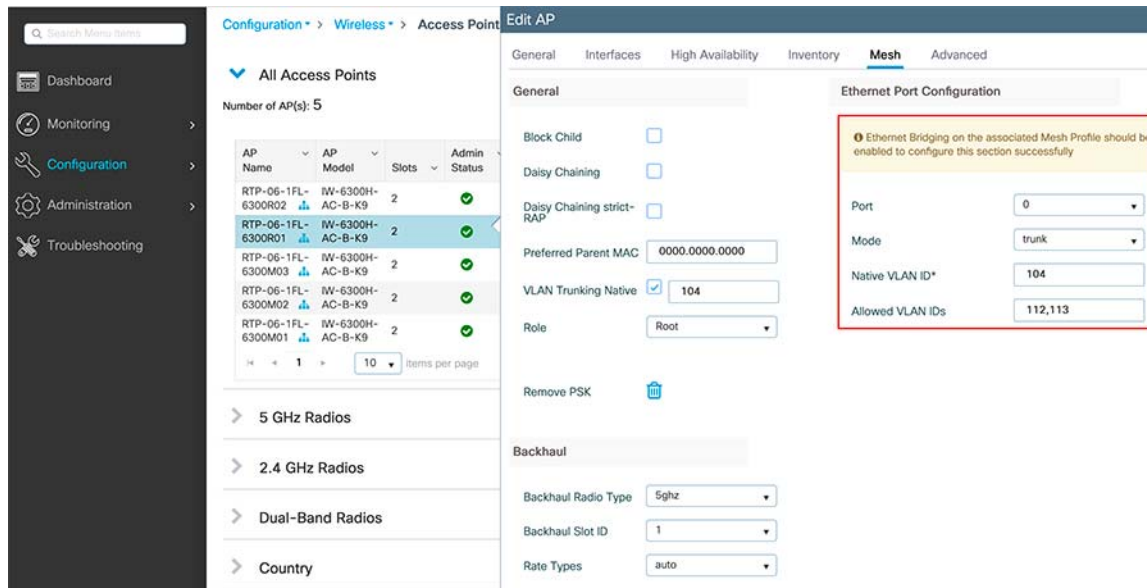
**5 GHz Band Backhaul**

Rate Types: auto

**2.4 GHz Band Backhaul**

Rate Types: auto

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.

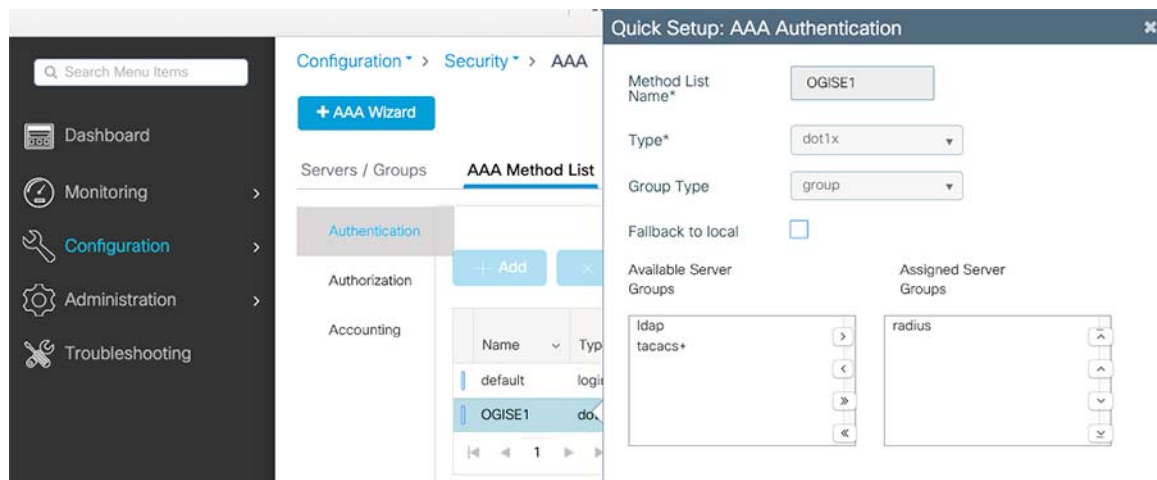
1. Declare a RADIUS server. Navigate to **Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > +Add**.

**Figure 62 Radius Server Configuration**

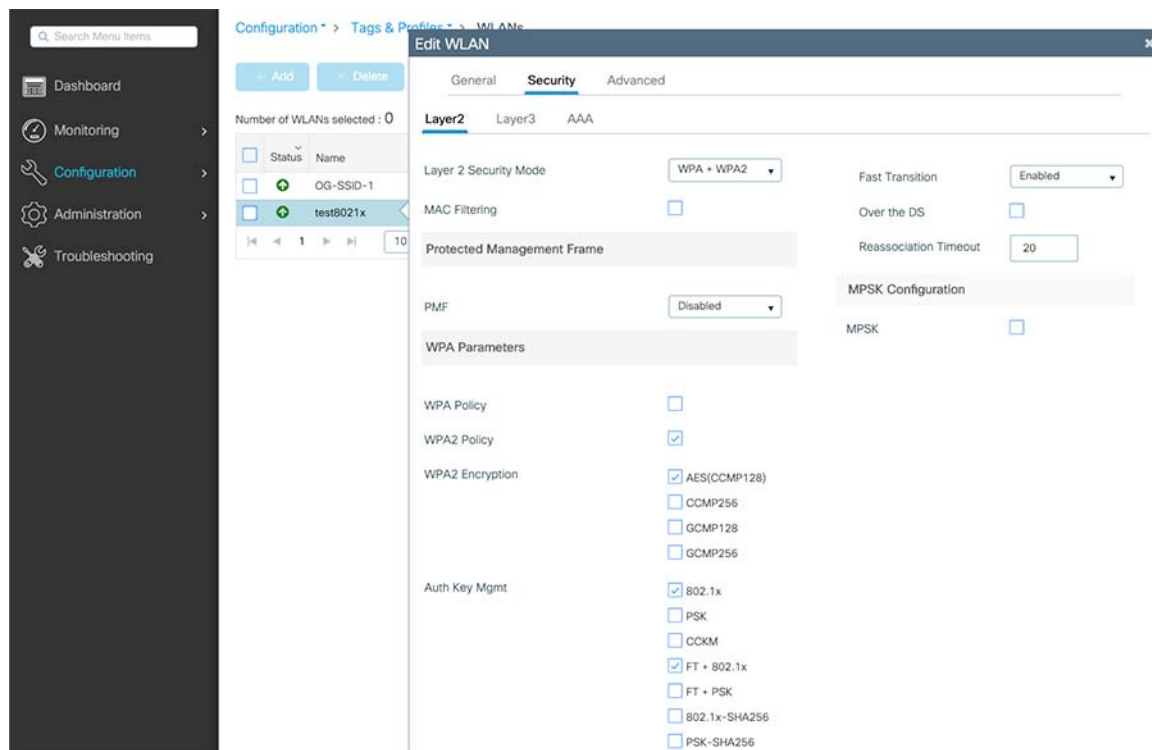
The screenshot displays the Cisco ISE configuration interface for editing a RADIUS server. The breadcrumb trail at the top reads: Configuration > Security > AAA. The left sidebar contains a search bar and a menu with options: Dashboard, Monitoring, Configuration (selected), Administration, and Troubleshooting. The main configuration area is divided into two tabs: 'Servers / Groups' and 'AAA Method List'. Under 'Servers / Groups', there are 'Add' and 'Delete' buttons. A list of servers is shown, with 'OGISE' selected. The right panel, titled 'Edit AAA Radius Server', contains the following fields:

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**.

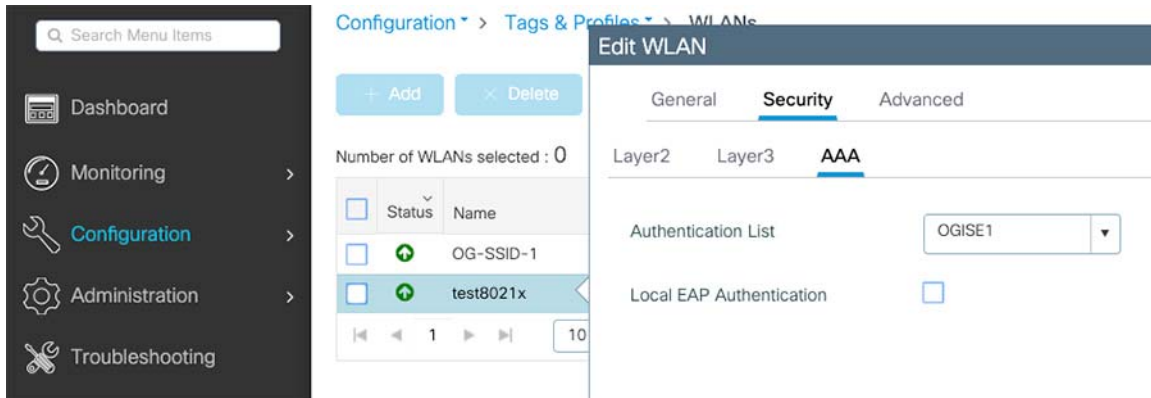
**Figure 63 Authentication Method List**

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

The Brownfield deployment model as shown in [Figure 3](#) and [Figure 4](#) represents a mixed deployment state for O&G customers in which the IW1500 LAP and the IW6300 LAP co-existence. The IW6300 LAP infrastructure reports to WLC5520 (verified with release 8.10.109.39) or Cat9800 (verified with release 17.1.1s); IW1552 reports to WLC3504 (verified with release 8.5.141.109).

Two combinations are shown below:

- WLC3504 primary and back pair inter-connect with WLC5520 primary and back pair with mobility tunnel
- WLC3504 primary and back pair inter-connect with C9800 WLC primary and back pair with mobility tunnel

Where WLC3504 is used to register and manage IW1552H LAP, WLC5520, or C9800; the WLC is used to register and manage IW6300 LAP.

## WLC Configurations

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:

- The WLC3504 (release 8.5) HA pair inter-connect with the WLC5520 (release 8.10) HA pair.

### 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.

## Detailed Configuration of the Deployment Models

Show commands:

### 3504:

```
(Cisco Controller) >show mobility summary
(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
  d4:e8:80:b2:d7:4b  10.5.1.51      Up          default
  0.0.0.0          Control and Data Path Down

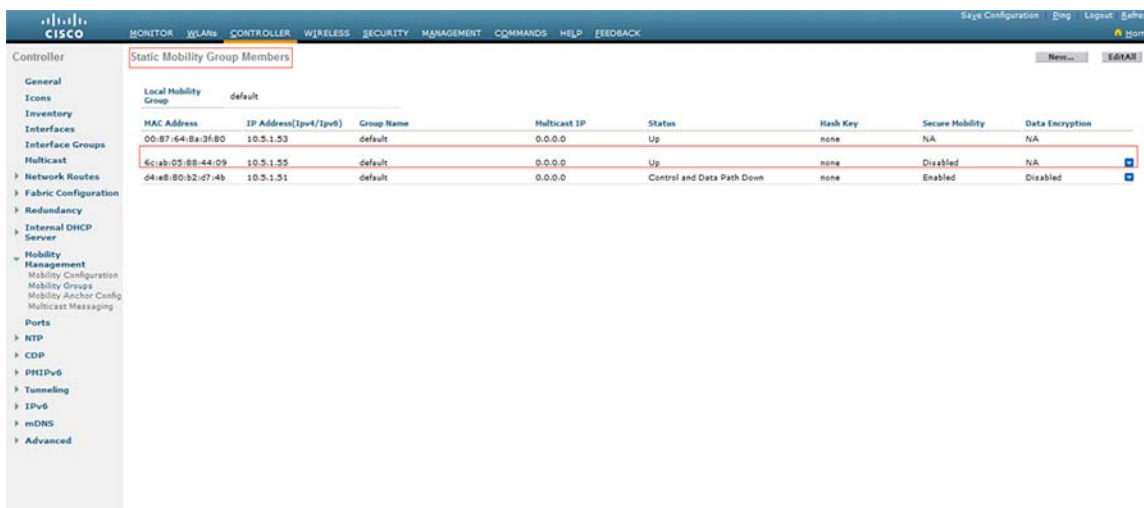
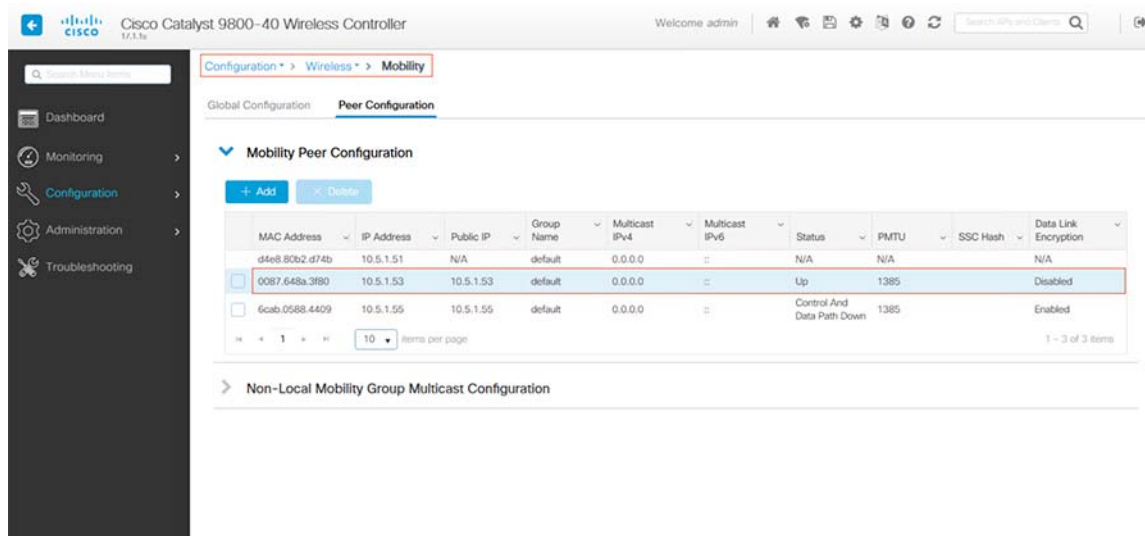
(Cisco Controller) >
```

### 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
  d4:e8:80:b2:d7:4b  10.5.1.51      Up          default
  0.0.0.0          Control and Data Path Down

(Cisco Controller) >?
```

**Figure 66 WLC3504 Mobility Group Configuration****Figure 67 Catalyst 9800 Mobility Group Configuration**

### Bridge Group Name (BGN)

Brownfield mixed mesh deployment requires several technologies to be enabled to register and manage IW1552H LAP clusters and IW6300 LAP clusters. This includes: Bridge Group Name (BGN) and DHCP option 43 and option 60 described previously.

### BGN

BGN provides a logical grouping mechanism for preventing two mesh networks on the same channel to communicate with each other, where, IW1552H 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:

## Detailed Configuration of the Deployment Models

- 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 mins, break the connection and scan again.

Given the separate BGN groups segmenting between IW1552H RAP extended cluster with IW6300 RAP extended cluster, each IW1552H 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.

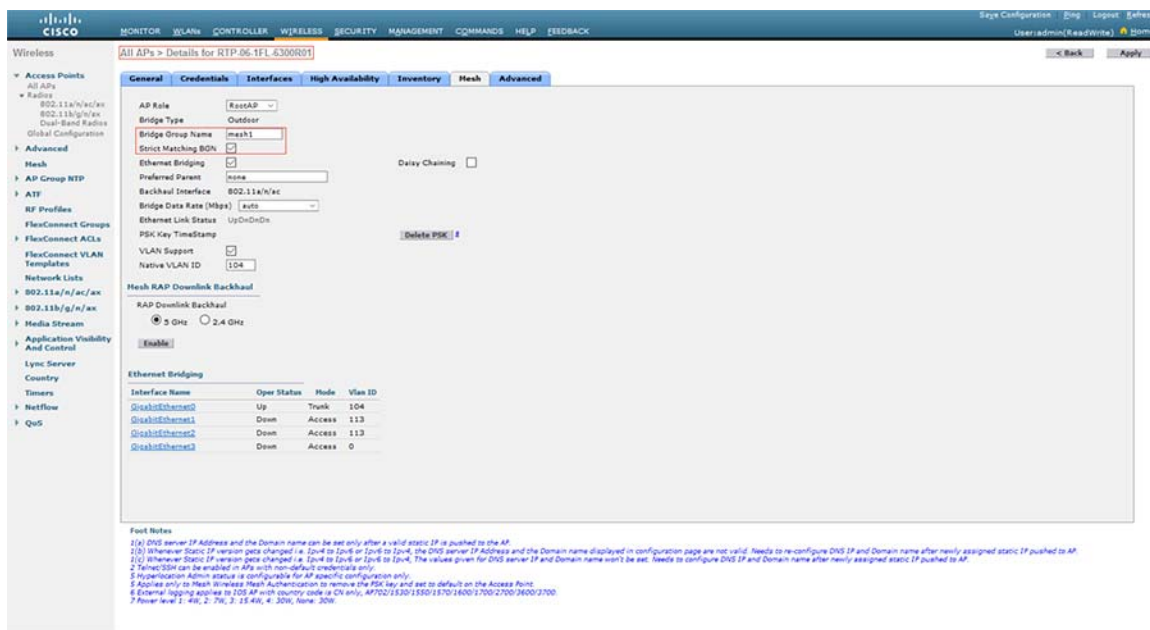
Two types of extended MESH clusters segmented by unique BGN are described below:

- 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 BGP
- 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.

**Figure 68 6300 RAP Bridge Group Name Configuration**



## Detailed Configuration of the Deployment Models

Figure 69 6300 MAP Bridge Group Name Configuration

Wireless

All APs > Details for RTP-06-1FL-6300M02

General Credentials Interfaces High Availability Inventory Mesh Advanced

AP Role: MeshAP

Bridge Type: Outdoor

Bridge Group Name: mesh2

Strict Matching BDN: ☒

Ethernet Bridging: ☒ Daisy Chaining: ☐

Preferred Parent: none

Backhaul Interface: 802.11a/n/ac

Bridge Data Rate (Mbps): auto

Ethernet Link Status: Up/Down/Up

PSK Key TimeStamp: [Delete PSK]

VLAN Support: ☒

Native VLAN ID: 104

Mesh RAP Downlink Backhaul

RAP Downlink Backhaul: ☒ 5 GHz ☐ 2.4 GHz

Ethernet Bridging

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

Foot Notes

1) (a) DNS server IP Address and the Domain name can be set only after a valid static IP is pushed to the AP.  
 1(b) Whenever Static IP version gets changed i.e. 1p-v4 to 1p-v6 or 1p-v6 to 1p-v4, 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.  
 2) Whenever Static IP version gets changed i.e. 1p-v4 to 1p-v6 or 1p-v6 to 1p-v4, 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.  
 3) Telnet/SSH can be enabled in APs with non-default credentials only.  
 4) External logging applies to 1552 AP with country code is CN only. AP702/1550/1551/1570/1600/1700/2700/2800/2700.  
 5) Applies only to Mesh Wireless Mesh Authentication to remove the PSK key and set to default on the Access Point.  
 6) External logging applies to 1552 AP with country code is CN only. AP702/1550/1551/1570/1600/1700/2700/2800/2700.  
 7) Power level: 1: 40, 2: 70, 3: 15-40, 4: 200, Name: 200.

Figure 70 1552 RAP Bridge Group Name Configuration

Wireless

All APs > Details for RTP-06-1FL-1552

General Credentials Interfaces High Availability Inventory Mesh Advanced

AP Role: RootAP

Bridge Type: Outdoor

Bridge Group Name: mesh2

Strict Matching BDN: ☒

Ethernet Bridging: ☒

Preferred Parent: none

Backhaul Interface: 802.11a/n

Bridge Data Rate (Mbps): auto

Ethernet Link Status: Up/Down/Up

PSK Key TimeStamp: [Delete PSK]

VLAN Support: ☒

Native VLAN ID: 104

Mesh RAP Downlink Backhaul

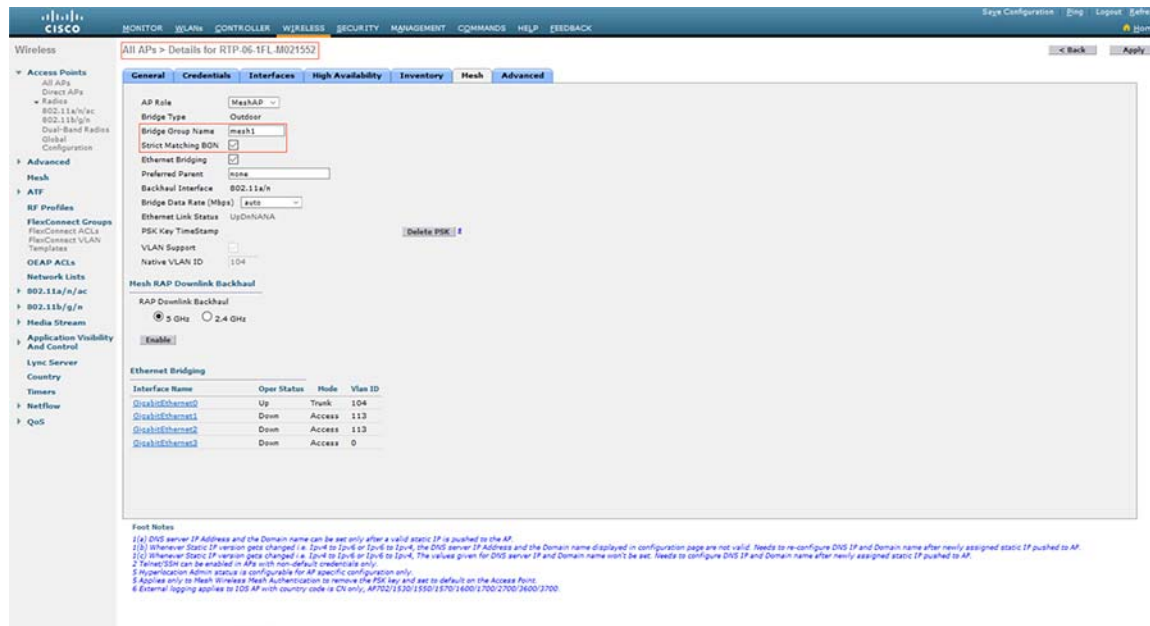
RAP Downlink Backhaul: ☒ 5 GHz ☐ 2.4 GHz

Ethernet Bridging

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

Foot Notes

1(a) DNS server IP Address and the Domain name can be set only after a valid static IP is pushed to the AP.  
 1(b) Whenever Static IP version gets changed i.e. 1p-v4 to 1p-v6 or 1p-v6 to 1p-v4, 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.  
 2) Whenever Static IP version gets changed i.e. 1p-v4 to 1p-v6 or 1p-v6 to 1p-v4, 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.  
 3) Telnet/SSH can be enabled in APs with non-default credentials only.  
 4) External logging applies to 1552 AP with country code is CN only. AP702/1550/1551/1570/1600/1700/2700/2800/2700.  
 5) Hyperoperation Admin status is configurable for AP specific configuration 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 1552 AP with country code is CN only. AP702/1550/1551/1570/1600/1700/2700/2800/2700.

**Figure 71 1552 MAP Bridge Group Name Configuration**

## Mesh Configurations

General MESH WLAN employs outdoor mesh access points (APs: IW1552 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 downlink backhaul, 2.4Ghz radio will used for client access, convergence mode will be configured with “VERYFAST” with Channel Change Notification (CCN) and background Scanning enabled for fast convergence.

### Configuration Steps

#### 3504 and 5520:

1. For configuring MESH got to WLC UI Wireless, select each **AP > MESH**.
2. Assign AP Role, Bridge Group Name, select Strict Matching BGN (option), 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

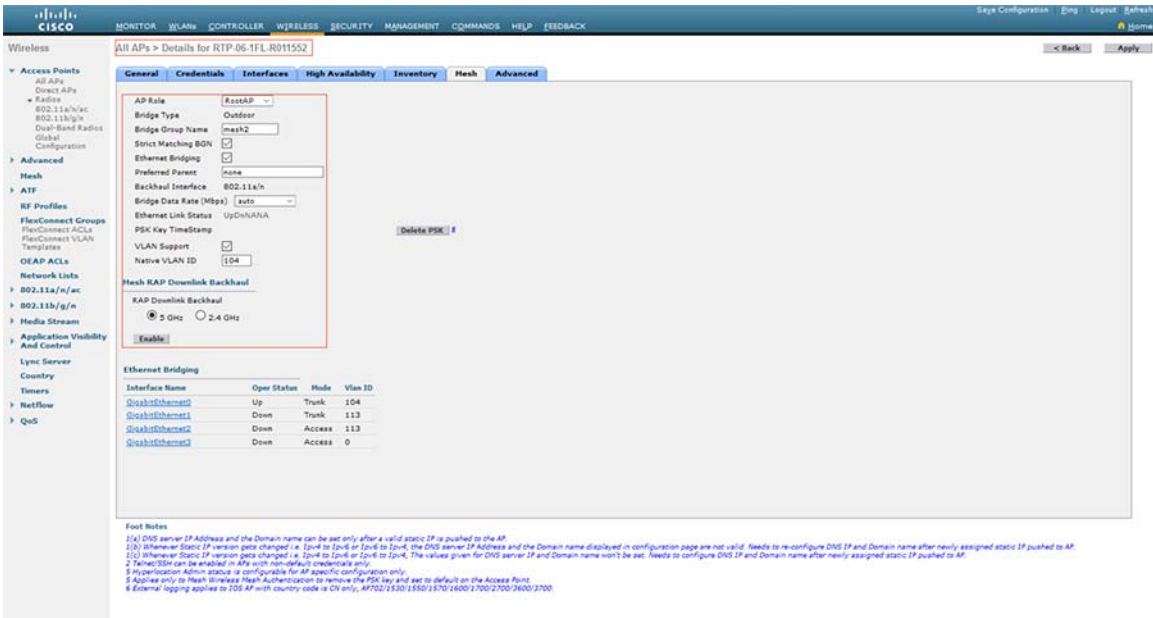
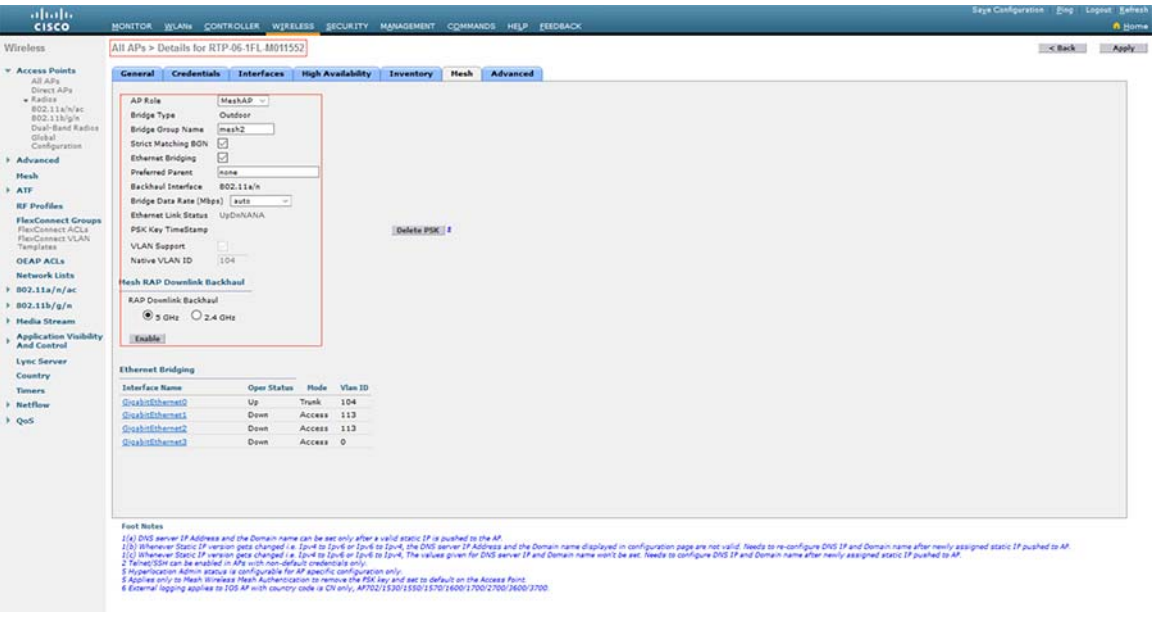


Figure 73 1552 MAP MESH Configuration





**Figure 74 6300 RAP MESH Configuration**

The screenshot shows the Cisco Wireless LAN Controller configuration interface for a 6300 RAP MESH. The 'Mesh' tab is active, displaying the following configuration:

- AP Rule:** MeshAP
- Bridge Type:** Outdoor
- Bridge Group Name:** mesh1
- Strict Matching BDN:** ☒
- Ethernet Bridging:** ☒
- Preferred Parent:** none
- Backhaul Interface:** 802.11a/n/ac
- Bridge Data Rate (Mbps):** auto
- Ethernet Link Status:** Up/Dn/Dn
- PSK Key TimeStamp:** ☐
- VLAN Support:** ☒
- Native VLAN ID:** 104
- Mesh RAP Downlink Backhaul:**
  - RAP Downlink Backhaul:** ☒ 5 GHz ☐ 2.4 GHz
  - Enable:** ☒

**Ethernet Bridging Table:**

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) 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.
- 5) Hyperoperation Admin status is configurable for AP specific configuration only.
- 6) Hyperoperation Admin status is configurable for AP specific configuration only.
- 7) External logging applies to IOS AP with country code is CH only. AP702/1530/1550/1570/1600/1700/2700/2800/3700.
- 8) Power level 1: 40, 2: 70, 3: 15-40, 4: 30, None: 200.

**Figure 75 6300 MAP MESH Configuration**

The screenshot shows the Cisco Wireless LAN Controller configuration interface for a 6300 MAP MESH. The 'Mesh' tab is active, displaying the following configuration:

- AP Rule:** MeshAP
- Bridge Type:** Outdoor
- Bridge Group Name:** mesh2
- Strict Matching BDN:** ☒
- Ethernet Bridging:** ☒
- Preferred Parent:** none
- Backhaul Interface:** 802.11a/n/ac
- Bridge Data Rate (Mbps):** auto
- Ethernet Link Status:** Up/Dn/Up
- PSK Key TimeStamp:** ☐
- VLAN Support:** ☒
- Native VLAN ID:** 104
- Mesh RAP Downlink Backhaul:**
  - RAP Downlink Backhaul:** ☒ 5 GHz ☐ 2.4 GHz
  - Enable:** ☒

**Ethernet Bridging Table:**

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

**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) 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.
- 5) Hyperoperation Admin status is configurable for AP specific configuration only.
- 6) Hyperoperation Admin status is configurable for AP specific configuration only.
- 7) External logging applies to IOS AP with country code is CH only. AP702/1530/1550/1570/1600/1700/2700/2800/3700.
- 8) Power level 1: 40, 2: 70, 3: 15-40, 4: 30, None: 200.

**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.

## 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.



Detailed Configuration of the Deployment Models

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.

Figure 76 3504 MAC Filter Configuration

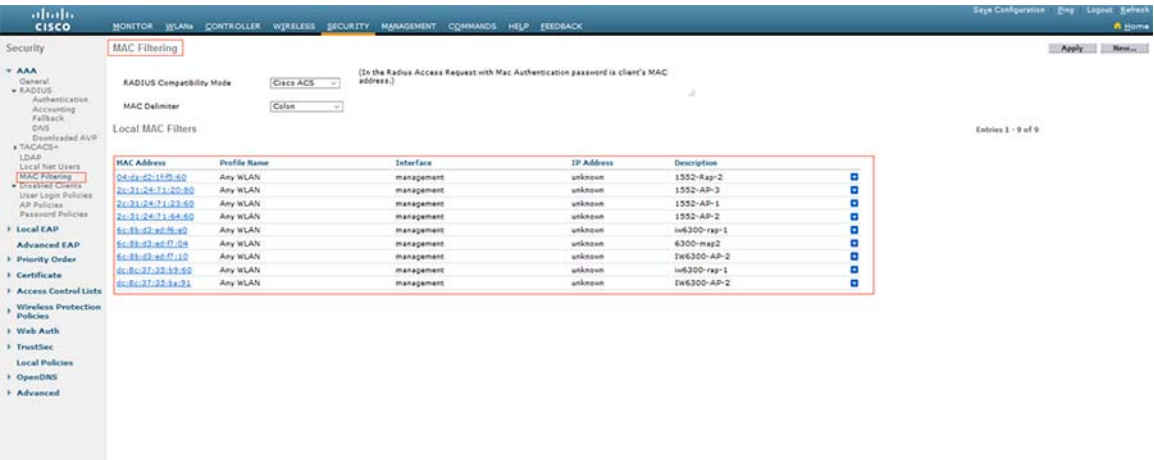
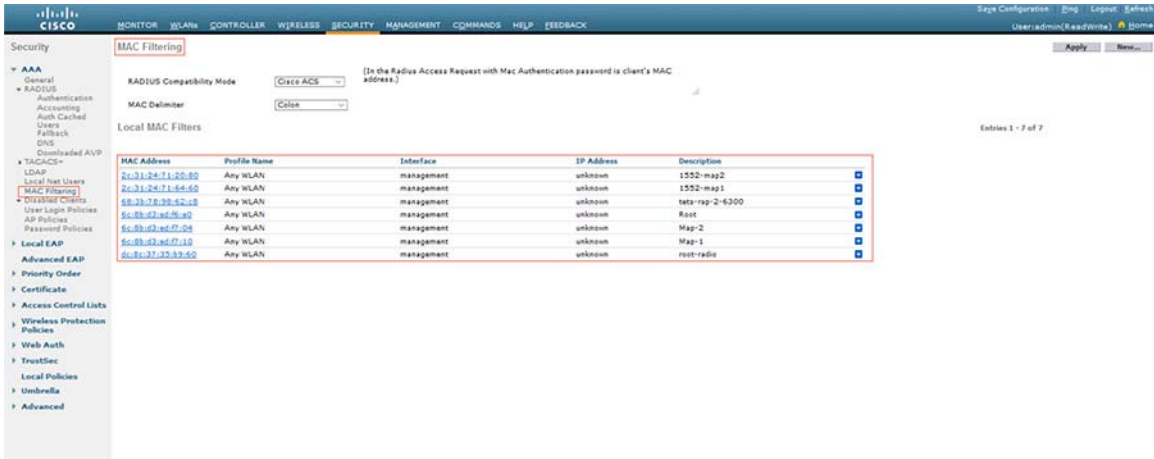


Figure 77 5520 MAC Filter Configuration



WLAN Configuration

O&G MESH WLAN infrastructure deployment follows Cisco Wireless MESH Design & Deployment Guide, Release 8.6 ([https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-6/b\\_mesh\\_86/Site\\_Preparation\\_and\\_Planning.html](https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-6/b_mesh_86/Site_Preparation_and_Planning.html)), with the following snapshots to show a detailed deployment examples for controller and WLAN respectively.

3504:

Figure 78 3504 WLC Controller Interface Configuration

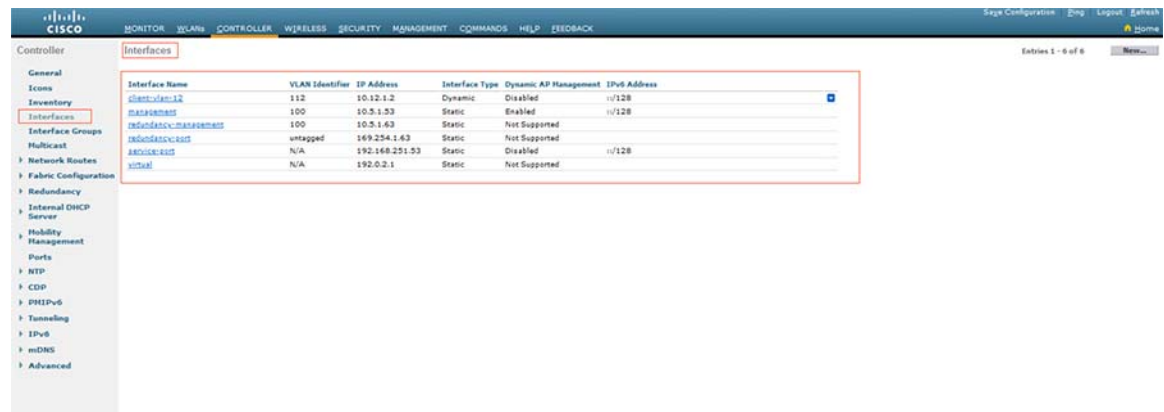
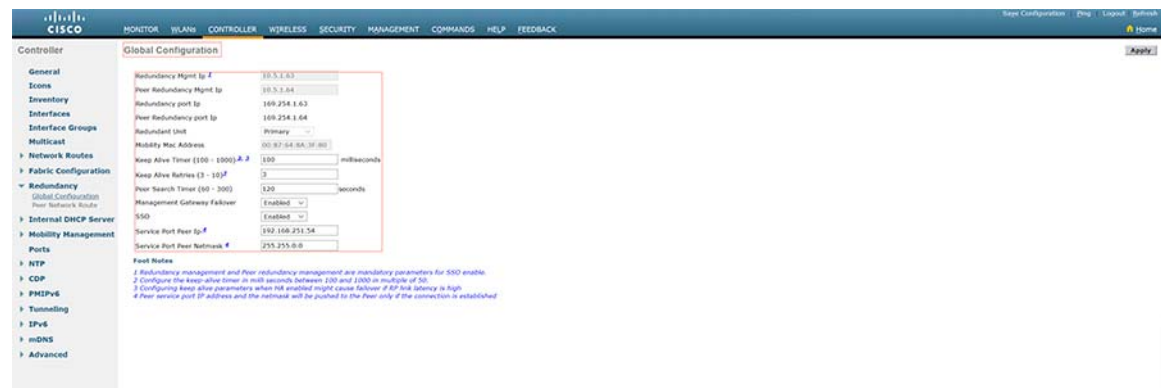


Figure 79 3504 WLC Controller Management Interface Configuration



Detailed Configuration of the Deployment Models

Figure 80 3504 WLC Controller Dynamic Interface Configuration

MONITORWLANCONTROLLERWIRELESSSECURITYMANAGEMENTCOMMANDSHelpFEEDBACK

Save ConfigurationPingLogoutRefresh

Controller

Interfaces > Edit

General

Icons

Inventory

Interfaces

Interface Groups

Multicast

Network Routes

Fabric Configuration

Redundancy

Internal DHCP Server

Mobility Management

Ports

NTP

CDP

PREIPv6

Tunneling

IPv6

mDNS

Advanced

General Information

Configuration

Physical Information

Interface Address

DHCP Information

Access Control List

mDNS

External Module

Interface Name

MAC Address

Configuration

Guest Lan

Quarantine

Quarantine Vlan Id

NAS-ID

Physical Information

Port Number

Backup Port

Active Port

Enable Dynamic AP Management

Interface Address

VLAN Identifier

IP Address

Netmask

Gateway

IPv6 Address

Prefix Length

IPv6 Gateway

Link Local IPv6 Address

DHCP Information

Primary DHCP Server

Secondary DHCP Server

DHCP Proxy Mode

Enable DHCP Option 82

Enable DHCP Option 6

OpenDNS

Access Control List

ACL Name

URL ACL

mDNS

mDNS Profile

External Module

3G VLAN

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and this may result in loss of connectivity for some clients.

5520:

Figure 81 5520 WLC Controller Interface Configuration

MONITORWLANCONTROLLERWIRELESSSECURITYMANAGEMENTCOMMANDSHelpFEEDBACK

Save ConfigurationPingLogoutRefresh

Controller

Interfaces

General

Icons

Inventory

Interfaces

Interface Groups

Multicast

Network Routes

Fabric Configuration

Redundancy

Mobility Management

Ports

NTP

CDP

PREIPv6

Tunneling

IPv6

mDNS

Advanced

Lawful Interception

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
client-vlan-112	112	10.12.1.3	Dynamic	Disabled	11/128
management	100	10.5.1.55	Static	Enabled	11/128
redundancy-management	100	10.5.1.65	Static	Not Supported	
redundancy-8021	untagged	169.254.1.65	Static	Not Supported	
8021a-8021	N/A	192.168.251.55	Static	Disabled	11/128
virtual	N/A	192.0.2.1	Static	Not Supported	

## Detailed Configuration of the Deployment Models

**Figure 82 5520 WLC Controller Management Interface Configuration**

Controller

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Save Configuration Log Logout Refresh

User: admin(Read/Write) Home

Controller

Interfaces > Edit

General Information

Interface Name management

MAC Address 6c:ab:05:88:44:09

Note: Changing Management interface attributes are not allowed when Redundancy mode(SSO) is enabled

Configuration

Quarantine ☐

Quarantine Vlan Id 0

NAT Address

Enable NAT Address ☐

Interface Address

VLAN Identifier 100

IP Address 10.5.1.35

Netmask 255.255.255.0

Gateway 10.5.1.1

IPv6 Address None

Prefix Length 128

IPv6 Gateway None

Link Local IPv6 Address fe80::6aeb:3f:fe8b:440a::64

Physical Information

Port Number 1

Backup Port 0

Active Port 1

Enable Dynamic AP Management ☒

DHCP Information

Primary DHCP Server 10.5.1.20

Secondary DHCP Server 0.0.0.0

DHCP Proxy Mode Enabled

Enable DHCP Option 82 ☐

Enable DHCP Option 6 OpenDNS ☐

Access Control List

ACL Name none

URL ACL none

IPv6 ACL Name none

mDNS

mDNS Profile none

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

**Figure 83 5520 WLC Controller Dynamic Interface Configuration**

Controller

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Save Configuration Log Logout Refresh

User: admin(Read/Write) Home

Controller

Interfaces > Edit

General Information

Interface Name client-vlan-112

MAC Address 6c:ab:05:88:44:09

Configuration

Guest Lan ☐

Quarantine ☐

Quarantine Vlan Id 0

NAS-ID none

Physical Information

Port Number 3

Backup Port 2

Active Port 1

Enable Dynamic AP Management ☐

Interface Address

VLAN Identifier 112

IP Address 10.12.1.3

Netmask 255.255.255.0

Gateway 10.12.1.1

IPv6 Address None

Prefix Length 128

IPv6 Gateway None

Link Local IPv6 Address fe80::6aeb:3f:fe8b:440a::64

DHCP Information

Primary DHCP Server 10.5.1.20

Secondary DHCP Server None

DHCP Proxy Mode Enabled

Enable DHCP Option 82 ☐

Enable DHCP Option 6 OpenDNS ☐

Access Control List

ACL Name none

URL ACL none

mDNS

mDNS Profile none

External Module

3G VLAN ☐

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

MONITOR
WLANS
POLYMER
SECURITY
MANAGEMENT
COMMANDS
HELP
FEEDBACK

WLANS

WLANS

Advanced

WLANS > Edit "OG-SSID-1"

General
Security
QoS
Policy-Mapping
Advanced

Profile Name
OG-SSID-1

Type
WLAN

SSID
OG-SSID-1

Status
☒ Enabled

Security Policies
[WPA2][Auth(PSK)][Auth(FT PSK)]  
(Modifications done under security tab will appear after applying the changes.)

Radio Policy
All

Interface/Interface Group
client-wlan-12

Multicast Vlan Feature
☐ Enabled

Broadcast SSID
☒ Enabled

NAS-ID
none

Foot Notes

- Web Policy cannot be used in combination with P80s.
- FlacConnect Local Switching is not supported with Override Interface ACLs.
- When FlacConnect Local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS.
- When FlacConnect Local authentication is disabled, AP on connected mode will use RADIUS as NAS and AP as NAS while in standalone mode.
- When client exclusion is enabled, a Timeout value of zero means infinity (will require administrative override to reset excluded clients).
- Client WPA is not active unless WPA2 is configured.
- Learn Client IP is configurable only when FlacConnect Local Switching is enabled.
- WPA and open or AES are mutually exclusive. WPA2 is supported in all cases.
- Value zero implies there is no restriction on maximum clients allowed.
- MAC Filtering is not supported with FlacConnect Local authentication.
- MAC Filtering should be disabled.
- Guest-tunneling, Local switching, DHCP Relay should be disabled.
- Non-associated-client feature and Central Access feature are not supported with FlacConnect Local authentication.
- LAN based central switching is not supported with FlacConnect Local authentication.
- Enabling dot1x mode will prevent clients from deriving broadcast and multicast packets.
- Fast Transition is supported with WPA2 and open security policy.
- Override Bandwidth Contracts parameters are specific to per-Radio of AP. A value of zero (0) indicates that the value specified in the selected QoS profile will take effect.
- When Diagnostic Channel is enabled, TCP Blocking Action will be assigned to Drop Action.
- Port should be disabled before configuring RADIUS or CoS or PPS.
- This configuration override only Web Authentication Type and External Webauth URL. Radmact URL on global config always override the URL on each WLAN. Keep the configuration on global blank if you need per WLAN redirect.

The screenshot shows the Cisco IOS configuration interface for WLANs. The top navigation bar includes 'Cisco', 'MONITOR', 'LWANS', 'PORTAL', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The main title is 'WLANs > Edit "OG-SSID-1"'. The left sidebar shows 'WLANs' and 'Advanced'. The main content area is titled 'Layer 2 Layer 3 AAA Servers' and has tabs for 'General', 'Security', 'QoS', 'Policy-Mapping', and 'Advanced'. The 'Security' tab is selected, showing 'Layer 2 Security 1' with a dropdown menu set to 'WPA+WPA2'. Below this, there are several configuration options: 'MAC Filtering' (disabled), 'Fast Transition' (disabled), 'Fast Transition Over the DS' (disabled), 'Reassociation Timeout' (20 seconds), 'Protected Management Frame' (disabled), 'PMF' (disabled), 'WPA+WPA2 Parameters' (WPA Policy, WPA2 Policy, WPA2 Encryption, and OSSEN Policy), and 'Authentication Key Management' (set to '802.11'). The bottom section contains 'Foot Notes' with 20 numbered items providing detailed information about the configuration options.

**Layer 2 Security 1** (WPA+WPA2)

MAC Filtering ☐

Fast Transition ☐ (Enable)

Fast Transition Over the DS ☐ (20) Seconds

Protected Management Frame ☐ (Disabled)

PMF ☐ (Disabled)

WPA+WPA2 Parameters

WPA Policy ☐

WPA2 Policy ☐

WPA2 Encryption ☒ AES ☐ TKIP ☐ CCMP256 ☐ CCMP128 ☐ CCMP256

OSSEN Policy ☐

Authentication Key Management ☒ 802.11

**Foot Notes**

- Web Policy cannot be used in combination with PMF.
- PMF (Protected Management Frame) is not supported with Override Interface ACLs.
- When FastConnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS.
- When FastConnect local authentication is disabled, AP on connected mode will use BGC as NAS and AP as NAS with its on-standalone mode.
- When client exclusion is enabled, Timeout value of zero means infinity (will require administrative override to re-add excluded clients).
- Client MPF is not active unless WPA2 is configured.
- Guest Client IP is configurable only when FastConnect Local Switching is enabled.
- WPA2 and open or AES security should be enabled to support higher 11n rates.
- Value zero implies there is no restriction on maximum clients allowed.
- NAC Filtering is not supported with FastConnect Local authentication.
- NAC Filtering should be enabled.
- Guest tunneling, Local switching, DHCP Required should be disabled.
- Non-associated Client Feature and Central Access Feature are not supported with FastConnect Local Authentication.
- WLAN based central switching is not supported with FastConnect Local Authentication.
- Enabling gsm-standalone will prevent clients from deauthenticating immediately and multi-run policies.
- Fast Transition is supported with WPA2 and open security policy.
- Override Bandwidth Constraints parameters are specific to per Radio of AP. A value of zero (0) indicates that the value specified in the selected QoS profile will take effect.
- When Diagnostic Channel is enabled, P2P Blocking Action will be assigned to Drop Action.
- PMF should be disabled before configuring 802.11n or CCMP or PMF.
- This configuration override only Web Authentication Type and External WPAauth URL. Redirect URL on global config always override the URL on each WLAN. Keep the configuration on global blank if you need per WLAN redirect.

Detailed Configuration of the Deployment Models

Figure 86 5520 WLAN Configuration

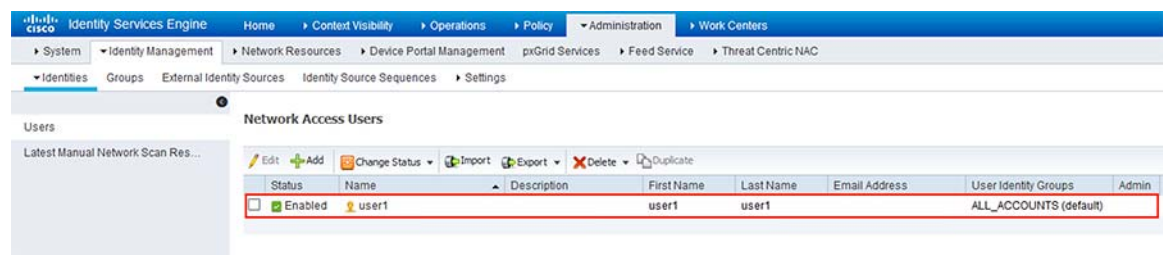
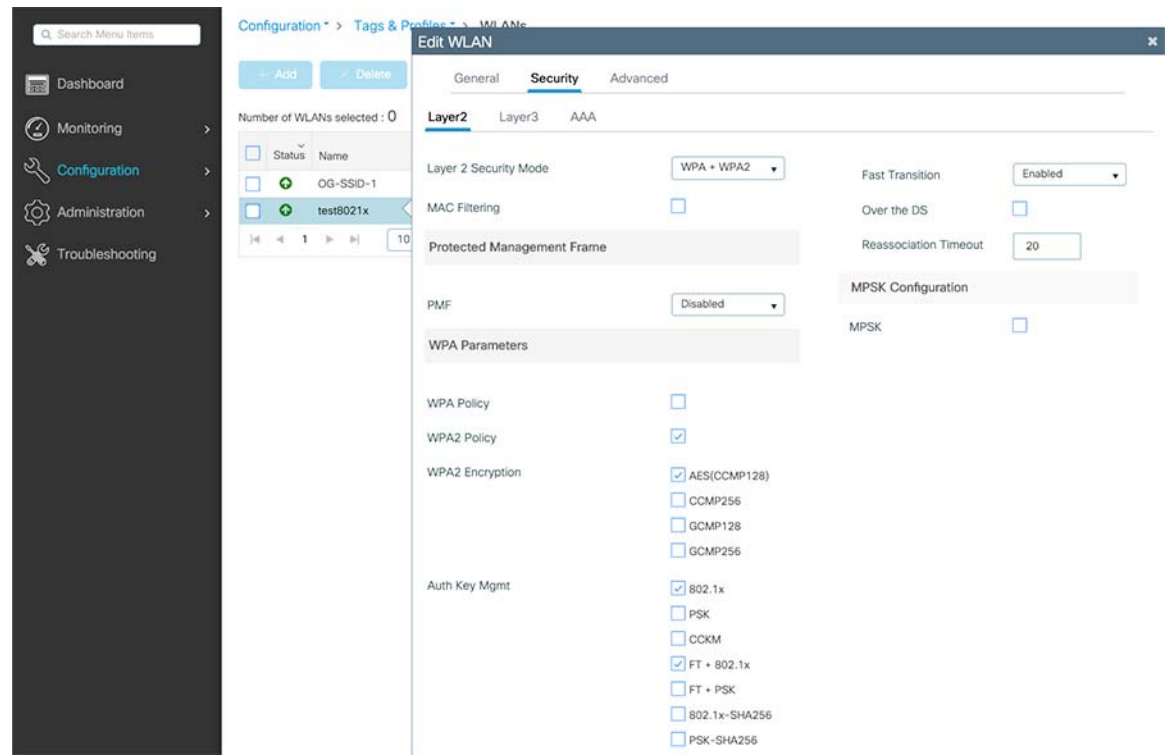


Figure 87 5520 WLAN Security Configuration



HA SSO on 3504 HA Pair and 5520 HA Pair

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.

Detailed Configuration of the Deployment Models

Configuration Steps

3504:

Figure 88 3504 WLC Controller Redundant Management Interface Configuration

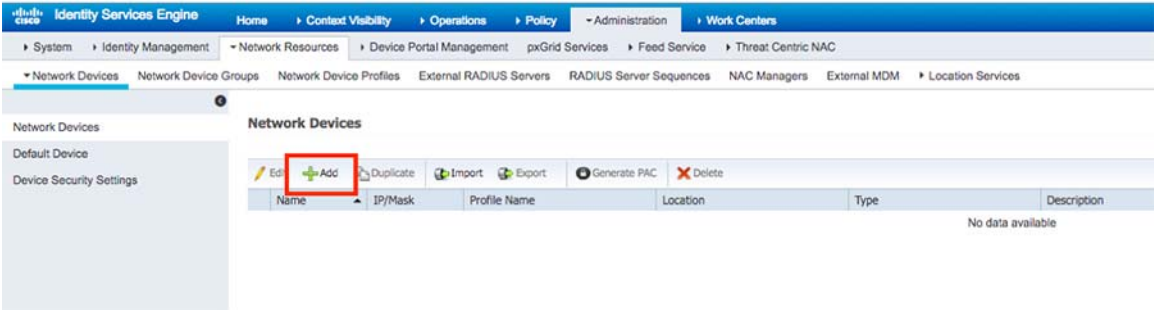
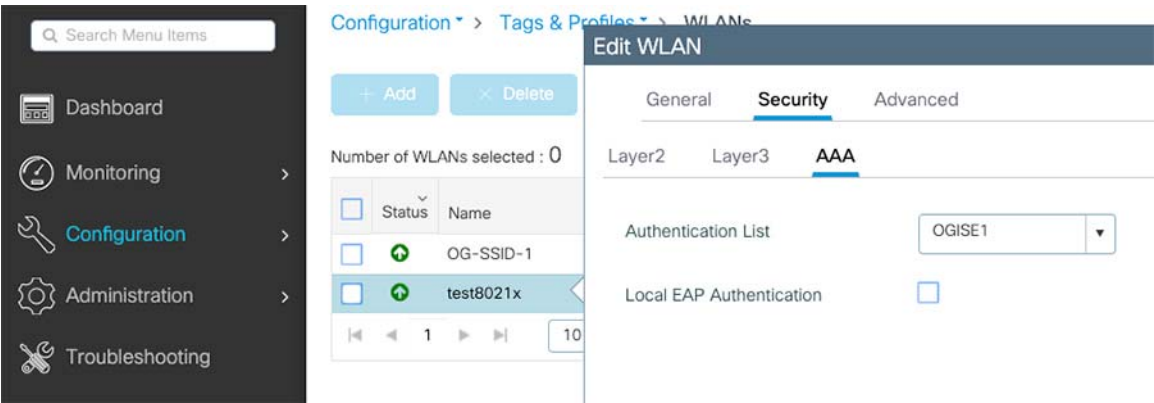


Figure 89 3504 WLC Controller Redundant Global Configuration



5520:

**Figure 90 5520 WLC Controller Redundant Management Interface Configuration**

Network Devices List > New Network Device

Network Devices

\* Name **IA-OG-5520-WLC-1**

Description

IP Address \* IP: **10.5.1.55** / 32

\* Device Profile **Cisco**

Model Name

Software Version

\* Network Device Group

Location **All Locations** Set To Default

IPSEC **Is IPSEC Device** Set To Default

Device Type **All Device Types** Set To Default

☒ **RADIUS Authentication Settings**

RADIUS UDP Settings

Protocol **RADIUS**

\* Shared Secret **\*\*\*\*\*** Show

Use Second Shared Secret ☐ Show

CoA Port **1700** Set To Default

RADIUS DTLS Settings

DTLS Required ☐ Show

Shared Secret **radius/dtls** Show

CoA Port **2083** Set To Default

Issuer CA of ISE Certificates for CoA **Select if required (optional)** Show

DNS Name

General Settings

Enable KeyWrap ☐ Show

\* Key Encryption Key **\*\*\*\*\*** Show

\* Message Authenticator Code Key **\*\*\*\*\*** Show

Key Input Format **ASCII** HEXADECIMAL

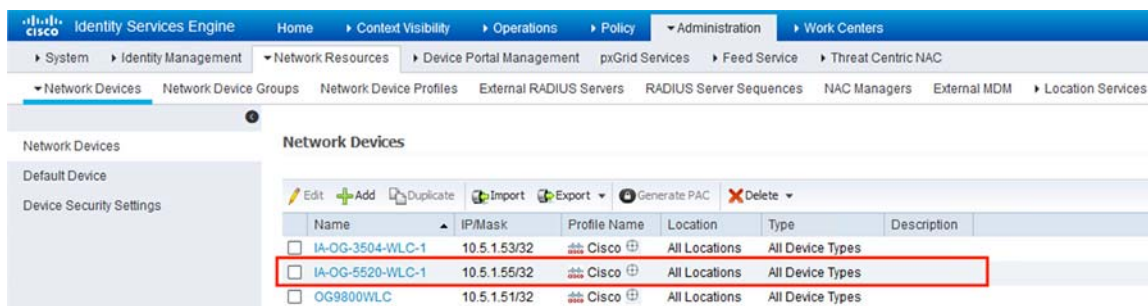
☐ TACACS Authentication Settings

☐ SNMP Settings

☐ Advanced TrustSec Settings

Submit Cancel



**Figure 91 5520 WLC Controller Redundant Global Configuration**

## 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
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..... 17 days 0 hrs 29 mins 37 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..... +61 C
Mgig Temp Alarm Limits..... -10 to 78 C
Mgig Temperature..... +50 C
External Temp Alarm Limits..... -10 to 71 C
External Temperature..... +44 C
Fan Status..... OK
Fan Speed Mode..... Disable

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

OUI Classification Failure Count..... 5
```

## Detailed Configuration of the Deployment Models

```

Memory Current Usage..... 35
Memory Average Usage..... 35
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) >

(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
Average Redundancy Peer Reachability Latency = 161 Micro Seconds
Average Management Gateway Reachability Latency = 472 Micro Seconds

```

(Cisco Controller) >

**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..... 4 days 4 hrs 19 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

```

## Detailed Configuration of the Deployment Models

```

Internal Temperature..... +21 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..... 3

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) >

(Cisco Controller) >show redundancy summary
    Redundancy Mode = SSO ENABLED
        Local State = ACTIVE
        Peer State = STANDBY HOT
        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 = 232 Micro Seconds
    Average Management Gateway Reachability Latency = 424 Micro Seconds
(Cisco Controller) >

```

## 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, page 87](#), refer to the use cases in this document.

## Detailed Configuration of the Deployment Models

3504:

Figure 92 1552 MAP Ethernet Bridging Configuration

The screenshot shows the Cisco Wireless LAN Controller configuration page for the AP 'RTP-06-1FL-M011552'. The 'Advanced' tab is selected, and the 'Ethernet Bridging' section is highlighted with a red box. The table below shows the configuration for the Ethernet Bridging interfaces:

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(a) DNS server IP Address and the Domain name can be set only after a valid static IP is pushed to the AP.
- 1(b) 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.
- 1(c) 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.
- 2 TunnelSSH can be enabled in APs with non-default credentials only.
- 3 Hyperlocation Admin status is configurable for AP specific configuration only.
- 4 Applies only to Mesh Wireless Mesh Authentication to remove the PSK key and set to default on the Access Point.
- 6 External logging applies to 105 AP with country code is CN only, AP702/1530/1550/1570/1600/1700/2700/3600/3700.

Figure 93 1552 RAP Ethernet Bridging Configuration

The screenshot shows the Cisco Wireless LAN Controller configuration page for the AP 'RTP-06-1FL-R011552'. The 'Advanced' tab is selected, and the 'Ethernet Bridging' section is highlighted with a red box. The table below shows the configuration for the Ethernet Bridging interfaces:

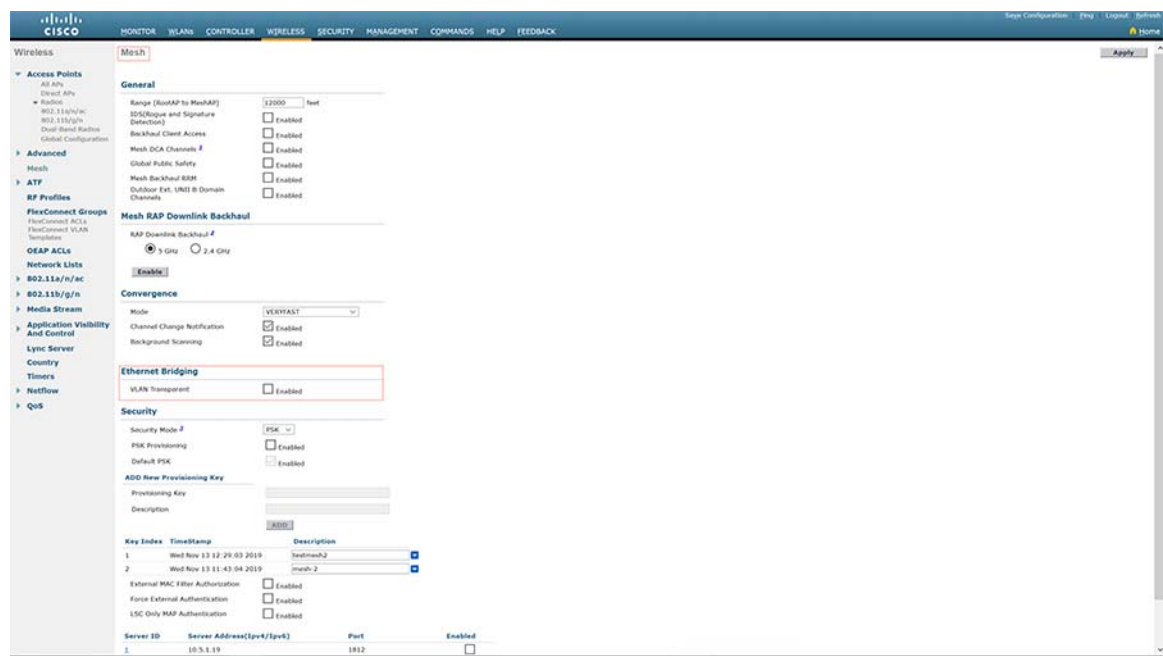
Interface Name	Oper Status	Mode	Vlan ID
GigabitEthernet0	Up	Trunk	104
GigabitEthernet1	Down	Trunk	113
GigabitEthernet2	Down	Access	113
GigabitEthernet3	Down	Access	0

Foot Notes:

- 1(a) DNS server IP Address and the Domain name can be set only after a valid static IP is pushed to the AP.
- 1(b) 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.
- 1(c) 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.
- 2 TunnelSSH can be enabled in APs with non-default credentials only.
- 3 Hyperlocation Admin status is configurable for AP specific configuration only.
- 4 Applies only to Mesh Wireless Mesh Authentication to remove the PSK key and set to default on the Access Point.
- 6 External logging applies to 105 AP with country code is CN only, AP702/1530/1550/1570/1600/1700/2700/3600/3700.

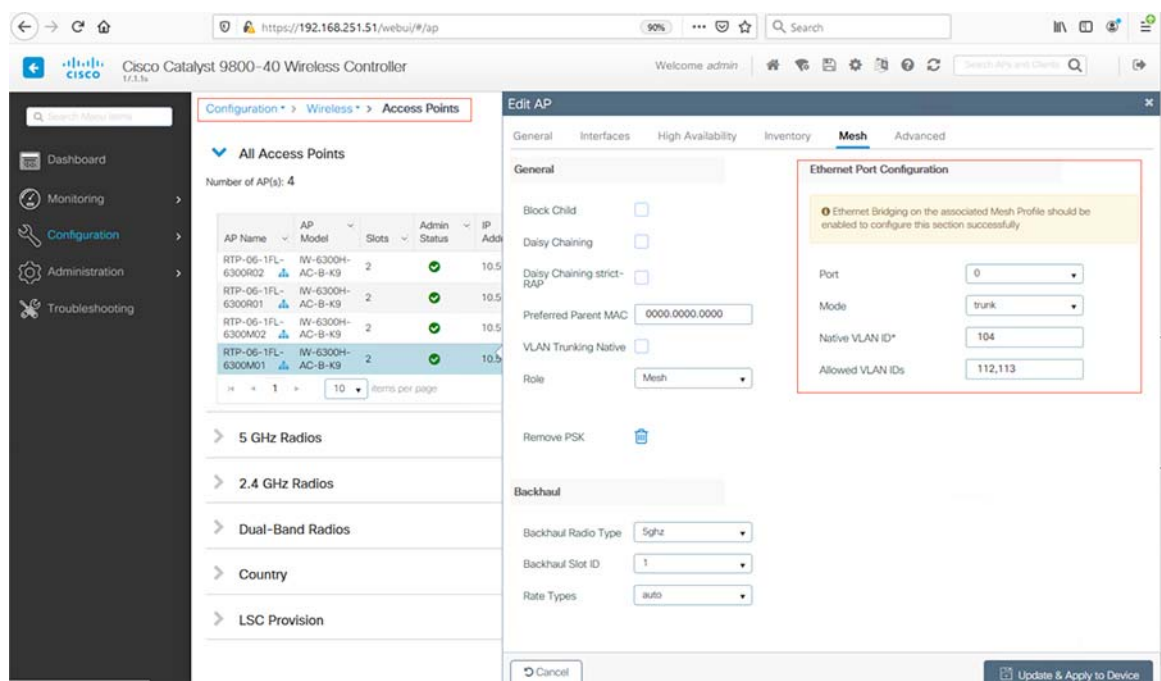
Detailed Configuration of the Deployment Models

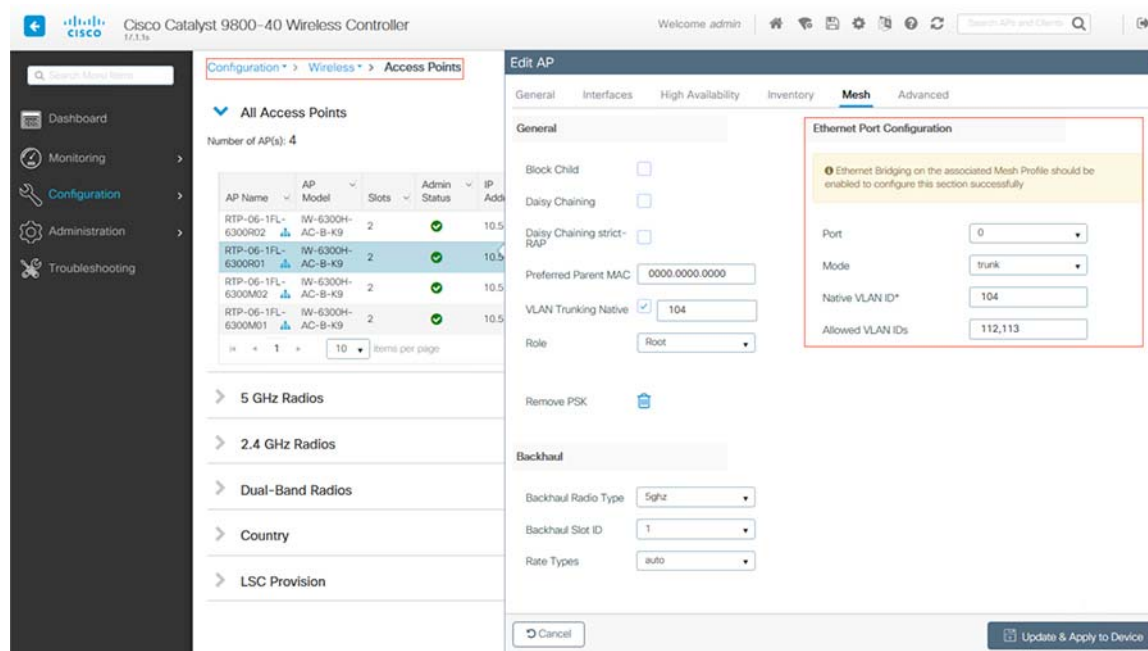
Figure 94 Wireless MESH Disable VLAN Transparency



5520:

Figure 95 6300 MAP Ethernet Bridging Configuration



**Figure 96 6300 RAP Ethernet Bridging Configuration**

## Wireless MESH Disable VLAN Transparency

- WLC3504 (release 8.5) HA pair inter-connect with Cat9800 (release 17.1.1s) HA pair scenario

### 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.

Show Commands:

### 3504:

```
(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			

Detailed Configuration of the Deployment Models

```
00:87:64:8a:3f:80 10.5.1.53 default
0.0.0.0 Up
d4:e8:80:b2:d7:4b 10.5.1.51 default
0.0.0.0 Up
```

17.1.1s:

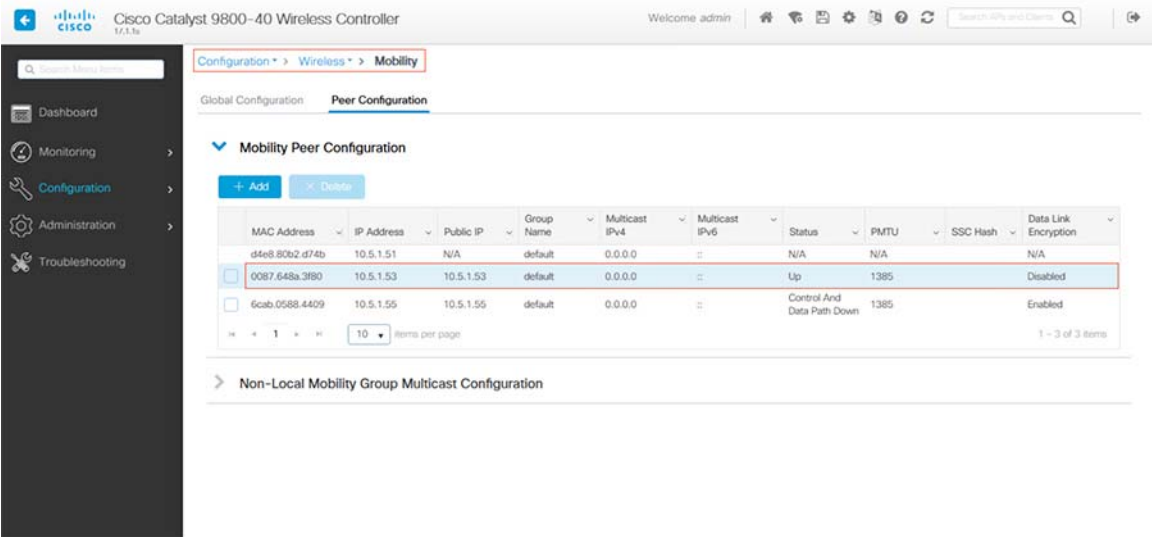
```
WLC#show wireless mobility summary
Mobility Summary
```

```
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			Public Ip		MAC Address
Group Name			Multicast IPv4	Multicast IPv6	
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			

Figure 97 Cat9800 Mobility Group Configuration



## WLC3504 Mobility Group Configuration

### MESH Backhaul Security (MAC Filter)

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

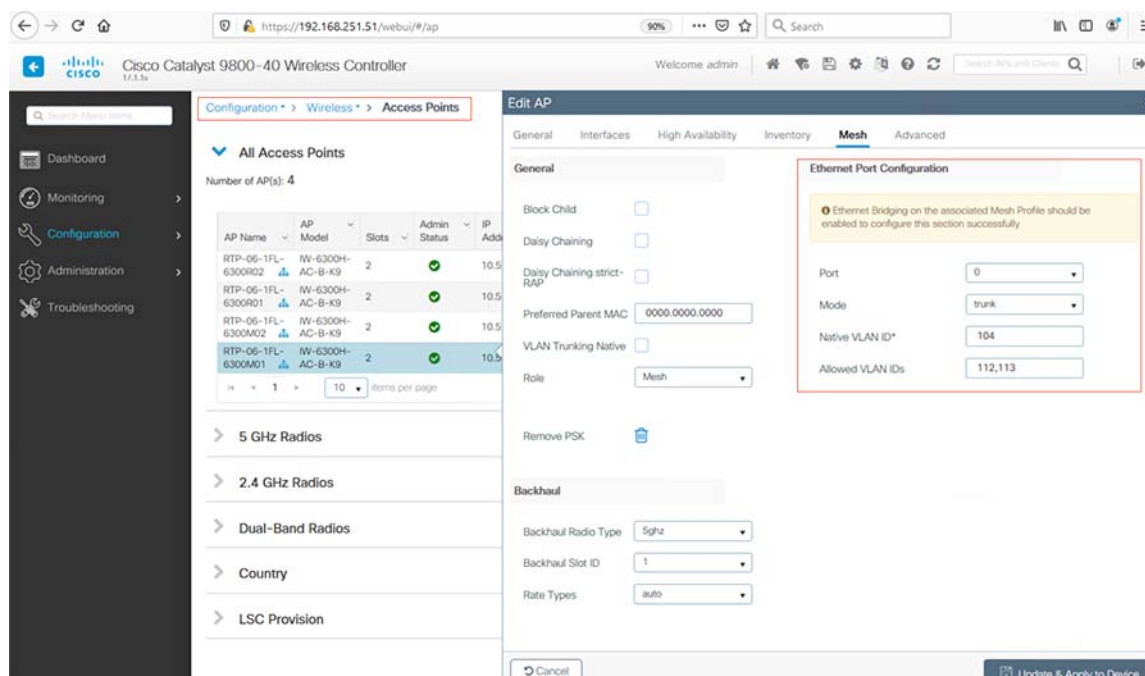
### Ethernet Bridging

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

```
IA-OG-C9300#sh arp | incl 113
Internet 10.13.1.1 - 0077.8d5f.8b7a ARPA Vlan113
Internet 10.13.1.11 181 0026.160c.9ae8 ARPA Vlan113
Internet 10.13.1.12 90 0026.160f.49a8 ARPA Vlan113
```

### Cat9800:

**Figure 98 6300 MAP Ethernet bridging Configuration**





Detailed Configuration of the Deployment Models

Figure 99 6300 RAP Ethernet Bridging Configuration

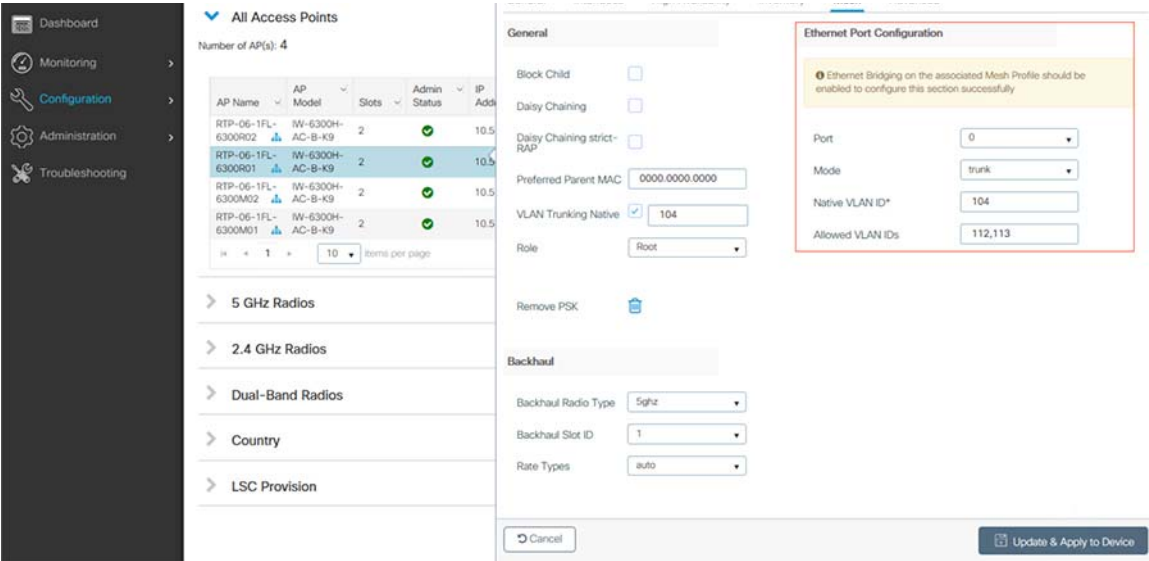
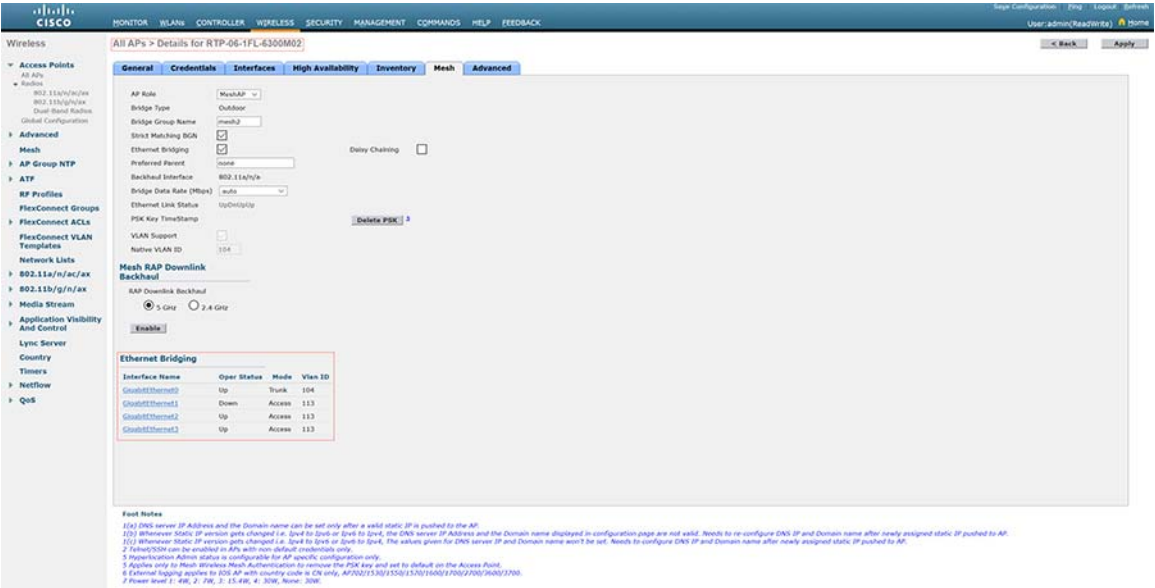


Figure 100 5520 6300 MESH Profile Disable Ethernet Bridging VLAN Transparency



## Detailed Configuration of the Deployment Models

3504:

Figure 101 1552 MAP Ethernet Bridging Configuration

Wireless > All APs > Details for RTP-06-1FL-M011552

General | Credentials | Interfaces | High Availability | Inventory | Mesh | Advanced

AP Role: MeshAP  
 Bridge Type: Outdoor  
 Bridge Group Name: mesh2  
 Strict Matching BGN: ☒  
 Ethernet Bridging: ☒  
 Preferred Parent: none  
 Backhaul Interface: 802.11a/n  
 Bridge Data Rate (Mbps): auto  
 Ethernet Link Status: Up/Dn/NANA  
 PSK Key Timestamp: [Delete PSK](#)  
 VLAN Support: ☒  
 Native VLAN ID: 104

Mesh RAP Downlink Backhaul  
 RAP Downlink Backhaul: ☒ 5 GHz ☐ 2.4 GHz  
 Enable:

Interface Name	Oper Status	Mode	Vlan ID
Gi0/0/100	Up	Trunk	104
Gi0/0/101	Down	Access	113
Gi0/0/102	Down	Access	113
Gi0/0/103	Down	Access	0

Foot Notes:  
 1(a) DNS server IP Address and the Domain name can be set only after a valid static IP is pushed to the AP.  
 1(b) 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.  
 1(c) 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.  
 2. TunnelSSH can be enabled in APs with non-default credentials only.  
 3. Hyperoperation Admin status is configurable for AP specific configuration only.  
 5. Applies only to Mesh Wireless Mesh Authentication to remove the PSK key and set to default on the Access Point.  
 6. External logging applies to IOS AP with country code is CH only. AP7502/1550/1570/1600/2700/2700/2600/3700.

Figure 102 1552 RAP Ethernet Bridging Configuration

Wireless > All APs > Details for RTP-06-1FL-R011552

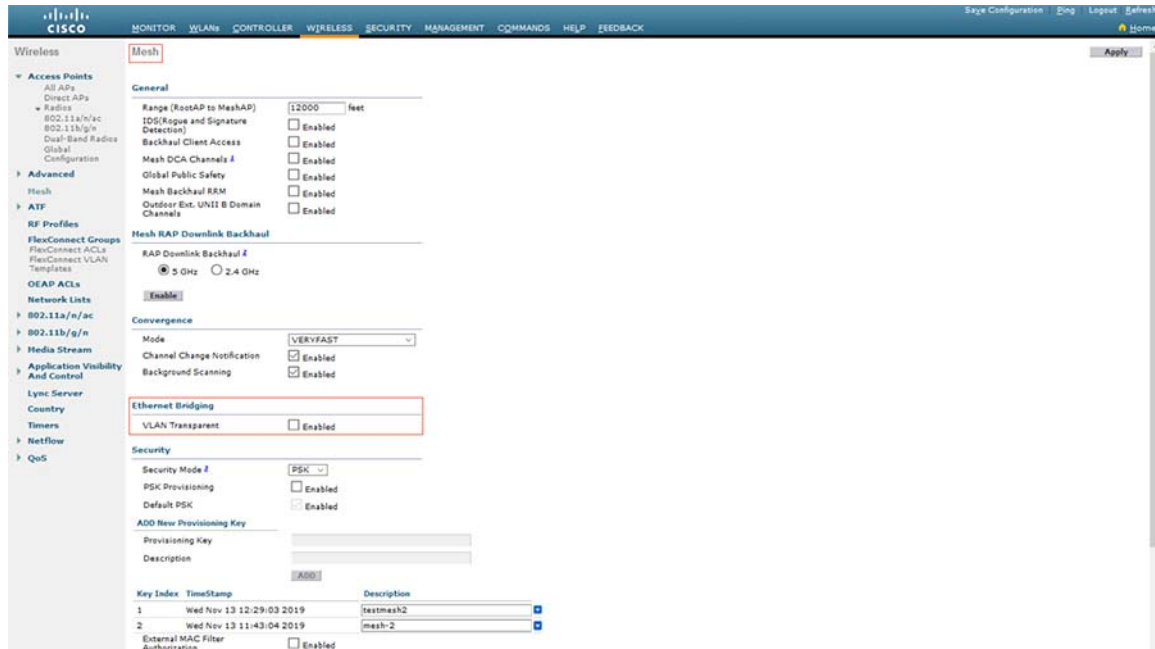
General | Credentials | Interfaces | High Availability | Inventory | Mesh | Advanced

AP Role: RootAP  
 Bridge Type: Outdoor  
 Bridge Group Name: mesh2  
 Strict Matching BGN: ☒  
 Ethernet Bridging: ☒  
 Preferred Parent: none  
 Backhaul Interface: 802.11a/n  
 Bridge Data Rate (Mbps): auto  
 Ethernet Link Status: Up/Dn/NANA  
 PSK Key Timestamp: [Delete PSK](#)  
 VLAN Support: ☒  
 Native VLAN ID: 104

Mesh RAP Downlink Backhaul  
 RAP Downlink Backhaul: ☒ 5 GHz ☐ 2.4 GHz  
 Enable:

Interface Name	Oper Status	Mode	Vlan ID
Gi0/0/100	Up	Trunk	104
Gi0/0/101	Down	Trunk	113
Gi0/0/102	Down	Access	113
Gi0/0/103	Down	Access	0

Foot Notes:  
 1(a) DNS server IP Address and the Domain name can be set only after a valid static IP is pushed to the AP.  
 1(b) 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.  
 1(c) 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.  
 2. TunnelSSH can be enabled in APs with non-default credentials only.  
 3. Hyperoperation Admin status is configurable for AP specific configuration only.  
 5. Applies only to Mesh Wireless Mesh Authentication to remove the PSK key and set to default on the Access Point.  
 6. External logging applies to IOS AP with country code is CH only. AP7502/1550/1570/1600/2700/2700/2600/3700.

**Figure 103 1552 MESH Disable Ethernet Bridging VLAN Transparency**

**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.

Both controllers AireOS need to have same mac address list under Mac filter tab for IW1552H and IW6300 to co-exist in the network.

Use Cases:

- Remote Access
- Emerson WiHart for condition-based monitoring

## 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 & green field deployment please reference the previous ethernet bridging configuration sections for this document.

## Location Services and Asset Tracking

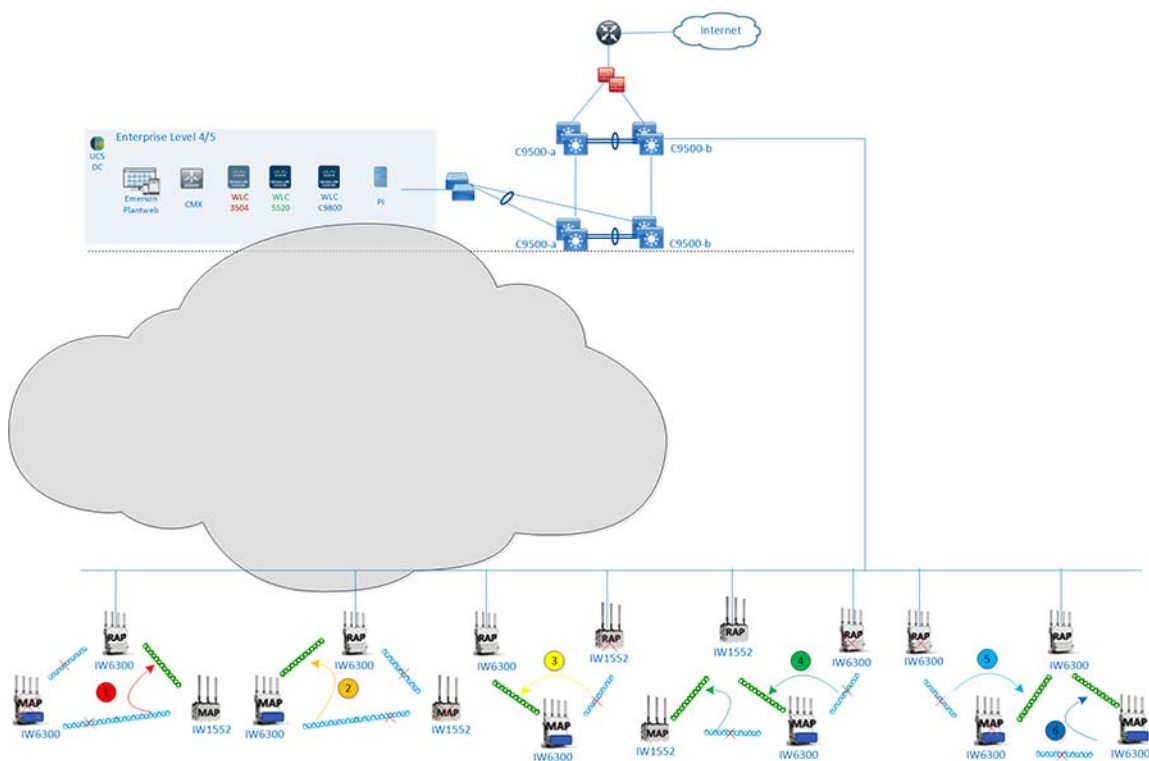
This solution uses the Cisco Connected Mobile Experiences (CMX) product to provide location services. CMX uses existing wireless infrastructure to calculate the location of the Wi-Fi devices and interferers such as BLE Beacons, microwave ovens, RFID tag, and etc. CMX uses RSSI triangulation from three nearby APs to located 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.

### Prime Infrastructure Location Service

Figure 104 is a snapshot of tracking parameters within CMX; these settings can be tuned to your network requirements.

**Figure 104 Prime Infrastructure Location Tracking Parameters**



## Troubleshooting

Debug Command:

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

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

show mesh config
```

## Troubleshooting

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

## ■ For general AP join issues (6300 RAP &amp; 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 &amp; 1552 MAP):

## – WLC:

```
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 &amp; 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
```

## Troubleshooting