• **1 | 1 - 1 | 1 -**CISCO ...

Oil and Gas Refinery WLAN MESH Implementation Guide

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

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

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

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

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

Deployment Models

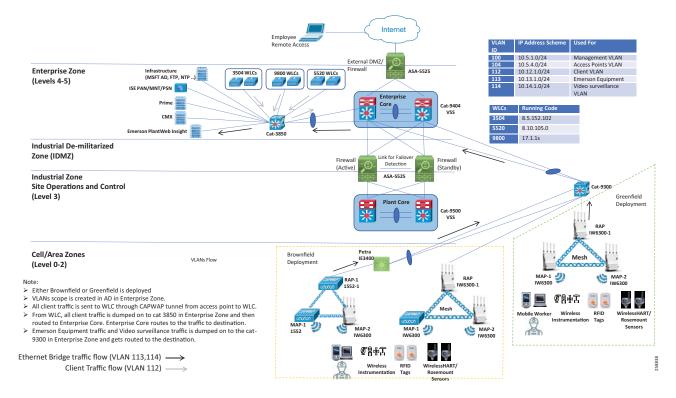


Figure 1 Oil and Gas Refinery WLAN MESH End-to-End Validation Topology

Deployment Models

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

A successful transition must meet the following requirements:

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

The focus of this document is:

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

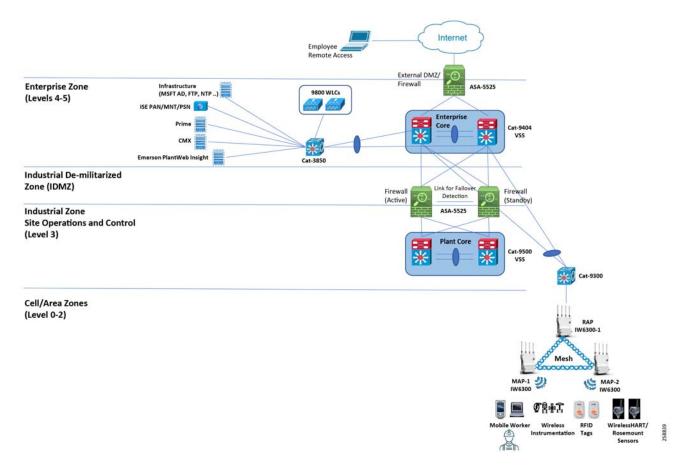
Greenfield Deployment

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

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

Deployment Models

Figure 2 Greenfield Deployment



Brownfield Deployment

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

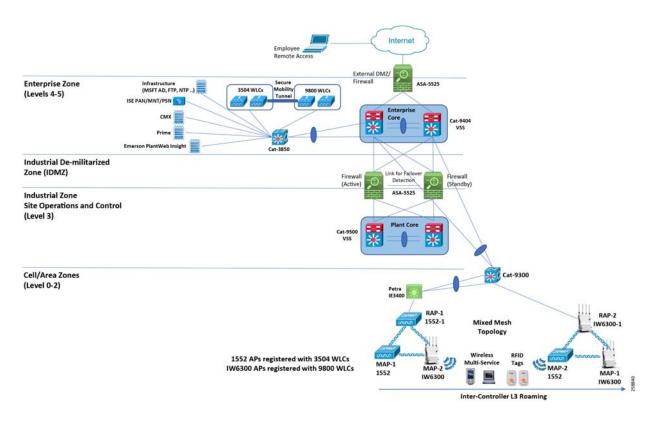
This deployment model uses two pairs of controllers running different code versions. Existing 1552 APs network is compatible with the AireOS controllers running 8.5 code. The IW6300 is compatible with the Cisco Catalyst 9800 WLCs or the AireOS controllers running 8.10 code.

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

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

Deployment Models

Figure 3 Brownfield Deployment with WLC3504 and Cat9800



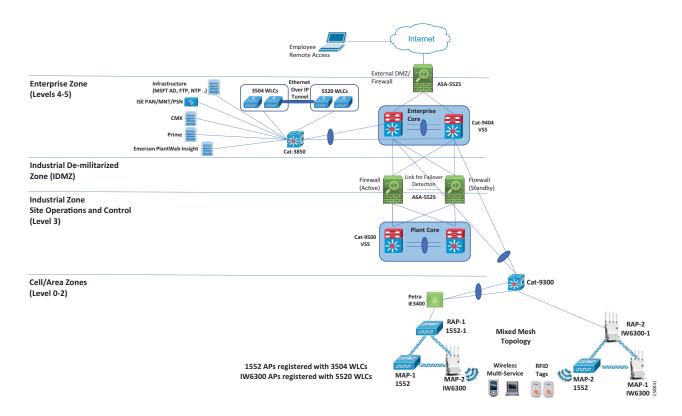


Figure 4 Brownfield Deployment with WLC3504 and WLC5520

Detailed Configurations of Components

Network Flow

The VLANs in Table 1 were used in the testbed; refer to the topology in Figure 4 for details.

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

Table 1 VLANs Used in the Testbed

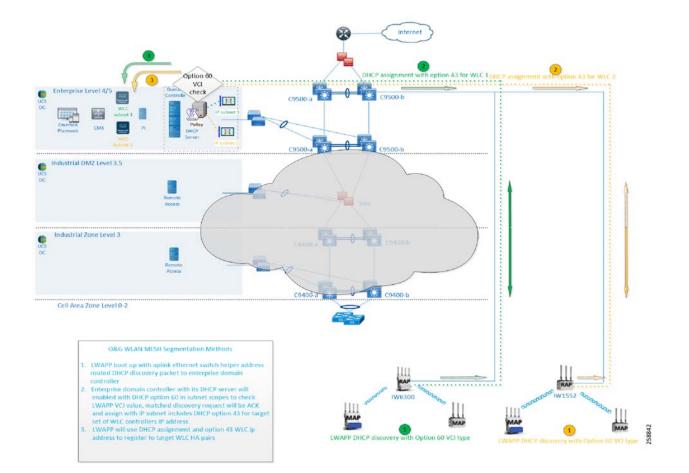
DHCP Flow for the APs

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
- 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.





Configuring Switches

Cisco C9400

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

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

Device> enable

2. Enter global configuration mode.

Device#configure terminal

3. Create a VLAN.

vlan <id> name <vlan name>

For example:

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

4. Create a VLAN interface.

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

For example:

IA-Ent-9404(config)#int vlan 112 IA-Ent-9404(config-if)#ip ad-dress 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>
```

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:

```
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 <id>
```

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

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

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:

```
!
1
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
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
1
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
1
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
1
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
```

```
Ţ
interface TwoGigabitEthernet1/0/4
description Connected to IE-3400
switchport trunk native vlan 104
 switchport trunk allowed vlan 104,113,150
 switchport mode trunk
channel-group 102 mode active
 service-policy output PTP-Event-Priority
1
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
1
```

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 gos-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
I.
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
1
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
1
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
I.
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
1
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
1
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
```

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

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
class-map match-all CIP-Implicit dscp 47
match access-group 102
class-map match-all CIP-Implicit dscp 55
match access-group 101
T.
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
1
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
1
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
1
```

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

 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	

dentity Services Engine	Home + Contex	t Visibility + Op	erations i	Policy -	Administratio	n 🛛 🕨 Work C	enters			
System - Identity Management	Network Resources	Device Portal N	lanagement	pxGrid Servic	os Foo	Service + T	hreat Centric NAC			
Identities Groups External Ident	ity Sources Identity	Source Sequences	• Settings							
Users	Network Acces	s Users								
Latest Manual Network Scan Results	/ Edit +Add	Change Status	@ Import	Export +	XDelete					
	Status	Name		Description		First Name	Last Name	Email Address	User Identity Groups	Admin
									No data available	

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

Figure 7 Adding Network Access User to ISE

cisco Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
	Network Resources Device Portal Management pxGrid Service Feed Service Threat Centric NAC
✓Identities Groups External Ident	ity Sources Identity Source Sequences
0	Network Access Users List > New Network Access User
Users	▼ Network Access User
Latest Manual Network Scan Res	* Name user1
	Status 🛃 Enabled 🗸
	Email
	▼ Passwords
	Password Type: Internal Users 🗸
	Password Re-Enter Password
	*Login Password Generate Password ()
	Enable Password Generate Password
	▼ User Information
	First Name user1
	Last Name user1
	▼ Account Options
	Description
	Change password on next login
	▼ Account Disable Policy
	Disable account if date exceeds 2020-04-21 (yyyy-mm-dd)
	▼ User Groups
	ALL_ACCOUNTS (default)
	Submit Cancel

The user is created. See Figure 8 below.

Figure 8 Network Access User Added to ISE

cisco Identity Services Engine	Home + Con	text Visibility > Ope	erations Policy Adm	ainistration > Wor	k Centers			
System Identity Management	Network Resource	B Device Portal M	anagement pxGrid Services	+ Feed Service +	Threat Centric NA	c		
-Identities Groups External Identity	Sources Identit	y Source Sequences	 Settings 					
0	Network Acce	ss Users						
Users		55 65615						
Users Latest Manual Network Scan Res	/ Edit 👍 Add		Delmport 🚯 Export 👻 🗙 Delet	te + DDDupicate				
	/ Edit - Add Status		Dimport Description	te → D_Dupicate First Name	LastName	Email Address	User Identity Groups	Admi

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

System Identity Management Ne	etwork Resources	Management pxGrid Services + F	ed Service + Threat Centric NAC		
Network Devices Network Device Group	ps Network Device Profiles Exte	ernal RADIUS Servers RADIUS Serve		ternal MDM Location Services	
etwork Devices	Network Devices				
Pefault Device	/ Edi 💠 Add 👌 Duplicate 👔	b Import 🚱 Export 🛛 🕞 Generate Pi	C X Delete		
Device Security Settings	Name IP/Mask	Profile Name	Location	Туре	Description
				No data ava	ilable

- 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.

System + Identity Management	Network Resources Device Portal Management pxGrid Service Feed Service Threat Centric NAC
Network Devices Network Device C	Sroups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services
0	Network Devices List > New Network Device
vork Devices	Network Devices
ault Device	* Name IA-OG-5520-WLC-1
ce Security Settings	Description
	IP Address • IP: 10.5.1.55
	a Device Device (in Device) (D
	* Device Profile 🏻 🏥 Cisco 💌 🕀
	Model Name 📃 👻
	Software Version 📃 👻
	* Network Device Group
	Location Al Locations O Set To Default
	IPSEC Is IPSEC Device O Set To Default
	Device Type All Device Types 📀 Set To Default
	RADIUS Authentication Settings
	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 (j)
	DTLS Required 🔲 🕢
	Shared Secret radius/dtls (7)
	CoA Port 2083 Set To Default
	Issuer CA of ISE Certificates for CoA Select if required (optional)
	DNS Name
	General Settings
	Enable KeyWrap () * Key Encryption Key Show
	Message Authenticator Code Key Key Input Format ASCI HEXADECIMAL
	SNMP Settings
	Advanced TrustSec Settings

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

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

Figure 11 WLC Added to Network Devices on ISE

cisco Identity Services Engine	Home Contex	t Visibility	ions Policy A	dministration	 Work Centers 	
System Identity Management	✓ Network Resources	Device Portal Mana	gement pxGrid Service	s Feed Servic	e Fhreat Centric N	IAC
Network Devices Network Device	ce Groups Network Dev	ce Profiles External I	RADIUS Servers RADIU	S Server Sequence	es NAC Managers	External MDM + Location Services
	0					
Network Devices	Network Device	5				
Default Device						
Device Security Settings	/ Edit 🕂 Add 🖟	Duplicate	Export - OGenerate	PAC XDelete -		
	Name	 IP/Mask 	Profile Name Lo	cation Type	Desc	ription
	A-OG-3504-W	LC-1 10.5.1.53/32	📩 Cisco 🕀 🛛 All	Locations All D	evice Types	
	M-OG-3304-V					
	A-OG-5520-W			Locations All D	evice Types	

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

cisco Identity Services Engine	Home	Operations F	Policy Administration	 Work Centers
Policy Sets Profiling Posture C	lient Provisioning Policy Element	S		
Dictionaries + Conditions - Resu	Its			
0				
- Authentication	Allowed Protocols Services For Policy Export go to Administrati	on > System > Backup	& Restore > Policy Export P	age
Allowed Protocols	/Edit 4Add RyDupicate	Delete		
Authorization	Service Name	Description		
Profiling	Allow EAP-FAST			
	Default Network Access	Default Allowe	ed Protocol Service	

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.



dentity Services Engine	Home
and the second	Client Provisioning Policy Elements
Dictionaries + Conditions - Re	
	Allowed Protocols Services List > Allow EAP-FAST
Authentication	Allowed Protocols
Allowed Protocols	Name Allow EAP-FAST
Authorization	Description
Profiling	
Posture	✓ Allowed Protocols
Client Provisioning	Authentication Bypass Process Host Lookup ()
	Authentication Protocols
	Allow PAP/ASCII
	Allow CHAP
	Allow MS-CHAPv1
	Allow MS-CHAPv2
	Allow EAP-MD5
	Allow EAP-TLS
	Allow LEAP
	Allow PEAP
	✓ ✓ Allow EAP-FAST
	EAP-FAST Inner Methods 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
	Allow Authentication of expired certificates to allow certificate renewal in Authorization Polic
	Use PACs O Don't Use PACs
	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 *
	Enable EAP Chaining
	Allow EAP-TTLS
	Preferred EAP Protocol LEAP *
	EAP-TLS L-bit ()
	Allow weak ciphers for EAP (i)
	Require Message-Authenticator for all RADIUS Requests D
	Save
	Dave Neper

Configure Policy Sets on the ISE Server

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

- 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

olicy Sets						ResetAll Hitcounti		Reset	Sav
+) Status	Policy Set Name	Description	Condition	ns	Allowed Protocols /	Server Sequence	Hits	Actions	v
0	OG WLC 802 tx EAP-FAST Users		AND	Wireless_802.1X Radius Called-Station-ID ENDS_WITH test802.1x	Allow EAP-FAST	× • +	30	¢	
Ø	Default	Default policy set			Default Network Acc	ess x + +	10	0	

4. Enter Rule Name, Conditions, Use, and Profiles, and then click Save. See Figure 15 below.

Policy Se		rvices Engine Home filing Posture Client Provis	Context Vi ioning P		Operations nents	* Poli	cy 🚺	Administration	♦ Work Ce	nters		License Warn	ing 🔺 🤉	0	•
olicus	Cote +	OG WLC 802.1x EAP-	EASTIL	ore								-	_		
												ResetAll Hito		Reset	
Search	Status	Policy Set Name	Descrip	tion		Conditi	ions					Allowed Protoc	ols / Server	Sequence	e Hit
Searon.	0	QG WLC 802 1x EAP-FAST Use	rs	_		AND		Wireless_802.1 Radius Called-		5_WITH test8021x		Allow EAP-FAS	т	× • +	3
							-								
 Authority 	enticatio	n Policy (2)													
+	Status	Rule Name	Cond	tions								Use		Hits	Action
Search	h														
												All_User_ID_Stores	**		
												✓ Options			
												If Auth fail			
	0	Authentication Rule 1	AND								REJECT * *			¢	
	0	Autoritication Rate 1	Parto	₽	Radius Called-S	tation-ID	alion-ID ENDS_WITH test8021x					If User not found		17	T
												REJECT	× *		
												If Process fail			
												DROP	* *		
												Internal Users	**		
	0	Default										> Options		0	¢
Auth	orization	Policy - Local Exceptions													
Auth	orization	Policy - Global Exceptions													
Autho	orization	Policy (2)													
-										Results					
(+)	Status	Rule Name	Cond	tions						Profiles		Security Groups		Hits	Action
Search	h		_												
	0	Authorization Rule 1	₽	Radius	Called-Station-ID	ENDS_W	VITH test8	8021x		[+ PermitAccess]	+	Select from list	- +	12	¢
-	Ø	Default								× DenyAccess	+	Select from list	- +	0	Ó

Figure 15 Authentication and Authorization Policies Added on ISE

Reset Save

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 encompasses 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:

- 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

elisite Prime Infrastr	ucture				Q . Application Search	🐥 😒 16 root	ROOT-DOMAIN
Maps / Wireless Maps	/ Site Maps (New!) \pm						00000
Domain Navigator	 Sites 				2 Site	🛛 📰 📰 🕅 Export -	Import - 0
Search	Search Sites	Status:	Sort: Name	• IL O II			Add Site
System Campus	+					System Campus	0 /
 B RTP-6 Unassigned 	-					\overline{B} 1 \clubsuit 1 \textcircled{O} 1 \textcircled{O} 1 \textcircled{A} 2 \bigcirc This Site has no coordinates.	a Ga to Site View
						Unassigned	0
							a Ga to Ste View

After the Site has been created, enter building parameters. See Figure 17 below.

Figure 17 Prime Infrastructure Add Building to site

					Q . Application Search	A 😣 16	root - ROOT-DOMAIN
Maps / Wireless Maps /					S Population States	÷ 🕹 10	
							0 Ø P
nain Navigator	Sites / System Campus Search Buildings	Status:	System campus now shows	e newly created site	1 Building		Add Building Add Outdo
System Campus	+	Status:	Sort Walle			RTP-6	
RTP-6						01 0 A2 Q4	
Floor-1							Go to Building Ve
Unassigned							
Unassigned							

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.



"listo" Prime Infrastructi	ure		Q - Application Search	🐥 😂 16	root - ROOT-DOMAIN 🔅
🐧 🛛 Maps / Wireless Maps / S	ite Maps (New!) 🔺				00700
Import Map Archive				9 📰 🗐 191	Export • Import •
	Choose Format	Select File	O Verity	Process	Bulk AP In CSV APs for GeoMap
Choose a map archive format					Map Archive
O 3rd Party XML / ZIP Format [suppo	rted schema definitions only]			10	
"wmlbe" contains the Schema Definition CosyNee contains may images contains com 4. Access point/Choke c 5. Yott, file may contain 2. Supported Vall, tar actored/ top), (multipart/20), (applicat Contains to may contains the Support for supporter	top file which contains 3 directions (mitDir, corfiles, it e XML, file guing definitions of Camput/Building/Duido poing mfo for Praimed AP to discovered AP. esponding images for Camput/Duidoor/Floor Areas as yonit/TboA Receiver definitions provided in XML shoul Mags and/or Calabation Data ap file mime formats (multipart/v-gtb)_ (application/ to point). (multiparti-ty-eo-compression), (application). from 3th Party based on supported Schema definition dischemid effinition, Supported XDL er grapel/graph for the support of the support	or/Floor Area, coordinates of AP/Chokepoint/TOAA Receive/Of bacified in the Xml d be available in the system. Import will not discover any device gab), [multipart/gap], [application/gab], [multipart/p-gab-com zer-commensed] in. This should contain 1 kml for each Floor in seperate direction	sstadel/Coverage Aread/Marken/Raik/Region//Planning Data etc., Calibrats In. Al undiscovered entities will be flagged as Error, Access pont/Choke po pressed), (application/in-gzp-compressed), [multipart/gzp-compressed], [application/in-gzp with floor images, 1 Xml for Camput/Biulding (buildings embedded in cam t/gap), (application/gzp), (multipart/in-gzp-compressed), (application/in-gzp	ont/TDoA Receiver should not have polication/gcio-compressed], [multi pus], 1 Xmi providing dimensions fo	e been assigned to any floor. part/x-tp], [application/x- ir Camput/Building. Please

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.



🗰 Prime Infrastructure - Nei X	+						
← → ♂ ☆	🛈 🙈 https://10	0.5.1.6/webacs/loginAction.do?actio	n=login&product=wcs&selectedCate	gory=en#pageId=c	om_cisco_ifm.	_web_page_inven	… ◙ ☆
😑 🖞 Prime Infrastr	ructure				- Application	Search	🔒 🔽 3 rox
Inventory / Device Mai	nagement / A	dd Device				×	
Device Groups	A		* SNMP Parameters				Selected 0 / Te
< ™ +		* General 🗸	Version	v3	•		Show Quick Filter
Search All				SNMP Retries	2		Last Inventory Colle
All Devices (2) Device Type (3)		* SNMP 🗸		SNMP Timeout	10	(Secs)	
Location	N	Telnet/SSH		* SNMP Port	161		
User Defined (j)		0	* Username	OGuser			
		HTTP/HTTPS	Mode	AuthPriv	•		
			Auth. Type	HMAC-MD5	•		
		Civic Location	Auth. Password			0	
			Privacy Type	CBC-DES	•		
			Privacy Password			0	
						1	
				Add Ve	erify Credentials	Cancel	
	_				_		
admin@Oil-Gas-Linux/etc/sysconf	ig 🤞 Prime Infra	astructure - Network Devi					

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

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

For SNMP configuration on the AireOS controller, refer to the *SNMP Configuration in:* https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/wireless_intrusion_detection_s ystem.html#id_16872

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

Figure 20 Prime Infrastructure Add Devices with SNMP discovery

	*	Inventory	ture	Q + Application Search
Q. Search tilenu		Device Management	gement / Network Devices *	
Dashboard	,	Network Devices Compute Devices (Deprecated)	Device Groups All Devices	
Monitor	,	Discovery Software Images Virtual Image Repository	+ • / X Admin State • Sync Groups & Sites • Export Device Revoke Certificate	Show
Configuration	•	Credential Profiles Network Audit	Add Device Jilley Admin Status Device Name Address DNS Name	Device Type Last Invento
Inventory	•	Configuration Archive	☑ Managed M-DG-3504-WLC-1 10.5.1.53 ■② 10.5.1.53	Cisco 3504 Wireless LAN Completed

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.



evice Groups		Groups / Device Type									Selected 0 / Total 3	00 0 00
<- ≣ +		X Sync Groups & Sit	tes 🔻 Configure	Monitor •	AP Up	grade	Group 🔻 🛛 🗗	oport Device	evoke Certificate	Show	Quick Filter	• 7
Q Search All All Devices (7)		AP Name	Ethernet MA	BaseRadio M	IP Address		Controller IP	Map Location	AP Group Na	Operational	Admin Status	Maintenance
Device Type ()										Registered ×		
▼ Unified AP (i)	0	RTP-06-1FL-6300M01	6c:8b:d3:ed:f7:10	dc:8c:37:35:ba	10.5.4.22	(\tilde{J})	10.5.1.55	System Camp	default-group	Registered	Enable	No
Cisco 1550 Series Unified Access	0	RTP-06-1FL-6300M02	6c:8b:d3:ed:f7:04	dc:8c:37:35:ba	10.5.4.27	(j)	10.5.1.55	System Camp	default-group	Registered	Enable	No
Cisco Catalyst IW6300 AC Heavy Wireless Controller () Location () User Defined ()	0	RTP-06-1FL-6300R02	68:36:78:98:62	68:3b:78:9d:47	10.5.4.21	<i>(j)</i>	10.5.1.55	System Camp	default-group	Registered	Enable	No

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

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

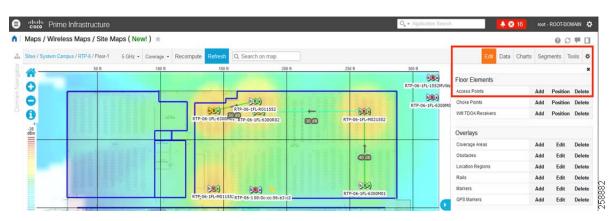


Figure 22 Prime Infrastructure Add Devices into Site Map

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

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

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

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

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

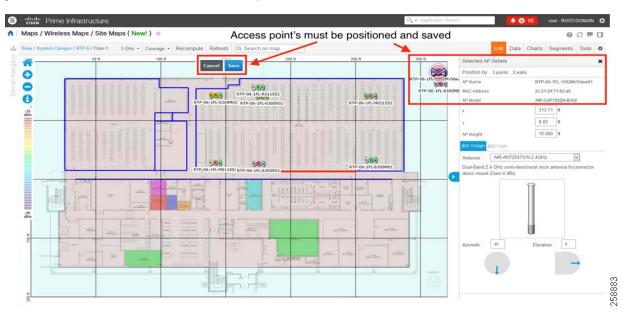


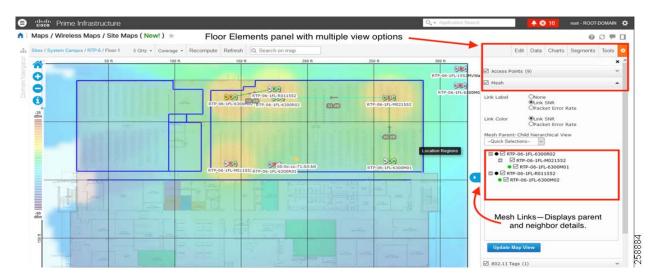
Figure 23 Prime Infrastructure Save Site Map

View Mesh Access Point Configurations Using Wireless Site Maps

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

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





Integration with CMX

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

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

Services / Mobility Service	es / Connected Mobile Experie	ances 🚖		
🖊 Edit 🛛 🗙 Delete 🛛 🕇 Add	Import Map to CMX Export M	ap from PI		
Device Name	IP Address	Software Version	Owner	
∠) cmx-10.6	10.5.1.10	10.6.2-46	jeharmon	
		Edit CMX * IP Address * Device Name * User Name * Dassword SSH Password Owner	10.5.1.10 cmx=10.6 admin cmxadmin emxadmin jeharmon	Verify

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.

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

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

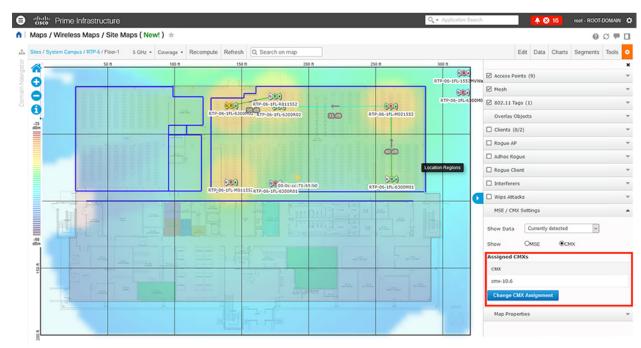


Figure 26 Prime Infrastructure and CMX Assignment

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

- Cisco Prime Infrastructure 3.7 User Guide https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-7/user/guide/bk_CiscoPrimeInfrastruct ure_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_cis co_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.

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/q os/b_166_qos_9400_cg/b_166_qos_9400_cg_chapter_01.html
- Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2SR https://www.cisco.com/c/en/us/td/docs/ios/qos/configuration/guide/12_2sr/qos_12_2sr_book.html

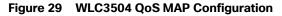
The following figures show the O&G WLAN MESH WLC QoS configuration details.



CISCO MONITOR	<u>W</u> LANS <u>C</u> ONTROLLER WIR	RELESS <u>s</u> ecur	RITY M <u>a</u> nagement c <u>o</u> mmands
WLANs	WLANs > Edit 'OG-SS	ID-1'	
 WLANS WLANS Advanced AP Groups 	General Security Quality of Service (QoS) Application Visibility AVC Profile Flex AVC Profile	QoS Polic Platinum (Enabled none ‡ none ‡	y-Mapping Advanced
	Netflow Monitor Fastlane Override Per-User Ban	none ¢ Disable ¢	acts (kbps) 16
		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 Bar	ndwidth Contr	acts (kbps) 16
		DownStream	UpStream

Figure 28 WLC3504 QoS Profile Configuration

	uluilu cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK
Wir	eless	Edit QoS	Profile	6						
	Access Points All APs Radios 802.11a/n/ac/ax 802.11b/g/n/ax Dual-Band Radios	QoS Profi Descriptio		platinum For Voice App	lications					
	Global Configuration	Per-User	Bandwidt	th Contracts ((kbps) *					
* *	Advanced			DownStre	am UpStre	am				
	lesh	Average (Data Rate	0	0					
+ 4	AP Group NTP	Burst Dat	a Rate	0	0					
+ 4	ATF	Average f	Real-Time R	ate 0	0					
F	RF Profiles	Burst Rea	al-Time Rate	0	0					
	FlexConnect Groups	Per-SSID	Bandwid	th Contracts	(kbps) *					
F	lexConnect VLAN			DownStre	am UpStre	am				
		Average [Data Rate	0	0					
	Network Lists	Burst Dat	a Rate	0	0					
▶ 8	302.11a/n/ac/ax	Average I	Real-Time R	ate 0	0					
) €	302.11b/g/n/ax	Burst Rea	al-Time Rate	0	0					
	Media Stream Application Visibility And Control	WLAN Qo Maximum		voice	\$					
			a area a subar est		•					
	ync Server		Default Priori		+					
	Country Timers	Multicast	Delault Prio	voice	_					
	Netflow	Wired Qo	S Protoco	ol.						
_		Protocol T	Гуре	802.1p						
	20S Profiles	802.1p Ta	ag	5						
	Roles Qos Map									
	Qua map	Foot Notes								
		1.Overrid is disable		Contracts paran	neters are spec	ific to per Radi	o of AP. The value z	ero (0) indicates	the featu	ire
		is disable								



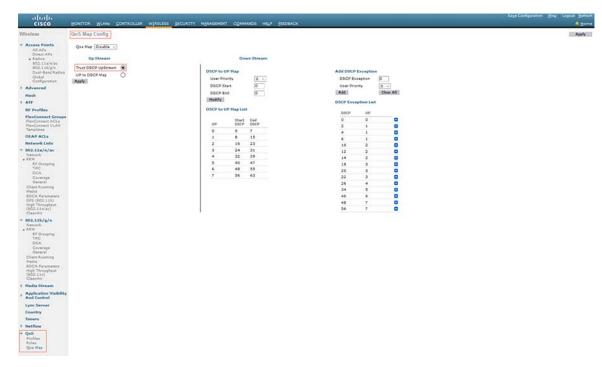
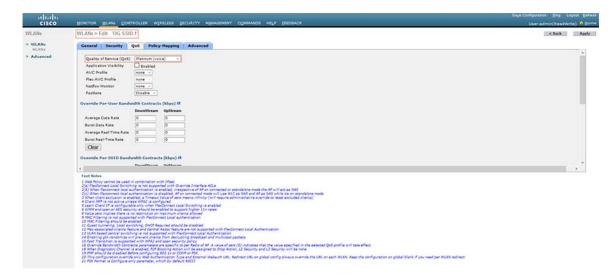


Figure 30 WLC5520 WLAN QoS Configuration



Detailed Configurations of Components

Figure 31 WLC5520 QoS Profile Configuration



Figure 32 WLC5520 WLAN QoS MAP Configuration

cisco	MONITOR WLANS CONTROLLER WIRELESS	SECURITY HANAGEMENT COMMANDS HELP FEEDBACK			Size Configuration Bing Lagout Beheat Usersadmin(Readwrite) 🕅 Bome
Wireless	QoS Map Config				Αρρίγ
* Access Points All APs • Radius	Qua Map Disable -				
802.11a/k/wc/ax 802.11b/g/n/ex Dual-Band Radios	Up Stream Trust DSCP UpStream	Down Stream			
Global Configuration	UP to DSCP Map	User Priority	Add DSCP Exception DSCP Exception	8	
+ Advanced Hesh	Apply	DSCP Start 0	User Priority	0	
+ AP Group NTP		DSCP End 0	[MM]	Clear All	
+ ATF		Modify	DSCP Exception List	,	
RF Profiles		OSCP to UP Hop List	DSCP UP		
FlexConnect Groups		Start fad	0 0		
+ FlexConnect ACLs		UP DSCP DSCP	2 1		
FlexConnect VLAN Templates		0 0 7	4 1	•	
Network Lists		2 16 23	6 1 10 2		
- 802.11a/n/ac/ax		3 24 31	12 2		
Natiork # RRM		4 32 39	14 2		
RF Grouping TPC		5 40 47 6 48 55	18 3		
DCA Coverage		7 54 63	20 3	0	
General			26 4		
Client Roaming Media			34 5		
EDCA Parameters OFS (602.11h)			46 6	•	
High Throughput (B02.11n/ac/ax) CleanAir		2	48 7 56 7	0	
B02.11b/g/n/wx Network REM RF TPC DCA Coverage General Clast Reaming Media					
EDCA Parameters High Throughput (B02.11n/ax) CleanAir					
Hedia Stream					
Application Visibility And Control					
Lync Server					
Country					
Teners					
 Netflow QoS Profiles Rales Qos Map 					

Figure 33 Cat 9800 WLAN QoS Configuration

Q. Search Menu Items	Configuration * >	Tags & Profiles -> Policy	Edit Policy Profile					
Dashboard	+ Add	× Delete	General Access	Policies QOS	and AVC Mobility	Advanced		
beamboard	to damage of		Auto QoS	Voice	•	Flow Monitor	IPv4	
Monitoring	>	Policy Profile Name	QoS SSID Policy			Egress	Search or Select	•
20		og-profile_WLANID_1	Q05 5510 Policy			-3.000		
Configuration		default-policy-profile	Egress	platinum	× •	Ingress	Search or Select	•
(O) Administration	> (4 - 4 1 >	► 10 v items per page	Ingress	platinum-up	× ·	Flow Monitor	IPv6	
X Troubleshooting			QoS Client Policy	Č.		Egress	Search or Select	•
			Egress	Search or Select	•	Ingress	Search or Select	•
			Ingress	Search or Select	•			
			SIP-CAC					
			Call Snooping					
			Send Disassociate					59
			Send 486 Busy					258859

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

Configuring HA SSO between two 9800 WLCs using the GUI:

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

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

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

Figure 34 Redundancy Configuration on active Catalyst 9800

Q. Search Menu Items	Administration * > Device		
📻 Dashboard	General	Redundancy Configuration	
Monitoring >	FTP/SFTP/TFTP	Redundancy Pairing Type	RMI+RP RP
Configuration >	Redundancy	Local IP*	10.5.1.61
(주) Administration >		Netmask*	255.255.255.0
X Troubleshooting		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

Q Search Menu Items	Administration - > Devi	ice	
Dashboard	General	Redundancy Configuration	ENABLED
	FTP/SFTP/TFTP	Redundancy Pairing Type	RMI+RP RP
	Redundancy	Local IP*	10.5.1.62
O Administration		Netmask*	255.255.255.0
C Troubleshooting		Remote IP*	10.5.1.61
No Housicshooting		Keep Alive Timer	1 x 100 (milliseconds
		Keep Alive Retries	5
		Active Chassis Priority*	1
		Standby Chassis Priority*	2

Figure 35 Redundancy Configuration on Stand-by Catalyst 9800

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 though 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
                                     H/W Current
Chassis# Role Mac Address Priority Version State
                                                               IP
_____
     Active d4e8.80b2.d740 2 V02 Ready
*1
                                                           10.5.1.61
2
       Standby d4e8.80b2.d080 1 V02 Ready
                                                             10.5.1.62
WLC#show redundancy
Redundant System Information :
Available system uptime = 2 days, 18 minutes
Switchovers system experienced = 0
           Standby failures = 0
      Last switchover reason = none
              Hardware Mode = Duplex
   Configured Redundancy Mode = sso
    Operating Redundancy Mode = sso
           Maintenance Mode = Disabled
             Communications = Up
Current Processor Information :
Active Location = slot 1
      Current Software state = ACTIVE
      Uptime in current state = 2 days, 18 minutes
              Image Version = Cisco IOS Software [Amsterdam], C9800 Software (C9800_IOSXE-K9),
Version 17.1.1s, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Sat 15-Feb-20 20:00 by mcpre
                     BOOT = bootflash:packages.conf,1;
                CONFIG_FILE =
```

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.

	General	Active Stati	stics Standby	Statistics										
	My State				ACTIVE			Redu	ndancy State				\$\$0	
Configuration >	Peer State				STANDBY HOT			Manu	al Swact				enabled	
Administration >	Unit				Primary			Com	munications				Up	
	Unit ID				1			Stand	sby Failures				0	
	Chassis I	Details _{Role} ~	MAC ~ Address	Priority	H/W Version	Current State	✓ IP Address	v	RMI IP Address	×.	Mobility MAC Address	~	Image version	Device Uptime
	•1	Active	d4e8.80b2.d740	2	V02	Ready	10.5.1.61		NA		d4e8.80b2.d74b		17.1.1s	3 days, 6 hours, 51 minutes
			100000000000000	1	V02	Ready	10.5.1.62		NA		d4e8.80b2.d08b		17.1.15	3 days, 6 hours, 56
	2	Standby	d4e8.80b2.d080			1.022220								minutes
		Standby	10 v Roma p	12		1.000								1 - 2 of 2

Figure 36 Monitor Redundancy Configuration

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

Configuring Mesh Profile

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

In the new configuration model, the controller has a default mesh profile. This profile is mapped to the default AP-join profile, which is in turn is 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.

 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

General	Alarm	
> Ethernet Bridging Allow BPDU	Max Hop Count	4
Subset Channel Sync	Recommended Max Children for MAP	10
Backhaul	Recommended Max Children for RAP	20
Extended UNII B Domain Channels	Parent Change Count	3
RRM	Low Link SNR (dB)	12
Security	High Link SNR (dB)	60
PSK Provisioning	Association Count	10
Default PSK		

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

Q. Search Menu Items	Configuration * > Wireless * >	Edit Mesh Profile			
	Global Config Profiles	General Advanced			
m Dashboard		Name*	MeshProfile1	Backhaul amsdu	
Monitoring ,	+ Add >> Delote	Description	MeshProfile1	Backhaul Client Access	
Configuration	Number of Profiles : 3	Range (Root AP to Mesh AP)	12000	Battery State for an AP	
Administration	Name	Multicast Mode	In-Out 🔹	Full sector DFS status	
	MeshProfile1	IDS (Rogue/Signature Detection)			
Y Troubleshooting	MeshProfile2				
	default-mesh-profile	Convergence Method	Very Fast		
	H 4 1 + H 10 +	Background Scanning			
		Channel Change Notification			
		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

ashboard			Security			5 GHz Band Backhau	al .	
lonitoring	>	- Add × Delete	Method	PSK	•	Rate Types	auto	
onfiguration	*	Number of Profiles : 3	Authentication Method	Enter Method		2.4 GHz Band Backh	aul	
dministration	*	Name MeshProfile1	Authorization Method	default	1.	Rate Types	auto	
ubleshooting		MeshProfile2	Ethernet Bridging					
		default-mesh-profile	VLAN Transparent					
		ia a 1 a ai 10 .	Ethernet Bridging					
			Bridge Group					
			Bridge Group Name	mesh1				
			Strict Match		0			

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

	← Add X Delete Enable WLAN	General Security	Advanced		
Dashboard		Profile Name*	OG-SSID-1	Radio Policy	All
Monitoring	Number of WLANs selected : 0	SSID*	OG-SSID-1	Broadcast SSID	
Configuration	Statue- Name - ID	WLAN ID*	1		
	0 06-SSID-1	Status			
Administration	> C O test8021x 2				
Troubleshooting	ia a 1 a ai 10 v items per page				

Figure 41 Example of PSK Security Configuration for Client Access

Edit WLA	N				
General	Security	Advanced			
Layer2	Layer3	AAA			
Layer 2 Se MAC Filter	ecurity Mode		WPA + WPA2 🔻	Fast Transition Over the DS	Enabled v
Protecte	d Managemo	ent Frame		Reassociation Timeout	20
PMF WPA Par	ameters		Disabled •	MPSK Configuration	
WPA Polic	у				
WPA2 Pol	icy				
WPA2 End	ryption		AES(CCMP128) CCMP256 GCMP128 GCMP256		
Auth Key M	Mgmt		 802.1x PSK CCKM FT + 802.1x FT + PSK 802.1x-SHA256 PSK-SHA256 		
PSK Form	at		ASCII		
PSK Type			Unencrypted v		
Pre-Share	d Key*				

Figure 42 Advanced Tab Configuration on WLAN

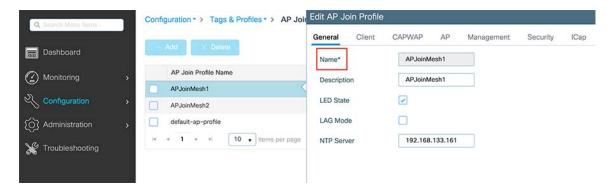
Edit WLAN	l			
General	Security	Advanced		
Coverage	Hole Detection		Universal Admin	
Aironet IE			Load Balance	
P2P Block	ing Action	Disabled 🔹	Band Select	
Multicast I	Buffer	DISABLED	IP Source Guard	
Media Str direct	fedia Stream Multicast-		WMM Policy	Allowed 🗸
Max Clie	ent Connection	ns	mDNS Mode	Bridging v
			Off Channel Scanni	ng Defer
Per WLAN	1	0		
Per AP Pe	r WLAN	0	Defer Priority	0 1 2
Per AP Ra	dio Per WLAN	200		
11v BSS	Transition Su	pport		
			Scan Defer 10 Time	00
BSS Trans	sition		Assisted Roaming (11k)
Disassocia to 3000 T	ation Imminent(C BTT)	200	-	
Optimized	Roaming	40	Prediction Optimization	
40 TBTT)	ation Timer(0 to		Neighbor List	
BSS Max	Idle Service		Dual Band Neighbor List	
BSS Max	Idle Protected			internet.)
Directed N	Aulticast Service	•	DTIM Period (in bea	icon intervais)
11ax			5 GHz Band (1-255)	1
			2.4 GHz Band (1-255)	1
Downlink	OFDMA		Device Analytics	
Uplink OF	DMA			
Downlink	MU-MIMO		Advertise Support	
Uplink MU	I-MIMO		Share Data with Client	
BSS Targe	et Wake Up Time	e		

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.
- 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

		+ Add × Doloto	General Client CAP	WAP AP Management	Security ICap	
Dashboard			General Hyperlocation	BLE Packet Capture		
) Monitoring	>	AP Join Profile Name	Power Over Ethernet		Client Statistics	Reporting Interval
		APJoinMesh1				in the second
Configuration	· C	APJoinMesh2	Switch Flag		5 GHz (sec)	90
Administration	> C	default-ap-profile	Power Injector State		2.4 GHz (sec)	90
Troubleshooting		+ 1 + + 10 + items per page	Power Injector Type	Unknown 🔹	Extended Module	8
			Injector Switch MAC	00:00:00:00:00:00	Enable	
			Code		Mesh	
			AP EAP Auth Configurati	on	Profile Name	MeshProfile1 +
			EAP Type	EAP-FAST .		Ciea
			AP Authorization Type	CAPWAP DTLS		

- 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

Q. Search Menu Rems	Configuration * > Tags & Profiles * > AP Jo	Edit AP Join Profile General Client CAPW	AP AP Management	Security ICap
Dashboard	Add Z Delets	Device User Creden	tials CDP Interface	
Monitoring	APJoinMesh1	TFTP Downgrade		Telnet/SSH Configuration
Configuration	APJoinMesh2	IPv4/IPv6 Address	0.0.0.0	Teinet 🔽
O Administration Y Troubleshooting	> is a 1 ≥ P 10 v items per page	Image File Name System Log	Enter File Name	AP Core Dump
		Facility Value	KERN	Enable Core Dump
		Host IPv4/IPv6 Address	255.255.255.255	
		Log Trap Value Secured (i)		

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

Q Search Menu Items	Configuration * > Tags & Profiles * > AP Join	Edit AP J	oin Profile	е		
		General	Client	CAPWAP	AP	Management
Dashboard	+ Add × Delete	Device	User	Credentials	CDP I	nterface
Monitoring >	AP Join Profile Name					
S	APJoinMesh1	User M	lanagemei	nt		
Configuration >	APJoinMesh2	Usernar	ne	admin		
(Ô) Administration →	default-ap-profile	Passwo	rd			
X Troubleshooting	H 4 1 F H 10 V items per page	Passwo	rd Type	clear		•
		Secret				
		Secret 1	Гуре	clear		•

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

Figure 47 Enabling CDP in AP Join Profile

		+ Add × Delete	General	Client	CAPWAP	AP	Managemen
Bashboard		+ Add × Delete	Device	User	Credentials	CDP In	terface
	>	AP Join Profile Name	CDP Sta	te		ก	
	50-2004 	APJoinMesh1	ODF Ste	ite	ENABLED	U	
Configuration	>	APJoinMesh2					
Administration	>	default-ap-profile					
Troubleshooting		I≪ ≪ 1 ► ► 10 v items per page					

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

Q. Search Mena Joms	Configuration * > Tags & Profiles * > Policy	Edit Policy Profile General Access Policies	QOS and AVC Mobility	Advanced	
Dashboard	+ Add × Delete Status × Policy Profile Name	A Configur	ing in enabled state will result in loss o	f connectivity for clients associated with	this profile.
♦ Configuration →	og-profile_WLANID_1 default-policy-profile	Name*	eg-profile_WLANID_1	WLAN Switching Policy	
 Administration Troubleshooting 	ie e 1 * H 10 V itoms por page	Description	og-profile_OG-SSID-1	Central Switching Central Authentication	ENABLED
(dGU) (offer val		Passive Client Encrypted Traffic Analytics	ENABLED DISABLED	Central DHCP Central Association	ENABLED
		CTS Policy		Flex NAT/PAT	DISABLED
		Inline Tagging SGACL Enforcement			
		Default SGT	2-65519		

4. On the Access Polices 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

Q. Search Monu Items	+ Add × Delete	General Access Policies	QOS and AVC Mobility Advance	bd		
📷 Dashboard	+ Add × Delate	RADIUS Profiling		WLAN ACL		
Monitoring	Status v Policy Profile Name	Local Subscriber Policy Name	Snarch or Saloct	IPv4 ACL	Search or Select 1	
	og-profile_WLANID_1 default-policy-profile	WLAN Local Profiling	Sec. Sec.	IPv6 ACL	Search or Soloot	
Administration	> 14 4 1 P H 10 v items per page	Global State of Device Classification	Disabled ()	URL Filters		-1-22
X Troubleshooting		HTTP TLV Caching		Pre Auth	Search or Select	•
		DHCP TLV Caching		Post Auth	Snarch or Select	•
		VLAN				
		VLAN/VLAN Group	VLAN0112 VLAN0112			
		Multicast VLAN	Enter Multicast VLAN			

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

Figure 50 QoS Configuration in Policy Profile

		General Access	Policies QOS and AVC	Mobility Adva	anced		
nashboard	+ Add × Deleto	Auto QoS	Voice		Flow Monito	or IPv4	
Monitoring >	Status v Policy Profile Name	NO. 47 ADJECTS				Sourch or Select	-
	og-profile_WLANID_1	QoS SSID Policy		2	Egress	posici o pener	•
Configuration	default-policy-profile	Egress	platinum x v		Ingress	Search or Select	•
Administration >	ie e 1 e el 10 v items per page	Ingress	platinum-up x +		Flow Monito	vr IPv6	
Troubleshooting		QoS Client Policy	e la companya de la c	23	Egress	Search or Select	•
		Egress	Search or Select	9	Ingress	Search or Select	٠
		Ingress	Search or Select				
		SIP-CAC					
		Call Snooping					
		Send Disassociate					
		Send 486 Busy					

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.



Name*	og-profile		
Description	Enter Description		
WLAN-POLIC Add × De	Y Maps: 2		
WLAN Profile		 Policy Profile 	~
OG-SSID-1		og-profile_WLANID_1	
test8021x		og-profile_WLANID_1	
4 4 1 ⊨ ⊨	10 🔻 items per page		1 - 2 of 2 items
Map WLAN and Po	licy		
WLAN Profile*	OG-SSID-1	Policy Profile*	og-profile_WLANID_ 🔻

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

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

Add RF Tag			×
Name*	og-profile		
Description	RF-profile		
5 GHz Band RF Profile	Global Config	•	
2.4 GHz Band RF Profile	Global Config	•	
Cancel		Apply to De	vice

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 though 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.

NTP S	erver Details			
+ Ad	d X Delete			C Refresh NTP Table
	Host Name v	Status v	VRF Name \checkmark	Source Address
	192.168.133.161	Peer (reachable)	Mgmt-intf	None
	192.168.133.171	Candidate (reachable)	Mgmt-intf	None
4 - 4	1 > > 10 - item	s per page		1 - 2 of 2 items

Figure 55 Verifying NTP Status

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 ass	ociations							
address	ref clock	st	when	poll	reach	delay	offset	disp
*~192.168.133.16	1 .MRS.	1	554	1024	377	0.628	1.493	1.129
+~192.168.133.17	1 .MRS.	1	357	1024	377	0.452	1.575	1.052
* sys.peer, # s	elected, + candi	date,	- outly	ver, x	falset	icker,	~ config	ured

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

Q. Search Menu Items		Configuration • >	Security - > AAA				
📻 Dashboard		+ AAA Wizard					
	>	Servers / Groups	AAA Method List	AAA Advanced			
	>	Global Config	MAC Address	Serial Number			
O Administration	>	RADIUS Fallback	+ Add	× Deleto	Belect File	③ L Upload File	
X Troubleshooting		Attribute List Name			🗅 test.csv 🛛 🖂		
		1000	MAC Addre	ess 🛛 🗸 Attribute List N	lame v WLAN Profile	 Description 	
		Device Authentication	6c8bd3edf	6e0 None		RTP-06-1FL-6300R01	
		AP Policy	683b78986	62c8 None		RTP-06-1FL-6300R02	
		Password Policy	H H 1	2 > ⊨ 10 • ite	ems per page	11 - 12 of 12 items	

- 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

AP in Site 1	Profile Name
AP in Site 2	Profile Name
AP in Site 3	Profile Name
AP in Site 4	Profile Name
AP in Site 5	Profile Name
AP in Site 6	Profile Name
AP in Site 7	Profile Name
	AP in Site 2 AP in Site 3 AP in Site 4 AP in Site 5 AP in Site 6

Changing an AP Role

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

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

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

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

Figure 58 AP Role as Root

Q. Search Menu Itema	Configuration • > Wireless • > Access Point	t Edit AP			
Dashboard	 All Access Points 	General Interfaces	High Availability Invent	tory Mesh Advanced Ethernet Port Configuration	n
Monitoring Monitoring Configuration	AP × AP × Admin Name Model Stots × Status	Block Child	0	• Ethernet Bridging on the as enabled to configure this sect	isociated Mesh Profile should be tion successfully
(O) Administration	RTP-06-1FL- IW-6300H- 2	Daisy Chaining Daisy Chaining strict- RAP		Port	0 •
X Troubleshooting	6300R01 d AC-B-K9 2 RTP-06-1FL- IW-6300H- 6300M03 A AC-B-K9 2	Preferred Parent MAC	· · · · · · · · · · · · · · · · · · ·	Mode Native VLAN ID*	trunk v
	RTP-06-1FL- IW-6300H- 2 6300M02 A AC-B-K9 2 RTP-06-1FL- IW-6300H- 2	VLAN Trunking Native	Root	Allowed VLAN IDs	113,112
	R11P-06-THE W*-5000H 2 ● 6300M001 A. AC-B-K9 2 ● H 1 ★ 10 • B 5 GHz Radios 5 5 5	Remove PSK			
	> 2.4 GHz Radios	Backhaul			
	> Dual-Band Radios	Backhaul Radio Type Backhaul Slot ID	5ghz •		
	> Country	Rate Types	auto 🔹		

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

5 2 3	Number of Flex+Bridge APs Number of Flex+Bridge RAPs Number of Flex+Bridge MAPs	0 0 0
2 3	Number of Flex+Bridge RAPs	0
2 3	Number of Flex+Bridge RAPs	0
2 3	Number of Flex+Bridge RAPs	0
3		
	Number of Flex+Bridge MAPs	0
,Pref Parent,Chan Util,Clients		
	==	
0), 0000.0000.0000, 0%, 0] 0), 0000.0000.0000, 1%, 0]		
0 5 5	000.0000.0000, 1%, 0] 50), 0000.0000.0000, 1%, 1] 000.0000.0000, 2%, 0] 50), 0000.0000.0000, 0%, 0] 50), 0000.0000.0000, 1%, 0] ernet Connected Mesh AP.	000.0000.0000, 1%, 0] 50), 0000.0000.0000, 1%, 1] 100.0000.0000, 2%, 0] 50), 0000.0000.0000, 0%, 0] 50), 0000.0000.0000, 1%, 0]

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.

^D Cancel

ecurity		5 GHz Band Backha	aul
Method	PSK v	Rate Types	auto
Authentication Method	Enter Method	2.4 GHz Band Back	haul
Authorization Method	default	Rate Types	auto 🔻
thernet Bridging			
VLAN Transparent			
Ethernet Bridging			
ridge Group			
Bridge Group Name	mesh1		
Strict Match			

Figure 60 Enabling Ethernet Bridge on Mesh Profile

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.

🗄 Update & Apply to Device

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

		ess Points			General Interface	s High Avai	ability Inv	ventory Mesh Advanced	3	
Bashboard	Number of AP(s):	10.5 (A 00.03)			General			Ethernet Port Configurat	ion	
Monitoring	*				Block Child			O Ethernet Bridging on the		e should
Configuration	> AP ~ Name	AP ~ Model	Slots	 ✓ Adm ✓ Stat 				enabled to configure this s	ection successfully	
Administration	> RTP-06-1FL- 6300R02	AC-B-K9	2	0	Daisy Chaining strict-			Port	0	
Troubleshooting	RTP-06-1FL- 6300R01 da	AC-B-K9		0		0000.0000.0	000	Mode	trunk	
•	RTP-06-1FL- 6300M03	AC-B-K9	2	0	Preferred Parent MAC		000	Native VLAN ID*	104	
	RTP-06-1FL- 6300M02	AC-B-K9	2	٥	VLAN Trunking Native	104		Allowed VLAN IDs	112,113	_
	RTP-06-1FL- 6300M01	IW-6300H- AC-B-K9	2	0	Role	Root	•			
	> 5 GHz R		• iten	ns per pag	Remove PSK	<u>ل</u>				
	> 2.4 GHz	Radios			Backhaul					
					Backhaul Radio Type	Sghz	•			
	> Dual-Ba	and Radios	5		Backhaul Slot ID	1	•			
	> Country				Rate Types	auto	•			

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

			Edit AAA Radius S	Server
Q Search Menu Items	Configuration * >	Security * > AAA	Name*	OGISE
🚃 Dashboard	+ AAA Wizard		Server Address*	10.5.1.19
	Servers / Groups	AAA Method List	PAC Key	
	+ Add	× Delete	Кеу Туре	0 🗸
~			Key*	
O Administration	> RADIUS	Servers Server Gro	Confirm Key*	
X Troubleshooting	TACACS+	Name ~	Auth Port	1812
	LDAP) OGISE	Acct Port	1813
		⊲ ⊲ 1 ⊳ ⊳	Server Timeout (seconds)	1-1000
			Retry Count	0-100
			Support for CoA	ENABLED

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



			Quick Setup: AAA	Authenticati	on
Q. Search Menu Items	Configuration * >	Security * > AAA	Method List Name*	OGISE1	
Dashboard			Type*	dot1x	•
Monitoring >	Servers / Groups	AAA Method List	Group Type	group	¥
Configuration >	Authentication		Fallback to local		
Administration >	Authorization	+ Add ×	Available Server Groups		Assigned Server Groups
Troubleshooting	Accounting	Name v Typ	ldap tacacs+	>	radius
		default logi		< >	
		OGISE1 do		**	2

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

Q. Search Menu Items	Con	figuratio	on * > Tags & Pr	Edit WLAN			×
Dashboard			× Delete	General Security Adv	anced		
Monitoring >	Num	ber of WL	ANs selected : 0	Layer2 Layer3 AAA			
Configuration >			Name	Layer 2 Security Mode	WPA + WPA2 🔹	Fast Transition	Enabled
Administration >		0	OG-SSID-1 test8021x	MAC Filtering		Over the DS	
Y Troubleshooting	14	- 1	▶ Þ [10	Protected Management Frame		Reassociation Timeout	20
						MPSK Configuration	
				PMF	Disabled 🔹	MPSK	
				WPA Parameters			
				WPA Policy			
				WPA2 Policy			
				WPA2 Encryption	AES(CCMP128)		
					CCMP256		
					GCMP256		
				Auth Key Mgmt	802.1x		
					ССКМ		
					FT + 802.1x		
					802.1x-SHA256		
					PSK-SHA256		

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

Q. Search Menu Items	Configuration * > Tags	Edit WLAN	
Dashboard	+ Add × Delete	General Security	Advanced
	Number of WLANs selected :	D Layer2 Layer3 AAA	
	Status Name	Authentication List	OGISE1
	OG-SSID-1	Automication List	
O Administration	> O test8021x	Local EAP Authentication	
X Troubleshooting	⊲ ⊲ 1 ⊳ ⊳	10	

Figure 65 WLAN Authentication Method List Configuration

For a detailed implementation guide, refer to:

Configure 802.1x Authentication on Catalyst 9800 Wireless Controller Series https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213919-configure-802-1x-authentication-on-catal.html

Brownfield Deployment Model

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

AireOS (8.5) to AireOS (8.10) Deployment

Configuring HA SSO on 3504 or 5520

WLC3504 and WLC5520 is enabled with high availability between its peer controllers to reduce downtime, which reply on each of the HA primary and backup WLC to keep a mirror copy of AP and the client database. HA is enabled by inter-connecting the Primary and back WLC dedicated redundant ports. Detailed Cisco WLC controller for 3504 and 5520 High Availability (SSO) deployment can be refer to *High Availability (SSO) Deployment Guide*. The following is the detailed example for 0&G brownfield deployment configuration.

cisco	MONITOR WLANS	CONTROLLER WIRELES	S <u>S</u> ECURITY	MANAGEMENT	COMMANDS HELP	FEEDBACK		ng Logout Befres
Controller	Interfaces						Entries 1 - 6 of 6	New
General	Interface Name	VLAN Identifie	r IP Address	Interface Type	Dynamic AP Manag	ement IPv6 Address		
	client-vlan-12	112	10.12.1.2	Dynamic	Disabled	::/128		
Inventory Interfaces	management	100	10.5.1.53	Static	Enabled	::/128		
	redundancy-manageme	nt 100	10.5.1.63	Static	Not Supported	100 fastar		
Interface Groups	redundancy-port	untagged	169.254.1.63	Static	Not Supported			
Multicast	service-port	N/A	192.168.251.53	Static	Disabled	::/128		
Network Routes Fabric Configuration	virtual	N/A	192.0.2.1	Static	Not Supported			
 Redundancy Global Configuration Peer Network Route Internal DHCP Server Mobility Management Ports NTP CDP PMIPv6 Tunneling IPv6 mDNS Advanced 								

Figure 66 3504 WLC Controller Redundancy Management Interface Configuration

Figure 67 3504 WLC Controller Redundancy Global Configuration

cisco	MONITOR WLANS CONTROLLER	R WIRELESS SE	CURITY MAI	AGEMENT	С <u>о</u> мм	ANDS	ANDS HELP	ANDS HELP FEEDBACK			
ntroller	Global Configuration									1	Apply
General	Redundancy Mgmt Ip 1	10.5.1.63									
Inventory	Peer Redundancy Mgmt Ip	10.5.1.64									
Interfaces	Redundancy port Ip	169.254.1.63									
Interface Groups	Peer Redundancy port Ip	169.254.1.64									
fulticast	Redundant Unit Mobility Mac Address	Primary ~ 00:87:64:8A:3F:80									
Network Routes	Keep Alive Timer (100 - 1000).2.3	100	milliseconds								
Fabric Configuration	Keep Alive Retries (3 - 10)2	3									
Redundancy	Peer Search Timer (60 - 300)	120	seconds								
Global Configuration Peer Network Route	Management Gateway Failover	Enabled V									
Internal DHCP Server	SSO	Enabled ~									
Mobility Management	Service Port Peer Ip-4	192.168.251.54									
Ports	Service Port Peer Netmask 4	255.255.0.0									
NTP	Foot Notes										
CDP	1 Redundancy management and Pee 2 Configure the keep-alive timer in n	r redundancy manager nilli seconds between 1	nent are mandat 00 and 1000 in	ory parameter multiple of 50.	rs for SSO enab	le.					
PMIPv6	3 Configuring keep alive parameters 4 Peer service port IP address and th					lished					
Tunneling											
IPv6											
mDNS											
Advanced											

cisco	MONITOR WLANS CO	NTROLLER WIRELESS	SECURITY	MANAGEMENT C	OMMANDS HELF	P FEEDB		a <u>v</u> e Configuration <u>P</u> i User:admin(i	
Controller	Interfaces							Entries 1 - 6 of 6	New
General	Interface Name	VLAN Identifier							
Icons	client-vian-112	112	10.12.1.3	Dynamic	Dynamic AP Mar Disabled		::/128		
Inventory	management	100	10.12.1.3	Static	Enabled		::/128		
Interfaces	redundancy-management	100	10.5.1.65	Static	Not Supported				
Interface Groups	redundancy-port	untagged	169.254.1.65	Static	Not Supported				
Multicast	service-port	N/A	192.168.251.55		Disabled		::/128		
Network Routes	virtual	N/A	192.0.2.1	Static	Not Supported				
Fabric Configuration		2018 C.							
Redundancy									
Mobility Management									
Ports									
NTP									
CDP									
PMIPv6									
Tunneling									
IPv6									
mDNS									
Advanced									
Lawful Interception									

Figure 68	5520 WLC Controller Redundancy Management Interface Configuration
-----------	---

Figure 69 5520 WLC Controller Redundancy Global Configuration

cisco	MONITOR WLANS CONTROLLER	WIRELESS SEC	URITY MANA	AGEMENT C	<u>o</u> mmands	HELP	FEEDBACK	Sage Configuration Ping Logo	
Controller	Global Configuration								A
General Icons Inventory Interfaces Mutticast Network Routes Fabric Configuration Redundancy Global Configuration Peer Network Route Mobility Management Ports NTP COP PMIPv6	Redundancy Mgmt Ip 1 Peer Redundancy Mgmt Ip Redundancy port Ip Redundancy port Ip Redundant Unit Mobility Mac Adress Keep Alive Retries (3 - 10) ² Peer Search Timer (100 - 1000)-2.3 Keep Alive Retries (3 - 10) ³ Peer Search Timer (60 - 300) Management Gateway Fallover Link encryption SSO Service Port Peer Ip-4 Service Port Peer Ip-4 Service Port Peer Netmask <i>s</i>	10.5.1.65 10.5.1.66 169.254.1.65 169.254.1.65 Primary V 6C:AB:05:88:44:09 100 33 120 Enabled V Disabled V 192.168.251.56 255.255.0.0	milliseconds seconds						
 Tunneling IPv6 mDNS Advanced Lawful Interception 	1 Redundancy management and Pee 2 Configure the keep-ailve parameters 3 Configuring keep alive parameters 4 Peer service part IP address and th	ailli seconds between 10 when HA enabled migh	00 and 1000 in n t cause failover i	nultiple of 50. If RP link latence	y is high				

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...... 86 days 3 hrs 15 mins 51 secs System Timezone Location...... (GMT -5:00) Eastern Time (US and Canada) System Stats Realtime Interval..... 5 System Stats Normal Interval..... 180 Configured Country..... US - United States Operating Environment..... Commercial (10 to 35 C) Internal Temp Alarm Limits..... -10 to 80 C Internal Temperature..... +60 C Mgig Temp Alarm Limits..... -10 to 78 C Mgig Temperature..... +50 C External Temp Alarm Limits..... -10 to 71 C External Temperature..... +46 C Fan Status..... OK Fan Speed Mode..... Disable State of 802.11b Network..... Disabled State of 802.11a Network..... Enabled Number of WLANs..... 2 Number of Active Clients..... 0 OUI Classification Failure Count...... 5 Memory Current Usage..... 36 Memory Average Usage..... 36 CPU Current Usage..... 0 CPU Average Usage..... 0 Flash Type..... Compact Flash Card Flash Size..... 1073741824 Maximum number of APs supported..... 150 System Nas-Id..... WLC MIC Certificate Types..... SHA1/SHA2 Licensing Type..... RTU (Cisco Controller) > show redundancy summary Redundancy Mode = SSO ENABLED Local State = ACTIVE Peer State = STANDBY HOT Unit = Primary Unit ID = 00:87:64:8A:3F:80 Redundancy State = SSO Mobility MAC = 00:87:64:8A:3F:80 Redundancy Port = UP BulkSync Status = Complete

(Cisco Controller) >show sysinfo

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

5520:

Manufacturer's Name..... Cisco Systems Inc. Product Name..... Cisco Controller Product Version...... 8.10.105.0 RTOS Version..... 8.10.105.0 Bootloader Version..... 8.3.15.177 Emergency Image Version..... 8.3.143.0 OUI File Last Update Time..... Tue Feb 06 10:44:07 UTC 2018 Build Type..... DATA + WPS System Name..... IA-OG-5520-WLC-1 System Location..... System Contact..... System ObjectID...... 1.3.6.1.4.1.9.1.2170 Redundancy Mode..... SSO IP Address..... 10.5.1.55 IPv6 Address..... :: System Up Time...... 73 days 7 hrs 12 mins 7 secs System Timezone Location...... (GMT -5:00) Eastern Time (US and Canada) System Stats Realtime Interval...... 5 System Stats Normal Interval..... 180 Configured Country..... US - United States Operating Environment..... Commercial (10 to 35 C) Internal Temp Alarm Limits..... 10 to 38 C Internal Temperature..... +22 C Fan Status..... OK State of 802.11b Network..... Enabled State of 802.11a Network..... Enabled Number of WLANs..... 2 Number of Active Clients..... 2 OUI Classification Failure Count..... 21 Memory Current Usage..... 11 Memory Average Usage..... 11 CPU Current Usage..... 0 CPU Average Usage..... 0 Flash Type..... Compact Flash Card Flash Size..... 1073741824 Power Supply 1..... Present, OK Power Supply 2..... Absent/Failed Maximum number of APs supported..... 1500 System Nas-Id..... WLC MIC Certificate Types..... SHA1/SHA2 Licensing Type..... RTU (Cisco Controller) > show redundancy summary Redundancy Mode = SSO ENABLED Local State = ACTIVE

Peer State = STANDBY HOT

```
Unit = Primary

Unit ID = 6C:AB:05:88:44:09

Redundancy State = SSO

Mobility MAC = 6C:AB:05:88:44:09

Redundancy Port = UP

BulkSync Status = Complete

Link Encryption = DISABLED

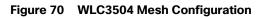
Average Redundancy Peer Reachability Latency = 264 Micro Seconds

Average Management Gateway Reachability Latency = 693 Micro Seconds
```

Mesh Configurations

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

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



cisco	MONITOR WLANS CONTROLLE	ER W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	FEE
Vireless	Mesh						
 Access Points All APs Direct APs Radios 802.11a/n/ac 802.11b/g/n 	General Range (RootAP to MeshAP) IDS(Rogue and Signature Detection)	12000	feet				
Dual-Band Radios Global Configuration	Backhaul Client Access	Enabled					
Advanced	Mesh DCA Channels	Enabled					
Mesh	Global Public Safety	Enabled					
ATF	Mesh Backhaul RRM	Enabled					
RF Profiles	Outdoor Ext. UNII B Domain Channels	Enabled					
FlexConnect Groups FlexConnect ACLs FlexConnect VLAN	Mesh RAP Downlink Backhau	ıl					
Templates	RAP Downlink Backhaul ²						
OEAP ACLs	O 5 GHz O 2.4 GHz						
Network Lists	Enable						
802.11a/n/ac				_			
802.11b/g/n	Convergence						
Media Stream	Mode	VERYFAST	\$				
Application Visibility	Channel Change Notification	🗹 Enabled					
And Control	Background Scanning	🕑 Enabled					
Country Timers	Ethernet Bridging						
Netflow	VLAN Transparent	Enabled					
▶ QoS	Security						
	Security Mode 2	PSK \$		0			
	PSK Provisioning	Enabled					
	Default PSK	Senabled					
	ADD New Provisioning Key						
	Provisioning Key						
	Description						
		ADD					
	Key Index TimeStamp		Description				
	1 Wed Nov 13 12:29:03	2019	testmesh2				



cisco	MONITOR WLANS CO	ONTROLLER	WIRELESS	SECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBAC
Wireless	Mesh							
 Access Points 								
All APs	General							
 Radios 802.11a/n/ac/ax 	Range (RootAP to MeshA	P)	12000	feet				
802.11b/g/n/ax Dual-Band Radios	IDS(Rogue and Signature Detection)		Enabled					
Global Configuration	Backhaul Client Access		Enabled					
Advanced	Mesh DCA Channels		Enabled					
Mesh	Global Public Safety		Enabled					
AP Group NTP	Mesh Backhaul RRM		Enabled					
ATF RF Profiles	Outdoor Ext. UNII B Dom Channels	nain	Enabled					
FlexConnect Groups	Mesh RAP Downlink I	Backhaul						
 FlexConnect ACLs 	RAP Downlink Backhaul	,						
FlexConnect VLAN Templates	S GHz 2.4 0							
Network Lists	Enable							
802.11a/n/ac/ax	Convergence							
802.11b/g/n/ax								
Media Stream	Mode	2000	VERYFAST	•				
Application Visibility And Control	Channel Change Notificat Background Scanning	tion	Enabled Enabled					
Lync Server								
Country	Ethernet Bridging							
Timers	VLAN Transparent		Enabled					
Netflow								
▶ QoS	Security							
	Security Mode ²		PSK \$					
	PSK Provisioning		Enabled					
	Default PSK		✓ Enabled					
	ADD New Provisioning H	(ev	. Enough					
	Provisioning Key							
	7990 304-54							
	Description		ADD					
	Key Index TimeStamp			Description				
	1 Tue Dec 10 0		8	testmesh2				

Configuration Steps

3504 and 5520

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



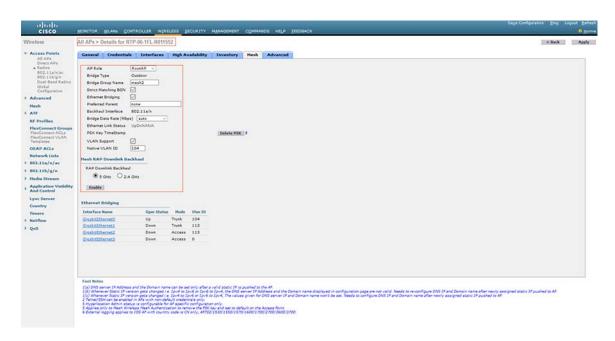


Figure 73 1552 MAP MESH Configuration

55	All APs > Details for	RTP-06-1FL-M0115	552					< Back	Apply
ess Points III APs Next APs	General Credent		High A	railability	Inventory	Hesh	Advanced		
adice 02.11a/n/ac 02.11b/g/n Nual-Band Radice Nual-Band Radice	AD Role Bridge Type Bridge Group Name Strict Matching BOI								
Configuration anced	Ethernet Bridging								
	Preferred Parent								
	Backhoul Interface	802.11a/n							
vofiles	Bridge Data Rate (N	tbps) auto 🛩							
Connect Groups	Ethernet Link Statu								
Connect ACLs Connect VLAN	PSK Key TimeStam	•			Delete PSK	E			
platen	VLAN Support								
PACLS	Native VLAN ID	104							
rork Lists 11a/n/ac	Hesh RAP Downlink	Backhaul							
11a/n/ac 11b/g/n	RAP Downlink Back	saul							
a Stream	● 5 GHz O	2.4 GHz							
ication Visibility Control	(Enable)								
Server	Ethernet Bridging								
irs.	Interface Name	Oper Status	s Node	Vian ID					
low	GrashitEthernetQ	Up	Trunk	104					
	GiusbitEthernet1 GiusbitEthernet2	Down	Access						
	GigsbitEthernet2	Down	Access						
	NOVER CONTRACTOR OF STATE	6-1-H	Access	v					
	Foot Notes								
	1(4) DNS server 1P Add 1/b) Whenever Static D	hese and the Domain nam Eversion cets chanced is	e can be se s. Iov4 to I	c only after a ovel or Jovel t	valid static IP is a Tov4, the DNS	pushed to the parver 17 Ado	was and the C	nain name displayed in configuration page are not valid. Reeds to re-configure DNS IP and Domain name after newly assigned static IP pushed to AP.	
	1(b) Whenever Static II	hess and the Domain nam Eversion gets changed is	e. I put to I,	ove or Jove t	a Ipv4, the DNS	server 17 Ado	freas and the D	rain rame displayed in configuration page are not valid. Needs to re-configure DNS 1P and Domain name after newly assigned static 1P pushed to AP. Domain name winit be are. Needs to configure DNS 1P and Domain name after newly assigned static 1P pushed to AP.	

Figure 74 6300 RAP MESH Configuration

altala			Segn Configuration Bog Logout Befret
CISCO	MONITOR WLANS CONTROLLER WIRELES	SS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK	Useriadmin(ReadWrite) 🙆 Bom
Wireless	All APs > Details for RTP-06-1FL-6300R01		< Back Apply
* Access Points All APs	General Credentials Interfaces H	tigh Availability Inventory Hesh Advanced	
	AP Bala Bedde	Derry Chaining Derry	water which hands are non-figure 1953. If and down in name yhat much assessed states 17 pushed to 44.

Figure 75 6300 MAP MESH Configuration

All APs > Details for RTP 06-TL E300M02 * Adday * Sail 00-110/00/00 0-00-100 Control 0-00-100 Con	aludo	100 Contra 1999-00 101	Colorest management com	-			Saya Caniforation ging Laport Bat
Access Plants Access Plants A Areas Sold Sild Nucleic Sold Sild Nucleic Balai Sold Sild Nucleic Balai Sold Sild Nucleic Balai Advanced Bidge Tops Owner Sold Sild Nucleic Bidge Tops Owner Advanced Bidge Tops Owner AF Decomp ITP Bidge Tops Owner Bidge Tops Owner Owner Bidge Tops Owner Decomp ItP Bidge Tops Owner<		MONITOR WLANS CO	ONTROLLER WIRE	LESS S	CURITY	MANAGEMENT COMMANOS HELP EEEDBACK	Useriadmin(ReadWrite) 🙆 B
All All All All Value V	Vireless	All APs > Details for R	RTP-06-1FL-6300M	102			< Back Appl
B02.113/v/c/m BA bala MaxbaD B03.113/v/c/m B04g Org Duan MaxbaD B03.113/v/c/m B04g Org Duan B04g Org Duan B03.113/v/c/m B04g Org Duan B02 B03.113/v/c/m B050 Org Duan B02 B03.113/v/c/m B050 Org Duan B02 B03.113/v/c/m B050 Org Duan Doing Orbing Duan B03.113/v/c/m B050 Org Duan Doing Orbing Duan B03.113/v/c/m B050 Org Duan Doing Orbing Duan B050 Org Duan B050 Org Duan Doing Orbing Duan B050 Org Duan B050 Org Duan Doing Orbing Duan B050 Org Duan B050 Org Duan Doing Orbing Duan B050 Org Duan Doing Orbing Duan Doing Orbing Duan B050 Org Duan Doing Orbing Duan Doing Orbing Duan B050 Org Duan Doing Orbing Duan Doing Orbing Duan B050 Org Duan Doing Orbing Duan Doing Orbing Duan B050 Orbing Duan Doing Orbing Duan Doing Orbing Duan B050 Orbing Duan Doing Orbing Duan Doing Orbing Orbing Duan	All APs	General Credentia	ls Interfaces	High Av	ailability	Inventory Hesh Advanced	
Advance/ Heak Sport Vet/Sing 60 // Compy 170 Optigr Chaining A Drough 170 Edwards 60 // Compy 170 Daily Chaining A TP Eschall Inferior 802.21 k0/vit Hocineset Compy Edwards 100 // Environment Compy P Fording Fileschment Compy Edwards 100 // Environment Compy Edwards 100 // Environment Compy P Fording Deset Immediate Inferiorment Compy Edwards 100 // Environment Compy P Fording Deset Immediate Inferiorment Compy Edwards 100 // Environment Compy P Fording Deset Immediate Inferiorment Compy Edwards 100 // Environment Compy D Lit // sig// Compy Teacher Inferiorment Compy Etwards 100 // Environment Compy Contry Etwards 100 // Compy Teacher Inferiorment Compy Open Advecter II 2 Open Access II 2 Open Access II 2 Immed Stream Open Access II 2 Open Access II 2 Immed Stream	802.11h/g/n/av Dual-Band Radies	Bridge Type	Outdear				
Net Charmet Brodping Output Data AP Groups (MP) Professe (Mp) Professe (Mp) Professe (Mp) Bodp Lots Acc (Mp) Bodp Lots Acc (Mp) Bit Professe Bodp Lots Acc (Mp) Bodp Lots Acc (Mp) Bit Professe Bodp Lots Acc (Mp) Bodp Lots Acc (Mp) Bit Professe Bodp Lots Acc (Mp) Bodp Lots Acc (Mp) Bit Professe Bodp Lots Acc (Mp) Bodp Lots Acc (Mp) Bit Professe Bodp Lots Acc (Mp) Bodp Lots Acc (Mp) Bit Professe Bodp Lots Acc (Mp) Bodp Lots Acc (Mp) Bit Professe Bodp Lots Acc (Mp) Bodp Lots Acc (Mp) Bit Acc (Mp) Nuk VAN ID Dio Hot (Mp) Bit Acc (Mp) Bodp Lots Acc (Mp) Bodp Lots Acc (Mp) Bit Acc (Mp) Bodp Lots Acc (Mp) Bodp Lots Acc (Mp) Bit Acc (Mp) Bodp Lots Acc (Mp) Bodp Lots Acc (Mp) Bit Acc (Mp) Bodp Lots Acc (Mp) Bodp Lots Acc (Mp) Bit Acc (Mp) Bodp Lots Acc (Mp) Bodp Lots Acc (Mp) Bit Acc (Mp) Bodp Lots Acc (Mp) Bodp Lots Acc (Mp) Bit A			And the second s				
AP Crog NPD Perfere Parent Inter AFT Bickhait Decisie Inter Bickhait Decisie Bickhait Decisie Inter File Cancet Charge Ether State Inter File Cancet Charge Ether State Inter Bickhait Decisie Inter Inter Bickhait Decisie <						Datay Chaining	
ATF Belakal Interfee BO21114/3/4E Brog Date State (1092) Solid State (1092) Solid State (1092) FilesCannet (Line States (1095) Belakal Piter (1092) Belakal Piter (1092) FilesCannet (Line States (1095) Belakal Piter (1092) Belakal Piter (1092) FilesCannet (Line States (1095) Belakal Piter (1092) Belakal Piter (1092) FilesCannet (Line States (1095) Belakal Piter (1092) Belakal Piter (1092) FilesCannet (Line States (1092) Belakal Piter (1092) Belakal Piter (1092) FilesCannet (Line States (1092) Belakal Piter (1092) Belakal Piter (1092) Boot (1102) FilesCannet (1002) Belakal Piter (1092) Belakal Piter (1092) Boot (1102) FilesCannet (1002) FilesCannet (1002) FilesCannet (1002) State (1102) FilesCannet (1002) FilesCannet (1002) FilesCannet (1002)							
NP Profile		Backhaul Interface	802.11a/n/ac				
FlacCannet Compo Behnet Lik Statis Upbrillip PSL Connet X ACIS PSL K (or mestane) PSL K (or mestane) PSL Connet X ACIS PSL K (or mestane) PSL K (or mestane) PSL Connet X ACIS Noine X ACIS ID ID- PSL K (or mestane) Noine X ACIS ID ID- PSL K (or mestane) Noine X ACIS ID ID- PSL K (or mestane) S O (or O) 2 - 0 O (or mestane) PSL K (or mestane) PSL K (or mestane) S O (or O) 2 - 0 O (or mestane) PSL K (or mestane) Particular X (or mestane) O (or S S O (or O) 2 - 0 O (or mestane) PSL K (or mestane) Particular X (or mestane) O (or S S O (or O) 2 - 0 O (or S S O (or O) 2 - 0 O (or S S O (or O) 2 - 0 O (or S S O (or O) 2 - 0 O (or S O (or O) 2 - 0 O (or S S O (or O) 2 - 0 O (or S S O (or O) 2 - 0 O (o		Bridge Data Rate (Mbp	pa) auto	~			
Flactioner Flactio		Ethernet Link Status	UpDnUpUp				
Templation Natro VLAN 1D Total Methods Lists Heak RAP Ownikk Eackhail RAP Ownikk Eackhail Agabactus VLukhity Imake Imake Agabactus VLukhity Imake Imake Station VLukhity Imake Imake Agabactus VLukhity Imake Imake Station VLukhity Imake Imake Agabactus VLukhity Imake Imake Station VLukhity Imake Imake Sta		PSK Key TimeStamp				Delete PSK 2	
Network laists Heak KAP Downlink Bickhaul 202.11//g/n/ar/ar RAP Downlink Bickhaul RAP Downlink Bickhaul Add Downlink Bickhaul RAP Downlink Bickhaul Bickhaul Raphichaul Bickhaul	FlexConnect VLAN	VLAN Support					
B02.11a/g/a/cac Henk RAP Ownikk ExcMail B02.11b/g/a/ax RAP Ownikk ExcMail B02.11b/g/a/ax S 0 H 0 2.4 0 H Applexture Visuble? Imake Tender Ethernet Endging Control Generation Of the Visuble? Fare Visuble ExcMail 0 po State Note Fare Visuble ExcMail 0 point Accesse 113 Fare Visuble ExcMail 0 point Accesse 113		Native VLAN ID	104				
ADD:11h/gr/av/av BD:11h/gr/av		Nesh RAD Downlink Re	without				
Workshop Syndam		Contraction of the second					
Application Visability Institute And Control Institute Visability Institute Country Ethernet Endiging Tensers Institutement Stabilithtement Oge State Retflow Stabilithtement Ops Stabilithtement Op Access Country Access	10.00 C 10.00 C 10.00						
And Central Linkement Events Favore Events Hindging Tenners Enderface Name Oper Status Node Visa 10 Netflow Schaftstammel 0 09 Track 104 QeS Schaftstammel 0 09 Access 133 Schaftstammel 0 09 Access 133		€ 5 GHz ∪ 2.4	4 GHz				
Country Ethernet Bridging Timers Interface Name Oper Status Node Visa ID Netflow Significations Up Track 164 Qe6 Significations Up Access 133 General Country General Country Marcess 133		Enable					
Net/Flow Stubilitanni2 Up Tunk 104 QoS Stubilitanni2 Dom Access 113 Generation Stubilitanni2 Up Access 133							
QuS <u>Qualificantal</u> Down Access 113 <u>Qualificantal</u> Up Access 113							
Grabitithemen2 Up Access 113	Netflow						
	QoS						
		GigsbitEthernet3	Up				
		A REAL PROPERTY AND A REAL					
		1(a) DNS server IP Addres 1(b) Whenever Static IP vi 1(c) Whenever Static IP vi 2 Telrec/SSH can be enable 5 Myperfocation Admin ata	ersion gets changed i a ersion gets changed i a led in APs with non-def stus la configurable for	I put to 1 I put to 1 Put creden AF specific	v6 or Ipv6 : v6 or Ipv6 : lais enly. configuratio	to 1pv4, the DNS server IP Address and the Domain name displayed in configuration page are not valid. Ne to 1pv4, the values given for DNS server IP and Domain name work be set. Needs to configure DNS IP and to only.	eds to re-configure DRS IP and Domain name after newly assigned static IP pushed to M. Domain name after newly assigned static IP pushed to M.
Field Blokes I/d Difference (FI Address and the Domain name gain be activity of the a valid static (FI as pophed to the AM. I/d Difference (FI Address and the Domain name gain be activity of points to by AR (D O) annual (FI Address and the Domain name displayed in configuration page an intravalid field to the AM. I/d Difference (FI Address and the Domain name gain be activity of points to by AR (D O) annual (FI Address and the Domain name displayed in configuration page an intravalid field to the AM. I/d Difference (FI Address and the Domain name gain be activity of points to by AR (D O) annual (FI Address and the Domain name displayed in configuration page an intravalid field to the AR (D O) annual (FI Address and The Domain name displayed in configuration page an intravalid field to the AR (D O) annual (FI Address and The Domain name displayed in configuration page an intravalid field to the AR (D O) annual (FI Address and The Domain name displayed in configuration page an intravalid field to the AR (D O) annual (FI Address and The Domain name displayed in configuration page an intravalid field to the AR (D O) annual (FI Address and The Domain name displayed in configuration page an intravalid field to the AR (D O) annual (FI Address and The Domain name displayed in configuration page an intravalid field to the AR (D O) annual (FI Address and The Domain name displayed in configuration page and the Domain name displayed and the Domain displayed and the Domain name displayed and the Domain displayed and the Domain name displayed and the Domain displayed and the Domain name displayed and the Domain displayed and the Dom		5 Applies only to Heah Wi 6 External lopping applies 7 Power level 1: 4W, 2: 70	to 105 AF with country	v code is C1	only, AP702	lary and set to default on the Access Point. /1530/1550/1550/2600/1700/2700/3600/3700	

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.

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

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

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

Figure 76 3504 MAC Filter Configuration

ecurity	MAC Filtering						Apply New
AAA General * RADIUS Authentication Accounting Fathack DAS Downloaded AVP TACACS+	RADIUS Compacibile MAC Delimiter Local MAC Filters		(In the Radius Access Request with Mac A address.)	uthentication password is client	I MAC		Entries 1 - 9 of 9
LDAP Local Net Users	MAC Address	Profile Name	Interface	IP Address	Description		
MAC Fultering	04-da-d2-15-55-60	Any WLAN	management	unknown	1552-Rap-2		
Disabled Clients	20-31/24:71:20:80	Any WLAN	management	unknown	1552-AP-3		
User Login Policies AD Policies	24:31:24:71:22.60	Any WLAN	management	unknown	1552-AP-1		
Password Policies	20.31/24:71:64:60	Any WLAN	management	unknown	1552-AP-2		
Local EAP	6c:85:d2:ed 16:e0	Any WLAN	management	unknown	iw6300-rap-1		
Advanced EAP	6c (0) (d) ed (7)(04	Any WLAN	management	unknown	6300-map2		
Priority Order	5c 61 d3 ed (7:10	Any WLAN	management	unknown	IW6300-AP-2	•	
Certificate	dc:8c:37:35.89.60	Any WLAN	management	unknown	iw6300-rap-1		
Access Control Lists	dcille:37:35/ba/91	Any WLAN	management	unknown	IW6300-AP-2		
Wireless Protection Policies Web Auth TrustSec Local Policies OpenDNS Advanced							

Figure 77 5520 MAC Filter Configuration

ecurity	MAC Filtering						Apply New
AAA General • RADDUS Authentication Accounting Auth Cached Users Fallback ONS	RADIUS Competibile MAC Delimiter Local MAC Filters		(In the Radius Access Request with Mac A address.)	Authentication password is client's	a MAC		Entries 1 - 7 of 7
Downloaded AVP TACACS+	HAC Address	Profile Name	Interface	1P Address	Description		
LDAP Local Net Users	24:31:24:71:20:00	Any WLAN	management	unknown	1552-map2	•	
MAC Filtaring	24(31)24(71)64:60	Any WLAN	management	unknown	1552-map1		
Disabled Clients	58-21-78-98-62ic8	Any WLAN	management	unknown	teta-rap-2-6300		
User Logis Policies AP Policies	Sci8bid2ied/6ieQ	Any WLAN	management	unknown	Root	•	
Password Policies	6c(8b)d3(ed-f7)04	Any WLAN	management	unknown	Mag-2		
Local EAP	Sci@bid2ied/7:10	Any WLAN	management	unknown	Mag-1		
Advanced EAP	dci8ci37/33,89.60	Any WLAN	management	unknown	rest-radie	•	
Priority Order							
Certificate							
Access Control Lists							
Wireless Protection Policies							
Web Auth							
TrustSec							
Local Policies							
Umbrella							
Concoreita							

WLAN Configurations

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

3504

Figure 78 3504 WLC Controller Interface Configuration

ontroller	Interfaces						Entries 1 - 6 of 6	New-
General	Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Hanagement	IPu6 Address		
Inventory	chent-vian-12	112	10.12.1.2	Dynamic	Disabled	1/128		
aterlaces	managament	100	10.5.1.53	Static	Enabled	1/128		
Interface Groups	redundance: management	100	10.5.1.63	Static	Not Supported			
fulticast	tecknikance: earl		169.254.1.63	Static	Not Supported			
Network Routes	annies: set		192.168.251.53	Static		n/128		
Fabric Configuration	<u>kattir</u>	N/A	192.0.2.1	Static	Not Supported			
Redundancy								
Server								
Server Hobility								
Internal DHCP Server Hobility Hanagement Ports								
Server Hobility Hanagement Ports								
Server Hobility Hanagement Ports NTP								
ierver tobility fanagement Ports ITP IDP								
lerver tobility fanagement Ports ITP IDP PUIPv6								
Server Hobility Hanagement Ports NTP CDP PHIPv6 Funneling								
lerver tobility fanagement Ports ITP IDP PUIPv6								

Figure 79 3504 WLC Controller Management Interface Configuration



cisco	MONITOR WLAN C	ONTROLLER WIRELESS SECURITY	MANAGEMENT C	OMMANDS HELP	FEDRACK	Saya Configuration 2	ing Lague
ontroller	Interfaces > Edit					<	lack Aj
General							
Icons	General Information						
Inventory	Interface Name	client-vlan-12					
Interfaces	MAC Address	00:87:64:8a:3f:81					
Interface Groups	NAC AVERES	0010110410101					
Hulticast	Configuration						
Network Routes Fabric Configuration							
tedundancy							
sternal DHCP		0					
Server	NAS-ID	P3/94					
Hobility	Physical Information						
lanagement orts	Port Number	1					
TP	Backup Port	0					
0P	Active Port	1					
PHIPv6	Enable Dynamic AP Management						
unneling	Interface Address						
Pv6	VLAN Identifier	112					
NONS	IP Address	10.12.1.2					
Advanced	Netmask	255.255.255.0					
	Gatenay	10.12.1.1					
	IPv6 Address	11					
	Prefix Length	128					
	IPv6 Gateway	[23					
	Link Local IPv6 Address	fe80::287:648;fe8e:380/64					
	DHCP Information						
	Primary DHCP Server	10.5.1.20					
	Secondary DHCP Server						
	OHCP Proxy Mode	Enabled ~					
	Enable DHCP Option 82						
	Enable DHCP Option 6 OpenDNS						
	Access Control List						
	ACL Name	none v					
	URLACL	nane ~					
	mDNS						
	mONS Profile	none v					
	External Hodule						
	30 VLAN						
	Note: Changing the Interface	parameters causes the WLANs to be a may result in loss of connectivity for					

Figure 80 3504 WLC Controller Dynamic Interface Configuration

Figure 81 3504 WLAN Configuration

ANs	WLANs > Edit 'OG-SSID-1'	< Back Apply	
WLANS		5.000	
YLANs ILLAns dysacced	Texnelly Q: Paky-Happing Advanced Type W.A.W. Status Status Type W.A.W. Status Status Security Paky-Happing Advanced Status Security Paky-Happing Status Status Development Control Status Status Maximum Status Status Status Status Maximum Status Status Status Status Status Maximum Status Status Status Status Status Status Maximum Status Status<		

Figure 82 3504 WLAN Security Configuration

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MONORMENT COMMANDS HELP EEEDBACK	Sage Configuration Bing Logout Bafest
WLANs	WLANs > Edit 'OG-SSID.1'	< Rack Apply
* WLANs	General Security QoS Policy-Mapping Advanced	
+ Advanced	Layer 2 Layer 3 AAA Servers	^
	Lyer2 Security 1 WAX-NAVA MAC Fridaring 1 WAX-PRAZ Fet Transition California Part Transition California VMA Fridaring 1 California WAX-Provide Transition California VMA Fridaring 1 California WAX Fridaring 1 Calif	

5520

Figure 83 5520 WLC Controller Interface Configuration

CISCO	MONITOR WLANS CONTROLLED	e wireuss sec	CURITY MANAGEN	ных сонимы	S HELP ETERBACK			Useriadmin(ReadW	vite) 🔒 Hom
ntroller	Interfaces							Entries 1 - 6 of 6	New
ieneral									
cons	Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Hanagement	1Pv6 Address			
nventory	clientislen:112	112	10.12.1.3	Dynamic		::/128			
sterfaces	management	100	10.5.1.55	Static		11/128	and the second se		
sterface Groups	reducidance-management	100	10.5.1.65	Static	Not Supported				
ulticast	tedundans-cost		169.254.1.65	Static	Not Supported				
etwork Routes	Antick: Kill		192.168.251.55	Static		:/128			
	xistual	N/A	192.0.2.1	Static	Not Supported				
abric Configuration									
edundancy									
obility anagement									
orts									
TP.									
OP									
HIPv6									
nneling									
Pv6									
DNS									
dvanced									
wful Interception									

ahaha					Saya Configuration Bing Lapout 5
CISCO	MONITOR MUANS CONTI	IOLLER WIRELESS SECURITY MANAGEME	NT COMMANDS HELP ETERBACK		Userradmin(ReadWrite) 🔒
ntroller	Interfaces > Edit				< Back Ap
General					
lcons	General Information				
Inventory	Interface Name m	anagement			
nterfaces	MAC Address 6	ciab:05:88:44:09			
Multicast	Note: Changing Management Inter	face accributes are not allowed when			
Network Routes					
Fabric Configuration	Configuration				
Redundancy	Quarantine				
Hobility	Quarantine Vian Id 0				
Hanagement	NAT Address				
Ports	Enable NAT Address				
COP	Interface Address				
PHIPv6	VLAN Identifier	100			
funneling	IP Address	10.5.1.55			
IPv6	Netmask	255.255.255.0			
mDNS	Gateway	10.5.1.1			
Advanced	IPv6 Address	11			
Lawful Interception	Prefix Length	128			
	IPv6 Gateway	0			
	Link Local IPv6 Address	fe80116ea813#ife881440a/64			
	Physical Information				
	Port Number	1			
	Backup Port	0			
	Active Port Enable Dynamic AP	1			
	Management				
	DHCP Information				
	Primary DHCP Server	10.5.1.20			
	Secondary DHCP Server	0.0.0			
	DHCP Proxy Mode	Disabled ~			
	Enable DHCP Option 82 Enable DHCP Option 6				
	OpenDNS				
	Access Control List				
	ACL Name	(nene v)	1Pv6 ACL Name	none v	
	URL ACL	[none v]			
	mDNS				
	mONS Profile	8046 V			

Figure 84 5520 WLC Controller Management Interface Configuration

Figure 85 5520 WLC Controller Dynamic Interface Configuration

allahi						Says Configuration Eng Logout
CISCO	MONITOR MLANS	CONTROLLER WIRELESS	SECURITY MANAGEMENT	COMMANDS HELP	EEDBACK	Useriadmin(ReadWrite) 🧖
ontroller	Interfaces > Edit					< Rack A
eneral						
come	General Information					
wentory	Interface Name	client-vlan-112				
sterfaces	MAC Address	6c/ab/05/88/44/0a				
nterface Groups	AND ADDRESS	2010/02/02/04/04				
ulticast etwork Routes	Configuration					
bric Configuration	Guest Lan					
dundancy	Quarantine					
obility	Quarantine Vian Id	0				
anagement	NAS-ID	none				
irts	Physical Information					
(P	Port Number	3				
0P	Backup Port	2				
HIPv6	Active Port	1				
unneling Pvő	Enable Dynamic AP Management					
DNS	Interface Address					
dvanced	VLAN Identifier	112				
wful Interception	IP Address	10.12.1.3	1			
	Netmask	255.255.255.0	1			
	Gatemay	10.12.1.1	1			
	IPv6 Address	FT				
	Prefix Length	128	1			
	IPv6 Gateway	23				
	Link Local IPv6 Addr	ess fe80::6eab:5#fe88:	440a/64			
	DHCP Information					
	Primary DHCP Server	10.5.1.20	1			
	Secondary DHCP Ser	ver	1			
	DHCP Prexy Mode	Enabled ~				
	Enable DHCP Option					
	Enable DHCP Option OpenONS	• •				
	Access Control List					
	ACL Name	none 😔				
	URL ACL	none ~				
	mDNS					
	mDNS Profile	nane	v			
	External Hodule					
	30 VLAN					
		ace parameters causes the WLANS				

Figure 86 5520 WLAN Configuration

		User:admin(ReadWrite) 9 Home
VLANs	WLANs > Edit 'OG-SSID-1'	< Back Apply
WLANs WLANs	General Security QoS Policy-Happing Advanced	
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 client-vlan-112 v	
	Group(G) Cremevian-112	
	Multicast Vlan Enabled	
	Broadcast SSID 🛛 Enabled	
	NAS-ID none	
	Lobby Admin Access	
	Food Notes I Web Philips sample do used in combination with Place I Web Philips and the set of the embination with Place I Web Philips and the set of the embination with Place I Web Philips and the embination of thembination of the embination of the embination of the embination	

Figure 87 5520 WLAN Security Configuration

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	Sage Configuration Ping L Userradmin(ReadW	
/LANs	WLANs > Edit 'OG-SSID-1'	< Back	Apply
WLANs WLANs	General Security QoS Policy-Happing Advanced		
Advanced	Layer 2 Layer 3 AAA Servers		^
		^	
	Layer 2 Security 1 WPA2+WPA3 V		
	Security Type Personal V		
	MAC Filtering 1		
	AutoCoefig iPSK Enable		
	WPA2+WPA3 Parameters		
	Policy Wwpag Dwpag		
	Encryption Cipher CCMP128(AES)		
	Fast Transition		
	Fast Transition Enable v		
	Over the DS		
	Reassociation Timeout 20 Seconds		
	Protected Management Frame		
	PMF Optional ~		23
	- Annalised		
	For Notes		
	We holicy cannot be used in combination with lifese 2(a) Faccionent Local Switching in not supported with Overnide Interface ACLs 2(a) When Resonnets Local Switching in an esupported with Overnide Interface ACLs 2(b) When Resonnets Local Switching in an esupported with Overnide Interface ACLs 2(c) When Resonnets Local Switching in an esupported with Overnide Interface ACLs 2(c) When Resonnets Local Switching in an esupported with Overnide Interface ACLs 2(c) When Resonnets Local Switching in an esupported with Overnide Interface ACLs 2(c) When Resonnets Local Switching in an esupport Interface ACLs 2(c) When Resonnets Local Switching is a configured 3(c) Resonnet Local Switching in an esupport and an estimation (Interface and Mark and General Walk and Walk and General Walk walk of		N redirect.

Mobility Group

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

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

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

Figure 88 WLC3504 Mobility Group Configuration

troller	Static Mobility Group	Members						New	EditA
eneral cons	Local Hobility di Group di	ifault							
iterfaces	MAC Address	IP Address(Ipv4/Ipv6)	Group Name	Multicast IP	Status	Hash Key	Secure Hobility	Data Encryption	
iterface Groups	00:87:64:8#:3/:80	10.5.1.53	default	0.0.0.0	Up	none	NA	NA	
ulticast	6ciab:05:88:44:09	10.5.1.55	default	0.0.0.0	Up	none	Disabled	NA	
etwork Routes	d4:e8:80:b2:d7:4b	10.5.1.51	default	0.0.0.0	Control and Data Path Down	none	Enabled	Disabled	
The second second second second									
dundancy									
abric Configuration edundancy sternal DHCP stver									
edundancy iternal DHCP rever sobility snagement tobility Configuration tobility Oroups tobility Anchor Config									
dundancy ternal DHCP rver sbility magement obility Configuration obility Anchor Config ulticast Messaging									
edundancy iternal DHCP inver obility snagement obility Configuration obility Ancher Config ulticast Messaging orts									
edundancy ternal DHCP rver sobilty snagement sobilty Configuration sobilty Anchor Config ubilicast Messaging ubicast Messaging ubicast Messaging pp									
dundancy ternal DHCP ever builty inagement obility Configuration obility droups obility Anchor Config- ulticast Messaging ets P P HIPv6									
Hundancy ternal DHCP rver biblity inagement sbility (Tanga sbility Ancher Config uticizest Messaging trts p p IIPv6 inmeling									
edundancy iternal DHCP prover anagement ability Configuration ability Configuration ability Configuration ability Configuration ability Configuration anagement pp pp pp pp pp pp pp pp pp p									
edundancy ternal DHCP ever source ballity snagement solity Configuration solity Orapis solity Ancher Config uticizest Messaging uticizest Messaging tris pp sp HIPv6 mmeling									

Figure 89 WLC5520 Mobility Group Configuration

cisco	MONITOR MUNIS	CONTROLLER WIRELESS	SECURITY	MANAGEMENT COMMAND	S HELP SEE	MACK				Jeenadmin(ReadWr	ite) 🖪 Ho
Controller	Static Mobility Grou	p Members								New-	EditAll
General Icons	Local Hobility Group	default.									
Inventory Interfaces	HAC Address	IP Address(Ipv4/Ipv6)	Group Name		ulticast IP	Status	Hash Key	Secure Hobility	Data Encryption	High Cipher	
Interface Groups	6ciab:05:88:44:09	10.5.1.55	default	0	0.0.0	Up	none	NA	NA	NA	
Hulticast	00:87:64:81:31:80	10.5.1.53	default	0	0.0.0	Up	none	Disabled	NA	NA	
Network Routes	d4(e8(80)b2)d7(4b	10.5.1.51	default	0	0.0.0	Control and Data Path Down	none	Enabled	Enabled	Disabled	
Fabric Configuration											
Redundancy											
Mobility Groups Mobility Anchor Config Multicast Messaging											
Ports											
NTP											
CDP											
PHIPV6											
Tunneling											
1Pv6											
mDNS											
Advanced											
Lawful Interception											

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

3504

(Cisco Controller) > show mobility summary

Mobility Protocol Port Default Mobility Domain	
Multicast Mode I	
Mobility Domain ID for 802.11r	0xac34
Mobility Keepalive Interval 1	10
Mobility Keepalive Count	3
Mobility Group Members Configured	3
Mobility Control Message DSCP Value (0

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

5520

(Cisco Controller) > show mobility summary

Default Mobility Do Multicast Mode DTLS Mode Mobility Domain ID Mobility Keepalive Mobility Keepalive Mobility Group Memb	ort main for 802.11r Interval Count ers Configured ssage DSCP Value	default Disabled Disabled 0xac34 10 3 3	
Controllers configu	red in the Mobility	Group	
MAC Address	IP Address		Group Name
Multicast IP		Status	
00:87:64:8a:3f:80	10.5.1.53		default
0.0.0.0		Up	
6c:ab:05:88:44:09	10.5.1.55		default
0.0.0.0		Up	

Ethernet Bridging

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

Ethernet bridging should be enabled for the following scenarios:

- Integration of Emerson Sensors
- Video Surveillance

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

3504

Figure 90 1552 MAP Ethernet Bridging Configuration

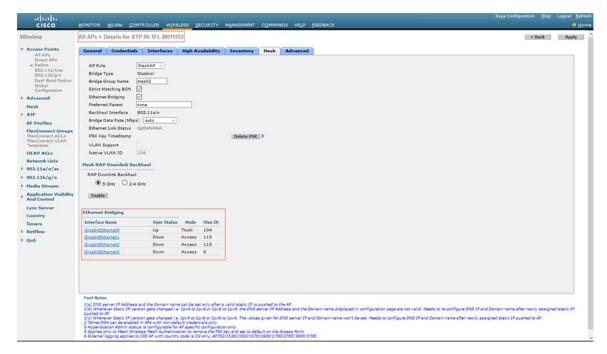


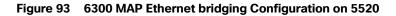
Figure 91 1552 RAP Ethernet Bridging Configuration

cisco	MONITOR WLANS CONT	ROLLER WIRE	uss go	CURITY	MANAGEMENT	сония	NDS HELP	Sage Configuration Ping L EEEDBACK	0
reless	All APs > Details for RTP	06-1FL-R0115	52					< Back	Apply
Access Puints Air Ary Predia Predia Configuration Advanced Bash Advanced Heah Art FiseConnet Croups FiseConnet Cours FiseConnet Cours FiseConnet Cours FiseConnet Cours FiseConnet Cours FiseConnet Cours Bash Network Lists B03.111/g/a B03.111/g/a	Bridge Trye Bridge Grup Name Bridge Grup Name Bridge Grup Name Bridge Grup Name Brackhal Stark (May) Ethernet Bridge Braker Bridge Dara Rate (May) Ethernet Link Statur (May) PSK Kay TimsStamp VLAN Sigpert VLAN ID 1 Heah RAP Downlike Backki RAP Dominike Backkal Brack Statur (May)	 22.11a/n auto ~ DDnNANA D4 haul	High Avi	sifability	Towestory Delete PSX	Hesh	Advanced		
nd Control ync Server	Enable								
ountry	Ethernet Bridging								
mers	Interface Name	Oper Status		Vian ID					
etflow	GigabitEthernet0 GigabitEthernet1	Up Down	Trunk	104					
5	GigabitEthernet2	Down	Access						
	Giosbit[themet2	Down	Access						
	pushed to AP.	on gets changed i e on gets changed i e n Afs with non-defs i is configurable for ss Mesh Authentics	Ipv4 to Ip Ipv4 to Ip suit credenti Af specific stion to reme	vili ér Ipvili ti vili er Ipvili ti als enly. configuratio va the PSK i	o Ipv4, the DNS : o Ipv4, The value n only, lav and sat to de	ierver IP A s given for fault on the	Sdress and the DNS server IP Access Point	Domain name displayed in configuration page are not valid. Needs to re-configure DNS 1P and Domain name after newly assigned and Domain name work be set. Needs to configure DNS IP and Domain name after newly assigned static IP pushed to AP. 2000.	matic I



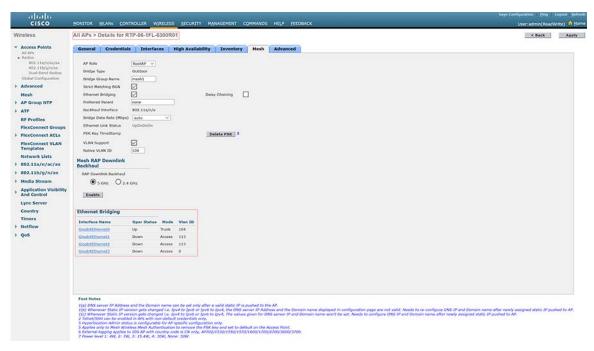
Access Points An Ady Redux Redux Redux Redux for Acades David for Acades Cable Configuration Advanced Meah AP Geoph NTP ATF RF Profiles	Mesh Banar (Dock/Eto Hes/A/E) DOS(Dock/Eto Hes/A/E) DOS(Dock/Eto Hes/A/E) Bachad Clieft Alcess Hesh DCA Obsceles & Cabal Adat Safety Hesh Eschar/REH Ocksor 41: UBI Bomen	13000 Neet Crubbo Crubbo Crubbo Crubbo		
All Are Bather NR2.513.0/r/sc/as NR2.513.0/r/sc/as Dual: band flades Citized Configuration Advanced Mesh AP Group NTP ATP RF Profiles	Ranja (BookAP to MexhAP) IDE(Book and Signature Defection) Bockhard Clieft Acress Heah DCA Channels ³ (Johal Public Safety Heah Bochard RBH Outdoor ERL WILL B Donse	Crubbot		
N2.213/h/kc/ax N2.213/h/kc/ax Dual-band Radies Cabled Configuration Advanced Mesh AP Group NTP ATP RF Profiles	105(Rope and Signature Detection) Bochaul Client Acons Heah DCA Channels ⁸ Gotal Public Safety Heah Dickhaul RBM Oudsour Eat, UNIT B Damain	Crubbot		
FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates Network Lists	Channels Mesh RAP Downlink Backhaul RAP Countink Backhaul ² (© 5 GHz) 2.4 GHz DOWNLINE	Cutled Cutled		
802.11a/n/ac/ax	Convergence			
802.11b/g/n/ax Media Stream Application Visibility And Control Lync Server	Hode Channel Change Notification Beckground Scanning	VRWAST v fination tratien		
Country	Ethernet Bridging			
Timers Netflow	WAN Transparent	C tracked		
Qos	Security			
	Security Mode 2 HSC Provinsions Defruit FIGE ADD Rever Provinsioning Kry Provinsions Kry Revery Eddex Kry Eddex Time Dec (10.45.2.50.2015) 2 Woll Rev 13 11:42.55.201 Control Mod. Provinsioning Sciences Mod. P		8	

5520



cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK								Saye Configuration Eng Lopout Bet User:admin(ReadWrite) 🕅 H											
Vireless	All APs > Details fo	r RTP-06-1FL-	-6300M)2														< Back	1	Apply
A Access Points A A Ars A Access Points A A Ars A Redos BD: 11 Montal BD: 11 Montal A Ars A Ars A Advanced Mesh A Advanced Mesh A Arr RF Profiles PiexConnect Groups PiexConnect ACLs PiexConnect ACLs PiexConnect ACLs PiexConnect ACLs PiexConnect ACLs PiexConnect ACLs PiexConnect ACLs Montal B 02:111a/n/ac/ax B 02:111a/n/ac/ax	All Area Decision to Concern General Creden All Rule Indep Type Bridge Group Area Strict Hatchards (SIN Element Bridging Prefamed Areas) Element Bridging Prefamed Areas Bridge Date State Element Link Sthis Element Bridging Prefamed Areas Bridge Date State Strict Walk Distance Market All Distance Rule Desminish Rasha State State Castal	tials Interfa MeshAB Outdoor mesh2 Pome 602.11s/n/e bes) autometh2 104 104	ices	High Availabil	by Invest		fesh	Advanced												Арру
Lync Server																				
Country Timers	Ethernet Bridging																			
Netflow	Interface Name	Oper Status																		
	GlosbitEthernet@	Up	Trunk	104																
QoS	GloabitthernetI	Down	Access																	
	Giosbitthemet2 Giosbitthemet3	Up	Access																	
	Foot Notes 1(a) DNS server IP Add 1(b) Whenever Static II 1(c) Whenever Static II 1(c) Whenever Static II 5 Hyperkadion Admin	P version gets chan P version gets chan vabled in APs with n	iged i.e. 3) ged i.e. 1) ion-defau	will to Ipv6 or Ip will to Ipv6 or Ipv t credentials only	6 to Ipv4, the 6 to Ipv4, The	DNS server	IP ASS	ves and the De	nain name I Domain n	displayed ame won3	d in config 17 be set. i	puration pag	ge øre not va sofigure DNS	elid. Needs to re IP and Domain	-configure DN name after n	S IP and Dom wly assigned	sin nome ofter n static IP pushed	ewly assigned state to AP.	k IP a	ushed to AF







սիսիս		e oversee oneres		100000000000	Service Sciences of the	Sage Configuration Ping Logout Refresh
CISCO	MONITOR WLANS CONTROLL	ER WIRELESS SECURIT	Y MANAGEMENT	COMMANDS	HELP FEEDBACK	User:admin(ReadWrite) 🔒 Home
Wireless	Mesh					Apply
Access Points All APs Radios	General					
802.11a/n/ac/ax	Range (RootAP to MeshAP)	12000 feet				
802.11b/g/n/ax Dual-Band Radios	IDS(Rogue and Signature Detection)	Enabled				
Global Configuration	Backhaul Client Access	Enabled				
Advanced	Mesh DCA Channels	Enabled				
Mesh	Global Public Safety	Enabled				
AP Group NTP	Mesh Backhaul RRM	Enabled				
▶ ATF	Outdoor Ext. UNII B Domain Channels	Enabled				
RF Profiles						
FlexConnect Groups	Mesh RAP Downlink Backhau	ul 🦲				
FlexConnect ACLs	RAP Downlink Backhaul 2					
FlexConnect VLAN Templates	● 5 GHz ○ 2,4 GHz					
Network Lists	Enable					
802.11a/n/ac/ax	Convergence					
802.11b/g/n/ax	No. of the second s					
Media Stream	Mode	VERYFAST	Y			
Application Visibility And Control	Channel Change Notification Background Scanning	Enabled				
Lync Server						
Country	Ethernet Bridging					
Timers	VLAN Transparent	Enabled				
Netflow	von nonsporen	L Enabled				
▶ QoS	Security					
	Security Mode 2	PSK V				
	PSK Provisioning	Enabled				
	Default PSK	Enabled				
	ADD New Provisioning Key	Lindoled				
	Provisioning Key					
	Description					
		ADD				
	Key Index TimeStamp	Description				
	1 Tue Dec 10 04:53:30 2	Manufacture and a second				
	2 Wed Nov 13 11:42:55	_				
	External MAC Filter Authorization	Enabled				
	Force External Authentication	Enabled				
	LSC Only MAP Authentication	Enabled				
	Server ID Server Address	(Ipv4/Ipv6)	Port	Enabled	1	
	1 10.5.1.19		1812			

BGN

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

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

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

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

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

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

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

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

- If BGN is mismatched, the AP will join a mesh network of another BGN, but after 15 minutes, the AP will drop AWPP and scan for its own BGN link. BGN mismatch will incur instability; adds a higher AWPP priority on BGN group does not strand AP with misconfigured 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.

Note: A general Mesh Deployment recommendation includes:

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

Figure 96 6300 RAP Bridge Group Name Configuration

CISCO	MONITOR WLANK CONTROLLER	WIRELESS ;	SECURITY	MANAGEMENT COMMANDS HELP EEEDBACK	Useriadmin(ReadWrite) 🙆 🗠
fireless	All APs > Details for RTP-06-1FL-6	0009201	-		< Back Appl
Access Points All APs	General Credentials Interfa	es High A	vailability	Inventory Hesh Advanced	
Radios 002.11a/n/ac/as 002.11a/n/ac/as 002.11a/n/ac Dual-Band Radios Olobal Configuration Advanced Hesh AP Group NTP	AP Role RockD Bridge Type Outdoor Bridge Group Name mesh1 Strict Matching BDN - Ethemset Bridging Profered Parent Backhaol Interface 802.114/n/et]		Datas Chaning	
ATF RF Profiles	Bridge Data Rate (Mbps) auto	-			
RF Protes	Ethernet Link Status UpD=D=D=	1			
FlexConnect ACLs	PSK Key TimeStamp			Delete PSK 4	
FlexConnect VLAN Templates	VLAN Support				
Network Lists 802.11a/n/ac/ax	Hesh RAP Downlink Backhaul				
002.11b/g/n/ax	RAP Downlink Backhaul				
Hedia Stream	S GHz O 2.4 GHz				
Application Visibility And Control	Enable				
Lync Server Country	Ethernet Bridging				
Timers	Interface Name Oper 1				
Netflow	GigshitEthernetQ Up	Trynk	104		
QuS	GigabitEthernet1 Down OlcabitEthernet2 Down	Access			
	GigshitEthernet3 Down	Access			
	1(c) Whenever Static IP version gets chan, 2 Teinst/SSH can be enabled in APs with n S Hyperiocation Admin status is configure 5 Applies only to Mesh Wireless Hesh Auc	ped i.e. Ipv4 to red i.e. Ipv4 to r-default crede tie for AP specif ventication to re	Ipv6 or Ipv6 t Ipv6 or Ipv6 t ntials only. Is configuratio move the PSX i	 Ipv4, the DNS server IP Address and the Domain name displayed in configuration page. Ipv4, The values given for DNS server IP and Domain name won't be set. Reeds to configuration page. 	an ner val d. Nach is in nonfigure DNI 19 and Denam nerna after newly assigned static 19 pushed in AP. Sport DNI 19 and Domain name after newly assigned assis: 19 pushed in AP.

Figure 97 6300 MAP Bridge Group Name Configuration

cisco	MONITOR WLANK CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMAN	DS HELP	Saye Cenfiperation _Bing Lo DBACK Usersadmin(ReadWir	
Wireless	All APs > Details for RTP-06-1F	-6300M02						Apply
Access points Access points Access Access Solar (1) of the Solar (1) of the Solar (1) of the Other (1) of the AP Perfect AP	AP Bale MultiP Didge Type Ovdeser Bridge Type News Mesh Bridge Type News Mesh Bridge Type News Mesh Bridge Type News Mesh Bridge Over Reserved States Dharner (Long Over Reserved States) (Second Bridge Over Reserved States) (Second Bridge Over Reserved States) RAD Dynamick Backhard RAD Dynamick Backhard RAD Dynamick Backhard RAD Dynamick Backhard RAD Dynamick Backhard RAD Dynamick Backhard Batterice News Operatority States Ethermet Bindging Taterice News Operatority States Backhard Backhard District News Operatority States States Backhard Backhard District News Operatority States	v Kate v V	cess 113 cess 113 cess 113 cess 113 de sec only after a d to Jord or Jord o d to Jord or Jord o	o Ipv4, the DNS s Ipv4, The value	particular II for	hess and the D	n name datalyng i e card hyndria na gang an ett viel. Reed i na e-cardigen 2010 IP and Band an energ Anne ett y statigen 4 static IP publied to M.	

Figure 98 1552 RAP Bridge Group Name Configuration

CISCO	MONITOR MLANE CONTROLLER	No. of Concession, Name			The Indiana	Andrew College of L		0 Ho
Vireless	All APs > Details for RTP-06-1FL-R	11552					< flack	Apph
Access Points	General Credentials Interfac	ns High A	vailability	Inventory	Hesh	Advanced		
All APS All APS Social Social Social Social Configuration Configuratio Configuratio Configuration Configuration Configuration Con	Ctherms. Ctheras Bindging Taterface Name Oper 5 Disabilithment Oper 5 Oper 5 Op		Vias ID 104 113 113	Delete PSK	μ			
	Feet Notes 1(a) DOS serves IP Address and the Danas 1(b) Whenever Start: IP version gets chang 1(c) Whenever Start: IP version gets chang 1 Table (SS can be enabled in 40m with in 5 Tapperform Admin starts in a configure 5 Categorization Admin starts in a configure 6 Categoria (DoS Am with c	ed i.e. 1pv4 to 1 ed i.e. 1pv4 to 1 -defeuit creder le for AP specifi entication to re	Ipv6 or Ipv6 to I Ipv6 or Ipv6 to I ntials only. Ic configuration (move the PSK iso	(pv4, the DNS s (pv4, The value only, c and set to def	a given for suit on the	Idness and the DNS server IF. Access Point	lanan name displayed in configuration page are not usild. Reeds to re-configure DVS IP and Domain name efter newly assigned static IP publied to AP. of Domain name win't be set. Needs to configure DVS IP and Domain name efter newly assigned static IP publied to A name	

Figure 99 1552 MAP Bridge Group Name Configuration

cisco	MONITOR WLANS CONTROLLED	wijkeless p		NAVAGEMENT	COMMAN	S HELP	Sign Canfiguration Bing Lapout Before EDBACK A game
Wireless	All APs > Details for RTP-06-1F	L-M021552					< Rack Apply
 Access Public Access Public Access Public Boding Boding Boding Comparison Advanced Heak Heak ACT BF Prefixes Heak ACT BF Prefixes House Comparison ACT BF Prefixes House Comparison Activated Comparison Activate	AP Rais MultiP Bridge Type Outdoor Unique Trays Name Tenth Bridge Type Tenth Tenth Bridge Type Tenth Tenth Bridge Tenth Ream (Mays) Ethernese Link States Bridge Dan Ream (Mays) Ethernese Link States Bridge Dan Ream (Mays) Ethernese Link States RAD Downlink Backhaul RAD Downlink Backhaul BAD Downlink Backhaul BAD Downlink Backhaul Bridge Dan Ream (Mays) Ethernese Biologing Ethernese Biologing Ethernese Biologing Date Tables Ethernese Biologing Date Theory (Markow) Read Downlink Backhaul Disk Contents Disk Contents Disk Bachhaunt Disk Bach	v A v A v A v A v A v A v A v A v A v A	104 113 113 0 poti or Toyle to poti or Toyle to poti or Toyle to solate only contragenetics	I DV4, the DNS s I DV4, The value conly. ev and set to def	1 Developed for of the A	ness and the D NS server IP at trease Point.	

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

Configuring HA SSO

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

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

Mesh Configurations

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

MESH Backhaul Security (MAC Filter)

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

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

WLAN Configurations

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

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

Mobility Group

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

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

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

Figure 100 Catalyst 9800 Mobility Group Configuration

Q. Source Menu Arms			nfiguration		 Mobility Configuration 															
Dashboard		001 001		-	n conngaration															
) Monitoring	, `	M	obility Peer	Con	figuration															
		+ /	Add X T																	
	· ·																			
Administration	>		MAC Address	4	IP Address	P	ublic IP	×	Group Name	~	Multicast IPv4	×	Multicast IPv6	~	Status		PMTU	Ŷ	SSC Hash	Data Link Encryption
Troubleshooting			d4e8.80b2.d74b		10.5.1.51	N	/A		default		0.0.0.0	_			N/A		N/A			N/A
			0087.648a.3f80		10.5.1.53	10	0.5.1.53		default		0.0.0				Up		1385			Disabled
			6cab.0588.4409		10.5.1.55	10	0.5.1.55		default		0.0.0.0				Control And Data Path Dov	wn.	1385			Enabled
		ж. 2	4 1 × H		10 + Rema p	er pag	90													1 - 3 of 3 items
)	No	on-Local Mo	bilit	y Group Mult	icas	t Config	gura	tion											
	-																			

Figure 101 3504 WLC Mobility Group Configuration

Controller	Static Mobility Grou	p Members						New	EditAll
General Icons	Local Mobility Group	default							
Inventory Interfaces	MAC Address	IP Address(Ipv4/Ipv6)	Group Name	Multicast IP	Status	Hash Key	Secure Mobility	Data Encryptio	on.
Interface Groups	00:87:64:8a:3f:80	10.5.1.53	default	0.0.0.0	Up	none	NA	NA	
Multicast	6c:ab:05:88:44:09	10.5.1.55	default	0.0.0.0	Up	none	Disabled	NA	
Network Routes	d4:e8:80:b2:d7:4b	10.5.1.51	default	0.0.0.0	Up	none	Enabled	Disabled	
Fabric Configuration									
Internal DHCP Server Mobility Management Mobility Configuration Mobility Groups Mobility Anchor Config Multicast Messaging									
Ports									
NTP									
CDP									
PMIPv6									
Tunneling									
IPv6									
mDNS									
Advanced									

Show Commands:

(Cisco Controller) >show mobility summary

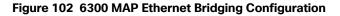
Mobility Protocol Port..... 16666 Default Mobility Domain..... default Multicast Mode Disabled Mobility Domain ID for 802.11r..... 0xac34 Mobility Keepalive Interval..... 10 Mobility Keepalive Count..... 3 Mobility Group Members Configured...... 3 Mobility Control Message DSCP Value..... 0 Controllers configured in the Mobility Group MAC Address IP Address Group Name Multicast IP Status 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: ΙP Public Ip MAC Address Multicast IPv4 Multicast IPv6 Group Name 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 0.0.0.0 default :: Up

Ethernet Bridging

1385

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



(←) → C ² ⁽¹⁾ ⁽²⁾	🔞 https://192.168.251.51/webui/#/ap	(90%)	🖾 🗘	Search	lin 🖸 🤇	\$ ≓
Cisco Cal	talyst 9800-40 Wireless Controller	Welco	me admin 🛛 🖷	* * * * * * *	Seed all and Dark Q	
Q. Search Moral Imma	Configuration * > Wireless * > Access Points	Edit AP				×
Dashboard	All Access Points Number of AP(s): 4	General Interfaces High /	Availability Inver	tory Mesh Advanced	Ē.]
Configuration	AP Name v Model Slots v Status Admin	Block Child		Ethernet Bridging on the as enabled to configure this sect	isociated Mesh Profile should be tion successfully	
(c) Administration	RTP-06-1FL- W-6300H- 2 0 10.5 6300R02 A AC-8-89 2 10.5 RTP-06-1FL- W-6300H- 2 0 10.5	Daisy Chaining strict-		Port	0 •	
X Troubleshooting	G00407 a. AC-8-K9 RTP-06-1FL- №-6300H- 6300M02 a. AC-8-K9 2 ◎ 10.5	Preferred Parent MAC 0000.000	00.0000	Mode Native VLAN ID*	trunk •	
	KIH-GB-TL- W-6300H- 2 S00M01	Role Mesh	•	Allowed VLAN IDs	112,113	
	> 5 GHz Radios	Remove PSK				
	> 2.4 GHz Radios	Backhaul				
	Dual-Band Radios	Backhaul Radio Type Sghz	•			
	> Country	Backhaul Slot ID	•			
	> LSC Provision	Rate Types auto	·			
		D Cancel			Update & Apply to D	Device

Figure 103 6300 RAP Ethernet Bridging Configuration

ordit Maryl Initia	Configuration * > Wireless * > Access Points	Edit AP	
shboard	 All Access Points 	General Interfaces High Availability General	Inventory Mesh Advanced Ethernet Port Configuration
	Number of AP(s): 4		
	AP ~ Admin ~ IP AP Name ~ Model Stots ~ Status Add	Block Child	 Ethernet Bridging on the associated Mesh Profile should be enabled to configure this section successfully
		Daisy Chaining strict-	Port 0 v
	RTP-06-1FL- W-6300H- 2 0 103 6300R01 A AC-8-K9 2 103 RTP-06-1FL- W-6300H- 2 100	Preferred Parent MAC 0000.0000	Mode trunk •
	6300M02 A AC-B-K9 2 0 103 RTP-06-1FL- W-6300H- 2 0 103	VLAN Trunking Native 2 104	Native VLAN ID* 104
	6300M01 A AC-8-K9 2 103	Role Root •	Allowed VLAN IDs 112,113
	> 5 GHz Radios	Remove PSK	
	> 2.4 GHz Radios	Backhaul	
	> Dual-Band Radios	Backhaul Radio Type 5ghz •	
	> Country	Backhaul Slot ID 1	
	> LSC Provision	Rate Types auto •	

Use Cases

BGN

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

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

Figure 104 BGN Configuration for Mesh profile on Catalyst 9800

Q. Search Menu Items		Configuration * > Wireless * >	Edit Mesh Profile			
		Global Config Profiles	General Advanced			
📷 Dashboard			Security		5 GHz Band Backha	ul
Monitoring	>	+ Add Selete	Method	PSK	Rate Types	auto
Configuration	>	Number of Profiles : 3	Authentication Method	Enter Method	2.4 GHz Band Back	haul
(O) Administration	>	Name MeshProfile1	Authorization Method	default	Rate Types	auto
💥 Troubleshooting		MeshProfile2	Ethernet Bridging			
		default-mesh-profile	VLAN Transparent			
		ie e 1 > >i 10	Ethernet Bridging			
			Bridge Group			
			Bridge Group Name	mesh1		
			Strict Match			

Use Cases

Remote Access

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

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

Emerson WiHart for condition-based monitoring

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

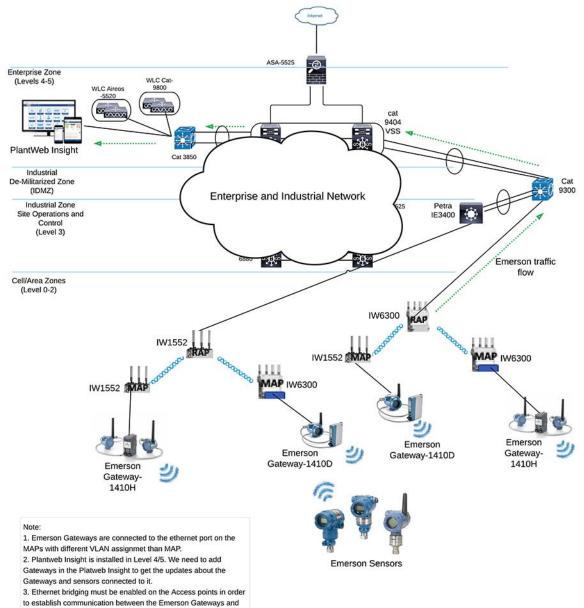
Use Cases

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

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

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





Platweb Insight.

Use Cases

Video Surveillance

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

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

Location Services and Asset Tracking

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

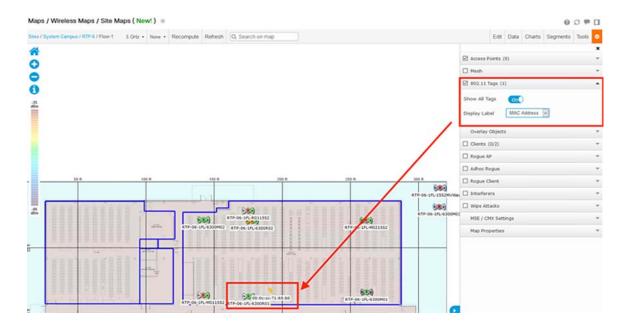


Figure 106 Asset tracking on Prime Infrastructure

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

Troubleshooting

Figure 107 Tracking Parameters

king			
ring	Tracking Parameters		
ation Setup	Network Location Service		
a Privacy	Elements	Active Value	Not Tracked
Retention	Wireless Clients	0	68
Server	Rogue Access Points	0	0
rade	Rogue Clients	0	0
	Interferers	0	0
	RFID Tags	2	0
	BLE Tags	0	0



Troubleshooting

Debug Command:

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

```
deb mesh error
   deb mesh convergence
   deb mesh link
   show mesh config
   show mesh backhaul
   show mesh status
   show capwap client rcb
For general AP join issues (6300 RAP & 6300 MAP):
   deb capwap client events
   deb mesh convergence
   deb mesh link
   show mesh config
   show mesh backhaul
   show mesh status
   show capwap client rcb
  For AP join security related issues (1552 RAP & 1552 MAP):
```

- WLC:

Troubleshooting

Debug client Debug dot1x all enable Debug aaa all enable

– MAP:

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

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

- WLC:

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

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

– MAP:

Debug mesh convergence Debug mesh security Debug dot1x

Appendix A: Integrating Emerson 1410S Gateway with IW6300

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

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

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

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

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

Notes:

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

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

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

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

Table 2 PoE Out Options for IW6300

Notes:

DC/DCW Power Input:

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

AC Power Input:

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

Table 3 PoE-Out Port Power Allocation

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

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

Table 4 Power Level and Power Capacity Mapping

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

For more details on powering procedures of IW6300 refer to Powering the IW6300 Access point.

Configuring Power Over Ethernet Out Functionality

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

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

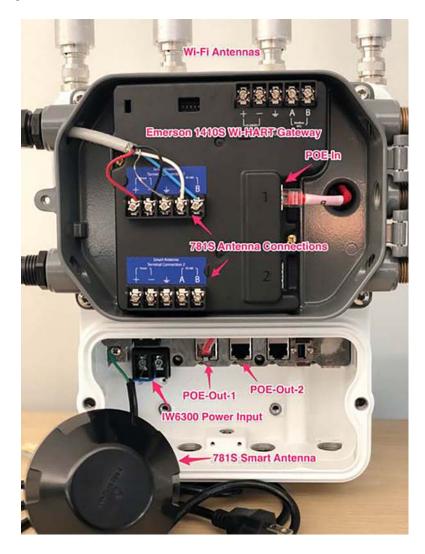


Figure 108 Emerson 1410S with 781S Smart Antenna embedded on IW6300

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

For AireOS Controller:

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

،، ،،، ،، cisco	MONITOR W	ANS <u>C</u> ON	ITROLLEI	R W <u>I</u> RELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
WLANs	Ap Groups >	Edit 'dei	fault-gr	oup'					
WLANs	General	WLANs	APs	802.11u	Location	Ports/Module	Intelligent	t Capture	8
Advanced							Apply		
AP Groups	LAN Ports								
	LAN (4)(5)	ENABLE	POE 2	Power Level 15	RLAN 12				
	LAN1 Z		۵	2	None	0			
	LAN2			None 📀	None				
	LAN3				None				
	LAN4 8				None				
	External Mo	dule							
	LAN	EN	ABLE R	LAN					
	External Mo USB Module		0 (None 😒					

Figure 109 LAN Port Configuration on AP Group on AireOS Controller

For Catalyst 9800 Wireless Controller:

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

Configuring RLAN:

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

Figure 110 Creating RLAN Profile

Add RLAN Profile		×
General Security		
Profile Name*	poeout	
RLAN ID*	1	
Status		
Client Association Limit	0	
mDNS Mode	Bridging •	
"Cancel		Apply to Device

Figure 111 Creating RLAN Policy

eral Access Policie	es Advanced		
	A Configuring in enabled state wi	Il result in loss of connectivity for clients	associated with this policy.
Policy Name*	poeout	RLAN Switching Polic	ey.
Description	Enter Description	Central Switching	ENABLED
Status		Central DHCP	DISABLED
PoE			
Power Level	2 •		
Cancel			Apply to Dev

Mapping RLAN Policy to Policy tag:

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

Figure 112	Mapping RLA	N Policy to Poli	cy Tag
------------	-------------	------------------	--------

Edit Policy Tag						×
Name* Description	og-profile Enter Description					
VULAN-POLICY	' Maps: 2					
+ Add X Del	ete					
WLAN Profile		~	Polic	y Profile		v ¹
OG-SSID-1			og-pi	rofile_WLANI	D_1	
test8021x			og-pi	rofile_WLANI	D_1	
H 4 1 H H	10 🗸 items per page					1 - 2 of 2 items
RLAN-POLICY + Add × Del Port ID	ete		~	RLAN Policy	Profile	
			×.	RLAN POIC	y Prome	~
ia a 0 > >i	10 v items per page					No items to display
Map RLAN and Polic	су					
Port ID*	1 •					
RLAN Profile*	poeout v		RLAN Profile	Policy e*	poeout	•
	×		4			
Cancel					🗄 Upd	ate & Apply to Device

Enabling LAN port on Access point:

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

For more detailed steps on configuring Remote LAN and PoE Out refer to the guide.

To configure PoE on a specific Access point:

For AireOS Controller:

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

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

General	Credentials	Interfaces	High Availability	Inventory	Mesh Adv	anced			
thernet I	nterfaces								
	nfiguration								
	et Interface#	CDP State							
0	et interface#								
1									
2		ă							
3		ē.							
Interfa	ice		atus Tx Unicast Packet	s Rx Unicast Pa	ackets Tx Non-L	Inicast Packets	Rx Non-Unicast Packets		
Gigabit	Ethernet0	DOWN	0	0	0		0		
	Ethernet1	DOWN	0	0	0		0		
LAN1		DOWN	0	0	0		0		
LAN2		DOWN	0	0	0		0		
CDP Cor	nfiguration	CDP State							
0	5101#								
1									
	Slot# Radio Inte	_	ule Type S	Sub Band	Admin Status	Oper Status	CleanAir/SI Admin Status	CleanAir/SI Oper Status	Regulatory Domain
0	802.11b/g/r				Enable	UP	Enable	DOWN	Supported
1	802.11a/n/a				Enable	UP	Enable	UP	Supported
AN Ports									
Juit Porta									
	of Ports	2							
Number	ide	۲							
Number		wer Level Z							
Number an Overri Port	ide	۲							

For Catalyst 9800 Controller:

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

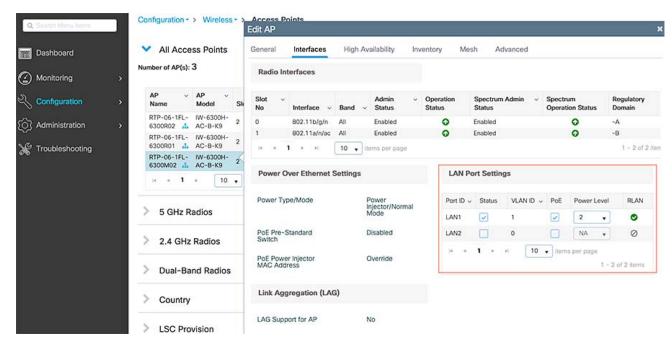


Figure 114 LAN Port Configuration on specific Access point on Catalyst 9800 Controller

To check the power status on the Access point:

From Controller CLI:

Catalyst 9800:

To check for specific access point from WLC:

WLC#show ap	name RTP-06-1	FL-6300M02]	lan port summ	nary	
LAN Port sta	atus for AP R1	P-06-1FL-630	0M02		
Port ID	status	vlanId	poe	power-level	RLAN
LAN1	Enabled	1	Enabled	2	Enabled
LAN2	Disabled	0	Disabled	NA	Disabled

AireOS Controller:

To check the status on AP profile: (Cisco Controller) >show wlan apgroups

Total Number of AP Groups..... 1

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

Oil and Gas Refinery WLAN MESH Implementation Guide

Appendix A: Integrating Emerson 1410S Gateway with IW6300

RF Profile _ _ _ _ _ _ _ _ _ . 2.4 GHz band..... <none> WLAN ID Interface Network Admission Control Radio Policy OpenDnsProfile --More-- or (q)uit _ -----_____ ----client-vlan-112 Disabled 1 None None client-vlan-112 2 Disabled None None *AP3600 with 802.11ac Module will only advertise first 8 WLANs on 5GHz radios. NTP Server Index Server IP Auth ---------------Lan Port configs ------POE Power Level LAN Status RLAN Enabled Enabled 2 Disabled Disabled None _ _ _ _ _ - - -1 None 2 None 3 Disabled None 4 Disabled Disabled None To check for specific access point from WLC: (Cisco Controller) > show ap lan port-summary RTP-06-1FL-6300M02 LAN Port configuration for AP RTP-06-1FL-6300M02 Lan Override Disabled Port Status POE Power Level -----LAN1 ENABLED ENABLED LAN2 DISABLED DISABLED None 2 (Cisco Controller) > From Access point CLI: RTP-06-1FL-6300M02#show power status Device ID: 0xc4, Firmware Reversion:0x40, Bus:3, Address:0x24 Operating Mode: Semiauto Available: 35.3(w) Used:7.0(w) Remaining:28.3(w) Oper Power Class Max Config Power Interface Admin
 POE-out 1
 Up
 ON
 6.2
 15.4
 7.0

 POE-out 2
 Down
 OFF
 0.0
 0.0
 30.0

For more details on configuring Power Over Ethernet Out functionality refer to Power Over Ethernet Configuration.