Outdoor Mobility Design Guide

Contents

Introduction

This document provides design guidance for deploying Mobility Infrastructure in the outdoors. This document touches briefly only the relevant products which are suitable and recommended for Mobility deployments in the outdoors. For a complete understanding of these product lines, refer to the respective product updates on the Cisco website or go through the respective deployment guides.

Note: You need a special autonomous image on the autonomous access points (APs) being used as Work Group Bridge (WGB) or Mobile Access Router (MAR) for interoperability with Unified CAPWAP infrastructure.

Important, helpful links are provided in the Annexure attached in the end.

Today's travelers are demanding more safe, secure, and reliable methods of transportation for personal and business needs. With the increased demand by people to be connected anywhere at any time, the mobility in the outdoors using rail or any other infrastructure is gearing up to meet these growing demands from their passengers. While mobile phones may provide a solution for voice communications, they have not proven useful in delivering business and personal data communications that the public has become accustomed to using.

In order to deliver a more reliable, safe, and secure transportation solution, rail operations must improve through the use of mobile technologies. By providing high speed, reliable mobile communications, not only to the train, but to any other infrastructure, travelers and employees can stay connected to their business and personal information.

With millions of travelers a year, the transportation industry has been moving rapidly to expand and improve rail operations through mobile technologies (solutions).

Main business motivators for mobility are real-time access to data versus batch updates, improved surveillance operations inside the moving trains that helps in location tracking in the event of an emergency, reduced costs, and increased communications bandwidth by replacing the use of satellite and/or cellular links with land based wireless links.

Cisco unified wireless architecture provides reliable high-bandwidth connectivity on moving trains. This design guide helps you understand how to build such a system effectively.

Wireless technologies are designed using radio systems which are subject to radio wave interference. Causes of this interference may be accidental or deliberate. Regardless of the source, interference can interrupt the wireless connection, disabling any solution that depends on WI-FI. Given such risks, solutions that impact public safety should not depend SOLELY on wireless technologies. Redundant, overlapping, and independent systems (e.g. both wired and wireless) are preferred. In the context of train control systems, examples of overlapping, redundant systems include, but are not limited to: pairing wireless technologies with two or more independent systems, mechanical systems (e.g. "deadman switch"), train control signaling over metallic rails, and on-board and central human oversight (train driver) or central control supervisors. Should one system fail, another independent system would still be available, helping reduce risks to public safety.

Mobility deployment can be divided into two main sections. First is stationary infrastructure in which the fast roaming wireless client will interoperate, and the second is mobile infrastructure consisting of the wireless roaming client itself. There are some specific Cisco wireless products which have a peculiar feature set making them suitable for Mobility.

Stationary infrastructure can be created using Cisco Outdoor Mesh Access Points (MAPs) (AP1520 series). Do not try to create a mesh network in the outdoors using indoor MAPs (AP1130 and AP1240) as these APs are not ruggedized for outdoor use and have limited power. Use an indoor MAP indoors only.

Similarly, for roaming infrastructure, you can either use Cisco wireless Autonomous APs in the WGP mode, or the Cisco Mobile Access Router MAR3200.

The feature set of the respective products which make them suitable for Mobility will be highlighted in this document.

Stationary Infrastructure Using MAPs

Outdoor deployments also require specialized radio frequency (RF) skills, may have a lower user density than indoor deployments, and may be deployed in an environment that is less regulated than inside a building. These features put pressure on the total cost of ownership (TCO) of the outdoor solutions, and require a solution that is easy to deploy and maintain.

The Cisco wireless mesh networking solution enables cost-effective and secure deployment of enterprise, campus, and metropolitan outdoor Wi-Fi networks.

AP1520 Series MAPs are based on CAPWAP operating with Cisco Wireless LAN Controllers (WLCs) and Cisco Wireless Control System (WCS) software to provide centralized and scalable management, high security, and mobility that is seamless between indoor and outdoor deployments.

Multiple WLCs can be grouped together into a mobility group, so that all the APs managed by them form a single, seamless wireless domain. The maximum number of WLCs in a single group is 24. This is discussed more in depth later in this document.

Detailed information about various controllers and their capabilities can be found at this link: http://www.cisco.com/en/US/products/ps6302/Products_Sub_Category_Home.html.

Designed to support ease of deployments, the Cisco 1520 Series MAP based on CAPWAP, easily and securely joins the mesh network, and is available to manage and monitor the network through the controller and WCS graphical or command-line interface (CLI). Compliant with Wi-Fi Protected Access 2 (WPA2) and employing hardware-based Advanced Encryption Standard (AES) encryption between wireless nodes, the Cisco 1520 Series MAP provides end-to-end security.

AP1520 has been certified to IP67, NEMA4X specifications, eliminating the need to have additional NEMA or other weatherproof enclosures and can operate in temperatures ranging from -40°C all the way to +55°C without any external temperature influencing devices. The entire unit is designed to withstand and still operate in severe conditions including very high wind and precipitation of all types.

The AP1520 platform (AP1524 and AP1522) as a whole is a modular design and can be configured with these optional uplink interfaces:

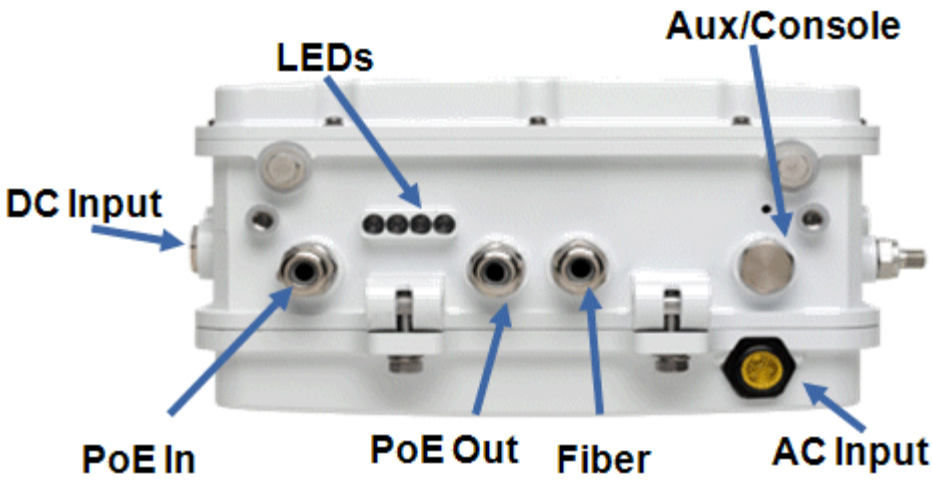
- Cable Modem DOCSIS 2.0 with Cable Power Supply
- Fiber Interface with 100BaseBX SFP
- 1000BaseT Gig Ethernet

This platform also gives a PoE output 802.3af ready port to connect any peripheral devices (like cameras).

The 1520 Series AP supports four Gigabit Ethernet interfaces:

- Port 0 (g0) - Power over Ethernet input port-PoE (in)
- Port 1 (g1) - Power over Ethernet output port-PoE (out)
- Port 2 (g2) - cable connection
- Port 3 (g3) - fiber connection

Interfaces on a MAP



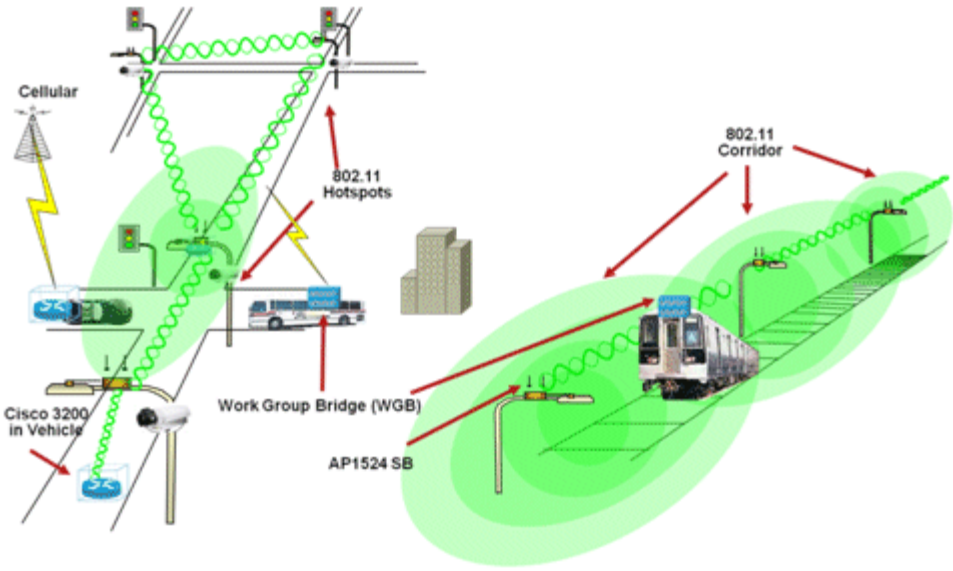
The AP1520 platform has given birth to many MAPs like AP1522, AP1524PS (Public Safety), and AP1524SB (Serial Backhaul).

With 7.0 code, you can order the AP1523 CV which has basically the same hardware as the AP1524SB, except that it has a built-in cable modem, similar to the AP1522PC-X-K9 model. In simpler terms, the AP1522 and AP1523CV can be configured with a cable modem while ordering, while the AP1524SB and AP1524PS models are not available with a cable modem.

Note: The AP1523CV is only available in –A domain with 7.0 code. In this document, all functionality explained for the AP1524SB is also applicable to the AP1523CV.

It becomes important to understand the AP1524SB key features which make it best suitable for a linear type of deployment. Mostly, mobility deployments require this type of infrastructure:

Infrastructure for Mobility Deployments



AP1524 Serial Backhaul (AIR-LAP1524SB-X-K9) Functionality

Radios and Channels

The AP1524 has three radios: one 2.4 GHz radio and two 5 GHz radios. Its 2.4 GHz radio is used primarily for client access. Two 5 GHz radios are primarily used for the backhaul. These two backhauls provide an uplink and downlink access. By keeping them on exclusive channels or frequency bands, the need to use the same shared wireless medium between the north and south-bound traffic in a mesh tree-based network is avoided. In simpler terms, we can say that each hop uses a different frequency. This improves performance and avoids the problems associated with a shared access medium.

It is important to understand which radio lies in which Slot. The AP1524SB has basically 4 slots, but only 3 slots are occupied by these 3 radios: AP1524SB: (Slot 0) 2.4GHz Client Access; (Slot 1 and 2) 5GHz radios: Uplink and downlink backhaul.

AP1524SB was launched in -A,-N and, C domain with release 6.0.

Note: In release 6.0, the 5 GHz radios only operate in the 5.8 GHz band with 5 channels (149 to 165).

With release 7.0, AP1524SB is available in -E, -K,-M, -S, and T domain. Also, with release 7.0, UNII2 and UNII2 Plus bands have been introduced in A domain on existing 5 GHz radios. As a result, both 802.11a radio units support the entire 5 GHz band. In other words, with release 7.0 the radios can operates in UNII-2 (5.25 – 5.35 GHz), UNII-2 plus (5.47 – 5.725 GHz), and upper ISM (5.725 – 5.850 GHz) bands.

Channel availability depends upon the regulatory domain. Overall, with the latest 7.0 release you get 5 channels in upper ISM band, 4 channels in UNII-2 band, and 11 channels in UNII-2 plus band. Refer to Table 1 for a complete overview of channels supported in each domain.

For the latest information on regulations, refer to the rules and regulations of your respective regulator domain.

Table 1: Channels Supported as per Regulatory Domain

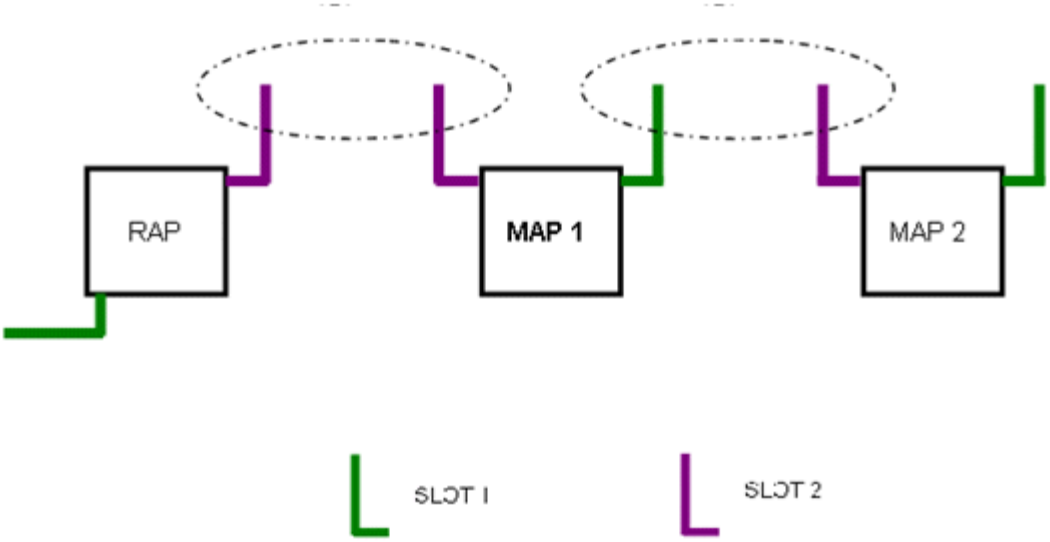
Channel ID	Frequency (Mhz)	Regulatory Domains								
		-A	-C	-E	-K	-M	-N	-P	-S	-T
4940-5100 MHz										
184	4920							Yes		
188	4940							Yes		
22/192	4960							Yes		
26/196	4980							Yes		
8	5040							Yes		
12	5060							Yes		
5250-5350 MHz										
52	5260									
56	5280	DFS			DFS					
60	5300	DFS			DFS					
64	5320	DFS			DFS					
5470-5725 MHz										
100	5500	DFS		DFS	DFS	DFS				DFS
104	5520	DFS		DFS	DFS	DFS				DFS
108	5540	DFS		DFS	DFS	DFS				DFS
112	5560	DFS		DFS	DFS	DFS				DFS
116	5580	DFS		DFS	DFS	DFS				DFS
120	5600				DFS					DFS
124	5620				DFS					DFS
128	5640									DFS
132	5660	DFS		DFS		DFS				DFS
136	5680	DFS		DFS		DFS				DFS
140	5700	DFS		DFS		DFS				DFS
5725-5850 MHz										
149	5745	Yes	Yes			DFS	Yes		Yes	Yes
153	5765	Yes	Yes			DFS	Yes		Yes	Yes
157	5785	Yes	Yes			DFS	Yes		Yes	Yes
161	5805	Yes	Yes			DFS	Yes		Yes	Yes
165	5825	Yes	Yes				Yes		Yes	Yes
Note 1: Channels marked Yes/DFS are channels supported in that domain.										
Note 2: Channels marked DFS are additionally DFS enabled channels, and require check for radar detection										
Note 3: This table is for up to 8dbi Antennas, for higher gain antennas please refer Huck Junior Regulatory Domain Settings Document										

Mesh Formation

Antenna locations for each radio are fixed and labeled. This is the configuration of the radios with the antennas:

- Slot 0: (11b) (Access)
- Slot 1: (11a, 5 GHz) (Universal Access) – Omni/ Directional Antenna
- Slot 2: (11a, 5 GHz) (Backhaul) – Directional Antenna

A Typical Mesh Network



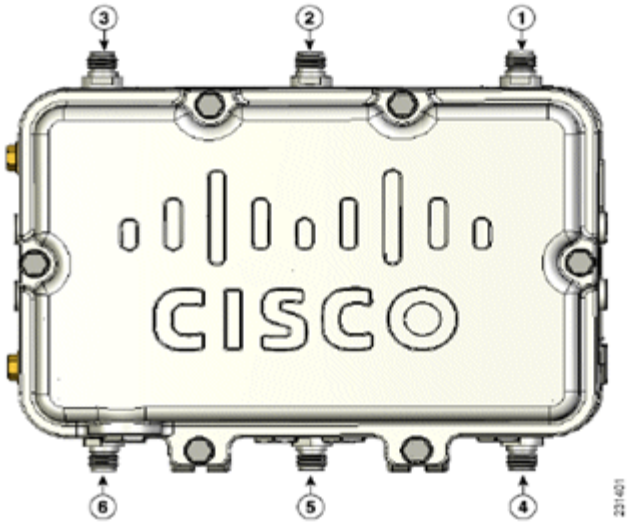
As shown in this figure, Slot 2 - 5 GHz radio in the Root Access Point (RAP) is used to extend the backhaul in the downlink direction, whereas Slot 2- 5 GHz radio in the MAP is used for the backhaul in the uplink. MAP extends Slot 1 radio in the downlink direction. AWPP beacons are only sent on the downlink to allow child APs to join.

Cisco recommends using a directional antenna with the Slot 2 radio at the minimum. The reasoning for this is explained later in this document.

The Slot 2 (5 GHz) radio is internally connected to Antenna Port 6.

Antenna Ports are labeled as (Hinged side facing forward):

Antenna Ports on the 1520 Series AP



1	Antenna port 1	**4**	Antenna port 4
2	Antenna port 2	**5**	Antenna port 5[1]
3	Antenna port 3	**6**	Antenna port 6

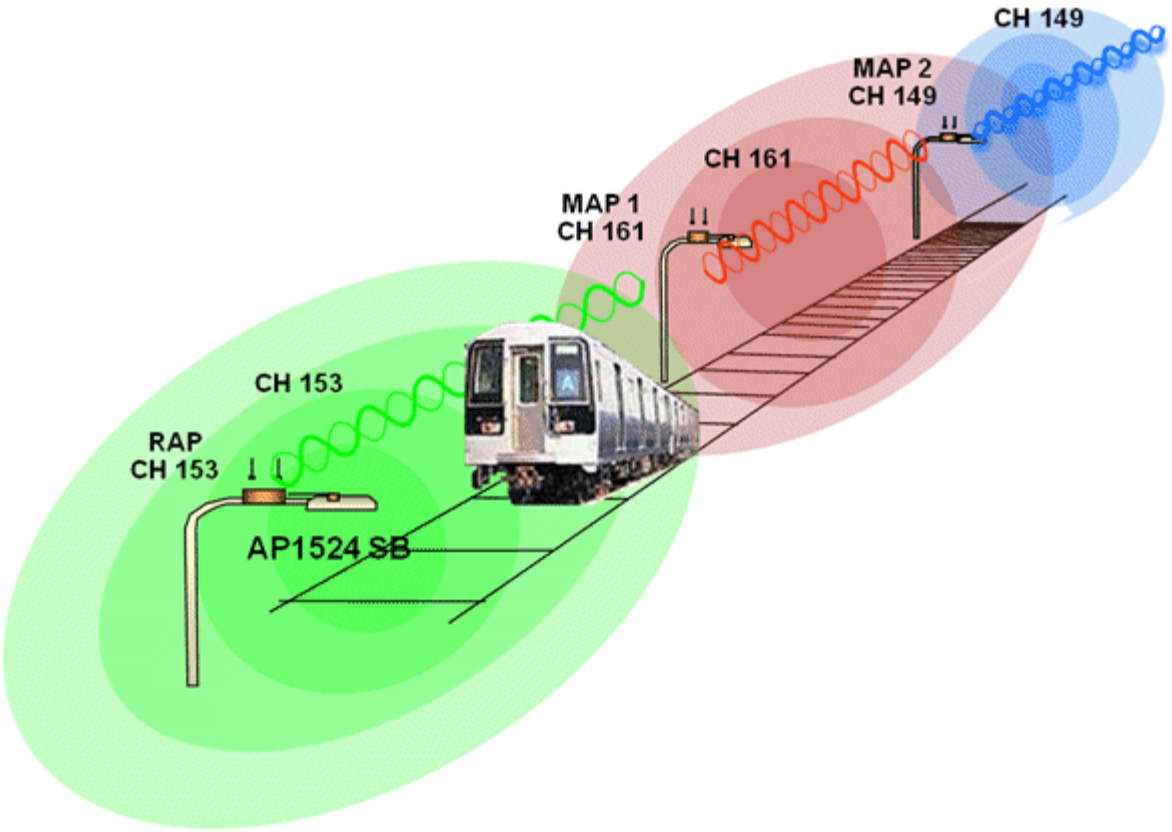
1. Reserved for future use. A plug is installed.

Antenna ports are labeled on the hardware and connected internally to the radios in each slot on the AP1524SB/AP1523CV SKU as:

- Antenna Port 1: 5 GHz (Slot 1 Radio)
- Antenna Port 2: 2.4 GHz (Slot 0 Radio)
- Antenna Port 3: 2.4 GHz (Slot 0 Radio)
- Antenna Port 4: 2.4 GHz (Slot 0 Radio)
- Antenna Port 5: Not connected
- Antenna Port 6: 5 GHz (Slot 2 Radio)

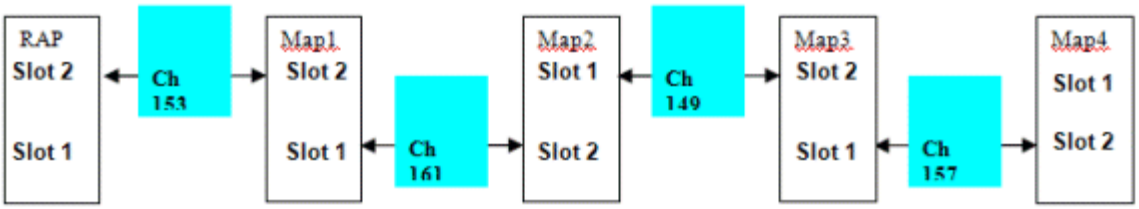
You have to configure the channel only on the RAP for the downlink, and then MAPs will do the channel selection in an automated fashion. Channels are picked automatically from the channel subset, giving each hop on a different channel. For example, the channel set for the 5.8 band is {149, 153, 157, 161, 165}. If the RAP downlink is selected to be channel 153, channel selection picks up alternate adjacent channels for the MAPs down the mesh tree.

Channel Selection in a Mesh Network



Every hop is not only a different channel, but also uses different pair of radios. So, in terms of slots, this is how it looks like per hop:

Slots per hop on a Mesh Network



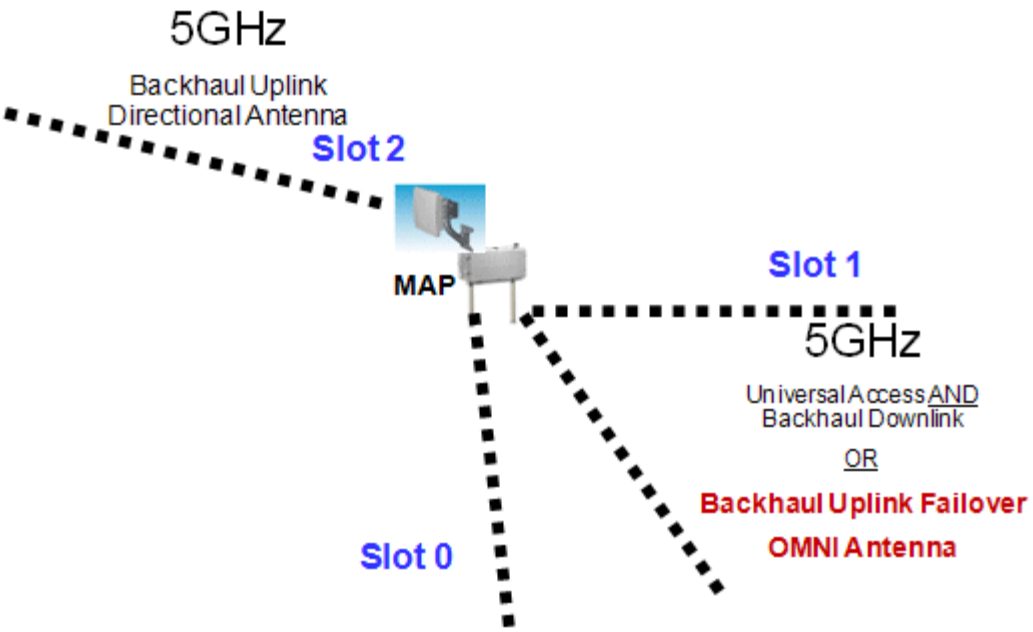
This arrangement not only provides high throughput down the mesh tree, as throughput is not decreased exponentially down the hops as compared to the AP1522 and AP1524PS models, but also provides high capacity and robust network against interference.

Note: Public Safety band (4.94 to 4.99 GHz) is not supported for either Backhaul or for client access. The reason is that we have only 2 channels in public safety list: 20 and 26. The interference between uplink and downlink cannot be avoided using these channels. Also, the network cannot have a mix of public safety and non public safety channels. Further, you cannot program the access radio channels from the controller for the AP1524SB model. This assignment is automatic depending on the channel selection for other slot radios on the AP.

Although primarily 2.4 GHz radio is used by clients to access the mesh infrastructure, but client access is also available on two 5 GHz radios. Client access on both the 5 GHz backhaul radios is called the Universal Client access feature. As the roaming wireless client can approach the AP1524SB linear deployment from north and south bound directions, Universal client access feature on both 5 GHz radios facilitates this.

Fall Back Mode

Fall Back Mode for a MAP



Slot 1 5 GHz radio in the MAP also performs one more important function. It can act as an uplink radio for the backhaul in case of these scenarios:

- Slot 2 Radio fails
- Antenna for Slot 2 Radio goes bad
- Slot 2 Radio is not able to find the uplink because of bad RF design
- Interference kicks in, and long-term fades disturb the uplink to an extend that slot 2 radio looses uplink connection more often

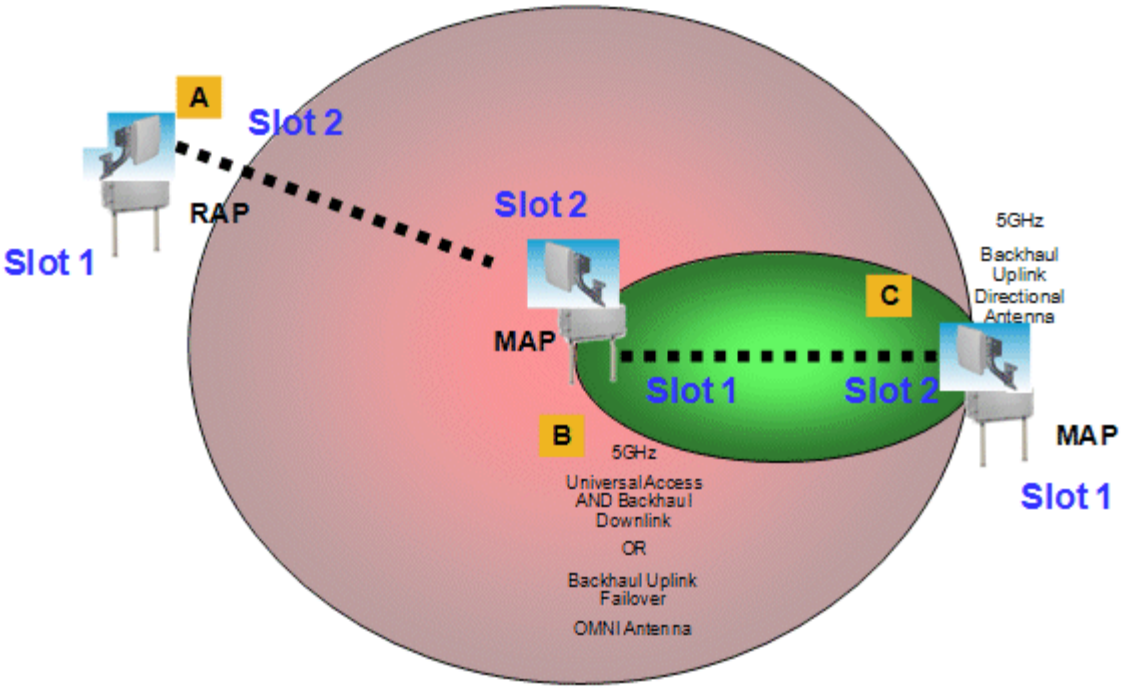
When Slot 1 radio takes over for the Slot 2 radio, it is called Fall Back Mode. The Slot 2 radio is put to sleep on a non-interfering channel. In other words, hardware is reduced to AP1522 (two radios). Slot1 radio is extended to the uplink. A 15-minute timer is set to attempt a re-scan to find a Parent on Slot 2 again.

Behavior on Parent Selection

After a parent is selected, neighbors are maintained and only searched on the same channel as the uplink. The downlink radio will **NOT** search for better neighbors; it will only be used to extend the tree for incoming children to join the tree. Downlink Radio will not process any beacons being heard.

When a RAP falls back as a MAP (RAP connection to the controller goes down), it will use only one of its backhaul radios to attempt to connect as a MAP (Best Parent). The second 5.8 GHz radio will not associate clients and will not form any mesh relationship.

Functional Routing of Three Radio Maps



For a proper linear alignment and focusing radio frequency in one direction, it is important to attach a directional antenna to the Slot 2 radios at the minimum. You should align and fine tune each link to minimize the hidden node effect. For example, in the above figure, MAP at location “C” should be aligned to MAP at location “B.” MAP at location “C” should not be able to see AP at location “A.” This can be achieved by first aligning the antennas and then optimizing each link by tuning the RF power.

For further details about AP1524SB and features refer to the Mesh Design and Deployment Guide Release 7.0.

Important Points Related to Mesh Product Line

- AP1524SB/AP1523CV can fully interoperate with AP1522, AP1524PS, AP1240 and AP1130 as a RAP or a MAP.
- With the 5.2 code, mesh world merged back with the main controller software release, or, in other words, we introduced mesh as a unified solution with 5.2 code which is on Cisco.com.
- Many new features to increase throughput and performance have been added in both 6.0 and 7.0 releases.
- Cisco has announced an end of life (EOL) for both the AP1505 and AP1510 MAPs. The last sale date was November 30, 2008. Customers are encouraged to migrate their networks to AP1520s.
- Release 5.2 or greater does not support AP1510 and 1505.

Mesh Configuration

Choose a Wireless LAN Controller

The wireless mesh solution is supported by Cisco 2100 Series, Cisco 4400 Series WLCs, 5500 Series WLCs, and Wireless integrated service module (WiSM). The Cisco 5500, WiSM, and 4400 controllers are recommended for wireless mesh deployments because they can scale to large numbers of APs and can support Layer 3 CAPWAP.

Note: For all controller platforms except 5500, MAPs (MESH APs) are counted as “half aps.” In other words, Mesh

Aps (MAPs)/(RAPs) are counted as “full aps” on the 5508 controller.

As a result, the high-end model WiSM can control and manage more than 300 Mesh APs. The WiSM is in the form factor of a line card and it fits into both the 6500 and 7600 chassis.

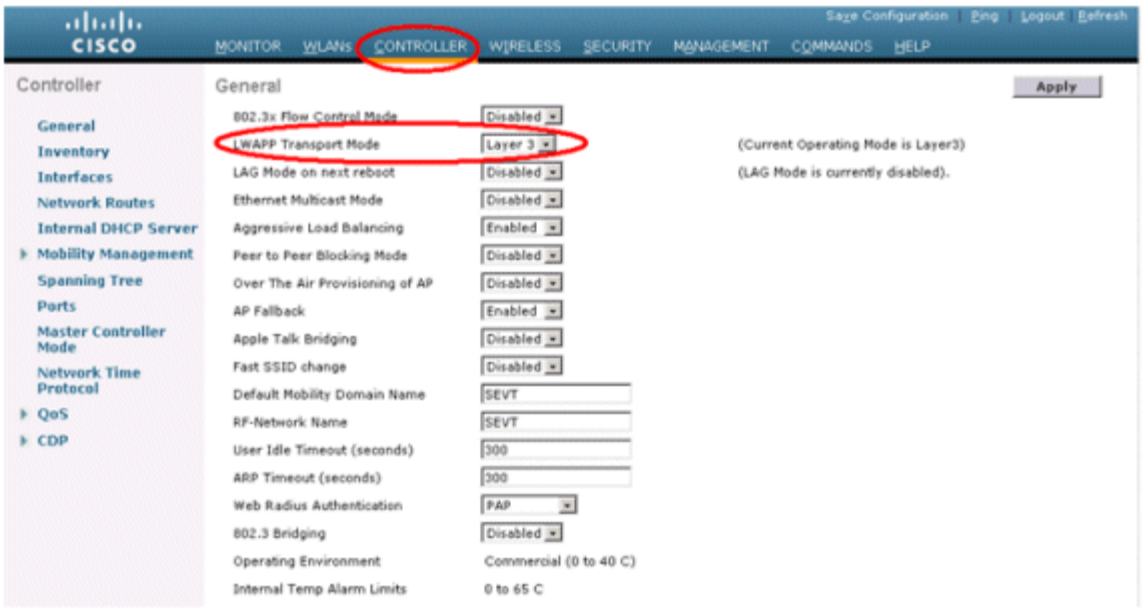
The 5508 controller Base License (LIC-CT5508-X) is sufficient for outdoor and indoor APs (AP152X). WPlus Licence (LIC-WPLUS-X) has been merged recently with Base license and is no longer required for indoor MAPs (1242s/1130s).

Detailed information about various controllers and their capabilities can be found at http://www.cisco.com/en/US/products/ps6302/Products_Sub_Category_Home.html.

CAPWAP carries control and data traffic between APs and the WLC. Control traffic is AES-CCM , but the Data Plane Transport Layer Security (DTLS) is not supported on mesh.

After choosing the controller, configure the controller in Layer 3 mode.

WLC in Layer 3 Mode



Upgrade the Controller to the 7.0 Code

Cisco recommends that you upgrade the controller to 7.0 code at the minimum, as this code brings in many useful features for Mobility.

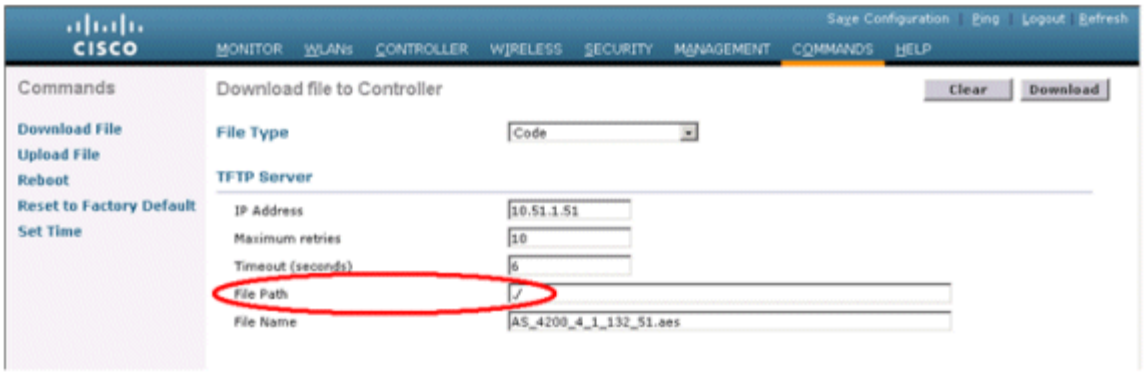
Note: Please save the running controller configuration with present code at some place for reference before upgrading. If you have to downgrade the network back to the old code for any reason, you will have the configuration handy. Although, the configuration will be preserved during the upgrade to the beta code.

Note: Officially, Cisco does not support Downgrades for controllers.

From the controller GUI interface, go to **Commands** > **Download file**. Choose **Code** as the **File Type** and give the IP address of your TFTP server. Define the path and the name of the file.

Note: Please use the TFTP Server that supports more than 32 MB File size transfers. For example, **tftpd32**. Under **File Path**, enter **./**.

Image Download on a WLC using TFTP



When finished installing the new firmware, verify via the CLI using the **show sysinfo** command that the new firmware is indeed in place:

```
(Cisco Controller) >show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 6.0.61.0
RTOS Version..................................... 6.0.61.0
Bootloader Version............................... 4.1.171.0
Emergency Image Version.......................... Error
Build Type....................................... DATA + WPS

System Name...................................... SEVT-CONTROLLER
System Location.................................
System Contact..................................
System ObjectID.................................. 1.3.6.1.4.1.14179.1.1.4.3
IP Address....................................... 10.51.1.10
System Up Time................................... 0 days 2 hrs 17 mins 13 secs
System Timezone Location.........................
Current Boot License Level.......................
Next Boot License Level.........................

Configured Country............................... US  - United States
Operating Environment............................ Commercial (0 to 40 C)
Internal Temp Alarm Limits....................... 0 to 65 C

--More-- or (q)uit
Internal Temperature............................. +53 C

State of 802.11b Network......................... Enabled
State of 802.11a Network......................... Enabled
Number of WLANs.................................. 1
3rd Party Access Point Support................... Disabled
Number of Active Clients......................... 0

Burned-in MAC Address............................ 00:0B:85:40:4A:E0
Crypto Accelerator 1............................. Absent
Crypto Accelerator 2............................. Absent
Power Supply 1................................... Absent
Power Supply 2................................... Present, OK
Maximum number of APs supported.................. 100
```

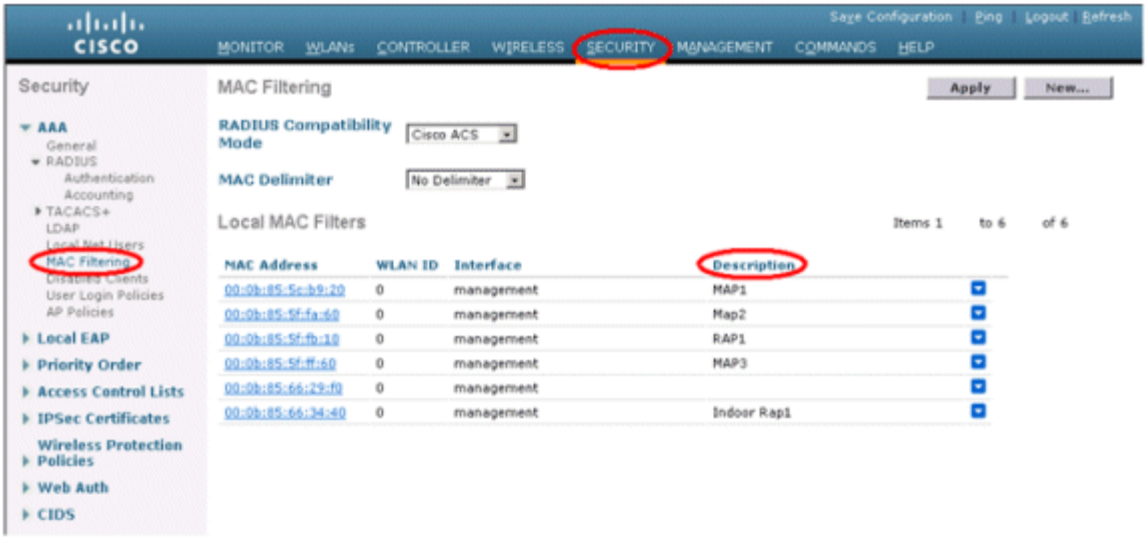
Add APs

MAPs can only join the controller if the BVI MAC address of the AP exists in the controller. MAC filtering is enabled by default. The Cisco controller maintains a MAP authorization MAC address list. The controller responds only to discovery requests from the outdoor radios that appear on the authorization list. On the controller, enter the MAC addresses of all the radios you will use in your network by performing the instructions below.

Note: For AP152X (IOS AP), the BVI MAC address is used on the controller as a MAC filter. Enter the BVI MAC Address of the APs on the controller. For 1240s and 1130s, Ethernet MAC is the BVI MAC and should be used in the controller. If the MAC Address of the AP is not labeled on the AP, issue this command on the AP console:

```
At AP console: sh int | i Hardware


AP0017.94fe.d43f#sh int | i Hardware
  Hardware is BVI, address is 0017.94fe.d43f (bia 0017.94fe.d43f)
  Hardware is 802.11G Radio, address is 0017.94fe.d430 (bia 0017.94fe.d430)
  Hardware is 802.11A Radio, address is 0017.94fe.d430 (bia 0017.94fe.d430)
  Hardware is 88E6131 Ethernet Switch Port, address is 0009.b7ff.dba4
       (bia 0009.b7ff.dba4)
  Hardware is 88E6131 Ethernet Switch Port, address is 0009.b7ff.dba5
       (bia 0009.b7ff.dba5)
  Hardware is 88E6131 Ethernet Switch Port, address is 0009.b7ff.dba6
       (bia 0009.b7ff.dba6)
  Hardware is 88E6131 Ethernet Switch Port, address is 0009.b7ff.dba7
       (bia 0009.b7ff.dba7)
```

On the controller GUI interface, go to **Security**, and choose **MAC Filtering** on the left side of the window. Click **New...** to enter the MAC addresses:



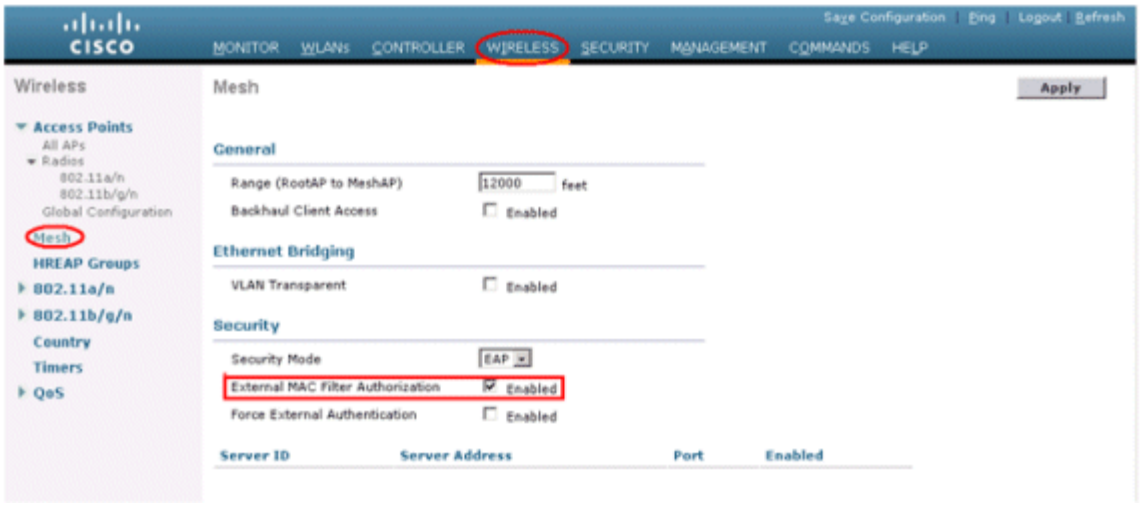
Also enter the names of the radios for convenience under **Description**. For example, like names of the cross streets where the radios have been installed for easy reference at any time.

Security

The other security that can be toggled is EAP (default) or PSK. You can also make a choice of Security mode as EAP, PSK, or External Authentication on the same page. From the GUI interface of the controller, use this path:

GUI Interface Path: **Wireless** > **Mesh**.

Enable Security on a MAP



Security can also be configured from the controller using this CLI:

```
(Cisco Controller) >config mesh security ?

eap             Enable mesh security EAP for Mesh AP.
psk             Enable mesh security PSK for Mesh AP.

rad-mac-filter Configure Mesh security radius mac-filter for Mesh AP.
force-ext-auth Configure Mesh security to force external authentication.
```

Security mode can be verified on the controller by these commands:

```
(Cisco Controller) >show mesh config

Mesh Range...................................... 12000
Backhaul with client access status.............. disabled
Background Scanning State....................... enabled

Mesh Security
   Security Mode................................ EAP
   External-Auth................................ disabled
   Use MAC Filter in External AAA server..... disabled
   Force External Authentication................ disabled

Mesh Alarm Criteria
   Max Hop Count................................ 4
   Recommended Max Children for MAP............. 10
   Recommended Max Children for RAP............. 20
   Low Link SNR................................. 12
   High Link SNR................................ 60
   Max Association Number....................... 10
   Association Interval......................... 60 minutes
   Parent Change Numbers........................ 3
   Parent Change Interval....................... 60 minutes

--More-- or (q)uit

Mesh Multicast Mode............................. In-Out
Mesh Full Sector DFS............................ enabled


Mesh Ethernet Bridging VLAN Transparent Mode..... disabled
```

```
(Cisco Controller) >show network summary

RF-Network Name............................. SEVT
Web Mode.................................... Disable
Secure Web Mode............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Web Mode Cipher-Option SSLv2......... Enable
Secure Shell (ssh).......................... Enable
Telnet...................................... Enable
Ethernet Multicast Mode..................... Disable
Ethernet Broadcast Mode..................... Disable
AP Multicast Mode........................... Unicast
```

```
IGMP snooping.............................. Disabled
IGMP timeout............................... 60 seconds
User Idle Timeout.......................... 300 seconds
ARP Idle Timeout........................... 300 seconds
Cisco AP Default Master.................... Disable
AP Join Priority........................... Disable
Mgmt Via Wireless Interface................ Enable
Mgmt Via Dynamic Interface................. Disable
Bridge MAC filter Config................... Enable
Bridge Security Mode....................... EAP
Mesh Full Sector DFS....................... Enable
--More-- or (q)uit
Over The Air Provisioning of AP's..... Disable
Apple Talk ................................ Disable
AP Fallback ............................... Enable
Web Auth Redirect Ports ................... 80
Fast SSID Change .......................... Disabled
802.3 Bridging ............................ Disable
```

External Authentication is supported through the use of one or more Cisco Secure Access Control Servers (ACSs). The ACS must be running version 4.1 or 4.2.

Note: ACS Express (5.0) has not been tested explicitly and initial tests indicate that it is incompatible with the existing VxWorks certificates.

Configuration is required on the controller and ACS. Support for external AAA is accomplished by validating the AP's certificate with the certificate installed on the ACS.

For an L3 mesh network, if one is using DHCP server, put the controller in L3 mode. Save the configuration and reboot the controller. Make sure you configure Option 43 on the DHCP server. After the controller has restarted, newly connected APs will receive their IP address from the DHCP server.

Option 43 can be used to populate the RAP controller address table with the address of a controller. This is very important if you are adding a RAP to a section of the network where it must traverse a Layer 3 hop to reach a controller. If the RAP has never been connected to a subnet where a controller is attached, it has never been able to discover this information.

The Cisco 152X Series MAPs accept an ASCII string format for Option 43 from a DHCP server. Cisco Aironet 152X Series APs use a comma-separated string format for DHCP Option 43. Other Cisco Aironet APs use the type-length-value (TLV) format for DHCP Option 43.

The AP152X series is an IOS platform, so it accepts Hex format for Option 43.

DHCP servers must be programmed to return the option based on the AP's DHCP Vendor Class Identifier (VCI) string (DHCP Option 60).

For Cisco IOS DHCP server configuration of Option 43, use these commands:

```
ip dhcp pool <pool name>
    network <IP Network> <Netmask>
    default-router <Default router>
    dns-server <DNS Server>
    option 43 hex  <0xf1> <1 byte len> <Controller IP addresses>
```

For example, if you want to configure 2 controllers IP addresses for a Huck, you have to configure Option 43 as a hexadecimal string in this format:

```
option 43 hex f10801041d0301041d21
              | ^ ^       ^
              | ^ ^       ^1.4.29.33
```

```
^ ^
^ ^1.4.29.3
^
^ length = 4 * number of ip addresses (4 * 2 = 8)

f1 is hardcoded value that needs to be added here
```

Here is an example from the DHCP server (which is a CAT6K that works for Huck):

```
ip dhcp pool vlan192
   network 1.4.29.0 255.255.255.0
   default-router 1.4.29.1
   option 60 ascii "Cisco AP c1520"
   option 43 hex f108.0104.1d03.0104.1d21
```

Add Option 60 for AP152X using this command:

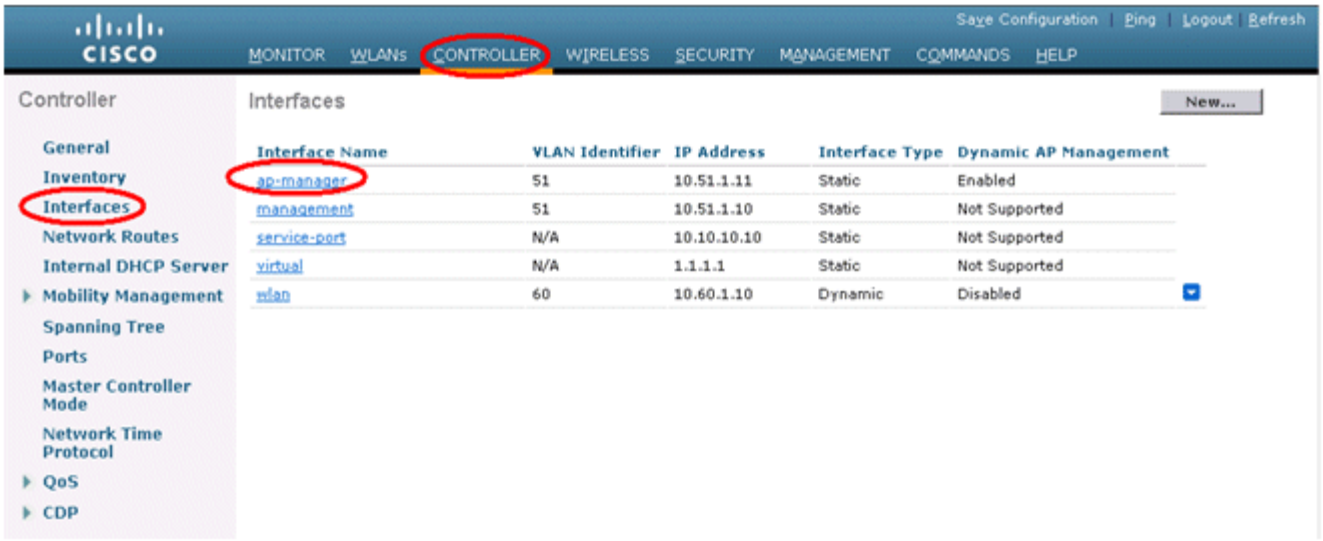
```
option 60 ascii "Cisco AP c1520"
```

Define AP Manager

For an L3 deployment, you must define the **ap-manager**. The AP Manager acts as a source IP address for communication from the Controller to the APs.

Path: **Controller** > **Interfaces** > **ap-manager** > **edit**.

AP Manager on the WLC



The **ap-manager** interface should be assigned an IP address in the same subnet and VLAN as your management interface.

Note: “AP-manager” is not required for WLC 5508. The Management Interface itself can act as a dynamic AP manager interface.

Mobility Group

The Mobility Group allows controllers to peer with each other to support seamless roaming across controller boundaries. APs learn the IPs of the other members of the mobility group after the CAPWAP Join process. A controller can be a member of a single mobility group of which up to 24 controllers are possible. Mobility is supported across 72 controllers. There can be up to 72 members (WLCs) in the mobility list with up to 24 members (WLCs) in the same mobility group (or domain) participating in client hand-offs. The main advantage of this feature is

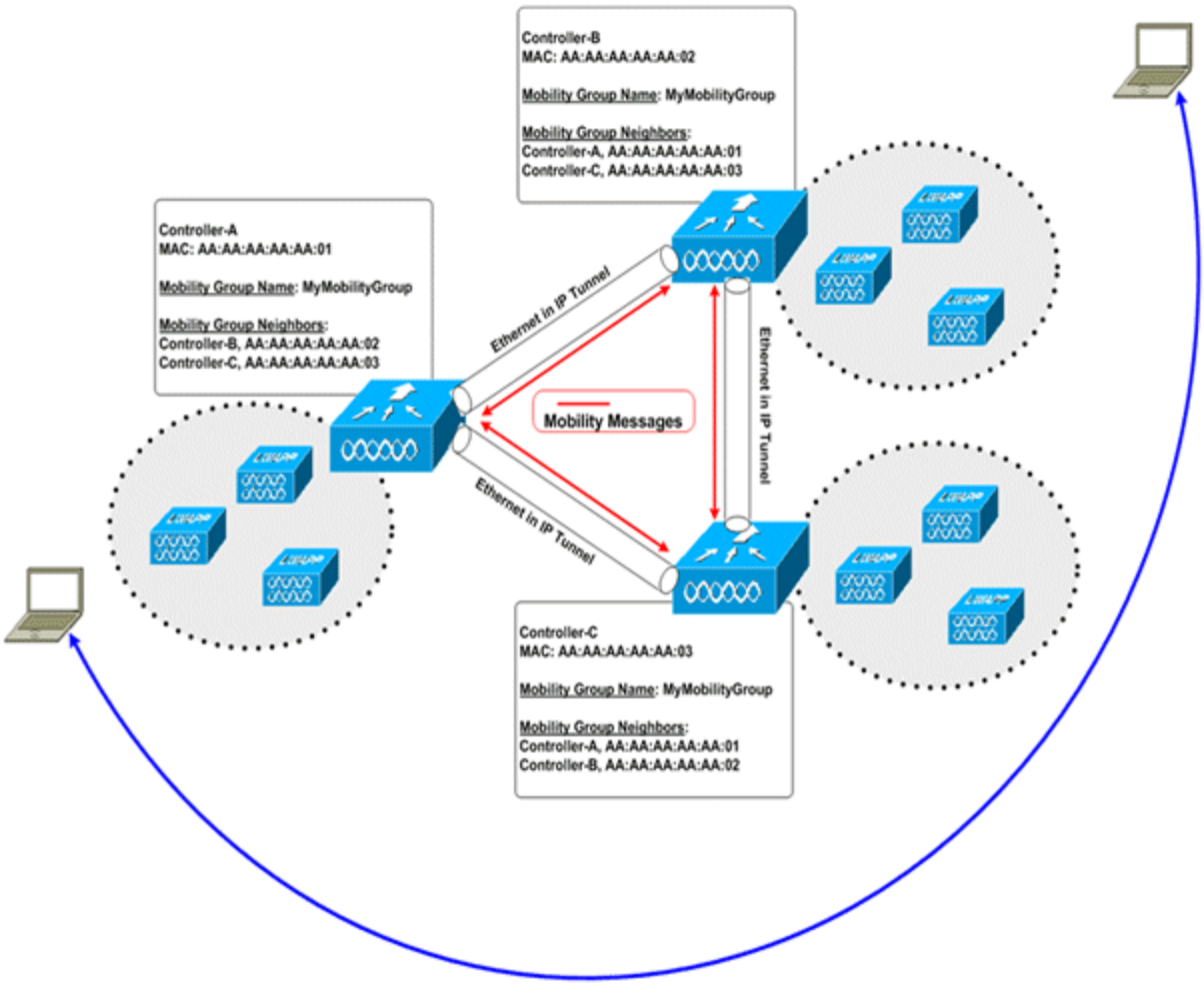
that IP address of the client does not have to be renewed in the same mobility domain. In other words, renewing an IP address is irrelevant in controller-based architecture by using this feature.

Clients can roam seamlessly (no IP address renewal, etc) between the mobility groups in a mobility domain. A mobility domain consists of all mobility groups configured. Large number of mobility groups can be created, constituting a mobility domain. The limit is 72 controllers total in a mobility domain.

Note: PMK cash only happens within the mobility group. As a result, fast roaming is possible within the mobility group, but seamless roaming is possible in a whole mobility domain (between mobility groups).

The controller members of this mobility group must be introduced manually, there is no protocol to auto-discover the other controllers which are members of our mobility group:

Mobility Group on the WLC



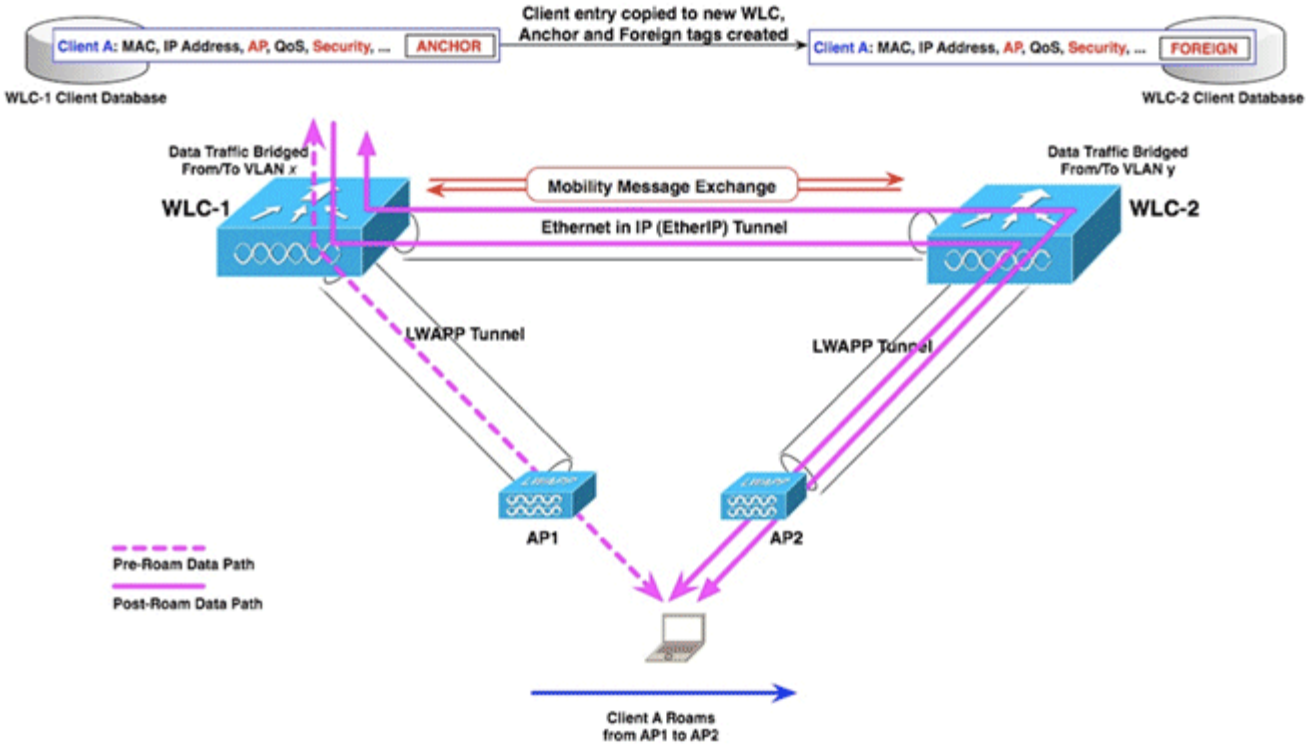
When a wireless client associates and authenticates to an AP, the AP's controller places an entry for that client in its client database. This entry includes the client's MAC and IP addresses, security context and associations, quality of service (QoS) contexts, the WLAN, and the associated AP. The controller uses this information to forward frames and manage traffic to and from the wireless client.

When the wireless client moves its association from one AP to another, the controller simply updates the client database with the newly associated AP. If necessary, new security context and associations are established as well.

When the client associates to an AP joined to a new controller, the new controller exchanges mobility messages with the original controller, and the client database entry is moved to the new controller. Data is tunneled between controllers using Ether in IP Tunnel (RFC3378). New security context and associations are established if necessary,

and the client database entry is updated for the new AP. This process remains transparent to the user.

Mobility Messages on the WLC



After initial setup, each WLC will only know about the local controller. The information regarding the other WLC must be introduced. Click **New**. You need for each WLC to configure the other WLC.

From the web interface, choose **Controller** > **mobility group**, and add the other WLC with its Management MAC address (the MAC address can be found under **Controller** > **Interface** > **Management**) and IP address.

Radio Roles

By default, a fresh AP out of the box has a radio role of a MAP. MAPs have a wireless connection and no direct wired connection to the WLC. MAPs always converge through a RAP.

A RAP must be explicitly configured as a RAP. This drastically reduces the configuration effort as now you have to just preconfigure the RAPs – and RAPs are fewer in number as compared to MAPs.

You can use the controller CLI to pre-configure the radio roles on an AP provided the AP is physically connected to the switch or you can see the AP on the switch as a RAP or a MAP:

```
(CiscoController) >config ap role ?

rootAP          RootAP role for the Cisco Bridge.
meshAP          MeshAP role for the Cisco Bridge.

(CiscoController) >config ap role meshAP ?

<Cisco AP>      Enter the name of the Cisco AP.

(CiscoController) >config ap role meshAP Map3

Changing the AP's role will cause the AP to reboot.
Are you sure you want to continue? (y/n) y
```

Role of a MAP

Installation and Connection Check

Deploy the radios (MAPs) at the desired locations.

Refer to the deployment guide for mesh.

Refer to the hardware installation guide.

Connect the AP you want as a RAP to the networking closet consisting of the WLC and other networking components, etc.

You should be able to see all the radios on the controller:

Radios on the WLC

```
(Cisco Controller) >show mesh ap summary

AP Name  AP Model           BVI MAC            CERT MAC           Hop  Bridge Group
                                                                      Name
------ ------------------  ----------------- ----------------- ---  -----------
HPRAP1 AIR-LAP1524PS-A-K9  00:1e:14:48:43:00 00:1e:14:48:43:00  0    test

HJRAP1 AIR-LAP1522AG-A-K9  00:1d:71:0d:e1:00 00:1d:71:0d:e1:00  0    huckmesh

HPMAP1 AIR-LAP1524PS-A-K9  00:1b:d4:a7:78:00 00:1b:d4:a7:78:00  1    test

HJMAP1 AIR-LAP1522AG-A-K9  00:1d:71:0c:f4:00 00:1d:71:0c:f4:00  1    huckmesh

HJMAP2 AIR-LAP1522AG-A-K9  00:1d:71:0c:f0:00 00:1d:71:0c:f0:00  1    huckmesh

HJMAP1 AIR-LAP1522AG-A-K9  00:1d:71:0d:d5:00 00:1d:71:0d:d5:00  1    huckmesh


Number of Mesh APs.............................. 6
Number of RAPs.................................. 2
Number of MAPs.................................. 4
```

On the controller GUI interface, click **Wireless** to see the RAP and MAPs.

RAPs and MAPs on the WLC

All APs

Search by AP MAC [ ] Search

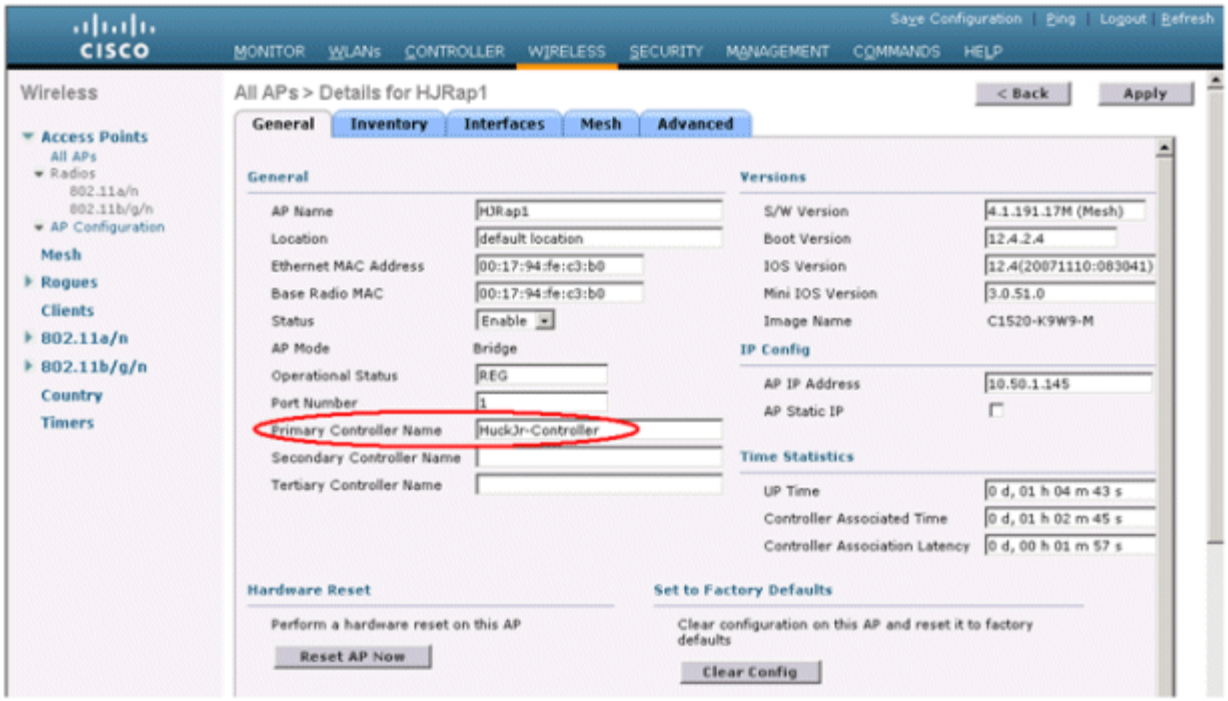
AP Name	AP MAC	AP Up Time	Admin Status	Operational Status	AP Mode	Certific Type
iMeshRap1	00:19:30:76:32:72	0 d, 22 h 24 m 25 s	Enable	REG	Local	MIC
HJRAP1	00:1d:71:0d:e1:00	0 d, 22 h 12 m 37 s	Enable	REG	Bridge	MIC
HJMAP3	00:1d:71:0d:d5:00	0 d, 22 h 05 m 04 s	Enable	REG	Bridge	MIC
HJMAP1	00:1d:71:0c:f4:00	0 d, 22 h 04 m 48 s	Enable	REG	Bridge	MIC
HJMAP2	00:1d:71:0c:f0:00	0 d, 22 h 04 m 53 s	Enable	REG	Bridge	MIC
HPRAP1	00:1e:14:48:43:00	0 d, 05 h 35 m 24 s	Enable	REG	Bridge	MIC
HPMAP1	00:1b:d4:a7:78:00	0 d, 22 h 04 m 25 s	Enable	REG	Bridge	MIC

If you have more than one controller connected to the same mesh network, then you must specify the name of the primary controller using global configuration for every AP, or specify primary controller on every node; otherwise, the least loaded controller will be preferred. If the APs were previously connected to a controller, they already have learned the controller's name.

After you configure the controller name, the APs will reboot. Go to the AP Detail screen to see the AP's **Primary Controller Name**:

Path: **Wireless** > **Cisco APs** > **Detail**.

Primary Controller on the WLC



Take advantage of the High Availability feature by configuring the IP addresses of the controllers on each AP:

Configure High Availability feature on the WLC

Entering an IP address for the backup controller is optional. If the backup controller is outside the mobility group to which the MAP is connected (the primary controller), then you need to provide the IP address of the primary, secondary, or tertiary controller, respectively. The controller name and IP address must belong to the same primary, secondary, or tertiary controller. If not, the MAP cannot join the backup controller. AP failover priority for MAPs is always “critical.”

Note: APs reboot after High Availability is configured.

Rogue Detection

Make sure that rouge detection is off for outdoor MAPs. It has been disabled by default to preserve backhaul bandwidth. However, it is configurable using this command:

```
(controller) config mesh ids-state ?
```

enable - Enables IDS(Rogue/Signature Detection) reporting for outdoor MAPs.

disable - Disables IDS(Rogue/Signature Detection) reporting for outdoor MAPs.

Bridge Group Name

Bridge Group Names (BGN) controls the association of the APs. BGNs can logically group the radios to avoid two networks on the same channel from communicating with each other. This setting is also useful if you have more than one RAP in your network in the same sector (area). The BGN is a string of 10 characters maximum.

A factory-set bridge group name is assigned at the manufacturing stage (NULL VALUE). It is not visible to you. As a result, even without a defined BGN, the radios can still join the network. The AP reboots after BGN configuration.

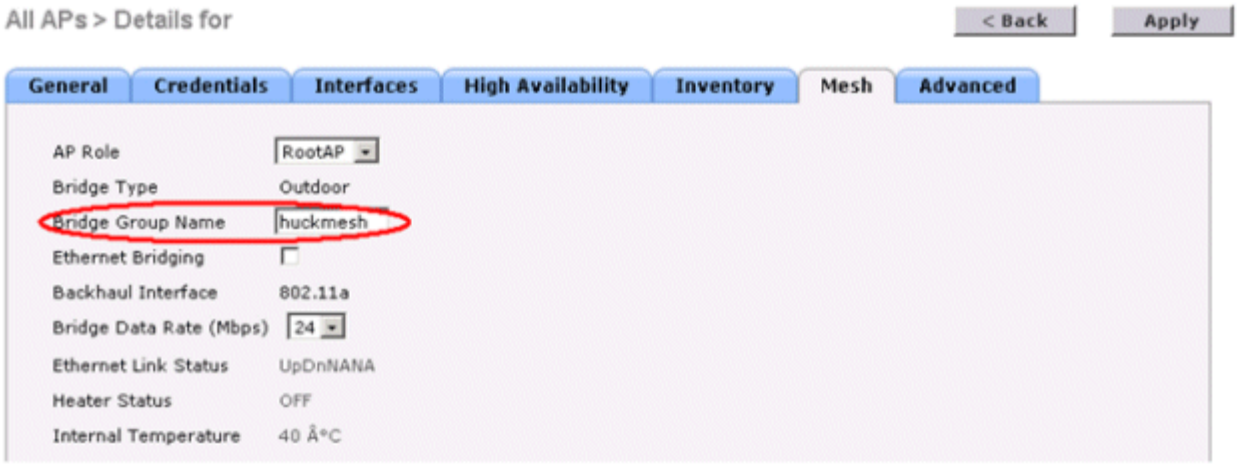
Note: The BGN should be configured very carefully on a live network. You should always start from the farthest node (last node) and move towards the RAP. The reasoning is that if you start configuring the BGN somewhere in the middle of the multihop, then the nodes beyond this point will be dropped as these nodes will have a different BGN (old BGN).

BGN is empty by default.

You can configure or verify the BGN using the controller GUI:

Path: **Wireless** >**All APs** > **Details**.

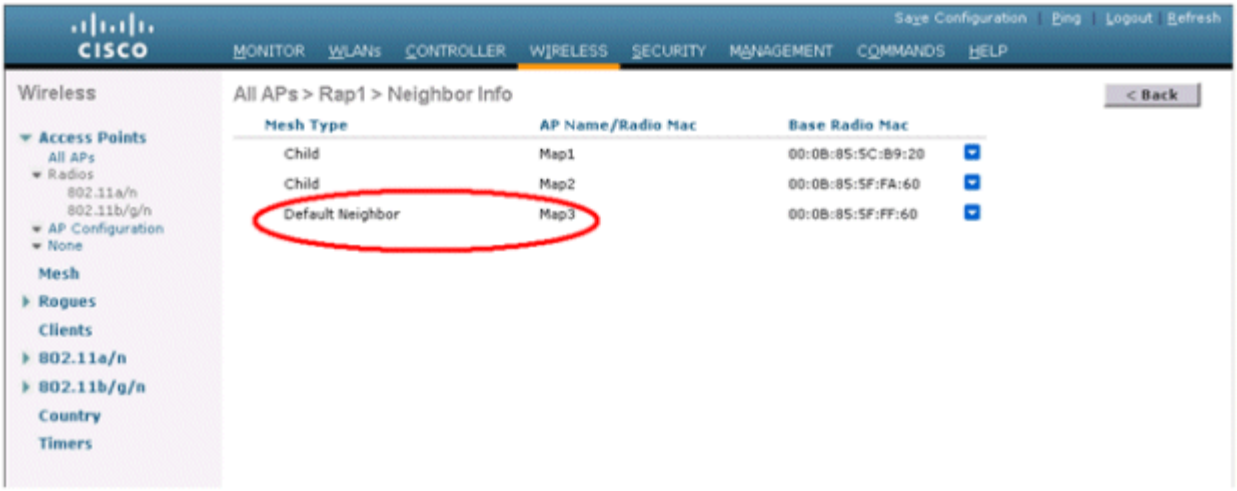
BGN on the WLC



If you have a running network, take a preconfigured AP with a different BGN and make it join the network. You will see this AP in the controller using “default” BGN after you add its MAC address in the controller:

```
(CiscoController) >show mesh path Map3:5f:ff:60

00:0B:85:5F:FA:60 state UPDATED NEIGH PARENT DEFAULT (106b), snrUp 48,
     snrDown 48, linkSnr 49
00:0B:85:5F:FA:10 state UPDATED NEIGH PARENT BEACON (86B), snrUp 72, snrDown 63,
     linkSnr 57
00:0B:85:5F:FA:10 is RAP
```

Neighbors on the RAP



AP152X using default BGN as a MAP, will associate wireless clients and form mesh relationships, but will not pass any Ethernet client traffic.

Make sure that you have matching BGNs for each spur of the deployment. Also, make sure you have no APs as “default parent or child,” as these APs will go into scan mode after 15 minutes and client connectivity will be lost.

Mobility deployment is very sensitive to “default BGNs,” as connectivity to the parent node and the clients are lost every 15 minutes.

Backhaul Interface

“Backhaul” is used only to create the wireless connection between the APs. The Backhaul Interface by default is 802.11a. You cannot change the backhaul interface to 11b/g.

In AP1524 SB, Slot 2 - 5 GHz radio in the RAP is used to extend the backhaul in the downlink direction, where as Slot 2 - 5 GHz radio in the MAP is used for the backhaul in the uplink. Cisco recommends using a directional antenna with Slot 2 radio. MAPs extend Slot 1 radio in the downlink direction with Omni or directional antenna also providing the client access. Client access can be provided on Slot 2 radio from 7.0 code and later.

Backhaul data rate plays an important role in a mobility deployment, as the data rate decides the minimum signal to noise ratio (SNR) requirement for each hop.

Data rates also affect the RF coverage and network performance. Lower data rates (such as 1 Mbps) can extend farther from the AP than can higher data rates (such as 54 Mbps). As a result, the data rate affects cell coverage and consequently the number of APs required. Different data rates are achieved by sending a more redundant signal on the wireless link, allowing data to be more easily recovered from noise. The number of symbols sent out for a packet at the 1 Mbps data rate is greater than the number of symbols used for the same packet at 11 Mbps. This means that sending data at the lower bit rates takes more time than sending the equivalent data at a higher bit rate, resulting in reduced throughput.

Typically, 24 Mb/s is chosen as the optimal backhaul rate because it aligns with the maximum coverage of the WLAN portion of the client WLAN of the MAP; that is, the distance between MAPs using 24 Mb/s backhaul should allow for seamless WLAN client coverage between the MAPs. A lower bit rate might allow a greater distance between MAPs, but there are likely to be gaps in the WLAN client coverage, and the capacity of the backhaul network is reduced. An increased bit rate for the backhaul network either requires more MAPs or results in a reduced SNR between MAPs, limiting mesh reliability and interconnection.

The controller CLI command for the Backhaul rate is:

(Cisco controller) > config ap bhrate *<backhaul rate> <ap-name>*

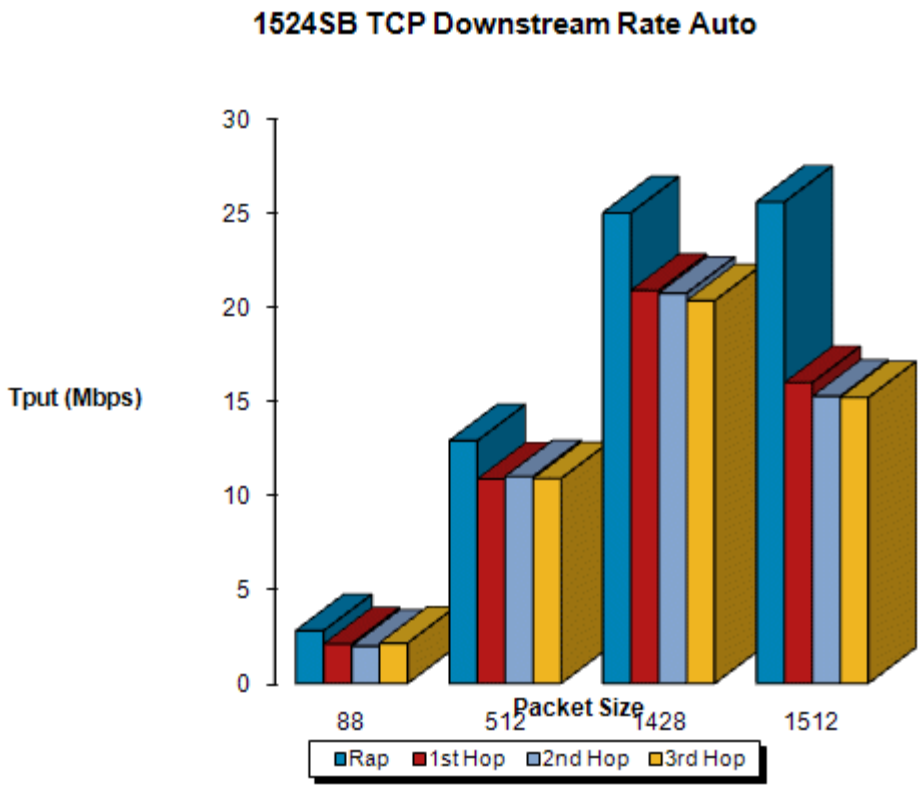
Dynamic Rate Adaptation

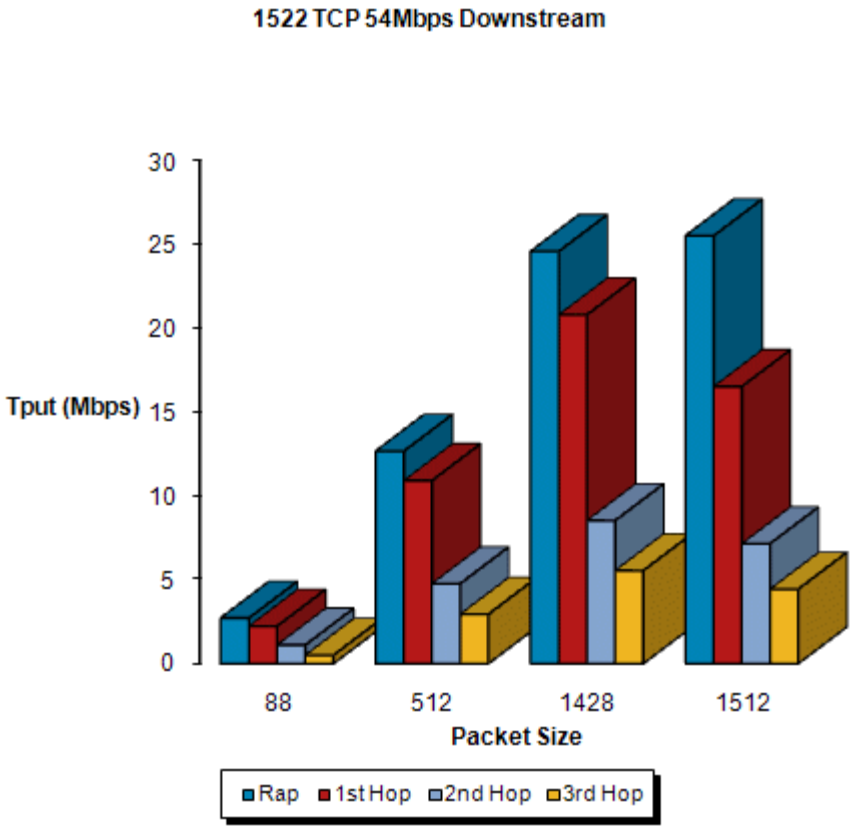
Dynamic Rate adaptation (DRA) was introduced for all mesh platforms in release 6.0. The rate selection is the key thing for proper utilization of the available RF spectrum. Clearly, rate can also affect the throughput of client devices, and throughput is a key metric used by industry publications to evaluate vendors' devices.

DRA introduces a process of estimating the optimal transmission rate for packet transmissions. It is important to properly select rates. If the rate is too high, packet transmissions will fail resulting in communications failure. If the rate is too low, the available channel bandwidth will not be used, resulting in inferior products, and the potential for catastrophic network congestion collapse.

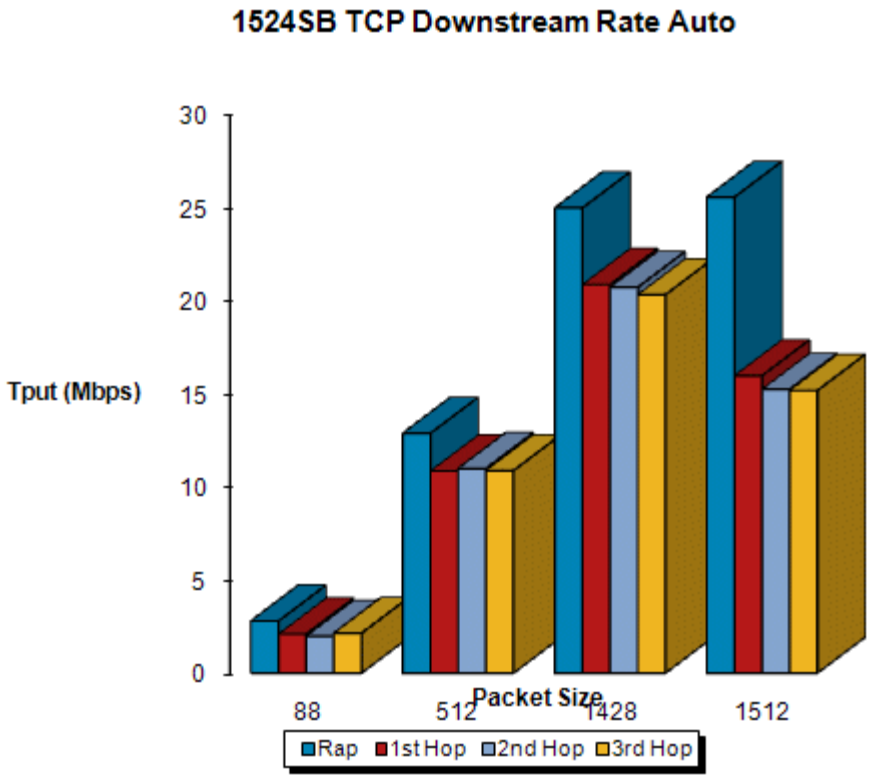
The default data rate for the mesh 5 GHz backhaul remains 24 MHz. To take advantage of DRA, configure the backhaul data rate to “auto.” With the “auto” setting, mesh backhaul picks the highest rate where the next higher rate cannot be used due to the conditions not being suitable for that rate and not because of conditions that affect all rates. For example, if mesh Backhaul chose 48 Mbps, then this decision has been taken after making sure that we cannot use 54 Mbps as there is not enough SNR for 54 and not because someone just turned on the microwave oven which will affect all rates.

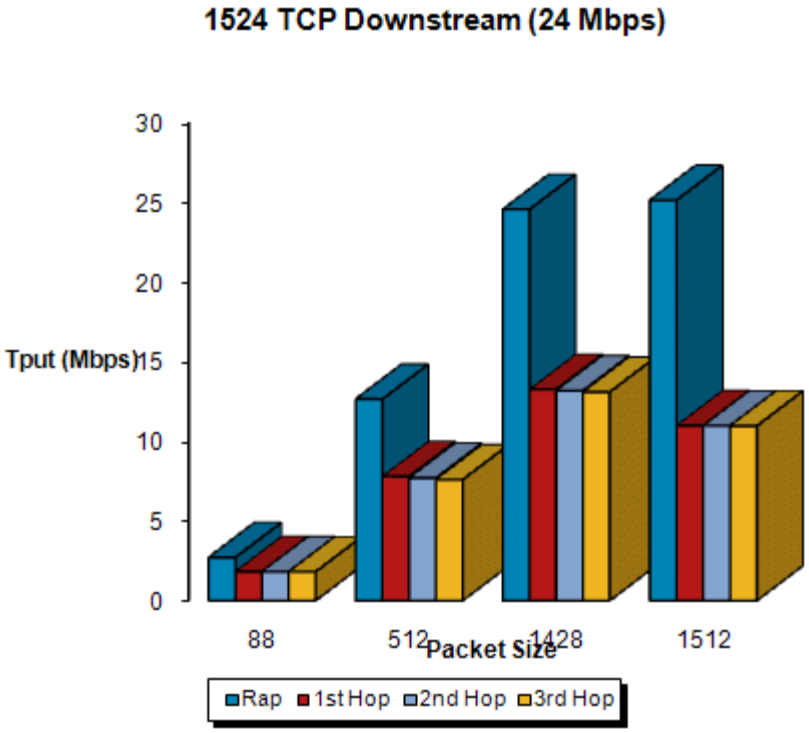
For Mobility deployments, Cisco recommends to take advantage of DRA. AP1524SB provides you with the best throughput, and throughput hardly degrades after the first hop. Its performance is much better than AP1522 and AP1524PS, because these APs have only a single radio for the backhaul uplink and downlink.





With DRA, each hop will use the best possible data rate for the backhaul. The data rate can be changed on a per-AP basis.

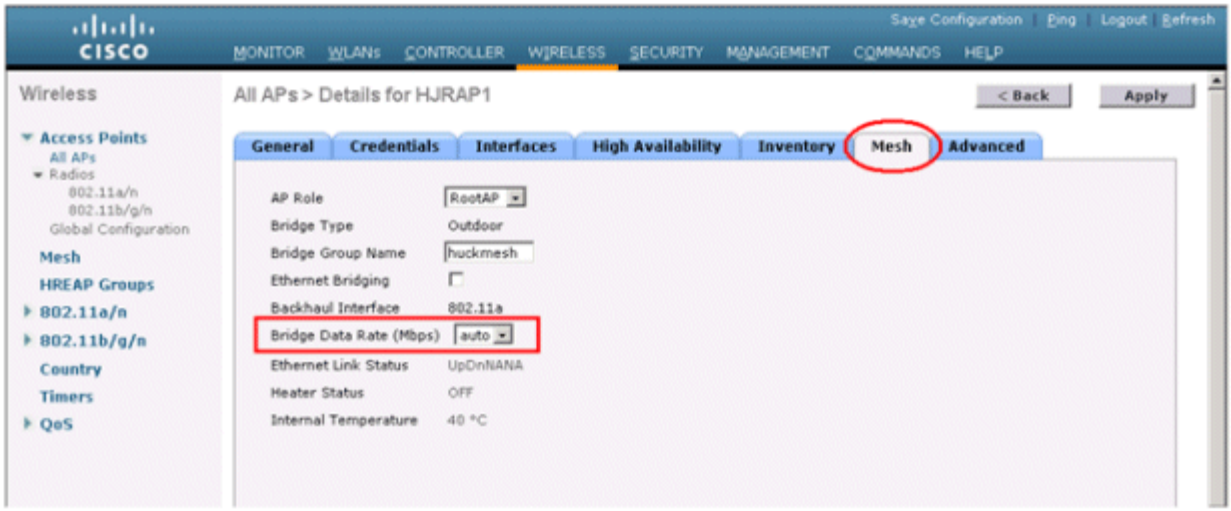




The data rate can be set on the backhaul on a per-AP basis. It is not a global command. After upgrading to 6.0 or later versions, the preconfigured value of the backhaul data rate will be preserved.

For example: If RAPon =24 Mbps, MAP1=18 Mbps etc, then the configurations will be preserved.

Data Rate on the Backhaul



Use this CLI to find out at what rate the backhaul is:

```
(Cisco Controller) >show ap bhate ?

<Cisco AP>     Enter the name of the Cisco AP.

(Cisco Controller) >show ap bhrate HPRAP1

Backhaul Rate is auto.
```

Use this CLI to configure the rate on the backhaul:

```
(Cisco Controller) >config ap bhrate ?

<rate in kbps> | "auto" Configures Cisco Bridge Backhaul Tx Rate.

(Cisco Controller) >config ap bhrate 36000 HPRAP1


(Cisco Controller) >show ap bhrate HPRAP1

Backhaul Rate is 36000.
```

Now, if the rate is set to “auto” and you want to know about the current rate being used on the backhaul, then use this CLI:

```
(Cisco Controller) >show mesh neigh summary HPRAP1

AP Name/Radio       Channel Rate Link-Snr Flags    State
-----------------   ------- ---- -------- -------  -----

00:0B:85:5C:B9:20   0       auto 4        0x10e8fcb8 BEACON
00:0B:85:5F:FF:60   0       auto 4        0x10e8fcb8 BEACON DEFAULT
00:0B:85:62:1E:00   165     auto 4        0x10e8fcb8 BEACON
OO:0B:85:70:8C:A0   0       auto 1        0x10e8fcb8 BEACON
HPMAP1              165     54   40       0x36     CHILD BEACON
HJMAP2              0       auto 4        0x10e8fcb8 BEACON
```

In the above screen, the RAP is using the "auto" backhaul data rate, and it is currently using 54 Mbps with its child MAP.

Serial Backhaul MAP Power and Channel Configuration

Configure the channel only on the RAP for the downlink, and then MAPs do the channel selection in an automated fashion. Channels are picked automatically from the channel subset giving each hop on a different channel.

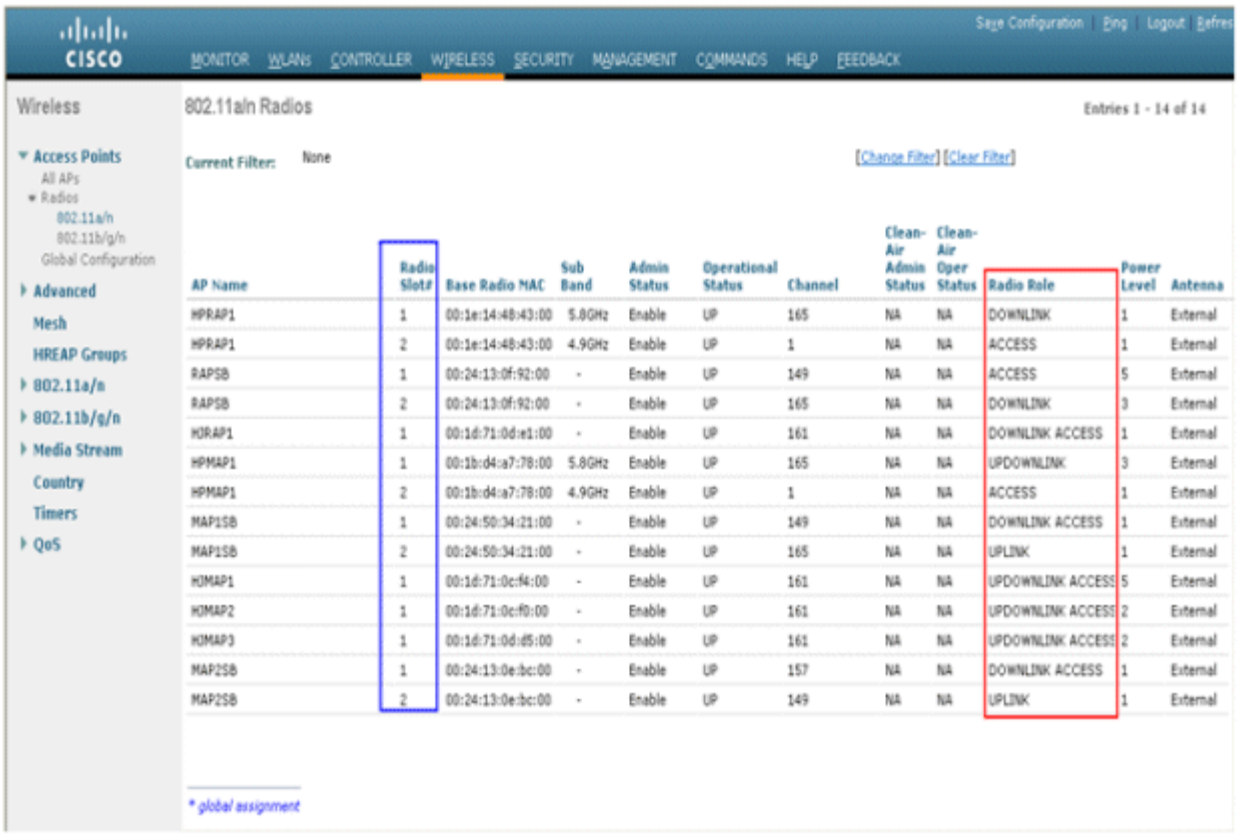
It is important to keep in mind the slot structure for radios as well. This command can be given to quickly check the

radio slot status:

```
(Cisco Controller 1) >show ap slots

Number of APs.................................... 9

AP Name             Slots  AP Model              Slot0   Slot1    Slot2   Slot3
------------------  -----  --------------------  ------- -------- ------- -------
HPRAP1               3     AIR-LAP1524PS-A-K9    b/g     a-5.8    a-4.9
RAPSB                3     AIR-LAP1524SB-A-K9    b/g     a-all    a-all
HJRAP1               2     AIR-LAP1522AG-A-K9    b/g     a-all
HPMAP1               3     AIR-LAP1524PS-A-K9    b/g     a-5.8    a-4.9
MAP1SB               3     AIR-LAP1524SB-A-K9    b/g     a-all    a-all
HJMAP1               2     AIR-LAP1522AG-A-K9    b/g     a-all
HJMAP2               2     AIR-LAP1522AG-A-K9    b/g     a-all
HJMAP3               2     AIR-LAP1522AG-A-K9    b/g     a-all
MAP2SB               3     AIR-LAP1524SB-A-K9    b/g     a-all    a-all
```

From the controller GUI, use this path: **Wireless** > **802.11a/n** under **Radios**.

Radio Slot Status



Along with the APs respective radio slots occupied and Radio Roles are displayed for a Serial Backhaul Deployment.

As shown in the above screenshot, Slot 2 - 5 GHz radio in the RAPSB (serial backhaul) is used to extend the backhaul in the DOWNLINK direction, whereas Slot 1 – 5 GHz radio in the RAPSB is used for client access. Slot 2- 5 GHz radio in the MAPSB is used for the UPLINK, and Slot 1 radio in the MAPSB is used for the DOWNLINK ACCESS Omni or directional antenna also providing the client access, and so on. With release 7.0 you can also have client access on Slot 2 radio. The above screenshot has been taken with 6.0 code, and has been changed with 7.0 code. For details, refer to "Dual 5 GHz Universal Client Access feature.

Dual Universal Client Access

As the roaming client can approach mesh infrastructure from either direction, so it becomes important to enable client

access on both the backhaul 5 GHz radios (Slot1 & 2). From 7.0 code release and later, client access is possible on both backhaul radios in AP1524SB and AP1523CV. Client access is disabled over both the Backhaul Radios by default.

Here are the guidelines to be followed for enabling or disabling client access on the radio slots constituting 5 GHz radios, irrespective of radios being used as downlink or uplink:

- You can enable client access on slot-1 even if client access on slot-2 is disabled.
- You can enable client access on slot-1 even if client access on slot-2 is disabled.
- If you disable client access on slot-1 the client access on slot-2 is automatically disabled on the CLI.
- For only disabling extended client access (on slot 2 radio) one has to use GUI.
- All the MAPs reboot whenever the client access is enabled or disabled.

The two 802.11a backhaul radios use the same MAC address. As a result, there may be instances where same WLANs map to the same BSSID on more than one slot.

For documentation purposes, we will call client access on Slot 2 radio as Extended Universal Access (EUA).

Configuration

Client access over both the backhaul radios can be configured either from the Controller CLI or Controller GUI or WCS. These configurations are explained here:

Configure EUA from Controller CLI

This command is used to enable client-access over both the backhaul radios. On executing this command, a warning message is generated indicating that the “same BSSID will be used on both the backhaul slots and all Serial Backhaul Mesh APs will reboot.”

```
config mesh client-access enable extended
```

This message is displayed:

```
Enabling client access on both backhaul slots
Same BSSIDs will be used on both slots
All Mesh Serial Backhaul APs will be rebooted
Are you sure you want to start? (y/N)
```

Both "Backhaul with client access status" and "Backhaul with client access extended status" can be determined using the **show mesh client-access** command.

```
show mesh client-access
```

The status appears:

```
Backhaul with client access status: enabled
Backhaul with client access extended status(3 radio AP): enabled
```

There is no explicit command to disable client-access only on Slot-2 (EUA). You have to disable client-access on both the backhaul slots using this command:

```
config mesh client-access disable
```

This message is displayed:

```
All Mesh APs will be rebooted
Are you sure you want to start? (y/N)
```

From the GUI, you can disable EUA without disturbing client access on the Slot 1 radio. But, again, the radios will reboot.

It is possible to enable client access only on Slot 1 and not on Slot 2 using this command:

```
config mesh client-access enable
```

This message is displayed:

```
All Mesh APs will be rebooted
Are you sure you want to start? (y/N)
```

Configure EUA from Controller GUI

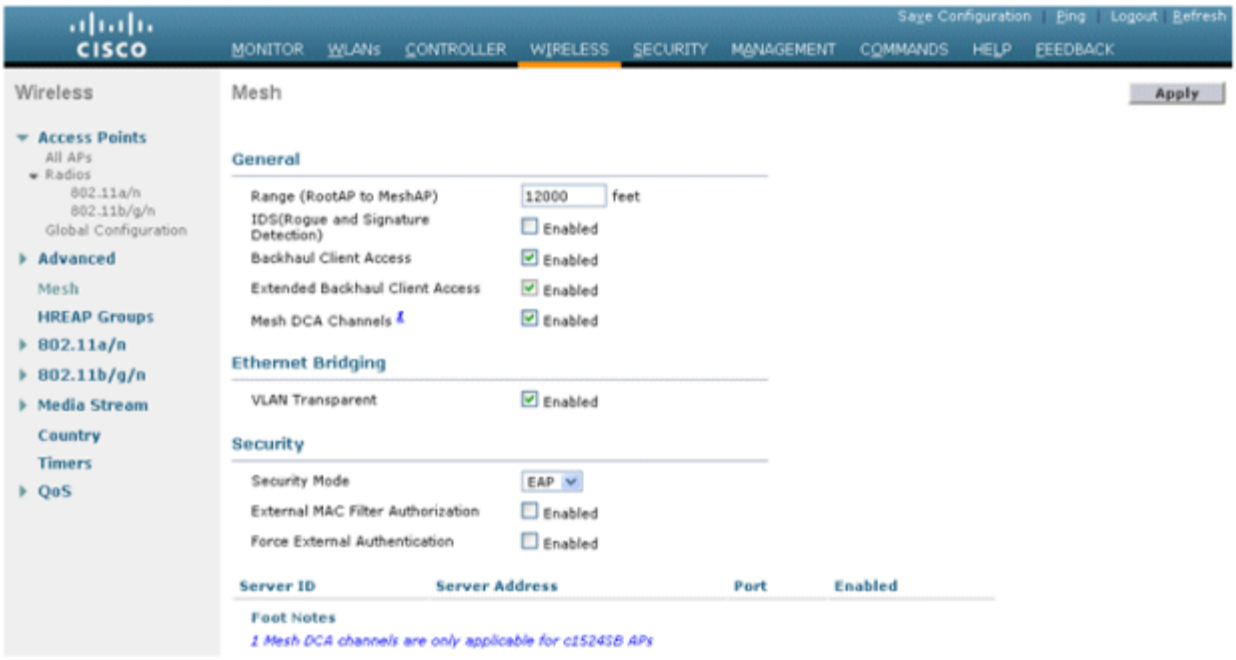
From the controller GUI, use this path: **Wireless** > **Mesh**.

Here is a screen capture of the controller GUI when Backhaul client access is disabled:

EUA on the WLC

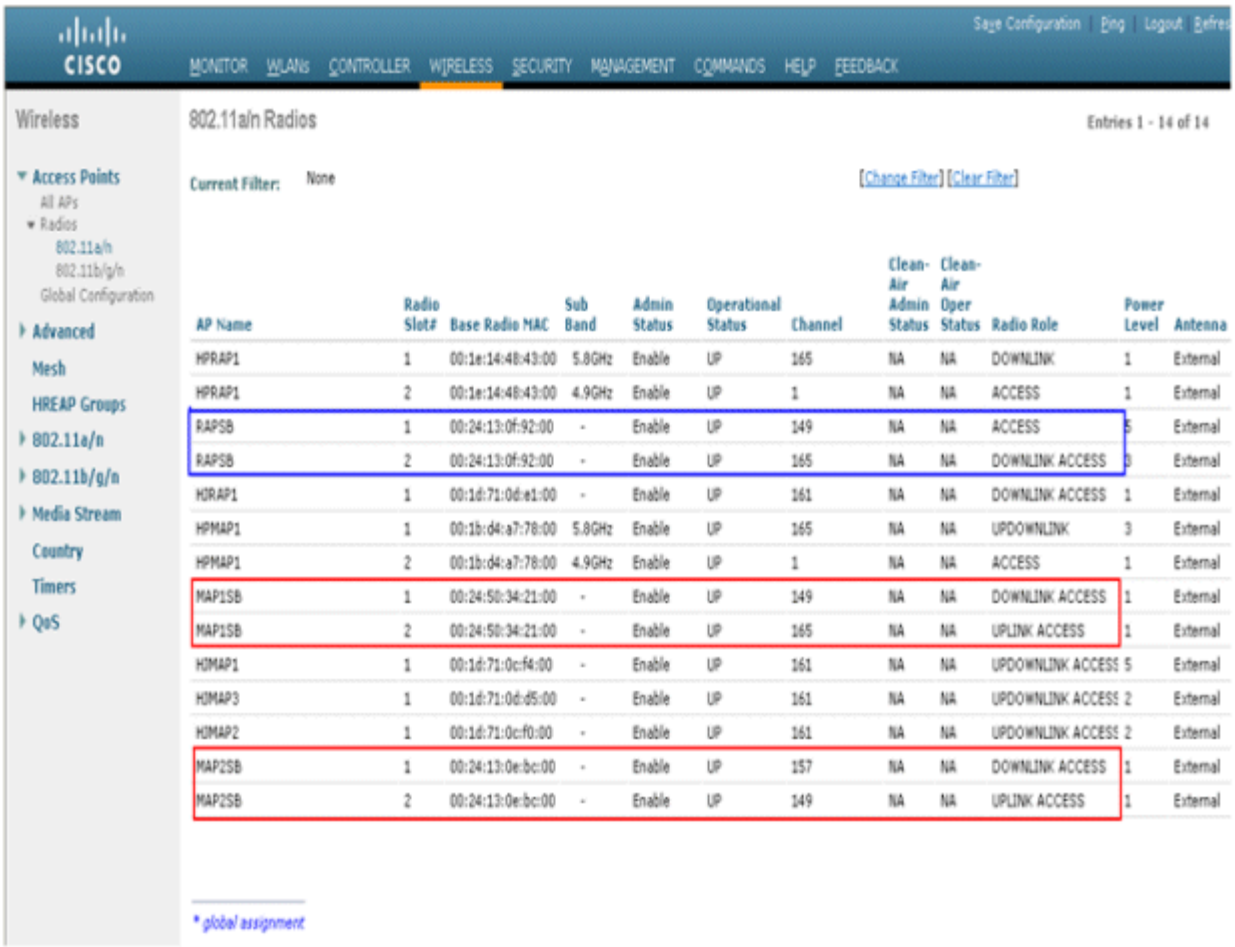
Choose the **Backhaul Client Access** check box to display the **Extended Backhaul Client Access** check box. A warning message will be generated after you click **Apply** with the **Extended Backhaul Client Access** option checked:

Configure Extended Backhaul Client Access

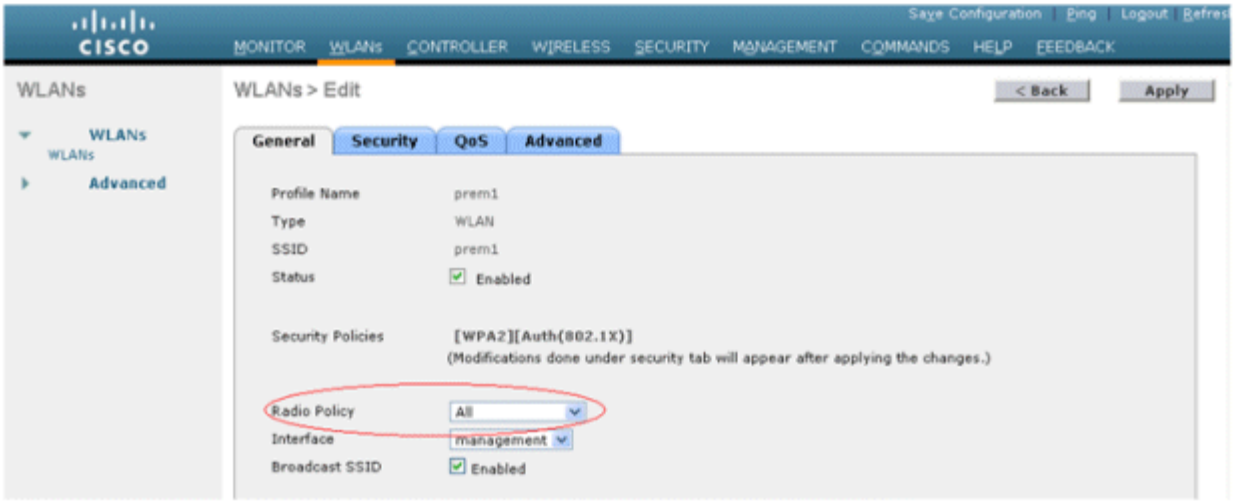


Once EUA is enabled, 802.11a radios are displayed as shown below. Slot 2 - 5 GHz radio in the RAPSB (serial backhaul) is used to extend the backhaul in the **DOWNLINK** direction, and is displayed as **DOWNLINK ACCESS**, whereas Slot 1 – 5 GHz radio in the RAPSB is used for client access is displayed as **ACCESS**. Slot 2 - 5 GHz radio in the MAPSB is used for the **UPLINK**, is displayed as **UPLINK ACCESS** and Slot 1 radio in the MAPSB is used for the **DOWNLINK ACCESS** with an Omni directional antenna also providing the client access, and so on.

802.11a Radios



Create a WLAN on the WLC with proper SSID mapped to the correct interface (VLAN). When you create a WLAN, it gets applied to all the radios by default. If you intend to enable client access only on the 802.11a radio, then choose the radio policy appropriately:

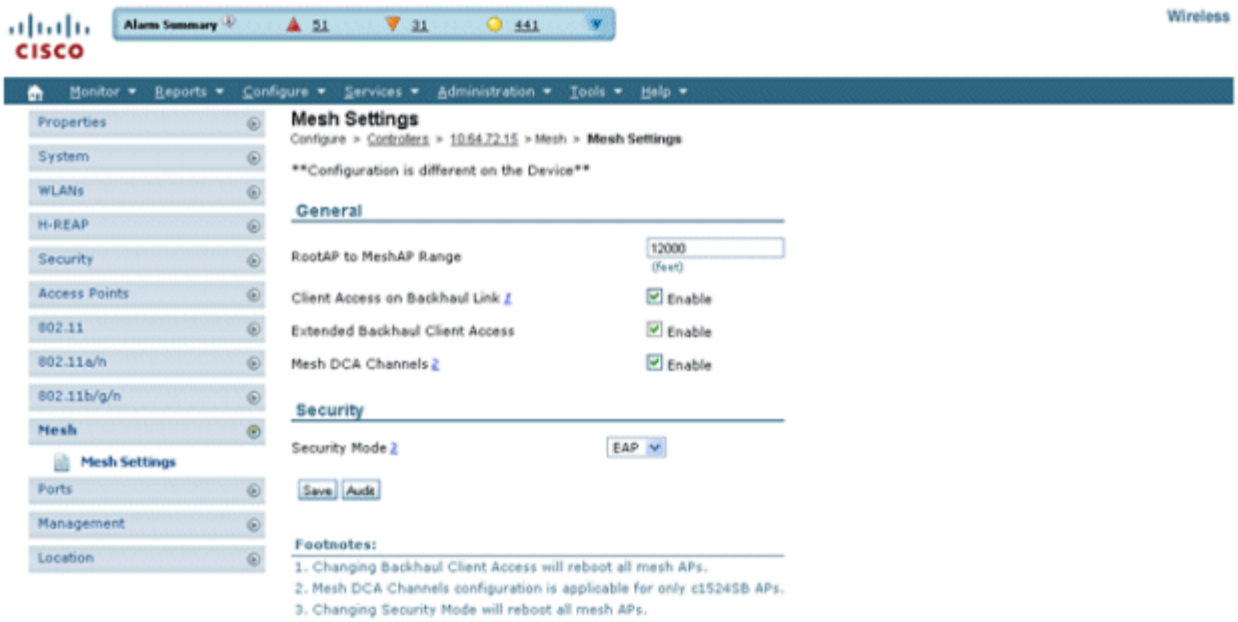


Configure EUA from WCS

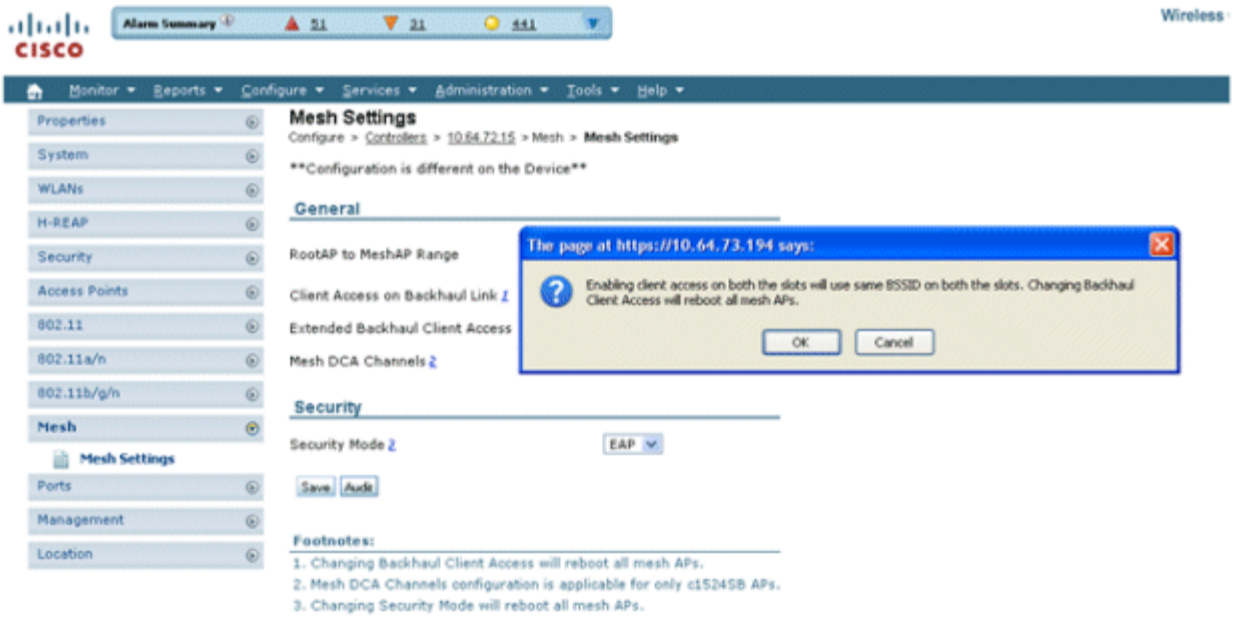
On the WCS, use this path: **configure** > **controllers** > **'controller ip'** > **Mesh** > **Mesh Settings**.

Here is the WCS mesh page when Backhaul Client Access is disabled:

Choose the **Client Access on Backhaul Link** check box to display the **Extended Backhaul Client Access** check box. A warning message will be generated after you click **Save** with the **Extended Backhaul Client Access** option checked:



Warning Message



Backhaul Channel Deselect

The basic purpose of this feature is to provide a means, by using which the end user can restrict the set of channels available to be assigned for the Serial Backhaul RAPs/MAPs. Normally, for the mesh world, channels are selected by the user for RAPs, and MAPs auto tune to RAP channels (for AP1522 and AP1522PS) or select channels automatically (AP1524SB and AP1523CV). Dynamic Channel Assignment (DCA) was not connected to the mesh world until release 6.0. However, with release 7.0, there is a connect between the DCA list and serial backhaul MAPs, only if someone uses (enables) this feature.

The way it works is that on removing certain channels from DCA list, and enabling the **mesh backhaul dca-channel command**, those channels will never be assigned to any serial backhaul APs, under any scenario. Even if radar is detected on all channels within the DCA list channels, the radio will be shut down rather than move to channels outside it. A trap message will be sent to the WCS, and a message will be displayed showing that the radio has been shut down because of DFS. The user will not be able to assign channel to serial backhaul RAP outside of the DCA list with

the **config mesh backhaul dca-channels enable**. However, this is not the scenario in the case of 1522/1524PS APs. For these APs, the user can assign any channel, even outside the DCA list in case of RAP, and the controller/AP can also select a channel outside the DCA list in case no radar free channel is available from within the list.

Since serial backhaul MAP channels are automatically assigned, this feature helps in regulating the set of channels that get assigned to MAPs. For example, if you do not want channel 165 to get assigned to any 1524 MAP, remove channel 165 from the DCA list and enable this feature.

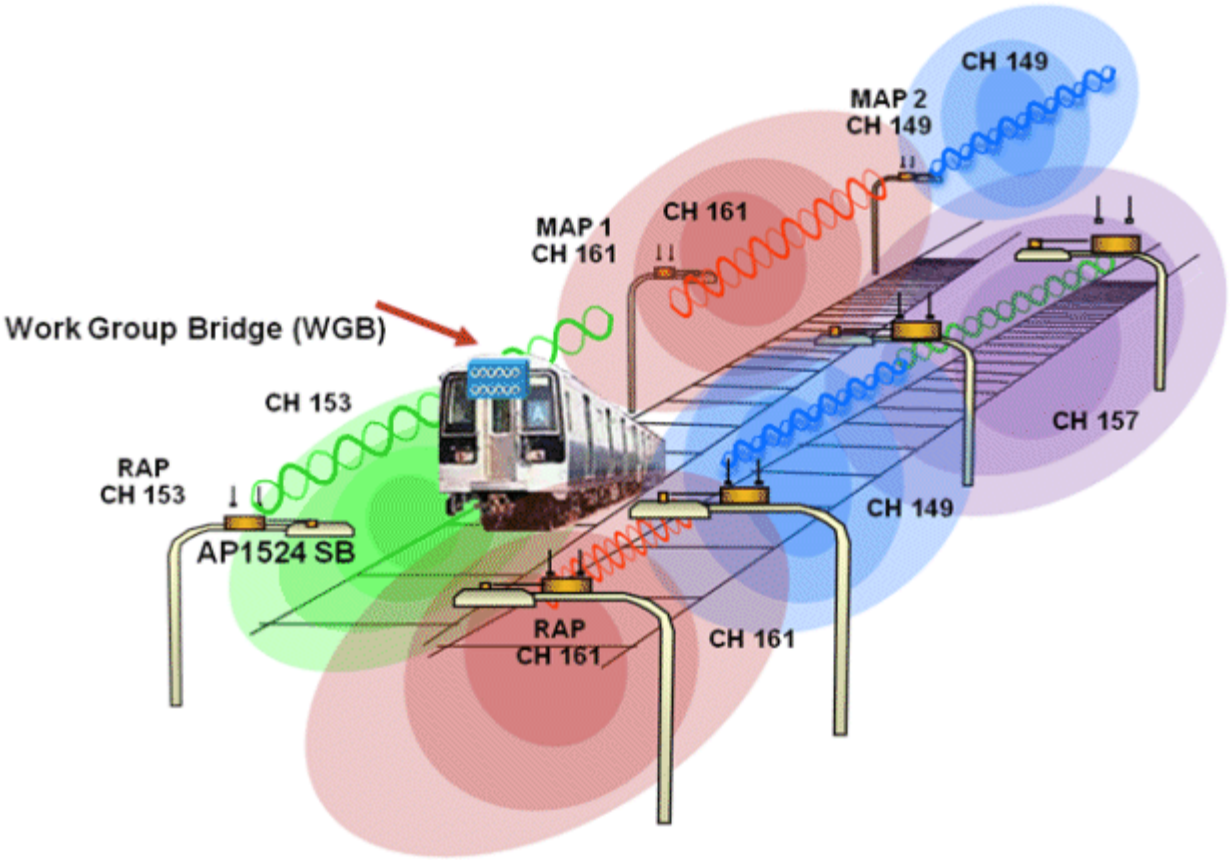
This feature is best suited for outdoor mesh inter-operability scenarios with indoor MAPs or WGBs which support a channel set different from outdoor APs. For example, channel 165 is supported by outdoor APs but not by indoor APs in -A domain.

The band select feature facilitates mobility of WGB or MAR3200 with mesh infrastructure, as it allows the user to configure a common set of channels available on MAPs and roaming WGB or MAR3200. By enabling the backhaul channel deselection feature, you can restrict channel assignment to only those channels which are available to autonomous APs and outdoor APs.

Note: Channel deselection is only possible in 7.0 code and later.

In some scenarios, you might have two linear tracks or roads for mobility side-by-side. As channel selection of MAPs happens automatically, so there can be a hop at a channel which is not available on the autonomous side, or the channel has to be skipped due to the same or adjacent channel being selected in the neighborhood AP which belongs to a different linear chain. You can do better frequency planning on two adjacent spurs by making use of this feature.

Mobility Side-by-Side



Configuration from CLI

1. Use the **show advanced 802.11a channel** command to review the channel list already configured in the DCA

list:

```
(Controller) >show advanced 802.11a channel
Automatic Channel Assignment
Channel Assignment Mode..................... AUTO
Channel Update Interval..................... 600 seconds
Anchor time (Hour of the day)................ 0
Channel Update Contribution................. SNI..
CleanAir Event-driven RRM option............ Enabled
CleanAir Event-driven RRM sensitivity....... Medium
Channel Assignment Leader................... 09:2b:16:28:00:03
Last Run.................................... 286 seconds ago
DCA Sensitivity Level....................... MEDIUM (15 dB)
DCA 802.11n Channel Width................... 20 MHz
DCA Minimum Energy Limit.................... -95 dBm
Channel Energy Levels
Minimum..................................... unknown
Average..................................... unknown
Maximum..................................... unknown
Channel Dwell Times
Minimum..................................... 0 days, 17 h 02 m 05 s
Average..................................... 0 days, 17 h 46 m 07 s
Maximum..................................... 0 days, 18 h 28 m 58 s
802.11a 5 GHz Auto-RF Channel List
Allowed Channel List.....................36,40,44,48,52,56,60,64,116,140
Unused Channel List.....................100,104,108,112,120,124,128,132,136
DCA Outdoor AP option....................... Disabled
```

2. To add a channel to the DCA list, use the **config advanced 802.11a channel add** <*channel number*> command. You can also delete a channel number from the DCA list using the **config advanced 802.11a channel delete** <*channel number*> command.

   Note: Before you add or delete the channel number from the DCA list, the 802.11a network needs to be disabled. Use the **config 802.11a disable network** and **config 802.11a enable network** commands in order to disable and enable the 802.11a network respectively.

   Also, you cannot directly delete a channel from the DCA list if it is assigned to any serial backhaul RAP. To delete a channel assigned to a RAP, you must first change the channel assigned to the RAP and then issue the **config advanced 802.11a channel delete** <*channel number*> command from the controller.

```
(Controller) >config 802.11a disable network
Disabling the 802.11a network may strand mesh APs. Are you sure you want to
continue? (y/n)y
(Controller) >config advanced 802.11a channel add 132
802.11a network needs to be disabled

(Controller) >config advanced 802.11a channel delete 116
802.11a 5 GHz Auto-RF:
Allowed Channel List....................... 36,40,44,48,52,56,60,64,116,
132,140
DCA channels for Serial Backhaul Mesh APs is enabled.
DCA list should have at least 3 non public safety channels supported by Serial
     Backhaul Mesh APs.
Otherwise, the Serial Backhaul Mesh APs can get stranded.
Are you sure you want to continue? (y/N)y
Failed to delete channel.
Reason: Channel 116 is configured for one of the Serial Backhaul RAPs.
Disable mesh backhaul dca-channels or configure a different channel for Serial
     Backhaul RAPs.
(Controller) >config advanced 802.11a channel delete 132
802.11a 5 GHz Auto-RF:
Allowed Channel List....................... 36,40,44,48,52,56,60,64,116,
132,140
DCA channels for Serial Backhaul Mesh APs is enabled.
DCA list should have at least 3 non public safety channels supported by Serial
     Backhaul Mesh APs.
Otherwise, the Serial Backhaul Mesh APs can get stranded.
Are you sure you want to continue? (y/N)y
(Controller) >config 802.11a enable network
```

3. Once a suitable DCA list has been created, use the **config mesh backhaul dca-channels enable** command to enable the backhaul channel deselection feature for serial backhaul mesh access point. You can issue the **config**

mesh backhaul dca-channels disable command in case the feature needs to be disabled.

Note: It is not required to disable the 802.11a network to enable/disable this feature.

```
(Controller) >config mesh backhaul dca-channels enable
802.11a 5 GHz Auto-RF:
Allowed Channel List..................... 36,40,44,48,52,56,60,64,116,
140
Enabling DCA channels for Serial Backhaul mesh APs will limit the channel set
     to the DCA channel list.
DCA list should have at least 3 non public safety channels supported by Serial
     Backhaul Mesh APs.
Otherwise, the Serial Backhaul Mesh APs can get stranded.
Are you sure you want to continue? (y/N)y
(Controller) >config mesh backhaul dca-channels disable
```

4. You can check the current status of the backhaul channel deselection feature using the **show mesh config** command.

```
(Cisco Controller) >show mesh config

Mesh Range....................................... 12000
Mesh Statistics update period.................... 3 minutes
Backhaul with client access status............... enabled
Background Scanning State........................ enabled
Backhaul Amsdu State............................. disabled

Mesh Security
   Security Mode................................. PSK
   External-Auth................................. enabled
      Radius Server 1............................ 9.43.0.101
   Use MAC Filter in External AAA server......... disabled
   Force External Authentication................. disabled

Mesh Alarm Criteria
   Max Hop Count................................. 4
   Recommended Max Children for MAP.............. 10
   Recommended Max Children for RAP.............. 20
   Low Link SNR.................................. 12
   High Link SNR................................. 60
   Max Association Number........................ 10
   Association Interval.......................... 60 minutes
   Parent Change Numbers......................... 3
   Parent Change Interval........................ 60 minutes


Mesh Multicast Mode.............................. In-Out
Mesh Full Sector DFS............................. enabled


Mesh Ethernet Bridging VLAN Transparent Mode..... enabled

Mesh DCA channels for Serial Backhaul Mesh APs..... disabled
```

5. To assign a particular channel to 1524 RAP downlink radio, use the **config slot** <*slot number*> **channel ap** <*ap-name*> <*channel number*> command.

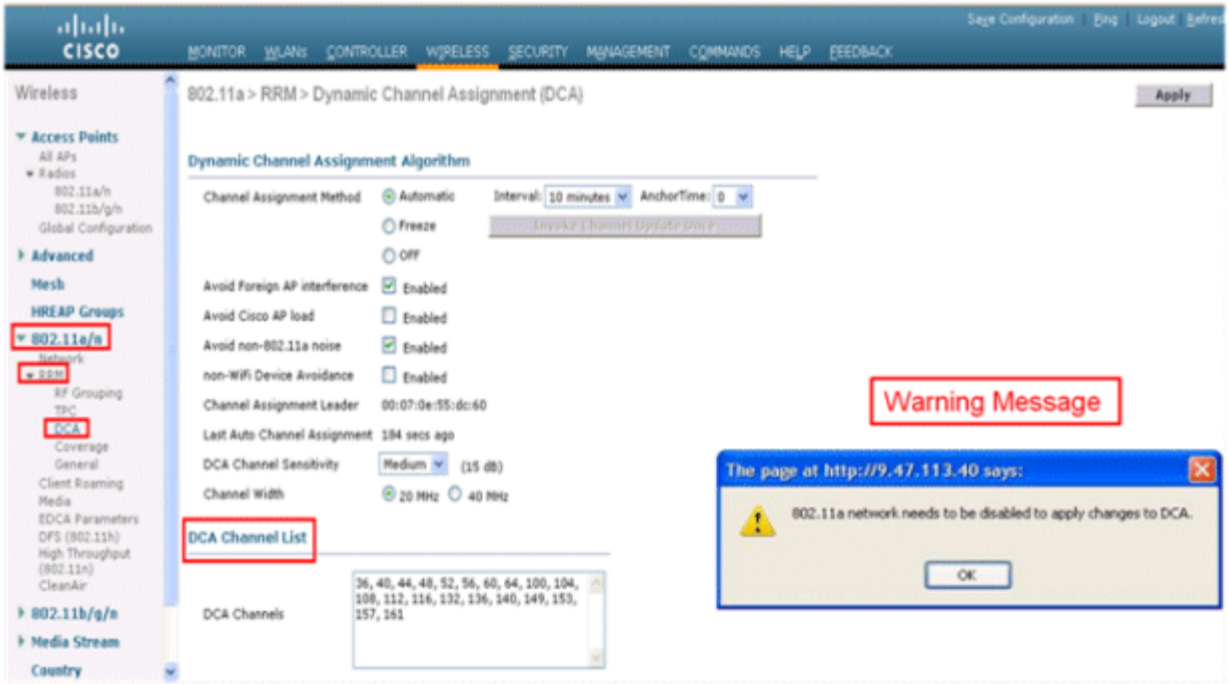
Note: Slot 2 acts as downlink radio in the case of 1524SB RAP. Also, if backhaul channel deselection is enabled, then you can assign only those channels which are available in the DCA list.

```
(Cisco Controller) >config slot 2 channel ap RAP2-1524 136
Mesh backhaul dca-channels is enabled. Choose a channel from the DCA list.
(Cisco Controller) >config slot 2 channel ap RAP2-1524 140
```

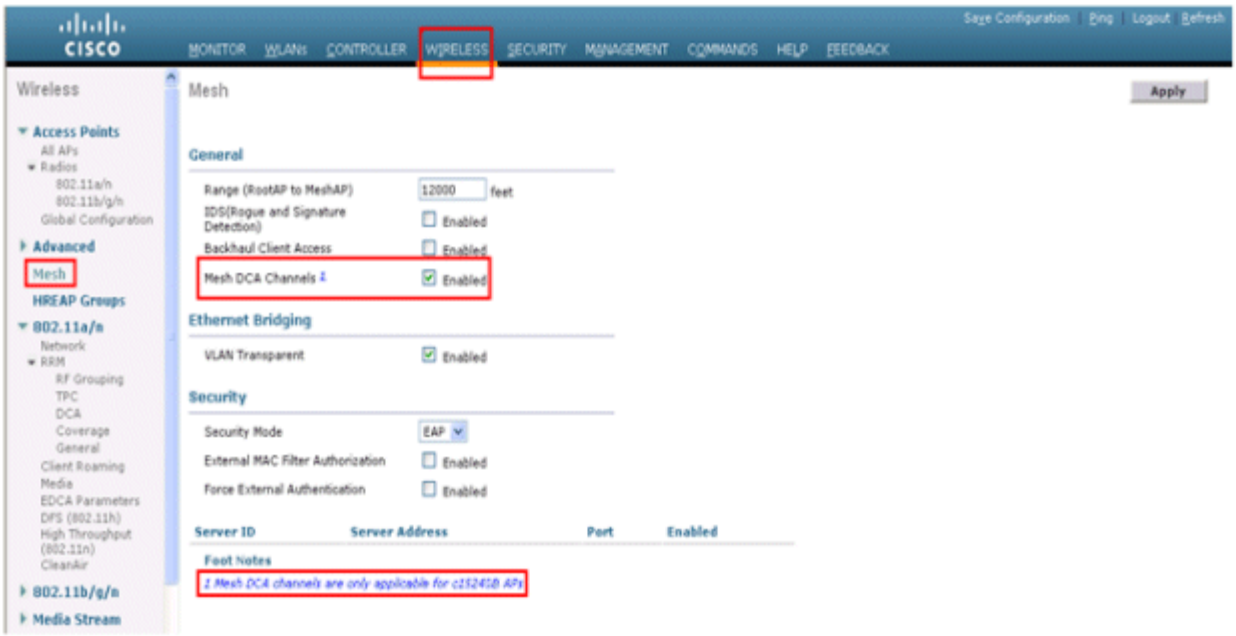
Configuration from GUI

Perform these steps to configure the DCA list and backhaul channel deselection feature:

Choose **Controller** > **Wireless** > **802.11a/n** > **RRM** > **DCA**, and choose one or more channels to be included in the DCA list:

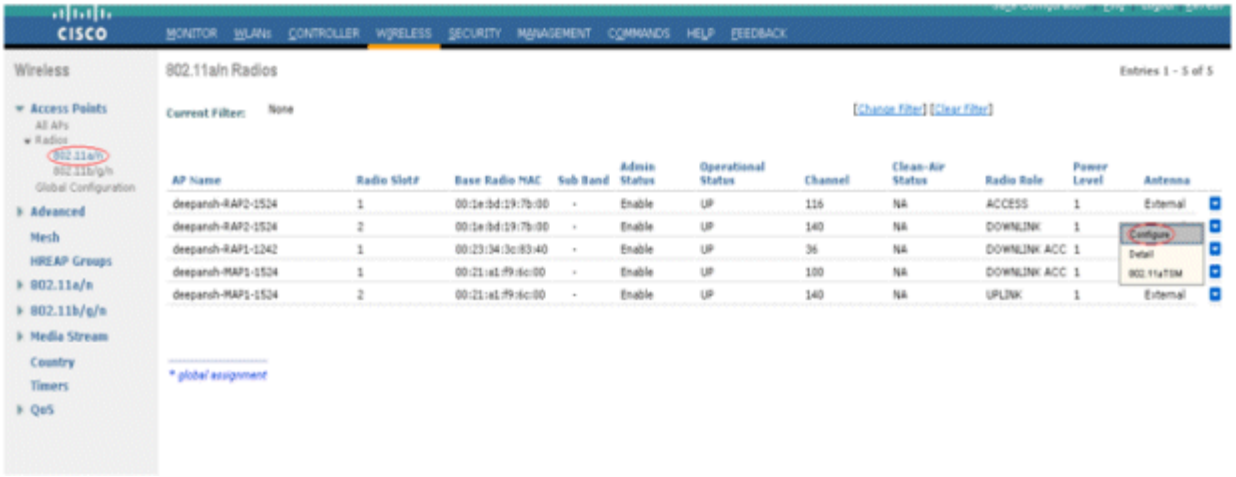


Choose **Wireless** > **Mesh**, and choose the **Mesh DCA Channels** option to enable backhaul channel deselection using the DCA list. This option is applicable for 1524SB APs.

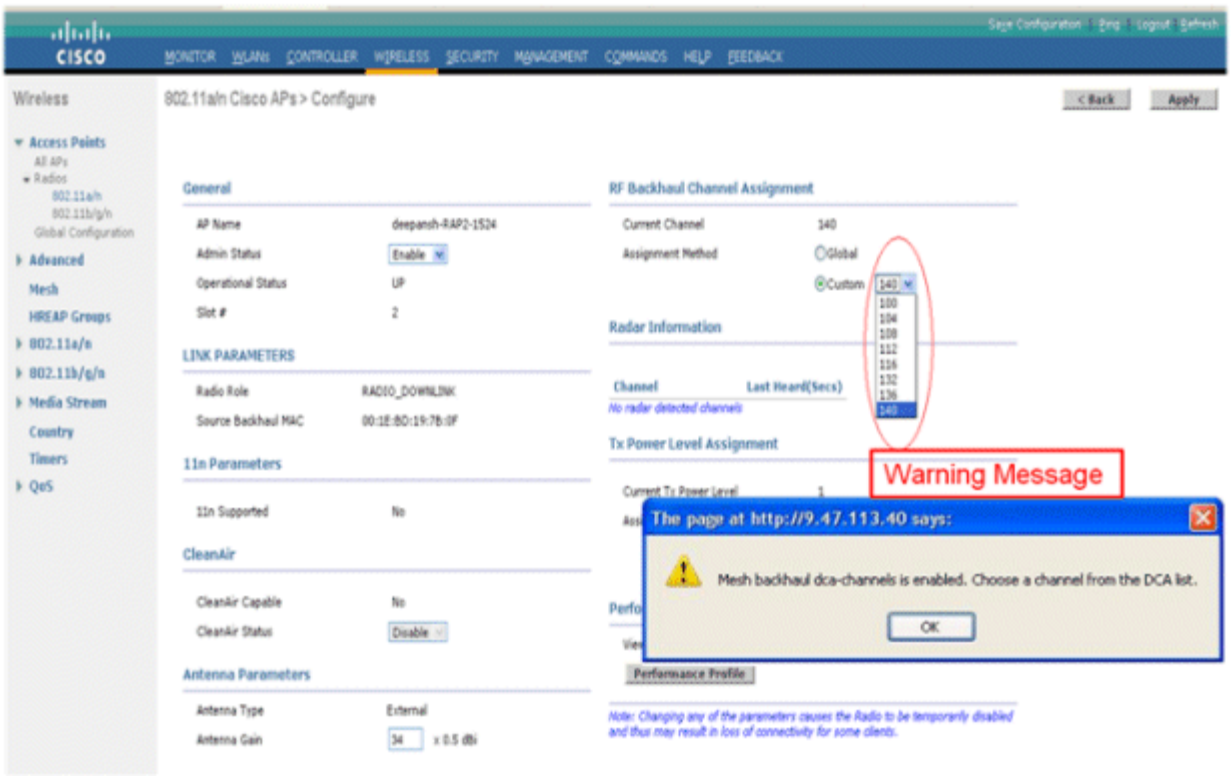


Perform these steps to set the channel for RAP downlink radio:

Choose **Wireless** > **Access Points** > **Radios** > **802.11a/n**, to configure channels on the RAP downlink radio. From the list of APs, choose the Antenna drop-down list for a RAP, and choose **Configure**:



From the **RF Backhaul Channel** assignment section, choose **Custom**, and then choose the channel for RAP downlink radio:



Useful Information/Things to Keep in Mind

- The channel for serial backhaul RAP 11a access radio and both 11a radios of serial backhaul MAPs get assigned automatically. They cannot be configured by the user.
- Watch for trap logs on the controller. In case of radar detection and subsequent channel change, you will see messages similar to this:

```
Channel changed for Base Radio MAC: 00:1e:bd:19:7b:00 on 802.11a
radio. Old Channel: 132. New Channel: 116. Why: Radar. Energy
before/after change: 0/0. Noise before/after change: 0/0.
Interference before/after change: 0/0.

Radar signals have been detected on channel 132 by 802.11a radio
with MAC: 00:1e:bd:19:7b:00 and slot 2
```

- For every serial backhaul AP, the channel on its downlink and uplink radio should always be non-interfering (for example, if uplink is channel 104, any of 100, 104 and 108 channels cannot be assigned for downlink radio on that AP). As a result, the alternate adjacent channel is also selected for 11a access radio on RAP.
- In case radar signals are detected on all channels except uplink radio channel, downlink radio will be shut and the uplink radio itself will act as both uplink and downlink (that is, behavior is similar to 1522 APs in this case).
- Radar detection gets cleared after 30 minutes, so any radio shut down due to radar detection should be back up and operational after this duration.
- There is a 60-second silence period immediately after moving to a DFS enabled channel (regardless of whether the channel change was due to radar detection or user configured in case of RAP), during which the AP is supposed to scan for radar signals without transmitting anything. Hence, the small period (60 seconds) of downtime may be observed in case of radar detection, if the new channel assigned is also DFS enabled. If radar detection is observed again on the new channel during the silence period, the parent will change its channel without informing the child AP, as it is not allowed to transmit during the silence period. In this case, the child AP will disassociate and go back to scan mode, rediscover the parent on the new channel, and then join back, leading to slightly longer (approximately three minute) downtime.
- In the case of RAP, the channel for downlink radio is always selected from within the DCA list, regardless of whether the backhaul channel deselection feature is enabled or not. Behavior is different for MAPs, which can pick any channel allowed for that domain, unless the backhaul channel deselection feature is enabled which will restrict the allowed channel set. As a result, it is recommended to have a lot of channels added to the 802.11a DCA channel list to prevent any radio getting shut down due to lack of channels even if the backhaul channel deselection feature is not in use.
- Since the same DCA list that was until now used for RRM feature is also being used for MAPs through the backhaul channel deselection feature, keep in mind that any addition/deletion of channels from the DCA list will affect the channel list input to the RRM feature for non MAPs as well. RRM is off for mesh.
- **Note:** In the case of the –M domain APs, a slightly longer time interval may be required for the mesh network to come up, since you now have a longer list of DFS enabled channels in –M domain, which each AP will be scanning before joining the parent, and therefore may take 25%-50% more time than normal to join.

Site Preparation and Planning

Cisco recommends that you perform a radio site survey before installing the equipment. A site survey reveals problems such as interference, Fresnel zone, or logistics problems. A proper site survey involves temporarily setting up mesh links and taking measurements to determine whether your antenna calculations are accurate. Be sure to determine the correct location and antenna before drilling holes, routing cables or mounting equipment. Visiting each site where each AP has to be deployed helps a lot. One can see if there is clear line of sight (LOS) available in both north and south directions.

Deployment Recommendations

These are design recommendations for mesh links:

- MAP deployment cannot exceed 35 feet in height above the street.
- MAPs are deployed with antennas pointed in both north and south directions with a little downtilt towards ground for a better link budget and LOS.
- Typical 5 GHz RAP-to-MAP distances are 1000 to 4000 feet.

- RAP locations are typically towers, tall buildings, or cable strands.
- Typical 5 GHz MAP-to-MAP distances are 500 to 1000 feet.
- MAP locations are typically short building tops or streetlights. MAPs should not be deployed on cable strands as there is no cable modem required in MAPs.
- Typical 2.4/ 5 GHz MAP-to-client distances are 300 to 500 feet.
- Client locations are typically laptops, CPEs, or professionally mounted antennas on top of the moving vehicle.

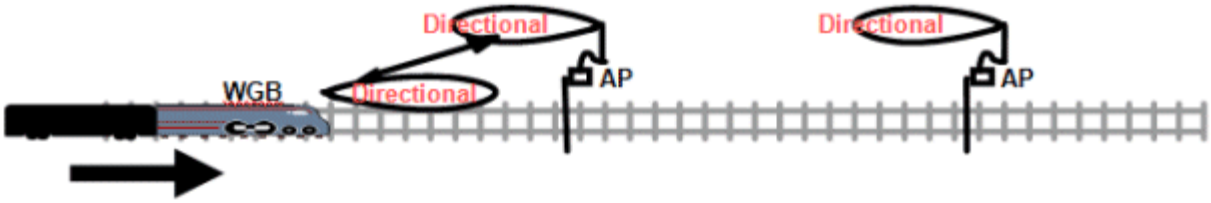
Be creative in selecting the antennas. Always consider gain, directivity, and polarization together while choosing an antenna.

Refer to the Cisco Aironet Antenna and Accessories Reference Guide on Cisco antennas and accessories.

It is advisable to go with directional antennas rather than omni-directional antennas as the coverage is focused along the tracks or linear paths. With proper positioning of directional antennas, you can focus most of the available RF energy on tracks. Along with using most of the RF energy, directional antennas also increase the range.

Antennas with a horizontal and vertical beam width of 30-50° are best suited for most of the deployments.

Beams

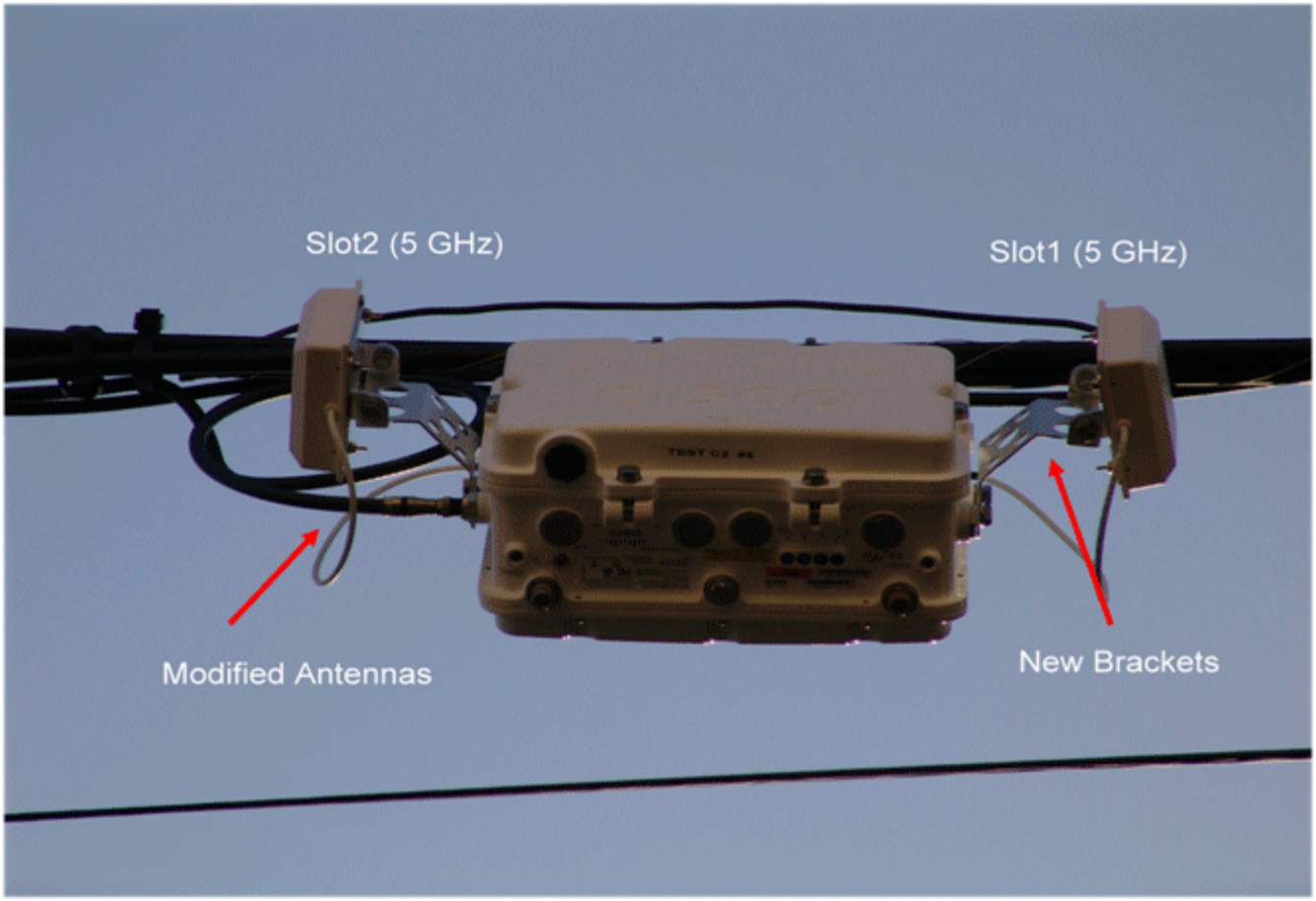


AP1524SB/1523CV has 5 N-connectors to attach 3 2.4 GHz antennas (for Maximum Ratio Combining) and 2 N-connector for 5 GHz antennas. Each radio has at least one TX/RX port. Each radio must have an antenna connected to at least one of its available TX/RX ports.

You can also choose non-Cisco Antennas. When choosing antennas from outside Cisco, keep these things in mind:

- Cisco does not track or maintain information about the quality, performance, or reliability of the non-certified antennas and cables.
- RF connectivity and compliance is the customer's responsibility.
- Compliance is only guaranteed with Cisco antennas or antennas that are of the same design and gain as Cisco antennas.
- The Cisco Technical Assistance Center (TAC) has no training or customer history with regard to non-Cisco antennas and cables.

Make sure that you have proper arrangements to mount these remote antennas next to the APs:



In a typical successful deployment, the customer deployed AP1523CVs on the cable strands running parallel to the rail tracks. Two directional antennas on both the backhaul radios were used, as trains carrying wireless clients was approaching from both sides.

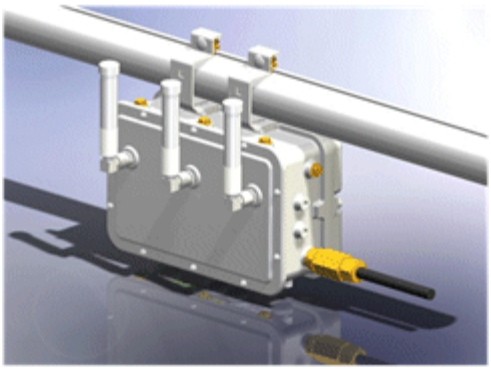
Special mounting brackets have been launched to attach these 14 dBi directional antennas to the AP itself.

If client access is required on 2.4 GHz in the outdoors, then take advantage of Maximum Ratio Combining by using at least 2 antennas on AP1520s for the 2.4 GHz band. There are compact antennas available for 2.4 GHz which are convenient to use.

5GHz radio (802.11a) in an AP1520 Series AP is Single In Single Out (SISO) architecture and 2.4GHz radio (802.11 b/g) is 1x3 Single In Multiple Out (SIMO) architecture.

The 2.4 GHz radio has one transmitter and three receivers. With its 3 receivers enabling maximum-ratio combining (MRC), this radio has better sensitivity and range than a typical SISO 802.11b/g radio for OFDM rates. When operating with data rates higher than 12 Mb/s, you can increase gain on a 2.4-GHz radio to 2.7 dB by adding two antennas and to 4.5 dB, by adding three antennas.

There are short right angle 5 GHz antennas available which can be attached directly to the AP:



This capture shows MAPs deployed on a pole top using 17 dBi sector antennas:

Low loss LMR600 cables run from these antennas to the MAP. Here, directional antennas are pointed in the opposite direction, and they are using alternate adjacent channels as per the design of the serial backhaul network, so the antenna separation is fine. Ideally, you should separate the antennas vertically by 10 feet for an alternate adjacent channel plan. This will also minimize the interference from “Front to Back” lobe radiations.

You may wonder, where is the MAP?

The MAP is installed on the ground. It is connected to the antennas on the pole using low loss cables.

AP Installed at Ground Level

Make sure that there are no other APs from our competitors deployed next to our APs, as this can create a lot of interference.

Closely Deployed Competitor AP

If there are lots of trees with leaves, they can absorb the RF energy, and this can create a big dent in the uplink budget from client to the AP which is already striving for a good RF connection to the mesh infrastructure.

This becomes extremely important to ensure that there are “clear” or “near” LOS conditions, not only between the APs, but also between the train and the AP.

If hanging the AP on the cable strands does not provide clear LOS conditions, special mounting arrangements can be made on the wooden poles as shown here:

Also, regarding “linear deployment,” what will happen if the track on which mobility is being implemented turns? Turning of the track will break the mesh hop connections. There are ways to handle this situation. One way is start a fresh spur of hops by deploying a RAP at the turn. It is very much required to install a parent AP at these locations, as the linear hop link will break if you do not do likewise.

RAP Installed at Turn

From a logistics angle, look for power options for the APs. There are multiple power options which AP1520 platform can accommodate.

Power options include:

- 90 to 480 VAC streetlight power
- 12 V DC
- Cable power
- PoE using a separate power injection system
    - For details on the power injection, its specifications, and installation refer to Cisco Aironet 1520 Series Outdoor Mesh Access Point Power Injector Installation Instructions.
- Internal battery backup power
- 802.3af-compliant PoE out to connect IP devices (such as a video cameras)

An optional battery backup module (part no. AIR-1520-BATT-6AH) is available for AP1520s. The integrated battery can be used for temporary backup power during external power interruptions. The battery run time for AP1520s is:

- 3-hour APoperation using 2 radios at 77°F (25°C) with PoE output port Off.
- 2-hour AP operation using two radios at 77°F (25°C) with PoE output port On.

Note: The battery pack is not supported on the AP cable configuration.

- To quickly check, if the APs are carrying the battery, and whether the batteries are charged or not, use this command that also shows the status of the four uplinks, heater, and the temperature of each AP. This command can also be run on a per AP basis:

```
(Cisco Controller) >show mesh env summary

AP Name             Temperature(C/F)  Heater  Ethernet  Battery
------------------  ----------------  ------  --------  -------
HPRAP1               38/100           OFF     UpDnNANA  N/A
HPRAP1               33/91            OFF     DnDnNANA  N/A
HJRAP1               39/102           OFF     UpDnNANA  94 %
HJMAP3               33/91            OFF     DnDnNANA  95 %
HJMAP2               35/95            OFF     DnDnNANA  99 %
HJMAP1               35/95            OFF     DnDnNANA  94 %
AP1510Map            33/91            OFF     DOWN      N/A
```

Signal to Noise Ratios

When doing cell planning and deciding the distances between the APs, it is important to decide things like typical spacing between the APs, hop count, minimum SNR between the APs (nodes) etc.

Cisco recommends that maximum distance between the two adjacent nodes should not exceed 2000 feet. Typical distance is 1000 feet. Max hops in one direction from a RAP should be kept to four hops for better control of things.

This table shows the minimum link SNR for each backhaul data rate:

Table 2: Backhaul Data Rates and Minimum LinkSNR Requirements

Data Rate	Minimum Required Link SNR

54 Mbps	31 dB
48 Mbps	29 dB
36 Mbps	26 dB
24 Mbps	22 dB
18 Mbps	18 dB
12Mbps	16 dB
9 Mbps	15 dB
6 Mbps	14 dB

The required minimum LinkSNR value is driven by the data rate and this formula:

Minimum SNR + fade margin

- Minimum SNR refers to an ideal state of non-interference, non-noise, and a system packet error rate (PER) of no more than 10%.
- Typical fade margin is approximately 9 to 10 dB.
- We do not recommend using data rates greater than 24 Mb/s in municipal mesh deployments as the SNR requirements do not make the distances practical. It is best to use Dynamic Rate Assignment feature for the backhaul rate to adjust as the available SNR requirements.

For a proper linear alignment and focusing radio frequency in one direction, it is important to attach a directional antenna to the Slot 2 radios at the minimum. You should align and fine tune each link to minimize the hidden node effect. Child nodes should only see and select the immediate parent, rather than jumping over to the next hop and selecting the respective AP as a parent. This can be achieved by first aligning the antennas and then optimizing each link by tuning the RF power.

There are some useful commands which should be used to check the health of the links between the nodes.

show mesh and **config mesh** are powerful commands used to verify interconnectivity in your network:

```
(Cisco Controller 1) >show mesh ?

env             Show mesh environment.
backhaul        Show mesh AP backhaul info.
neigh           Show AP neigh list.
```

```
path            Show AP path.
astools         show mesh astools list
stats           Show AP stats.
secbh-stats     Show Mesh AP secondary backhaul stats.
per-stats       Show AP Neighbor Packet Error Rate stats.
queue-stats     Show AP local queue stats.
security-stats Show AP security stats.
ap              Show mesh ap summary
config          Show mesh configurations.
secondary-backhaul Show mesh secondary-backhaul
ids-state       Show mesh ids-state
client-access   Show mesh backhaul with client access.
public-safety   Show mesh public safety.
cac             Show mesh cac.
```

```
(Cisco Controller 1) >config mesh ?
linktest       Run linktest on the backhaul between two neighboring APs.
linkdata       Retrieves sampled link test data from a AP.
range          range from RAP to MAP Cisco Bridge (150..132000)
astools        Configures mesh anti-stranding.
public-safety Enable/Disable 4.9GHz Public Safety Bands for Mesh AP.
battery-state Disables the Battery-State for an AP
client-access Enable/Disable backhaul with client access CiscoAP.
multicast      Configure Mesh Multicast Mode.
security       Set Bridge Security Mode.
radius-server Configure Mesh Radius Server
full-sector-dfs Configure Mesh full sector DFS status.
ids-state      Configures enabling/disabling of IDS)Rogue/Signature Detection)
                    Reporting for Outdoor Mesh APs
alarm          Configure mesh alarm parameters.
backhaul       Config Mesh Backhaul.
ethernet-bridging Mesh
```

The **show mesh path** command will show the MAC Addresses, radio roles of the nodes, channel, and Link SNR in dB for a particular path:

```
(Cisco Controller) >show mesh path HPRAP1

AP Name/Radio       Channel Rate Link-Snr Flags    State
-----------------  ------- ---- -------- -------  -----

HPRAP1             is a Root HP.
(Cisco Controller) >show mesh path HPMAP1

AP Name/Radio       Channel Rate Link-Snr Flags    State
-----------------  ------- ---- -------- -------  -----

HPRAP1              165     auto 37       0x10e8fcb8 UPDATED NEIGH PARENT BEACON

HPRAP1             is a Root AP.
```

The channel shown in the above command corresponds to Slot 2 radio channel in case of serial backhaul deployment using AP24SB/1523CV.

The **show mesh neigh** command shows the MAC addresses, parent-child relationships, Link SNRs in dB:

```
(Cisco Controller) >show mesh neigh ?

detail          Show Link rate neigh detail.
summary         Show Link rate neigh summary.
(Cisco Controller) >show mesh neigh summary HJRAP1

AP Name/Radio       Channel Rate Link-Snr Flags    State
-----------------  ------- ---- -------- -------  -----

00:0B:85:5C:B9:20  0       auto 4        0x10e8fcb8 BEACON
00:0B:85:5F:FF:60  0       auto 3        0x10e8fcb8 BEACON
00:0B:85:62:1E:00  165     auto 2        0x10e8fcb8 BEACON
00:19:30:76:32:72  0       auto 4        0x10e8fcb8 BEACON
00:1B:0C:DE:13:34  0       auto 4        0x10e8fcb8 BEACON
HJMAP2              161     54   45       0x36     CHILD BEACON
HJMAP1              161     54   65       0x36     CHILD BEACON
HJMAP3              161     54   44       0x36     CHILD BEACON


(Cisco Controller) >show mesh neigh summary HJMAP1
```

```
AP Name/Radio      Channel Rate Link-Snr Flags    State
-----------------  ------- ---- -------- -------  -----

00:0B:85:5C:B9:20  0       auto 4        0x10e8fcb8 BEACON
00:0B:85:5F:FF:60  0       auto 4        0x10e8fcb8 BEACON
00:0B:85:62:1E:00  165     auto 17       0x10e8fcb8 NEEDUPDATE BEACON DEFAULT
00:19:30:76:32:72  0       auto 19       0x10e8fcb8 BEACON
00:1B:0C:DE:13:34  0       auto 5        0x10e8fcb8 BEACON
00:1B:54:D1:FA:CE  0       auto 0        0x10e8fcb8 BEACON
HJMAP2             161     auto 37       0x10e8fcb8 UPDATED NEIGH BEACON
HJMAP3             161     auto 38       0x10e8fcb8 NEIGH BEACON
HJMAP1             161     36   59       0x24     UPDATED NEIGH PARENT BEACON
```

The **show mesh ap tree** command displays hop count, Link SNR, and BGN:

```
(Cisco Controller) >show mesh ap tree

 ======================================================
||  AP Name [Hop Counter, Link SNR, Bridge Group Name] ||
 ======================================================

[Sector 1]
----------
RAP[0, 0, shobhit]
  |-MAP1[1, 26, shobhit]
    |-MAP2[2, 14, shobhit]

------------------------------------------------------
Number of Mesh APs.............................. 3
Number of RAPs.................................. 1
Number of MAPs.................................. 2
------------------------------------------------------
```

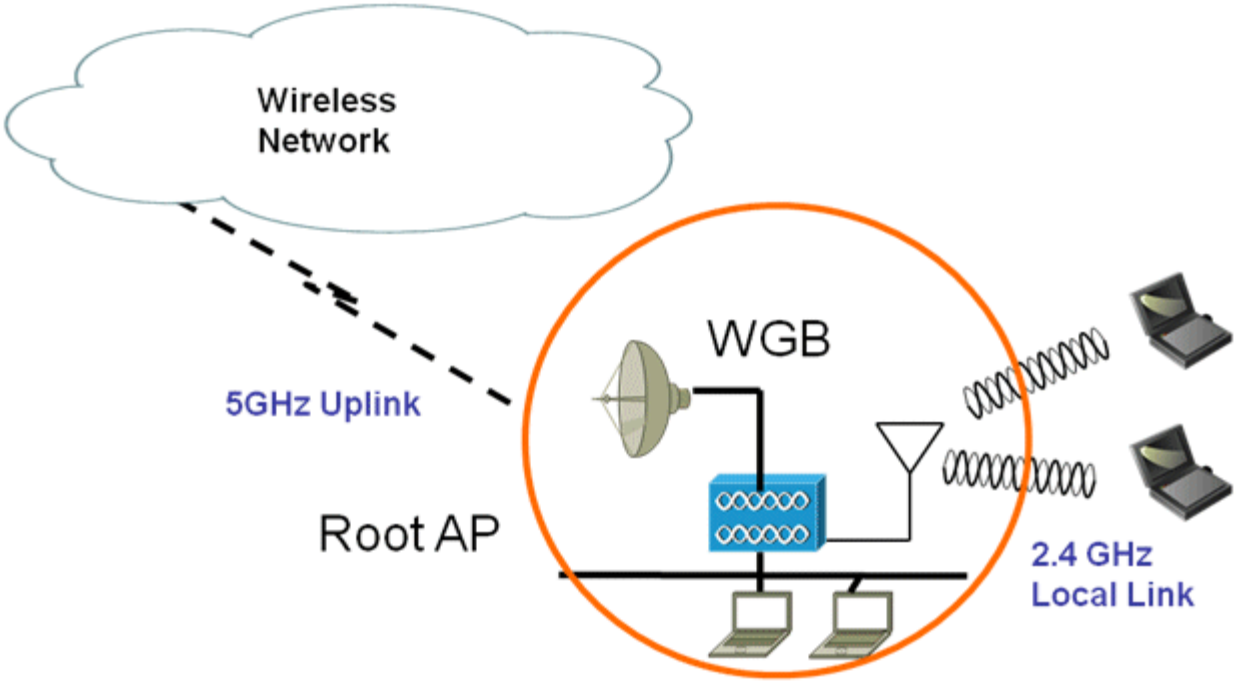
Roaming Client Infrastructure Using WGB Mode

A WGB is a small stand-alone unit that can provide a wireless infrastructure connection for Ethernet-enabled devices. Devices that do not have a wireless client adapter in order to connect to the wireless network can be connected to the WGB through the Ethernet port.

A WGB is a device which associates to an AP and provides transparent bridging to its wired clients. Each wired client that the WGB learns on its Fast Ethernet interface gets reported to the WGB's root by the use of Inter-Access Point (IAPP) messaging. IAPP is Cisco proprietary; it works only with Cisco APs.

WGB also provides a strong uplink towards the AP infrastructure using its high power and antenna gain. Conventional client embedded in the laptop cannot provide this type of strong uplink as it has limited power and almost 0 dBi antenna gain.

Roaming in WGB Mode



For roaming infrastructure, you can either use Cisco wireless autonomous APs in the WGB mode or the WMIC card on MAR3200 can be configured as WGB for the Wifi connection to the infrastructure APs installed along the railway tracks, road, or tunnel.

It is configured with **station role workgroup-bridge**.

There is another similar wireless mode called Universal WGB (uWGB). This configuration allows the WGB to associate to the Wifi infrastructure network as a client, it is called “universal” because it is viewed from the AP as a normal client with a single MAC address (the MAC address from the MARC). Universal WGB was made to have the WGB/WMIC compatible with non-Cisco APs. It is not tied to IAPP or CCX.

It is configured with **station role workgroup-bridge universal mac-address**, the mac-address being the one seen from the Infra AP.

uWGB is not as flexible as WGB in the sense that only a single client/interface can be supported behind it. There are few advantages of uWGB, like it is can be little faster as no IAPP, it is non-CCX, and can talk to any AP (including non Cisco) infrastructure. However, WGB can support multiple MAC/clients behind it without having to NAT or route.

Note: Outdoor MAPs support uWGB mode interoperability. Also, uWGB is only supported on MAR3200 802.11bg WMIC 3201. It is not supported on WMICs 3202 (4.9 GHz) and 3205 (5 GHz).

There are two modes in WGB autonomous APs: Infrastructure mode and client BSS mode. Infrastructure mode supports multiple VLANs behind WGB, and client BSS mode only supports single a VLAN behind WGB.

With 6.0 code in the current unified architecture, Cisco supports WGB association to a LWAPP/CAPWAP AP only in the client (or BSS) mode. There is no infrastructure mode support as in the case of autonomous solution. As a result, WGB is treated as a normal wireless client by the controller. In other words, Cisco does not support multiple VLANs behind the WGB.

With 7.0 code, multiple VLANs behind WGB are supported for wired clients only. This provides segregation of traffic based on VLANs for different applications running on different devices connected to a switch behind a WGB in the mesh network. If a customer has a mesh network typically consisting of 1524 APs with dual backhaul, traffic from WGB clients will be sent in the right priority queue in the mesh backhaul based on DSCP/dot1p values.

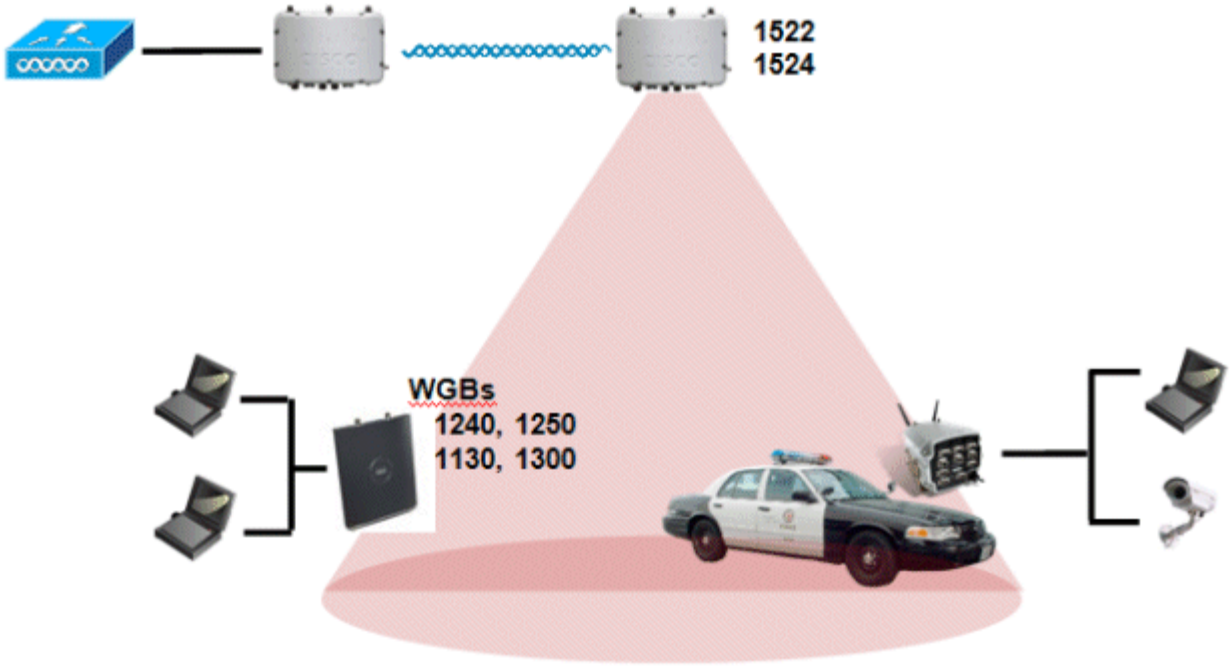
Note: You need a special autonomous image on the autonomous APs being used as WGB or MAR for interoperability with Unified CAPWAP infrastructure.

We recommend choosing any of these APs to be used as WGBs: AP1240, AP1250, AP1130, AP1310, or MAR3200.

APs with external antennas, like the AP1240, should be given preference as they give a comparatively better link budget.

WGB is fully interoperable with outdoor and indoor mesh infrastructure.

WGB Interoperability



	WGB								
RAP/MAP (BH 5GHz)									
	MAR3200			1240/1250		1130		1310	
	4.9GHz (5/10/20MHz)	5Ghz	2.4GHz	5Ghz	2.4GHz	5Ghz	2.4GHz	5Ghz	2.4GHz
1524SB/1524SB	x	✔	✔	✔	✔	✔	✔	x	✔
1524PS/1524PS	✔	x	✔	x	✔	x	✔	x	✔
1522/1522	✔	✔	✔	✔	✔	✔	✔	x	✔
1524SB/1522	x	✔	✔	✔	✔	✔	✔	x	✔
1524PS/1522	x	✔	✔	✔	✔	✔	✔	x	✔
1522/1524SB	x	✔	✔	✔	✔	✔	✔	x	✔
1522/1524PS	✔	x	✔	x	✔	x	✔	x	✔
1240/1130	x	✔	✔	✔	✔	✔	✔	x	✔

- BH—Backhaul

- RAP/MAP—Shows specific APs being used as a RAP/MAP combinations.

Note: Universal client access feature is not available on an AP1524PS (Public Safety) model.

Note: Although we are saying here that you can use the AP1250 AP as a WGB, it should be clear that you cannot get 802.11N advantages out of it, like using multiple streams, higher data rates and channel bonding, etc. This is a limitation because these features are not available on the mesh infrastructure side yet, although MAPs use SISO and SIMO techniques. 5GHz radio (802.11a) in AP1520 series AP is SISO architecture and 2.4GHz radio (802.11 b/g) is 1x3 SIMO architecture.

A 2.4 GHz radio has 1 transmitter and 3 receivers. With its 3 receivers enabling maximum-ratio combining (MRC), this radio has better sensitivity and range than a typical SISO 802.11b/g radio for OFDM rates.

For example, you do not configure the channel on the WGB, as it is a client. You configure the channel on the AP. As a result, if the AP is configured with a 40MHz wide channel, then the WGB should be capable of using the upper MCS rates. However, configuring wider channels than 20 MHz is not possible on the mesh side yet. In addition, Cisco has only 1 transmitter scheme (1x3), so legacy 802.11a/b/g only is possible.

Moreover, Cisco does not see any advantages of using an AP1252 vs. a 1242 as a WGB in an 11g/11a network due to these reasons:

- It costs more.
- It is much bigger and heavier.
- It uses more power.
- It does not support "distance" value (not relevant to mesh, would be relevant for a WGB client of an IOS bridge).

The advantages of the 1252 (faster CPU, more DRAM and flash, gig vs 100baseT) - none of them would provide any practical benefit in an 11g/a application.

Roaming Scalability

Cisco unified architecture provides a lot of scalability. As described earlier, WLCs can accommodate large number of APs. You can easily add controllers for redundancy. Up to 72 controllers can be part of an N+1 cluster. A mobility domain (consisting of a number of mobility groups) is a coverage area consisting of number of APs grouped together in which a client can have seemless roam without losing its session. The roaming scalability determination should start with an idea of how many APs can be in a single mobility domain.

If you consider an example of WiSM, a single WiSM controller can manage up to 300 APs. It is possible to have three mobility groups. Each mobility group can have up to 24 controllers. Therefore, it is possible to have 7200 APs in a single mobility group. This way, the solution can scale more than 100 miles. As a client can also freely fast roam within mobility groups and design can be scaled up to 72 controllers with client roaming seamlessly (not fast roaming as PMK is not cashed between mobility groups). So, you can have up to 21600 APs proving seamless roaming for many miles.

Similarly, if you consider WLC 5508, it can manage up to 500 APs. So, for 72 controllers for a client to roam seamlessly using 3 mobility groups, you can have 36000 APs, again provding seamless roaming for miles.

On the management side, 1 WCS can manage up to 3000 APs, or up to 750 Controllers at the high end. At the low end, 500 APs and 50 controllers. WCS navigator can manage 20 WCS and 20,000 APs.

Wireless Client Support in WGB

APs with two radios as WGB certainly provides a better advantage, as one of the radios can be used for client access and the second radio can be used for accessing the APs. Having 2 independent radios doing 2 independent functions provides better control and lowers the latency. Also, wireless clients on the second radio for WGB do not get disassociated by the WGB upon losing its uplink or in a roaming scenario. In simpler terms, one radio has to be configured as Root (radio role) and the second radio has to be configured as WGB (radio role).

Note: If one radio is configured as WGB, then the second radio cannot be a WGB or a Repeater.

These features are not supported for use with a WGB:

- Hybrid REAP
- Idle timeout
- Web authentication: If a WGB associates to a web-authentication WLAN, the WGB is added to the exclusion list, and all of the WGB wired clients are deleted. (Web-authentication WLAN is another name for Guest WLAN.)
- For wired clients behind WGB, MAC filtering, link tests, and idle timeout.

Points to Remember before Configuring

- Cisco recommends using 5 GHz radio for uplink to MAP infrastructure. By doing this, you can take advantage of strong client access on two 5 GHz radios available on MAPs. Also, the 5 GHz band mostly allows more Effective Isotropic Radiated Power (EIRP), and is less polluted. In a two radio WGB, configure 5 GHz radio (radio 1) mode as WGB. This radio will be used to access mesh infrastructure. Configure the second radio 2.4 GHz (radio 0) mode as Root for client access.
- On the autonomous APs, only one SSID can be assigned to the native VLAN. Multiple VLANs in one SSID are not possible on the autonomous side. In other words, SSID-to-VLAN mapping should be unique, as this is the way we segregate the traffic on different VLANs. On the other hand, in a unified architecture, multiple VLANs can be assigned to one WLAN (SSID).
- Only one WLAN (SSID) for wireless association of WGB to the AP infrastructure is supported. This SSID should be configured as infrastructure SSID and should be mapped to the native VLAN. WGB will drop everything which is not in native VLAN towards the mesh infrastructure.
- Dynamic interface should be created in the controller for each VLAN configured in the WGB.
- The second radio (2.4 GHz) on the AP should be configured for client access. You have to use the same SSID on both radios and map to native VLAN. If you create a separate SSID, then you will not be able to map it to native VLAN, due to unique VLAN/SSID mapping requirements. And, if you try to map the SSID to another VLAN, then you do not have multiple VLAN support for wireless clients as per today.
- All L2 security types are supported for the WLANs (SSIDs) for wireless client association in WGB.
- This feature has no dependability on AP platform. On the controller side, both mesh and non-mesh APs are supported.
- There is a limitation of 20 clients in WGB, if WGB is talking to AP infrastructure based on unified architecture. Those 20 clients include both wired and wireless clients. If WGB is talking to autonomous APs, then the client limit is very high.

- The controller treats the wireless and wired clients behind WGB as the same, so features like macfiltering and link test are not supported for wireless WGB clients from the controller.
- If required, a user can run a link test for WGB wireless client from an autonomous AP.
- Multiple VLANs for wireless clients associated to WGB is not supported.
- Multiple VLANs upto 16 are supported for wired clients behind WGB from release 7.0 and later.
- Roaming is supported for wireless and wired clients behind WGB. The wireless clients on the other radio will not be dissociated by the WGB upon losing its uplink or in a roaming scenario.

Cisco recommends you configure Radio 0 (2.4 GHz) as a Root (one of the mode of operations for Autonomous AP) and Radio 1 (5 GHz) as WGB.

Configuration Example

These are mandatory when you configure from CLI:

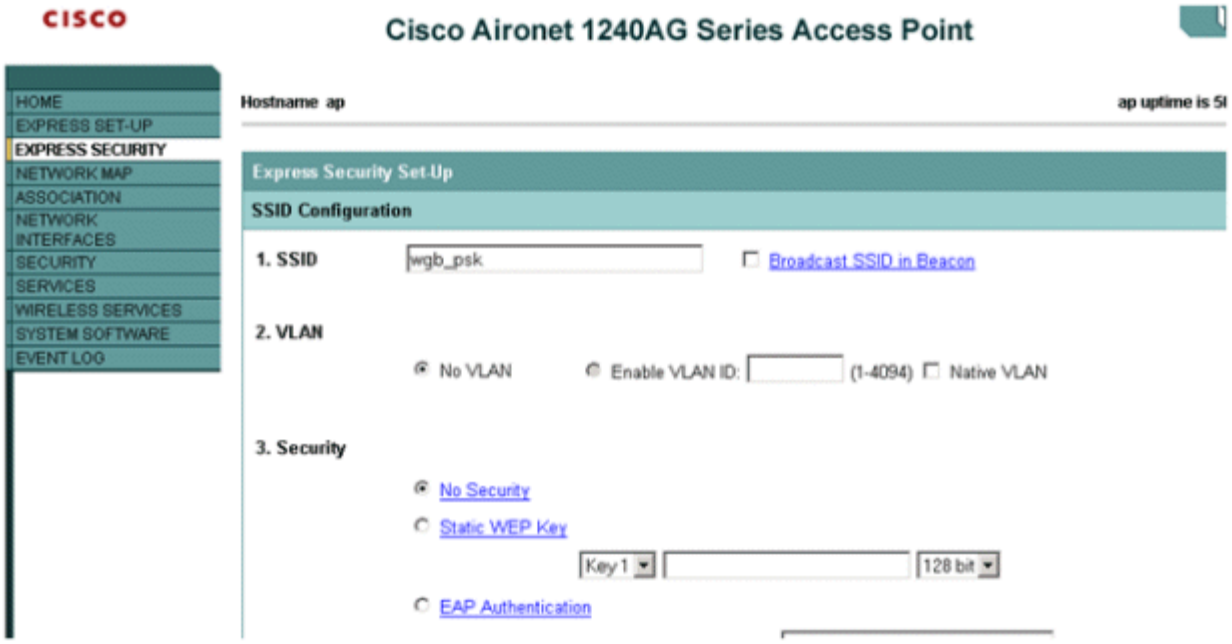
1. dot11 SSID (security for WLAN can be decided based on the requirement).
2. Map the sub interfaces in both the radios to a single bridge group.

   Note: Native VLAN is always mapped to Bridge Group 1 by default. For other VLANs Bridge Group number matches VLAN number, like for VLAN 46, Bridge Group is 46.
3. Map the SSID to the radio interfaces and define the role of the radio interfaces.

In this example, one SSID (WGBTEST) is being used on both the radios and the SSID is infrastructure SSID mapped to NATIVE VLAN 51. All radio interfaces are mapped to bridge group -1.

```
WGB1#config t
WGB1(config)#interface Dot11Radio1.51
WGB1(config-subif)#encapsulation dot1q 51 native
WGB1(config-subif)#bridge-group 1
WGB1(config-subif)#exit
WGB1(config)#interface Dot11Radio0.51
WGB1(config-subif)#encapsulation dot1q 51 native
WGB1(config-subif)#bridge-group 1
WGB1(config-subif)#exit
WGB1(config)#dot11 ssid WGBTEST
WGB1(config-ssid)#vlan 51
WGB1(config-ssid)#authentication open
WGB1(config-ssid)#infrastructiure-ssid
WGB1(config-ssid)#exit
WGB1(config)#interface Dot11Radio1
WGB1(config-if)#ssid WGBTEST
WGB1(config-if)#station-role workgroup-bridge
WGB1(config-if)#exit
WGB1(config)#interface Dot11Radio0
WGB1(config-if)#ssid WGBTEST
WGB1(config-if)#station-role root
WGB1(config-if)#exit
```

You can also use the GUI of an autonomous AP to configure these things. From the GUI, subinterfaces are automatically created once the VLAN is defined.

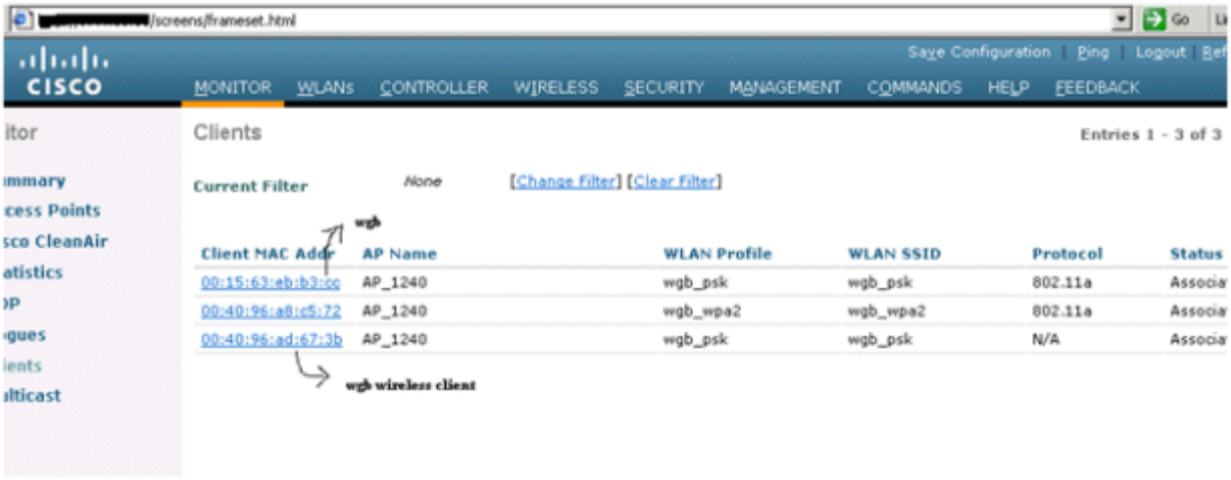


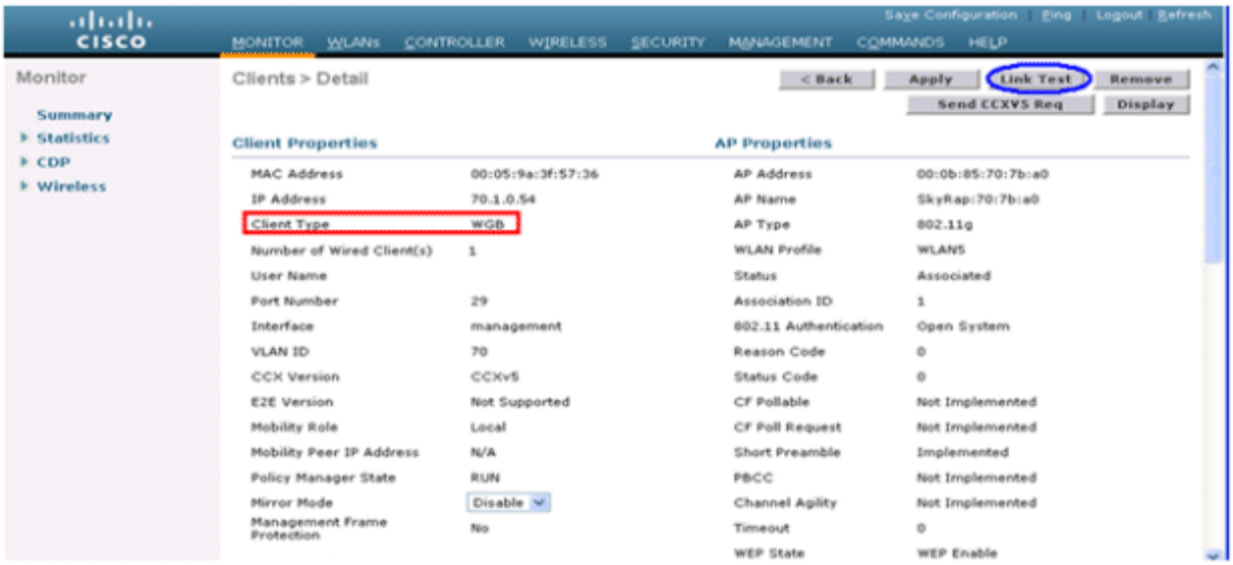
WGB Association Check

Both WGB association to controller and wireless client association to the WGB can be verified using the **show dot11 associations client** command in autonomous AP:

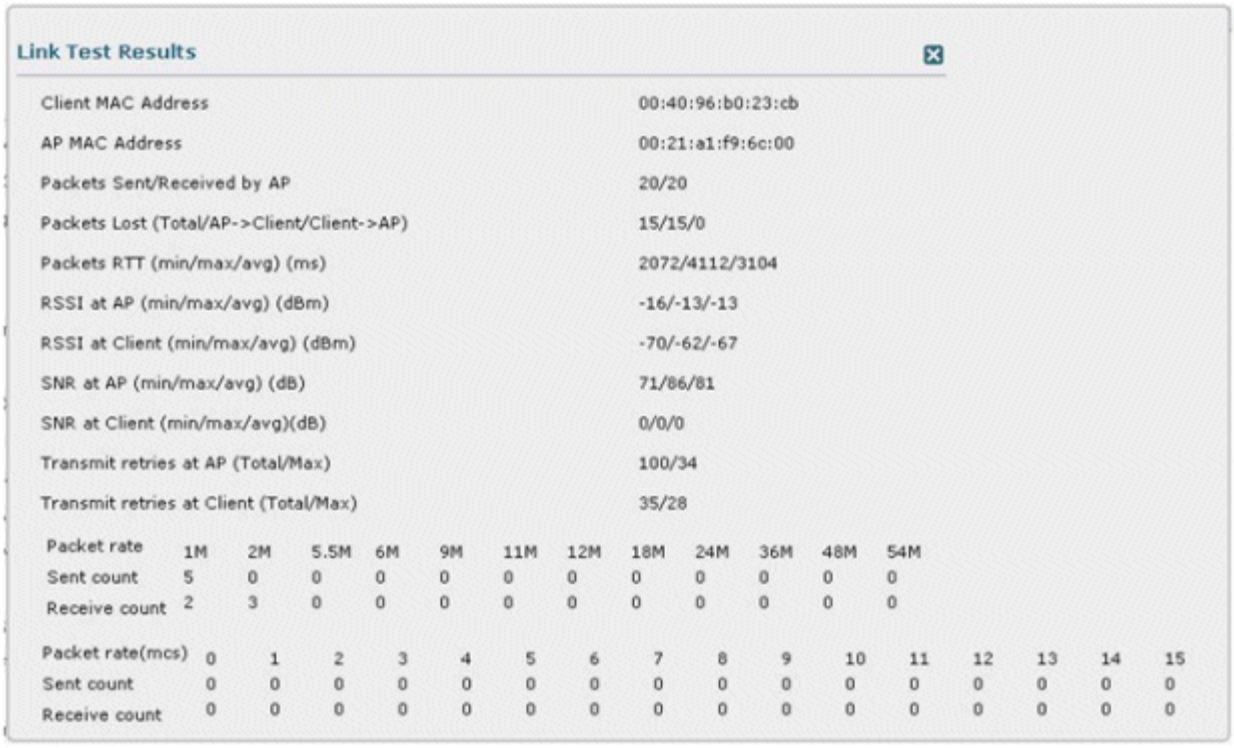
```
WGB#show dot11 associatoions client

802.11 Client Stations on Dot11Radio1:

SSID [WGBTEST] :

MAC Address    IP address      Device          Name   Parent          State
0024.130f.920e 10.51.1.10      LWAPP-Parent RAPSB   -               Assoc
```

From the controller, choose **Monitor** > **Clients**. The WGB and the wireless/wired client behind the WGB will be updated and the wireless/wired client is shown as the WGB client:





Link Test Result



A link test can also be run from the controller CLI using this command:

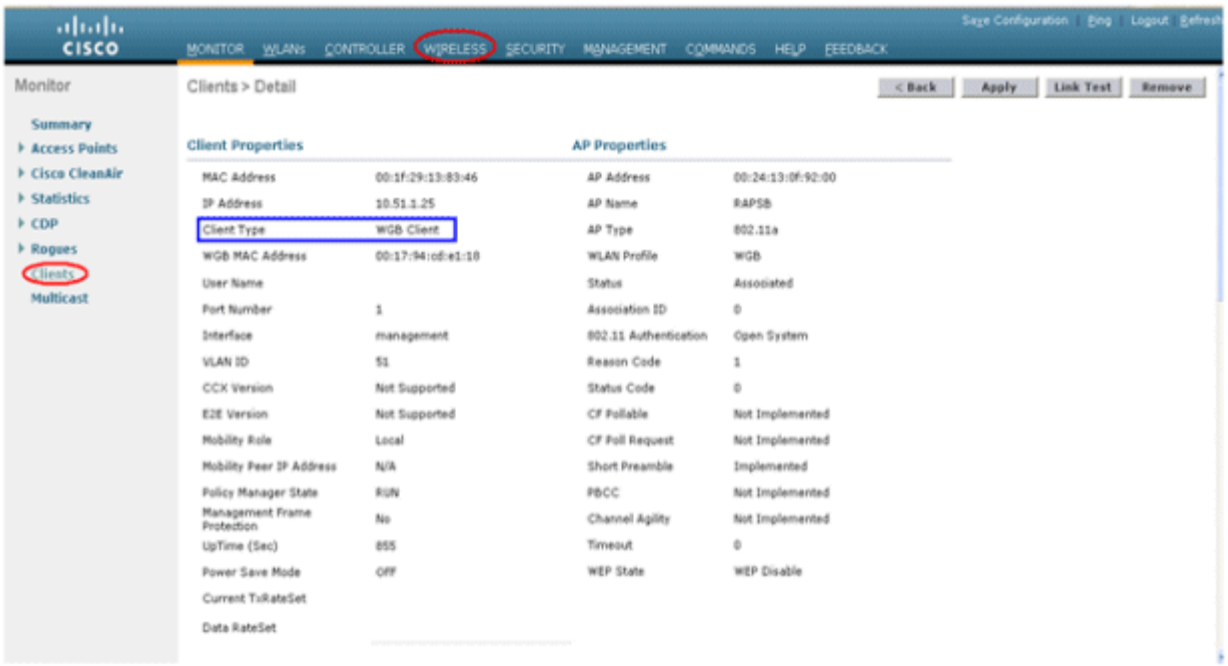
(Cisco Controller) > linktest *<client mac address>*

The link test from the controller is only limited to WGB, and it cannot be run beyond WGB from the controller to

wired or wireless client connected to WGB. You can run the link test for the wireless client connected to the WGB from the WGB itself using this command:

```
ap#dot11 dot11Radio 0 linktest target <client mac>
Start linktest to 0040.96b8.d462, 100 512 byte packets
ap#
POOR (4  % lost)      Time    Strength(dBm)    SNR  Quality        Retries
                       msec       In          Out     In          Out          In    Out
      Sent : 100,Avg   22         - 37        - 83    48           3    Tot:   34     35
Lost to Tgt:   4, Max 112         - 34        - 78    61          10    Max:   10      5
Lost to Src:   4, Min   0         - 40        - 87    15           3

Rates (Src/Tgt)      24Mb 0/5  36Mb 25/0  48Mb 73/0  54Mb 2/91
Linktest Done in 24.464 msec
```

WGB Wired/Wireless Client



TheseCLI commands are also convenient to use:

```
(Cisco Controller) >show wgb summary

Number of WGBs..................................... 2
MAC Address        IP Address     AP Name  Status  WLAN  Auth  Protocol  Clients
-----------------  -------------- ---------------- ---------- ----  ----  ---
00:1d:70:97:bd:e8  9.47.184.54    c1240    Assoc   2     Yes   802.11a    2
00:1e:be:27:5f:e2  9.47.184.55    c1240    Assoc   2     Yes   802.11a    5

(Cisco Controller) >show client summary
Number of Clients.............................. 7
MAC Address       AP Name  Status      WLAN/Guest-Lan Auth Protocol Port Wired
00:00:24:ca:a9:b4  R14     Associated      1          Yes   N/A      29   No
00:24:c4:a0:61:3a  R14     Associated      1          Yes  802.11a   29   No
00:24:c4:a0:61:f4  R14     Associated      1          Yes  802.11a   29   No
00:24:c4:a0:61:f8  R14     Associated      1          Yes  802.11a   29   No
00:24:c4:a0:62:0a  R14     Associated      1          Yes  802.11a   29   No
00:24:c4:a0:62:42  R14     Associated      1          Yes  802.11a   29   No
00:24:c4:a0:71:d2  R14     Associated      1          Yes  802.11a   29   No

(Cisco Controller) >show wgb detail 00:1e:be:27:5f:e2
Number of wired client(s): 5
MAC Address        IP Address      AP Name         Mobility    WLAN  Auth
-----------------  -------------- ----------------  ---------- ---- ----
00:16:c7:5d:b4:8f  Unknown         c1240            Local      2     No
00:21:91:f8:e9:ae  9.47.184.83     c1240            Local      2     Yes
00:21:55:04:07:b5  9.47.184.66     c1240            Local      2     Yes
00:1e:58:31:c7:4a  9.47.185.75     c1240            Local      2     Yes
00:23:04:9a:0b:12  Unknown         c1240            Local      2     No
```

WGB Roaming

Roaming time is the time taken by the WGB radio role to disassociate from one AP and reassociate to another AP. During this interval, there is no data transfer, and, therefore, the roaming time is significant to maintain the sessions.

Please note that the WGB role can be set either on any autonomous AP or on any of the wireless mic cards (WMIC) of the MAR (MAR3200).

Roaming involves two main processes:

- Scanning
- Reassociation

Scanning

WGB supports two main modes of roaming operation:

- Default “static” mode - Roaming is based on two main variables: packet retransmissions, or loss of eight consecutive beacons.
- Mobile station mode - On top of the previous variables, the AP can do periodic analysis of signal level drops and data rate shifts.

Basically, there are four conditions that trigger the WGB to start scanning for a better AP:

- The loss of eight consecutive beacons.
- A shift in the data rate.
- The maximum data retry count is exceeded (the default value is 64).
- A measured period of time of a drop in the signal strength threshold.

Only the last two items in this list are configurable and are explained here. The remainder are hard coded. When any of the above criteria is met, WGB will trigger a roaming process, scanning approximately 10 to 20ms/channel. You can also limit the channels to be scanned through configuration. Recommended use of channels in deployment is 3 for 802.11b/g in case of high performance application, although for low data throughput scenarios, it is possible to use a reduced set, to minimize scanning time.

Scanning methodology followed is “Active Scanning.” Instead of listening to beacons from APs, WGB will actively send out "probe request:" packets and waits for 20ms to get a response in every channel. The AP will stop scanning after it receives the first response with a satisfying signal. So, the scanning period may last approximately 40ms. This time may be shorter depending on radio hardware type.

Configure Workgroup Bridge for Roaming

There are two main forms to configure WGB roaming parameters:

- Use packet retries.
- Use the **mobile station** command.

Packet retries allow a more conservative approach, where WGB will not start a roaming process, until data loss is

detected or eight consecutive beacons are missed.

The mobile station will start a regular process on WGB to do “preemptive” roaming, which monitors the signal levels and rate speed changes, and force a new roaming before the current AP signal is too low. This scan process will trigger small gaps in radio transmission when the radio is performing the channel scan.

Both commands take this form, under the dot11Radio interface:

```
ap(config-if)#packet retries <data retry count>   {drop}
ap(config-if)#mobile station period X threshold Y (in dBm)
```

If the WGB starts scanning because of a loss of eight consecutive beacons, the message "Too many missed beacons" is displayed on the console. In this case, the WGB is acting as a Universal Bridge Client, much like any other wireless client in its behavior.

In some situations, it is interesting to use the optional "drop" option in the packet retries, to preserve the association, even on the failure to transmit a data packet. This is useful for challenging RF environments, where the roaming can be also triggered by mobile scan command.

The mobile station algorithm evaluates two variables: data rate shift and signal strength and responds as:

- If the driver does a long-term down shift in the transmit rate for packets to the parent, the WGB initiates a scan for a new parent (no more than once every configured period).
- If the driver does a long-term down shift in the transmit rate for packets to the parent, the WGB initiates a scan for a new parent (no more than once every configured period).

The data-rate shift can be displayed using this command:

```
debug dot11 dot11Radio 0 trace print rates
```

However, this will not show the actual data rate shift algorithm in action, but only the changes in data rate. This determines the time period to scan, depending on how much the data rate was decreased.

The **mobile station period** should be set depending on the application. The default is 20 seconds. This delay period prevents the WGB from constantly scanning for a better parent if, for example, the threshold is below the configured value.

Some situations may require a faster timer; for example, on high speed trains. The period should not be lower than the time that is required by the AP to complete the authentication process. For example, for 802.1x + CCKM networks, it should not be set below 2 seconds. PSK networks may use one second. The actual period will always have one second added to the timer, product of the AP scheduler resolution for this task.

The threshold sets the level at which the algorithm is triggered to scan for a better parent. This threshold should be set to noise+20dBm but not more than -70dBm (+70 because input for threshold is positive). The default is -70 dBm. The correct threshold will depend on the intended data rate, versus the coverage level offered in the environment where the WGB will operate. Assuming a proper coverage, we should set this threshold to be a little less than then "breaking point" for the needed data rate for the applications in use.

When you enable these settings, the WGB scans for a new parent association when it encounters a poor Received Signal Strength Indicator (RSSI), excessive radio interference, or a high frame-loss percentage. Using this criteria, a WGB configured as a mobile station searches for a new parent association and roams to a new parent before it loses its current association. When the mobile station setting is disabled (the default setting) the WGB does not search for a new association until it loses its current association.

The threshold values should be set as per the frequency band used, as it is directly related to the interference. For

example, the threshold for 2.4 GHz should be set a little higher (by 5 dB) as compared to 5GHz or 4.9 GHz band as 2.4 GHz band has comparatively more interference. Please note that threshold have negative values.

For example:

- For 2.4 GHz

```
ap(config-if)#mobile station period 3 threshold 70
```

- For 5 GHz

```
ap(config-if)#mobile station period 3 threshold 75
```

Configure a Workgroup Bridge for Limited Channel Scanning

In mobile environments such as railroads, a WGB instead of scanning all the channels will be restricted to scan only a set of limited channels in order to reduce the hand-off delay when the WGB roams from one AP to another. By limiting the number of channels the WGB scans to only those required, the mobile WGB achieves and maintains a continuous WLAN connection with fast and smooth roaming. This limited channel set is configured using this CLI command:

```
ap(config-if)#mobile station scan <set of channels>
```

The CLI command invokes scanning to all or specified channels. There is no limitation on the maximum number of channels that can be configured. The maximum number of channels that can be configured is restricted only by the number of channels a radio can support. When executed, the WGB only scans this limited channel set. This limited channel feature also affects the known channel list that the WGB receives from the AP to which it is currently associated. Channels are added to the known channel list only if they are also a part of the limited channel set.

Here is a configuration example for the aforementioned roaming configurations:

```
ap(config)#interface dot11radio 1
ap(config-if)#ssid outside
ap(config-if)#packet retries 16
ap(config-if)#station role workgroup-bridge
ap(config-if)#mobile station
ap(config-if)#mobile station period 3 threshold 50
ap(config-if)#mobile station scan 5745 5765
```

Use the **no mobile station scan** command to restore scanning to all the channels.

MAPs have leveraged WNBU 802.11 enhancements for fast roaming, such as QBSS IE, Neighboring AP information, Cisco Centralized Key Management (CCKM), etc. MAPs implement the CCXV4 enhancements like AP assisted roam, Enhanced neighbor List, and Roam reason report. Roaming time also depends upon the wireless security (authentication and encryption) settings on the WGB and the WLAN being used.

Being aware of the long scan time that pushes handover latency higher, there are three types of scans implemented for the WGB:

- Normal scan
- Fast scan
- Very fast scan

A **normal scan** begins on the associated channel and continues to cycle through the rest of the channels. For example, if the WGB with 13 channels was associated to an AP on channel 6, WGB will start its scan on channel 6 then 7, 8, 9,

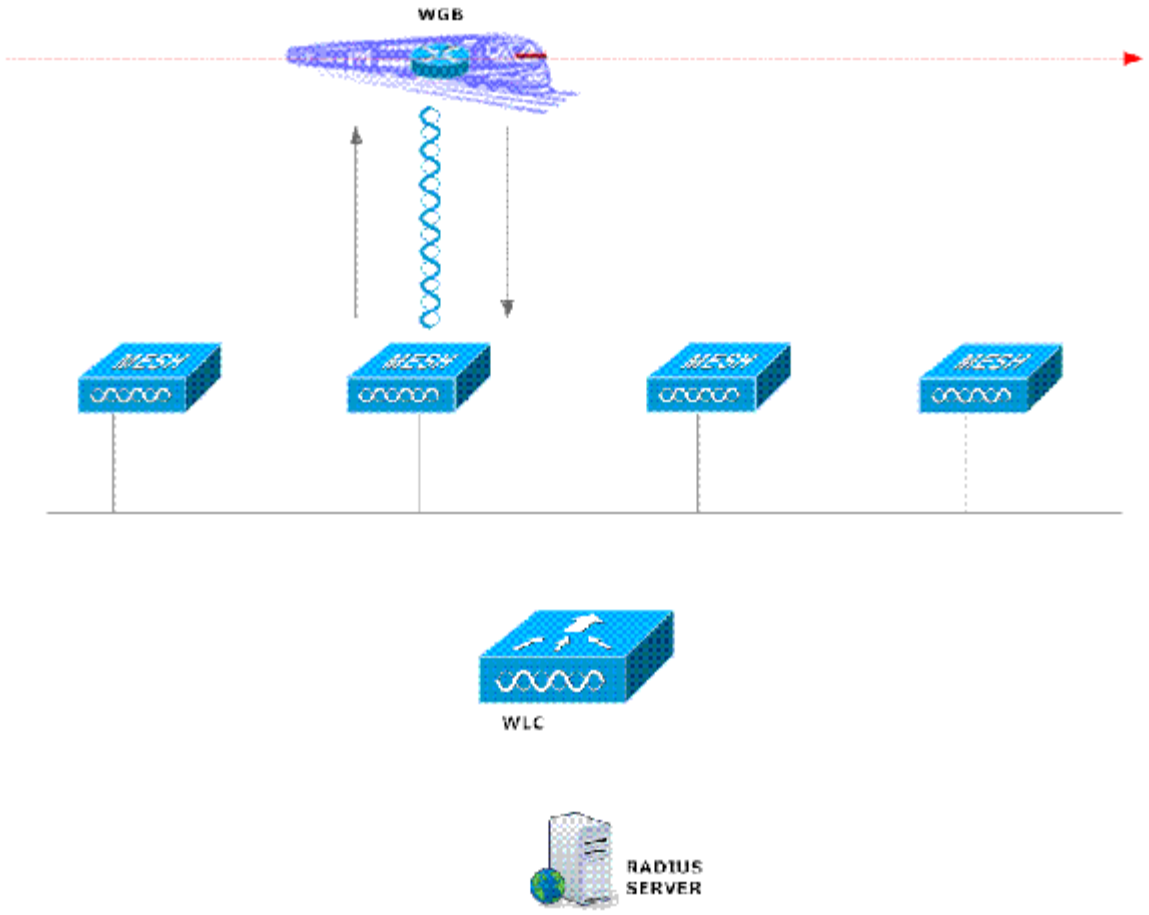
10, 11, 12, 13, 1, 2, 3, 4 and 5. Upon scanning all 11 channels and receiving more than one probe response, the WGB will perform a compare function that compares all responding APs to the one that it was previously associated with in means of signal level, load, and hops. If there was only a single responding AP, the WGB will not perform the compare function and tries to immediately authenticate and associate to the new AP.

The WGB performs a **fast scan** when traffic is between 10 and 20 packets per second. The WGB scans and associates to the first responding AP during a fast scan.

During a **very fast scan**, the WGB does not scan at all and tries to associate to the best AP in the adjacent list that is built up with IAPP and CCX.

After any scanning procedure is completed, the WGB compares the responding APs and tries to authenticate and to associate to the best AP.

The WGB Compares Responding APs



Configure Neighbor List Support

As mentioned previously, the WGB will receive a neighbor list of other potential parent APs which are in the area. In some scenarios, it is interesting to remove this, as the parent list may have“directionality.” For example, in a tunnel, as the train is moving on a given direction, the received list is only partially valid, as some of the neighbors for the current parent AP will not be reachable on the direction that the train is moving (train is moving away from some of them).

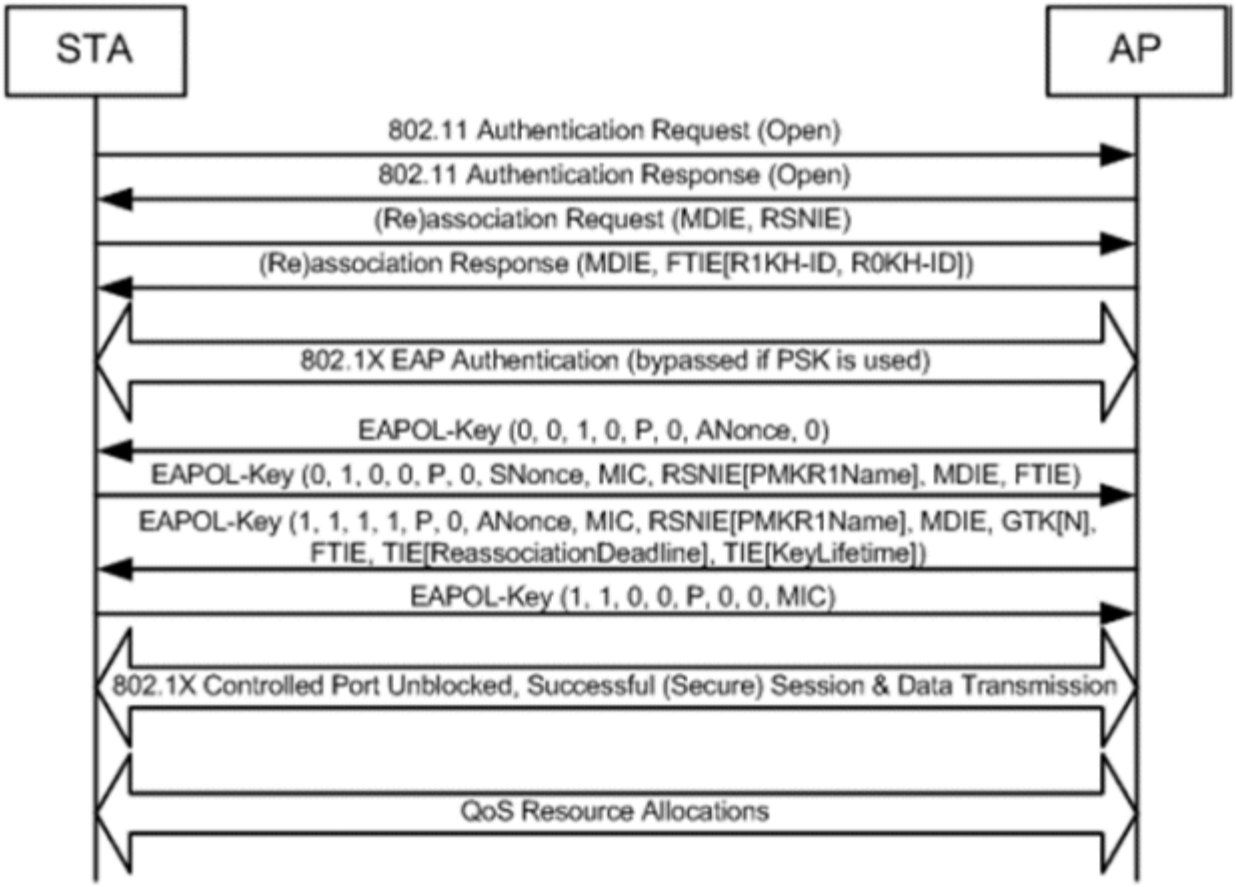
```
ap(config-if)# mobile station ignore neighbor-list
```

Reassociation

Once a neighbor AP is found which satisfies the signal characteristics, WGB will initiate switching over to the next AP. WGB will perform these steps:

1. Stop transmitting pending data.
2. Send authentication request.
3. Receive authentication response.
4. Send reassociation request.
5. Receive reassociation response.
6. Do 802.1x authentication.
7. Do EAPoL exchange.
8. Start transmitting data on new AP.

802.11 Standard Association Process Examples



For all the timers mentioned here, we do not consider retransmissions or timeouts that may vary from system to system due to configuration or implementation (autonomous and unified infrastructure have different timeout values for example). Extensible Authentication Protocol (EAP) retransmissions may range from 100ms to several seconds long, and radius retransmissions are normally in the area of 2 to 5 seconds. We show here a "best case" scenario, with little or no retransmissions happening. In real life, it is possible that some retransmissions are observed, depending on RF quality and/or network utilization.

IAPP update is a set of packet exchange between the WGB and WLC/WDS. This exchange may take around 10 to 200ms. This is only needed on WGB mode. If using Universal WGB mode, this step is not taking place. It allows the WGB to inform of the devices behind it, and starts their traffic flow.

Step 1 consists on AP exhausting its current radio TX queue. It may take few milliseconds depending on how busy is the RF medium, and how many packets are queued on the radio at the moment that the roaming is triggered. As this is not predictable, do not add it to the calculation. This can take a maximum of 4 seconds in the worst scenario.

Steps 2-3 packet exchanges are handled directly by root AP, and can happen in 1-2ms typically.

Steps 4 and 5 are sent to WLC in unified infrastructure, and should be handled in another 2ms plus any propagation delay added by the network between the AP and the WLC. In the case of an autonomous (IOS) infrastructure, they are handled directly by the AP.

Setp 6: 802.1X provides WLANs with strong, mutual authentication between a client and an authentication server. In addition, 802.1X provides dynamic per-user, per-session encryption keys, removing the administrative burden and security issues surrounding static encryption keys. 802.1X is supported by both WPA-Enterprise Mode and WPA2-Enterprise Mode.

With 802.1x the credentials used for authentication, such as logon passwords, are never transmitted in the clear, or without encryption, over the wireless medium. While 802.1X authentication provide strong authentication for wireless LANs via an EAP method. TKIP or AES are also needed for encryption in addition to 802.1X since standard 802.11 WEP encryption is vulnerable to network attacks.

After mutual authentication has been successfully completed, the client and RADIUS server each derive the same encryption key, which is used to encrypt all data exchanged. Using a secure channel on the wired LAN, the RADIUS server sends the key to wireless LAN controller, which stores it for the client. The result is per-user, per-session encryption keys, with the length of a session determined by a policy defined on the RADIUS server. When a session expires or the client roams from one AP to another, a reauthentication occurs and generates a new session key.

Some EAP types are more secure than others – i.e. EAP-LEAP has the username/password as a mschap has but is breakable, EAP-MD5 and EAP-NULL are very insecure.

These are more secure as the username/password are with secure type tunnels:

- EAP-FAST (EAP-Flexible Authentication via Secure Tunneling)
- EAP-TLS (Transport Layer Security)
- PEAP (Protected Extensible Authentication Protocol)
- EAP-TTLS (EAP-Tunneled TLS)

Cisco does not recommend the use of LEAP due to known vulnerabilities with dictionary attacks. EAP-Fast or EAP-TLS are the recommended more secure methods for authentication.

From the list above, only EAP-FAST and EAP-TLS are supported on the WGB. EAP-TLS requires a certificate server.

EAP-TLS is more secure in the fact that with EAP-FAST the user/password can be copied, with EAP-TLS, we use a certificate that will work only on the specific hardware.

EAP-TLS was developed by Microsoft Corporation to enable the use of EAP as an extension of PPP to provide authentication within PPP and TLS to provide integrity-protected cipher suite negotiation and key exchange.

EAP-TLS, which is defined in RFC 2716, uses X.509 public key infrastructure (PKI) certificate-authenticated IEEE

802.1X port-based access control and is specifically targeted to address a number of weaknesses in other EAP protocols such as EAP-MD5. However, in addressing these weaknesses, the complexity of deployment increases due to the fact that not only servers, but also clients require certificates for mutual authentication.

EAP-FAST was developed by Cisco and submitted to the IETF as an Internet draft in February 2004. The Internet draft was revised and submitted in April 2005. The EAP-FAST protocol is a client-server security architecture that encrypts EAP transactions within a TLS tunnel. While similar to PEAP in this respect, it differs significantly in that the EAP-FAST tunnel establishment is based upon strong shared secret keys that are unique to users. These secrets are called Protected Access Credentials (PACs) and may be distributed automatically (automatic or in-band provisioning) or manually (manual or out-of-band provisioning) to client devices. Because handshakes based upon shared secrets are intrinsically faster than handshakes based upon a PKI infrastructure, EAP-FAST is the significantly faster than EAP-TLS that provide encrypted EAP transactions. EAP-FAST can use certificates to authenticate its phase 2 by using EAP-TLS within the inner tunnel.

802.1x authentication may vary from 20ms to several seconds. The reason are the additional frame exchanges between client and end authenticator server plus that any retransmission timers on EAP which can take one or more seconds. This may involve talking to a radius server and/or external user data base, which may add some delay on the process.

802.1x uses an EAP method for authentication, each type may need a different quantity of exchanges to complete. For example, LEAP may finish in just 2 frames, but it is unsecure. EAP-TLS may need 10 or more exchanges depending on certificate size.

Step 7: After 802.1x is completed the device needs to complete EAPoL exchange to finish the key material generation for starting the encryption of the user data. This is 4 frames, and it may take around 20ms to finish

Step 8: After authentication is completed and key material is negotiated, the encryption can start, and WGB now now send data on the new AP.

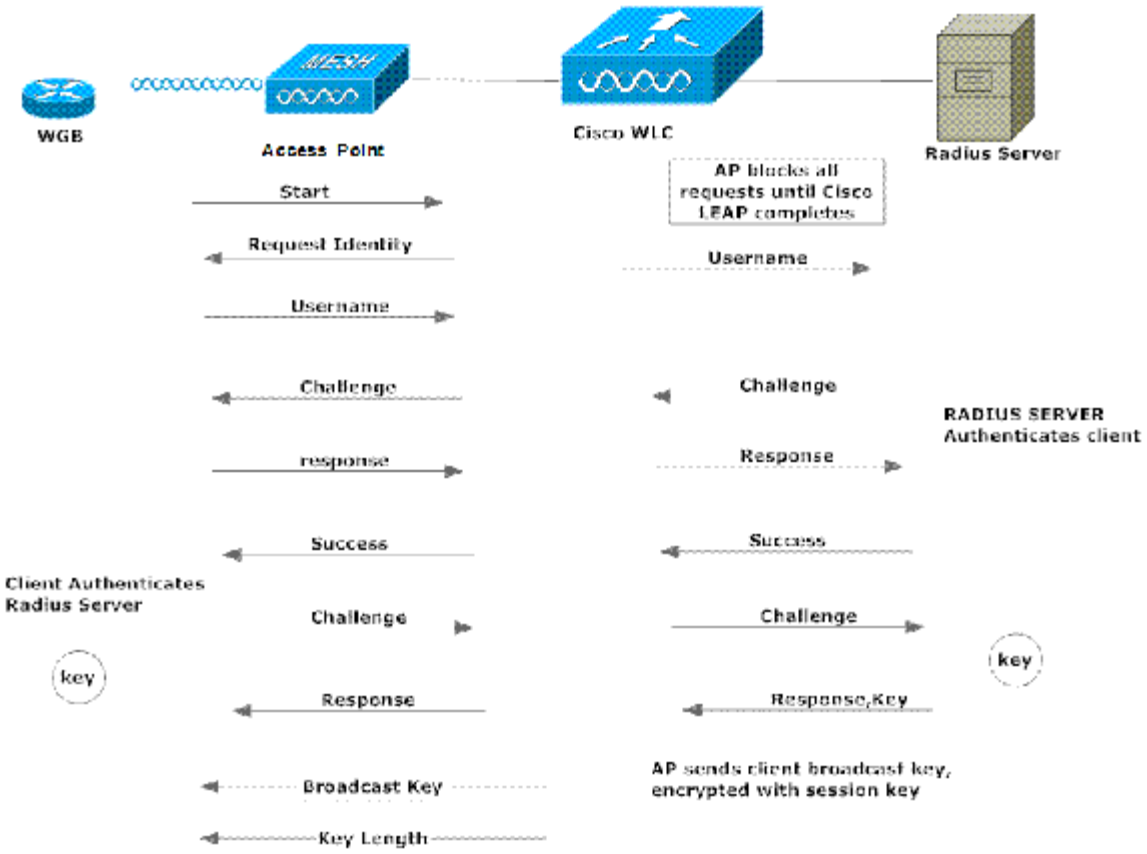
Cisco Centralized Key Management (CCKM)

To minimize 802.1x authentication time, Cisco supports the “fast secure roaming” (CCKM) feature. With the CCKM feature, 802.1x can happen in around 50-100ms.

Every time the WGB re-associates with a new AP, it needs to re-authenticate. Depending on the type of authentication, this can increase the roaming time especially when an AAA server is involved.

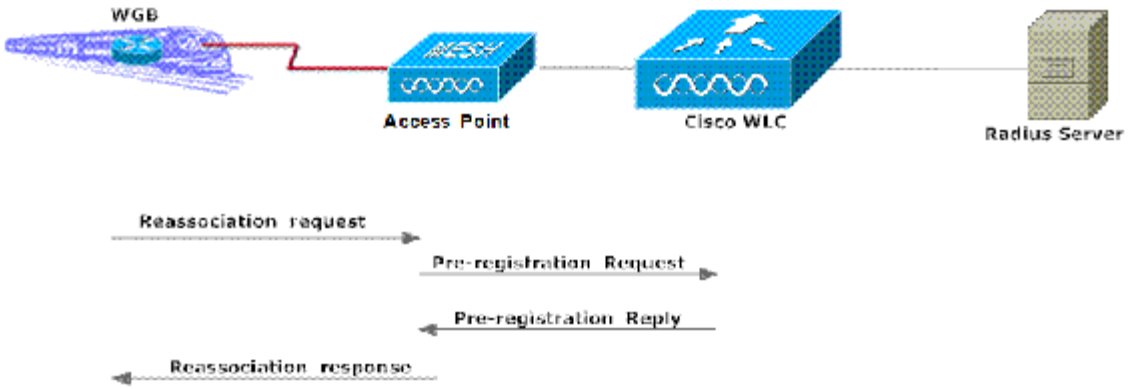
As shown here with LEAP, six exchanges are necessary with the radius server to complete the authentication. (EAP is similar):

LEAP Example



CCKM uses a fast rekeying technique that enables clients to roam from one AP to another. Full 802.1x/EAP authentication is not required. CCKM reduces the time required by the client to mutually authenticate with the new AP and derive a new session key during reassociation. CCKM fast secure roaming ensures that there is no perceptible delay in time-sensitive applications. CCKM is a CCXv4-compliant feature.

CCKM Example



With CCKM, the first association of the WMIC to the infrastructure will do a full 802.1x authentication + key material negotiation taking the steps as previously described.

Then on next roaming events, CCKM will do authentication at the same time it does the reassociation (Steps 4 and 5), and then reuse of the previously negotiated key material, on the first association.

In general, CCKM will remove 802.1x and EAPoL times from the full roaming process.

High-speed roaming of Cisco Compatible Extension (CX), version 4 (v4) clients is supported at speeds up to 70 mph

in outdoor mesh deployments of AP1522s and AP1524s. Roaming time depends upon various things, and this has been explained later in this section.

3 Cisco CX v4 Layer 2 client roaming enhancements are supported:

- **Access point assisted roaming**—This feature helps clients save scanning time. When a Cisco CXv4 client associates to an AP, it sends an information packet to the new access point listing the characteristics of its previous AP. Roaming time decreases when the client recognizes and uses an access point list built by compiling all previous APs to which each client was associated and sent (unicast) to the client immediately after association. The AP list contains the channels, BSSIDs of neighbor APs that support the client's current SSID(s), and time elapsed since disassociation.

- **Enhanced neighbor list**—This feature focuses on improving a Cisco CX v4 client's roam experience and network edge performance, especially when servicing voice applications. The AP provides its associated client information about its neighbors using a neighbor-list update unicast message.

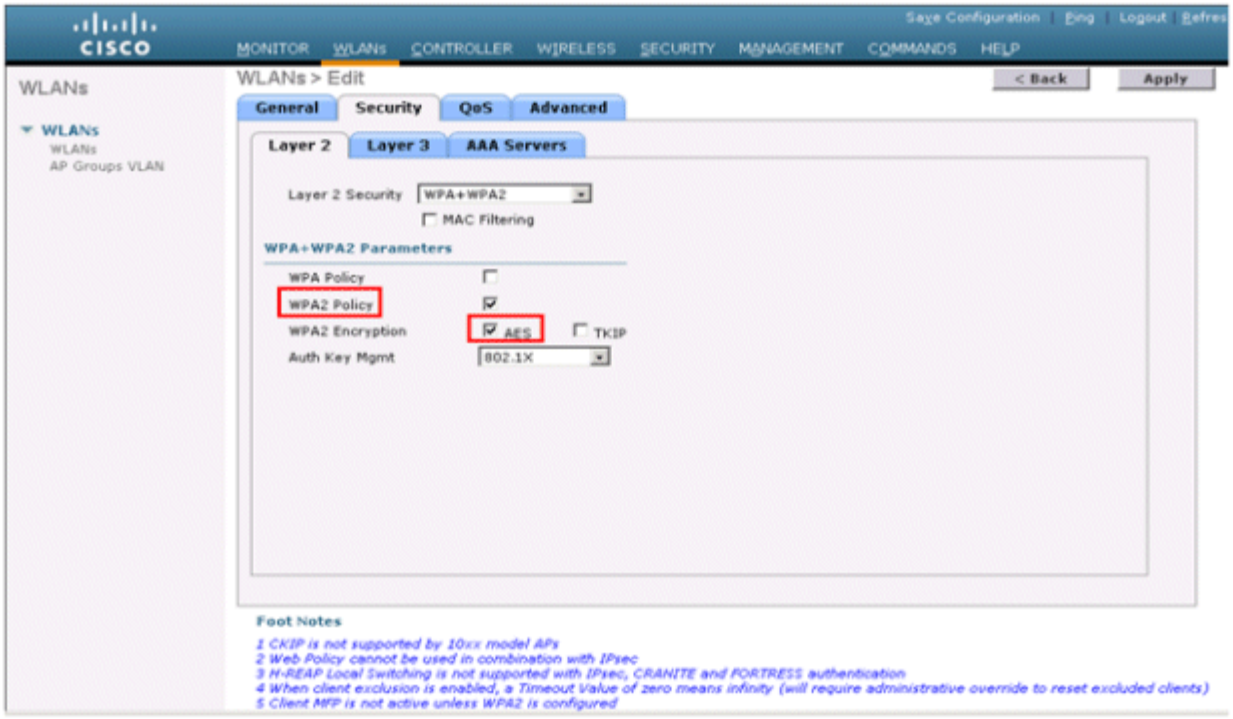
- **Roam reason report**—This feature enables Cisco CX v4 clients to report the reason why they roamed to a new AP. It also allows network administrators to build and monitor a roam history.

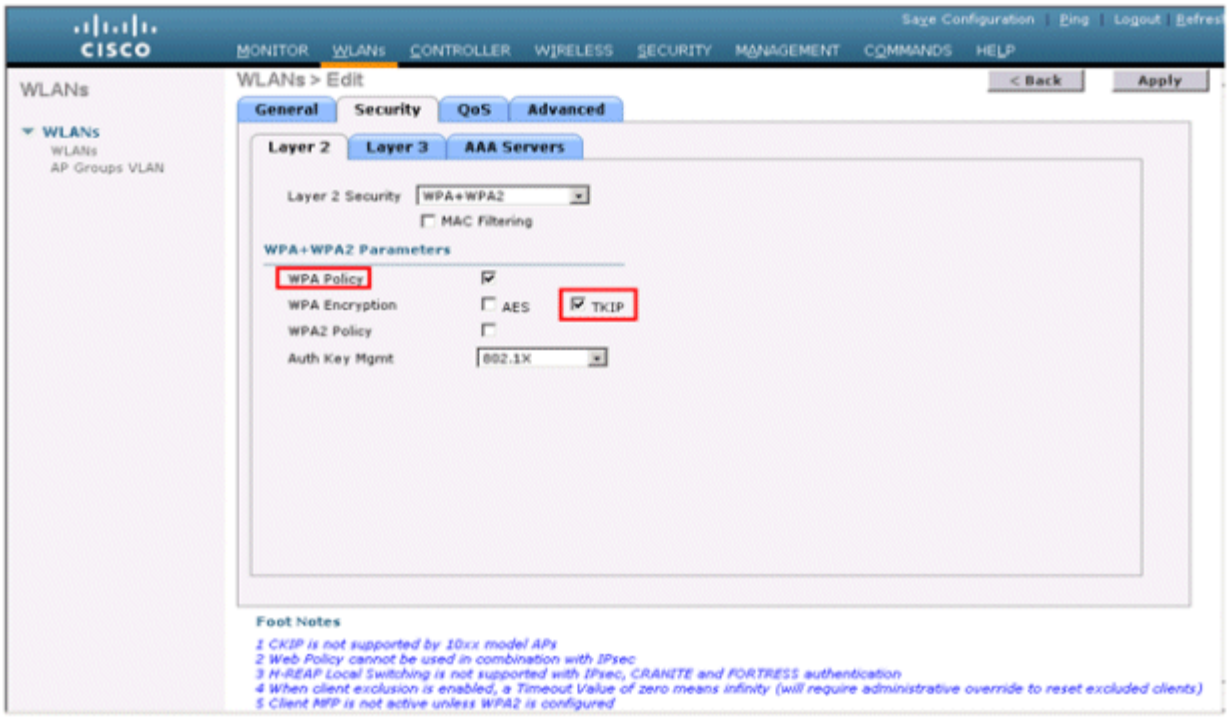
Encryption

The Cisco Unified Wireless Network includes support for the Wi-Fi Alliance certifications WPA and WPA2. WPA was introduced by the Wi-Fi Alliance in 2003. WPA2 was introduced by the Wi-Fi Alliance in 2004. All products Wi-Fi Certified for WPA2 are required to be interoperable with products that are Wi-Fi Certified for WPA.

WPA and WPA2 offer a high level of assurance for end users and network administrators that their data will remain private and that access to their networks will be restricted to authorized users. Both have personal and enterprise modes of operation that meet the distinct needs of the two market segments. The Enterprise Mode of each uses IEEE 802.1X and EAP for authentication. The Personal Mode of each uses PSK for authentication. Cisco does not recommend Personal Mode for business or government deployments because it uses a PSK for user authentication. PSK is not scalable and secure for Enterprise environments. WPA addresses all known WEP vulnerabilities in the original IEEE 802.11 security implementation bringing an immediate security solution to WLANs in both enterprise and small office/home office (SOHO) environments. WPA uses TKIP for encryption. WPA2 is the next generation of Wi-Fi security. It is the Wi-Fi Alliance's interoperable implementation of the ratified IEEE 802.11i standard. It implements the National Institute of Standards and Technology (NIST) recommended AES encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). WPA2 facilitates government FIPS 140-2 compliance.

For WLAN on the WLC, use either WPA1 or WPA2. For WPA2, **AES** is checked by default, and for WPA1, **TKIP** is checked by default:





Note: WGBs cannot associate to MAPs if colligated WLAN is configured with WPA1 (TKIP), +WPA2 (AES), and a corresponding WGB's interface is configured with ONLY one of these encryptions (either WPA1 or WPA2).

WPA(2)-PSK

On this mechanism, the PSK is used to create directly the Pairwise Master Key (PMK) bypassing the 802.1x process. It still has to do an EAPoL exchange.

The Actual Roaming time (Scanning + Reassociation + Overhead):

Application Roaming time = Scanning time + Reassociation time + WLC/WDS overheads (IAPP Update).

For WPA(2)-PSK the timings are 20-40ms (roaming scan) + 2ms (auth request) + 2ms (assoc req) + 20ms (EAPoL) + 3-100ms (IAPP). **Might vary from 47–164 ms.**

802.1x Authentication (without CCKM)

For 802.1x Authentication timings are20-40ms (roaming scan) + 2ms (auth request) + 2ms (assoc req) + 20-2500ms or more (dot1x) + 20ms (EAPoL) + 3-100ms (IAPP). **Might vary from 67–2664 ms.**

802.1x Authentication plus CCKM

20-40ms (roaming scan) + 2ms (auth request) + 2ms (assoc req) + 3-100ms (IAPP). **Might vary from 27–144 ms.**

Conclusion

CCKM is less susceptible to problems, as it has only two frames that need to be correctly sent to complete the roaming state change. The total time for successful roams is in average very small, which is useful for voice and/or video applications.

PSK is one alternative, but in average each roaming time is slower than CCKM and more probable to fail due to RF issues (more packet exchanges needed). Also, it is may be less secure depending on authentication key used. The benefit is a faster recovery time, when compared with the full 802.1x needed on CCKM failure scenario.

The main difference in PSK vs CCKM, is that for PSK, any retransmission of the EAPoL process will multiply the total time. In PSK you need to complete six frames exchange (association + EAPoL M1 to M4), which are the most critical point, as any failure here will affect the total roaming time.

A CCKM roaming failure means that the next roaming is 802.1x based (slow), then the subsequent roamings are CCKM again.

The situation is simple: either they use key caching, which we support and recommend to be CCKM, or work on a 802.1x based roaming, with times between 1 and 20 seconds on each roaming, which is not predictable.

Table 3: Roaming and Other Performance Numbers

Security Type	Roaming Delay	Probability
WPA2 802.1x with CCKM	< 200 msec	95% of time
WPA2 802.1x with CCKM	200 msec – 800 msec	4% of time
WPA2 802.1x with CCKM	>800 msec	1% of time

Note: Wireless technologies are designed using radio systems which are subject to radio wave interference. Causes of this interference may be accidental or deliberate. Regardless of the source, interference can interrupt the wireless connection, disabling any solution that depends on WI-FI. Given such risks, solutions that impact public safety should not depend SOLELY on wireless technologies. Redundant, overlapping, and independent systems (e.g. both wired and wireless) are preferred. In the context of train control systems, examples of overlapping, redundant systems include but

are not limited to: pairing wireless technologies with two or more independent systems, mechanical systems (e.g. “deadman switch”), train control signaling over metallic rails, and on-board and central human oversight (train driver) or central control supervisors. Should one system fail, another independent system would still be available, helping reduce risks to public safety.

Troubleshooting Tips

If a wireless client is not associating to a WGB, perform these steps to troubleshoot:

1. Verify the client configuration and make sure client configuration is proper.
2. Check the **show bridge** output in autonomous AP and conform the AP is reading the client MAC address in the right interface.
3. Confirm that sub interfaces corresponding to particular VLANs in different interfaces are mapped to the same bridge group.
4. If required, clear the bridge entry using the **clear bridge** command (remember this command will remove all wired and wireless clients associated in WGB and make them associate again).
5. Check **show dot11 association** output and conform WGB is associated to controller successfully.
6. WGB has a 20-client limitation, so make sure you have not exceeded the limit.

In a normal scenario if **show bridge** and **show dot11 association** outputs are as expected, the wireless client association should be successful.

If there are any WGB uplink problems, these commands can be used:

```
debug dot11 d0/1 tr pr uplink
debug dot11 wpa-cckm-km-dot1x
debug dot11 mgmt msg
debug dot11 mgmt int
```

Important Scenarios

- Wireless clients should be treated as a normal client for an autonomous AP and features like ACL, MAC Filtering, and authentication from LRS that can be applicable for these clients if configured from WGB (all autonomous features are supported).
- The wireless clients on the other radio should not be dissociated by the WGB upon losing its uplink or in a roaming scenario.
- Multicast should be supported for wireless clients behind WGB.
- Wireless clients behind WGB should get the same privilege of a wired client behind WGB in controller.

Multiple VLANs and QoS Support for WGB Wired Clients

Feature Overview

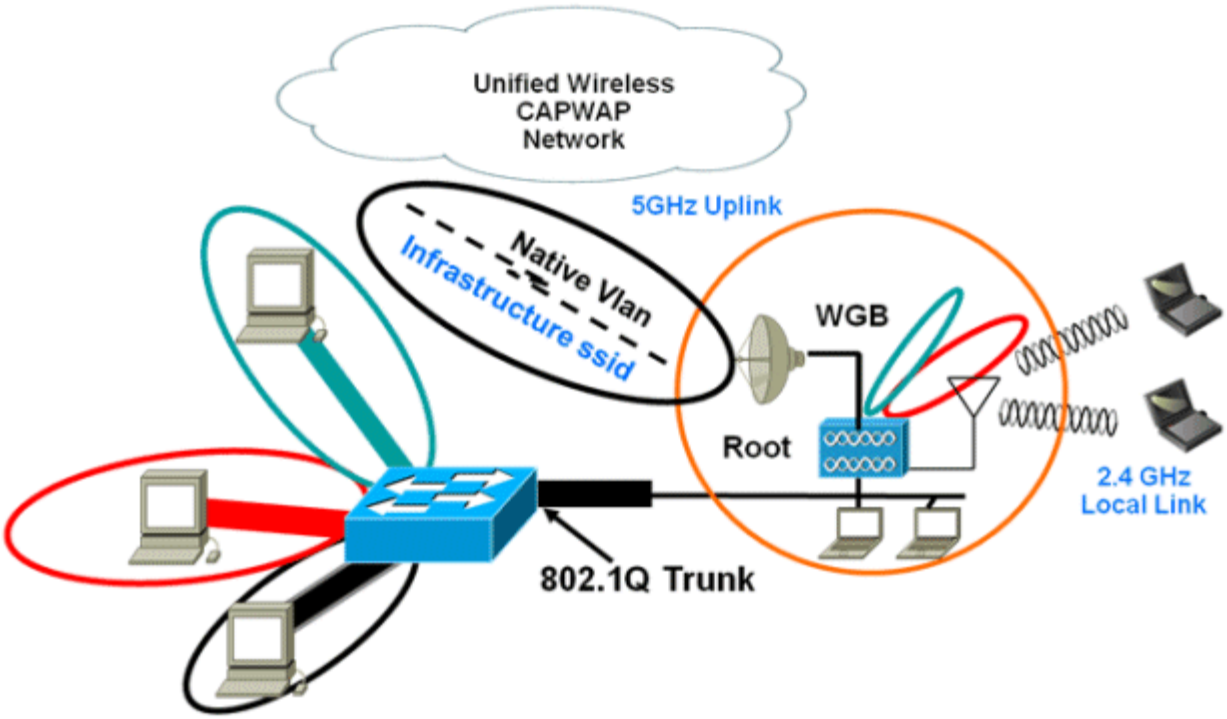
A WGB is a small stand-alone unit that can provide a wireless infrastructure connection for Ethernet-enabled devices. Devices that do not have a wireless client adapter in order to connect to the wireless network can be connected to the WGB through the Ethernet port. The WGB associates to the root AP through the wireless interface. In this way, wired clients get access to the wireless network.

This feature provides segregation of traffic based on VLANs for different applications running on different devices connected to a switch behind a WGB. Traffic from WGB clients will be sent in the right priority queue in the mesh backhaul based on DSCP/dot1p values.

Up to 16 VLANs are supported for wired clients behind WGB.

Note: You need a special autonomous image on the autonomous APs being used as WGB for interoperability with Unified CAPWAP infrastructure. This image will be merged with the next official autonomous release. This feature is not available for the MAR.

WGB and Multiple VLANs



WGB informs WLC about wired-client VLAN info in IAPP association message. WGB removes the 802.1q header from the packet while sending to the WLC. WLC will send the packet to WGB without 802.1q tag and WGB adds 802.1q header towards wired switch, based on destination MAC address.

WLC will treat the WGB client as a VLAN-client and forward the packet in the right VLAN interface based on the source MAC address

WGB unified client has to be enabled for multiple VLAN support on the WGB. This is disabled by default.

```
WGB(config)#workgroup-bridge unified-vlan-client
```

You have to configure subinterfaces on the WGB corresponding to the VLANs on the switch ports to which wired clients are connected.

Points to Remember before Configuring

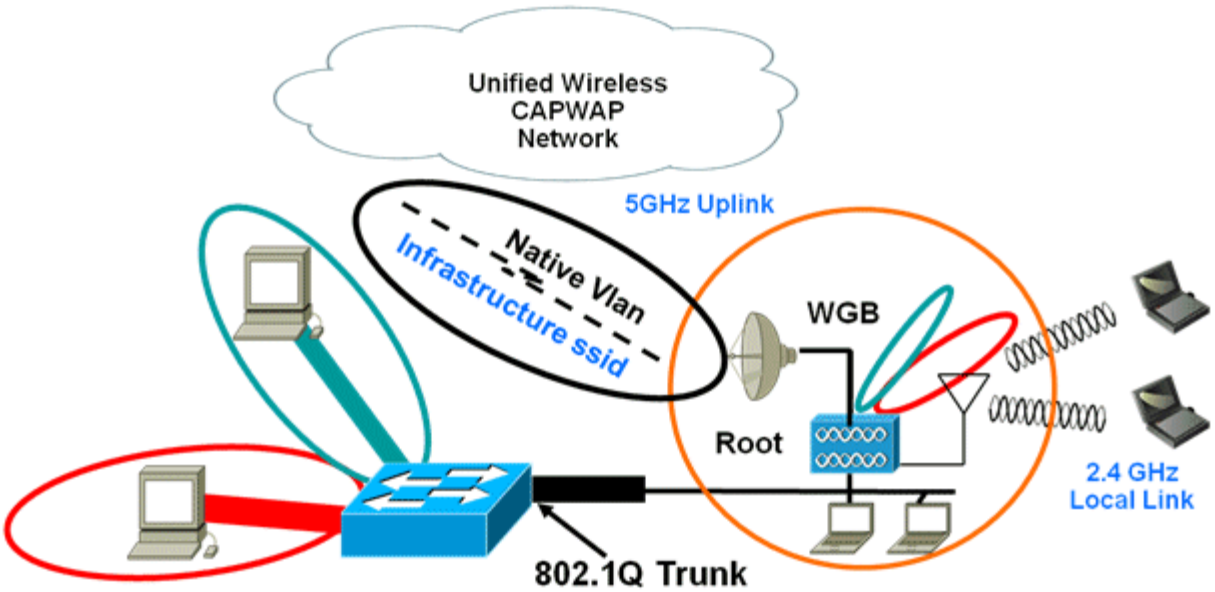
- Dynamic interface should be created in the controller for each VLAN configured in the WGB.
- Only one WLAN (SSID) for wireless association of WGB to the AP infrastructure is supported. This SSID should be configured as infrastructure SSID and should be mapped to the native VLAN. WGB will drop everything which is not in native VLAN towards the mesh infrastructure.

- WGB will read the switch port behind as a client in its MAC address table.
- It is recommended to configure the same native VLAN in the switch port connecting WLC, WGB, and in the switch behind the WGB.

  All native VLAN clients on the WGB Ethernet side will be part of the same VLAN in which WGB is asscoicated. WGB will be part of the VLAN to which the WLAN (in which WGB has associated) is mapped.

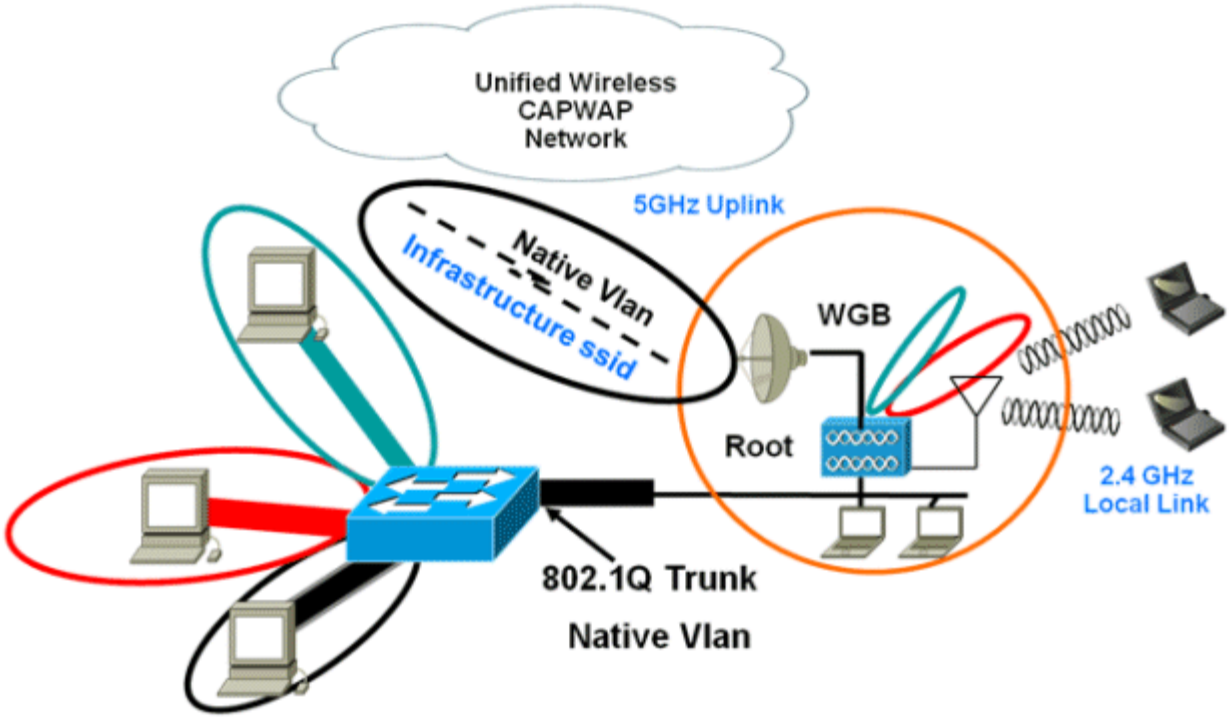
  For example, if a WGB 5 GHz radio (dot11radio 1) is mapped to a native VLAN 184, and the switch behind the WGB has wired clients only in VLAN 185 and 186, then you may not require the native VLAN on the switch port to be identical to the native VLAN on the WGB (VLAN 184). However, Cisco always recommends you configure the same native VLAN on the switch port as the native VLAN of WGB.

  Non-Identical Native VLANs



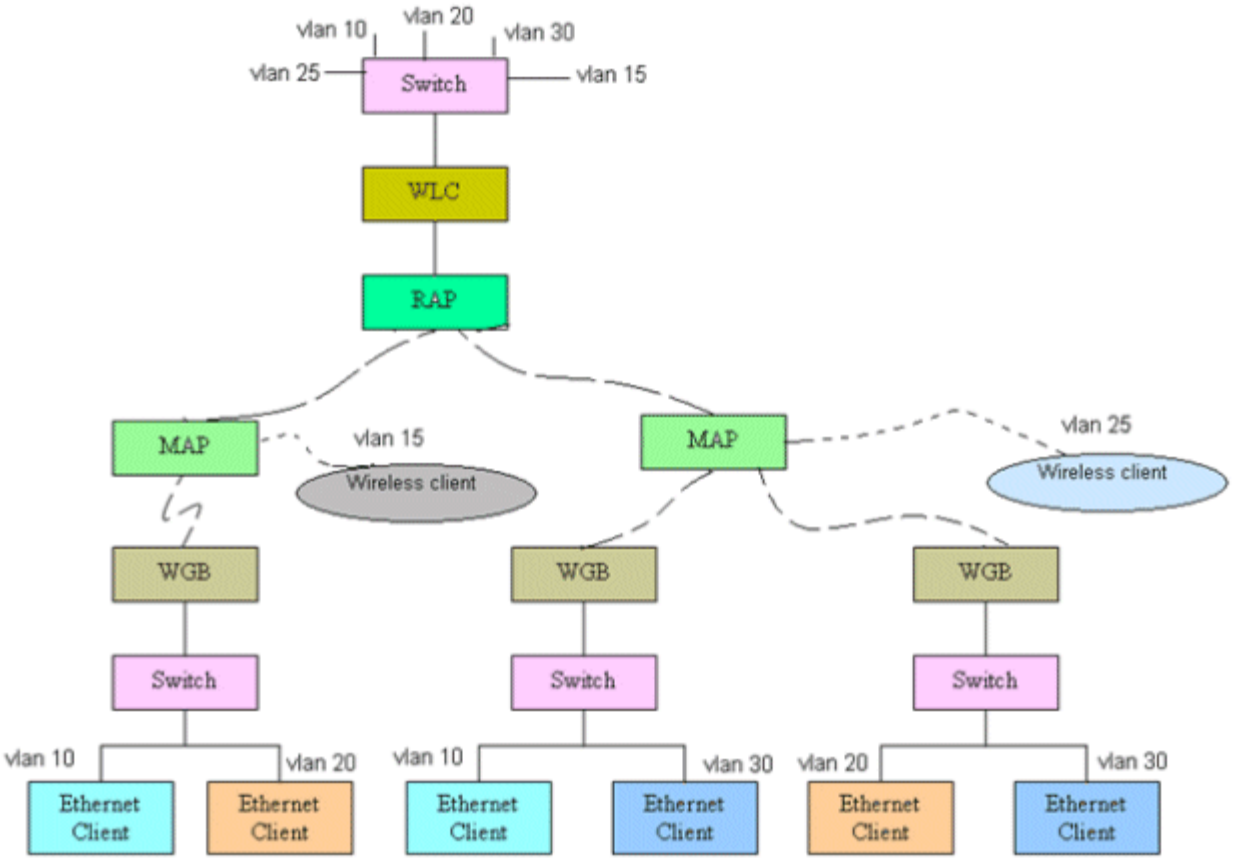
  Conversely, if you add 1 wired client in VLAN 184, and this VLAN client in the WGB belongs to the native VLAN, you have to define the same native VLAN on the switch.

  Same Native VLAN



- Inter-subnet mobility is supported with this feature for VLAN clients behind the WGB with a limitation that, dynamic interface for all VLANs of the WGB should be configured in all the controllers.
- Inter-operability with the VLAN-pooling feature is not supported. When the VLAN-pooling feature is enabled, the WGB and its native VLAN clients will be part of the same VLAN.
- AAA-override for WGB clients is not supported. However, AAA-override for WGB is supported.
- Only Layer-3 multicast is provided for WGB VLAN clients and there is no support for layer-2 multicast.
- There is limitation of 20 clients in WGB and wireless clients are included in this number.
- Link test for the WGB wired client is not supported.
- Roaming is supported for wireless and wired clients behind the WGB.
- Multicast is supported for wired clients behind the WGB
- Broadcast is supported.

Network Diagram



Configure via CLI in WGB (Example)

In this example, VLANs 184 and 185 exist on the wired switch behind the WGB. The WGB's native VLAN is 184. SSID is **auto-wgb** maped to native VLAN 184. Radio 1 (5 GHz) radio is being used to connect to the CAPWAP infrastructure using this SSID.

```
ap#config t
ap(config)#workgroup-bridge unified-vlan-client
ap(config)#int FastEthernet0.184
ap(config-subif)#encapsulation dot1q 184 native
ap(config-subif)#bridge-group 1
ap(config-subif)#exit
ap(config)#int FastEthernet0.185
ap(config-subif)#encapsulation dot1q 185
ap(config-subif)#bridge-group 185
ap(config-subif)#exit
ap(config)#int Dot11Radio 1.185
ap(config-subif)#encapsulation dot1q 185
ap(config-subif)#bridge-group 185
ap(config-subif)#exit
ap(config)#int Dot11Radio 1.184
ap(config-subif)#encapsulation dot1q 184 native
ap(config-subif)#bridge-group 1
ap(config-subif)#exit
ap(config)#dot11 ssid auto-wgb
ap(config-ssid)#authentication open
ap(config-ssid)#infrastructure-ssid
ap(config-ssid)#vlan 184
ap(config-ssid)#exit
ap(config)#int Dot11Radio 1
ap(config-if)#station-role workgroup-bridge
ap(config-if)#ssid auto-wgb
ap(config-if)#exit
ap(config)#bridge irb
ap(config)#hostname WGB
```

bridge irb is used to enable Integrated Routing and Bridging; something which Auto AP code has retained from other higher end platforms.

One has to create dynamic interfaces 184 and 185 on the WLC for the above configuration to work. WGB will update the WLC about wired-client VLAN information in the IAPP association message. WLC will treat the WGB client as a VLAN-client and forward the packet in the right VLAN interface based on the source MAC address. In the upstream direction, the WGB will remove the 802.1q header from the packet while sending to the WLC. In the downstream direction, the WLC will send the packet to the WGB without 802.1q tag and the WGB will add the 802.1q header based on destination MAC address, while forwarding the packet to the switch connecting the wired-client.

WGB Bridge Output

```
WGB#sh bridge
Total of 300 station blocks, 292 free
Codes: P - permanent, S – self

Bridge Group 1:
    Address             Action     Interface       Age   RX count   TX count
0023.049a.0b12          forward    Fa0.184          0        2          0
0016.c75d.b48f          forward    Fa0.184          0        21         0
0021.91f8.e9ae          forward    Fa0.184          0        110        16
0017.59ff.47c2          forward    Vi0.184          0        23         22
0021.5504.07b5          forward    Fa0.184          0        18         6
0021.1c7b.38e0          forward    Vi0.184          0        6          0

Bridge Group 185:
0016.c75d.b48f          forward    Fa0.185          0        10         0
001e.5831.c74a          forward    Fa0.185          0        9          0
```

WGB Detail on Controller

```
(Cisco Controller) >show wgb summary

Number of WGBs..................................... 2
MAC Address        IP Address   AP Name  Status   WLAN  Auth  Protocol  Clients
-----------------  -------------- -----------------  --------- ----  ----  ---
00:1d:70:97:bd:e8  9.47.184.54  c1240    Assoc    2     Yes   802.11a    2
00:1e:be:27:5f:e2  9.47.184.55  c1240    Assoc    2     Yes   802.11a    5
(Cisco Controller) >show client summary
Number of Clients.............................. 7
MAC Address       AP Name  Status         WLAN/Guest-Lan Auth Protocol Port Wired
00:00:24:ca:a9:b4  R14     Associated        1           Yes  N/A      29   No
00:24:c4:a0:61:3a  R14     Associated        1           Yes  802.11a  29   No
00:24:c4:a0:61:f4  R14     Associated        1           Yes  802.11a  29   No
00:24:c4:a0:61:f8  R14     Associated        1           Yes  802.11a  29   No
00:24:c4:a0:62:0a  R14     Associated        1           Yes  802.11a  29   No
00:24:c4:a0:62:42  R14     Associated        1           Yes  802.11a  29   No
00:24:c4:a0:71:d2  R14     Associated        1           Yes  802.11a  29   No

(Cisco Controller) >show wgb detail 00:1e:be:27:5f:e2
Number of wired client(s): 5
MAC Address        IP Address      AP Name         Mobility   WLAN  Auth
-----------------  -------------- -----------------  ---------- ---- ----
00:16:c7:5d:b4:8f  Unknown         c1240           Local      2     No
00:21:91:f8:e9:ae  9.47.184.83     c1240           Local      2     Yes
00:21:55:04:07:b5  9.47.184.66     c1240           Local      2     Yes
00:1e:58:31:c7:4a  9.47.185.75     c1240           Local      2     Yes
00:23:04:9a:0b:12  Unknown         c1240           Local      2     No

WGB_1#sh ip int brief
Interface                  IP-Address      OK?  Method   Status        Protocol
BVI1                       9.47.184.55     YES  DHCP     up              up
Dot11Radio0                unassigned      YES  unset    admindown       down
Dot11Radio1                unassigned      YES  TFTP     up              up
Dot11Radio1.184            unassigned      YES  unset    up              up
Dot11Radio1.185            unassigned      YES  unset    up              up
FastEthernet0              unassigned      YES  other    up              up
FastEthernet0.184          unassigned      YES  unset    up              up
FastEthernet0.185          unassigned      YES  unset    up              up
Virtual-Dot11Radio0        unassigned      YES  TFTP     up              up
Virtual-Dot11Radio0.184    unassigned      YES  unset    up              up
Virtual-Dot11Radio0.185    unassigned      YES  unset    up              up
```

Troubleshooting Tips

If a WGB client is not associating to the WGB, these steps can be used in order to troubleshoot:

1. The native VLAN configured on the WGB needs to be same on the switch port to which the WGB is connected. The switch port connected to the WGB should be Trunk.
2. Verify the client configuration and make sure the client configuration is proper.
3. Check the **show bridge** output in autonomous AP and confirm that the AP is reading the client MAC address in right interface.
4. Confirm sub interfaces corresponding to particular VLANs and sub different interfaces are mapped to the bridge group.
5. If required, clear the bridge entry using the **clear bridge** command (remember this command will remove all wired and wireless clients associated in the WGB and make them associate again).
6. The WGB has a 20-client limitation, so make sure you have not exceeded the limit.
7. Up to 16 VLANs are supported for Wired Clients behind WGB.

QoS on Mesh Infrastructure

Cisco supports 802.11e on the local access and on the backhaul. The MAPs prioritize user traffic based on classification and therefore all user traffic is treated on a best-effort basis.

Resources available to users of the mesh vary, according to the location within the mesh, and a configuration that provides bandwidth limitation in one point of the network can result in oversubscription in other parts of the network.

Similarly, limiting clients on their percentage of RF is not suitable for mesh clients. The limiting resource is not the client WLAN, but the resources available on the mesh backhaul. Similar to wired Ethernet networks, 802.11 WLANs employ Carrier Sense Multiple Access (CSMA), but instead of using collision detection (CD), WLANs use collision avoidance (CA). This means that instead of each station trying to transmit as soon as the medium is free, WLAN devices will use a collision avoidance mechanism to prevent multiple stations from transmitting at the same time.

The collision avoidance mechanism uses two values, called aCWmin and aCWmax. CW stands for contention window. The CW determines what additional amount of time an endpoint should wait, after the interframe space (IFS), to attempt to transmit a packet. Enhanced distributed coordination function (EDCF) is a model that allows end devices that have delay-sensitive multi-media traffic to modify their aCWmin and aCWmax values to allow for statically greater (and more frequent) access to the medium.

Cisco APs support EDCF-like QoS. This provides up to eight queues for QoS. These queues can be allocated in several different ways:

- Based on TOS / DiffServ settings of packets.
- Based on Layer 2 or Layer 3 access lists.
- Based on VLAN.
- Based on dynamic registration of devices (IP phones).

The Cisco Aironet 1520, in conjunction with Cisco controllers, provides a minimal integrated services capability at the

controller, in which client streams have maximum bandwidth caps, and a more robust differentiated services (diffServ) capability based on the IP DSCP values and QOS WLAN overrides.

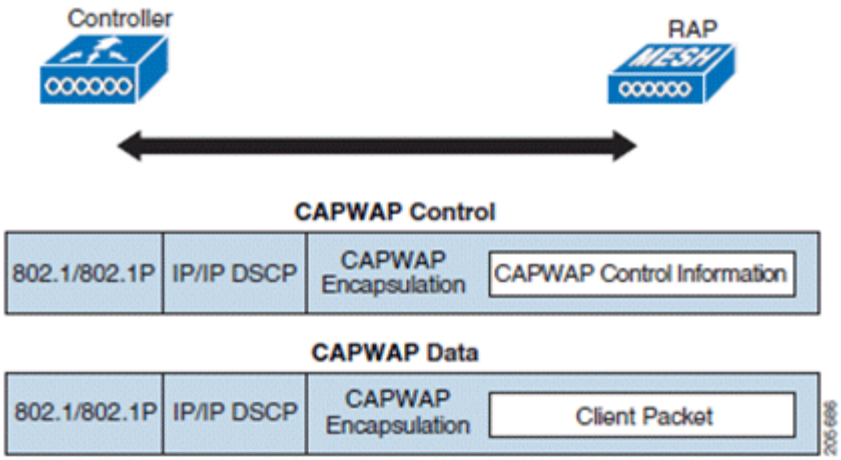
When the queue capacity has been reached, additional frames are dropped (tail drop).

Encapsulation

There are several encapsulations used by the mesh system. These include CAPWAP control and data between the controller and RAP, over the mesh backhaul, and between the MAP to the client. The encapsulation of bridging traffic (non-controller traffic from a LAN) over the backhaul is the same as the encapsulation of CAPWAP data.

There are two encapsulations between the controller and the RAP. The first is for CAPWAP control, and the second for CAPWAP data. In the control instance, CAPWAP is used as a container for control information and directives. In the instance of CAPWAP data, the entire packet, including the Ethernet and IP headers, is sent in the CAPWAP container (see Encapsulations).

Encapsulations

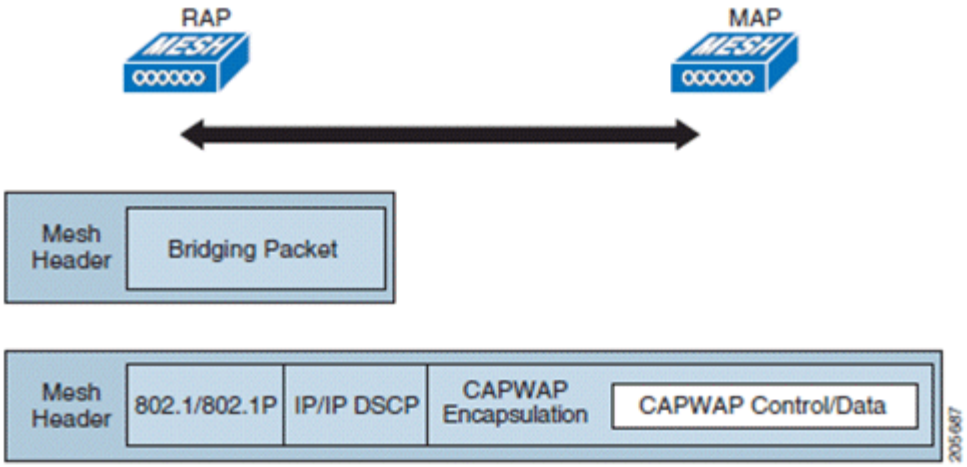


For the backhaul, there is only one type of encapsulation, encapsulating mesh traffic. However, two types of traffic are encapsulated: bridging traffic and CAPWAP control and data traffic. Both types of traffic are encapsulated in a proprietary mesh header.

In the case of bridging traffic, the entire packet Ethernet frame is encapsulated in the mesh header (see Encapsulating Mesh Traffic).

All backhaul frames are treated identically, regardless of whether they are MAP to MAP, RAP to MAP, or MAP to RAP.

Encapsulating Mesh Traffic



In the case of bridging, the frames are transmitted as they are received at the ingress to the AP Ethernet port.

Queuing on the APs

The AP uses a high-speed CPU to process ingress frames, Ethernet, and wireless on a first-come first-serve basis. These are queued for transmission to the appropriate output device, either Ethernet or wireless. Egress frames can be destined for either the 802.11 client network, the 802.11 backhaul network, or Ethernet.

The Cisco Aironet 1520 Series AP supports four FIFOs for wireless client transmissions. These FIFOs correspond to the 802.11e platinum, gold, silver, and bronze queues, and obey the 802.11e transmission rules for those queues. The FIFOs have a user configurable queue depth.

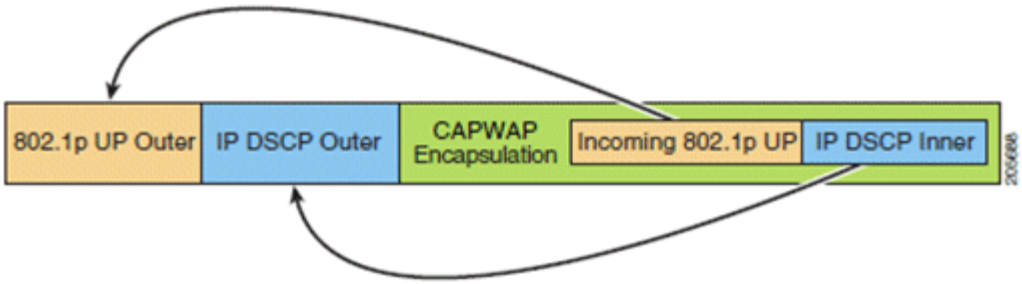
Likewise, the backhaul (frames destined for another outdoor Access Point) uses four FIFOs, though user traffic is limited to gold, silver, and bronze. The platinum queue is used exclusively for CAPWAP control traffic and Voice, and has been reworked from the standard 802.11e parameters for CWMIN, CWMAX, and so on, to provide more robust transmission but higher latencies.

Similarly, the 802.11e parameters for CWMIN, CWMAX, and so on, for the gold queue have been reworked to provide lower latency at the expense of slightly higher error rate and aggressiveness. The purpose of these changes is to provide a channel more conducive to video applications.

Frames destined for Ethernet are queued as FIFO, up to the maximum available transmit buffer pool (256 frames). There is a support for Layer 3 IP Differentiated Services Code Point (DSCP), so marking of the packets is there as well.

(In the controller to RAP path for the data traffic, the outer DSCP value is set to the DSCP value of the incoming IP frame. If the interface is in tagged mode, the controller sets the 802.1Q VLAN ID, and derives the 802.1p UP (outer) from 802.1p UP incoming and the WLAN default priority ceiling. Frames with VLAN ID 0 will not be tagged (see Controller to RAP Path).

Controller to RAP Path



For CAPWAP, control traffic to the IP DSCP value is set to *46*, and the 802.1p user priority is set to *7*. Prior to transmission of a wireless frame over the backhaul, regardless of node pairing (RAP/MAP) or direction, the DSCP value in the outer header is used to determine a backhaul priority. The following sections describe the mapping between the four backhaul queues the AP uses and the DSCP values shown in Backhaul Path QoS.

Table 4: Backhaul Path QoS

DSCP Value	Backhaul Queue
2, 4, 6, 8-23	Bronze
26, 32-63	Gold
46-56	Platinum
All others, including 0	Silver

Note: The platinum backhaul queue is reserved for CAPWAP control traffic, IP control traffic, and Voice Packets. DHCP, DNS and ARP requests are also transmitted at the platinum QoS level. The mesh software inspects each frame to determine whether it is an CAPWAP control or IP control frame in order to protect the platinum queue from use by non-CAPWAP applications.

For a MAP to the client path, there are two different procedures, depending on whether the client is a WMM client or a normal client. If the client is a WMM client, the DSCP value in the outer frame is examined, and the 802.11e priority queue is used (see MAP to Client Path QoS).

Table 5: MAP to Client Path QoS

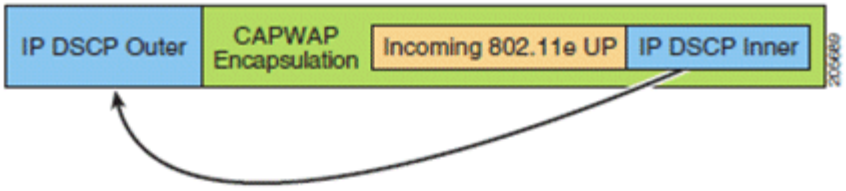
DSCP Value	Backhaul Queue
2, 4, 6, 8-23	Bronze
26, 32-45, 47	Gold
46, 48-63	Platinum
All others, including 0	Silver

Queuing on the APs

If the client is not a WMM client, the WLAN override (as configured at the controller) determines the 802.11e queue (bronze, gold, platinum, or silver), on which the packet is transmitted.

For client towards AP, there are modifications made to incoming client frames in preparation for transmission on the mesh backhaul or Ethernet. For WMM clients, MAP illustrates the way in which the outer DSCP value is set from an incoming WMM client frame.

MAP to RAP Path



The minimum of the incoming 802.11e user priority and the WLAN override priority is translated using the information listed in to determine the DSCP value of the IP frame. For example, if the incoming frame has as its value a priority indicating the gold priority, but the WLAN is configured for silver priority, the minimum priority of silver is used to determine the DSCP value.

Table 6: DSCP to Backhaul Queue Mapping

DSCP Value	802.11e UP	Backhaul Queue	Packet Types
2, 4, 6, 8 - 23	1, 2	Bronze	Lowest priority packets if any
26, 32-34	4, 5	Gold	Video packets
46 - 56	6, 7	Platinum	CAPWAPP Control, AWPP, DHCP/DNS, ARP packets, Voice packets
All others, including 0	0, 3	Silver	Best-effort, CAPWAPP Data packets

In the event that there is no incoming WMM priority, the default WLAN priority is used to generate the DSCP value in the outer header. In the event that the frame is an originated CAPWAP control frame, the DSCP value of 46 is placed in the outer header.

With the 5.2 code enhancements, DSCP information is preserved in AWPP header.

All wired client traffic is restricted to a max. 802.1p UP value of 5, except DHCP/DNS and ARP packets, they will go

through the platinum queue.

The non-WMM wireless client traffic gets the default QoS priority of its WLAN. While, the WMM wireless client traffic may have maximum 802.11e value of 6, but they must be below the QoS profile configured for its WLAN. If admission control is configured, WMM clients must use TSPEC signaling and get admitted by CAC.

The CAPWAPP data traffic carries wireless client traffic and hence has the same priority and treatment as wireless client traffic.

Now that the DSCP value is determined, the rules described earlier for the backhaul path from RAP to MAP are used to further determine the backhaul queue on which the frame is transmitted. Frames transmitted from the RAP to the controller are not tagged. The outer DSCP values are left intact, as they were first constructed.

Bridging Backhaul Packets

Bridging services are treated a little differently from regular controller-based services. There is no outer DSCP value in bridging packets because they are not CAPWAP encapsulated. Therefore, the DSCP value in the IP header as it was received by the AP is used to index into the table as described in the path from AP to AP (backhaul).

Bridging Packets from and to a LAN

Packets received from a station on a LAN are not modified in any way. There is no override value for the LAN priority. Therefore, in bridging mode the LAN must be properly secured. The only protection offered to the mesh backhaul is that non-CAPWAP control frames that map to the platinum queue are demoted to the gold queue.

Packets are transmitted to the LAN precisely as they are received on ingress at entry Ethernet to the mesh.

The only way to integrate QoS between Ethernet ports on AP1520 and 802.11a is by tagging Ethernet packets with DSCP. The AP1520 will take the Ethernet packet with DSCP and will place it in the appropriate 802.11e queue.

The 1520 does not tag DSCP itself:

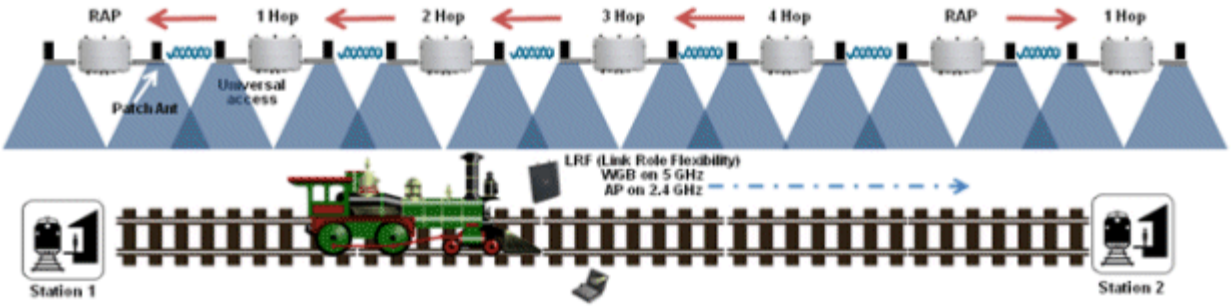
- On the ingress port, the 1520 sees a DSCP tag and will encapsulate the Ethernet frame and apply the corresponding 802.11e priority.
- On the egress port, the 1520 decapsulates the Ethernet frame and places it on the wire with an untouched DSCP field.

The Ethernet devices, like video cameras, should have the capability to mark the bits with DSCP value to take advantage of QoS.

WGB Installation

An AP in WGB mode is installed in the moving train or vehicle. This AP will connect to the wireless infrastructure network along the rail tracks or road in a linear fashion. The WGB will do fast roaming and maintain connectivity if all the necessary configurations are done on the WGB and AP infrastructure.

Moving Train Example



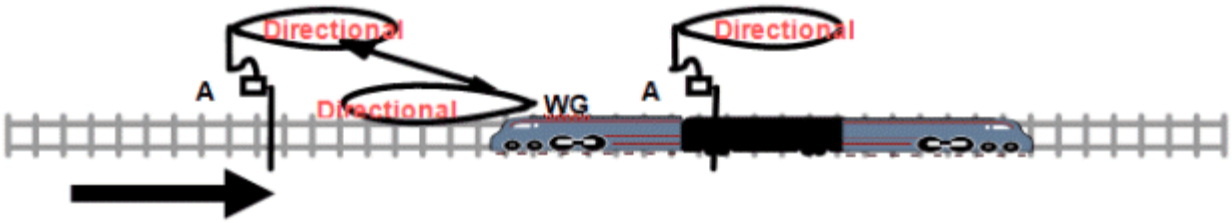
Here also, it is advisable to go with directional antenna for better usage of RF energy. Patch antennas are preferable in this case as it will not be affected by wind resistance on fast moving trains.

The trains are regularly subjected to washing with water jets and chemicals and if the WGB APs are mounted outside, they may get damaged. Trains also run at high speeds, so it is important to choose antenna which is meant for outdoors and can withstand a strong wind speeds. Strong winds may tear apart the antenna if mounted outside.

A WiFi client roaming is typically triggered by low signal strength, a rise in packet error rate, or AP loading considerations. In the above case, when the AP is operating in the head of the train, The WiFi signal on WGB will gain in signal strength as the train moves closer to the AP, then the signal changes from the strongest state to the weakest state at the point AP roams. This will delay the time AP to do roaming.

When the WGB is mounted on the tail of the train car, the WiFi signal on the WGB will gain in strength as the train moves away from the AP it is associated to. The signal changes from the weakest state to the strongest state at the point AP roams and this enables the AP to make roaming decision faster.

Train AP

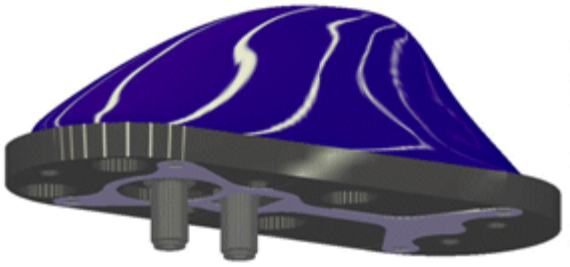


Therefore, it is advisable to mount the Train AP on the tail of the train.

Diversity is an important aspect of getting more gain. One should try to get max advantage of it—as the more the link budget in the uplink, the better is the performance. Chose an antenna which has two input ports and can honor diversity ports coming from the APs. Make sure to use low loss cables connecting antenna and the access point. If you are using single port antenna, then please make sure that you have switched off diversity, as diversity with single antenna can create worse conditions.

The following figure shows a 13 dBi 5 GHz external antenna with two ports, from Huber+Suhner with 30 degrees Vertical and Horizontal Bandwidths. Antenna is mounted at the back part of the coach. Of course, if the same train is moving in north and south direction than two WGBs can be installed in each coach/car of the train at two extreme ends. This will not only increase the redundancy, but also increase the capacity of accommodating clients, as a single WGB can only associate 20 clients while talking to a unified AP infrastructure.

13 dBi 5 GHz External Antenna



13 dBi 5 GHz External Antenna Mounted in Coach

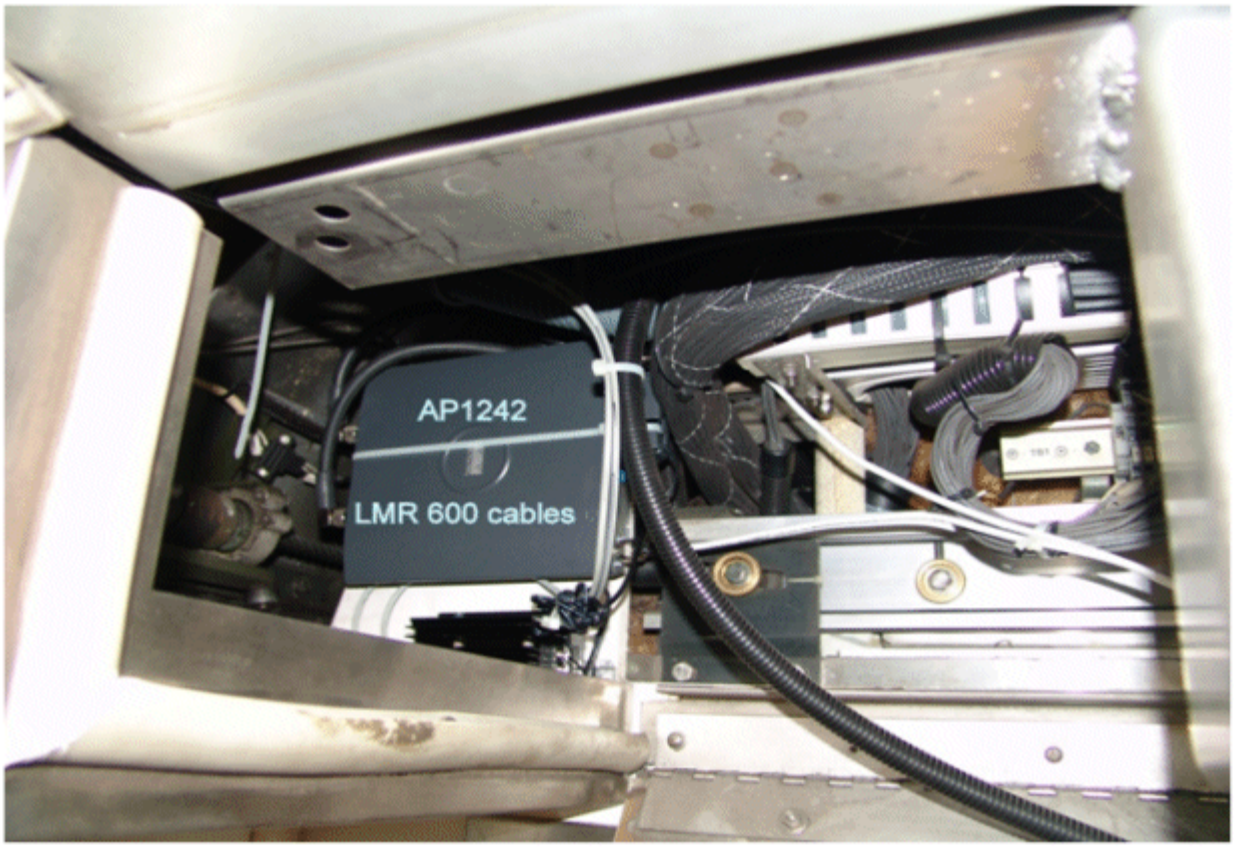
If mounting the antenna outside the moving vehicle is not possible, then antennas can typically be clamped or fixed to the glass facing outside in front of the train. The glass screen on the train may induce a loss of 2-4 db depending on the thickness. The antenna should have enough gain to compensate for that loss.

Antennas Mounted to Glass

Sometimes, train tracks can have high power lines overhead (up to 4,000 watts). These trains run off electric power, instead of coal or diesel. Although these power lines do not create RF interference, they do create special grounding requirements for antennas which go on train rooftops. Many vendors like Huber+Suhner specialize in providing train antennas that meet these requirements.

For installing a WGB, always proceed with an “out of site- out of mind” approach to avoid vandalism. A WGB inside the train has to provide coverage for 2.4 GHz access. As a result, proper care should be taken to install these antennas in an unobstructed manner. The following picture shows a one such installation in one of the corner inside a train coach inside the roof. It is completely hidden and is not visible. Two low loss RF cables have been taken outside from the two antenna ports of AP1242 and attached to the external third-party antenna. This picture shows a cross-section of the train coach where the AP1242 WGB has been installed:

Cross-Section of Train Coach



This cross section is actually covered with the metallic cover matching the internal body structure of the coach exactly.

Note that client access can also be made available for the passengers or customers standing on the platform, waiting station etc, as infrastructure of the MAP is already there. As a result, client access can be provided on both 5 GHz and 2.4 GHz directly from the MAPs. Now the clients will move from autonomous APs (WGB) to unified CAPWAP APs (mesh). The good part of this client access is that it does not require fast roaming! Another good part is that a strong link budget is available not only in the downlink direction due to high power, but also in the uplink direction due to multiple antennas. For 2.4 GHz client access directly from the MAPs, maximum ratio combining (MRC) can be used to take advantage of higher receiver gains. When operating with data rates higher that 12 Mb/s, you can increase gain on a 2.4-GHz radio to 2.7 dB by adding 2 antennas and to 4.5 dB, by adding 3 antennas.

You also have to check as to how much voltage is available on the train or the moving vehicle. Sometimes third-part arrangements have to be made to up convert or down convert available voltage to power on the WGB. Generally in the USA, 72V is available on the train, so 72-48V DC voltage converters have to be installed and cables have been run internally for every coach to bring the 72V DC power from the train engine to every coach.

Mobile Access Router

The Cisco 3200 Series MAR consists of 1 or more PC104/Plus modules that stack together to form a wireless router configuration. These modular card combinations are either available as card bundles or as complete systems assembled in a Cisco 3200 rugged enclosure.

Cisco 3200 Series MAR

The Cisco Rugged Enclosure Option for the 3200 Series is designed for in-vehicle use, addressing the specific mobility needs of the public safety, transportation, defense, and homeland security markets. The Rugged Enclosure Option is completely sealed and is designed to withstand harsh environments, including large variations in temperature and altitude, intense shock/vibration, and exposure to dampness, moisture, or dust.

Please refer to the Cisco 3200 Series Rugged Integrated Services Routers Enclosures data sheet for more information and further details of the rugged enclosure.

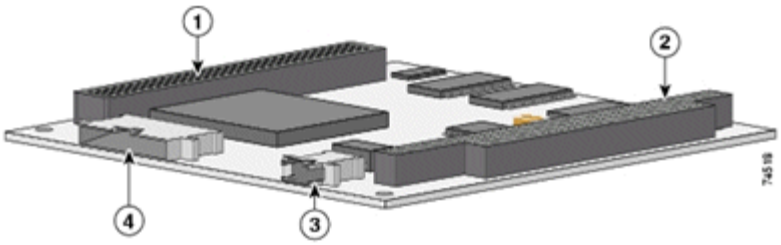
The Cisco 3200 Series Router bundles consist of the Cisco 3230 and the Cisco 3270 models. The bundle consists of a Mobile Access Router Card (MARC), a Serial Mobile Interface Card (SMIC), a Fast Ethernet Switching Mobile Interface Card (FESMIC), wireless mobile interface cards (WMICs) and a Mobile Router Power Card (MRPC).

For your reference, the MAR3230 bundle is shown here:

For more information on Cisco 3200 card bundles refer to the Cisco 3230 Rugged Integrated Services Routers data sheet.

MARC

The MARC is an IOS router 3250:



It includes the host processor, memory, and headers for the Fast Ethernet, console, and auxiliary signals for the router.

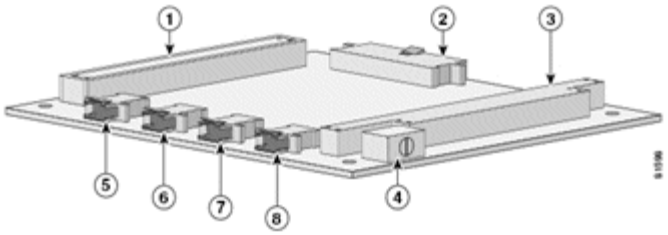
1: PCI BUS, 2: ISA BUS, 3: Fast Ethernet, 4: Multifunction Header

The PCI bus connector supports communication between the SMIC, the FESMIC, and the MARC. The WMIC communicates with the router through an internal Fast Ethernet port and is configured through an independent console

port; the WMIC only draws power from the bus.

FESMIC

The FESMIC is a 4-port Fast Ethernet switch:



1: PCI BUS, 2:LED connector, 3: ISA BUS, 4: Rotary switch, 5-8:Fast Ethernet headers.

The position of the rotary switch determines the port assignments. The rotary position for the MAR installed on the buses will be 2, which corresponds to Fast Ethernet 2/0-2/3. The card communicates to the MARC through the PCI bus.

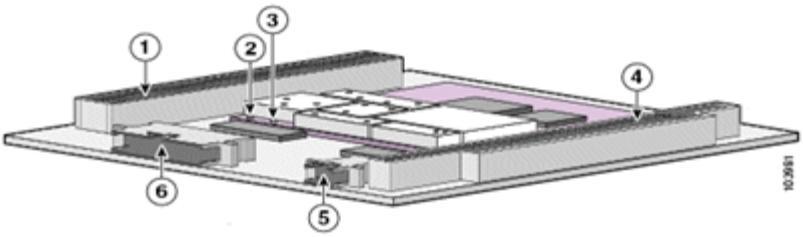
WMIC

There are three types of WMICs, depending upon the frequency band:

- “802.11a” interface card 5 GHz (C3205WMIC-TPEK9)
- “802.11bg” interface card 2.4 GHz (C3201WMIC-TPEK9)
- “802.11a” interface card 4.9 GHz (C3202WMIC-TPEK9)

There are 2 of them on the MAR 3230.

They can be configured as a WGB. The WGB is similar to an AP client:



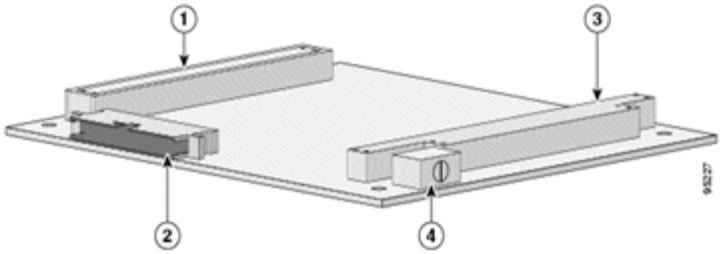
It will allow the MAR to connect to the infrastructure APs along the track/railroad or inside the tunnel, etc.

1: PCI BUS, 2: Left Antenna, 3: Right Antenna, 4: ISA BUS, 5: Fast Ethernet, 6: LED and console connector.

The WMIC does not use the PCI and ISA bus. It communicates with the router through an internal Fast Ethernet port.

SMIC

The SMIC provides the router with up to four high-speed sets of serial signals in both data terminal equipment (DTE) and data circuit equipment (DCE) modes:



1: PCI BUS, 2: 60-pin multifunction header for Serial 0 and Serial 1 signals , 3: ISA BUS, 4: Rotary switch

The PCI bus connector supports communication between the SMIC and the MARC. The position of the rotary switch determines the port assignments. Although the rotary switch has 8 positions, only position 0, 1, and 2 are supported on the 4-port SMIC.

MRPC

The MRPC:

The DC/DC power card is a ruggedized, application-specific, triple-output, PC/104—Plus-compatible converter. It accepts 12-VDC or 24-VDC inputs from a vehicle battery system and provides fully protected 3.3V, 5V, and 12V outputs. The AC/DC power adapter provides a compatible DC input when not being used in a 12-VDC or 24-VDC application.

The 3200 has multiple interfaces:

- Ethernet interfaces are used to connect any in-vehicle wired clients, such as laptop, camera, or telematics devices to the network.
- Serial interfaces provide connectivity to wireless WAN modems that connect to cellular networks such as CDMA or GPRS.
- WMIC is configured as a WGB for connectivity to wireless networks.

The advantage of using MAR3200 is that it can give backup connectivity over cellular networks such as GPRS or CDMA. The wireless 802.11 connections are treated as preferred services because they offer the most bandwidth. However, when a WLAN connection is not available, cellular technology provides a backup link. Connection priority can be set by routing priority or by the priority for Mobile IP.

Cisco Support Community - Featured Conversations

Cisco Support Community is a forum for you to ask and answer questions, share suggestions, and collaborate with

your peers. Below are just some of the most recent and relevant conversations happening right now.

Related Information

- **Technical Support & Documentation - Cisco Systems**