MeshConnex Overview

HOW TO GUIDE

June 2014

Revision 1.0

Author: C04220

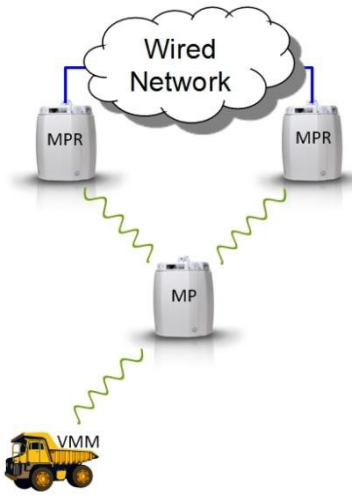
Table of Contents

1. Wireless Mesh Networking

1.1 What is a wireless mesh network?

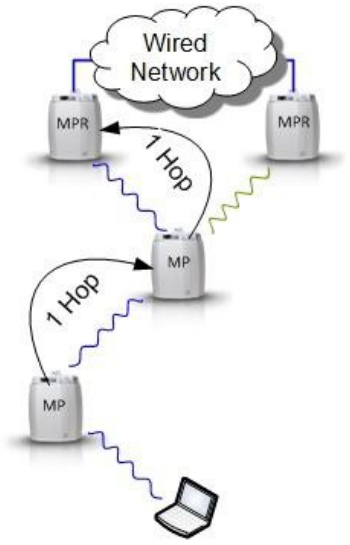
A wireless mesh network is similar to a wired internet network. Each mesh enabled access point acts as a router/repeater. A mesh network provides multihop connectivity so that traffic from one AP can be forwarded through another to reach the intended destination. This multi hopping capability eliminates the need for a dedicated wired connection to every AP. Mesh networks are also self healing such that the network will reform in the event an AP fails. This self healing characteristic can prevent single a point of failure.

In a mesh network AP's can operate in several different modes. Meshpoint Roots (MPR) are AP's that have a wired backhaul connection. Meshpoint Root AP's serve as gateway devices between the wireless network and the wired network. AP's that do not have a wired backhaul and function as repeater devices are referred to as Meshpoints (MP). Both Meshpoint Root and Meshpoint AP's provide wireless client access. The mesh network also supports mobile Meshpoints referred to as VMM's or Vehicle Mounted Modems. VMM's provide mesh connectivity while traversing throughout the wireless mesh network at vehicular speeds.



In a mesh network Meshpoints forward all traffic into the wired network through Meshpoint Roots. Meshpoints always look for the optimum path to a Meshpoint Root AP. The path between any two AP's is considered one hop. The path from any given Meshpoint to a Meshpoint Root may consist of multiple hops. It is important to note that a path with a single hop may not be better than a path with multiple hops. In a WiNG enabled mesh network,

MeshConnex or MCX automatically determines the optimum, highest performing path to each Meshpoint Root AP.

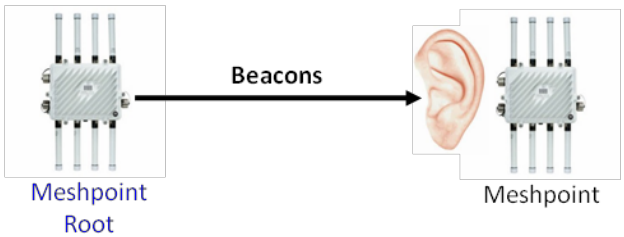


1.2 MeshConnex Overview

MeshConnex (or MCX), is the mesh network engine in WiNG. MCX provides efficient routing, low hop latency (~ 2.2ms per hop), low routing overhead, high-speed handoffs and proven scalability. MCX provides "make before break" path changes in infrastructure and mobility modes by proactively maintaining a table of alternative paths to Meshpoint Root AP's. MCX can change paths immediately if a better one becomes available. This proactive approach allows a mesh AP to make intelligent path decisions in a dynamically changing RF environment.

How Mesh Links are Formed

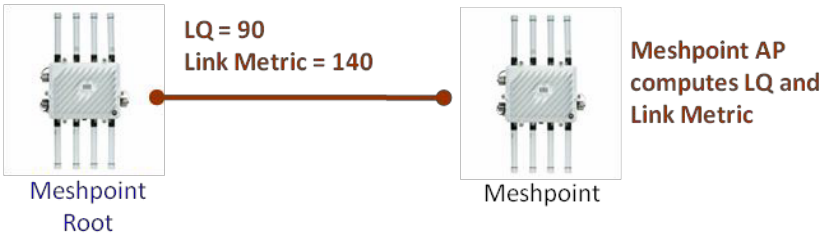
In order to create a mesh network, MCX must be enabled on each AP that will participate in the mesh. To enable MCX a "meshpoint" must be configured and assigned (mapped) to a radio interface. In a typical deployment one radio will be dedicated to mesh (e.g. 5 GHz) with a single meshpoint mapped. WiNG does supports up to (2) separate meshpoints per radio however in most cases a single radio/meshpoint is used. Once a meshpoint has been mapped to a radio interface, AP's will exchange "mesh" beacons. Beacons are used to identify mesh neighbors. Beacons from a neighboring AP's are used to compute a Link Quality and Link Metric to each neighbor.



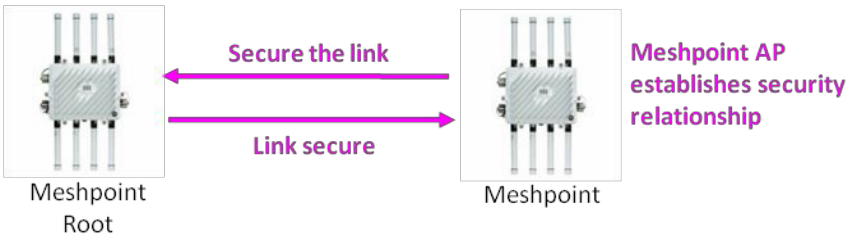
Link Quality (LQ) is defined as the measure of the probability of a packet being successfully received by the neighbor. This can be thought of as the packet completion rate or PCR. LQ is calculated for each neighbor AP and is represented by a number from 0 to 100, the higher the better. An LQ of 90-100 is considered excellent while < 60 is considered poor.

90 – 100	Excellent
80 – 90	Very Good
70 – 80	Good
60 – 70	Moderate
< 60	Poor

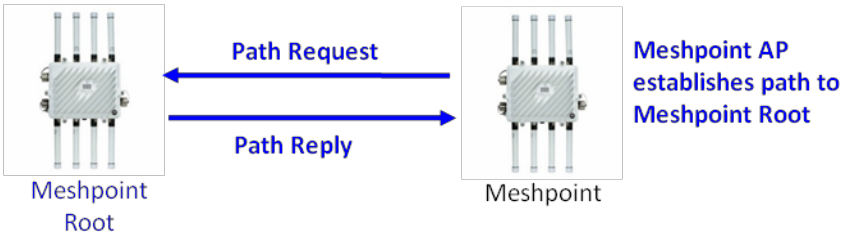
The Link Metric represents the "cost" of a specific link. It essentially describes the cost of using this link (i.e. expected time that will be taken to send a packet over this individual link). The Link Metric is represented by a number from 1 to 65535. The lower the number the better the Link Metric with 100-200 considered excellent (in general any Link Metric > 1500 is not usable with the exception of configuring preferred interfaces to be discussed later). MCX will continuously calculate the Link Metric to each neighbor. When comparing two Link Metrics between neighbors, a neighbor with 2x the metric would effectively take twice as long to transmit a packet.



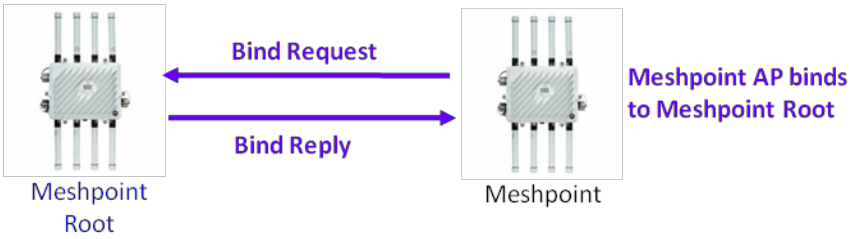
Once an AP computes a Link Quality and Link Metric to each neighbor a security relationship must be established. Open and PSK security methods are supported. If PSK security is used all traffic will be encrypted.



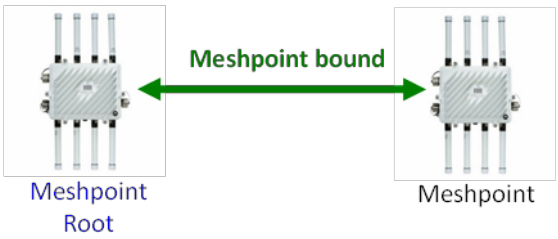
Based on the AP's computed Link Metric to each neighboring AP, along with each neighbor's path metric to their Meshpoint Root, the AP will determine the best path to a Meshpoint Root. In this example the neighbor is a Meshpoint Root, thus the Link Metric to this neighbor is equal to the Path Metric. The AP will now setup a path.



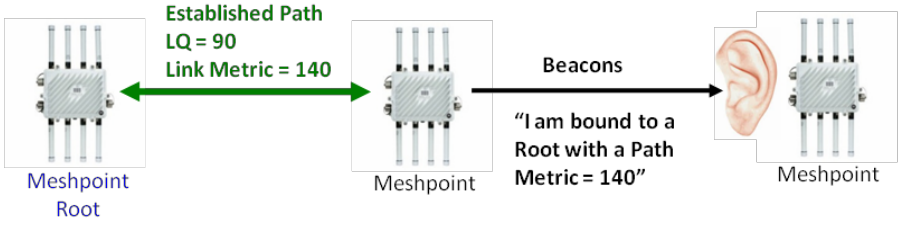
After the path has been setup the Meshpoint AP will “bind” to the Meshpoint Root. Binding essentially designates that the Meshpoint will use that specific Meshpoint Root as its gateway AP.



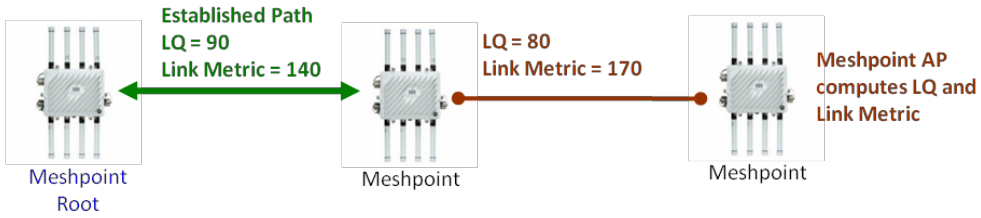
Once the binding process is complete the mesh link is fully formed and ready to use.



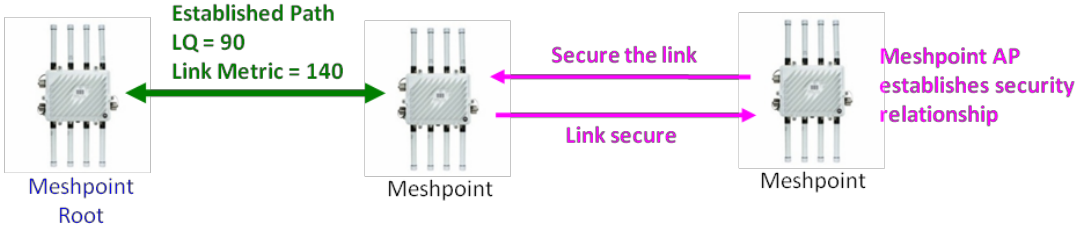
In the next example an additional Meshpoint has been added. Note that the beacon received from the Meshpoint that is already bound includes its Path Metric to the Meshpoint Root.



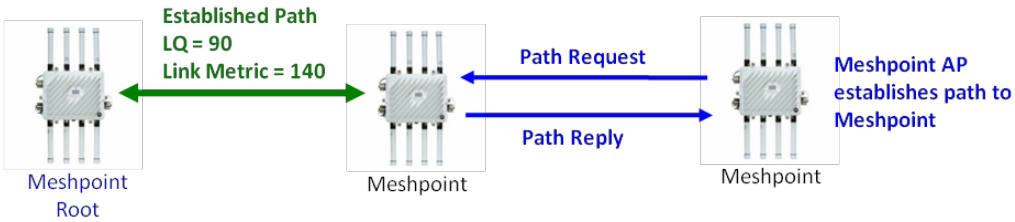
Link Quality and Link Metric are calculated.



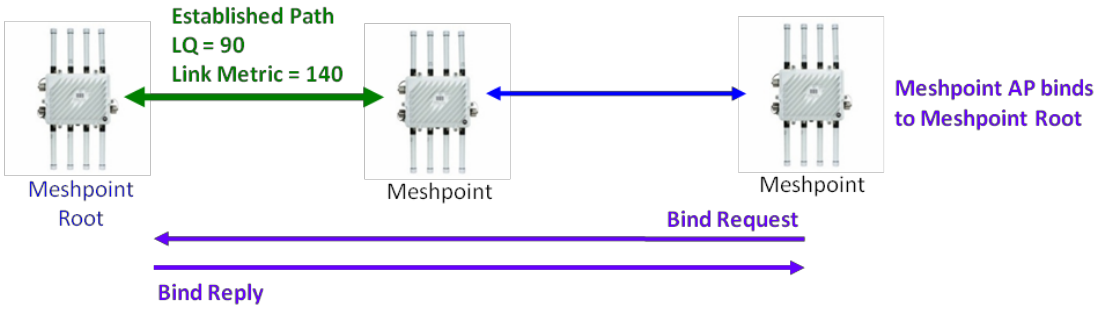
A security relationship is initiated.



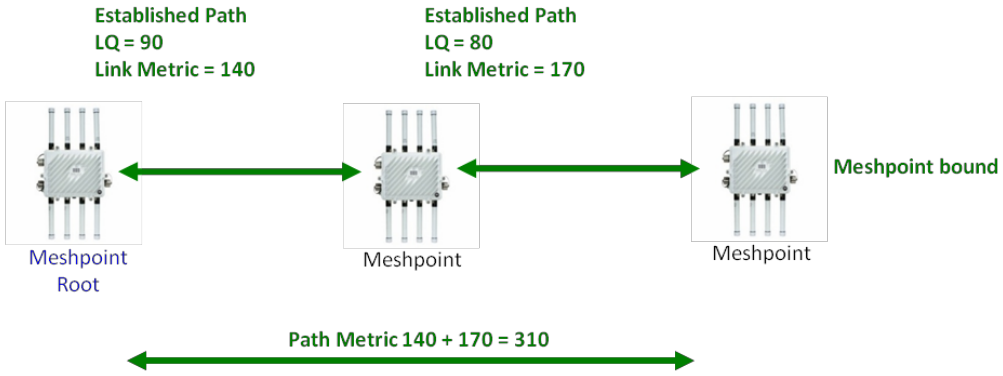
Next the AP establishes a path to the neighbor.



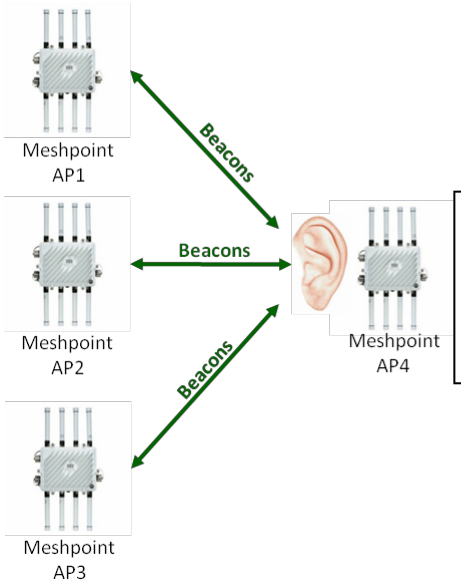
Once the path has been established the AP will send a bind request to the Meshpoint Root.



Finally a complete path to the Meshpoint Root has been established. Note that the Path Metric for the additional AP is equal to the sum of the Link Metrics along the path.



It is important to note that the Path Metric and number of hops to the current bound Meshpoint Root is included in the beacon. In the example below AP4 has three neighbors each with an existing path to a Meshpoint Root. Since AP3 has the lowest Path Metric, AP4 will bind to the Meshpoint Root AP3 is currently bound to.



AP4 Neighbor Table

	LQ	Link Metric	Path Metric	Hops to Root
AP1	84	250	1052	4
AP2	90	110	790	3
AP3	81	220	350	2

1.3 Configuration Models

When planning a mesh deployment there are three configuration models to consider. These models are largely dependent on the number of AP's in the network.

The first model is referred to as the **Standalone** model. The standalone model has no central configuration source and each AP must be configured independently. This model is often used for isolated sites with a limited number of AP's. When using mesh the MeshConnex policy must

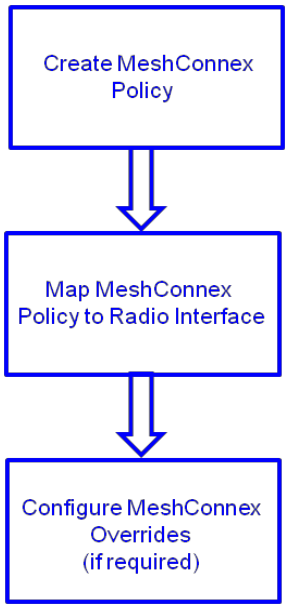
be configured on each AP individually. Any changes will require the network operator to touch each individual AP.

The next configuration model is referred to as **Virtual Controller**. In this model, one of the AP's will also act like a controller which allows basic centralized configuration. A single device profile can be configured and shared amongst all AP's. This model is used in isolated sites with less than 24 AP's. When using MCX a single MeshConnex Policy can be created and shared via the virtual controller.

The **Controller** based configuration model provides the most features and centralized configuration options. If a location has more than 24 AP's than the **Controller** based configuration model is strongly recommended. Multiple configuration profiles are supported allowing the network operator more configuration flexibility and granularity. This model is also recommended for multi site deployments which require centralized management. Multiple MeshConnex Policies and configuration profiles can be created and shared.

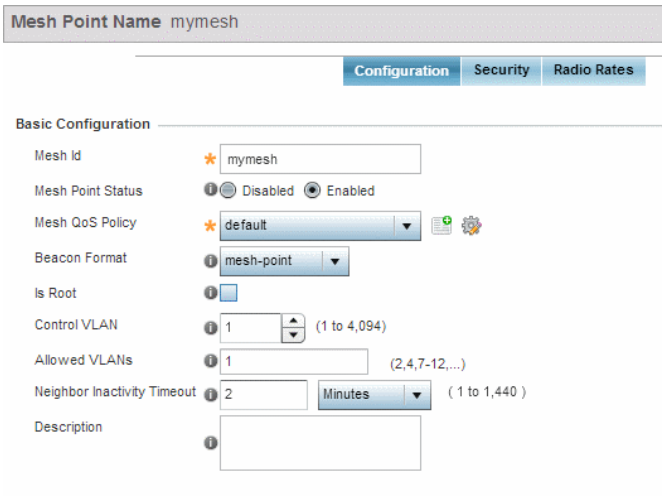
1.4 MeshConnex Configuration

To setup a basic mesh there are three areas to consider. First a MeshConnex Policy must be created. The MeshConnex Policy will contain all of the specific mesh configuration items and security credentials required for AP's to form mesh links. Next, this policy must be applied or "mapped" to a radio interface e.g. the 5 GHz radio. This should be done in the AP's device profile. Finally, any specific Meshpoint device overrides should be added if required (*Note: detailed configuration steps are covered in the MeshConnex How To March/2014*)



1.4.1 MeshConnex Policy

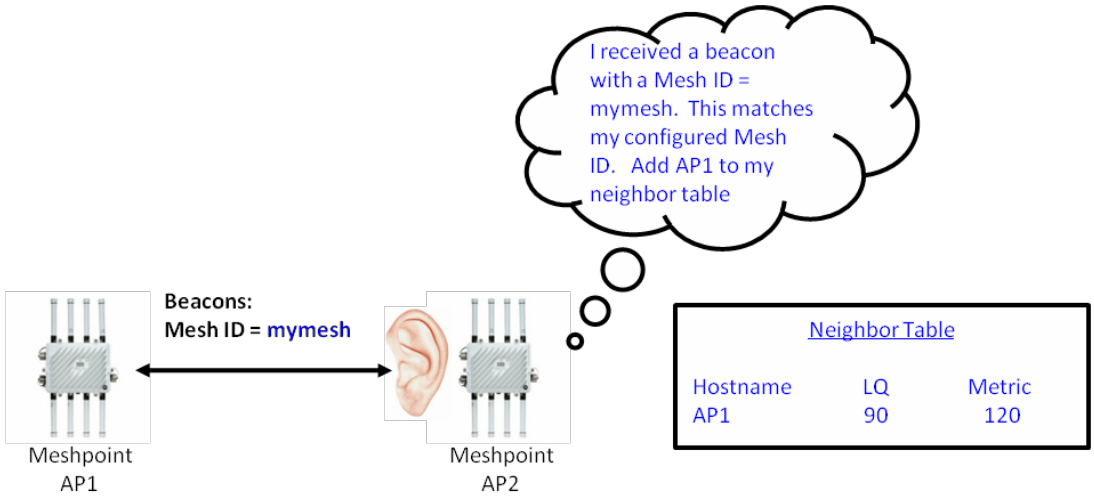
In order for AP's to mesh a meshpoint must be configured. In WiNG this is done in the MeshConnex Policy.



The following key configuration items include the following:

1.4.1.1 Mesh ID

The Mesh ID is an identifier used to delineate different mesh networks. AP's must have the same Mesh ID in order to form mesh links. When a MeshConnex policy is configured and mapped to a radio interface the AP will send out "mesh" beacons which are used to build the meshpoint neighbor table. When AP's have meshpoints configured they exchange beacons and the Mesh ID is checked. If an AP receives a mesh beacon and the Mesh ID does not match its own configured Mesh ID, the beacon is dropped. If the Mesh ID matches then the AP will add an entry for the neighbor in table called the meshpoint neighbor table.



1.4.1.2 Beacon Format

There are two beacon format choices available when configuring the MCX.

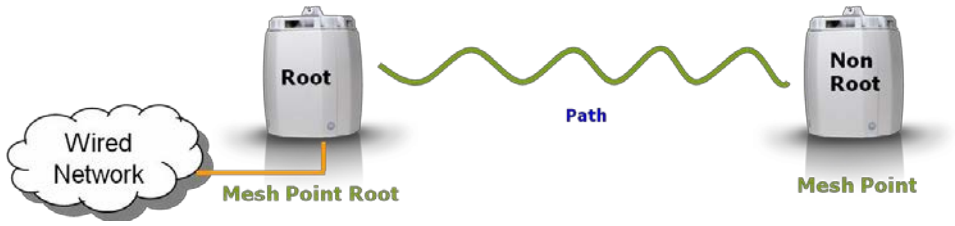
Mesh Point Mode – This format is the 802.11s compliant beacon method. This is the preferred format to use except when interoperating with legacy mesh products such as MotoMesh Duo. Also note that when using this beacon method the mesh point bss will not appear on a wireless client utility. This is preferable as the mesh bss is hidden from standard wireless clients

Access Point Mode – When this beacon format is used the AP bit is turned on in the beacon. This format should be used when interoperating with the legacy MotoMesh Duo product. Note that when this beacon format is used the mesh bss will appear on a wireless client utility.

Note that different beacon formats will not mesh.

1.4.1.3 Root / Non Root Setting

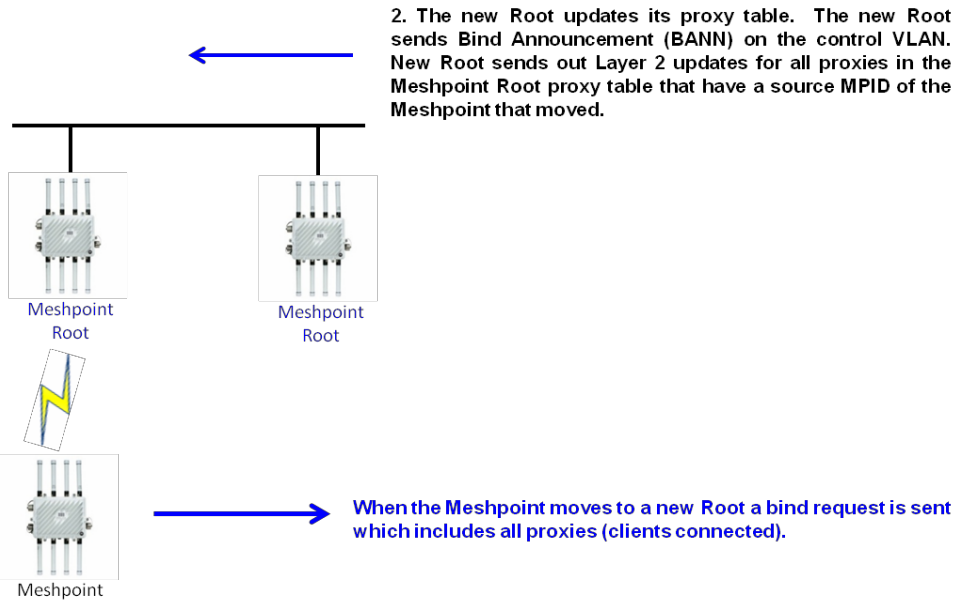
An AP configured with a meshpoint can either be designated as a Root or Non Root AP. Root AP's will have a wired backhaul connected and are considered gateway devices between the wired and wireless network. They are referred to as "Meshpoint Root" AP's. Mesh AP's that do not have a backhaul connection are simply referred to as "Meshpoints". A VMM is a meshpoint with additional settings and will be discussed later.



While the Root setting can be configured in the MeshConnex policy it is a best practice to define whether or not an AP is Root via a profile, device override, or enabling the backhaul detection feature. Thus the MeshConnex policy should not have the Root designation configured.

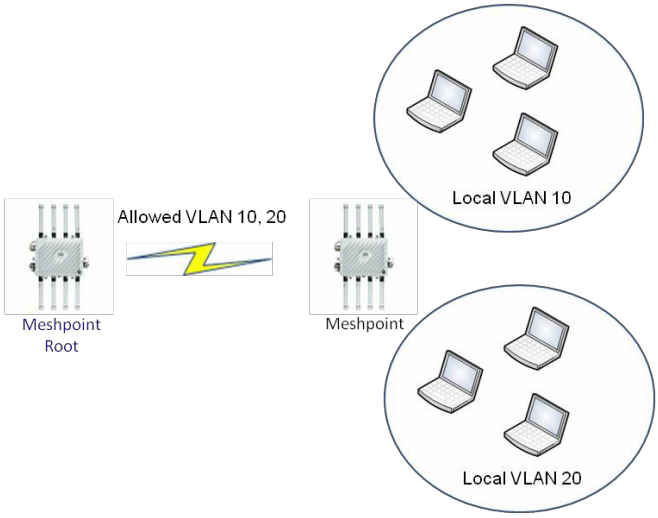
1.4.1.4 Control VLAN

The control VLAN in the MeshConnex policy configuration is used to facilitate Root to Root communication for handoffs. Thus this VLAN only has significance for Meshpoint Roots. When a Meshpoint AP, wireless client, or VMM moves from under one Root to another a bind announcement (BANN) is sent on control VLAN to alert the wired infrastructure and other MeshPoint Roots that the MAC address of a Meshpoint, client devices, or VMM has moved. Also, Layer 2 updates are sent on any VLAN configured on the device that has moved. These broadcast Layer 2 updates ensure that all Roots and Core infrastructure is aware that all client MAC's being proxied by the AP that has moved is aware of the change.



1.4.1.5 Allowed VLAN

VLAN tagged traffic is supported across the mesh network. The allowed VLANs field in the MeshConnex policy is used to define which VLANs are allowed to pass traffic on the mesh. VLANs added to the allowed VLANs field are used for local VLANs (e.g. non MiNT tunneled VLANs). Thus any VLAN tagged traffic from an AP (WLAN or via Ethernet) will be allowed to cross the mesh (non-tunneled) as long as the VLAN is included in the allow VLAN field in the MeshConnex policy configuration.



1.4.1.6 Neighbor Idle Timeout

The neighbor idle timeout is the amount of time that must pass in which no traffic is received from a neighbor before it is declared offline. This is typically set to a low value such as 1-2 minutes such that a non functioning neighbor will have a minimum impact on the mesh network. If a neighboring AP stops sending beacons this timeout will ensure that the neighbor will be removed from the meshpoint neighbor table.

1.4.1.7 Security Settings

Security used by the mesh is configured in the MeshConnex policy. There are two supported security methods:

Open Mode
The open security method involves a simple 2-way handshake. The exchange is as follows:
AP1 → I want to use open security → AP2
AP2 → Ok, use open security → AP2

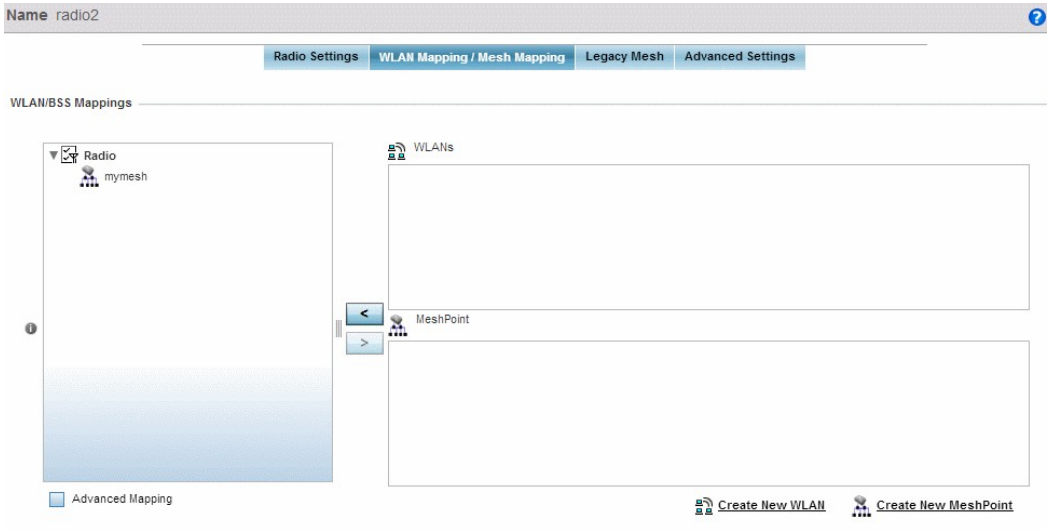
PSK Mode
The PSK security method involves multiple handshakes. The exchange is as follows:
AP1 → I want to use psk security → AP2
AP2 → Ok, use psk security → AP2
AP1 → Standard 4-way from 802.11i → AP2

The AP will establish a security session with each neighbor and add an entry for each neighbor in a table called the meshpoint security table.

```
AP7161.AP1(config-meshpoint-Mesh)#?
Mesh Point Mode commands:
allowed-vlans          Set the allowed VLANs
beacon-format          The beacon format of this meshpoint
control-vlan           VLAN for meshpoint control traffic
data-rates             Specify the 802.11 rates to be supported on this meshpoint
description            Configure a description of the usage of this meshpoint
meshid                 Configure the Service Set Identifier for this meshpoint
neighbor               Configure neighbor specific parameters
no                     Negate a command or set its defaults
root                   Set this meshpoint as root
security-mode          The security mode of this meshpoint
shutdown               Shutdown this meshpoint
use                    Set setting to use
wpa2                   Modify ccmp wpa2 related parameters
clrscr                 Clears the display screen
commit                 Commit all changes made in this session
do                     Run commands from Exec mode
end                    End current mode and change to EXEC mode
exit                   End current mode and down to previous mode
help                   Description of the interactive help system
revert                 Revert changes
service                Service Commands
show                   Show running system information
```

1.4.2 Mapping the MeshPoint

After a Meshpoint has been created it must be mapped to a radio interface. This should be done via the AP device profile. The Meshpoint is mapped in the same manner as a WLAN in WiNG. In a typical deployment one radio is usually dedicated for meshing.



AP7161.AP1(config-profile-outdoor-if-radio-2)#meshpoint mymesh bss 1

1.4.3 MeshConnex Overrides

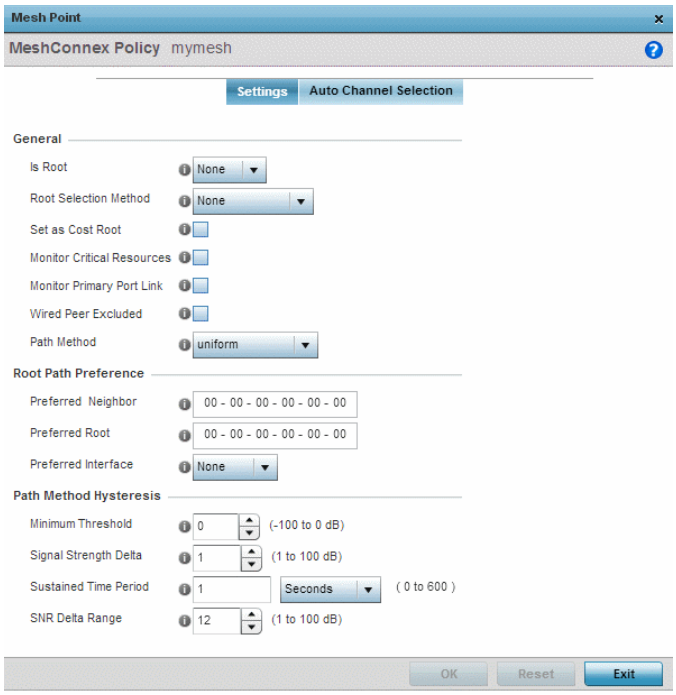
Next overrides need to be considered. For example, if an AP is going to a Meshpoint Root i.e. it will be connected to the wired network it needs to be designated as a Root AP. There are several options available to accomplish this. For a small network with standalone AP's this can be done via a device override. On the device itself the Root option would be configured. For controller based networks multiple device profiles can be used. For example a device profile for only Root AP's can be created with the Root option configured in the meshpoint settings. Another method would be to use a single AP profile with backhaul detection configured. Then, in the MeshConnex policy, the Is Root option can be checked. If a device using this profile does not detect a backhaul connection then it will convert itself from a Meshpoint Root to a Meshpoint (Non Root). CRM is discussed in a later section.

1.4.3.1 Path Method

Another override to consider is the path method. For regular infrastructure meshing the path method of ***uniform*** should be used. If a VMM is being used then the path method should be set to ***mobile-snr-leaf*** (discussed in MeshConnex and Mobility). The path method of ***snr-leaf*** is used for special infrastructure cases in it is more desirable to make path decisions based on snr then metric based. ***Bound pair*** should only be used for rail deployments and is discussed in Dynamic MeshConnex section.

- **none**
    - Same as uniform

- **uniform**
  - Normal PCR metric routing
- **mobile-snr-leaf**
  - SnR based routing
  - Turns on mobility bit
  - Turns on leaf bit (leaf AP's cannot hop through each other)
  - Uses SnR in auto channel selection
- **snr-leaf**
  - SnR based routing
  - Turns on leaf bit (leaf AP's cannot hop through each other)
  - Uses SnR in auto channel selection
- **boun l pair**
  - Used in rail deployments
  - Turns on bound pair mode




```
AP7161.AP1(config-device-5C-0E-8B-6D-B4-E4-meshpoint-Mesh)#?
Mesh Point Device Mode commands:
acs             Configure auto channel selection parameters
exclude         Exclude neighboring Mesh Devices
hysteresis      Configure path selection SNR hysteresis values
monitor         Event Monitoring
no              Negate a command or set its defaults
path-method     Path selection method used to find a root node
preferred       Configure preferred path parameters
```

root	Set this meshpoint as root
root-select	Root selection method parameters
clrscr	Clears the display screen
commit	Commit all changes made in this session
do	Run commands from Exec mode
end	End current mode and change to EXEC mode
exit	End current mode and down to previous mode
help	Description of the interactive help system
revert	Revert changes
service	Service Commands
show	Show running system information

1.4.3.2 Preferred Settings

With MeshConnex, the mesh network is self forming and self healing. MeshConnex automatically optimizes the network without user intervention. However, there may be times in which the network operator might feel it necessary to influence how the mesh network behaviors. For instance there may be a situation in which multiple paths have equivalent link metrics which might result in frequent path changes. Setting a preferred neighbor in the meshpoint configuration settings can help stabilize this.

Preferred Neighbor
In the device configuration tree under **Mesh Point** the user has the ability to specify a preferred neighbor. This setting can be used to bias a device using MCX mesh to utilize a specific neighbor when sending traffic. For example suppose a Non Root AP has multiple neighbors each with a path back to a Root AP. If for some reason the user determines that the chosen neighbor / path back to the Root needs to be changed a preferred neighbor can be configured. To configure a preferred neighbor the user would enter in the IFID (Interface ID) of the neighbor's mesh radio into the preferred neighbor field.

The network operator also has the ability to influence which Meshpoint Root AP a particular Meshpoint uses. This can be helpful when trying to balance the number of Meshpoints under a Meshpoint Root when the number of AP's in a network for minimal and Meshpoint AP's are all binding under the same Meshpoint Root. This is done by using the preferred Root setting.

Preferred Root
In the device configuration tree under **Mesh Point** the user has the ability to specify a preferred Root. This setting can be used to bias a device using MCX mesh to utilize a specific Root AP. The user may configure this setting if they determine that a Non Root device should utilize a specific root. This is often used in a linear deployment to help influence Root selection. To configure a preferred Root the user would enter in the MPID of the Root's mesh radio into the preferred Root field.
When running mesh on multiple radios on the same AP MeshConnex will automatically send traffic over the radio that has the best path back to a Meshpoint Root. However, the network operator has the ability to set a preferred radio interface biasing which mesh will be actively forwarding traffic. This is done using the preferred interface.

Preferred Interface
In the device configuration tree under **Mesh Point** the user also has the ability to specify a preferred interface. This is often used when the AP is configured with MCX on multiple radios and the user would like to prioritize which radio is used for mesh.

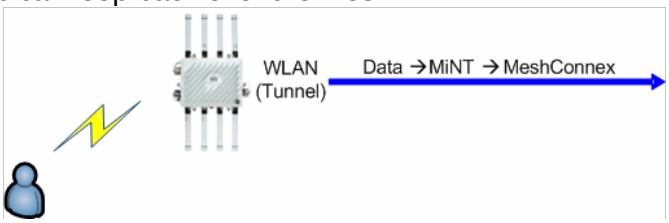
2. MeshConnex Miscellaneous

2.1 VLANs and MeshConnex

VLANs are supported across the mesh network. VLANs can be extended (i.e. tunneled over MiNT), local, or a combination of the two.

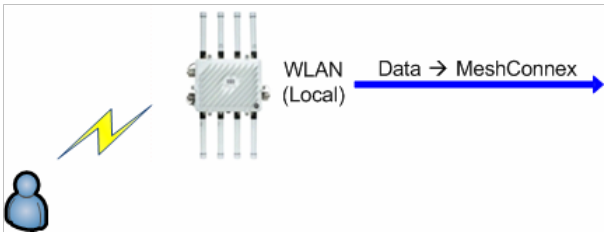
2.1.1 Extended VLANs

Configuring a WLAN with the bridging mode set to tunnel client data will be VLAN tagged and encapsulated inside of MiNT. This is referred to as an extended VLAN. This traffic is then sent over MeshConnex and forwarded to the controller. Thus client data is VLAN tagged, encapsulated in MiNT, and then encapsulated in MeshConnex. The Meshpoint Root AP will remove the MeshConnex header and forward the VLAN encapsulated MiNT traffic to the controller. When a WLAN using a tunneled VLAN is mapped to a mesh AP it is important to ensure that the VLAN is NOT configured in the MeshConnex Policy allowed VLAN list. Otherwise tunnel traffic can loop back over the mesh.



2.1.2 Local VLANs

Configuring a WLAN with the bridging mode set to local will not encapsulate VLAN tagged traffic inside of MiNT. In this method the wireless controller is removed from the data path. Client data is VLAN tagged and encapsulated directly in MeshConnex. The Meshpoint Root AP will remove the MeshConnex header and forward the to the wired network infrastructure for handling. Local VLANs must be configured in the MeshConnex Policy allowed VLAN list. Otherwise these VLANs will not be able to cross the mesh network.



2.1.3 MCX Control VLAN

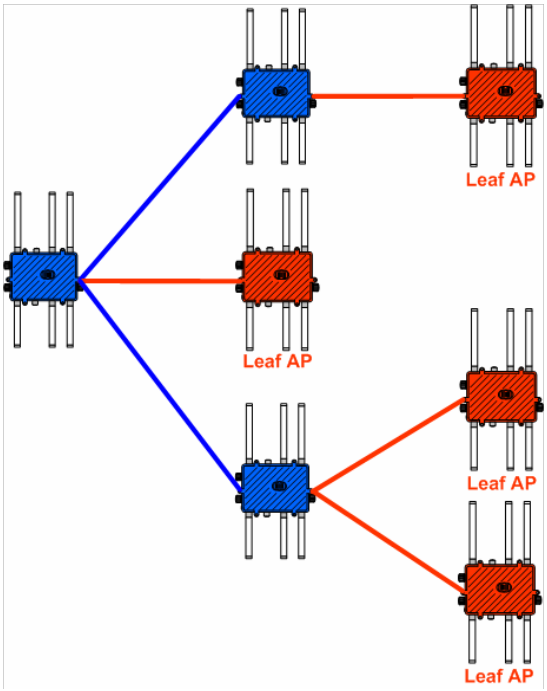
The control VLAN in the MeshConnex policy configuration is used to facilitate Root to Root communication for handoffs. Thus this VLAN only has significance for Meshpoint Roots. This VLAN is MCX specific and is not to be confused with any other control VLAN. When a Meshpoint AP, wireless client, or VMM moves from under one Root to another a bind announcement (BANN) is sent on control VLAN to alert the wired infrastructure and other MeshPoint Roots that the MAC address of a Meshpoint, client devices, or VMM has moved.

Also, Layer 2 updates are sent on any VLAN configured on the device that has moved. These broadcast Layer 2 updates ensure that all Roots and Core infrastructure is aware that all client MAC's being proxied by the AP that has moved is aware of the change. The control VLAN must not be the same as any tunneled VLAN.

2.2 MeshConnex and Mobility

MeshConnex supports mobile meshing enabling vehicles of all types' secure and reliable wireless broadband connectivity at high speed. Mobile access points can be used for connectivity to the Internet, offloading DVR content, live streaming video, database access and other high bandwidth applications. Bus systems, rail, public safety, and mining operations are ideal candidates for mobile meshing. MeshConnex enables mobility features when an AP is operating as a Vehicle Mounted Modem or VMM.

In an infrastructure only mesh deployment, AP's are usually configured with the "uniform" path method. The uniform path method allows Meshpoint AP's to hop through one another when finding a path to a Meshpoint Root AP. When an AP is operating in VMM mode all AP's are considered leaf nodes i.e. they cannot hop through one another. Thus one VMM cannot hop through another VMM to reach a Meshpoint Root AP. This enhances performance and facilitates high speed handoffs. The path method "snr-leaf" should be configured on all VMM's.



Also, snr-leaf mode changes path decisions from metric based to SnR based. Thus the next hop path with the strongest SnR will also be chosen. In a mobile scenario AP's are not in any one position long enough for metrics to settle thus the reason why decisions are based on SnR.

If vehicular speed is greater than 30mph A-MPDU aggregation should be disabled. Testing has shown higher throughput performance since in a mobile scenario packet loss is to be expected, and the loss of aggregated packet is very costly in terms of overall throughput.

VMM Configuration Guides

For additional configuration detail on VMM the following guides are available:

- **WiNG How To Vehicle Mounted Modem**
- **MeshConnex Best Practices VMM**
- **MeshConnex and VMM Best Practices in Mining Environments**

2.3 Backhaul Detection Feature

Meshpoint Root AP's are the gateway devices between the wireless and wired network. MCX backhaul detection monitors the backhaul connection and takes appropriate steps in the event the wired backhaul is disrupted. If a Meshpoint Root AP's backhaul fails, without backhaul detection, the Meshpoint Root AP will continue to advertise that it is Root AP. All meshpoints under the affected Root will remain bound and will continue to forward traffic to the MeshPoint Root.

With backhaul detection enabled, Meshpoint Root AP's that experience a backhaul failure will stop advertising themselves as Root. They will also covert from a Meshpoint Root AP to Meshpoint AP.

Configuration options for backhaul-state monitoring include:

Physical connectivity - utilizes the primary port link loss detection

Logical connectivity - utilizes the Critical Resource Monitoring (CRM) feature

Backhaul state changes trigger corresponding notification events that MCX will act upon accordingly and automatically without user intervention as shown in the table below:

	MCX Backhaul Detection Disabled		MCX Backhaul Detection Enabled	
MP Configured as:	**Root**	**Non-Root**	**Root**	**Non-Root**
Backhaul up	Root	Non-Root	Root	Non-Root
Backhaul down	Root	Non-Root	Non-Root	Non-Root

CRM

Allows a critical resource (an IP address of a gateway or critical server) to be monitored.

Employs ARPs

- Default source IP address of 0.0.0.0. Can be modified with a service command
- Must be limited to a specific VLAN and a physical port

- Bound to the port MAC not the switch MAC to ensure the packets are always bridged back to the port and removing the possibility they will be bridged over the mesh
- Allows for a single rule with multiple targets to be installed
- Allows for multiple rules to be installed

Loop Prevention

- Redundant links may be created causing a copy of the same packet to be sent over multiple paths and hence a bridging loop when either of the following occurs:
    - A logical connection failure (critical resource down)
    - A physical connection failure, a root changing to non root, then the connection is restored
- To prevent loops, MCX on a converted Meshpoint (root acting as non-root) limits ingress and egress traffic on its wired ports to the CRM traffic only
- Loop prevention is scaled down to limited loop prevention if all the non-root CRM monitoring mesh points have no path to a root. Limited loop prevention allows packets in from the wired ports, but only allows packets from the AP itself out. This allows administrative access to the AP even if both CRM and mesh are down.

MCX backhaul detection is disabled by default and must be enabled in order for MCX to react to backhaul state changes

2.4 MeshConnex and Automatic Channel Selection

In release WiNG 5.5.0 and beyond, Smart-RF is no longer used for meshpoint scanning (however Smart-RF is still used for WLAN's). MeshConnex Auto Channel Selection MCX-ACS is now used. As expected the AP country code will determine which channels will be available for scanning. Unlike Smart-RF the channel list to be scanned by MCX-ACS is located under the RF Domain. In the GUI this is listed as "Smart Scan". Unlike Smart-RF there is no dynamic power control in MCX-ACS. Power will default to max (if no power value has been configured). Setting a radio with a MeshPoint mapped to "smart" will enable MCX-ACS.

When using MCX-ACS channel list authority is located under the RF Domain settings and is enabled by the "***channel-list dynamic***" command. Channel lists can be defined for both 2.4GHz and 5GHz meshing.

rf-domain default
country code us
channel-list dynamic
channel-list 5GHz 149,153,157,161,165

2.4.1 MeshPoint Root MCX-ACS Scan Types

Startup Scan

This scan is performed when a configuration change is made to the channel list, meshpoint, and or radio (also when the AP is powered up and MCX-ACS has already been configured). This type of scan is intrusive and will break existing mesh links.

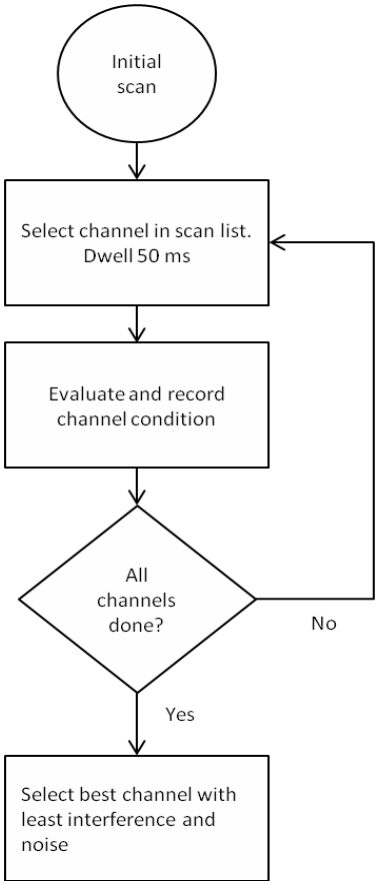
On Demand Scan
This “background” scan is done to monitor changes to channel conditions and is performed at an interval define in the ACS configuration. This type of scan is NOT intrusive and will NOT break existing mesh links.

2.4.1.1 MeshPoint Root Startup Scan

This scan can be triggered by:

- AP is powered up (MCX-ACS has already been configured)
- A change to the configured channel list (add/remove channels)
- Disable/enable radio
- A change to the RF-mode (2.4GHz/5GHz)
- A change in radio placement (indoor/outdoor)
- A change in the MeshPoint configuration

This scan uses a default dwell time of 50ms and channels are sampled in succession without delay and the channel with the least amount of interference is chosen. After the channel is selected the configured channel hold down timer is started.

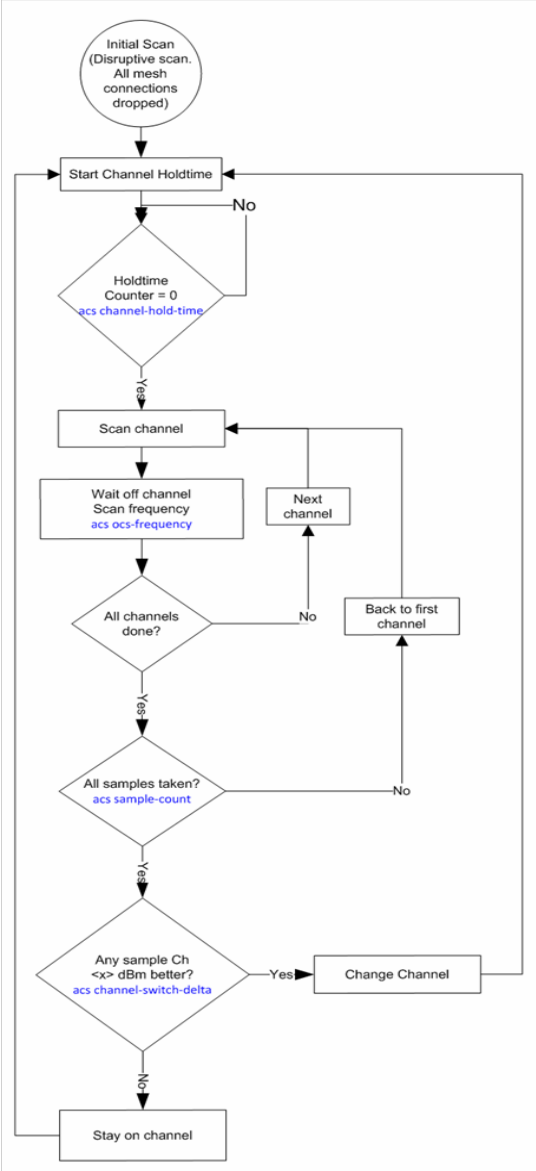


2.4.1.2 MeshPoint Root On Demand Scans

Once the initial triggered “startup” scan is complete the AP will periodically on demand scan to evaluate channel conditions. This on demand scan will not break existing mesh links. The AP will wait a channel hold period before starting on demand scans. The default period is 30 minutes.

Example 5.x configuration

acs channel-width 5GHz auto
acs priority-meshpoint 5GHz somewhere
acs ocs-duration 5GHz 50
acs ocs-frequency 5GHz 6
acs sample-count 5GHz 5
acs channel-hold-time 5GHz 1800
acs channel-switch-delta 5GHz 10



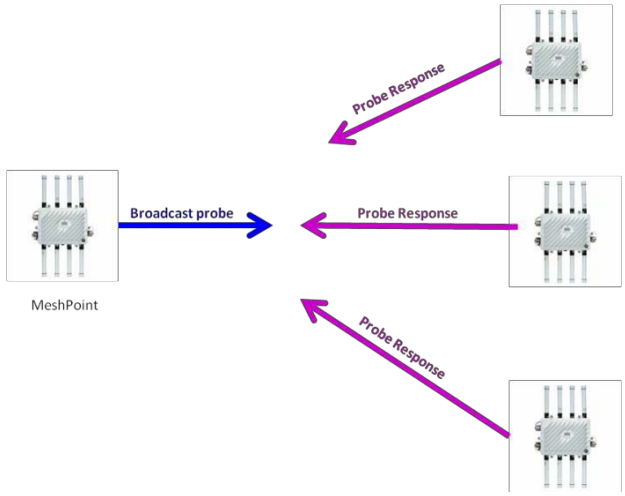
2.4.2 MeshPoint MCX-ACS Scan Types

The following MCX-ACS commands are applicable when configuring ACS on a MeshPoint (Non Root).

acs channel-width <2.4GHz/5GHz> <20MHz/40MHz/auto> (default auto)
acs priority-meshpoint <2.4GHz/5GHz> <MP name>
acs path-min <2.4GHz/5GHz> <100-20000> (default 1000)
acs path-threshold <2.4GHz/5GHz> <800-65535> (default 1500)
acs tolerance-period <2.4GHz/5GHz> <10-600> (default 60 seconds)

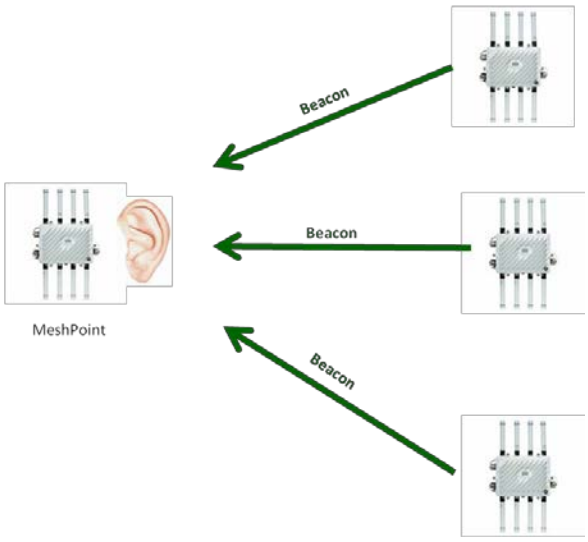
2.4.2.1 MeshPoint Active Scan

MeshPoints use a special active scan to speed up the mesh convergence time. When scanning, a MeshPoint will send a broadcast probe. If a surrounding like configured MeshPoint hears this probe, it will respond with a special directed response. Dwell time on each channel is 120ms. This response is used by the sender to compute a "mesh score".



2.4.2.2 Meshpoint Passive Scan (DFS channels)

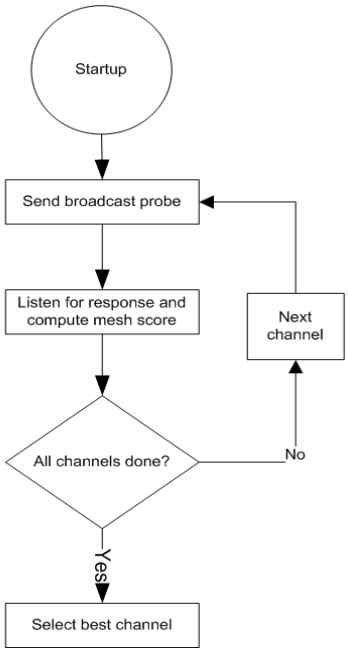
When operating on DFS channels active scanning cannot be used (since active transmissions are not permitted on DFS channels). Instead, a triggered scan with a dwell period of 300ms. During this dwell period the MeshPoint will listen for beacons to determine mesh score and interference levels.



2.4.2.3 Meshpoint MCX-ACS Scan Triggers

Initial Startup /Configuration Change

An active scan is performed (non DFS channels) when a configuration change is made to the channel list, meshpoint, and or radio (also when the AP is powered up and MCX-ACS has already been configured.



Sample Debug

Feb 04 10:25:11 2014: DOT11: meshpoint:rd[1] ACS state scanning channel 149
Feb 04 10:25:11 2014: DOT11: meshpoint:rd[1] **ACS sending mcx probe on channel 149**
Feb 04 10:25:11 2014: DOT11: meshpoint:ACS noise floor on channel 149 is -92
Feb 04 10:25:11 2014: DOT11: meshpoint:rd[1] ACS state scanning channel 153
Feb 04 10:25:11 2014: DOT11: meshpoint:rd[1] **ACS sending mcx probe on channel 153**
Feb 04 10:25:11 2014: DOT11: meshpoint:ACS noise floor on channel 153 is -90

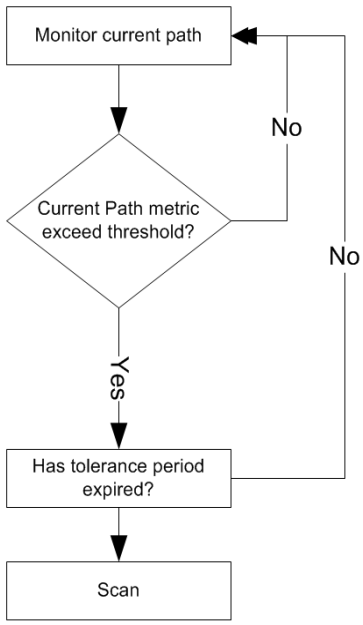
Feb 04 10:25:11 2014: DOT11: meshpoint:rd[1] ACS state scanning channel 157
Feb 04 10:25:11 2014: DOT11: meshpoint:rd[1] **ACS sending mcx probe on channel 157**
Feb 04 10:25:11 2014: DOT11: meshpoint:ACS noise floor on channel 157 is -97
Feb 04 10:25:11 2014: DOT11: meshpoint:rd[1] ACS chan list done,position 3 max-chan 3

Path Degradation

An active scan is performed (non DFS channels) when the current root path metric stays degraded past the configured threshold.

acs path-threshold 5GHz 1500
Default is 1500 milliseconds

acs tolerance-period 5GHz 60
Default is 1 minute



The following debug output shows how a MeshPoint continuously monitors the current path. If the current path metric exceeds the configured threshold an active scan will be triggered.

Sample Debug

Feb 04 10:08:53 2014: DOT11: meshpoint:rd[1] rssi=-79(-63) **score=197** root_hops=1 last_heard_ms=8 nexthop[1]:5C-0E-8B-6D-8F-90
Feb 04 10:08:58 2014: DOT11: meshpoint:rd[1] rssi=-79(-63) **score=197** root_hops=1 last_heard_ms=96 nexthop[1]:5C-0E-8B-6D-8F-90
Feb 04 10:09:03 2014: DOT11: meshpoint:rd[1] rssi=-79(-63) **score=196** root_hops=1 last_heard_ms=80 nexthop[1]:5C-0E-8B-6D-8F-90
Feb 04 10:09:08 2014: DOT11: meshpoint:rd[1] rssi=-79(-63) **score=196** root_hops=1 last_heard_ms=68 nexthop[1]:5C-0E-8B-6D-8F-90
Feb 04 10:09:13 2014: DOT11: meshpoint:rd[1] rssi=-79(-63) **score=196** root_hops=1 last_heard_ms=52 nexthop[1]:5C-0E-8B-6D-8F-90
Feb 04 10:09:18 2014: DOT11: meshpoint:rd[1] rssi=-79(-63) **score=196** root_hops=1 last_heard_ms=36 nexthop[1]:5C-0E-8B-6D-8F-90
Feb 04 10:09:23 2014: DOT11: meshpoint:rd[1] rssi=-79(-63) **score=196** root_hops=1 last_heard_ms=24 nexthop[1]:5C-0E-8B-6D-8F-90
Feb 04 10:09:28 2014: DOT11: meshpoint:rd[1] rssi=-79(-63) **score=195** root_hops=1 last_heard_ms=4 nexthop[1]:5C-0E-8B-6D-8F-90)
Feb 04 10:09:33 2014: DOT11: meshpoint:rd[1] rssi=-79(-63) **score=195** root_hops=1 last_heard_ms=92 nexthop[1]:5C-0E-8B-6D-8F-90
Feb 04 10:09:38 2014: DOT11: meshpoint:rd[1] rssi=-80(-63) **score=195** root_hops=1 last_heard_ms=76 nexthop[1]:5C-0E-8B-6D-8F-90

Minimum Path Setting

There is also a minimum path metric configuration item that is used during the channel selection process. When a scan evaluates channels looking for the best path back to a MeshPoint Root it will also consider a minimum metric when making this decision. If the minimum is not met the channel / path will not be considered.

acs path-min <2.4GHz/5GHz> <100-20000>
Default is 1000

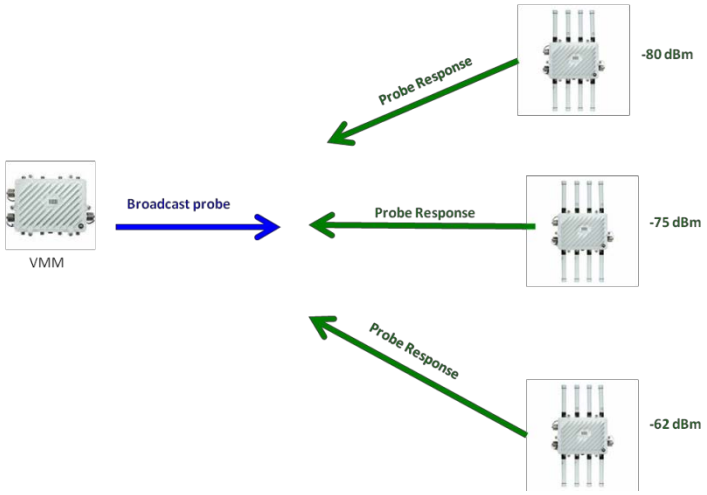
2.4.3 VMM ACS Configuration Parameters

The following MCX-ACS commands are applicable when configuring ACS on a VMM:

acs channel-width <2.4GHz/5GHz> <20MHz/40MHz/auto> (default auto)
acs priority-meshpoint <2.4GHz/5GHz> <MP name>
acs snr-delta 5GHz 5 <2.4GHz/5GHz> <1-100 dBm> (default 5)
acs signal-threshold 5GHz -65 <2.4GHz/5GHz> <-100 -0 dBm> (default -65)

2.4.3.1 VMM ACS Single Radio

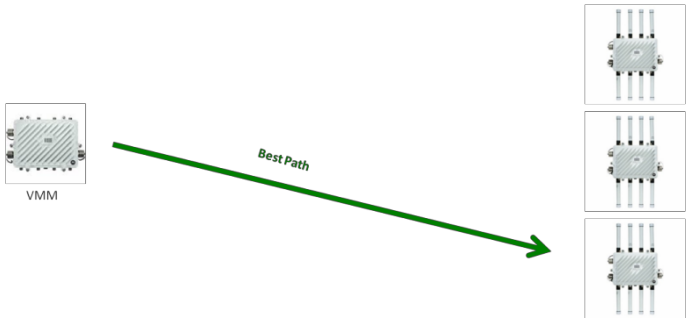
VMMs are “mobile” meshpoints that use the signal strength of nearby meshpoints to determine channel and path selection. Just like a regular MeshPoint active scan a broadcast probe is used to look for potential next hop candidates. The channel dwell time is 50ms on non DFS channels and 120ms on DFS channels.



The channel selected is based on the next hop with the strongest signal strength. If the VMM currently has no next hop then the next hop found via broadcast probing with the strongest signal level will be chosen. If the VMM has an active next hop, then a potential candidate next hop found via broadcast probing will only be selected if its signal strength is greater than the existing next hop by a configured delta value.

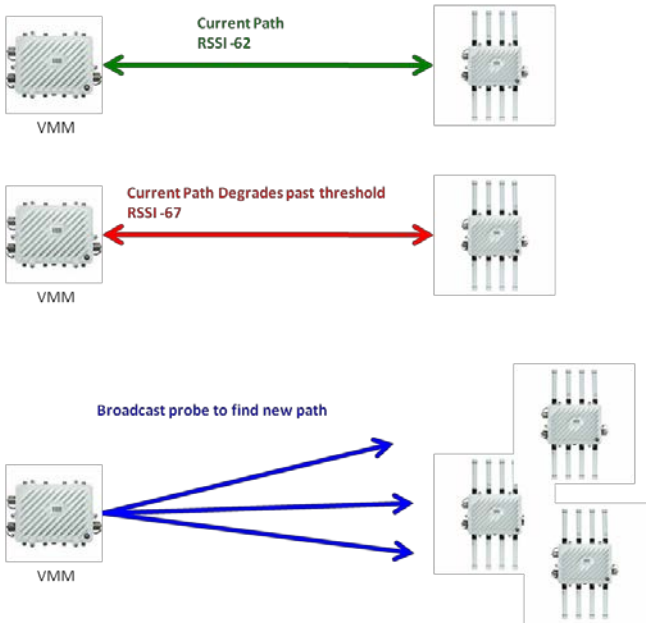
acs snr-delta <2.4GHz/5GHz> <1-100 dBm> (default 5)

Example:
In the example below, the VMM was just powered on and had no existing next hop. Therefore after performing the active scan via the broadcast probe, the next hop with the strongest signal level was chosen.

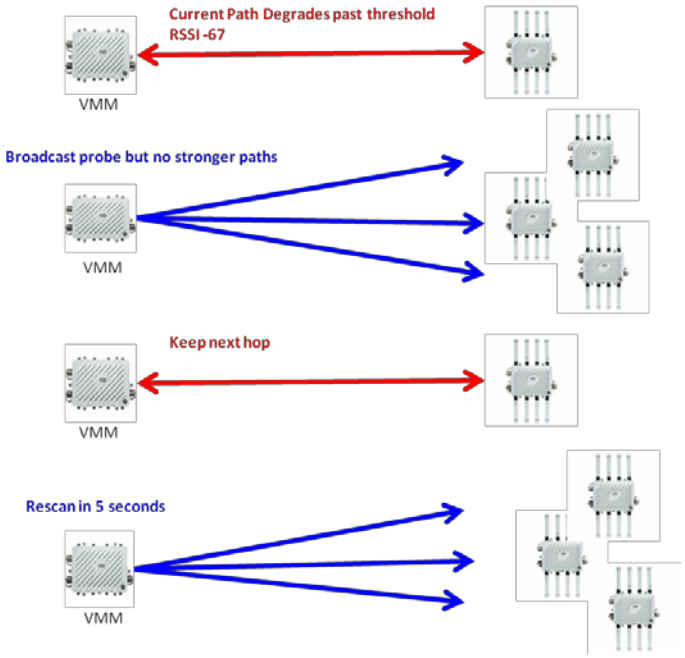


If the signal strength of the current next hop drops below the configured threshold, or a beacon from the current next hop is not received after one second a scan will be performed.

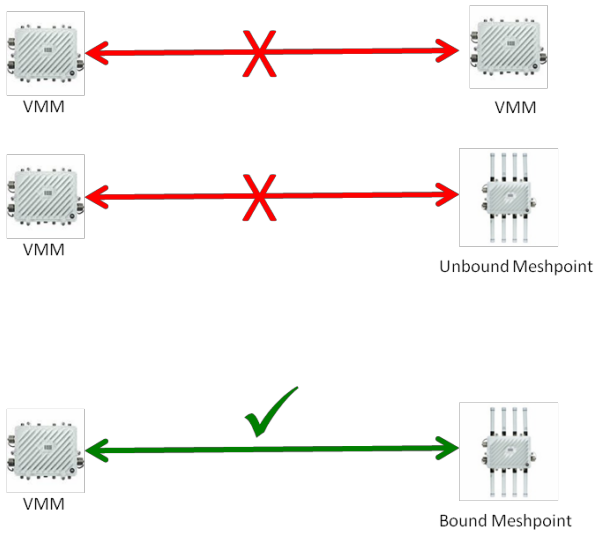
Example:
The signal threshold has been configured as -65 dBm.
acs signal-threshold 5GHz **-65**



Note that if the current next hop path degrades below the configured threshold AND if after a scan using broadcast probes does not yield a better candidate, the current degraded next hop will be kept and the scanning process will repeat. However the rescan interval is limited to every 5 seconds.



Note that a VMM is configured with a path method of mobile snr leaf. VMMs will never choose a next hop that is another snr leaf device. Thus VMMs will not "hop" through each other. Also, a VMM will not hop through a candidate meshpoint that is not bound to a meshpoint root.

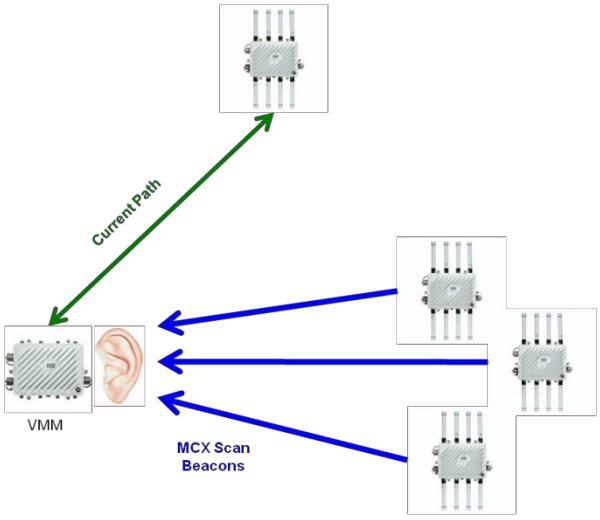


2.4.3.2 VMM ACS Dual Radio

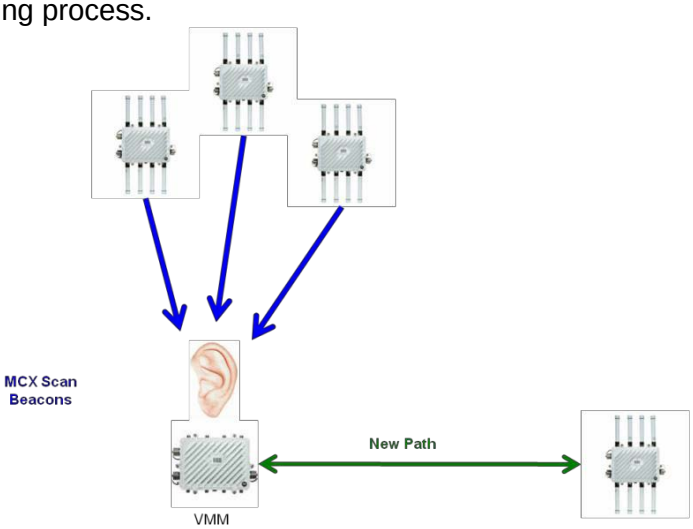
Just as in the single radio case VMMs configured to scan on both radios use the signal strength of nearby meshpoints to determine channel and path selection. While one radio is using and monitoring a mesh link, the other radio is continuously scanning for better candidates. If both radios in the same band than the scan is passive (no broadcast probing)

Example:
Radio 1 – 5GHz

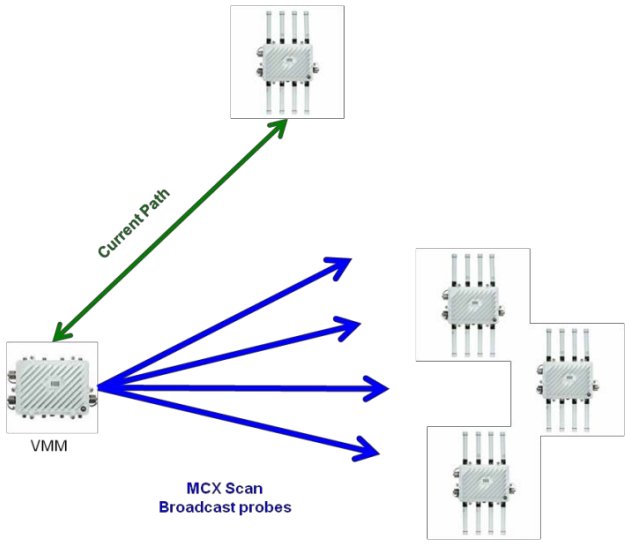
Radio 2 – 5GHz



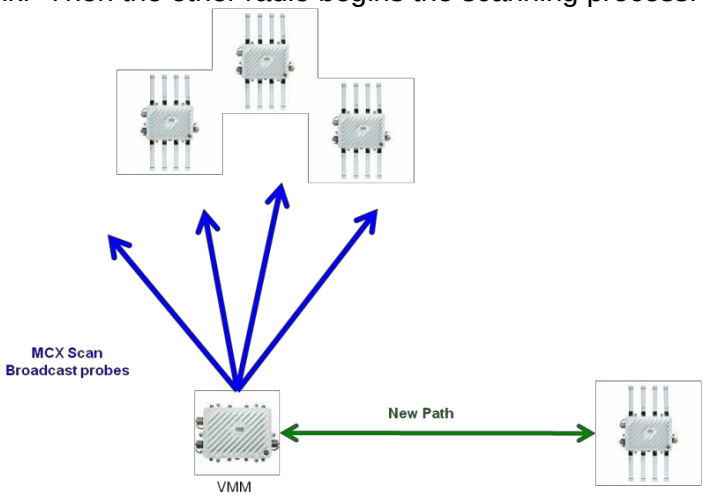
If the scanning radio finds a better next hop candidate the radio exits scanning mode, configures the radio with the next hop candidate's channel, and establishes a mesh link. Then the other radio begins the scanning process.



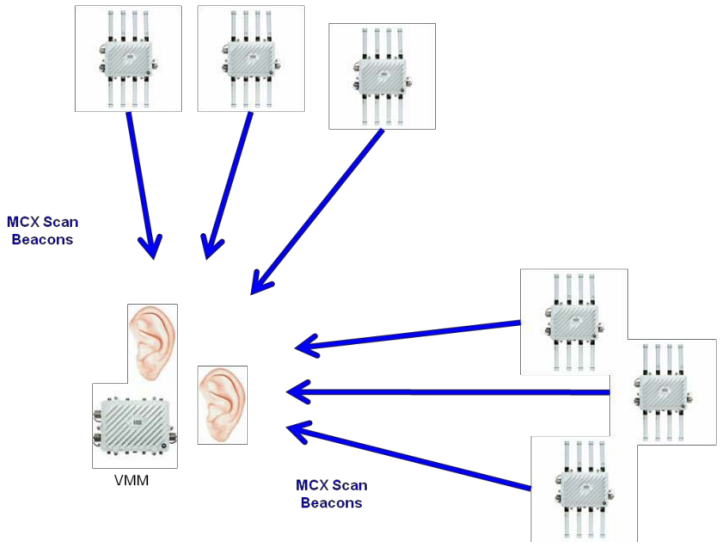
If the VMM is configured to scan on both radios and the radios are on different bands then the scanning radio will utilize an active scan (broadcast probes) to find a better next hop candidate.



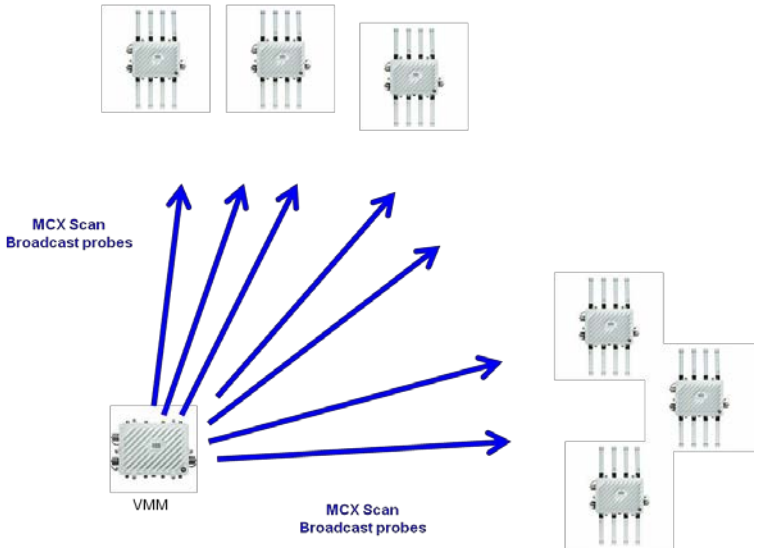
If the scanning radio finds a better next hop candidate (a better next hop candidate will only be selected if its signal strength is greater than the existing next hop by a configured delta value) the radio exits scanning mode, configures the radio with the next hop candidates channel, and establishes a mesh link. Then the other radio begins the scanning process.



If the both radios do not have an established mesh link then both will scan. In this example both radios are on the same band.



If the both radios do not have an established mesh link then both will scan. In this example the radios are on different bands



2.5 MeshConnex and Spanning Tree

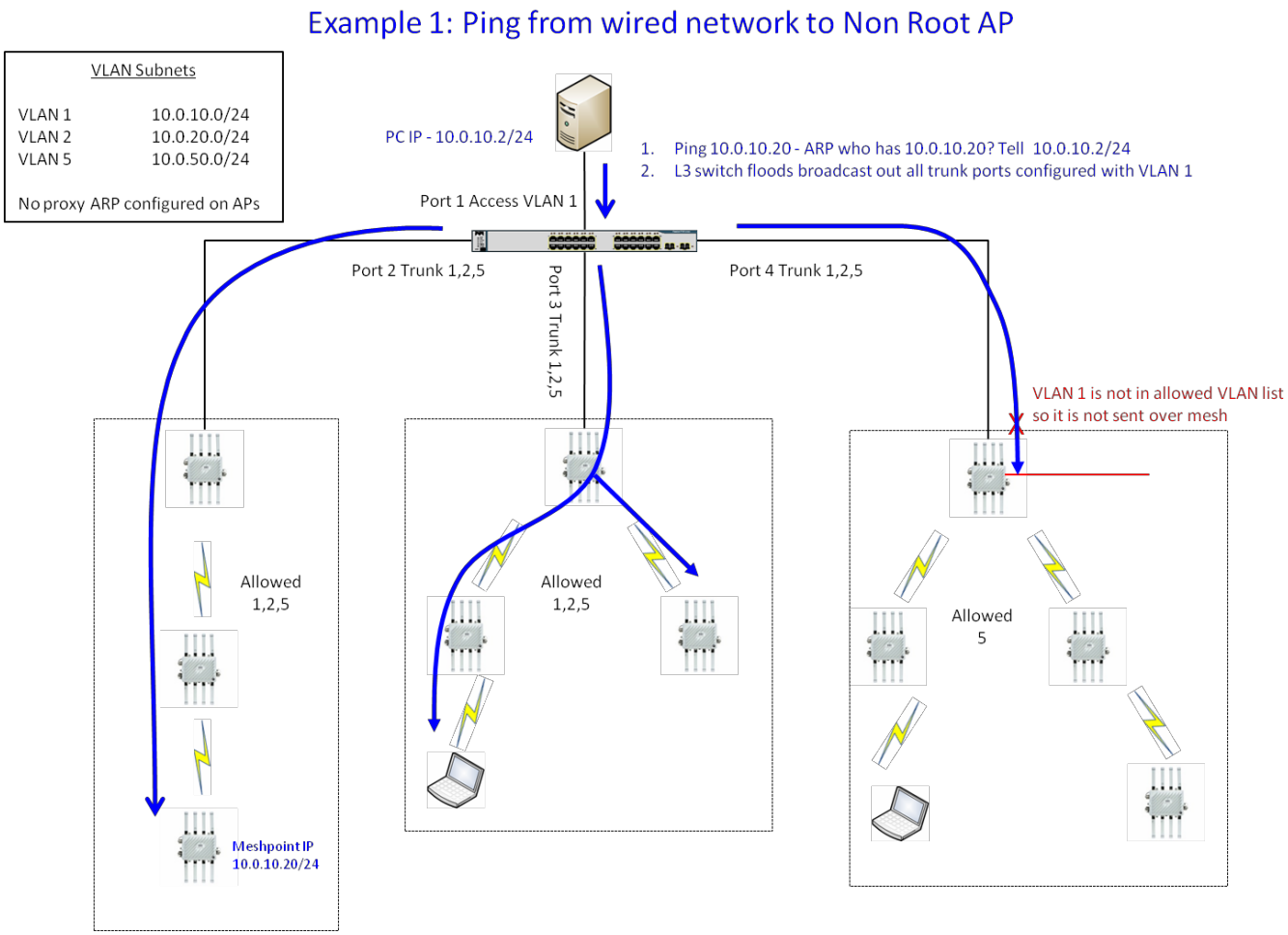
Prior to WiNG 5.5 BPDU's are not sent over MeshConnex links. In WiNG 5.5 if an AP is running MeshConnex and does not have STP configured then it will blindly forward BPDU's over MeshConnex links. Thus BPDU's are passed over MCX but the AP does not participate in the spanning tree process. If the AP has STP configured (MSTP), only the Ethernet ports participate and BPDUs are not sent across the MeshConnex links. In any case, spanning tree is not used for loop prevention on MeshConnex links. MeshConnex is inherently loop free with the exception of when a Meshpoint (Non Root) is mistakenly connected to the core network. This can cause a network loop. Primary port link monitoring and critical resource monitoring (CRM) should be used to prevent a network loop due to a Meshpoint (Non Root) being wired into the core network.

2.6 MeshConnex and Broadcast Traffic

The next several examples describe how broadcast traffic is handled by MeshConnex.

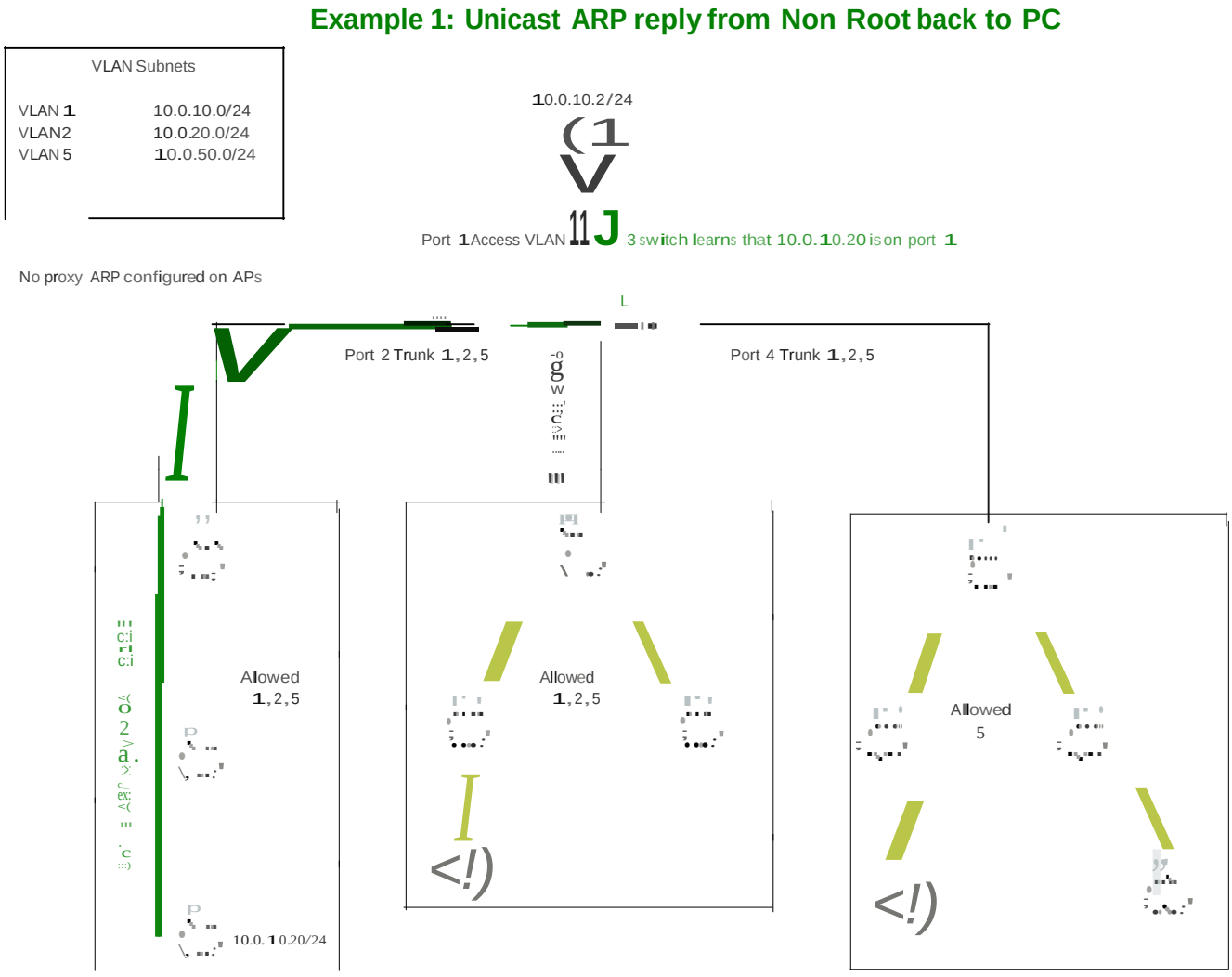
2.6.1 ARP Example 1

In the following example three Meshpoint Root APs are connected to a Layer 3 switch in the core network. A user on a core network PC (10.0.10.2) initiates a ping to 10.0.10.20 which is a Meshpoint AP. The destination IP, 10.0.10.20, is on VLAN 1, and the ARP request is flooded out on each switch port that has VLAN configured. The ARP request will only be sent across the mesh network if VLAN 1 is included in the Meshpoint Policy allowed VLAN list.



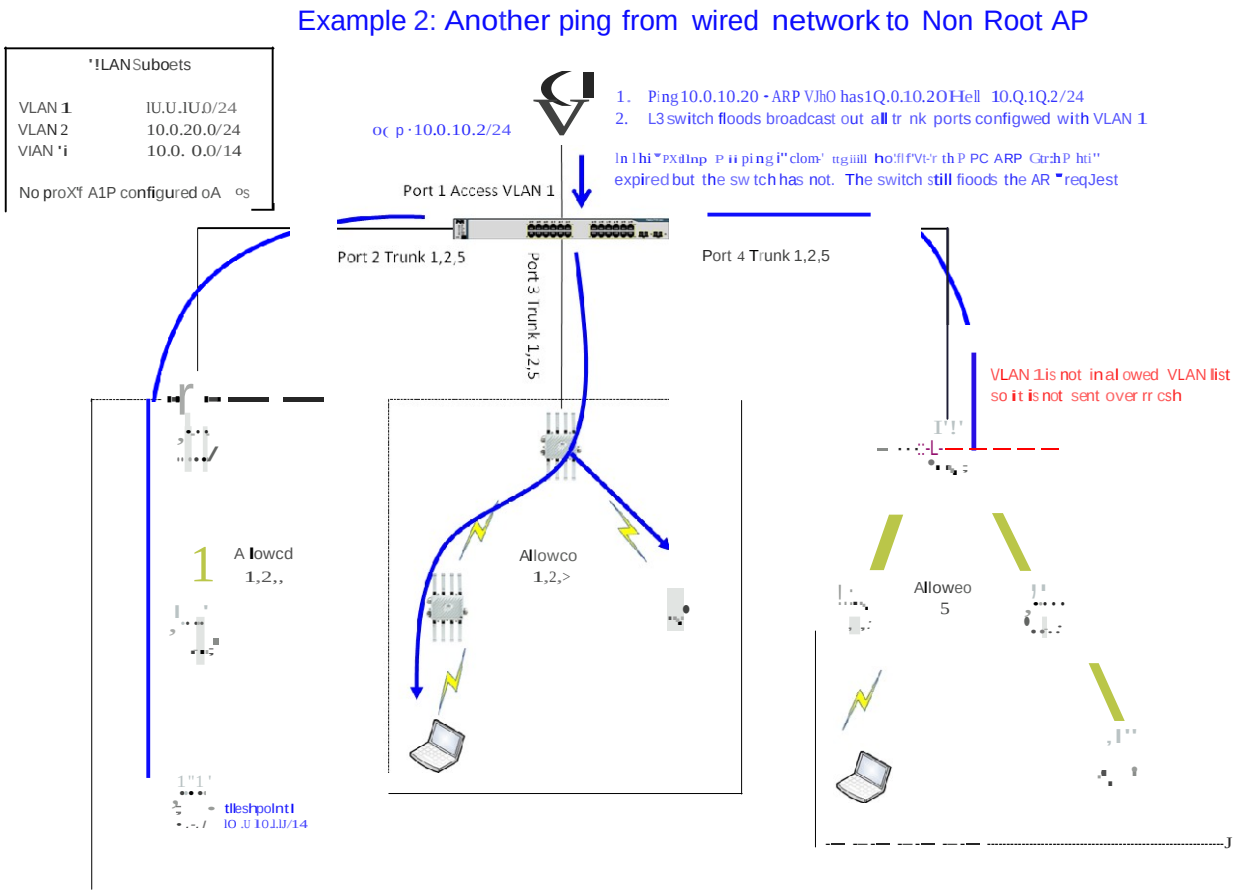
2.6.2 ARP Reply Example 1

Once the ARP request is received by the destination, a unicast ARP reply is sent back to the source, 10.0.10.2.



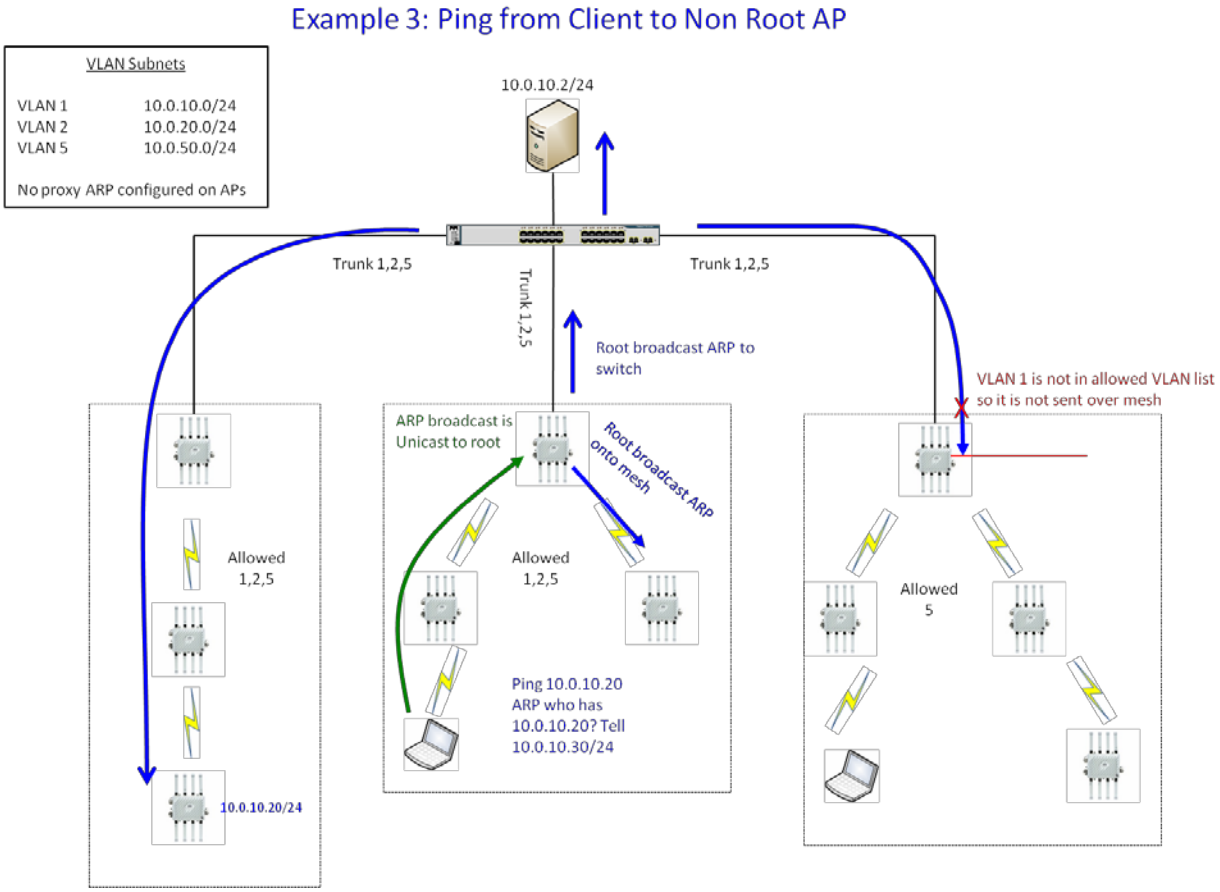
2.6.3 ARP Example 2

In this example a user on the core network PC initiates another ping to 10.0.10.20. The ARP cache on the PC has expired but not on the Layer 3 switch. However, the Layer 3 switch still floods the ARP request out all ports configure with VLAN 1.



2.6.4 ARP Example 3

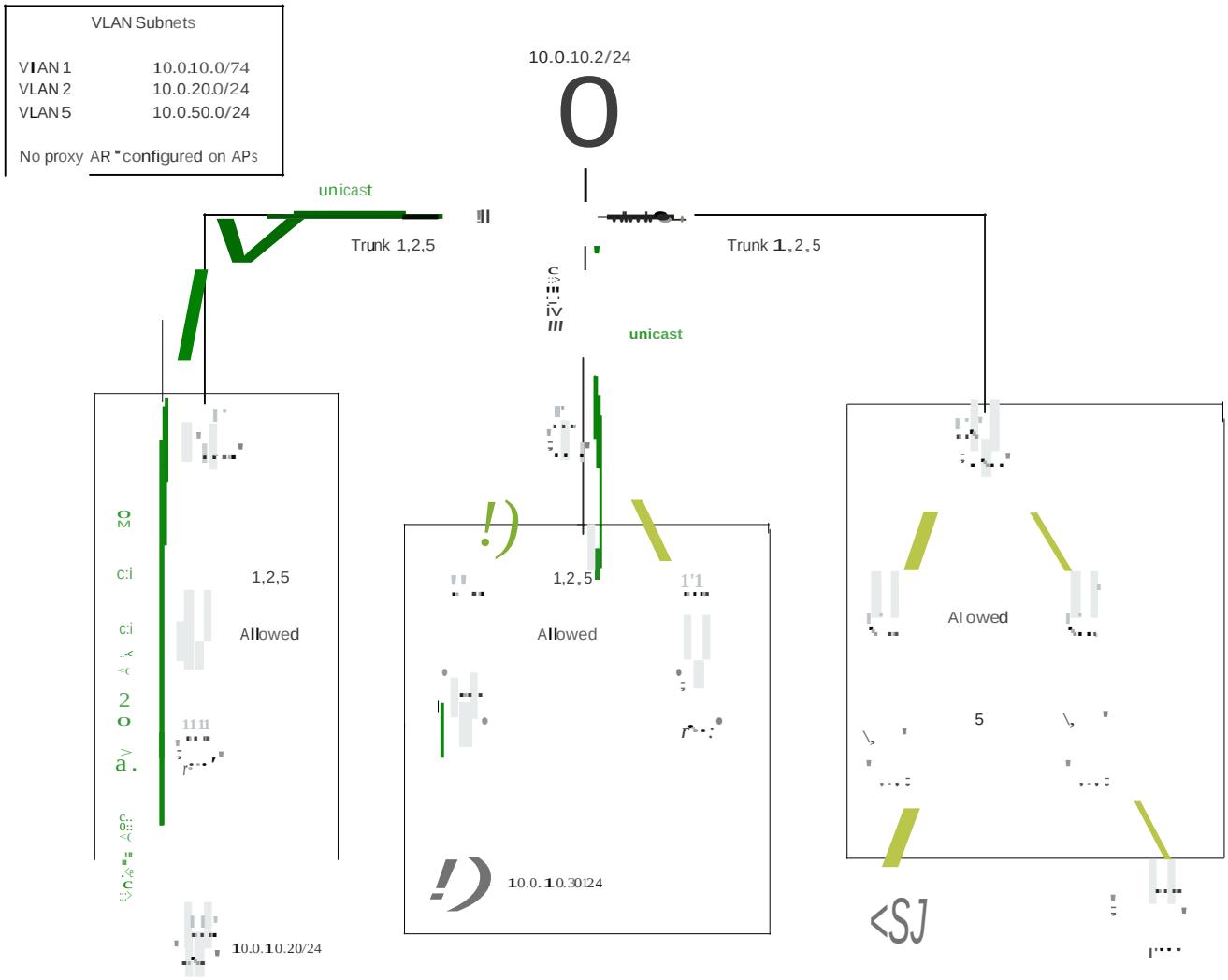
In this example a wireless client pings Meshpoint 10.0.10.20 (note that in this example the client is on the same subnet assigned to the AP's. This is not recommended and is being shown as an example only). When the Meshpoint AP the client is attached to receives the broadcast, the Meshpoint AP unicasts the request to the Meshpoint Root. The Meshpoint Root will forward the broadcast to the core network as well as back into the mesh network (Note that a sequence number is assigned to each broadcast and a Meshpoint will drop a broadcast message if it has already received one with the same sequence number).



2.6.5 ARP Reply Example 3

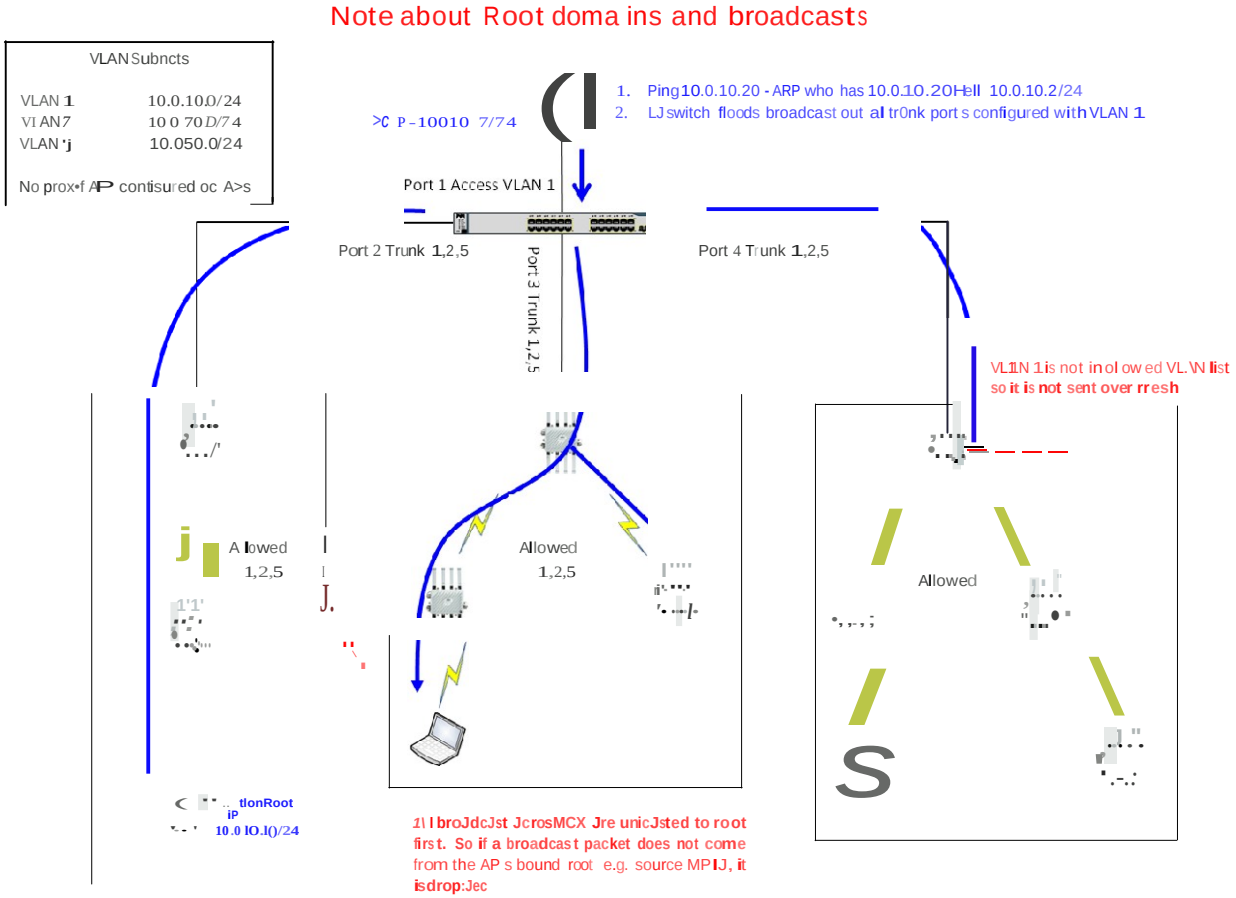
Once the ARP request is received by the destination, a unicast ARP reply is sent back to the wireless client, 10.0.10.30 as shown below.

Example 3: Unicast ARP reply to Client



2.6.6 Root Domains and Broadcasts

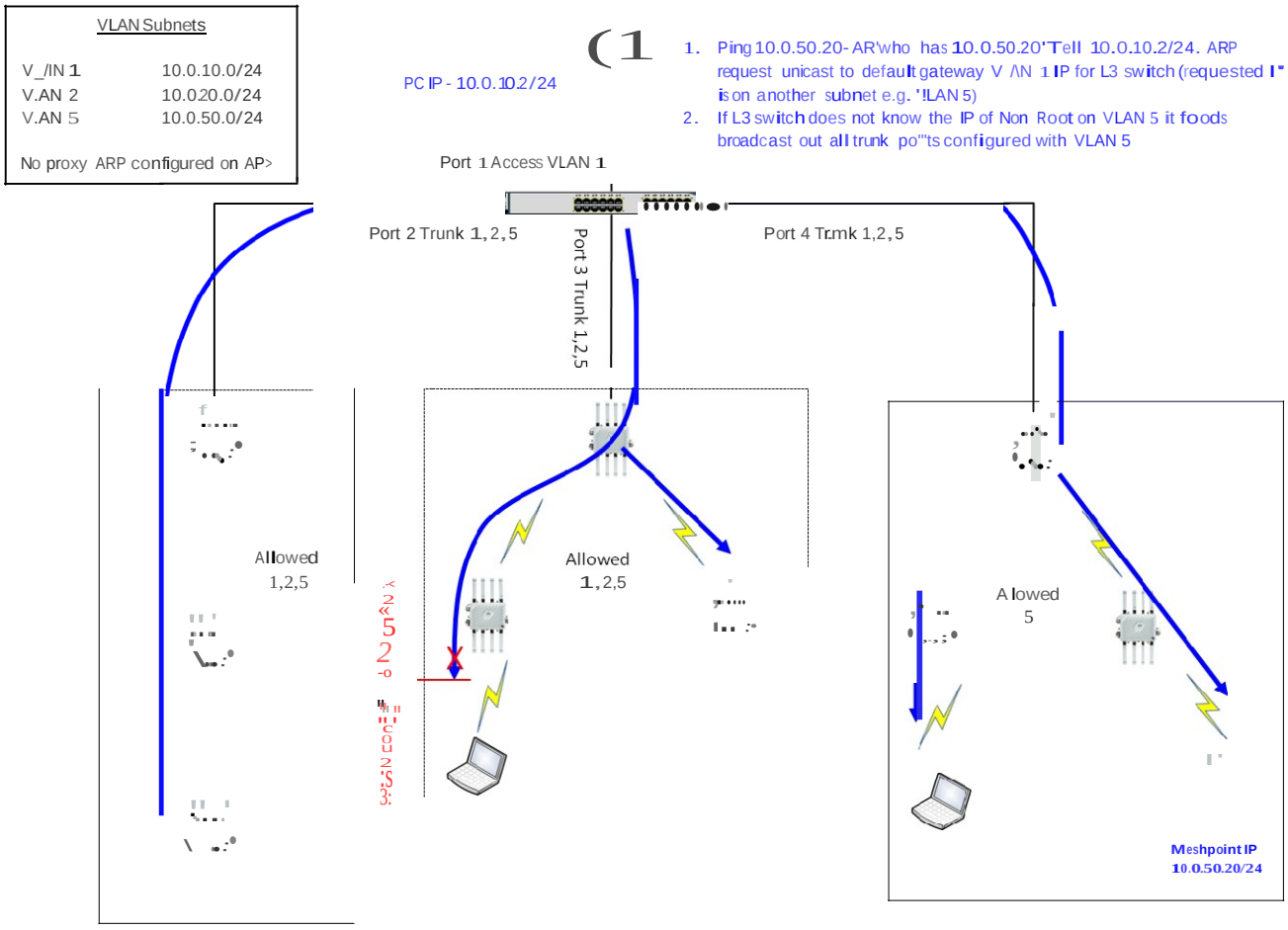
In the example below there are three Root domains. As shown in previous examples all broadcasts across MCX are unicasted to a Meshpoint Root first. If a Root broadcasts traffic across the mesh and it is received by a Meshpoint AP under another Root (e.g. another Root domain) the receiving AP will drop the traffic since the source Mesh Point ID is not the Root it is bound to.



2.6.7 ARP Example 4

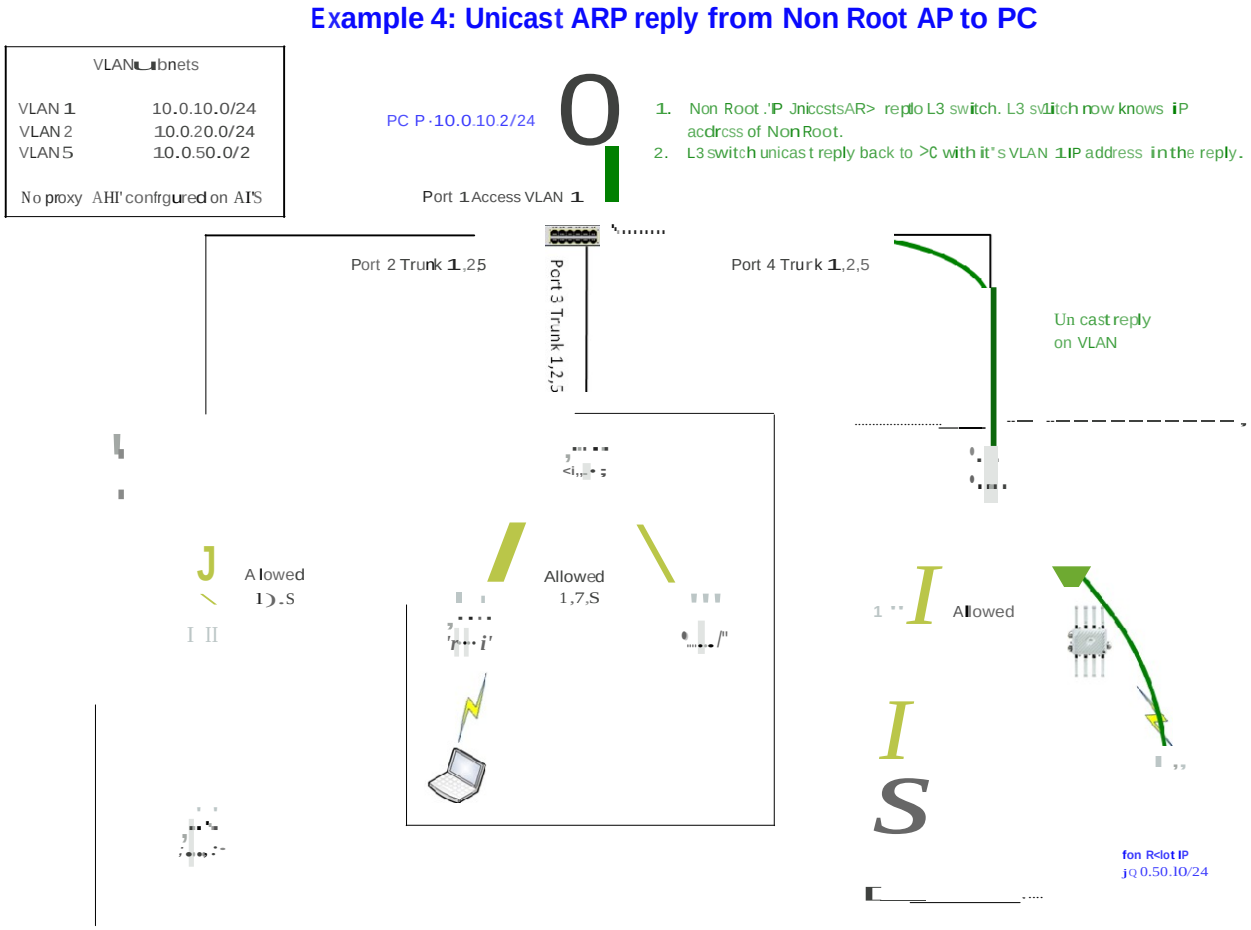
In the following example a user on a core network PC (10.0.10.2) initiates a ping to 10.0.50.20 which is a Meshpoint AP on a different VLAN. The destination IP, 10.0.50.20, is on VLAN 5, and the ARP request is flooded out on each switch port that has VLAN configured.

Example 4: Ping from VLAN 1 PC to Non Root AP on VLAN 5



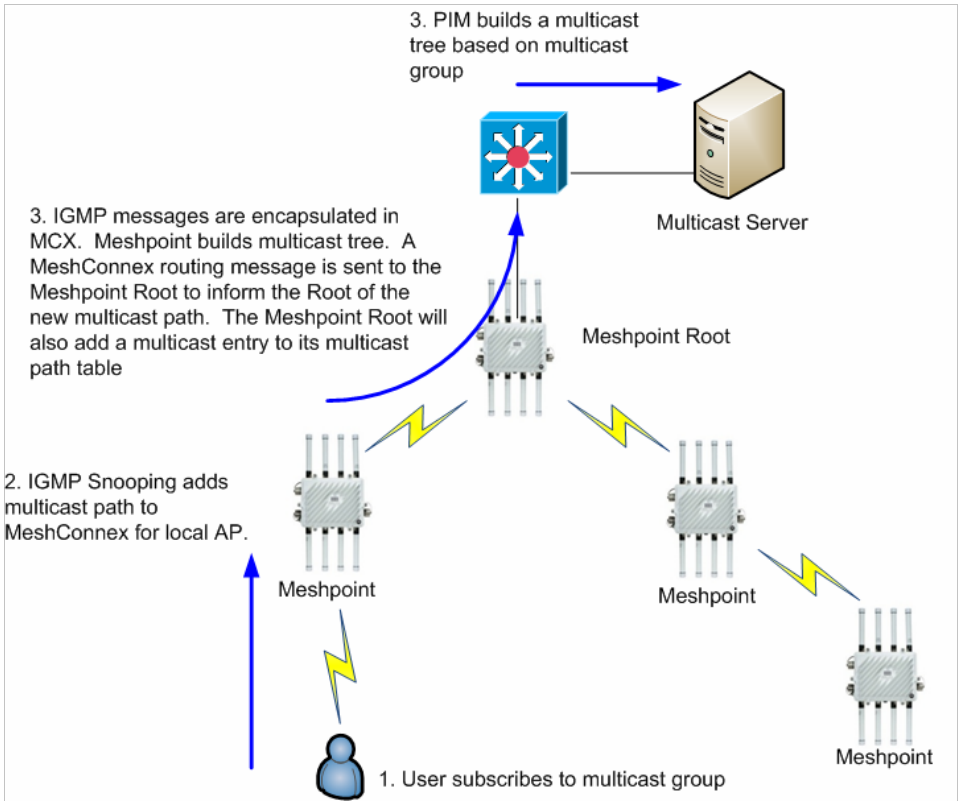
2.6.8 ARP Reply Example 4

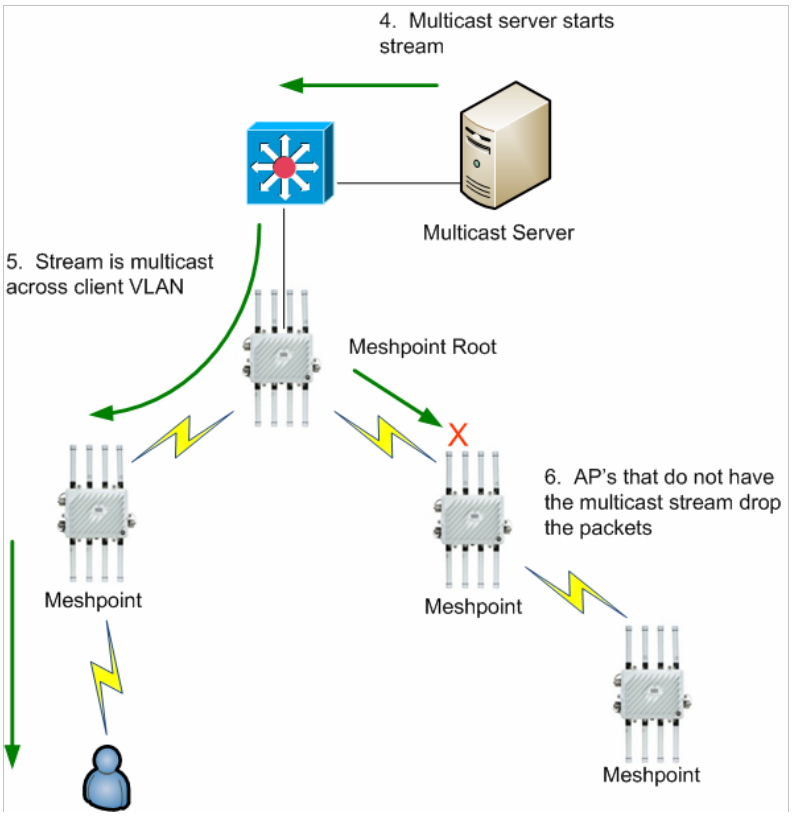
Once the ARP request is received by the destination, a unicast ARP reply is sent back to the wireless client, 10.0.10.2 as shown below.



2.7 MeshConnex and Multicast Traffic

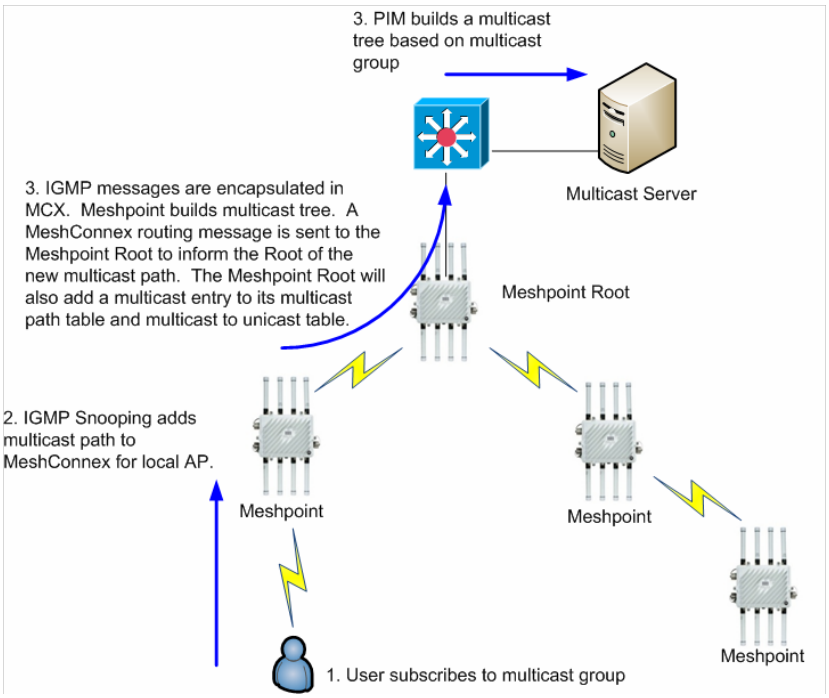
MeshConnex is designed to support efficient multicast traffic delivery over the mesh network. MCX utilizes IGMP snooping to efficiently determine which AP's require a multicast stream. The Meshpoint Root holds information on multicast group subscription for its associated subscribers and maps subscribed group members to L2 multicast addresses for routing in the wireless mesh network. The Meshpoint Root uses an IGMP filter to inform the MCX routing protocol of the Layer 2 multicast MAC addresses subscribed by the proxies and local Meshpoint AP. A multicast route table is maintained for each mesh enabled AP, containing information including the multicast group MAC address, hop count, and routing metrics to the multicast group core. IGMP snooping provides MeshConnex with a mechanism to prune multicast traffic from mesh links that do not contain a multicast listener (an IGMP client). Packets are filtered out when there is no multicast subscription. If IGMP snooping is disabled on the AP, MeshConnex will flood multicast traffic to all the paths available in its path table.
The example below illustrates how MeshConnex handles a multicast request.

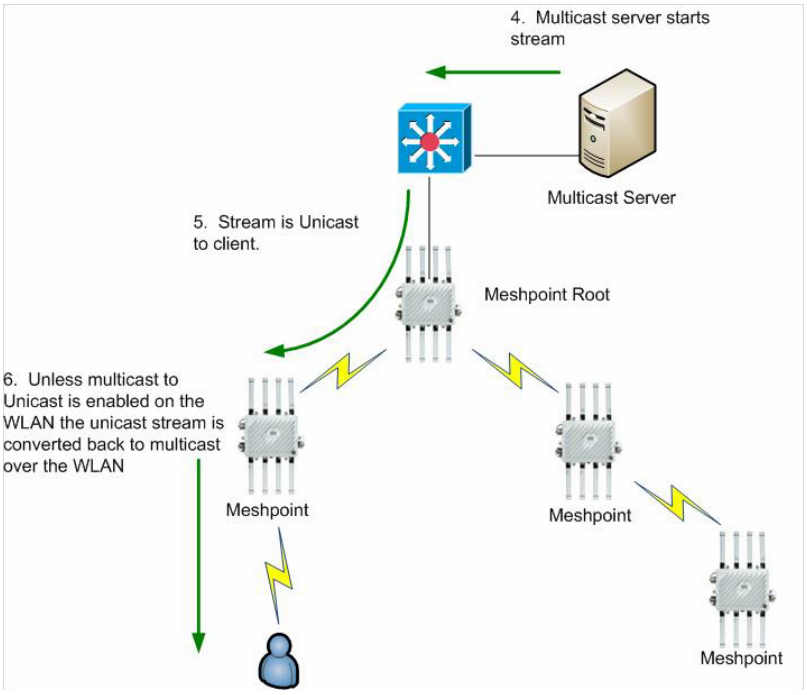




2.7.1 Multicast to Unicast (Accelerate Multicast)

By default multicast traffic is sent over the wireless network at either the lowest or highest basic rate depending upon radio configuration (interface radio→Advance Settings →Broadcast/Multicast Transmit Rate). To increase the quality of video traffic multicast packets whose addresses are configured are converted to unicast packets for clients that have registered via IGMP. The number of clients per radio can be limited.





Multicast Table

Mesh Point Name – This is the name of the configured mesh point on the AP being viewed.

Mesh Point ID – The Mesh Point ID is automatically chosen by MCX. For APs configured with a single radio mesh this ID will be the BSSID of the mesh radio. On APs that are running mesh on multiple radios the Mesh Point ID will be the BSSID of the radio that was added first. In most cases this will be done on startup and will be radio 1.

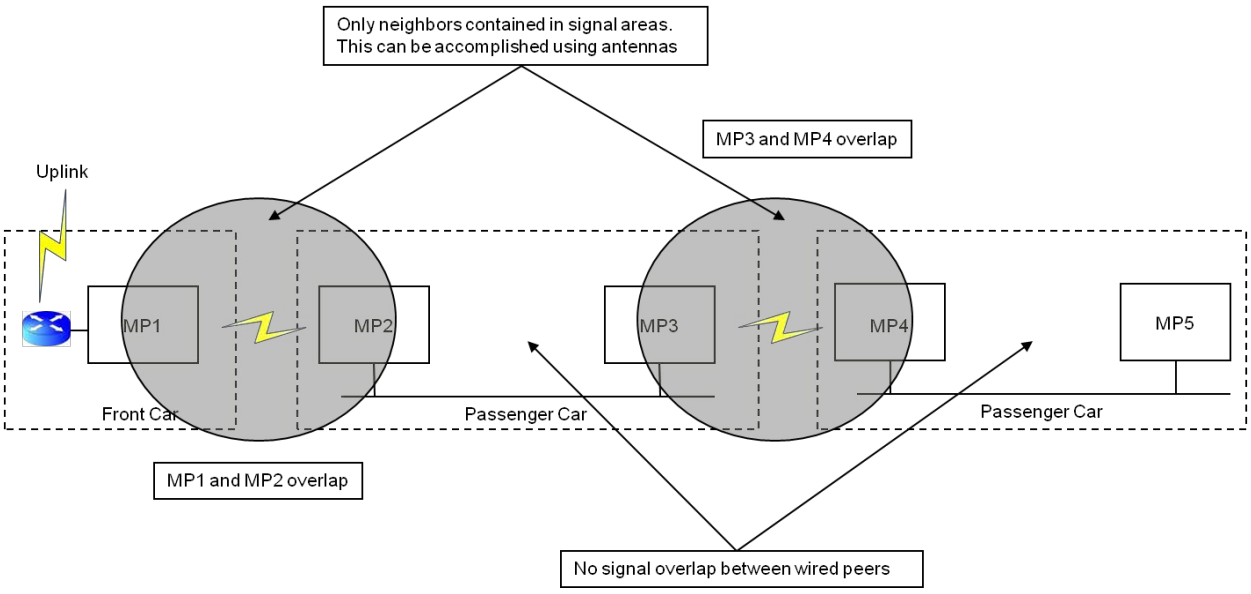
Member Address – This field lists the MPID of the AP that has the multicast subscriber attached to it.
Group Address – This field lists the multicast MAC for the multicast IP address being used.
Path Timeout – This field lists in ms how long to keep the multicast subscription active. Note that a -1 indicates “forever”.

2.8 Dynamic MeshConnex

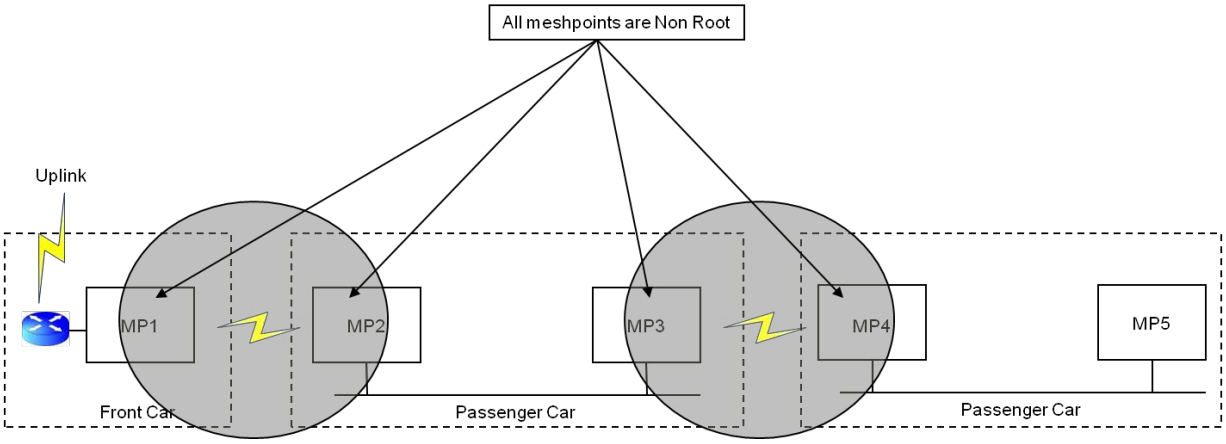
MeshConnex also supports a mode of operation called dynamic mesh. This mode is used in rail applications. With this mode of operation MeshConnex will automatically determine Meshpoint Root and Non Root behvaior. The use of dynamic meshing requires specific deployment requirements and careful attention must be made to ensure the proper behavior is achieved.

2.8.1 Proximity Method

With this method there is no selection of a Meshpoint Root or Meshpoint. All AP’s are considered Meshpoint APs. AP’s must be deployed on the train such that an AP can only have a single neighbor. These neighboring AP’s must be deployed such that they have overlapping signal areas. This can be accomplished by adjusting power and using directional antennas. Neighboring AP’s will essentially establish a point to point link between them.



The proximity method establishes a point to point mesh link between two meshpoints. This method only works on meshpoints with overlapping signal areas

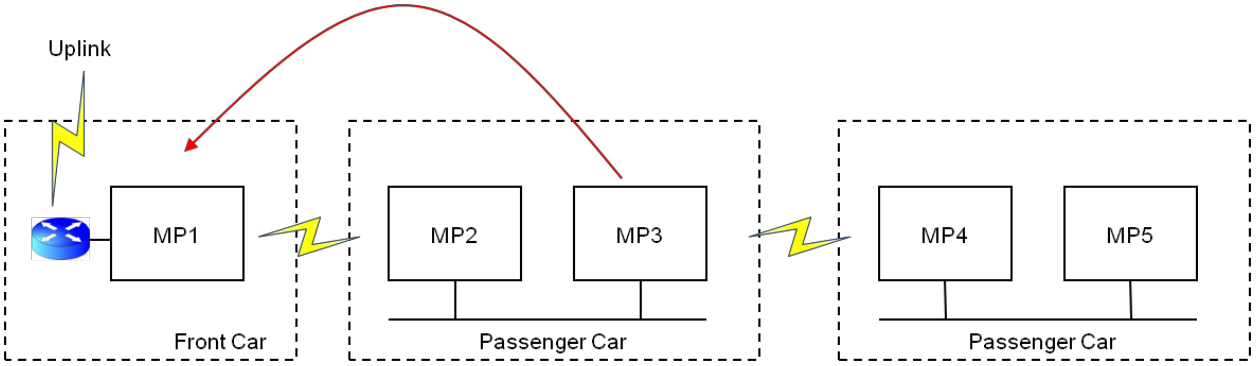


2.8.1.1 Configuration

The following configuration items need to be configured in the device profile under meshpoint device.

Hysteresis

Hysteresis is used to help ensure the correct neighbor is chosen in the respective signal areas. For example a minimum RSSI threshold can be set forcing the meshpoint to only consider a neighbor if a minimum RSSI is met. In this example, MP1 should only hear beacons from MP2. However the Hysteresis min-threshold letting is used to ensure that beacons received at an RSSI weaker than the configured threshold will be dropped e.g. if MP1 heard a beacon from MP3. This will ensure that a mesh link will not be formed.

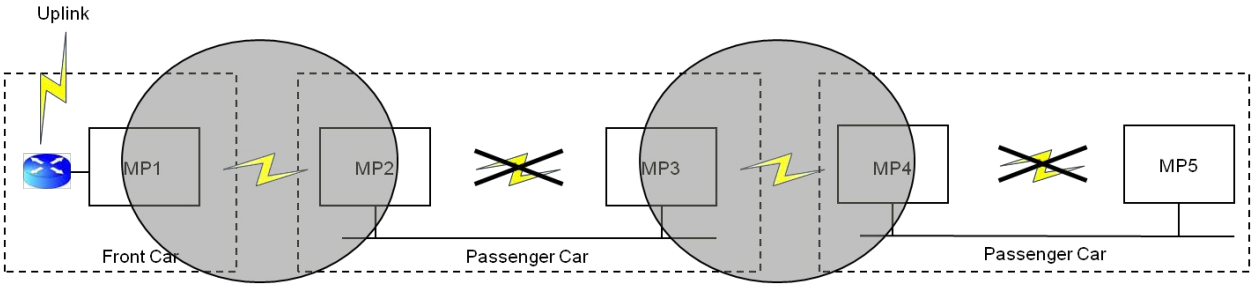


CLI Command:
hysteresis min-threshold -60

Wired Peer Exclusion

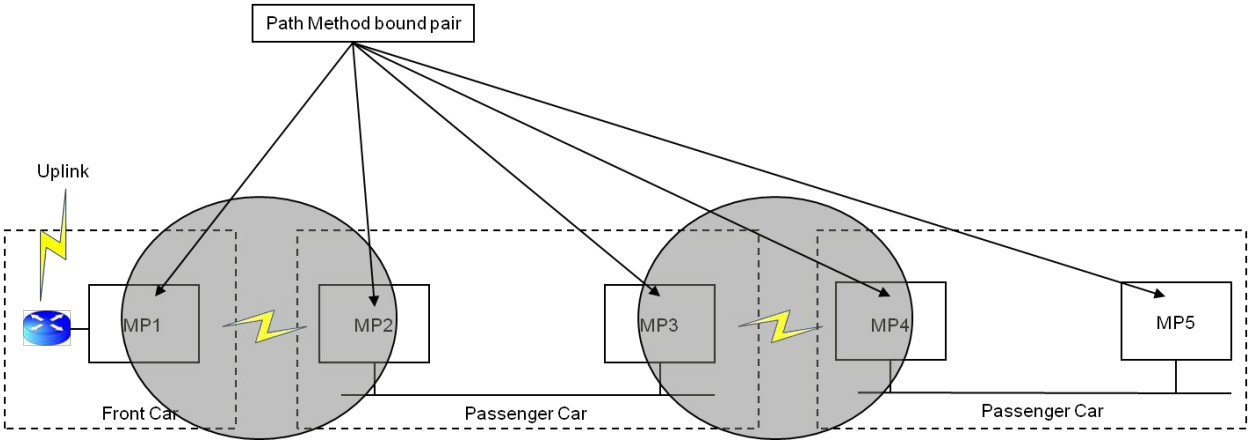
When configuring the meshpoint the Wired Peer Exclusion feature will prevent these wired devices from forming a mesh link (even though they should not since their signal areas do not overlap). Beacons exchanged between wired APs will be dropped by either AP when Wired Peer Exclusion is enabled. An AP that receives beacons from a neighbor that is also wired (as determined by the MINT cost to that AP) will be "excluded" from forming a mesh link.

CLI Command:
exclude wired-peer mint-level-1



Bound Pair

The Path Method is set to bound-pair. This instructs the meshpoint bind with a single meshpoint.

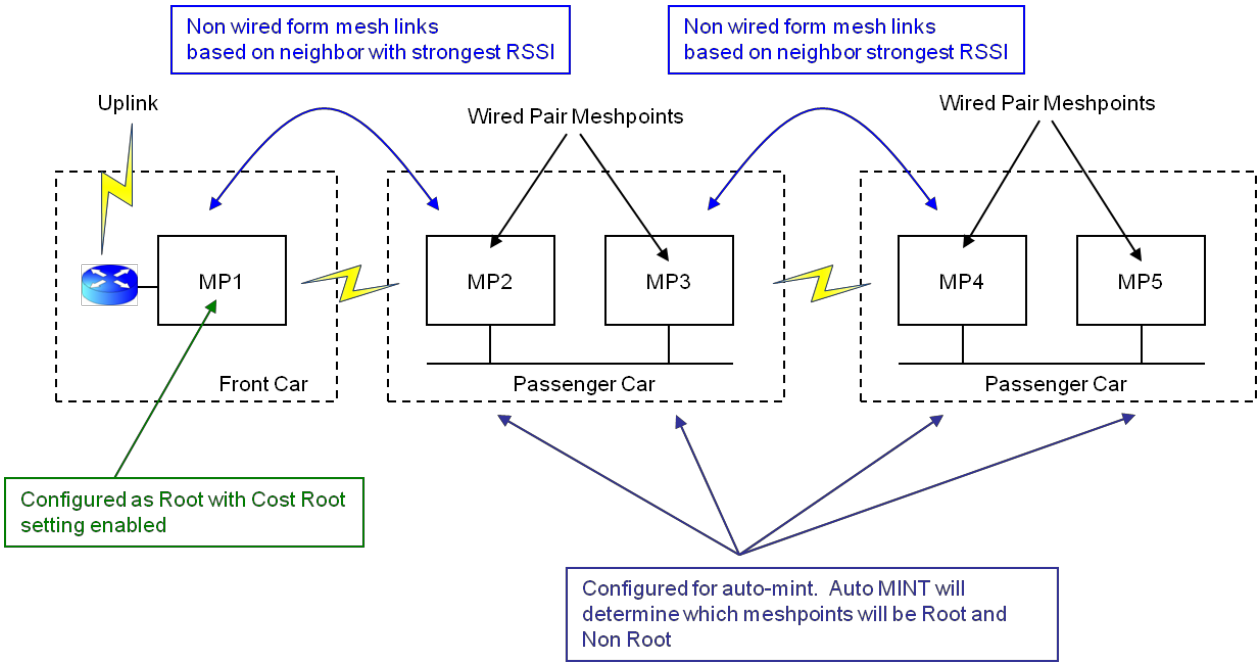


CLI Command:
path-method bound-pair

2.8.2 Auto Mint Method

With this method mint will be used to determine if the AP will operate as a Meshpoint Root or Meshpoint AP. Only the AP located at the front of the train is set to Root and is considered the gateway AP. The Wired Pair Exclusion setting which is configured on all meshpoints except the gateway AP allows a meshpoint to discover wired meshpoints on the same wired network

through mint links. Wired Pair meshpoints will not form a mesh link as they will ignore each other's beacons. Non wired meshpoints will form mesh links according to the neighbor with the strongest RSSI as determined by snr-leaf and dynamic mesh hysteresis settings. An AP will be set to Meshpoint AP (Non Root) if the shortest path back to gateway AP (Cost Root) is over an MCX link. An AP will be set to a Meshpoint Root AP if the shortest path back to Gateway AP (Cost Root) is a wired link.

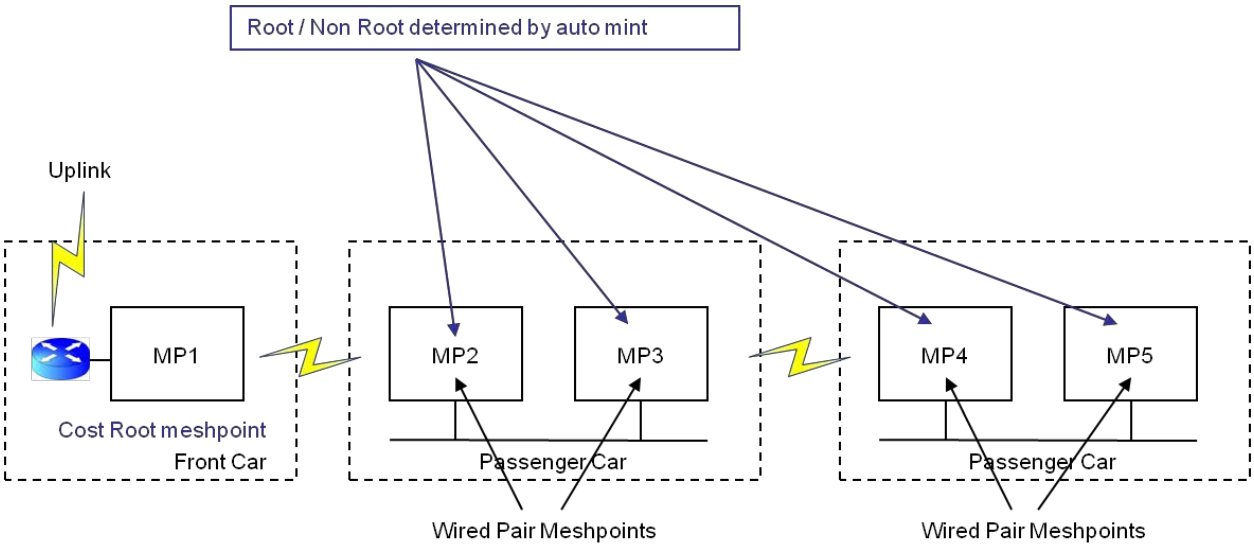


2.8.2.1 Configuration

The following configuration items need to be configured in the device profile under meshpoint device.

Auto Mint

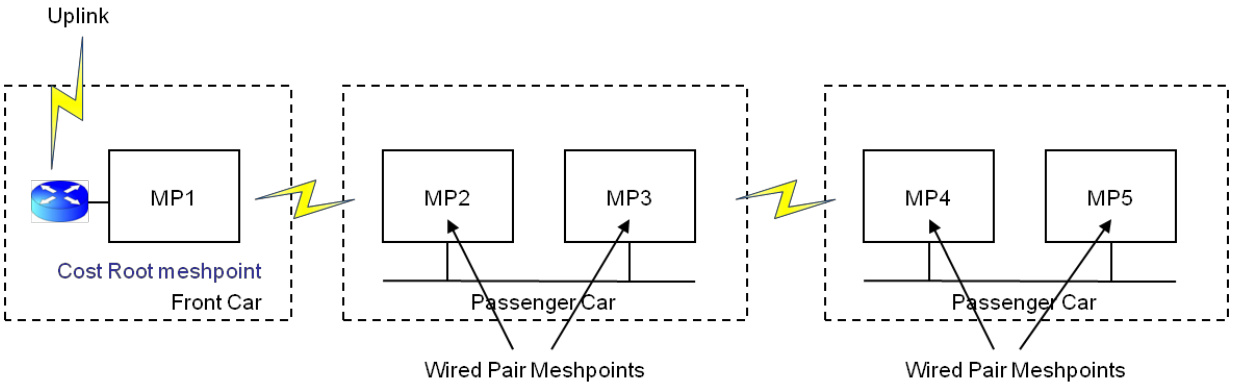
In this example, MP2, MP3 and MP4 are configured for auto-mint. Note that MP1 is not configured for auto-mint. It is configured as a Root with Root Selection Method None and Cost Root enabled.



On MP2, MP3, and MP4

CLI Command:
root select-method auto-mint

MP1 is configured as a Cost Root with Root Selection Method None. Since MP1 is the Root and the gateway for the network it must be configured as a Cost Root mesh point.

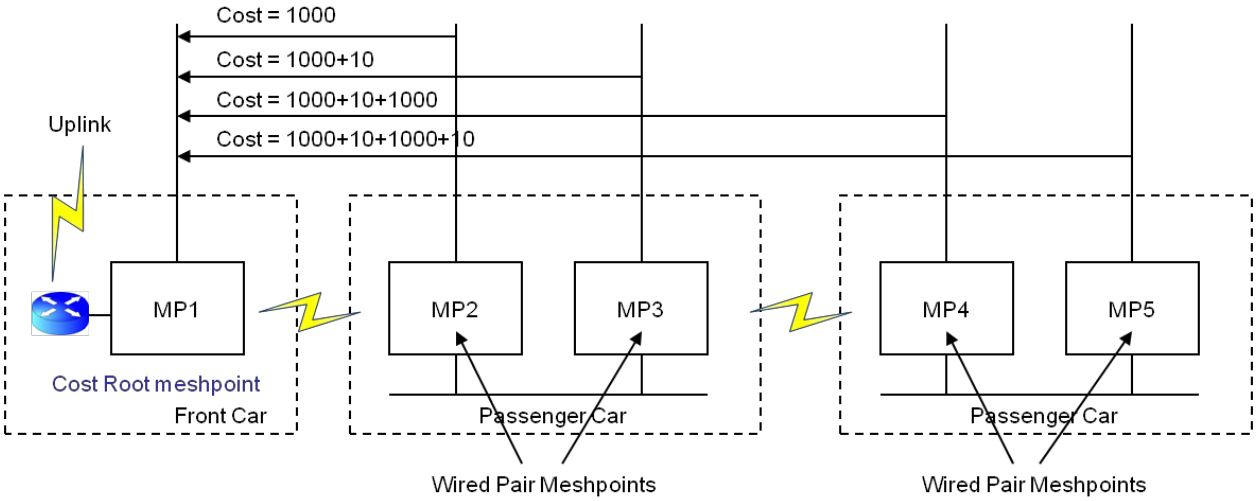


On the gateway AP MP1:

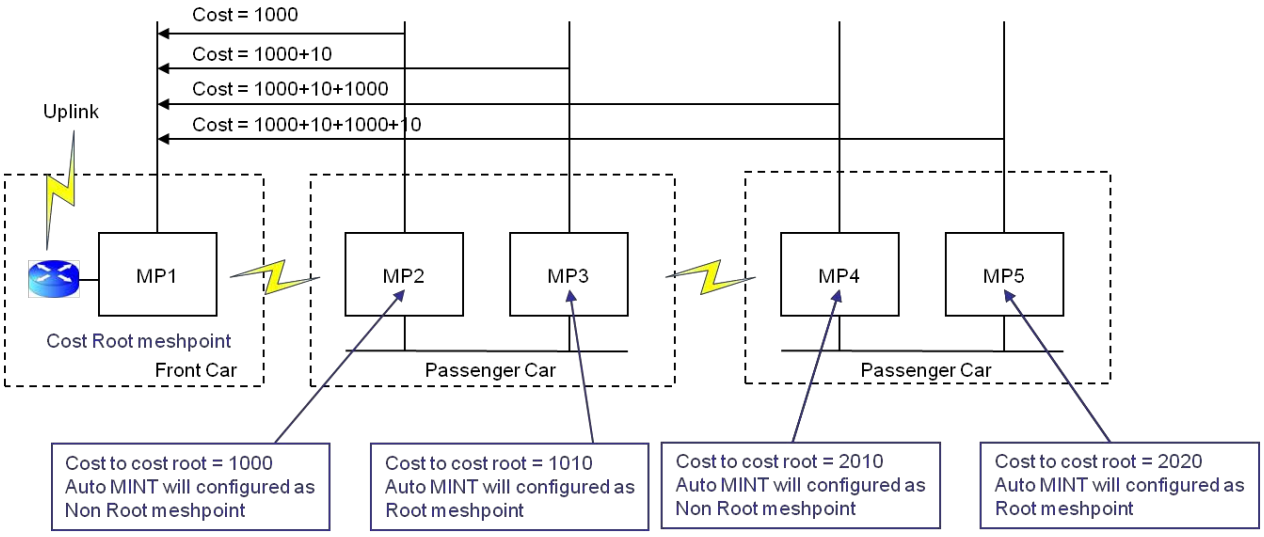
CLI Command:
root select-method none
root-select cost-root

Auto Mint determines the best path cost to the Cost Root meshpoint. The path cost to the Cost Root meshpoint is shared in beacons. In this example to MP1:

Wired Path Cost = 10
MCX Path Cost = 1000



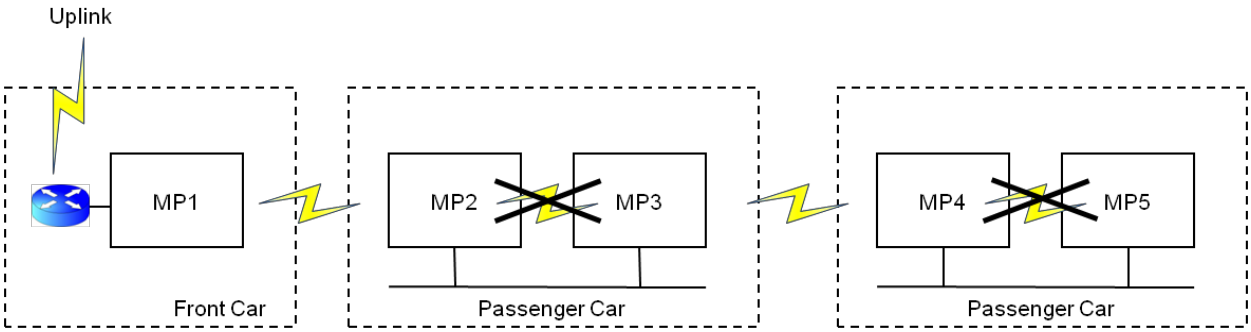
If the link with the shortest path cost to the cost root is an MCX mesh link then the meshpoint will be configured as a Non Root, otherwise it will be configured as a Root.



Wired Peer Exclusion

When configuring the meshpoint the Wired Peer Exclusion feature will prevent these wired devices from forming a mesh link (even though they should not since their signal areas do not overlap). Beacons exchanged between wired APs will be dropped by either AP when Wired Peer Exclusion is enabled. An AP that receives beacons from a neighbor that is also wired (as determined by the MINT cost to that AP) will be “excluded” from forming a mesh link.

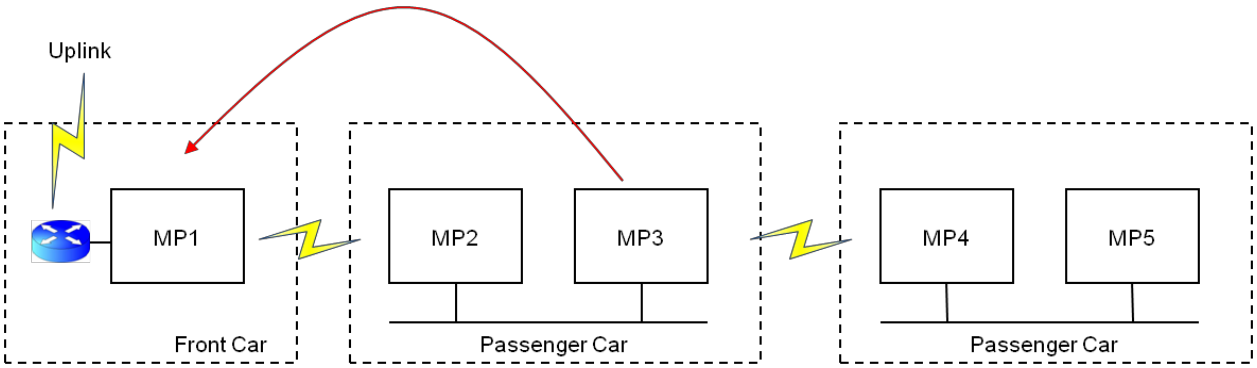
CLI Command:
exclude wired-peer mint-level-1



Hysteresis

Hysteresis is used to help ensure the correct neighbor is chosen in the respective signal areas. For example a minimum RSSI threshold can be set forcing the meshpoint to only consider a neighbor if a minimum RSSI is met.

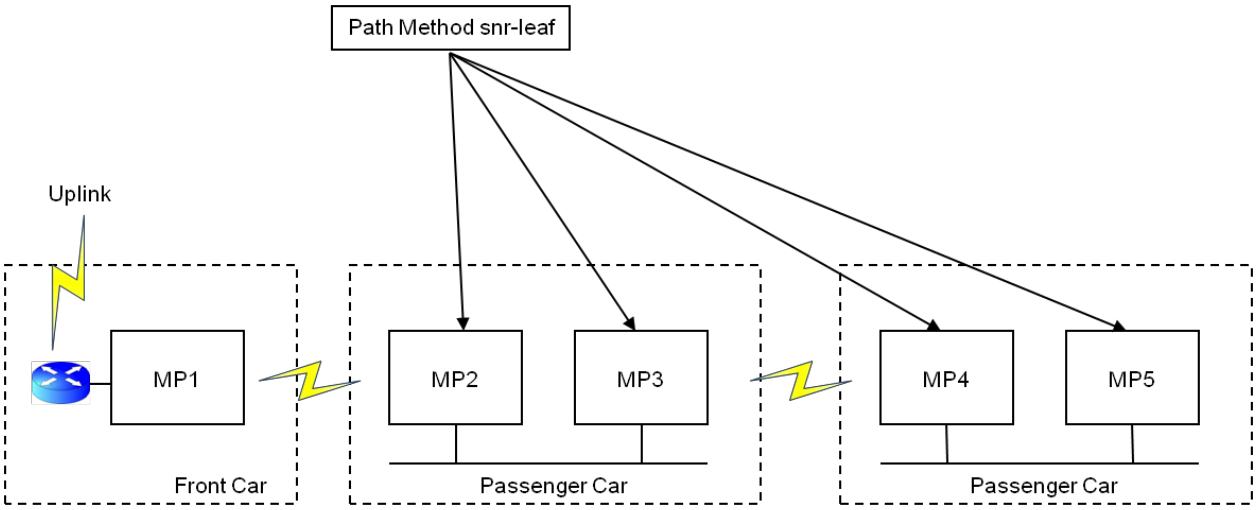
In this example, MP1 should only hear beacons from MP2. However the Hysteresis min-threshold letting is used to ensure that beacons received at an RSSI weaker than the configured threshold will be dropped e.g. if MP1 heard a beacon from MP3. This will ensure that a mesh link will not be formed.



CLI Command:
hysteresis min-threshold -60
In this example signals with an RSSI weaker that -60 dBm will be ignored

snr-leaf

The Path Method is set to snr-leaf. This instructs the meshpoint to form mesh links based on signal strength only. This along with the Minimum Threshold hysteresis is used mesh link formation.



CLI Command:
path-method snr-leaf

3. MeshConnex Show / Debug Commands

The following CLI commands are used to display information about an AP's neighbors, path to the Root, and other meshpoint statistics.

Commands:

- **show adoption status** – used to see if the AP has been adopted by a controller or virtual controller.
- **show mint links** – used to verify that MiNT links have formed.
- **show mint lsp-db** – used to display detailed information on each adjacency.
- **show wireless meshpoint neighbor detail** – used to display the neighbor table.
- **show wireless meshpoint neighbor statistics rf** – used to display the signal level from each neighbor.
- **show wireless meshpoint path detail** – used to show the path table.
- **show wireless meshpoint root detail** – used to show the Root table.
- **show wireless meshpoint security detail** – used to show the link security to each neighbor.
- **show wireless meshpoint proxy detail** – used to show the devices proxied by the AP.
- **show wireless meshpoint** – used to show meshpoint configuration as well as if the AP is Root.
- **show wireless meshpoint detail** - used to show additional meshpoint configuration such as control and allowed VLAN's.
- **show wireless meshpoint config** – used to see if the meshpoint is enabled.
- **show wireless meshpoint multicast detail** – used to see any multicast subscribers on the AP.
- **more system:/proc/dataplane/wireless/radio/radio<1|2>-stats** – used to view radio statistics such the PCR at each data rate.
- **service clear wireless radio statistics** – used to clear the radio stats.

On Controller:

- **show wireless meshpoint tree on <rf-domain>** - used to display a text graphic showing each mesh AP and the AP's meshing under it.

Debug:

- **show logging** - used to show current logging status.
- **logging monitor debugging** – used to enable logging on the current ssh or telnet session.
- **debug wireless meshpoint level <debug|error|info|warn>** - used to debug all meshpoint related events including path changes, auto channel selection, etc.

4. MeshConnex Tables

4.1 Neighbor Table

Mesh Point Name – This is the name of the configured mesh point on the AP being viewed.
Mesh Point ID – The Mesh Point ID is automatically chosen by MCX. For AP's configured with a single radio mesh this ID will be the BSSID of the mesh radio. On AP's that are running mesh on multiple radios the Mesh Point ID will be the BSSID of the radio that was added first. In most cases this will be done on startup and will be radio 1.
Neighbor Mesh Point ID – This is the Mesh Point ID of the listed neighbor.
Neighbor IFID – This is the interface ID of the listed neighbor.
Root MPID – This is the Mesh Point ID of the Root AP being used by the listed neighbor.
Is Root – This field indicates whether or not the listed neighbor is a Root AP.
Mobility – This field indicates if the listed neighbor is a mobile node e.g. VMM (Vehicular Mounted Modem).
Radio Interface – This field indicates the radio interface being used to reach the listed neighbor.
Hops – This field indicates the number of hops to the listed neighbor.
Resourced – This field indicates that whether or not the listed neighbor is resourced. The resourcing of a link is part of the neighbor initialization process. Note that resourced neighbors remove from the total available WLAN clients supported on a device.
Link Quality - This field lists the link quality. Link quality is a measurement of the success of packets being received by the neighbor. When no active traffic is being sent to a neighbor the Link Quality measurement is predicted via the exchange of hello packets. When there is active traffic being passed to a neighbor the Link Quality measurement is based on real MAC layer feedback. Link Quality ranges from 0 to 100 with 100 being the best link. A link quality measurement of 90-100 is considered excellent.
Link Metric – The Link Metric is a measure of performance of the link to the neighbor. The Link Metric ranges from 1 to 65,535 with lower numbers being better. However a single hop Link Metric > 1500 generally denotes a link that cannot be used. When viewed in the neighbor table the Link Metric value is a 1 hop measurement while in the Path table the Link Metric is the sum of all of the Link Metrics along the path to the Root.
Root Metric – This field lists the total Link Metric as seen by the listed neighbor to the Root AP.

Rank – This field indicates by a ranking number how important a device is. This is used in resource allocation. Ranks range from -1 to 8. -1 indicates a different mesh id or failed authentication; 0 indicates the same mesh, different root; 1 indicates the same root; 2 indicates active peer path; 3 indicates bound, or could improve via the local node; 4 indicates unbound; 5 indicates bound through local node; 6 indicates good uplink to next best root; 7 indicates good uplink to recommended root; 8 indicates current uplink to root. Please note that wireless WLAN clients will remove resources of 3 or less.
Age – This field indicates in ms the last time a beacon was heard from the listed neighbor.

4.2 Security Table

Mesh Point Name – This is the name of the configured mesh point on the AP being viewed.
Mesh Point ID – The Mesh Point ID is automatically chosen by MCX. For AP's configured with a single radio mesh this ID will be the BSSID of the mesh radio. On AP's that are running mesh on multiple radios the Mesh Point ID will be the BSSID of the radio that was added first. In most cases this will be done on startup and will be radio 1.
Radio Interface – This field indicates the radio interface being used to reach the listed neighbor in which the security relationship has been established.
IFID – This field indicates the BSSID of the radio of the listed security association.
Link State – This field lists the security state of the link to the listed neighbor. Links transition from the Init State, to In Progress, then either to Enabled or Failed. When a link has been successfully initialized and a security relationship has been established the link will enter the Enabled state.
Link Timeout – This field lists the time in seconds before the link must be refreshed.
Keep Alive – This field indicates whether or not a keep alive should be implemented to the listed security association. For example, if the listed neighbor is attached to another Root AP the keep alive field may not be set.

4.3 Path Table

The following fields are in the Path table:

Mesh Point Name – This is the name of the configured mesh point on the AP being viewed.
Mesh Point ID – The Mesh Point ID is automatically chosen by MCX. For AP's configured with a single radio mesh this ID will be the BSSID of the mesh radio. On AP's that are running mesh on multiple radios the Mesh Point ID will be the BSSID of the radio that was added first. In most cases this will be done on startup and will be radio 1. Note that this may change after rebooting a device if radio 2 was added first.
Destination – This field lists the Mesh Point ID of the destination for the listed path. For Root AP's destinations will be other Mesh Point AP's. For Non Root AP's destinations will be Non Root AP's as well as Root AP's.
Next Hop IFID – The Next Hop Interface ID is the MAC address of the next hop's mesh radio.
Is Root – This flag indicates whether or not the AP listed in the Path table is configured as a Root AP.
MiNT ID – This is the Layer 2 MiNT ID of the AP listed in the Path table.
Hops - This field indicates the number of hops to the Root AP.

Mobility – This field indicates if mobility is enabled on the AP listed in the path table. This will always be False for a path to a Root AP.
Metric – This field indicates the path metric to the Root AP. This metric is the sum of all of the link metrics along each hop to the Root AP. The lower the number the better the metric.
Path State – This field lists the current state of the Path. Path States can be Valid, Request Timeout, Expired, In Progress, or Forward to Root. Active paths being used will be listed as Valid. Request timeout indicate there was no response to a path request. Expired indicates that a path is about to be removed. In Progress indicates that a path is being established. Forward to Root indicates that a device can be reached through the Root.
Bound – This indicates if the AP is bound to the Root AP listed in the Path table. The AP will not use the listed Root until it is bound. Bind states can be Bound, Unbound, Proxy Updated, Disfavored, or Removed.
Path Timeout – This field indicates the time in seconds remaining until the path is declared invalid. This timeout value will continue to refresh as long as the path remains valid.
Sequence – This field lists the sequence number of the Path Request.

4.4 Root Table

Mesh Point Name – This is the name of the configured mesh point on the AP being viewed.
Recommended – This indicates the recommended Root AP to use.
Root MPID – This is the Mesh Point ID of the listed Root AP.
Next Hop IFID – The Next Hop Interface ID is the MAC address of the next hop's mesh radio in the path back to the listed Root.
Radio Interface – This is the radio interface being used to reach the listed Root.
Bound – This indicates if the AP is bound to the Root AP listed in the Path table. The AP will not use the listed Root until it is bound. Bind states can be Bound, Unbound, Proxy Updated, Disfavored, or Removed.
Metric – This field indicates the path metric to the listed Root AP. This metric is the sum of all of the link metrics along each hop to the listed Root AP. The lower the number the better the metric.
Interface Bias – This field list the preferred interface if one has been set.
Neighbor Bias – This field lists the preferred neighbor if one has been set.
Root Bias – This field lists the preferred Root if one has been set.

4.5 Proxy Table

Mesh Point Name – This is the name of the configured mesh point on the AP being viewed.
Mesh Point ID – The Mesh Point ID is automatically chosen by MCX. For AP's configured with a single radio mesh this ID will be the BSSID of the mesh radio. On AP's that are running mesh on multiple radios the Mesh Point ID will be the BSSID of the radio that was added first. In most cases this will be done on startup and will be radio 1.
Proxy Address – This field lists the MAC address that is being proxied.
Age – This field indicates the time in seconds that have elapsed since the proxy was added.
Proxy Owner – This field indicates the AP which owns the proxy device.
VLAN – This field indicates the VLAN in which the proxy is using.

5. Terminology

- **Neighbor**: A Mesh Point that has been heard from via a beacon.
- **Link**: A connection between two Mesh Points.
- **Link Metric**: The *cost* of a specific link (i.e. expected time that will be taken to send a packet over this individual link). It is calculated for each link in the neighbor table.
- **Link Quality**: A measure of the probability of a packet being successfully received by the neighboring node. It is calculated for each link in the neighbor table.
- **Mesh Point Root (MPR)**: A Mesh Point with a wired connection to the core network / cloud.
- **Mesh Point (MP)**: An MCX instance that has been configured on an AP. This enables the AP to "*mesh" to* other AP's.
- **Path**: The link(s) being utilized to allow communications between two Mesh Points.
- **Path Metric**: Represents the *cost* of an entire end-to-end route. Route Metric is the sum of the individual Link Metric metrics of all the links that forms a path between a specific source and destination.
- **Proxy**: A non meshing device (e.g. camera or laptop) directly connected to a non Root Mesh Point.