Cisco Aironet 1500 Series Wireless Mesh AP
Version 5.0 Design Guide

Last revised: February 23, 2009

This document provides design guidance for the deployment of the Cisco Aironet 1500 Series Lightweight Outdoor Wireless Mesh Access Point (referred to subsequently as the Cisco 1500 Series Mesh AP or simply 1500 Series Mesh AP), which operates 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. Designed to support zero-configuration deployments, the Cisco 1500 Series Mesh AP 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 1500 Series Mesh AP provides end-to-end security.

Contents

Solution Overview 4
Outdoor Wireless Benefits 4
Outdoor Wireless Challenges 4
Solution Features and Benefits 4
Solution Components 6
Cisco 1500 Series Mesh AP 6
Cisco Wireless LAN Controllers 8
Wireless Control System (WCS) 9
Frequency Bands 10
Deployment Modes 13
Wireless Mesh 13
Wireless Backhaul 14
Solution Overview

This section provides an overview of the Cisco Aironet 1500 Series Wireless Mesh AP Version 4.1 solution.

Outdoor Wireless Benefits

The Cisco wireless mesh networking solution enables cost-effective and secure deployment of enterprise, campus, and metropolitan outdoor Wi-Fi networks. Standards-based wireless access takes advantage of the growing popularity of inexpensive Wi-Fi clients, enabling new service opportunities and applications that improve user productivity and responsiveness.

Outdoor Wireless Challenges

As the demand for outdoor wireless access increases, customers faced with tight budgets and reduced resources must respond with wireless LAN (WLAN) solutions that take full advantage of existing tools, knowledge, and network resources to address ease of deployment and WLAN security issues in a cost-effective way. An outdoor WLAN solution that excels in the unique attributes of wireless mesh technology, effectively supports current networking requirements, and lays the foundation for the integration of business applications is needed.

Outdoor wireless solutions offer a number of challenges, compared with a standard indoor WLAN, particularly in the following areas:

- Environment
- Coverage
- Total cost of ownership (TCO)

The outdoor environment is harsher than the indoor environment and therefore requires specialized equipment or enclosures to contain and protect indoor equipment that is deployed outdoors.

Outdoor deployments attempt to cover wider areas than indoor deployments. The main challenges for the outdoors are interference and finding a wired connection, although power is often available.

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

Solution Features and Benefits

The Cisco 1500 Series Mesh AP provides the following features and benefits:

- Self-configuring and self-healing mesh
The Cisco 1500 Series Mesh AP can be installed anywhere power is available, without the need for a network connection. Intelligent wireless routing is based on the Adaptive Wireless Path Protocol (AWPP), which is designed specifically for wireless environments. AWPP enables a remote access point to dynamically optimize the best route to the connected network within the mesh, providing resiliency to interference and helping ensure high network capacity.

Deployment and management costs for the 1500 Series Mesh AP are reduced through support of zero-configuration deployments and through the ability of the APs to self-heal in response to interference or outages. The 1500 Series Mesh AP can act as a relay node and can associate clients at the same time. The 1500 Series Mesh AP has a dedicated radio for the backhaul and another radio for the local access, allowing the mesh network to maximize use of the total available channels and minimize the occurrence of interference. This results in more capacity than is available with solutions that use only a single radio. When more capacity is needed, additional sectors can be enabled, such as provisioning a network connection to a remote access point. The mesh dynamically re-optimizes itself when this is done.

- **Zero-touch configuration**
  Using the Cisco Lightweight Access Point Protocol (LWAPP) features, the 1500 Series Mesh AP can discover its LWAPP controller and automatically download the correct configuration and software for its role in the wireless mesh network.

- **Cisco Adaptive Wireless Path Protocol (AWPP)**
  Wireless mesh networks have unique features and requirements, and to address these features and requirements, Cisco Systems has developed a new protocol, AWPP, which allows each node to determine its neighbor or parent intelligently, choosing the optimal path toward the controller. Unlike traditional routing protocols, AWPP takes RF details into account.
  The AWPP automatically determines the best path back to the LWAPP controller by calculating the cost of each path in terms of signal strength and number of hops. After the path is established, AWPP continuously monitors conditions and changes routes to reflect changes in conditions. AWPP also performs a smoothing function to signal condition information to ensure that the ephemeral nature of RF environments does not impact network stability.

- **Easy to deploy and manage**
  The Cisco wireless mesh solution brings all the ease of deployment and management of the Cisco Unified Wireless Solution to the wireless mesh solution.

- **Robust embedded security**
  A core component of the Cisco Unified Wireless solution is the use of X.509 certificates and AES encryption for LWAPP transactions. This X.509 and AES encryption is embedded into the wireless mesh solution with LWAPP transactions and all traffic between 1500 Series Mesh AP nodes being AES encrypted. The complete packet path is from the Cisco controller to APs, and eventually to the users. The controller encapsulates user packets and forwards them to the correct RAP over Ethernet. RAP then encrypts the user data packets and transfers them over the backhaul. Data packets might travel through multiple MAPs before reaching the destination MAP. After receiving the encrypted user data, the destination MAP decrypts them and sends them over the air to the client using the encryption method specified by the client.

- **Robust software**
  The Cisco Mesh solution provides robust, optimal parent selection and fast convergence. Cisco Mesh software contains mechanisms to guard against stranded AP conditions. The Cisco Mesh solution has a software-based recovery mechanism so the customer does not have to dispatch a technician to fix an AP problem. The network automatically recovers from misconfigurations, such as a wrong IP address, DHCP server errors, bridge group name typo's or misprovisioning of the
network. In addition, Cisco Systems has an exclusion list algorithm that allows the child node to intelligently put the parent node in the exclusion list and its future reuse would depend on the loyalty and history of the parent.

- **Provides seamless mobility**
  The same seamless mobility features delivered through the Cisco Unified Wireless solution are delivered in the wireless mesh solution.
- **Operates over Layer 2 or Layer 3 network**
  Just as the Cisco Unified Wireless solution allows the LWAPP APs to communicate with the controller via a Layer 2 or Layer 3 network, this flexibility is extended to the wireless mesh solution.
- **Highly scalable**
  The Cisco 1500 Series Mesh AP solution can scale to 24 controllers each with up to 16 MBSSIDs and 256 VLANs. Each 4400 controller can support more than 100 1500 Series Mesh APs. Capacity in a mesh network can be increased conveniently by adding MAPs at the edge of the network or configuring more RAPs in the network. This is covered in more detail in Controller Planning, page 44.
- **Identical indoor and outdoor policy management**
  The Cisco 1500 Series Mesh AP uses the same tools and features as other Cisco Unified Wireless solutions. The management platform, Wireless Control System (WCS), is a much stronger product that not only offers more advanced features, but is also more scalable. Up to 150 controllers and 2500 access points can be managed by a single WCS.

**Solution Components**

The Cisco Wireless Mesh solution has three core components:

- Cisco 1500 Series Mesh AP
- Cisco Wireless LAN controller
- Cisco Wireless Control System (WCS)

**Cisco 1500 Series Mesh AP**

The Cisco 1500 Series Mesh AP is the core component of the wireless mesh solution, and leverages existing and new features and functionality in the Wireless LAN controllers and the WCS.

The Cisco 1500 Series Mesh AP, as shown in Figure 1, is the primary component for outdoor bridging and wireless mesh solutions.
There are two types of Cisco 1500 Series Mesh APs:

- The AP1510—An outdoor access point consisting of two simultaneous operating radios:
  - One 2.4 GHz radio that is used for client access.
  - One 5.8/4.9 GHz radio that is used for data backhaul to other 1500 Series Mesh APs.
- The AP1505—An outdoor access point consisting of a single 2.4 GHz radio that is used for both backhaul and client access.
A wide variety of antennas that provide flexibility when deploying the 1500 Series Mesh AP over various terrains are available. The 5.8 GHz frequency radio uses 802.11a technology and is used in the system as the backhaul or relay radio. Wireless LAN client traffic passes either through the AP backhaul radio, or is relayed through other 1500 Series Mesh APs until it reaches the LWAPP controller Ethernet connection.

The 1500 Series Mesh AP also has a 10/100 Ethernet connection to provide bridging functionality. This Ethernet connection supports power over Ethernet (PoE) through a separate power injection system.

Note

The power injector is unique for this product; other Cisco power injection solutions are not suitable for use with the Cisco 1500 Series Mesh AP.

The Cisco 1500 Series Mesh AP uses LWAPP to communicate to a wireless controller and other 1500 Series Mesh APs in the wireless mesh.

The 1500 Series Mesh AP is designed to be mounted upside-down with its antennas pointed toward the ground, as shown in Figure 2.

**Figure 2** 1500 Series Mesh AP Installation

---

**Cisco Wireless LAN Controllers**

The wireless mesh solution is supported by the Cisco 2000 Series and Cisco 4400 Series Wireless LAN Controllers (WLCs). The Cisco 4400 Series WLC (see Figure 3) is recommended for wireless mesh deployments because it can scale to large numbers of access points, and can support both Layer 2 and Layer 3 LWAPP.
Wireless Control System (WCS)

The Cisco Wireless Control System (WCS) is the platform for wireless mesh planning, configuration, and management. It provides a foundation that allows network managers to design, control, and monitor wireless mesh networks from a central location.

With Cisco WCS, network administrators have a solution for RF prediction, policy provisioning, network optimization, troubleshooting, user tracking, security monitoring, and wireless LAN systems management. Graphical interfaces make wireless LAN deployment and operations simple and cost-effective. Detailed trending and analysis reports make Cisco WCS vital to ongoing network operations.

Cisco WCS runs on a server platform with an embedded database. This provides the scalability necessary to manage hundreds of WLCs, which in turn can manage thousands of Cisco lightweight access points. WLCs can be located on the same LAN as Cisco WCS, on separate routed subnets, or across a wide-area connection.

Figure 4 shows the interconnections between the controllers, WCS, and the 1500 Series Mesh APs.
**Frequency Bands**

The 5GHz Band is actually a conglomerate of three bands in the USA: 5.150-5.250(UNII 1), 5.250-5.350(UNII 2), and 5.725-5.875(UNII 3) GHz. UNII-1 and the UNII-2 bands are contiguous and are indeed treated by 802.11a as being a continuous swath of spectrum 200MHz wide, more than twice the size of the 2.4GHz ISM band (see Figure 5).

**Figure 5**

<table>
<thead>
<tr>
<th>Frequency Bands</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>US (FCC)</strong></td>
</tr>
<tr>
<td>Conducted</td>
</tr>
<tr>
<td>Power</td>
</tr>
<tr>
<td>Tx Output</td>
</tr>
<tr>
<td>Power</td>
</tr>
<tr>
<td>2 Channels</td>
</tr>
<tr>
<td>4.94</td>
</tr>
<tr>
<td>20dBm</td>
</tr>
<tr>
<td>4.99</td>
</tr>
<tr>
<td>5 Channels</td>
</tr>
<tr>
<td>5.15</td>
</tr>
<tr>
<td>5.25</td>
</tr>
<tr>
<td>5.35</td>
</tr>
<tr>
<td>4 Channels</td>
</tr>
<tr>
<td>5.470</td>
</tr>
<tr>
<td>24dBm</td>
</tr>
<tr>
<td>5.725</td>
</tr>
<tr>
<td>ISM 30dBm</td>
</tr>
<tr>
<td>5.825</td>
</tr>
<tr>
<td>4 Channels</td>
</tr>
<tr>
<td>5.850</td>
</tr>
<tr>
<td><strong>Europe</strong></td>
</tr>
<tr>
<td>Radiated</td>
</tr>
<tr>
<td>Power</td>
</tr>
<tr>
<td>EIRP (with</td>
</tr>
<tr>
<td>Antenna)</td>
</tr>
<tr>
<td>2 Channels</td>
</tr>
<tr>
<td>4.94</td>
</tr>
<tr>
<td>23dBm</td>
</tr>
<tr>
<td>4.99</td>
</tr>
<tr>
<td>23dBm</td>
</tr>
<tr>
<td>5.15</td>
</tr>
<tr>
<td>5.25</td>
</tr>
<tr>
<td>5.35</td>
</tr>
<tr>
<td>4 Channels</td>
</tr>
<tr>
<td>5.470</td>
</tr>
<tr>
<td>24dBm</td>
</tr>
<tr>
<td>5.725</td>
</tr>
<tr>
<td>UNI-3, 30dBm</td>
</tr>
<tr>
<td>5.825</td>
</tr>
<tr>
<td>30dBm</td>
</tr>
<tr>
<td><strong>Japan</strong></td>
</tr>
<tr>
<td>Hub Radios</td>
</tr>
<tr>
<td>Licensed</td>
</tr>
</tbody>
</table>

In addition to FCC, other main regulatory domains for operation in 5GHz are the European Telecommunications Standards Institute (ETSI), Japan, China (Mainland China), Israel, Singapore and Taiwan (Republic of China).

Refer to the Cisco web site for compliance information, and also verify with your local regulatory authority what is permitted within your country:


The ETSI recommended frequency band for bridging is 5.470 to 5.725 GHz offering almost eleven channels with the same EIRP rules as the FCC. In exchange of this wide spectrum, the ETSI recommendation mandates the inclusion of two features not currently found in 802.11 products, Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC). DFS and TPC are the two functions handled quite well by the HyperLAN2 specification. The IEEE 802.11h standard covers the DFS and TPC that will apply to the 5 GHz band.

Figure 6 shows the RF power (conducted) allowed in the 2.4 GHz band.
Figure 6 RF Power (Conducted) Allowed in the 2.4 GHz Band—A=America, E=Europe, J=Japan

Regulatory Domains
With up to 8 dBi 2.4 GHz Antennas

<table>
<thead>
<tr>
<th>Channel ID</th>
<th>Frequency (MHz)</th>
<th>Data Rate (Mbps)</th>
<th>1-1 CCK</th>
<th>6-36 OFDM</th>
<th>48 OFDM</th>
<th>54 OFDM</th>
<th>All</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>-A</td>
<td>-E</td>
<td>-P</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2400-2484  MHz</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>2412</td>
<td>23</td>
<td>19.5</td>
<td>19.5</td>
<td>19.5</td>
<td>14</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>2</td>
<td>2417</td>
<td>23.5</td>
<td>21.5</td>
<td>21.5</td>
<td>21</td>
<td>14</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>3</td>
<td>2422</td>
<td>24</td>
<td>23</td>
<td>22</td>
<td>21</td>
<td>14</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>4</td>
<td>2427</td>
<td>24</td>
<td>24</td>
<td>22</td>
<td>21</td>
<td>14</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>5</td>
<td>2432</td>
<td>24</td>
<td>24</td>
<td>22</td>
<td>21</td>
<td>14</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>6</td>
<td>2437</td>
<td>24</td>
<td>24</td>
<td>22</td>
<td>21</td>
<td>14</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>7</td>
<td>2442</td>
<td>24</td>
<td>24</td>
<td>22</td>
<td>21</td>
<td>14</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>8</td>
<td>2447</td>
<td>24</td>
<td>24</td>
<td>22</td>
<td>21</td>
<td>14</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>9</td>
<td>2452</td>
<td>24</td>
<td>24</td>
<td>22</td>
<td>21</td>
<td>14</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>10</td>
<td>2457</td>
<td>23.5</td>
<td>21.5</td>
<td>21.5</td>
<td>21</td>
<td>14</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>11</td>
<td>2462</td>
<td>23</td>
<td>19.5</td>
<td>19.5</td>
<td>19.5</td>
<td>14</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>12</td>
<td>2467</td>
<td>23</td>
<td>19.5</td>
<td>19.5</td>
<td>19.5</td>
<td>14</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>13</td>
<td>2472</td>
<td>23</td>
<td>19.5</td>
<td>19.5</td>
<td>19.5</td>
<td>14</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>14</td>
<td>2484</td>
<td>23</td>
<td>19.5</td>
<td>19.5</td>
<td>19.5</td>
<td>14</td>
<td>14</td>
<td>14</td>
</tr>
</tbody>
</table>

Figure 7 shows the antenna gains certified for use with the 1500 Series AP.

Figure 7 Antenna Gains Certified for Use with the 1500 Series AP

Antenna Gains Certified

<table>
<thead>
<tr>
<th>Frequency Band</th>
<th>Antenna Type</th>
<th>Max Gain</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4 GHz</td>
<td>Omni-Directional</td>
<td>8 dBi</td>
</tr>
<tr>
<td>4.9 to 5.850 GHz</td>
<td>Omni-Directional</td>
<td>7.5 dBi</td>
</tr>
<tr>
<td>4.9 to 5.850 GHz</td>
<td>Patch</td>
<td>14 dBi</td>
</tr>
<tr>
<td>5.4 to 5.850 GHz</td>
<td>Patch</td>
<td>17 dBi (for US)</td>
</tr>
</tbody>
</table>

Orderable Antennas

<table>
<thead>
<tr>
<th>Frequency Band</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIR-ANT2455V-N</td>
<td>2.4 GHz, 5.5 dBi Omni-Directional</td>
</tr>
<tr>
<td>AIR-ANT5175V-N</td>
<td>4.9 to 5.8 GHz, 7.5 dBi Omni-Directional</td>
</tr>
<tr>
<td>AIR-ANT58G10SSA-N</td>
<td>5.8 GHz, 9.5 dBi Sector</td>
</tr>
</tbody>
</table>

Figure 8 shows the additional third-party antennas supported with the 1500 Series AP.
Deployment Modes

The Cisco 1500 Series Mesh AP solution supports multiple deployment modes, including the following:

- Wireless mesh
- WLAN backhaul
- Point-to-multipoint wireless bridging
- Point-to-point wireless bridging

Wireless Mesh

In the wireless mesh deployment, there are multiple 1500 Series Mesh APs deployed as part of the same network, as shown in Figure 9.
Figure 9 Wireless Mesh Deployment

One or more of the 1500 Series Mesh APs have a wired connection to their WLC, and these are designated as rooftop mesh APs (RAPs). Other 1500 Series Mesh APs that relay their wireless connections to connect to the controller are called mesh access points (MAPs). The MAPs use the AWPP to determine the best path through other 1500 Series Mesh APs to their controller. The various possible paths between the MAPs and RAPs form the wireless mesh that is used to carry traffic from WLAN clients connected to MAPs in that mesh, and also to carry traffic from devices connected to the MAP Ethernet ports.

The WLAN mesh can simultaneously carry two different traffic types: WLAN client traffic and MAP Ethernet port traffic. WLAN client traffic terminates on the WLC, and the Ethernet traffic terminates on the Ethernet ports of the 1500 Series Mesh APs. Mesh membership in the WLAN mesh is controlled in a variety of ways. MAC authentication of the 1500 Series Mesh APs can be enabled to ensure that the APs are included in a database of APs authorized to use the WLAN controller. 1500 Series Mesh APs are configured with a shared secret for secure AP-to-AP intercommunication, and a bridge group name can be used to control mesh membership, or segmentation. The configuration of these features is described later in this document.

Wireless Backhaul

Cisco 1500 Series Mesh APs can provide a simple wireless backhaul solution, where the 1500 Series Mesh AP is used to provide 802.11b/g services to WLAN and wired clients. This configuration is basically a wireless mesh with one MAP. Figure 10 shows an example of this deployment type.
**Solution Overview**

**Figure 10  Wireless Backhaul Deployment**

Point-to-Multipoint Wireless Bridging

In the point-to-multipoint bridging scenario, a RAP acting as a root bridge connects multiple MAPs as non-root bridges with their associated wired LANs. By default, this feature is disabled for all MAPs. If Ethernet bridging is used, you must enable it on the controller for the respective MAP and for the RAP. Figure 11 shows a simple deployment with one RAP and two MAPs, but this configuration is fundamentally a wireless mesh with no WLAN clients. Client access can still be provided with Ethernet bridging enabled, although if bridging between buildings, MAP coverage from a high rooftop might not be suitable for client access.

**Figure 11  Wireless Point-to-Multipoint Bridge Deployment**

Point-to-Point Wireless Bridging

In a point-to-point bridging scenario, a 1500 Series Mesh AP can be used to extend a Layer 2 network by using the backhaul radio to bridge two segments of a switched network, as shown in Figure 12. This is fundamentally a wireless mesh network with one MAP and no WLAN clients. Just as in point-to-multipoint networks, client access can still be provided with Ethernet bridging enabled, although if bridging between buildings, MAP coverage from a high rooftop might not be suitable for client access.
If you intend to use an Ethernet bridged application, we suggested that you enable the bridging feature on the RAP and on all MAPs in that segment. Also verify that any attached switches to the Ethernet ports of your MAPs are not using VLAN Trunking Protocol (VTP). VTP can reconfigure the trunked VLANs across your mesh and possibly cause a loss in connection for your RAP to its primary WLC. If improperly configured, it can take down your mesh deployment.

**Solution Description**

The wireless mesh solution has the following three main components:

- LWAPP WLAN
- Wireless mesh bridge connections
- AWPP wireless mesh routing

**LWAPP WLAN**

The wireless mesh solution provides the same feature set to mesh WLAN clients as are provided by the Cisco Unified Wireless solution set for the indoor WLAN. Because the design and configuration of this solution is adequately covered in other documents, it is not addressed in this document.

**Wireless Mesh Connections**

The Ethernet ports of the 1500 Series Mesh AP are bridged with the wireless mesh, acting as a transparent bridge between all Ethernet ports of nodes within that mesh. For example, the simple mesh shown in Figure 13 results in a logical multi-port bridge of all Ethernet ports, as illustrated in Figure 14.
Figure 13  Simple Mesh Example

Figure 14  Wireless Mesh Virtual Multi-Port Bridge
Solution Description

Note that the controller does not participate in this bridging, and that the traffic terminates at the 1500 Series AP Ethernet port. Take care in mesh deployments to block unnecessary multicast traffic to prevent wireless backhaul capacity from being consumed unnecessarily.

Also note that for bridged traffic, the controller does not act as a central coordination point. The data traffic for the multipoint bridge is simply bridging traffic through the shortest path calculated by the AWPP.

The bridge network is transparent to dot1q and Spanning Tree protocols.

Mesh Authentication

When a 1500 Series Mesh AP comes up in a mesh, it uses its Primary Master Key (PMK) to authenticate to a parent or a neighboring 1500 Series Mesh AP. There is a four-way handshake using this primary key to establish an AES session. Next, the new AP establishes an LWAPP tunnel to the controller and is then authenticated against the MAC filter list of the controller.

Next, the controller pushes the bridge shared secret key to the AP via LWAPP, after which it re-establishes the AES session with the parent AP.

Wireless Mesh Encryption

As previously described, the wireless mesh bridges traffic between the MAPs and the RAPs. This traffic can be from wired devices being bridged by the wireless mesh, or LWAPP traffic from the mesh APs. This means that the wireless mesh could be carrying traffic that is either clear text or encrypted, depending on the wireless LAN settings and other overlaying applications; this traffic is always AES encrypted when it crosses a wireless backhaul link. The AES encryption is established as part of the Mesh AP establishing neighbor relationships with other Mesh APs. The bridge shared secret is used to establish unique encryption keys between mesh neighbors. All APs establish an LWAPP connection to the controller through AES-encrypted tunnels between APs.

Simple Mesh Deployment

The key components of the simple mesh deployment design (see Figure 13) are the following:

- **WCS**—Key component in the management, operation, and optimization of the mesh network.
- **LWAPP controller**—Controls the authentication and management of the 1500 Series Mesh AP and client WLANs.
- **Router between the network and the mesh**—Provides a Layer 3 boundary where security and policy enforcement can be applied.

The router also provides Layer 2 isolation of the RAP. This is necessary because the RAP bridges traffic from its local Ethernet port to the mesh, so this traffic must be limited to that necessary to support the solution so that resources are not consumed by the unnecessary flooding of traffic.

- **RAP**—Provides the “path” home for the MAP traffic
- **A number of MAPs**

Note that the RAP wireless connection is to the center of the MAP mesh, which is an optimal configuration that minimizes the average number of hops in the mesh. A RAP connection to the edge of a mesh would result in an increase of hops.

Figure 15 shows one possible logical view of the physical configuration shown in Figure 13, with MAP5 as the path home for all other MAPs.
Figure 16 shows an alternate logical view, in which the signal-to-noise ratio (SNR) on the diagonal paths to MAP5 is small enough for the MAPs to consider taking an extra hop to get to MAP5.
In both the cases above, MAP5 is the path home for all traffic. Ideally, the coverage from the RAP should be such that other MAPs, such as MAP2 for example, have a path back to the RAP, and traffic could be routed via MAP 2 in case of a loss of signal to MAP 5, as shown in Figure 17.
AWPP Wireless Mesh Routing

The introduction of wireless mesh brings with it a new routing protocol, the Cisco Adaptive Wireless Path Protocol (AWPP).

This protocol is designed specifically for wireless mesh networking in that its path decisions are based on link quality and the number of hops. AWPP is also designed to provide ease of deployment, fast convergence, and minimal resource consumption. AWPP takes advantage of the LWAPP WLAN, where client traffic is tunneled to the controller and is therefore hidden from the AWPP process. Also, the advance radio management features in the LWAPP WLAN solution are available to the wireless mesh network and do not have to be built into AWPP.

Cisco is a leading member of the Simple, Efficient, and Extensible Mesh (SEEMesh) consortium. The Cisco mesh model has become solidly embedded in one of the main contending proposals for the 802.11 task group, which is moving towards becoming a mesh standard for the industry. The combined design, known as Hybrid Wireless Mesh (routing) Protocol (HWMP), serves both the fixed type of deployments and the mobile deployments. HWMP is favored by other SEEMesh supporters because it combines low complexity with great flexibility. AWPP has been selected as the draft foundation for HWMP. Cisco Systems has taken a leading role in setting standards in the mesh field. The 802.11 standard is expected to be published by September of 2007.

Traffic Flow Within the Mesh

In Wireless Mesh Connections, page 15, a model of a virtual multi-port bridge is suggested for explaining how traffic is bridged across the wireless mesh. This model is equally applicable for traffic going to RAP and MAP MAC addresses as it is destined for MAC addresses connected to the RAPs or MAPs; that is, the 1500 Series Mesh AP builds a table of MAC addresses to associate with the peer in the mesh. It is by this table that the 1500 Series Mesh AP knows where to forward a frame, and AWP is used to build this table on each mesh AP.

An important point to remember is that the WLAN clients are not involved in AWP or the MAC address tables as they LWAPP tunnel to the controller, and the wireless mesh routing and addressing is transparent to the WLAN clients. The MAC address tables that are built by AWP contain only the MAC addresses of the 1500 Series Mesh APs, and wired clients connected to the 1500 Series Mesh APs.

Mesh Neighbors, Parents, and Children

A neighbor within a mesh is an AP that is within RF range that has not been selected as a parent or a child because its “ease” values are lower than another neighboring AP (refer to Ease Calculation, page 23).

A parent AP is one that is selected as the best route back to the RAP based on the best ease values. A parent can be either the RAP itself or another MAP. A child of an AP is an AP that has selected the parent AP as the best route back to the RAP. (See Figure 18.)
The goal of AWPP is to find the best path back to a RAP that is part of its bridge group name (BGN). To do this, the mesh AP actively solicits for neighbor APs. During the solicitation, the mesh AP learns all of the available neighbors back to a RAP, determines which neighbor offers the best path, and then synchronizes with that neighbor.

Figure 19 shows the state diagram for a mesh AP when it is trying to establish a connection.

Using release 4.0 software, the AWPP state machine has been optimized to offer better routing and convergence and reconvergence capabilities to AP1500 nodes. These optimizations enable faster channel scanning for neighbor nodes, discovering and constructing neighbor lists across all backhaul channels, selecting parent nodes from this list and quickly converging to a different parent on the same channel or a different channel in case of current parent failure.

The mesh AP must first decide whether it is a RAP. A mesh AP becomes a RAP if it can communicate with an LWAPP controller through its Ethernet interface. If the mesh AP is a RAP, it can go straight to the maintain state. In the maintain state, the mesh AP has established an LWAPP connection to the

---

**Figure 18**  **Parent, Child, and Neighbor**

![Parent, Child, and Neighbor](image)

**Figure 19**  **Mesh AP State Diagram**

![Mesh AP State Diagram](image)
controller so it does not need to seek other mesh APs, but simply responds to solicitations. If the mesh AP is not a RAP, it starts a scan process where the mesh AP scans all available channels and solicits information from other mesh APs.

This behavior has two main implications:

- The RAP does not change channels, and therefore the channel used to build the mesh from a RAP is defined in the RAP configuration. By default, the RAP uses channel 161 if it is an outdoor AP.
- The mesh is built from the RAP out, because initially only the RAP can respond to solicitations.

If the mesh AP is not a RAP, it follows the state diagram above in the following modes:

- **Scan**—The AP scans all the backhaul channels using mesh beaconing. This mechanism is similar to the 802.11 beaconing mechanisms used by wireless access networks, except the protocol frames conform to the AWPP frames on the backhaul. The frame used for beaconing is broadcast NEIGHBOR_RESPONSE called NEIGHBOR_UPDATE sent unsolicited.
- **Essentially, NEIGHBOR_UPDATE frames are advertised by the network so that new nodes can scan and quickly discover neighbors. The generation rule is that each RAP and MAP broadcast NEIGHBOR_UPDATE frames after being connected to the network (via a WLAN controller). Any neighbor updates with SNRs lower than 10 Db are discarded. This process is called passive scanning.
- **Seek**—Solicits for members of the mesh. Successful responses to these solicitations become neighbors. These neighbors must have only the same bridge group name and same shared secret.
- **Sync**—The mesh AP learns the path information from each of its neighbors, and the neighbor with the greatest ease becomes the parent of the soliciting mesh AP. If the neighbors report multiple RAPs, the RAP with the greatest ease is chosen.
- **Authenticate**—The mesh AP authenticates to the controller through a connection established through its parent AP. This AP authentication is standard LWAPP AP authentication, and the mesh AP is already part of the mesh and using the mesh to communicate with its LWAPP controller.
- **Maintain**—The mesh AP responds to other mesh AP solicitations, and regularly solicits to determine any changes in the mesh. It is only after entering the maintain state that the mesh AP is visible to the LWAPP controller and WCS. Note that in the maintain state, the solicitations occur only on the channel defined by the mesh RAP, whereas a mesh AP in seek mode solicits on all channels, only stopping when it has found a parent AP.

The passive scanning mechanism enables a new mesh node to scan through all available channels and discover neighbors who might belong to different sectors. A typical mesh backhaul design should be around per-sector channel allocation. In such a design, if the new node does not belong to a particular sector, it can quickly move to other channels which are likely to have neighbors of its compatible sector. If a mesh backhaul is designed around different sectors with the same bridge group name and different channels, the passive scanning mechanism is also useful for nodes in the bordering areas of the sectors where there might be closely comparable neighbors on different channels.

The passive scanning mechanism using mesh beacons is efficient because it minimizes the amount of time spent on each channel, minimizes the number of channels sought by the Optimal Parent Selection (OPS) algorithm, and turns around scanning results quickly for later states of the AWPP state machine. Despite consuming periodic airtime, the mechanism brings significant benefits to the 802.11 backhaul radio with omni antennas.

### Choosing the Best Parent

The OPS algorithm is implemented in the Seek state of the AWPP state machine. The basic idea of the parent selection in the new AWPP is as follows for both a RAP or MAP with radio backhaul:
A list of channels with neighbors is generated by passive scanning in the Scan state, which is a subset of all backhaul channels.

The channels with neighbors are sought by actively scanning in Seek state and the backhaul channel is changed to the channel with the best neighbor.

The parent is set to the best neighbor and the parent-child handshake is completed in Seek state.

Parent maintenance and optimization occurs in the Maintain state.

All AWPP parent selection metrics remain unchanged from the pre-release 4.0 implementation. This algorithm is run at startup and whenever a parent is lost and no other potential parent exists, usually followed by an LWAPP network and controller discovery. All neighbor protocol frames carry the channel information. Both parent maintenance and optimization techniques remain unchanged, as described in the following paragraphs, for completion.

Parent maintenance occurs by the child node sending a directed NEIGHBOR_REQUEST to the parent and the parent responding with a NEIGHBOR_RESPONSE.

Parent optimization and refresh occurs by the child node sending a NEIGHBOR_REQUEST broadcast on the same channel it has a parent on, and evaluating all responses from neighboring nodes on this channel. Until background scanning is implemented, off-channel optimization cannot occur. However, in most practical mesh networks, only a single channel backhaul is designed, especially with the current AP1500. Therefore, this should not be an issue except in a network where the same bridgegroupname is used across sectors and there are MAPs in bordering regions of the sectors.

A parent AP is the AP that has best path back to a RAP. AWPP uses ease to determine the best path. Ease can be considered the opposite of cost, and the preferred path is the path with the higher ease.

**Ease Calculation**

Ease is calculated using the SNR and hop value of each neighbor, and applying a multiplier based on various SNR thresholds. The purpose of this multiplier is to apply a spreading function to the SNRs that reflects various link qualities.

In Figure 20, MAP2 prefers the path through MAP1 because the adjusted ease (436906) though this path is greater then the ease value (262144) of the direct path from MAP2 to RAP.

### Figure 20   Parent Path Selection

A parent AP is chosen by using the adjusted ease, which is the ease of each neighbor divided by the number of hops to the RAP:

$$\text{adjusted ease} = \min \left( \frac{\text{ease at each hop}}{\text{Hop count}} \right)$$

**Parent Decision**

A parent AP is chosen by using the adjusted ease, which is the ease of each neighbor divided by the number of hops to the RAP:
SNR Smoothing

One of the challenges in WLAN routing is the ephemeral nature of RF. This must be considered when analyzing an optimal path and deciding when a change in path is required. The SNR on a given RF link can change substantially from moment to moment, and changing route paths based on these fluctuations results in an unstable network, with severely degraded performance. To effectively capture the underlying SNR but remove moment-to-moment fluctuations, a smoothing function is applied that provides an adjusted SNR.

In evaluating potential neighbors against the current parent, the parent is given 20% of “bonus-ease” on top of the parent’s calculated ease, in order to reduce the ping-pong effect between parents. This implies that a potential parent must be significantly better in order for a child to make a switch. Parent switching is transparent to LWAPP and other higher-layer functions.

Loop Prevention

To ensure that routing loops are not created, AWP discards any route that contains its own MAC address. That is, routing information apart from hop information contains the MAC address of each hop to the RAP; therefore, a 1500 Series Mesh AP can easily detect and discard routes that loop.

CLI Commands

The LWAPP controller on the WCS provides a number of views of the wireless mesh state. The following controller commands are useful for viewing the wireless mesh:

- `show mesh path`
- `show mesh summary`
- `show mesh neigh`
- `show mesh stats`
- `show mesh linkrate`
- `show mesh range`

These commands use the AP name as input. The AP names can be found using the `show AP summary` command:

```
(Cisco Controller) >show ap summary

AP Name             Slots  AP Model             Ethernet MAC       Location
------------------  -----  -----------------   -----------------  ----------------
Rap:5f:fb:10         2     AP1500              00:0b:85:5f:fb:10  default_location 1
Map1:5c:b9:20        2     AP1500              00:0b:85:5c:b9:20  default_location 1
Map2:5f:fa:60        2     AP1500              00:0b:85:5f:fa:60  default_location 1
Map3:5f:ff:60        2     AP1500              00:0b:85:5f:ff:60  default_location 1
```

Note how the AP names in this example are a combination of a meaningful name and the AP MAC address. This is a recommended practice because it makes it easier to find a particular AP among a list of MAC addresses.

show mesh path

The following is an example of the `show mesh path` command, where the path through the wireless mesh from a mesh AP to the RAP is given:

```
(Cisco Controller) >show mesh path Rap:5f:fb:10
00:0b:85:5f:ff:60 is RAP
```

```
**Solution Description**

(Cisco Controller) > `show mesh path Map1:5c:b9:20`
00:08:5F:FB:10 state UPDATED NEIGH PARENT BEACON (86B), snrUp 65, snrDown 56, linkSnr 51
00:08:5F:FB:10 is RAP

(Cisco Controller) > `show mesh path Map2:5f:fa:60`
00:08:5F:FB:10 state UPDATED NEIGH PARENT BEACON (86B), snrUp 72, snrDown 63, linkSnr 56
00:08:5F:FB:10 is RAP

**Note**

The difference in the uplink and downlink SNRs should not be greater than 10 decibels. If it is more than 10 decibels then changing the channel might solve the problem. A spectrum analyzer can also be used to provide greater insight into RF issues.

**show mesh summary**

The following are examples of the `show mesh summary` command for both a RAP and a MAP.

Notice that the RAP has only children, and a MAP has at least a parent but can also have children.

(Cisco Controller) > `show mesh summary Rap:5f:fb:10`
00:0B:85:1B:78:90 state DEFAULT (1060), snrUp 0, snrDown 5, linkSnr 0
00:0B:85:5C:33:20 state (60), snrUp 0, snrDown 10, linkSnr 0
00:0B:85:5C:B9:20 state CHILD (160), snrUp 0, snrDown 55, linkSnr 0
00:0B:85:5F:FA:60 state CHILD (160), snrUp 0, snrDown 63, linkSnr 0
00:0B:85:5F:FF:60 state (60), snrUp 0, snrDown 6, linkSnr 0

(Cisco Controller) > `show mesh summary Map1:5c:b9:20`
00:08:51:B7:98:90 state UPDATED (61), snrUp 14, snrDown 15, linkSnr 15
00:08:5B:1B:79:90 state DEFAULT (1061), snrUp 0, snrDown 7, linkSnr 0
00:08:5B:5C:1E:10 state NEEDUPDATE (260), snrUp 9, snrDown 13, linkSnr 9
00:08:5B:5C:33:20 state UPDATED CHILD (161), snrUp 20, snrDown 22, linkSnr 12
00:08:5B:5F:FA:60 state UPDATED NEIGH BEACON (869), snrUp 45, snrDown 51, linkSnr 50
00:08:5B:5F:FB:10 state UPDATED NEIGH PARENT BEACON (86B), snrUp 66, snrDown 55, linkSnr 51
00:08:5B:5F:FF:60 state UPDATED BEACON (861), snrUp 7, snrDown 2, linkSnr 1

In the output from this command, the snrUP is how this AP sees its received-signal-strength-indication (RSSI) from its neighbor. snrDown is what that neighbor is reporting back as its RSSI to the AP. The linkSnr is a weighed and filtered measurement based on the snrUp value. Note that snrUp and linkSnr is zero (0) for the RAPs.

**show mesh neigh**

The following are examples of the `show mesh neigh` command. The child AP sample shows the examples of the information used by AWPP, showing the ease values, and the vector information that gives the path back to the RAP.

(Cisco Controller) > `show mesh neigh poletop:7a:70`

AP MAC : 00:0B:85:1B:78:90

FLAGS : 161 UPDATED CHILD
worstDv 255, Ant 0, channel 0, biters 0, ppiers 10
Numroutes 1, snr 0, snrUp 37, snrDown 35, linkSnr 32
adjustedEase 0, unadjustedEase 0
Solution Description

### show mesh stats

The following is an example of the `show mesh stats` command where traffic statistics for a given mesh AP are given.

```
(Cisco Controller) >show mesh stats MAP:03:70
AP MAC : 00:0B:85:53:03:70
Poletop AP in state Maint
rxNeighReq 840151, rxNeighRsp 938730
txNeighReq 315153, txNeighRsp 840151
tnextchan 0, nextant 0, downAnt 0, downChan 0, curAnts 0
tnextNeigh 1, malformedNeighPackets 0, poorNeighSnr 52174
blacklistPackets 0, insufficientMemory 0
authenticationFailures 0
Parent Changes 4, Neighbor Timeouts 21
```

### show mesh linkrate

The following is an example of the `show mesh linkrate` command where the SNR and bit rates between mesh APs are shown.

```
(Cisco Controller) >show mesh linkrate Rooftop:D6:80 poletop:7a:70
MAC : 00:0B:85:18:7A:70
State : assoc|joined
RxSignalStrength : 29   AckSignalStrength : 29
Rx Data Rate : 18        Tx Data Rate : 18

(Cisco Controller) >show mesh linkrate poletop:7a:70 poletop 78:90
MAC : 00:0B:85:18:1B:78:90
State : assoc|joined
RxSignalStrength : 35   AckSignalStrength : 35
Rx Data Rate : 18        Tx Data Rate : 18
```
Note

In this example, the rooftop is the source and the pole top is the destination.

This command is not used extensively. If you enter the `show mesh linkrate` command several times in succession, you will see the rates change from 6mbps to 18mbps and 12mbps (ACKs). 6 Mbps is the data rate for LWAPP, 18 Mbps is the data rate for backhaul data, and 12 Mbps is the rate for acknowledgements.

**show mesh range**

With the software releases prior to release 4.0 (4.0.155.0), there was a hard-coded bridging distance limitation of 12000 feet (2.25 miles) between the 1500 Series Mesh APs, even though the radio had a capability to go much further in distance. This distance limitation has been removed in the release 4.0 software release. The distance is configurable up to 132,000 feet (25 miles):

(Cisco Controller) >config mesh
range range from RAP to MAP Cisco Bridge (150..132000)

The default setting for range is 12000 feet. When you change the setting, the access points reboot (RAP and MAPs). Use the `show mesh range` command to view the settings:

(Cisco Controller) >show mesh range
MESH Range 14000

**Traffic Flow**

The traffic flow within the wireless mesh can be divided into the following three components:

- Overlay LWAPP traffic that flows within a standard LWAPP AP deployment; that is, LWAPP traffic between the LWAPP AP and the LWAPP controller.
- Wireless mesh data frame flow.
- AWP protocol exchanges.

Because the LWAPP model is well known and the AWP protocol is proprietary, only the wireless mesh data flow is described. The key to the wireless mesh data flow is the address fields of the 802.11 frames being sent between mesh APs.

An 802.11 data frame can use up to four address fields: receiver, transmitter, destination, and source. The standard frame from a WLAN client to an AP uses only three of these address fields because the transmitter address and the source address are the same. However, in a WLAN bridging network, all four address fields are used because the source of the frame might not be the transmitter of the frame, because the frame might have been generated by a device “behind” the transmitter.

**Figure 21** shows an example of this type of framing. The source address of the frame is MAP:03:70, the destination address of this frame is the controller (the mesh is operating in Layer 2 mode), the transmitter address is MAP:D5:60, and the receiver address is RAP:03:40.
As this frame is sent, the transmitter and receiver addresses change on a hop-by-hop basis. AWP is used to determine the receiver address at each hop. The transmitter address is known because it is the current AP. The source and destination addresses are the same over the entire path.

Note that if the RAP controller connection is Layer 3, the destination address for the frame is the default gateway MAC address, because the MAP has already encapsulated the LWAPP in IP to be sent to the controller, and is using the standard IP behavior of using ARP to find the MAC address of the default gateway.

Each AP within the mesh forms an LWAPP session with a controller. WLAN traffic is encapsulated inside LWAPP and is mapped to a VLAN interface on the controller. Bridged Ethernet traffic can be passed from each Ethernet interface on the mesh and does not have to be mapped to an interface on the controller. (See Figure 22.)
Design Details

Each outdoor wireless mesh deployment is unique, and each environment has its own challenges with available locations, obstructions, and network infrastructure availability, in addition to the design requirements based on users, traffic, and availability. This section describes important design considerations and provides an example of a wireless mesh design.

Wireless Mesh Constraints

When designing and building a wireless mesh network with the 1500 Series Mesh AP, there are a number of system characteristics to consider. Some of these apply to the backhaul network design and others to the LWAPP controller design:

- Recommended backhaul is 18 Mbps

18 Mbps 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 18 Mbps backhaul should allow for seamless WLAN client coverage between the MAPs.

A lower bit rate might allow a greater distance between 1500 Series Mesh APs, 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 1500 Series Mesh APs, or results in a reduced SNR between mesh APs, limiting mesh reliability and interconnection.

The wireless mesh backhaul bit rate, like the mesh channel, is set by the RAP.

The required minimum LinkSNR for backhaul links per data rate is shown in Table 1.

<table>
<thead>
<tr>
<th>Data Rate</th>
<th>Minimum Required LinkSNR (dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>54 Mbps</td>
<td>Not supported</td>
</tr>
<tr>
<td>48 Mbps</td>
<td>Not supported</td>
</tr>
<tr>
<td>36 Mbps</td>
<td>26</td>
</tr>
<tr>
<td>24 Mbps</td>
<td>22</td>
</tr>
<tr>
<td>18 Mbps</td>
<td>18</td>
</tr>
<tr>
<td>12 Mbps</td>
<td>16</td>
</tr>
<tr>
<td>9 Mbps</td>
<td>15</td>
</tr>
<tr>
<td>6 Mbps</td>
<td>14</td>
</tr>
</tbody>
</table>

- The required minimum LinkSNR is driven by the data rate and the following formula: Minimum SNR + fade margin. Table 2 summarizes the calculation by data rate.
  - 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 18 Mbps in municipal mesh deployments as the SNR requirements do not make the distances practical
Table 2  Minimum Required LinkSNR Calculations by Data Rate

<table>
<thead>
<tr>
<th>Date Rate</th>
<th>Minimum SNR (dB) +</th>
<th>Fade Margin =</th>
<th>Minimum Required LinkSNR (dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>5</td>
<td>9</td>
<td>14</td>
</tr>
<tr>
<td>9</td>
<td>6</td>
<td>9</td>
<td>15</td>
</tr>
<tr>
<td>12</td>
<td>7</td>
<td>9</td>
<td>16</td>
</tr>
<tr>
<td>18</td>
<td>9</td>
<td>9</td>
<td>18</td>
</tr>
<tr>
<td>24</td>
<td>13</td>
<td>9</td>
<td>22</td>
</tr>
<tr>
<td>36</td>
<td>17</td>
<td>9</td>
<td>26</td>
</tr>
</tbody>
</table>

- **Number of backhaul hops is limited to eight, but three to four is recommended**
  The number of hops is recommended to be limited to three–four primarily to maintain sufficient backhaul throughput, because each mesh AP uses the same radio for transmission and reception of backhaul traffic. This means that throughput is approximately halved over every hop. For example, the maximum throughput for an 18 Mbps is approximately 10 Mbps for the first hop, 5 Mbps for the second hop, and 2.5 Mbps for the third hop.

- **Number of MAPs per RAP**
  There is no current software limitation of how many MAPs per RAP you can configure. However, it is suggested that you limit this to 20 MAPs per RAP.

- **Number of APs per controller**

- **Number of controllers**
  The number of controllers per mobility group is limited to 24.

**Client WLAN**

The mesh AP client WLAN delivers all the WLAN features derived by a standard LWAPP deployment for b/g clients with the full range of security and radio management features.

The goals of the client WLAN must be considered in the overall mesh deployment:

- What bit rates are required?
  - Higher bit rates reduce coverage and are limited by the mesh backhaul

- What throughput is required?
  - What are the application throughput requirements, and how many simultaneous clients are expected on a Cisco 1500 Series Mesh AP?

- What coverage is required?
  - Is the coverage between different 1500 Series Mesh APs required to be contiguous, or is the mesh deployment a collection of separate active zones?

**QoS Features**

Cisco supports 802.11e on the local access and on the backhaul. The mesh APs prioritize user traffic based on classification, and therefore all user traffic is treated on a best-effort basis.
We do not generally recommend that QoS profiles be applied to users of the mesh network. 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 attend 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 1500, 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).

**Encapsulations**

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

There are two encapsulations between the controller and the RAP. The first is for LWAPP control, and the second for LWAPP data. In the control instance, LWAPP is used as a container for control information and directives. In the instance of LWAPP data, the entire packet, including the Ethernet and IP headers, is sent in the LWAPP container (see Figure 23).
For the backhaul, there is only one type of encapsulation, encapsulating MESH traffic. However, two types of traffic are encapsulated: bridging traffic and LWAPP 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 Figure 24).

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

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

**Queuing on the Access Point**

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 1500 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 LWAPP control traffic, 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 voice applications.

Frames destined for Ethernet are queued as FIFO, up to the maximum available transmit buffer pool (256 frames). With 4.0.155.0 support for Layer 3 IP Differentiated Services Code Point (DSCP), marking of the packets has been added.

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 Figure 25).

![Figure 25 Controller to RAP Path](image)

For LWAPP control traffic 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 Table 3.

### Table 3 Backhaul Path QoS

<table>
<thead>
<tr>
<th>DSCP Value</th>
<th>Backhaul Queue</th>
</tr>
</thead>
<tbody>
<tr>
<td>2, 4, 6, 8-23</td>
<td>Bronze</td>
</tr>
<tr>
<td>26, 32-63</td>
<td>Gold</td>
</tr>
<tr>
<td>None</td>
<td>Platinum</td>
</tr>
<tr>
<td>All others, including 0</td>
<td>Silver</td>
</tr>
</tbody>
</table>

**Note**

The platinum backhaul queue is reserved for LWAPP control traffic and IP control traffic, and other important traffic. DHCP and ARP requests are also transmitted at the platinum QoS level. The mesh software inspects each frame to determine whether it is an LWAPP control or IP control frame in order to protect the platinum queue from use by non-LWAPP 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 Table 4).

### Table 4  MAP to Client Path QoS

<table>
<thead>
<tr>
<th>DSCP Value</th>
<th>Backhaul Queue</th>
</tr>
</thead>
<tbody>
<tr>
<td>2, 4, 6, 8-23</td>
<td>Bronze</td>
</tr>
<tr>
<td>26, 32-45, 47</td>
<td>Gold</td>
</tr>
<tr>
<td>46, 48-63</td>
<td>Platinum</td>
</tr>
<tr>
<td>All others, including 0</td>
<td>Silver</td>
</tr>
</tbody>
</table>

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 Access Point, there are modifications made to incoming client frames in preparation for transmission on the mesh backhaul or Ethernet. For WMM clients, Figure 26 illustrates the way in which the outer DSCP value is set from an incoming WMM client frame.

### Figure 26  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 Table 5 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 5  802.11e User Priority to DSCP Mapping

<table>
<thead>
<tr>
<th>IEEE 802.11e User Priority</th>
<th>DSCP Value in the Outer LWAPP Header</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>16</td>
</tr>
<tr>
<td>3</td>
<td>24</td>
</tr>
<tr>
<td>4</td>
<td>32</td>
</tr>
<tr>
<td>5</td>
<td>40</td>
</tr>
<tr>
<td>6</td>
<td>48</td>
</tr>
<tr>
<td>7</td>
<td>56</td>
</tr>
</tbody>
</table>
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 LWAPP control frame, the DSCP value of 46 is placed in the outer header.

Now that the DSCP value is determined, the rules described earlier for the back haul 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 LWAPP 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-LWAPP 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 AP1500 and 802.11a is by tagging Ethernet packets with DSCP. The AP1500 will take the Ethernet packet with DSCP and will place it in the appropriate 802.11e queue.

The 1500 does not tag DSCP itself:

- On the ingress port, the 1510 sees a DSCP tag and will encapsulate the Ethernet frame and apply the corresponding 802.11e priority.
- On the egress port, the 1510 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.

### Doppler Effect

Doppler has no measurable impact on the UDP throughput up to a velocity of 36,000km/h. For higher velocities, the throughput first decreases to 1Mbit/s. Connections are lost at a velocity of > 92,000 km/h, as shown in Figure 27.
Design Example

This section provides an example of a design for WLAN coverage in an urban or suburban area, adhering to the compliance conditions for United States domain.

Cell Planning and Distance

The starting point is the RAP-to-MAP ratio. There is currently no hard limitation of MAPs per RAPs, but the current recommended maximum number is 20 MAPs per RAP. For the backhaul, there is a typical cell size radius of 1000 feet. One square mile in feet is 5280^2 square feet, so the number of cells comes out to be nine, and you can cover one square mile with approximately three or four hops. (See Figure 28 and Figure 29.)
For 2.4 GHz, the local access cell size radius is 600 feet. One cell size comes out to be $1.310 \times 10^6$ square feet, so the number of cells is 25 per square mile. (See Figure 30 and Figure 31.)
Figure 30 600 Feet

600 feet (typical distance)

One square mile, 25 cells

Figure 31 Path Loss Exponent 2.5 to 3.0

Figure 32 shows a schematic of the wireless mesh layout.
The RAP shown in Figure 32 is simply a place holder; the goal is to use the RAP location in combination with RF antenna design to ensure that there is a good RF link to the MAPs within the core of the cell. This means that the physical location of the RAP could be on the edge of the cell, and a directional antenna is used to establish a link into the center of the cell. This means that the wired network location for a RAP might play host to the RAPs of multiple cells, as shown in Figure 33.

When the basic cell composition is settled, the cell can be replicated to cover a greater area. When replicating the cells, a decision needs to be made whether to use the same backhaul channel on all cells or to change backhaul channels with each cell. In the example shown in Figure 34, various backhaul channels per cell have been chosen to reduce the co-channel interference between cells.
Choosing various channels reduces the co-channel interference at the cell boundaries, at the expense of faster mesh convergence, because MAPs must fall back to seek mode to find neighbors in adjacent cells. In areas of high traffic density, co-channel interference has the highest impact, and this is likely to be around the RAPs. If RAPs are clustered in one location, a different channel strategy is likely to give optimal performance; if RAPs are dispersed among the cells, using the same channel is less likely to degrade performance.

When laying out multiple cells, use channel planning similar to standard WLAN planning to avoid overlapping channels, as shown in Figure 35. If possible, the channel planning should also minimize channel overlap in cases where the mesh has expanded to cover the loss of a RAP connection, as shown in Figure 36.
Figure 35  Laying out Various Cells

Figure 36  Failover Coverage

Figure 37 and Figure 38 compare radio cell sizes using a single radio (1505) AP and a dual band (1510) AP.
When deploying a dual band AP versus a single band AP, the AP density (number per square mile) is driven by the access system gain. Therefore, single and dual band APs can be spaced approximately the same with a few exceptions.

Capacity with single band APs is half that with dual band APs.

To achieve similar capacity with the 1505 as with the 1510, more RAPs are needed. Because of the RAP locations typically being elevated above the mesh, interference and noise is now more of a concern, and the first hop distance may be shorter for the AP 1505, so more RAPs may be needed. In addition, because the backhaul and access is now shared, dividing the throughput virtually in half to a single user, more
RAPs are needed to ensure throughput. Aggregate bandwidth is also being divided in the case of the AP 1505 because backhaul and access is shared. All these factors lead to the requirement for more RAPs/APs in a square mile.

The 2.4 GHz band does provide better propagation characteristics, but 2.4 GHz is an unlicensed band and has historically been affected with more noise and interference to date than the 5 GHz band. In addition, because there are only three backhaul channels in 2.4 GHz, co-channel interference would result. Therefore, the best method to achieve comparable capacity is by reducing system gain (that is, transmit power, antenna gain, receive sensitivity, and path loss) to create smaller cells. Keep in mind that these smaller cells require more APs per square mile (greater AP density).

How do these cell sizes scale when lower power is used; for example, in the EMEA domain?

The EIRP allowed for EMEA for the 1500 Series AP is approximately 10 dB lower than for a North American 1500, typically 20 dBm versus 30 dBm. This is because of ETSI versus FCC regulations, which can result in only half the range when assuming a propagation exponent of 3.5. However, this pertains only to the downlink; that is, the AP transmitting to the client receiving. Because the range is typically uplink limited, and a typical client has less than 20 dBm EIRP (typically 14 to 17 dBm conducted with about 0 dBi antenna gain), Cisco believes that the EMEA AP density is about the same as the North American AP density.

For example, the assumptions for calculations are as follows:

- Client conducted transmit power—14 dBm
- Client antenna gain—0 dBi
- Client receive sensitivity— -70 dBm for 54 Mbps
- AP receive sensitivity— -72 dBm for 54 Mbps
- System Gain = Transmit Power + Transmit Antenna Gain + Receive Antenna Gain - Receive Sensitivity

**ETSI Reg Domain (20 dBm Maximum EIRP)**

- 5 dBi gain antenna on AP:
  - UL system gain—14 dBm + 0 dBi + 5 dBi - (-72 dBm) = 91 dB
  - DL system gain—14 dBm + 5 dB + 0 dB - (-70 dBm) = 89 dB

  **Note** Range is downlink-limited by 2 dB.

- 8 dBi gain antenna on AP:
  - UL system gain—14 dBm + 0 dBi + 8 dB - (-72 dBm) = 94 dB
  - DL system gain—11 dBm + 8 dB + 0 dB - (-70 dBm) = 89 dB

  **Note** Range is downlink-limited by 5 dB.

The conclusion for ETSI is that the 8 dBi antenna provides the best uplink system gain but the range is limited by the downlink in both cases.

**North American Reg Domain (36 dBm Maximum EIRP)**

- 5 dBi gain antenna on AP
- UL system gain—14 dBm + 0 dBi + 5 dBi - (-72 dBm) = 91 dB
- DL system gain—24 dBm + 5 dBi + 0 dBi - (-70 dBm) = 99 dB

Note: Range is uplink-limited by 8 dB.

- 8 dBi gain antenna on AP
  - UL system gain—14 dBm + 0 dBi + 8 dBi - (-72 dBm) = 94 dB
  - DL system gain—24 dBm + 8 dBi + 0 dBi - (-70 dBm) = 102 dB

Note: Range is uplink limited by 8 dB.

The conclusion for N.A is that the 8 dBi antenna provides the best downlink and uplink system gain, but the range is limited by the uplink in both cases.

Comparison between North American System Gain and ETSI System Gain

- ETSI systems are downlink-limited, North American systems are uplink limited;
- 8 dBi antennas increase range in both regulatory domains, but only in the uplink in the ETSI systems;
- With 5 dBi antennas, the worst case system gain, when considering both uplink and downlink, is 2 dB worse in ETSI systems compared to North American systems, which equates to 12 percent less range when assuming a propagation exponent of 3.5.
- With 8 dBi antennas, the worst case system gain, when considering both uplink and downlink, is 5 dB worse in ETSI systems compared to North American systems, which equates to 28 percent less range when assuming a propagation exponent of 3.5.

Controller Planning

At a maximum, you can have 24 controllers in a mobility group, and the current maximum number of non-Mesh APs per controller is 100. With 24 controllers, this provides a maximum of 2400 APs (see Figure 39).

For clarity, non-Mesh APs are referred to as normal APs in this document.

The ground rule is that MAP is counted as half the AP, and the RAP is counted as a full normal AP for the controller.

\[ X + 0.5 \ Y = \text{Supported AP Count} \]

Key: \( X = \text{RAP}, \ Y = \text{MAP} \)
Another parameter that should be kept in mind is the “network device limit.” This is an upper-ceiling value found in controllers, which is related to CPU usage. The network device limit for the 4404 Series controllers is 150 Aps. Therefore, the total number of APs (either RAP or a MAP) cannot exceed 150. If you are planning a network with one RAP, then you cannot have more than 149 MAPs. If the network device limit did not apply, then you could have 99 X 2 = 198 MAPs.

In most cases, the full controller capacity is not normally used in this manner, because some of the controllers are used to increase availability; for example, an n+1 system with 23 active controllers and one controller providing backup services.

Other factors that impact the total number of APs are the wired network connecting the RAPs and controllers. If this network allows the controllers to be equally available to all APs without any impact on WLAN performance, the APs can be evenly distributed across all controllers for maximum efficiency. If this is not the case, and controllers are grouped into various clusters or PoPs, the overall number of APs and therefore coverage are reduced.

For example, you can have 24 4400 Series controllers in a mobility group, and each 4400 Series controller supports 100 normal APs. This gives a total number of 2400 possible APs per mobility group.

**Multiple Wireless Mesh Mobility Groups**

Keep in mind that wireless mesh built by the maximum number of controllers in a mobility group is not truly the maximum size of WLAN coverage because this is simply the maximum size of the mobility group. The WLANs that are part of a mobility group can be replicated in another mobility group, and a WLAN client is able to roam between these mobility groups.

When roaming between mobility groups, the roaming can be Layer 2 roaming or Layer 3 roaming, depending on the network topology behind the wireless mesh networks.
Increasing Mesh Availability

In the previous section, a wireless mesh cell of one square mile was created and then built upon. This wireless mesh cell has similar properties to the cells used to create a cellular phone network; that is, although the technology might define the maximum size of the cell, smaller cells can be created to cover the same physical area, providing greater availability or capacity. This is done by adding RAPs to the cell. Just as in the larger mesh deployment, the decision is whether to use RAPs on the same channel, as shown in Figure 40, or to use different channels, as shown in Figure 41. The addition of RAPs into an area adds capacity and resilience to that area.

Figure 40  Two RAPs per Cell with the Same Channel
Layer 2 or Layer 3 Encapsulation

It is generally recommended that Layer 3 encapsulation be used because it gives greater flexibility in RAP and controller placement. Even if it is possible to put the RAP and its associated controllers on the same subnet, Cisco recommends that the RAP and the controllers be separated by a router hop, because this controls the Layer 2 traffic going into the RAP Ethernet interface, and simplifies the network design if more RAPs or controllers need to be added.

Multiple RAPs

If multiple RAPs are to be deployed, the purpose for deploying these RAPs needs to be considered. If the RAPs are being deployed to provide hardware diversity, the additional RAP(s) should be deployed on the same channel as the primary RAP to minimize the convergence time in a scenario where the mesh transfers from one RAP to another. When planning RAP hardware diversity, the 32 MAPs per RAP limitation should be remembered.

If the additional RAPs are being deployed to primarily provide additional capacity, the additional RAPs should be deployed on a different channel to its neighboring RAPs to minimize the interference on the backhaul channels.

Adding the second RAP on a different channel also reduces the collision domain through channel planning or through root AP (RAP) cell splitting. Channel planning allocates different non-overlapping channels to mesh nodes in the same collision domain to minimize the collision probability. RAP cell splitting is a simple, yet effective, way to reduce the collision domain. Instead of deploying one RAP with omni-directional antennas in a mesh network, two or more RAPs with directional antennas can be deployed. These RAPs collocate with each other and operate on different frequency channels, thus dividing a large collision domain into several smaller ones that operate independently.
If the mesh AP bridging features are being used with multiple RAPs, these RAPs should all be on the same subnet to ensure that a consistent subnet is provided for bridge clients.

If you build your mesh with multiple RAPs on different subnets, MAP convergence times increase if a MAP has to failover to another RAP on a different subnet. One way to limit this from happening is to use different BGNs for segments in your network that are separated by subnet boundaries.

**Multiple Controllers**

The consideration in distance of the LWAPP controllers from other LWAPP controllers in the mobility group, and the distance of the LWAPP controllers from the RAPs, is similar to the consideration of an LWAPP WLAN deployment in an enterprise.

There are operational advantages to centralizing LWAPP controllers, and these advantages need to be traded off against the speed and capacity of the links to the LWAPP APs and the traffic profile of the WLAN clients using these APs.

If the WLAN client traffic is expected to be focused on particular sites such as the Internet or a data center, centralizing the controllers at the same sites as these traffic focal points gives the operational advantages without sacrificing traffic efficiency.

If the WLAN client traffic is more peer-to-peer, a distribute controller model might be a better fit. It is likely that a majority of the WLAN traffic are clients in the area, with a smaller amount of traffic going to other locations. Given that many peer-to-peer applications can be sensitive to delay and packet loss, it is best to ensure that traffic between peers takes the most efficient path.

Given that most deployments see a mix of client server traffic and peer-to-peer traffic, it is likely that a hybrid model of LWAPP controller placement is used, where points of presence (PoPs) are created with clusters of controllers placed in strategic locations in the network.

In all cases, remember that the LWAPP model used in the wireless mesh network is designed for campus networks; that is, it expects a high-speed, low-latency network between the LWAPP APs and the LWAPP controller.

**Indoor WLAN Network to Outdoor Mesh**

Mobility groups can be shared between outdoor mesh networks and indoor WLAN networks. It is also possible for a controller to control indoor LWAPP APs and 1500 Series Mesh APs simultaneously. The same WLANs are broadcast out both the indoor AP and the 1500 Series Mesh APs.

**Voice**

The 1500 Series Mesh AP is 802.11e capable, and QoS is supported on the local 2.4 GHz access and for the 5 GHz/4.9 GHz backhaul. Although we have Call Admission Control (CAC) in CCXv4 clients (which provides CAC between AP and the client), real voice support will come only when we can have CAC on the backhaul too. Therefore, voice calls across 1500 Series Mesh APs are not currently fully supported. However, testing shows that it takes numerous voice calls to saturate the mesh network.

**Connecting the Cisco 1500 Series Mesh AP to Your Network**

The wireless mesh has two locations where traffic terminates on the wired network. The first location is where the RAP attaches to the wired network, and where all bridged traffic connects to the wired network. The second location is where the LWAPP controller connects to the wired network; this is where WLAN client traffic from the mesh network connects to the wired network. This is shown
schematically in Figure 42. The WLAN client traffic from LWAPP is tunneled at Layer 2, and matching WLANs should terminate on the same switch VLAN as where the controllers are collocated. The security and network configuration for each of the WLANs on the mesh depend on the security capabilities of the network to which the controller is connected.

**Figure 42**  
Mesh Network Traffic Termination

This section provides implementation details and configuration examples.

**Mesh WLAN**

The Cisco 1500 Series Mesh AP solution uses 802.11 technologies for both the client WLAN and the backhaul. This means that the Cisco 1500 Series Mesh AP solution has the same characteristics and behaviors as an 802.11 solution when determining range, throughput, and power.

**Hidden Nodes**

The mesh backhaul uses the same 802.11a channel for all notes in that mesh, and this can introduce hidden nodes into the WLAN backhaul environment, as shown in Figure 43.
Figure 43 shows the following three MAPs:

- MAP X
- MAP Y
- MAP Z

If MAP X is the route back to the RAP for MAPs Y and Z, both MAP X and MAP Z could be sending traffic to MAP Y at the same time. Because of the RF environment, MAP Y can see traffic from both MAP X and Z, but MAP X and Z cannot see each other. This means that the carrier sense multi-access (CSMA) mechanism does not stop MAP X and Z from transmitting during the same time window; if either of these frames is destined for a MAP, it is corrupted by the collision between frames and requires retransmission.

Although all WLANs at some time can expect some hidden node collisions, the fixed nature of the MAPs make hidden node collisions a persistent feature of the mesh WLAN backhaul under some traffic conditions such as heavy loads and large packet streams.

Both the hidden node problem and the exposed node problem are inherent to wireless mesh networks because mesh APs share the same backhaul channel. Because these two problems can affect the overall network performance, the Cisco Mesh solution seeks to mitigate these two problems as much as possible. For example, the AP1510 has two radios: one for backhaul access on 5GHz channel and the other for 2.4GHz client access. In addition, the radio resource management (RRM) feature enables cell breathing and automatic channel change, which can effectively decrease the collision domains in a mesh network.

There is an additional solution that can help to further mitigate these two problems. To reduce collisions and to improve stability under high load conditions, the 802.11 MAC uses an exponential backoff algorithm, where contending nodes back off exponentially and re-transmit packets whenever a perceived collision occurs. Theoretically, the more retries a node has, the smaller the collision probability will be. In practice, when there are only two contending stations and they are not hidden stations, the collision probability becomes negligible after just 3 retries. Collision probability increases when there are more contending stations. Therefore, when there are many contending stations in the same collision domain, a higher retry limit and a larger maximum contention window are necessary. Further, collision probability does not decrease exponentially when there are hidden nodes in the network. In this case, RTS/CTS exchange can be used to mitigate the hidden node problem.
Co-Channel Interference

In addition to hidden node interference, co-channel interference can also impact performance. Co-channel interference is where adjacent radios on the same channel interfere with the performance of the local mesh. This interference takes the form of collisions or excessive deferrals by CSMA. In both cases, performance of the mesh is degraded. With appropriate channel management for the wireless mesh, co-channel interference should be able to be minimized.

Outdoor Site Survey

Deploying WLAN systems outdoors requires a different skill set to indoor wireless deployments. Considerations such as weather extremes, lightning, physical security, and local regulations need to be taken into account. When deploying the Cisco Wireless Routing network, similar guidance to that used in outdoor bridging can applied, and experience in deploying outdoor wireless bridging solutions is an advantage.

When determining the suitability of a successful mesh link, define how far the mesh link is expected to transmit and at what radio data rate. Remember that the data rate is not directly included in the wireless routing calculation, and that it is generally recommended that the same data rate is used throughout the same mesh (the recommended rate is 18 Mbps). Design recommendations for mesh links are as follows:

- MAP deployment can not exceed 35 feet in height above the street.
- MAP is deployed with antennas pointed down toward the ground.
- Typical 5 GHz RAP-to-MAP distances are 1000–4000 feet.
- RAP locations are typically towers or tall buildings.
- Typical 5 GHz MAP-to-MAP distances are 500–1000 feet.
- MAP locations are typically short building tops or streetlights.
- Typical 2.4 GHz MAP-to-client distances are 300–500 feet.
- Client locations are typically laptops, CPEs, or professionally house-mounted antennas.

Determining Line of Sight

Because the mesh radio waves have very high frequency in the 5 GHz band, the radio wavelength is small; therefore, the radio waves do not travel as far as radio waves on lower frequencies, given the same amount of power. This higher frequency range makes the mesh ideal for unlicensed use because the radio waves do not travel far unless a high-gain antenna is used to tightly focus the radio waves in a given direction.

This high gain antenna configuration is recommended only for connecting the RAP to the MAP mesh; to optimize mesh behavior Omni antennas are used, because mesh links are limited to one mile (1.6 km). The curvature of the earth does not impact line-of-site calculations because the curvature of the earth changes every six miles (9.6 km).

Weather

In addition to free space path loss and line of sight, weather can also degrade a mesh link. Rain, snow, fog, and any high humidity condition can slightly obstruct or affect line of sight, introducing a small loss (sometimes referred to as rain fade or fade margin), which has little effect on the mesh link. If you have established a stable mesh link, weather should not be a problem; however, if the link is poor to begin with, bad weather can degrade performance or cause loss of link.
Fresnel Zone

A Fresnel zone is an imaginary ellipse around the visual line of sight between the transmitter and receiver. As radio signals travel through free space to their intended target, they could encounter an obstruction in the Fresnel area, degrading the signal. Best performance and range is attained when there is no obstruction of this Fresnel area. Fresnel zone, free space loss, antenna gain, cable loss, data rate, link distance, transmitter power, receiver sensitivity, and other variables play a role in determining how far your mesh link goes. Links can still occur as long as 60–70 percent of the Fresnel area is unobstructed, as illustrated in Figure 44 and Figure 45.

**Figure 44**  
*Point-to-Point Link Fresnel Zone*

**Figure 45**  
*Typical Obstructions in Fresnel Zone*

It is possible to calculate the radius of the Fresnel zone (in feet) at any particular distance along the path using this equation:

\[ F_1 = 72.6 \times \text{SQR}(\text{Distance}/4 \times \text{Frequency in GHz}) \]

Where \( F_1 \) = the first Fresnel zone radius (ft.). \( D \) = total path length (mi.). \( f \) = frequency (GHz)

Normally, 60 percent of the first Fresnel zone clearance is recommended, so the above formula for 60 percent Fresnel zone clearance can be expressed as: 0.60 \( F_1 \) = 43.3 \( \times \) SQR (distance/4x Frequency in GHz). These calculations are based on a flat terrain. Figure 46 shows the removal of an obstruction in the Fresnel zone of the wireless signal.
Fresnel Zone Size in Wireless Mesh Deployments

To give an approximation of size of the maximum Fresnel zone to be considered, at a possible minimum frequency of 4.9 GHz, the minimum value changes depending on the regulatory domain. The minimum figure quoted is a possible band allocated for public safety in the USA; and maximum distance of one mile gives a Fresnel zone of clearance requirement of $9.78 \text{ ft} = 43.3 \times \text{SQR}(1/(4 \times 4.9))$. This clearance should be relatively easy to achieve in most situations. In most deployments, distances are expected to be less than one mile, and the frequency greater than 4.9 GHz, making the Fresnel zone smaller. Every mesh deployment should consider the Fresnel zone as part of its design, but in most cases, it is not expected that meeting the Fresnel clearance requirement is an issue.

Site Survey

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. Determine the correct location and antenna before drilling holes, routing cables, and mounting equipment.

Note

When power is not readily available, use an unrestricted power supply (UPS) to temporarily power the mesh link.

Pre-Survey Checklist

Before attempting a site survey, determine the following:

- How long is your wireless link?
- Do you have a clear line of sight?
- What is the minimum acceptable data rate within which the link runs?
- Is this a point-to-point or point-to-multipoint link?
- Do you have the correct antenna?
- Can the access point installation area support the weight of the access point?
- Do you have access to both of the mesh site locations?
- Do you have the proper permits, if required?
- Do you have a partner? Never attempt to survey or work alone on a roof or tower.

Figure 46 Removing Obstructions in Fresnel Zone
- Have you configured the Mesh 1500 Series APs before you go onsite? It is always easier to resolve configuration or device problems first.
- Do you have the proper tools and equipment to complete your task?

**Note**  
Cellular phones or handheld two-way radios can be helpful for performing surveys. See the bridge installation section for more tips on surveys.

**Mesh AP and Controller Configuration**

**Figure 47** shows the mesh configuration flow chart.

---

**Figure 47  Mesh Configuration Flow Chart**

1. Record MAC address of AP's to be used in the mesh
2. Set Controller in L2 mode
3. Enter MAC addresses of AP's into MAC filter of controller
4. Enable Zero Touch Configuration
5. Leave Mesh in L2 Mode or enable L3 Mode
6. If you plan to USE L2 mode configure bridge group names and turn off Zero Touch deployment mode after all AP's have joined the MESH
7. Before you turn on L3 mode in the controller you must assign IP address to the AP's unless you are using DHCP
8. Configure the Primary, Secondary and Tertiary controllers on each AP
9. Configure the Bridge Group Name for the AP's to use
10. Enable L3 mode save and reboot
11. Configure multiple controllers
12. Leave as a simple single controller mesh
13. Configure mobility groups of the controllers within the mesh

**Note**  
For more detailed information on configuration options with a graphical user interface, see the following URL: [http://www.cisco.com/en/US/docs/wireless/controller/6.0/configuration/guide/c60mesh.html](http://www.cisco.com/en/US/docs/wireless/controller/6.0/configuration/guide/c60mesh.html)
MAC Address Authentication

Record the MAC address of APs to be used in the mesh. APs need to authenticate to the controllers, so their MAC address must be added to the MAC filter of the controller using the following command:

```
config auth-list add mac AP-MAC
```

This can also be configured in the security section of the web GUI.

AP Roles

By default, the 1500 Series Mesh APs are shipped with a radio role set to MAP. Therefore, the radio role for a RAP must be changed to RAP. You can change this configuration on the APs by statically setting them as rooftop APs or mesh APs with the following command:

```
(Cisco Controller) >config ap role (rootAP, mesh AP, default)
```

The radio role can also be changed using the GUI.

Note that the radio role “AUTO” has been removed with the current software release. The primary backhaul setting algorithm has also been modified by this release. This also adds a high-level of resiliency for each mesh node. The algorithm can be summarized as follows:

- A MAP always sets the Ethernet port as “primary backhaul” if it is UP, otherwise 802.11A radio (this gives the network administrator the ability to configure it as a RAP the first time and recover it in-house). For fast convergence of the network, we recommend to not connect any Ethernet device to the MAP for its initial joining to the mesh network.
- A MAP failing connect to a WLAN controller on a UP Ethernet port, sets 802.11A radio as primary backhaul. Failing to find a neighbor or failing to connect to a WLAN controller via any neighbor on 802.11A radio will cause the primary backhaul to be UP on the Ethernet port again.
- A MAP connected to a WLAN controller over an Ethernet port does not build a mesh topology (unlike a RAP).
- A RAP always sets the Ethernet port as the primary backhaul.
- If the Ethernet port is DOWN on a RAP, or a RAP fails to connect to a WLAN controller on a UP Ethernet port, the 802.11A radio is set as the primary backhaul. Failing to find a neighbor or failing to connect to a WLAN controller via any neighbor on the 802.11A radio will cause the primary backhaul to be the Ethernet port again.

Keeping the roles of mesh nodes distinct using the above algorithm greatly helps avoid an AP being in an unknown state and thus become stranded in a live network.

Shared Secrets

Ensure that the zero-touch configuration on the controller is enabled. It is enabled by default, but it is important to verify this in the wireless configuration section under bridging. This allows the APs in the mesh to get the shared secret key from the controller. This is the only configuration that is currently needed for Layer 2 mode.

Layer 2 mode is useful for pre-configuring APs before their deployment. For larger deployments, we recommend that you configure in Layer 3 mode.

**Note**

You cannot recover the shared secret from a controller or AP, so it is very important to save your shared secret somewhere in an offline document. If it is lost, you must configure a new shared secret. In the CLI, issue the `config network bridging-shared-secret string` command.
The shared secret key can be seen in the clear text format by issuing the `show network` command:

```bash
Cisco Controller) show network
RF-Network Name: training2
Web Mode: Enable
Secure Web Mode: Enable
Secure Shell (ssh): Enable
Telnet: Enable
Ethernet Multicast Mode: Enable
User Idle Timeout: 300 seconds
ARP Idle Timeout: 300 seconds
ARP Unicast Mode: Disabled
Cisco AP Default Master: Disable
Mgmt Via Wireless Interface: Disable
Bridge AP Zero Config: Enable
Bridge Shared Secret: cisco
Allow Old Bridging Aps to Authenticate: Disable
Over The Air Provisioning of APS: Enable
Mobile Peer to Peer Blocking: Disable
Apple Talk: Disable
AP Fallback: Enable
Web Auth Redirect Ports: 80
Fast SSID Change: Disabled
```

**Bridge Group Name (BGN)**

BGN can be used to logically group the APs in the mesh. Although by default, the APs come with a null value BGN to allow association, we recommend that you set a BGN. You can make this configuration change via the CLI or GUI using the following command:

```
config ap bridgegroupname set Bridge Group Name Cisco AP
```

**Note** BGNs can be a maximum of ten characters.

When configuring BGN on a live network, ensure that you configure from the furthest MAP and work your way back to the RAP. This is very important because you risk stranding a child MAP that cannot associate with a parent that could have an updated BGN.

Use different BGNs to logically group different parts of your network. This is useful in situations where you have RAPs within the same RF area and you are trying to keep segments of your mesh separated.

If you want to add a new AP to a running network, you must pre-configure the BGN on the new AP. However, if you are bringing up the mesh network from the scratch using new, out-of-the-box APs, the BGN is preset in the APs to a NULL value. APs join in a new network using this default value of the BGN.

You can verify the BGN of an AP by using the following command:

```
show ap config general Cisco AP
```

**Misconfiguration of BGN**

An AP can be wrongly provisioned with a bridgegroupname other than the one it is intended for. Depending on the network design, this AP might or might not be able to reach out and find its correct sector or tree. If it cannot reach a compatible sector, it can become stranded.
In order to recover such a stranded AP, the concept of default bridgegroupname has been introduced with release 4.0 code. The basic idea is that an AP that is unable to connect to any other AP with its configured bridgegroupname, it attempts to connect with the bridgegroupname of default. All nodes running release 4.0 implemented software accept other nodes with this bridgegroupname.

The algorithm of detecting this strand condition and recovery is as follows:

1. Passively scan and find all neighbor nodes, regardless of their bridgegroupname.
2. The AP attempts to connect to the neighbors heard with my own bridgegroupname using AWPP.
3. If Step 2 fails, attempt connecting with default bridgegroupname using AWPP.
4. For each failed attempt of Step 3, exclusion-list the neighbor and attempt to connect the next best neighbor.
5. If the AP fails to connect with all neighbors in Step 4, reboot the AP.
6. If connected with default bridgegroupname for 30 minutes, re-scan all channels and attempt to connect with the correct bridgegroupname.

**Note**

When an AP is able to connect with the default bridgegroupname, the parent node reports the AP as a default child/node/neighbor entry on the WLAN controller, so that a network administrator is aware of the stranded AP. In subsequent software release, this condition will generate an SNMP trap from the controller to WCS. Such an AP cannot accept any client, other mesh nodes as its children, nor can it pass any data traffic through.

Do not confuse an unassigned BGN (null value) with DEFAULT, which is a mode the AP will use to connect in the case of it not finding its own BGN.

When using DEFAULT, the AP will not operate as a mesh node, it will just be in maintenance mode to access via the controller:

```
(Cisco Controller)> 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:FB:10 state UPDATED NEIGH PARENT BEACON (86B) snrUp 72, snrDown 63, linkSnr 57
00:0B:85:5F:FA:60 is RAP
```

**IP Addressing**

IP addressing is needed for the APs when the controller is running in Layer 3 mode. You need to configure the APs with an IP address if DHCP is not available. Use Layer 2 mode on a controller to configure the APs address if DHCP is not available. In the CLI, issue the following command:

```
config ap static-IP enable AP IP addr IP netmask
```

To configure via the GUI, go to Wireless > Cisco APs > Details. (we recommend that you use DHCP to avoid this.)

**DHCP**

RAPs and MAPs can use DHCP to configure their addresses. By default, a Windows DHCP server sends its response by an IP broadcast (255.255.255.255). However, it can be configured to send DHCP responses via unicast.
Open the DHCP server registry and find or create the key. Create a new DWORD value, or modify the existing value called “IgnoreBroadcastFlag”. Set it to the values listed below.

(Default) REG_SZ (value not set)  
IgnoreBroadcastFlag REG_DWORD 0x00000000 (0)

HKEY_LOCAL_MACHINE\CurrentControlSet\Services\DHCP\Server\Parameters

Registry Settings
System Key: [HKEY_LOCAL_MACHINE\CurrentControlSet\Services\DHCP\Server\Parameters]  
Value Name: IgnoreBroadcastFlag  
Data Type: REG_DWORD (DWORD Value)  
Value Data: 1 = always broadcast (default), 0 = only broadcast if client requests

After the changes have been committed close your registry and reboot the server.

**Note**

Modifying the registry can cause serious problems that could require you to reinstall your operating system. Cisco cannot guarantee that problems resulting from modifications to the registry can be solved. Use the information provided at your own risk.

**Option 43**

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 an RAP to a section of the network where it must transverse 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 1500 Series Mesh APs accept an ASCII string format for Option 43 from a DHCP server. Cisco Aironet 1500 Series access points use a comma-separated string format for DHCP Option 43. Other Cisco Aironet access points use the type-length-value (TLV) format for DHCP Option 43. DHCP servers must be programmed to return the option based on the access point’s DHCP Vendor Class Identifier (VCI) string (DHCP Option 60).

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

```
ip dhcp pool <pool name>  
    network <IP Network> <Netmask>  
    default-router <Default router>  
    dns-server <DNS Server>  
    option 43 ascii <Controller IP addresses>
```

It is possible to separate multiple controllers with commas, such as the following example:

```
option 43 ascii “10.51.1.10,10.51.1.11”
```

Add Option 60 using the following command:

```
option 60 ascii “Cisco AP.LAP1510”
```

For more information on configuring Option 43, see the application note “Configuring DHCP Option 43 For Lightweight Cisco Aironet Access Points” in the Getting Started Guide: Cisco Aironet 1500 Series Outdoor Mesh Access Points at the following URL:


There is also more information on the AP controller address table in Mobility Groups, page 59.
Switch Name

For Layer 3 mode, the APs also require that the switch name is configured on each AP. You can also use Layer 2 mode and the controllers CLI or GUI to make this configuration:

```
config ap primary-base Switch Name Cisco AP
```

Enabling Layer 3 Mode

Before enabling Layer 3 mode, you must configure your APs with the IP address. See the section above for AP IP address commands.

```
config switchconfig mode L3
```

You must save and reboot for this configuration to take effect.

```
save config
reset system
```

After the reboot, you must define the ap-manager interface:

```
config interface create ap-manager vlan-id
config interface address ap-manager IP address
```

Note

The ap-manager interface must be on the same VLAN and subnet as the management interface.

Mobility Groups

A set of controllers can be configured as a mobility group. A mobility group allows you to deploy multiple controllers in a network and have the devices dynamically share important information between them and to forward data traffic when inter-controller roaming is supported. The important information shared includes client device context and state, and controller loading information. With this information, the network can support inter-controller WLAN device roaming, AP load balancing, and redundancy. Figure 48 shows the mobility group concept.
Along with the switch name, the RAP or MAP needs the address of the controller or controllers if it is to transverse a Layer 3 hop to reach a controller. To populate the AP with these addresses, you can connect the AP to a subnet where a controller is attached and allow broadcast auto discovery, or use DHCP Option 43, as previously described. If a controller has a mobility group configured with other controllers in it, the RAP or MAP with an established LWAPP tunnel is populated with the addresses of all the controllers listed in its mobility group.

The basic requirements for controller devices in a mobility group are the following:

- IP connectivity between management interfaces on all wireless LAN controller (WLC) devices.
- All WLC devices must be configured with the same mobility group name. The mobility group name is case sensitive.
- All WLC devices must be configured with to use the same virtual interface IP address.
- Each WLC device is configured with the MAC address and IP address of all the other mobility group members.

Configure the mobility group domain using the following command:

```plaintext
config mobility group domain domain_name ASCII String up to 31 characters, case sensitive
```

Configure the mobility group members on all controllers within the mobility group domain:

```plaintext
config mobility group member add MAC addr IP addr
```
Layer 2 and Layer 3 Deployments

In a Layer 2 LWAPP mesh configuration, the APs and the controller are on the same Layer 2 Ethernet broadcast domain, as shown in Figure 49.

Figure 49 Layer 2 LWAPP Mesh Connections

In a Layer 3 LWAPP mesh configuration, the APs and the controller are separated by a router, as shown in Figure 50. IP addressing and proper routing in between the APs and the controller is required.

Figure 50 Layer 3 LWAPP Mesh Connections

AP RADIUS Authentication with Cisco Secure ACS Server

For smaller mesh or point-to-point bridge network deployments, a simple MAC filter list suffices. When a network reaches much larger sizes, RADIUS AP authentication should be used. This eliminates the need of imputing all of the MACs of each AP in the mesh on every controller within the network.

Note

External RADIUS authentication of 1500 series mesh access points is not supported in release 4.1.17x.0 given changes in the security protocol. All 1500 mesh access points must be defined in the local MAC filter of the controller to ensure proper authorization with the EAP-FASTv2 certificates on the local AAA server.

Controller Configuration for RADIUS Authentication

First, you must be at a RADIUS server that is used for authentication:

```bash
config radius auth add index IP addr port [ascii/hex] secret
```
This command contains the following fields:

- **index**—Used to define multiple RADIUS servers.
- **IP addr**—IP address of the Cisco ACS server you are going to use for authentication.
- **port**—UDP port on which you are configured to send RADIUS messaging; standard RADIUS authentication messaging runs on port 1812.
- **ascii/hex**—Defines the shared secret format.
- **secret**—Password used between the RADIUS server and the controller.

By default, if this is the first RADIUS server added to the controller, it comes up as the default RADIUS server for both network users and management. For AP authentication, all that is needed is for the network users to be enabled, so it is fine to disable management by using the following command (and entering the RADIUS server index):

```
config radius auth management index (enable/disable) index
```

For the APs to authorize against the AAA server, you must also enable it within the AP Policies section. Use the following command:

```
config auth-list ap-policy authorize-ap enable
```

Note: MACs that you have configured in the MAC filter list supersede any that are configured in ACS.

**Cisco ACS Configuration**

Perform the following steps for Cisco ACS configuration.

**Step 1** Add each of your controllers as an NAS under the network configuration section of ACS, as shown in Figure 51.
Step 2  Enter their host names and IP address and the key that matches what you have configured on the controller as the RADIUS server secret, as shown in Figure 52.

Figure 51  Adding Controller as a NAS in ACS

Figure 52  Configuring Controller as a NAS on ACS
Step 3  Select to use RADIUS (IETF) Authentication type, and submit.

Step 4  Each AP now needs to be added as a RADIUS user. This is done in the User Setup section of ACS, as shown in Figure 53.

Figure 53  Adding AP as a RADIUS User in ACS

Step 5  When configuring the user in ACS, make sure to use the MAC address as the real name and password for the user, as shown in Figure 54. Also use the Cisco Secure Database.
Private VLANs (PVLANs) can be used with a 1500 Series Mesh AP deployment to block broadcast traffic between rooftop APs and to secure the wired access to a RAP on an Ethernet network. It is suggested to use PVLANs on a mesh deployment where you are not using Ethernet bridging. PVLANs break Ethernet bridging because it allows only the RAPs to communicate with the controllers on the network.

When using PVLANs, use a different subnet for your mesh than for the management interfaces of your controllers.

Perform the following steps to configure a PVLAN,

Step 1: Make sure that you have VTP mode set to transparent,
Step 2: Add a VLAN to be used as your isolated VLAN. This is the VLAN where your RAPs are.

Use the following commands:

```
ROUTER(config)#vlan <VLAN ID>
ROUTER(config-vlan)#private-vlan isolated
```
Step 3  Configure the primary private VLAN into which you put your default gateway, using the following commands:

```
ROUTER(config)#vlan <VLAN_ID>
ROUTER(config-vlan)# private-vlan primary
ROUTER(config-vlan)# private-vlan association <VLAN_ID>
```

**Note**  Note the association is to the isolated VLAN, so use the VLAN ID of the isolated VLAN.

Step 4  For each interface where you have a RAP, you must configure the switchport private VLAN host association, and set the switchport mode to “private-vlan host.” This associates the interface host to the private VLAN.

Use the following command:

```
MESH-3750(config-if)# description RAP interface
MESH-3750(config-if)# switchport private-vlan host-association <VLAN_ID> <VLAN_ID>
```

**Note**  Note that the first VLAN ID is ID of the VLAN you configured as the primary, and the second VLAN ID is the VLAN you configured as the isolated.

```
MESH-3750(config-if)# switchport mode private-vlan host
```
Sample Configuration

Current configuration : 5952 bytes
!
vtp mode transparent
!
!
vlan 93
  private-vlan primary
  private-vlan association 94
!
vlan 94
  private-vlan isolated
!
vlan 95-96,98-99,101,172,200
!
!
!
interface GigabitEthernet1/0/15
  description MESH-RAP interface
  switchport private-vlan host-association 93 94
  switchport mode private-vlan host
  spanning-tree portfast
!
interface GigabitEthernet1/0/16
  description MESH-RAP interface switchport private-vlan host-association 93 94
  switchport mode private-vlan host
  spanning-tree portfast
!
interface GigabitEthernet1/0/17
  description MESH-RAP interface
  switchport private-vlan host-association 93 94
  switchport mode private-vlan host
  spanning-tree portfast
!

interface GigabitEthernet1/0/25
  description MESH-Controller1 interface
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface GigabitEthernet1/0/26
  description MESH-Controller2 interface
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface Vlan93
  ip address 10.15.93.1 255.255.255.0
  private-vlan mapping 94
!

interface Vlan99
  description controller vlan
  ip address 10.15.99.1 255.255.255.0
!
Firewall Configuration

There are a few packet types that need to be allowed to pass from the RAPs to the controllers. It is recommended to firewall in-between RAPs and controllers to block all other types of packets. If you are using the bridged Ethernet feature of the 1500 Series Mesh AP, this can be used as a good starting point for security. Depending on what device or application you are connecting to the bridged Ethernet port, allow the application-specific ports.

The following suggestions are made for a mesh that is operating in LWAPP Layer 3 mode:

- BootPS is used for DHCP, so this must remain unblocked for the mesh APs to receive DHCP IP addresses. BootPS is sent on UDP port 67.
- For LWAPP, UDP port 12222 is used for data, and UDP port 12223 is used for control. Unblock both of these ports.
- Leave UPD ports 6000–7000 open for Radio Resource Management (RRM), which will be added for backhaul links in future code.

Troubleshooting Considerations

This section provides troubleshooting information.

Debug Commands

The following two commands are very helpful to see the messages being exchanged between APs and the controller (see Figure 55).

(Cisco Controller) >debug lwapp events enable
(Cisco Controller) >debug disable-all

You can use the debug command to see the flow of packet exchanges that occur between the AP and the controller. The AP initiates the discovery process. An exchange of credentials takes place during the Join phase to authenticate that the AP is allowed to join the mesh network.

Upon a successful join completion, the AP will send an LWAPP configuration request. The controller responds with a configuration response. When a Configure Response is received from the controller, the AP will evaluate each configuration element and implement them.
Mon Sept 19 11:53:56 2005: Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:0e:05:80 on port ’1’
Mon Sept 19 11:53:56 2005: Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:0e:05:80 on Port 1
Mon Sept 19 11:54:07 2005: Received LWAPP JOIN REQUEST from AP 00:0b:85:0e:05:80 on port ’1’
Mon Sept 19 11:54:08 2005: LWAPP Join-Request MTU path from AP 00:0b:85:0e:05:80 is 1500, remote debug mode is 0
Mon Sept 19 11:54:08 2005: Successfully Plumb AP 00:0b:85:0e:05:80 into fast path with IP Address 1.100.49.10, next hop MAC 00:0b:85:0e:05:80 on VLAN 149
Mon Sept 19 11:54:08 2005: Successfully transmission of LWAPP Join-Reply to AP 00:0b:85:0e:05:80
Mon Sept 19 11:54:08 2005: Register LWAPP event for AP 00:0b:85:0e:05:80 slot 0
Mon Sept 19 11:54:08 2005: Register LWAPP event for AP 00:0b:85:0e:05:80 slot 1
Mon Sept 19 11:54:08 2005: Received LWAPP CONFIGURE REQUEST from AP 00:0b:85:0e:05:80
Mon Sept 19 11:54:08 2005: Updating IP info for AP 00:0b:85:0e:05:80 -- static 1, 1.100.49.10/255.255.255.0, gtw 1.100.49.1
Mon Sept 19 11:54:08 2005: spam Verify RegDomain Not set for slot 0
Mon Sept 19 11:54:08 2005: spam Verify RegDomain Not set for slot 1
Mon Sept 19 11:54:08 2005: spamEncodeDomainSecretPayload:Send domain secret skycaptain<6f,89,4e,cf,4d,c0,94,ed,9c,60,60,93,d3,19,c0,69,cc,f2,77,05> to AP 00:0b:85:0e:05:80
Mon Sept 19 11:54:08 2005: Successfully transmission of LWAPP Config-Message to AP 00:0b:85:0e:05:80
Mon Sept 19 11:54:08 2005: Running spamEncodeCreateVapPayload for SSID ‘mjoyceQA’
Mon Sept 19 11:54:08 2005: Running spamEncodeCreateVapPayload for SSID ‘mjoyceQA’
Mon Sept 19 11:54:08 2005: AP 00:0b:85:0e:05:80 associated. Last AP failure was due to AP reset

Unknown Bridge Shared Secret

If an AP has a misconfigured bridge shared secret key, it is not allowed on the mesh. If Zero-Touch is enabled, the AP derives the key from the controller or neighbor AP.

If the Zero-Touch has been turned off, the AP is never able to re-join the mesh network.
If this has happened, turn Zero-Touch back on so that the AP can get the new bridge shared secret.

Ensure that “Allow Old Bridging Aps to Authenticate” is disabled. There is a long history behind this. It is disabled by default. If it is enabled, then the shared secret key configured on the controller will not be passed to the APs. Use the show network command to verify these settings:

```
Cisco Controller) show network
RF-Network Name:training2
Web Mode:Enable
Secure Web Mode:Enable
Secure Shell (ssh):Enable
Telnet:Enable
Ethernet Multicast Mode:Enable
User Idle Timeout:300 seconds
ARP Idle Timeout:300 seconds
ARP Unicast Mode:Disabled
Cisco AP Default Master:Disable
Mgmt Via Wireless Interface:Disable
Bridge AP Zero Config:Enable
Bridge Shared Secret:cisco
Allow Old Bridging Aps to Authenticate:Disable
Over The Air Provisioning of APS:Enable
Mobile Peer to Peer Blocking:Disable
Apple Talk:Disable
AP Fallback:Enable
Web Auth Redirect Ports:80
Fast SSID Change:Disabled
```

There is another very important aspect of Bridge Shared Master Key (BMK) and PMK. A new AP that has not yet been used will first try its PMK to establish the LWAPP connection to the controller. It will fail twice with PMK. After failing twice, it will establish the LWAPP connection, download the configured BMK, reboot, and then join the controller with BMK.

A used AP with a different BMK will first use this BMK to establish the LWAPP connection. After failing twice with the misconfigured BMK, it will use the PMK to establish a successful session to the controller. It will then download the correct BMK from the controller, reboot, and then join the controller with the correct BMK. This is covered in more detail in Convergence Analysis, page 73.

### Misconfiguration of the MESH AP IP Address

Although most practical Layer 3 networks are deployed using DHCP IP address management, manual IP address management and allocating IP addresses statically to each mesh node might be preferred by some network administrators. Manual AP IP address management can be a nightmare for large networks, but it might make sense in small to medium size networks (approx. 10-100 mesh nodes) given the number of mesh nodes are relatively small compared to client hosts.

Statically configuring the IP address on a mesh node has the possibility of putting a MAP on a wrong network, such as a subnet or VLAN. This could prevent an AP from successfully resolving the IP gateway, eventually failing to discover a WLAN controller. In such a scenario, the AP falls back to its DHCP mechanism and automatically attempts to find a DHCP server and obtains an IP address from it. This fallback mechanism prevents a mesh node from being potentially stranded from a wrongly configured static IP address and allows it to obtain a correct address from a DHCP server on the network.

When you are manually allocating IP addresses, we recommend that you make IP addressing changes from the furthest AP child first and work your way back to the RAP. This also applies if you relocate equipment. For example, if you uninstall a mesh access point and redeploy it in another physical location of the mesh network that has a different addressed subnet.
Another option is to take a controller in Layer 2 mode with a RAP to the location with the misconfigured MAP. Set the bridge group name on the RAP to match the MAP that needs the configuration change. Add the MAP’s MAC address to the controller. When the misconfigured MAP comes up in the AP summary detail, configure it with an IP address.

**Misconfiguration of DHCP**

Despite the DHCP fallback mechanism, there is still a possibility that an AP can become stranded, if any of the following conditions exist:

- There is no DHCP server on the network.
- There is a DHCP server on the network, but it does not offer an IP address to the AP, or if it gives a wrong IP address to the AP (for example, on a wrong VLAN or subnet).

These conditions can strand an AP that is configured with or without a wrong static IP address or with DHCP. Therefore, it is necessary to ensure that when an AP is unable to connect after exhausting all DHCP discovery attempts or DHCP retry counts or IP gateway resolution retry counts, it attempts to find a controller in Layer 2 mode. In other words, an AP attempts to discover a controller in Layer 3 mode first and in this mode, attempts with both static IP (if configured) or DHCP (if possible). The AP then attempts to discover a controller in Layer 2 mode. After finishing a number of Layer 3 and Layer 2 mode attempts, the AP changes its parent node and re-attempts DHCP discovery. Release 4.0 software does just that, plus it exclusion-lists the parent node through which it was unable to obtain the correct IP address.

**Identifying the Node Exclusion Algorithm**

Depending on the mesh network design, it is entirely possible that a node finds another node “best” according to its routing metric (even recursively true), yet it is unable to provide the node with a connection to the correct WLAN controller or correct network. It is the typical “honeypot” AP scenario caused by either misplacement or provisioning or the design of the network or by the dynamic nature of an RF environment exhibiting such conditions that optimize the AWPP routing metric for a particular link in a persistent or transient manner. Such conditions are generally difficult to recover from in most networks and could blackhole or sinkhole a node completely, taking it out from the network. Possible symptoms include, but are not limited to:

- A node connects to the honeypot, but cannot resolve the IP gateway when configured with static IP address, or cannot obtain the correct IP address from DHCP server, or cannot connect to a WLAN controller.
- A node ping-pongs between a few honeypots or circles between many honeypots (in worst-case scenarios).

Cisco Mesh software tackles this difficult scenario using a sophisticated node exclusion-listing algorithm. This node exclusion-listing algorithm uses an exponential backoff and advance technique much like TCP sliding window or 802.11 MAC. The basic idea relies on the following four major steps:

- Honeypot detection—The honeypots are first detected via the following steps. A parent node is set by the AWPP module, by:
  - A static IP attempt in LWAPP module.
  - A DHCP attempt in the DHCP module.
  - An LWAPP attempt to find and connect to a controller fails.
Honeypot conviction—When a honeypot is detected, it is placed in an exclusion-list database with its conviction period to remain on the list. The default is 32 minutes. Other nodes are then attempted as parents in the following order, falling back to the next, upon failing the current mechanism:

- On the same channel.
- Across different channels (first with its own bridgegroupname and then with default).
- Another cycle, by clearing conviction of all current exclusion-list entries.
- Rebooting the AP.

- Non-honeypot credit—It is often possible that a node is not a really a honeypot, but appears to be due to some transient backend condition, such as:
  - The DHCP server is either not up-and-running yet, has failed temporarily, or requires a reboot.
  - The WLAN controller is either not up-and-running yet, has failed temporarily, or requires a reboot.
  - The Ethernet cable on the RAP was accidentally disconnected.

Such non-honeypots must be credited properly from their serving times so that a node can come back to them as soon as possible.

- Honeypot expiration—Upon expiration, an exclusion-list node must be removed from the exclusion-list database and return to normal state for future consideration by AWPP.

- Honeypot reporting—Honeypots are reported to the controller via LWAPP mesh neighbor message to the controller, which shows these on the Bridging Information page. A message is also displayed the first-time an exclusion-listed neighbor is seen. In subsequent software release, an SNMP trap will be generated on the controller for this condition so that WCS can record the occurrence. Figure 56 shows the bridging details.

Because there could be many nodes attempting to join or re-join the network after an expected or unexpected event, a hold-off time of 16 minutes is implemented. This means that no nodes are exclusion-listed during this period of time after system initialization.

This exponential backoff and advance algorithm is unique and has the following useful properties:

- It allows a node to correctly identify the parent nodes whether it is a true honeypot or is just experiencing temporary outage conditions.
• It credits the good parent nodes according to the time it has enabled a node to stay connected with the network and the crediting requires lesser and lesser time over period in order to bring the exclusion-list conviction period to be very low for real transient conditions and not so low for transient to moderate outages.

• It has built-in hysteresis for encountering the initial condition issue where many nodes try to discover each other only to find that those are not really meant to be in the same network.

• It has built-in memory for nodes that can appear as neighbors sporadically so they are not accidentally considered as parents if they were, or are supposed to be, on the exclusion-list database.

The node exclusion-listing algorithm is constructed to guard the mesh network against serious stranding, which was observed in customers’ networks. It integrates into AWPP in such a way that a node can quickly (re-)converge and find the correct network under many kinds of adversities.

Convergence Analysis

The following qualifiers have been defined for describing convergence of a mesh AP:

• Convergence: The time for a mesh AP taken to establish a stable LWAPP connection with a WLAN controller starting from the time when it was first booted up.

  Convergence is a natural quantity and time to converge is result of an action on the network by a network administrator, where an AP experiences one of the following situations:
  - Starting up for the first time.
  - Needs to be rebooted due to hard upgrades, such as image, BMK, or bridgegroupname.
  - Lost network connection due to soft upgrades, such as backhaul channel or data rate change.

• Reconvergence: Under a network failure condition, the time for a mesh AP taken to re-establish a stable LWAPP connection with a WLAN controller starting from the time when the failure occurred.

  Reconvergence is a serious condition in any network and much of challenge in fast reconvergence lies in detecting the failure quickly.

• Network convergence or reconvergence: The above definitions apply to a single node in the network. When the overall network convergence is expected, it is defined by the convergence time taken by the last node to join the network.

The following sections describe the elements involved in each type of convergence and reconvergence in worst-case scenarios. Most of these convergence scenarios apply to MAPs only.

Startup Convergence

There are three types of convergence factors:

• Mandatory: All systems must do convergence and software does this automatically.

• Optional: Some systems might do convergence and software does this automatically.

• Manual: This is invoked by a network administrator.
### RAP Convergence

When an out-of-the-box RAP is first powered-up, it needs to go through the following cycles in order to join an up-and-running network (Note that there is no such thing as an out-of-the-box RAP as all mesh APs ship as MAPs. A target RAP needs to be provisioned first. It first joins the network as a MAP over Ethernet and then needs to be configured as a RAP. Here, LWAPP join includes the prior step of LWAPP discovery as well.):

1. Boot-up and system initialization (mandatory)
2. IP address from DHCP server (optional)
3. LWAPP join with PMK (mandatory)
4. LWAPP Image upgrade (optional)
5. Re-boot and system initialization (mandatory)
6. IP address from DHCP server (optional)
7. LWAPP re-join with PMK (mandatory)
8. LWAPP BMK download (mandatory)
9. LWAPP Join with BMK (mandatory)
10. LWAPP configure role to RAP (manual)
11. Re-boot and system initialization (mandatory)
12. LWAPP re-join with BMK (mandatory)

Despite being similar to a regular AP1000, the time taken for a fresh RAP to converge in a mesh network is significantly higher due to BMK and role implementations for a RAP.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initially, a new AP will repeat Step 7 three times as it will fail twice with PMK. After failing twice it will establish the LWAPP connection, download the configured BMK, reboot, and then join the controller with BMK.</td>
</tr>
<tr>
<td>An AP that has previously been used with a different BMK will use its BMK first (Step 9) to establish the LWAPP connection. After failing twice with the misconfigured BMK, it will use the PMK to establish a successful session to the controller. It will then download the correct BMK from the controller, reboot, and then join the controller using the correct BMK.</td>
</tr>
</tbody>
</table>

### MAP Convergence

When a MAP first powered-up, it needs to go through the following cycles in order to join an up-and-running network. Note that this MAP has a radio backhaul and hence, the same cycles apply to RAP as well if it was backhauling over air.

1. Boot-up and system initialization (mandatory).
3. IP address from DHCP server (optional).
4. LWAPP join with PMK (mandatory).
5. LWAPP Image upgrade (optional).
6. Re-boot and system initialization (mandatory).
8. IP address from DHCP server (optional).
9. LWAPP join with PMK (mandatory).
10. LWAPP BMK download (mandatory).
12. LWAPP re-join with BMK (mandatory).

Software Upgrade Convergence

Software upgrade involves downloading the new software from a WLAN controller followed by re-initialization of a MAP/RAP. If the controller does not use “cascaded reboot” using another controller, then convergence time is usually much higher. Because, when the controller reboots with new software, all APs associated with it lose LWAPP connection and have to re-establish it again. Which means convergence times vary according to the MAP location in the network with respect to the RAP.

If cascaded reboot is used, the network outage is reduced, however, the top-down flow of the image upgrades usually cause an almost similar chaotic scenario. This happens because, each higher-level node starting with go through the following steps before the next-level nodes can upgrade themselves:

1. Software version mismatch detection (mandatory).
2. LWAPP image upgrade (mandatory).
3. Re-boot and system initialization (mandatory).
4. IP address from DHCP server (optional).
5. LWAPP join with BMK (mandatory).

The lower-level nodes can establish a link after these steps are completed (except RAP). Then, they realize the software version mismatch and follow the same process as above. Additionally, they need to establish an LWAPP connection with the controller prior to following the above steps. Hence, the additional steps include:

7. Parent set and parent authentication (mandatory).
8. IP address from DHCP server (optional).
9. LWAPP join with BMK (mandatory).

Note

The key is in determining what the network is trying to do.

Throughput Analysis

Throughput depends on packet error rate and hop count.

Throughput is calculated as:

\[
\text{Throughput} = \text{BR} \times 0.5 \times \frac{1}{n} \times \text{PSR}
\]

BR = Raw Backhaul rate, i.e. 18, 24 Mbps
n = backhaul hop count
PSR = Packet Success Rate = (1.0-\text{PER}) = (0.0 .. 1.0)
Two assumptions apply to this calculation:

- There is no other traffic on the mesh.
- \(1/n\) factor is based on all hops hearing each other.

Generally, the throughput numbers per hop are as shown in Table 6.

<table>
<thead>
<tr>
<th>Hops</th>
<th>Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>One</td>
<td>~10Mbps</td>
</tr>
<tr>
<td>Two</td>
<td>~5Mbps</td>
</tr>
<tr>
<td>Three</td>
<td>~3Mbps</td>
</tr>
<tr>
<td>Four</td>
<td>up to 1Mbps</td>
</tr>
</tbody>
</table>

Capacity and throughput are orthogonal concepts. Throughput is one user's experience at node \(N\) and total area capacity is calculated over the entire sector of \(N\)-nodes and is based on the number of ingress and egress RAPs, assuming separate non-interfering channels.

For example, 4 RAPs at 10Mbps each deliver 40Mbps total capacity. So, one user at 2 hops out, logically under each RAP, could get 5Mbps each of TPUT, but consume 40Mbps of backhaul capacity.

With the Cisco Mesh solution, the per-hop latency is less than 10 msecs, and the typical latency numbers per hop range from 1~3 msecs. Overall jitter is also less than 3 msecs.

Throughput depends on the type of traffic being passed through the network. Traffic can be User Datagram Protocol (UDP) or Transmission Control Protocol (TCP). UDP sends a packet over Ethernet with a source and destination address and a UDP protocol header. It does not expect an acknowledgement (ACK). There is no assurance that the packet is delivered at the application layer.

TCP is similar to UDP but it is a reliable packet delivery mechanism. There are packet acknowledgments and a sliding window technique is used to allow the sender to transmit multiple packets before waiting for an ACK. There is a maximum amount of data the client will transmit (called a TCP socket buffer window) before it stops sending data. Sequence numbers are used to track packets sent and to ensure that they arrive in the correct order. TCP uses cumulative ACKs and the receiver reports how much of the current stream has been received. An ACK might cover any number of packets, up to the TCP window size.

TCP uses slow start and multiplicative decrease to respond to network congestion or packet loss. When a packet is lost, the TCP window will be cut in half and the back-off retransmission timer will be increased exponentially. Wireless is subject to packet loss due to interference issues and TCP will react to this packet loss. There is also a slow start recovery algorithm that is used to avoid swamping a connection when recovering from packet loss. The natural effect of these algorithms in a lossy network environment is to lessen the overall throughput of a traffic stream.

By default, the maximum segment size (MSS) of TCP is 1460 bytes, which results in a 1500-byte IP datagram. Therefore, TCP fragments any data packet that is larger than 1460 bytes, which can cause at least 30% throughput drop. In addition, the Cisco controller encapsulates IP datagrams in the 48-byte LWAPP tunnel header as illustrated in Figure 57. Therefore, any data packet that is longer than 1394 bytes is also fragmented by the controller, which results in up to 15% throughput decrease.
Managing the Cisco 1500 Series Mesh AP with WCS

Cisco WCS is a complete platform for enterprise-wide WLAN systems management. It provides a wide range of tools for visualizing and controlling the mesh, including histograms of signal-to-noise ratio, mesh detail information, 1500 Series Mesh AP neighbor and link information, seven-day temporal link information, and tools to identify and avoid RF interference.

Cisco WCS provides a centralized platform for managing a complete network of Cisco 1500 Series Mesh APs and Cisco 4400 Series Wireless LAN controllers, simplifying mesh planning and deployment and creating a cost effective way of managing and securing ongoing mesh wireless operations.

WCS Mesh AP Configuration

WCS provides an administrator a global few of every AP within the mesh. APs are searchable, which allows for easy configuration changes when needed. As shown in Figure 58, you can see that every configuration option you have in the controller’s GUI is available inside WCS.
**WCS Controller Configuration**

This section describes how to use WCS to manage a network.

**Adding a Controller to WCS**

To add a controller to the WCS, simply select the **Add Controller** option and enter the IP address, for the controller, as shown in **Figure 59**. APs that have LWAPP sessions with added controllers appear in WCS as configurable elements. Although they are now seen in WCS as an element, you still need to add them to the associated map location.
Outdoor Campus Maps

Outdoor campus maps let you drill down to specific outdoor areas. (See Figure 60.)
Adding APs and Antennas

Add the APs and attach the antennas for 2.4 GHz and the 5 GHz (see Figure 61).
**Heat Maps**

Outdoor areas with heat maps display what coverage the mesh is providing. (See Figure 62.)
Mesh Topology

The mesh topology can be displayed, with arrows indicating parent relationship. Link quality is indicated by color. You can drag your mouse over each link to get more information or click on it for the link details. (See Figure 63.)
Quick Link Information

By simply moving the mouse over a link, you can get information, such as linkSnr, link type, and ease value (see Figure 64).
Hierarchical Mesh AP Management

To get a hierarchical view of the network, click the Tree button, as shown in the red box in Figure 65. You can also choose a few RAPs and have a sectional view of a big mesh network.
RF Management Features

This section provides information on the RF management features.

SNR Graphs

Both up and down SNR graphs are available for each link, as shown in Figure 66 and Figure 67.
Mesh Links

Each link inside the WCS GUI has detailed information including the metrics of the link. The link SNR is the average SNR of the uplink and the downlink SNR. (See Figure 68.)
The Adjusted Link Metric field shows the value used to determine the least cost path to the RAP. This value is the ease to get to the rooftop access point and accounts for the number of hops. The lower the ease value, the less likely the path is used. (See Figure 69.)

The Unadjusted Link Metric shows the least path to get to the RAP unadjusted by the number of hops. The higher the value for the unadjusted link, the better the path is. (See Figure 70.)
The Parent Link Metric is the path value for getting to the first parent AP (toward the RAP).