Overview

This chapter describes the Cisco Unified Wireless Network Solution (UWN) and the mesh networking solution. In addition, this chapter describes the access point operating modes and security mechanisms.

This chapter contains the following sections

About the Cisco Unified Wireless Network Solution

The UWN is designed to provide 802.11 wireless networking solutions for enterprises and service providers. The Cisco UWN simplifies deploying and managing large-scale wireless LANs and enables a unique best-in-class security infrastructure. The operating system manages all data client, communications, and system administration functions, performs Radio Resource Management (RRM) functions, manages system-wide mobility policies using the operating system Security solution, and coordinates all security functions using the operating system security framework.

The Cisco UWN consists of Cisco wireless LAN controllers and their associated Cisco lightweight access points controlled by the operating system.

The Cisco UWN supports client data services, client monitoring and control, and all rogue access point detection, monitoring, and containment functions. The Cisco UWN uses Cisco lightweight access points, Cisco wireless LAN controllers, and the optional Cisco WCS to provide wireless services to enterprises and service providers.

Note This document refers to Cisco wireless LAN controllers throughout. Unless specifically called out, the descriptions herein apply to all Cisco wireless LAN controllers, including but not limited to Cisco 2000 series wireless LAN controllers, Cisco 4100 series wireless LAN controllers, Cisco 4400 series wireless LAN controllers, and the controllers on Cisco Wireless Services Modules (WiSMs).

About the Cisco Mesh Networking Solution

The mesh networking solution, which is part of the Cisco unified wireless network solution, enables two or more Cisco Aironet lightweight mesh access points (hereafter called *mesh access points)* to communicate with each other over one or more wireless hops to join multiple LANs or to extend 802.11b wireless coverage. Cisco mesh access points are configured, monitored, and operated from and through any Cisco wireless LAN controller deployed in the mesh networking solution.

The mesh access points are programmed to investigate their environment when they boot up, and perform internal configuration based on whether or not the mesh access point has a wired connection to the LAN. When the mesh access point is wired to a wireless LAN controller it auto-configures as a roof-top access point, and when the mesh access point is not wired to a wireless LAN controller it auto-configures as a pole-top access point.

The mesh access points are also programmed to find and associate with their nearest neighbors when they boot up. Thus, pole-top access points associate with other pole-top access points and any roof-top access point that they find, and roof-top access points associate with other pole-top access points after associating with a wireless LAN controller.

These two design features ensure that the mesh networking solution is self-healing when mesh access points are installed and when they recover from a power failure.

In all deployments, the backhaul is carried from one mesh access point to another mesh access point across one 802.11 radio, while client access is provided by another 802.11 radio. This design ensures that the mesh networking solution throughput is minimally impacted by client traffic.

Typical Cisco Mesh Networking Solution Deployments

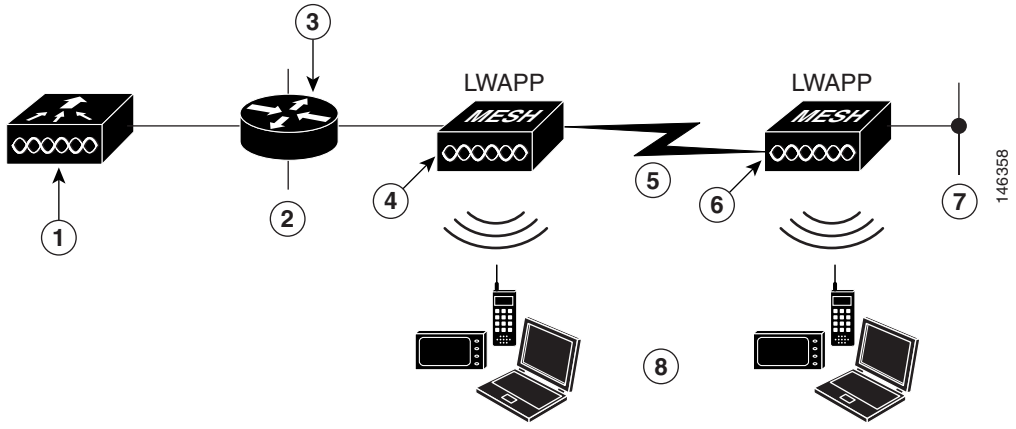
Supported mesh networking solution deployments are of one of three general types:

- Point-to-Point Deployment, page 1-2
- Point-to-Multipoint Deployment, page 1-3
- Mesh Deployment, page 1-5

Point-to-Point Deployment

In this simplest configuration, the mesh access points provide wireless access and backhaul to wireless clients, and can simultaneously support bridging between one LAN and a termination to a remote Ethernet device or another Ethernet LAN. Figure 1-1 shows a one-hop point-to-point deployment.

Figure 1-1 Point-to-Point Deployment



1	Cisco wireless LAN controller	**2**	LAN 1
3	Router or Switch — Required when network is used for bridging LAN at Point 2 and LAN at Point 7.	**4**	Roof-top access point: Cisco Aironet 1030 remote edge lightweight access point or Cisco Aironet 1500 series lightweight outdoor access point.
5	Wireless Backhaul	**6**	Pole-top access point Cisco Aironet 1030 remote edge lightweight access point or Cisco Aironet 1500 series lightweight outdoor access point. (See Note)
7	Optional wired connection to Ethernet termination device (such as a camera) or LAN 2; requires a Router or Switch at Point 3. (See Note)	**8**	Wireless Clients

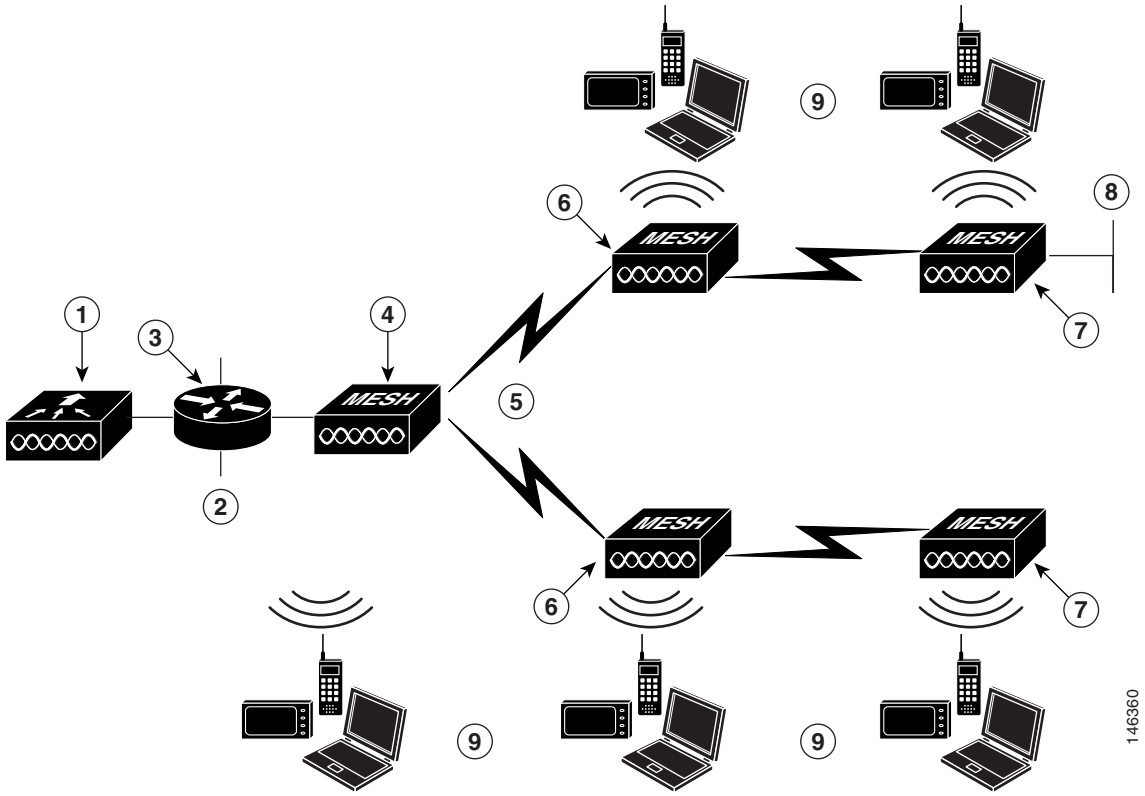
Note Cisco Aironet 1030 remote edge lightweight access points and Cisco Aironet 1500 series lightweight outdoor access points support single-hop deployments. However, Cisco Aironet 1500 series lightweight outdoor access points are required to support multi-hop backhaul deployments.

Point-to-Multipoint Deployment

In this configuration, the mesh access points provide wireless access and backhaul to wireless clients, and can simultaneously support bridging between one LAN and one or more terminations to Ethernet devices or other Ethernet LANs. Figure 1-2 shows a two-hop point-to-multipoint deployment.

Regardless of the number of hops in the point-to-multipoint deployment, the mesh access points on each branch are configured to talk only with the mesh access points on their branch, and not with mesh access points on other branches.

Figure 1-2 Point-to-Multipoint Deployment



1	Cisco wireless LAN controller	**2**	LAN 1
3	Router or Switch—Required when network is used for bridging LAN at Point **2** and LAN at Point **8**	**4**	Roof-top access point: Cisco Aironet 1030 remote edge lightweight access point or Cisco Aironet 1500 series lightweight outdoor access point
5	Wireless Backhaul	**6**	Pole-top access point: Cisco Aironet 1030 remote edge lightweight access point or Cisco Aironet 1500 series lightweight outdoor access point (See Note)
7	Pole-top access point: Cisco Aironet 1500 series lightweight outdoor access point (See Note)	**8**	Optional wired connection to Ethernet termination device (such as a camera) or LAN 2; requires a Router or Switch at Point **3**
9	Wireless clients		

Note Cisco Aironet 1030 remote edge lightweight access points and Cisco Aironet 1500 series lightweight outdoor access points support single-hop deployments. However, Cisco Aironet 1500 series lightweight outdoor access points are required to support multi-hop backhaul deployments.

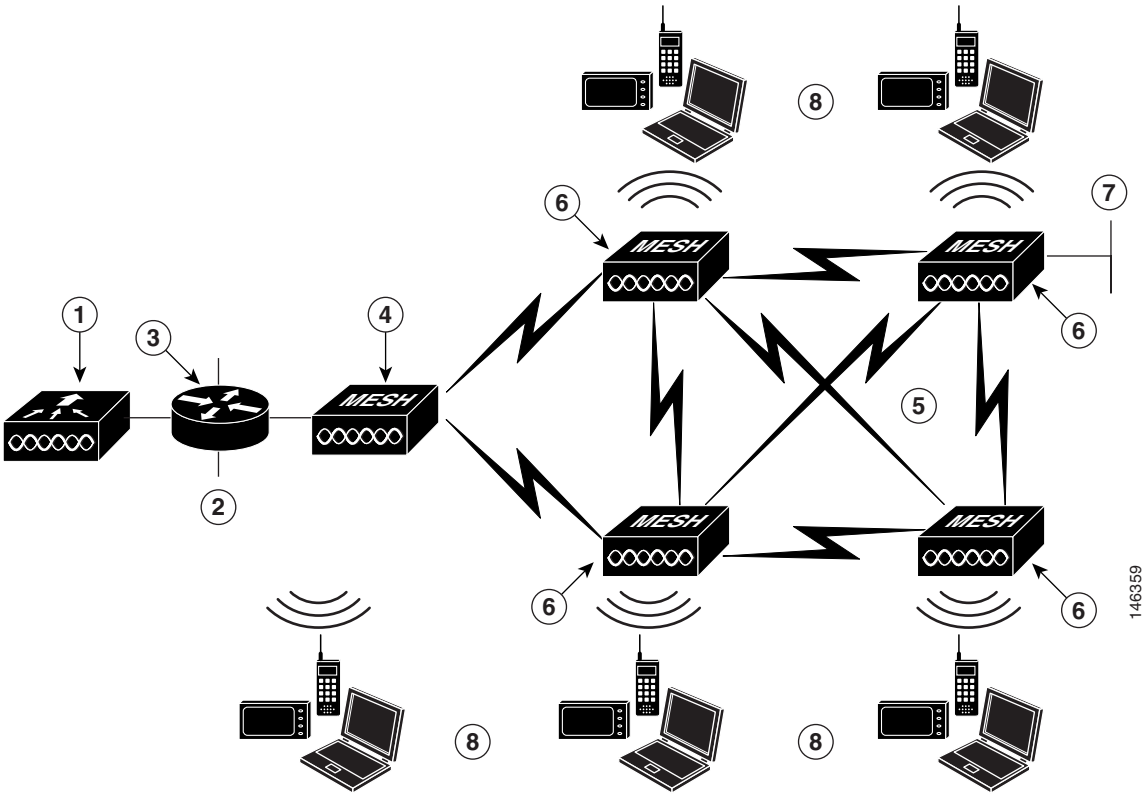
Mesh Deployment

In this configuration, the mesh access points provide wireless access and backhaul to wireless clients, and can simultaneously support bridging between one LAN and one or more terminations to Ethernet devices or other Ethernet LANs. Figure 1-3 shows a typical mesh deployment.

Regardless of the number of hops in the point-to-multipoint deployment, the mesh access points on each branch are configured to talk to all other mesh access points within range in the deployment. Also, when any of the backhaul links fails, the mesh access points automatically reroute the traffic using another path. This results in a mesh networking solution that is self-configuring and self-healing.

Note Cisco Aironet 1030 remote edge lightweight access points support single-hop deployments while Cisco Aironet 1500 series lightweight outdoor access points support both single- and multi-hop deployments. As such, Cisco Aironet 1500 series lightweight outdoor access points can be used as roof-top access points and as pole-top access points one or more hops from the Cisco wireless LAN controller.

Figure 1-3 Mesh Deployment



1	Cisco wireless LAN controller	**2**	LAN 1
3	Router or Switch -- Required when network is used for bridging LAN at Point **2** and LAN at Point **7**	**4**	Roof-top access point: Cisco Aironet 1030 remote edge lightweight access point or Cisco Aironet 1500 series lightweight outdoor access point
5	Wireless Backhaul	**6**	Pole-top access point: Cisco Aironet 1500 series lightweight outdoor access point (Note)
7	Optional wired connection to Ethernet termination device (such as a camera) or LAN 2; requires a Router or Switch at Point **3**	**8**	Wireless clients

Access Point Operating Modes (Roles)

You can operate the Cisco Aironet 1030 remote edge lightweight access points and Cisco Aironet 1500 series lightweight outdoor access points in one of the following roles:

- "Roof-top Access Point (RAP)" on page 1-6
- "Pole-top Access Point (PAP)" on page 1-6

Roof-top Access Point (RAP)

RAPs have a wired connection to a Cisco wireless LAN controller. They use the backhaul wireless interface to communicate with neighboring PAPs. RAPs are the parent node to any bridging or mesh network and connect a bridge or mesh network to the wired network; therefore, there can only be one RAP for any bridged or mesh network segment.

Note When using the mesh networking solution for LAN-to-LAN bridging, do not connect a RAP directly to a Cisco wireless LAN controller. A switch or router between the Cisco wireless LAN controller and the RAP is required because Cisco wireless LAN controllers do not forward Ethernet traffic coming from an LWAPP-enabled port. RAPs can work in Layer 2 or Layer 3 LWAPP mode.

Pole-top Access Point (PAP)

PAPs have no wired connection to a Cisco Wireless LAN controller. They can be completely wireless, supporting clients communicating with other PAPs or RAPs, or they can be used to connect to peripheral devices or a wired network. The Ethernet port is disabled by default for security reasons, but you should enable it for PAPs. Refer to "Configuring Cisco Aironet Lightweight Mesh Access Points" on page 2-1 for more information about enabling Ethernet bridging.

Note Cisco Aironet 1030 remote edge lightweight access points support single-hop deployments while Cisco Aironet 1500 series lightweight outdoor access points support both single- and multi-hop deployments. As such, Cisco Aironet 1500 series lightweight outdoor access points can be used as rooftop access points and as pole-top access points one or more hops from the Cisco Wireless LAN controller.

Access Point Startup Sequence

The following list describes what happens when the RAP and PAP start up:

- All traffic travels through the RAP and the Cisco wireless LAN controller before being sent to the LAN.
- When the RAP comes up, the PAPs automatically connect to it.
- The connected link uses a shared secret to generate a key that is used to provide AES (Advanced Encryption Standard) for the link. For more information, refer to "Access Point Security Mechanisms" on page 1-7.
- Once the remote PAP connects to the RAP, the mesh access points can pass data traffic.
- Users can change the shared secret and otherwise configure the mesh access points using the Cisco command line interface (CLI), the Cisco Web user interface of the controller, or the Cisco Wireless Control System (Cisco WCS). See "Configuring Cisco Aironet Lightweight Mesh Access Points" on page 2-1 for more information. Cisco recommends that you modify the shared secret.

Access Point Security Mechanisms

Listed below are some of the built-in mesh access point security mechanisms:

- The Cisco wireless LAN controller maintains a mesh access point bridge authorization MAC address list. The Cisco wireless LAN controller responds only to discovery requests from mesh access point bridges that appear on the authorization list. This authorization list is separate from the AP authorization list. The bridge authorization list cannot be disabled.
- The Cisco wireless LAN controller uses two independent keys to perform bridge authentication. One key is pre-assigned during manufacturing and is common to all mesh access points. This is the default shared secret. The second key should be configured to allow the entry of the first mesh access point MAC address onto the mesh access point authorization table. This is the mesh access point bridge shared secret. Both the default shared secret and the bridge shared secret have the same attributes and requirements of an 802.11i pre-shared key. Refer to "Configurable Cisco Aironet Lightweight Mesh Access Point Parameters" on page 2-6.
- The Cisco wireless LAN controller uses the default shared secret to allow a mesh access point to initially join, and to allow initial configuration of the bridge shared secret.
- After being configured with a bridge shared secret, the mesh access point performs the discovery and join operations using the bridge shared secret for key exchanges with its neighbors and for the Join Authenticator.