Deployment Guide: Cisco Mesh Networking Solution

Release 3.2

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-8470-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

• Turn the television or radio antenna until the interference stops.

• Move the equipment to one side or the other of the television or radio.

• Move the equipment farther away from the television or radio.

• Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Deployment Guide: Cisco Mesh Networking Solution

Preface

This section describes the objectives, audience, organization, and conventions of the *Deployment Guide: Cisco Mesh Networking Solution.*

Audience

This guide is for the networking professional who plans deployments and initial configuration of the Cisco Unified Wireless Network Solution, hereafter referred to as the *Cisco UWN* and the Cisco Mesh Networking Solution, hereafter referred to as the *mesh networking solution*. To use this guide, you should have experience working with Cisco Aironet lightweight access points and be familiar with the concepts and terminology of wireless local area networks.

Purpose

This guide provides the information you need to plan and initially configure your mesh networking solution, including procedures for using the CLI commands that have been created or changed for use with the mesh networking solution. It does not provide detailed information about these commands.

Organization

This guide contains the following chapters:

Chapter 1, "Overview," 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.

Chapter 2, "Access Point Installation and Configuration," describes how to install and configure Cisco Aironet mesh access points.

Conventions

This publication uses these conventions to convey instructions and information:

Command descriptions use these conventions:

- Commands and keywords are in **boldface** text.
- Arguments for which you supply values are in italic.
- Square brackets ([ ]) mean optional elements.
- Braces ({ }) group required choices, and vertical bars (|) separate the alternative elements.
- Braces and vertical bars within square brackets ([{ | }]) mean a required choice within an optional element.

Interactive examples use these conventions:

- Terminal sessions and system displays are in screen font.
- Information you enter is in boldface screen font.
- Nonprinting characters, such as passwords or tabs, are in angle brackets (< >).

Notes and cautions use these conventions and symbols:

Note Means *reader take note.* Notes contain helpful suggestions or references to materials not contained in this manual.

Caution Means *reader be careful.* In this situation, you might do something that could result in equipment damage or loss of data.

Related Publications

For more information about outdoor access points and related products, refer to the *Release Notes for Cisco Wireless LAN Controllers and Cisco Lightweight Access Points for Cisco Unified Wireless Network Solution,* which describes features and caveats for the outdoor access points. These notes are available on the Cisco CCO website at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/wireless/index.htm

Other related publications are:

- *Cisco Wireless LAN Controller Command Reference*
- *Wireless LAN Controller Online Help*
- *Wireless Control System Online Help*
- *Quick Start Guide: Cisco Aironet 1000 Series Lightweight Access Points with External Antennas*

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

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

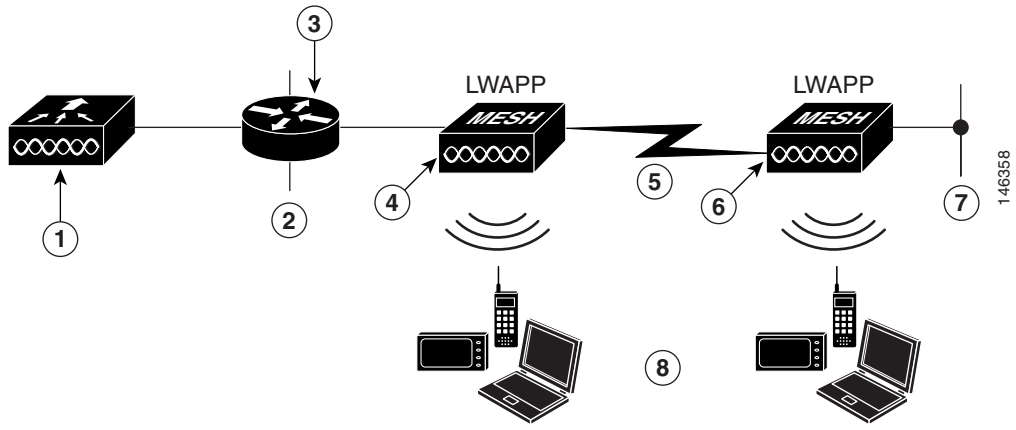
Supported mesh networking solution deployments are of one of three general types:

- 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 (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

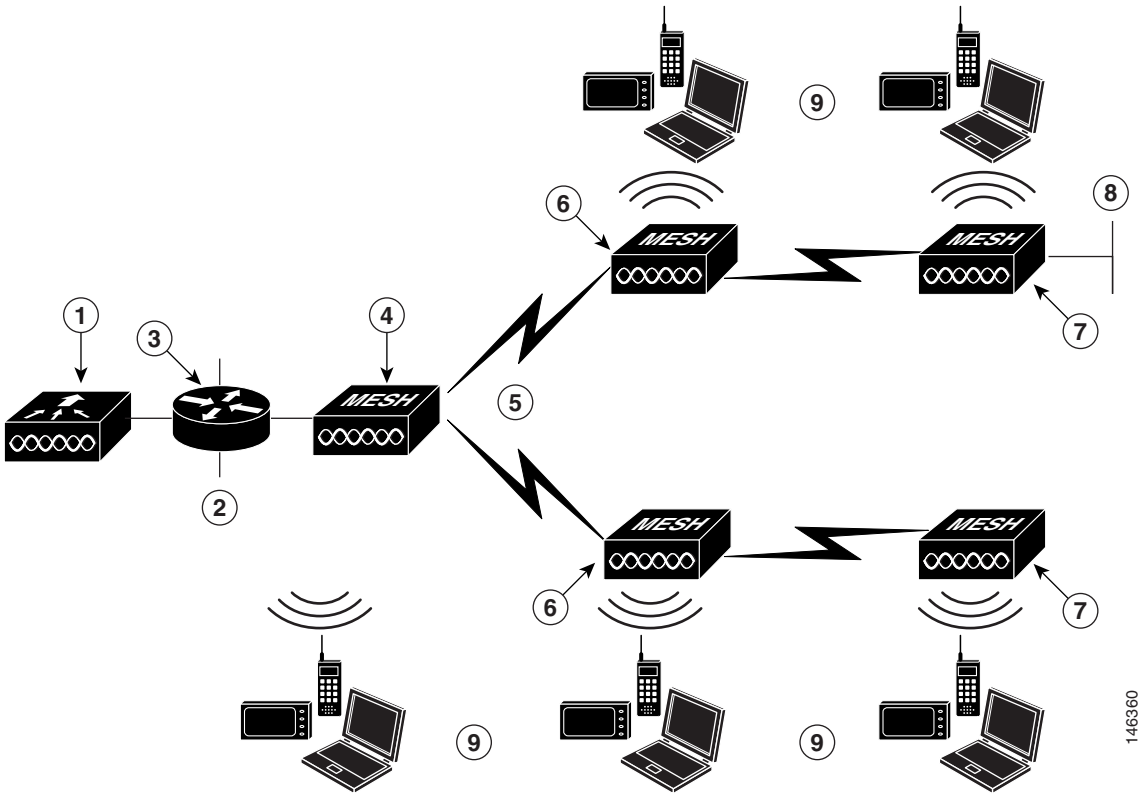
Note Cisco Aironet 1030 remote edge lightweight access points and Cisco Aironet 1500 series lightweight outdoor access points support single-hop deployments. However, Cisco Aironet 1500 series lightweight outdoor access points are required to support multi-hop backhaul deployments.

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 (Note)
7	Pole-top access point: Cisco Aironet 1500 series lightweight outdoor access point (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.

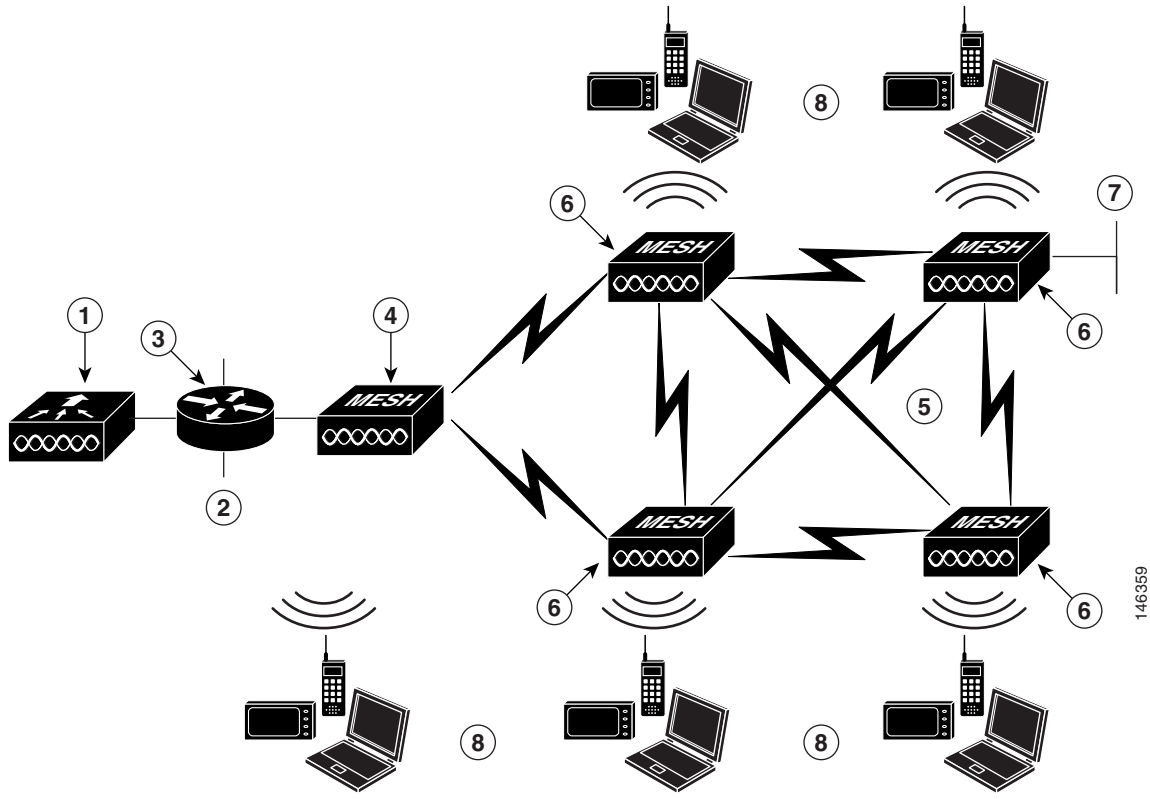
Mesh Deployment

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 1-7
- "Pole-top Access Point (PAP)" on page 1-7

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. For more information, refer to "Zero Touch Configuration" on page 2-3.
- 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 1-8.
- 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). Refer to "Tools for Configuring the Cisco Aironet Lightweight Mesh Access Point Parameters" on page 2-7 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.

Access Point Installation and Configuration

This chapter describes how to install and configure Cisco Aironet mesh access points.

This chapter contains the following sections

Installing Cisco Aironet Lightweight Mesh Access Points

- To install a Cisco Aironet 1030 remote edge lightweight access point, refer to the *AP1020 and AP1030 Cisco Aironet 1000 Series Lightweight Access Points with External Antennas - Quick Start Guide.*
- To install a Cisco Aironet 1500 series lightweight outdoor access point, refer to the *Quick Start Guide: Cisco Aironet 1500 Series Lightweight Outdoor Access Points.*
- Also refer to the *Cisco Wireless LAN Controller Configuration Guide* for additional information on updating and configuring the wireless LAN controllers and associated mesh access points.

After you have installed the mesh access points, follow these steps to complete your installation.

Configuring Cisco Aironet Lightweight Mesh Access Points

This section describes how to configure the mesh access points. It includes the following sections:

Configuring the LWAPP Mode

In the Layer 2 LWAPP mode, mesh access points do not need to be configured. In this case, mesh access point configuration is optional. However, to use the access points without a DHCP server in the Layer 3 LWAPP mode, you need to configure the access points to use static IP.

To configure the access points to use static addresses, follow these steps:

Step 1 Switch the controller to the Layer 2 LWAPP mode.

Step 2 Repeat the following steps for every access point:

a. Connect the access point to the switch connected to the controller (connect only one access point at a time).

b. Use the switch's CLI to configure the IP address of the access point.

Step 3 Change the controller back to the Layer 3 LWAPP mode.

Step 4 Save the configuration.

Step 5 Restart the switch and Define the ap-manager interface.

Once the network is in the Layer 3 LWAPP mode, you can change the IP address of the access point from the CLI or GUI.

Caution Do not configure an access point's static address in a live network because doing so causes the access point to restart. If the access point is a RAP, then the entire network goes down.

Configuring the Cisco Wireless LAN Controller

Zero Touch configuration is enabled by default on the Cisco wireless LAN controller. To understand Zero Touch configuration, refer to "Zero Touch Configuration" on page 2-3. To enable or disable Zero Touch configuration, refer to "Enabling or Disabling Zero Touch Configuration" on page 2-4.

Configuring MAC Filtering

For a mesh access point to connect to a Cisco wireless LAN controller, you need to add the access point to the controller's MAC filtering list.

To add the access point to a controller's MAC filtering list, do one of the following:

- In the Web user interface of the controller, choose the **MAC filtering** option (**Security > AAA > MAC Filtering**) and manually add the mesh access points.
- In Cisco WCS, go to the **MAC filtering** template (**Configure > Templates > Security > MAC Filtering**); create a list of bridging mesh access points, and send them to multiple Cisco wireless LAN controllers.

Zero Touch Configuration

If Zero Touch configuration is enabled on the Cisco wireless LAN controller, the mesh access point does the following to accomplish a secure Zero Touch:

1. When a mesh access point is first installed, it tries to find its role automatically. If it has a wired connection to a LAN with a Cisco wireless LAN controller, it assumes the role of RAP; otherwise it becomes a PAP.
2. Next, the mesh access point determines the backhaul channel.
   - If it is a RAP, it already has a secure LWAPP connection to the Cisco wireless LAN controller and uses the configured RAP backhaul interface (Default: 802.11a).
   - If it is a PAP, it scans the backhaul interfaces and channels for neighbor mesh access points. When it finds a neighbor mesh access point with the same bridge group name and a path back to the Cisco wireless LAN controller, it makes that mesh access point its parent. If the PAP finds more than one neighbor mesh access point, it uses a least-cost algorithm to determine which parent has the best path back to the Cisco wireless LAN controller.

   Note When the mesh networking solution includes one or more mesh access points, make sure that all the access points can operate on the same channel as that of the root access point.

3. To set up a secure LWAPP connection with the Cisco wireless LAN controller, the PAP sends its default shared secret key and MAC address to set up a temporary secured connection. The Cisco wireless LAN controller validates the MAC address against the allowed devices list, and if found, it sends the shared secret key to the PAP and disconnects.The PAP stores the shared secret key and uses it to set up a secure LWAPP connection.
4. If a PAP loses connection to the Cisco wireless LAN controller, it searches for valid neighbors using the mesh access point bridge group name and scans the backhaul interfaces and channels. When it finds a neighbor mesh access point, it makes that mesh access point its parent. If it already has a shared secret key, it uses that key and tries to set up a secure LWAPP connection to the Cisco wireless LAN controller. If the shared secret key does not work, it uses the shared default secret key and attempts to get a new shared secret key.

Note The RAP offers service in one band for the clients and uses another band for backhaul (communication between the mesh access points).

Note Zero Touch configuration may not work if the RAP is a Cisco Aironet 1030 remote edge lightweight access point, and the PAP is a Cisco Aironet 1500 series lightweight outdoor access point. The Cisco Aironet 1030 remote edge lightweight access point defaults to channel 52, and the Cisco Aironet 1500 series lightweight outdoor access point cannot operate on that channel.

Enabling or Disabling Zero Touch Configuration

You can enable or disable Zero Touch configuration using the Web user interface or Cisco WCS.

Web User Interface

Path: Wireless > Bridging

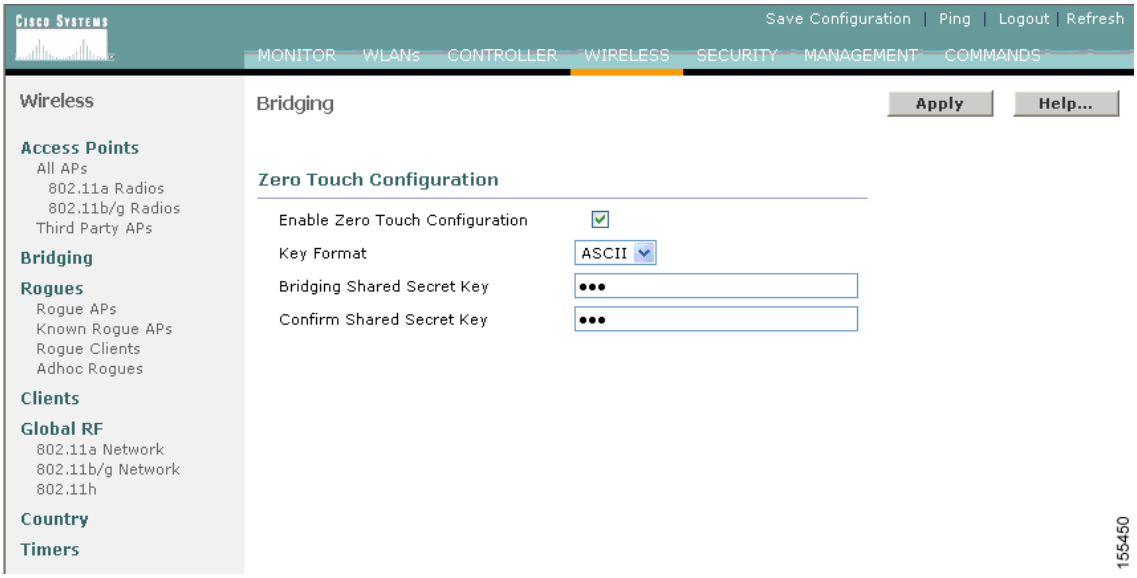


Table 2-1 describes the bridging parameters.

Table 2-1 Bridging Parameters

Parameter	Description
Zero Touch Configuration	By default, this check box is checked. When you disable this option, the Cisco wireless LAN controller does not provide the shared secret key. For the mesh access point to establish a connection to the Cisco wireless LAN controller, pre-configure the mesh access point shared secret key using the Cisco wireless LAN controller CLI as described in the Cisco *Wireless LAN Controller Command Reference.* When you enable this option, the mesh access point gets the shared secret key from the Cisco wireless LAN controller with the default shared key. Usage: As the administrator, you can enable this feature and allow all the mesh access points to join the network. After the network is stabilized, you can disable this feature, which further secures your networks against any rogue access points that might try and get the shared secret key from the Cisco wireless LAN controller. **Note** Even when you enable this option, the mesh access points are checked against the MAC filter list before they are allowed to communicate with the Cisco wireless LAN controller.

Table 2-1 Bridging Parameters (Continued)

Key Format	Specify the Shared Secret Key format. It can be ASCII or Hex.
Bridging Shared Secret Key	This field is enabled only if the Zero Touch Configuration option is enabled. This is the key that is provided to the mesh access points for them to establish a secure LWAPP connection with the Cisco wireless LAN controller. The key should be at least 32 characters long in Hex or ASCII format. A default shared secret key is assigned at the manufacturing stage. It is not visible to you. **Note** When you change the shared secret key, the Cisco wireless LAN controller automatically sends the change to all of the RAPs, which causes the PAPs to lose connectivity until they are able to obtain the new shared secret key from the Cisco wireless LAN controller.
Confirm Shared Secret Key	Confirm the shared secret key.

Click **Apply** to save the changes made.

For more information, refer to the *Cisco Web User Interface Online Help*.

Cisco WCS User Interface

Path: Configure > Controllers (click an IP address item, click 802.11, and then click Bridging to access this page).

A section of the screen is displayed below.

The field parameters are the same as in Web user interface. Refer to "Web User Interface" on page 2-4 for details.

Click **Save** to save the changes or click **Audit** to validate the changes made.

For more information, refer to the *Cisco WCS User Interface Online Help.*

Cisco Wireless LAN Controller CLI

Table 2-2 lists the commands to configure Zero Touch configuration using the Cisco wireless LAN controller CLI.

Table 2-2 Zero Touch Configuration Commands

Parameter	Commands
Zero Touch Configuration	**config network zero-config** {**enable** | **disable**} This command let's you enable or disable Zero Touch configuration.
Bridging Shared Secret Key	**config network bridging-shared-secret** *name* This command lets you specify the key that is provided to the mesh access points for them to establish a secure LWAPP connection with the Cisco wireless LAN controller. The key should be at least 32 characters long in Hex or ASCII format.
Key Format	**config network bridging-shared-secret** *key* This command lets you specify the Shared Secret Key format. It can be ASCII or Hex.

Configurable Cisco Aironet Lightweight Mesh Access Point Parameters

Table 2-3 lists the mesh access point parameters that you can configure:

Table 2-3 Configurable Mesh Access Point Parameters (continued)

Parameter	Values	Description
Shared Secret Key	Any key in ASCII or Hex format that is at least 32 characters long. A default shared secret key is assigned at the manufacturing stage. It is not visible to you.	The shared secret key is provided by the Cisco wireless LAN controller during the connection process. This can be set manually to avoid using the default shared secret key to get the key from the Cisco wireless LAN controller. If the shared secret key is not correct, the access point uses the default shared key to get the key from the Cisco wireless LAN controller.
Role	• Auto • RAP • PAP Default: Auto	Indicates if a mesh access point is a RAP or PAP. **Auto:** When the mesh access point comes up, it automatically determines if it can be a RAP or PAP. **RAP/PAP:** The access point's role is pre-defined by you.
Ethernet Bridging	• Enabled • Disabled Default: Disabled	Specifies whether ethernet bridging on the access point is enabled or disabled.

Table 2-3 Configurable Mesh Access Point Parameters (continued)

Parameter	Values	Description
Bridge Group Name	This is a string of a maximum of 10 characters. A default mesh access point bridge group name is assigned at the manufacturing stage. It is not visible to you. The Bridge Group Name field appears blank in the GUI until you change it.	Use bridge group names to logically group the mesh access points to avoid two networks on the same channel from communicating with each other. For the mesh access points to communicate, they must have the same bridge group name. **Note** For configurations with multiple RAPs, make sure that all RAPs have the same bridge group name to allow failover from one RAP to another. Conversely, for configurations where separate sectors are required, make sure that each RAP and associated PAPs have separate bridge group names.
Data Rate	A rate in Mbps. Default for 802.11a: 18 Mbps	This is the rate at which data is shared between the mesh access points. This is fixed for a whole network. Default data rate is 18 Mbps, which you should use for the backhaul. Valid data rates: • for 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 **Note** NEVER change the data rate for a deployed mesh networking solution. If you do, each RAP and PAP may need to be manually reconfigured to restore the network.

Tools for Configuring the Cisco Aironet Lightweight Mesh Access Point Parameters

The mesh access point parameters can be configured to varying levels using Cisco WCS, the Cisco wireless LAN controller command line interface (CLI) or the Cisco wireless LAN controller Web user interface). Table 2-4 lists the details.

Table 2-4 Mesh Access Point Parameter Configuration Tools

	Parameter				
Tool	Role	Shared Secret Key	Bridge Group Name	Data Rate	Ethernet Bridging
Cisco wireless LAN controller CLI	Yes	Yes	Yes	Yes	Yes
Cisco wireless LAN controller Web user interface	No	Yes	No	Yes	Yes
Cisco WCS	No	Yes	No	Yes	Yes

Note The following section provides only a general overview of the configuration methods. Refer to the individual guides for detailed information.

Cisco Wireless LAN Controller CLI

Table 2-5 lists the commands to configure the mesh access point parameters using the Cisco wireless LAN controller CLI.

Table 2-5 CLI-Configurable Mesh Access Point Parameters

Parameter	Commands
Data Rate (Mbps)	**config ap bhrate** *rate ap-name* The data rates for 802.11a can be: 6, 9, 12, 18, 24, 36, 48, 54
Bridge Group Name	**config ap bridgegroupname set** *name* The name is a string of up to 10 characters.
Role	**config ap role** *role* The role can be Auto, RAP, or PAP. By default, the role is set to Auto.
Bridging Shared Secret Key	**config network bridging-shared-secret** *name* This command lets you specify the key that is provided to the mesh access points for them to establish a secure LWAPP connection with the Cisco Wireless LAN controller. The key should be at least 32 characters long in Hex or ASCII format.
Ethernet Bridging	**config ap bridging** {**Enable** | **Disable**} Use this command to enable or disable Ethernet-to-Ethernet bridging on Cisco access points.

Table 2-6 lists related commands.

Table 2-6 CLI Commands for Viewing Backhaul Interface and Data Rate Information

Purpose	Use This CLI Command
To view the current backhaul interface	**show ap bhmode** <*ap-name*>
To view the current data rate	**show ap bhrate** <*ap-name*>

For more information, refer to the *Cisco Wireless LAN Controller Command Reference.*

Web User Interface

Table 2-7 lists the path to be used in the Web user interface to configure the mesh access point parameters.

Table 2-7 Web User Interface Path for Configuring Mesh Access Point Parameters

Parameter	Path
Data Rate (Mbps)	Wireless > Access Points > All APs
Ethernet Bridging	Click **Detail**. The Data Rate and Ethernet Bridging parameters are in the Bridging Information section.

A section of the screen is displayed below.

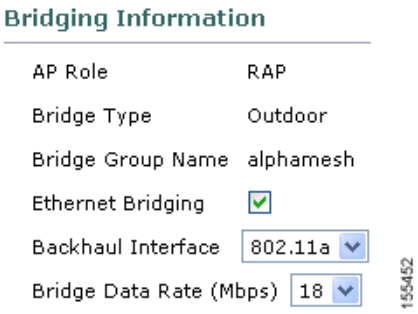


Table 2-8 describes the parameters.

Table 2-8 Bridging Information Parameters

Parameter	Description
AP Role	Not an editable field. Specifies if the mesh access point is a RAP or PAP. Role can be configured using the CLI.
Bridge Type	Not an editable field. Specifies whether the mesh access point is an indoor or outdoor access point. Configure using the CLI.
Bridge Group Name	Not an editable field. Specifies the mesh access point bridge group name.
Bridge Data Rate	Set the data rate. The drop-down list displays the data rates depending on the backhaul interface.
Ethernet Bridging	Check this check box to enable Ethernet bridging.

Click **Apply** to save your changes.

For more information, refer to the *Cisco Web User Interface Online Help*.

Cisco WCS User Interface

Table 2-9 lists the path in the Cisco WCS user interface to configure the mesh access point parameters.

Table 2-9 WCS User Interface Path for Configuring Mesh Access Point Parameters

Parameter	Path
Data Rate (Mbps)	Configure > Access Points Click the name of the access point. The Data Rate and Ethernet Bridging parameters are in the Bridging Information section.
Ethernet Bridging	

A section of the screen is displayed below.

Table 2-10 describes the parameters.

Table 2-10 Bridging Information Parameters

Parameter	Description
Role	Not an editable field. Specifies whether the mesh access point is a RAP or PAP. Role can be configured using Zero Touch configuration.
Bridge Group Name	Not an editable field. Specifies the mesh access point bridge group name.
Type	Not an editable field. Specifies if the mesh access point is an indoor or outdoor AP.
Backhaul Interface	Not an editable field. Specifies the backhaul setting of the mesh access point.
Data Rate (Mbps)	Set the data rate. The drop-down list displays the data rates depending on the backhaul interface set.
Ethernet Bridging	Check this check box to enable Ethernet bridging.

Click **Save** or **Audit** to validate the changes made.

For more information, refer to the *Cisco WCS User Interface Online Help.*

B

Backhaul Interface The 802.11a wireless protocol used to route packets between the RAP and PAP. For example, a PAP configured with the 802.11a backhaul interface serves clients on the 802.11b protocol and routes the client packets to its parent and neighboring access points on the 5 GHz 802.11a band.

C

CRC Packet A cyclic redundancy check packet is an error packet that ends on an eight-bit boundary and has a valid length, but the four byte checksum at the end of the packet is incorrect.

F

Frame Alignment Packet A frame alignment packet is an error packet that does not end on an eight-bit boundary (there are seven or less bits after the end of the last byte).

L

LWAPP The Light Weight Access Point Protocol (LWAPP) is a protocol allowing a Cisco Wireless LAN Controller to interoperably control and manage a collection of Cisco Aironet lightweight access points. The protocol is independent of wireless Layer 2 technology, but an 802.11 binding is provided.

N

Nonce Nonce is a parameter that varies with time. A nonce can be a time stamp, a visit counter on a Web page, or a special marker intended to limit or prevent the unauthorized replay or reproduction of a file.

Because a nonce changes with time, it is easy to tell whether or not an attempt at replay or reproduction of a file is legitimate; the current time can be compared with the nonce. If it does not exceed it or if no nonce exists, then the attempt is authorized. Otherwise, the attempt is not authorized.

O

Oversize Packet Oversize packet is an error packet that is longer than Ethernet's maximum packet size of 1518 bytes.

P

PAPs Pole-top access points (PAPs) have no wired connection to a Cisco Wireless LAN Controller. They can be completely wireless supporting clients, communicating to other PAPs and a RAP to get access to the LAN, or wired and serving as bridge to a remote LAN.

R

RAPs Roof-top Access Points have a wired LWAPP connection back to a Cisco Wireless LAN Controller. They use the backhaul wireless interface to communicate to neighboring pole-top access points. RAPs are the parent node to any bridging or mesh network and connect a bridge or mesh network to the wired network; therefore, only one RAP can exist for any bridged or mesh network.

Runt Packet Runt packet is an error packet that is less than the Ethernet's minimum packet size of 64 bytes.