



Overview

Cisco Aironet access points are wireless LAN transceivers that serve as the center point of a stand-alone wireless network or as the connection point between wireless and wired networks. In large installations, wireless users within radio range of an access point can roam throughout a facility while maintaining seamless, uninterrupted access to the network.

Your access point can contain two radios: a 2.4-GHz radio in an internal mini-PCI slot and a 5-GHz radio module in an external, modified cardbus slot. The access point supports one radio of each type, but it does not support two 2.4-GHz or two 5-GHz radios. You can configure the radios separately, using different settings on each radio.

The access point uses a browser-based management system, but you can also configure the access point using a terminal emulator, a Telnet session, Secure Shell (SSH), or Simple Network Management Protocol (SNMP).

This chapter provides information on the following topics:

- [Key Features, page 1-2](#)
- [Management Options, page 1-3](#)
- [Roaming Client Devices, page 1-3](#)
- [Network Configuration Examples, page 1-8](#)

Key Features

This section describes the key features of the access point firmware. The following are the key features of this firmware version:

- Multiple IEEE 802.11 service set identifiers (SSIDs) allow you to create different levels of network access and to access virtual LANs (VLANs). You can configure up to 16 separate SSIDs to support up to 16 VLANs for each access point radio. Each VLAN can have a different wireless security configuration so that the devices that support the latest Cisco security enhancements can exist alongside legacy devices. This additional access point functionality enables a variety of users having different security levels to access different parts of the network.
- Quality of service (QoS), which allows various devices on the network to communicate more effectively. The access point now supports QoS for wireless Voice over IP (VoIP) telephones and downlink prioritized channel access for streaming audio and video traffic. Filters can also be set to prioritize traffic based on VLAN, VoIP address-based filters, protocol, or port.
- Proxy Mobile IP provides a method for seamless inter-subnet roaming. When you enable proxy Mobile IP on your access points, client devices that roam from one subnet to the next maintain their IP address and session. The access point acts as a Mobile IP proxy for client devices that do not have mobile IP software installed. The access point informs the foreign agent router that the client has roamed to another subnet, while the foreign agent directs the home agent to reroute packets to it.
- Centralized administrator authentication uses an AAA server to authenticate users if the user administration feature is enabled on the access point. When a login is attempted, the AAA server verifies the user login and passes back the appropriate privileges for the user or an administrator.
- Better handling of lost Ethernet links causes a number of actions to be executed when an access point loses backbone connectivity:
 - No action—the access point continues to maintain associations with clients and manages traffic between them, but traffic to the backbone is not passed. When the backbone is restored, the access point begins passing traffic to and from the wired network.
 - Switch to repeater mode—the access point tries to connect to a root access point using any of the configured SSIDs. If it cannot connect, all clients are disassociated and the access point removes itself from the wireless network until connectivity is restored.
 - Shut the radio off—all clients are disassociated and the access point removes itself from the wireless network until backbone connectivity is restored.
 - Restrict to SSID—the access point allows association using a restricted SSID (for administrator troubleshooting and diagnosis purposes).
- Authentication server management includes two new features in release 12.01T1:
 - Display of active authentication servers—for each authentication type: 802.1x/LEAP, MAC, or Admin Authentication (if enabled), the active server is identified by a green color.
 - Automatic return to primary authentication server—if the selected RADIUS server (primary) is not reachable after a predetermined period of time-out and retries, the access point uses the next server listed.
- Reporting access points that fail authentication with LEAP provides a passive method of detecting rogue access points in a LEAP enabled network. It is passive because access points do not actively look for or detect a rogue access point in the wireless network. Instead, the access point depends on LEAP enabled clients to report rogue access points.

- Secure Shell (SSH) support for providing a strong user authentication and encryption of management traffic. SSH is a software package that provides a cryptographically secure replacement for or an alternative to Telnet. It provides strong host-to-host and user authentication as well as secure encrypted communications over a non secure network. The feature operates as follows:
 - The SSH server on the access point listens to its TCP port 22 for requests.
 - When a request from a client is received, the access point sends a public key, supported cipher specification details, and supported authentication type (password only) to the client.
 - The client generates a double encrypted session key and sends it to the access point along with the chosen cipher specification.
 - The access point authenticates the client based on a user ID and password when the user manager feature is enabled.
 - If authentication is successful, all management traffic between the client and access point is encrypted using the session key.

Management Options

You can use the access point management system through the following interfaces:

- A web-browser interface
- A command-line interface (CLI)
- Simple Network Management Protocol (SNMP)

The access point's management system pages are organized the same way for the web- browser interface and the CLI. The examples in this manual are all taken from the browser interface. [Chapter 2, "Using the Management Interfaces"](#) provides a detailed description of each management option.

Roaming Client Devices

If you have more than one access point in your wireless LAN, wireless client devices can roam seamlessly from one access point to another. The roaming functionality is based on signal quality, not proximity. When a client's signal quality drops, it roams to another access point.

Wireless LAN users are sometimes concerned when a client device stays associated to a distant access point instead of roaming to a closer access point. However, if a client's signal to a distant access point remains strong, the client will not roam to a closer access point. If client devices checked constantly for closer access points, the extra radio traffic would slow throughput on the wireless LAN.

Quality of Service Support

The access point now supports Cisco's QoS, primarily in the area of wireless VoIP telephones from Spectralink and Symbol Technologies Corporation. The access point also provides priority classification, prioritized queueing, and prioritized channel access for other downlink IEEE 802.11 traffic such as streaming audio or video traffic.

With this software release, the access point does not include any QoS enhancements in Cisco IEEE 802.11 client software.

What is QoS?

QoS refers to the ability of a network to provide improved service to selected network traffic over various underlying technologies including Ethernet and wireless LANs. In particular, QoS features provide improved and more predictable network service by providing the following services:

- Improving loss characteristics
- Avoiding and managing network congestion
- Prioritizing service to different kinds of network traffic
- Shaping network traffic
- Setting traffic priorities across the network

Limitations and Restrictions

The QoS implementation on the access point has the following limitations and restrictions:

- Provides only prioritized QoS for downlink traffic on IEEE 802.11 links and does not support a general purpose QoS signalling protocol, uniform admission control, guaranteed bandwidth, and other features that are generally associated with parametized QoS.
- Supports rudimentary admission control mechanisms for Spectralink and Symbol VoIP phones.
- Does not provide a method for prioritizing uplink traffic on IEEE 802.11 links.
- Does not offer 802.1X authentication for Symbol VoIP phones because those phones do not support an 802.1X type such as LEAP or EAP-TLS.
- The DTIM beacon period must be small to support jitter-sensitive streaming multicast audio and video applications.
- Supports IEEE 802.11e EDCF-like channel access prioritization but does not support IEEE 802.11e QoS frame formats.

Related Documents

The following documents provide more detailed information pertaining to QoS design and configuration:

- *Cisco IOS Switching Services Configuration Guide*
- *Cisco Internetworking Design Guide*
- *Cisco Internetworking Technology Handbook*
- *Cisco IOS Quality of Service Solutions Command Reference, Version 12.2*
- *Cisco Internetworking Troubleshooting Guide*

These documents are available on Cisco.com.

VLAN Support

Version 12.01T1 supports VLAN technology by mapping SSIDs to VLANs. With the multiple-SSID capability, the access point can support up to 16 VLAN subnets.

What is a VLAN?

A switched network can be logically segmented into virtual local area networks (VLANs), on a physical or geographical basis, or by functions, project teams, or applications. For example, all workstations and servers used by a particular workgroup team can be connected to the same VLAN regardless of their physical connections to the network or the fact that they might be intermingled with devices for other teams. Reconfiguration of VLANs can be done through software rather than physically unplugging and moving devices or wires.

A VLAN can be thought of as a broadcast domain that exists within a defined set of switches. A VLAN consists of a number of end systems, either hosts or network equipment (such as bridges and routers), connected by a single bridging domain. The bridging domain is supported on various pieces of network equipment, such as LAN switches that operate bridging protocols between them with a separate group for each VLAN.

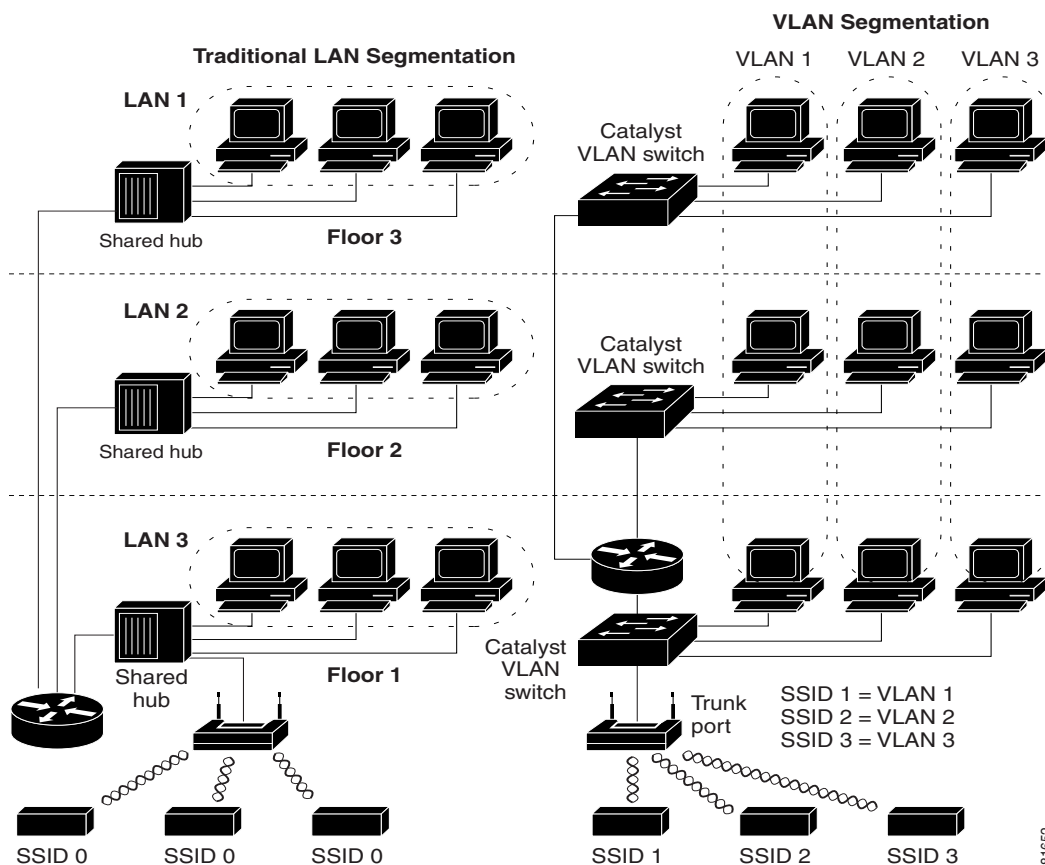
VLANs are created to provide the segmentation services traditionally provided by routers in LAN configurations. Routers in VLAN topologies provide broadcast filtering, security, address summarization, and traffic-flow management. None of the switches within the defined group will bridge any frames, not even broadcast frames, between two VLANs. Several key issues must be considered when designing and building switched LAN networks.

- LAN segmentation
- Security
- Broadcast control
- Performance
- Network management
- Communication between VLANs

VLANs are extended into the wireless realm by adding IEEE 802.1Q tag awareness to the access point. Frames destined for wireless LAN clients on different VLANs are transmitted by the access point wirelessly on different SSIDs with different WEP keys. The only clients that can receive and process packets are those with the correct WEP keys. Conversely, packets coming from a client associated with a certain VLAN are 802.1Q tagged before they are forwarded onto the wired network.

[Figure 1-1](#) illustrates the difference between traditional physical LAN segmentation and logical VLAN segmentation with wireless devices connected.

Figure 1-1 LAN Segmentation and VLAN Segmentation with Wireless Components



Related Documents

The following documents provide more detailed information pertaining to VLAN design and configuration:

- *Cisco IOS Switching Services Configuration Guide*
- *Cisco Internetworking Design Guide*
- *Cisco Internetworking Technology Handbook*
- *Cisco Internetworking Troubleshooting Guide*

Incorporating Wireless Devices into VLANs

A WLAN is generally deployed in an enterprise campus or branch office for increased efficiency and flexibility. WLANs are one of the most effective methods for connecting to an enterprise network. With version 12.01T1, you can configure your wireless devices to operate in a VLAN.

The basic wireless components of a VLAN consist of an access point and a set of clients associated to it using wireless technology. The access point is physically connected through a trunk port to the network switch on which the VLAN is configured. The physical connection to the VLAN switch is through the access point's Ethernet port.

In fundamental terms, the key to configuring an access point to connect to a specific VLAN is by configuring an SSID to map to that VLAN. Because VLANs are identified by a VLAN ID, it follows that if an SSID on an access point is configured to map to a specific VLAN ID, a connection to the VLAN is established. When this connection is made, associated wireless client devices having the same SSID are able to access the VLAN through the access point. The VLAN processes data to and from the clients the same way that it processes data to and from wired connections. The fact that the client is wireless has no impact on the VLAN.

The VLAN feature now enables users to deploy wireless devices with greater efficiency and flexibility. For example, one access point can now handle the specific requirements of multiple users having widely varied network access and permissions. Without VLAN capability, multiple access points, one for each VLAN, would have to be employed to serve classes of users based on the access and permissions they were assigned.

A VLAN Example

The following simplified example shows how wireless devices can be used effectively in a VLAN environment on a college campus. In this example, three levels of access are available through VLANs configured on the physical network:

- Student access—lowest level of access; ability to access school’s intranet, obtain class schedules and grades, make appointments, and perform other student-related activities
- Faculty access—medium level of access; ability to access internal files, read to and write from student databases, access the intranet and Internet, and access internal information such as human resources and payroll information
- Management access—highest level of access; ability to access all internal drives and files, and perform management activities

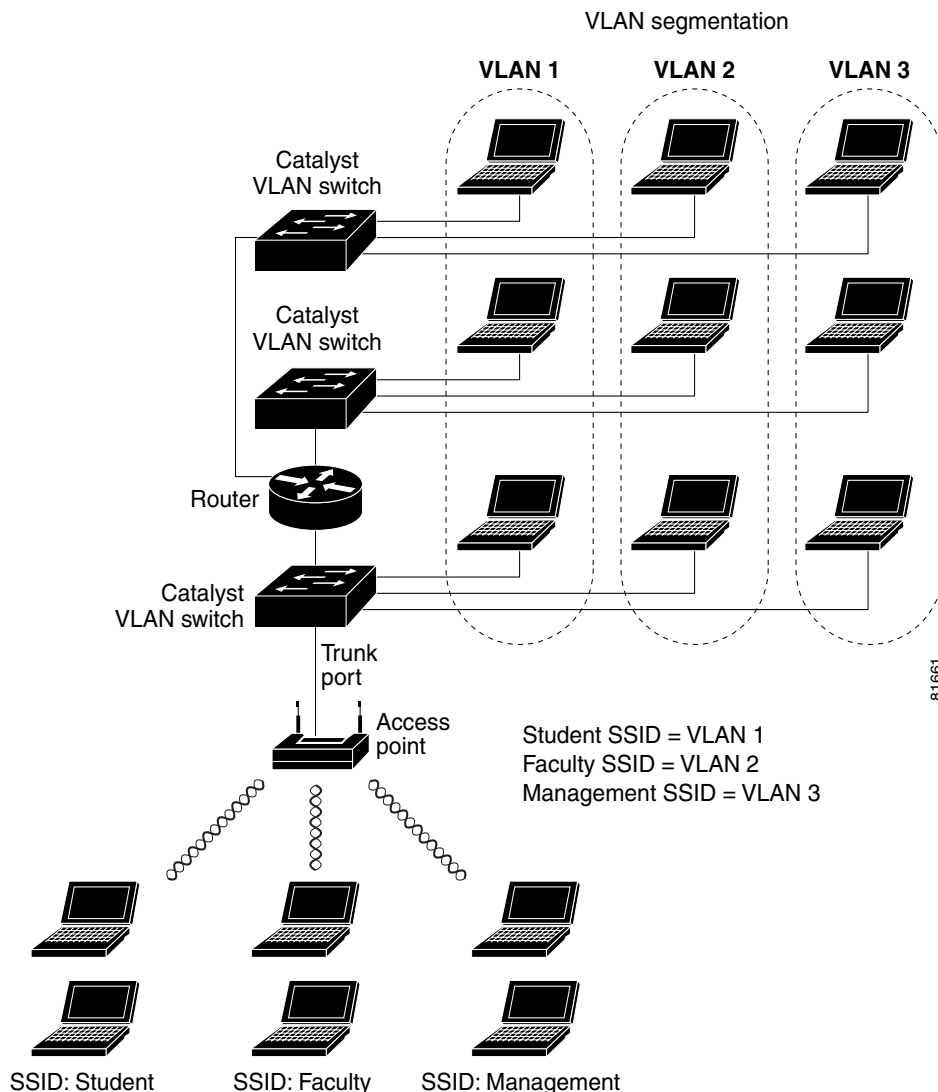
In this scenario, a minimum of three VLAN connections would be required: one for each level of access discussed above. The access point can handle up to 16 SSIDs; therefore, the following basic design could be employed as shown in [Table 1-1](#).

Table 1-1 Access Level SSID and VLAN Assignment

Level of Access	SSID	VLAN ID
Student	Student	01
Faculty	Faculty	02
Management	Management	03

Using this design, setting up the clients is based on the level of access each user requires. A typical network diagram using this design would look like the one shown in [Figure 1-2](#).

Figure 1-2 VLAN Example



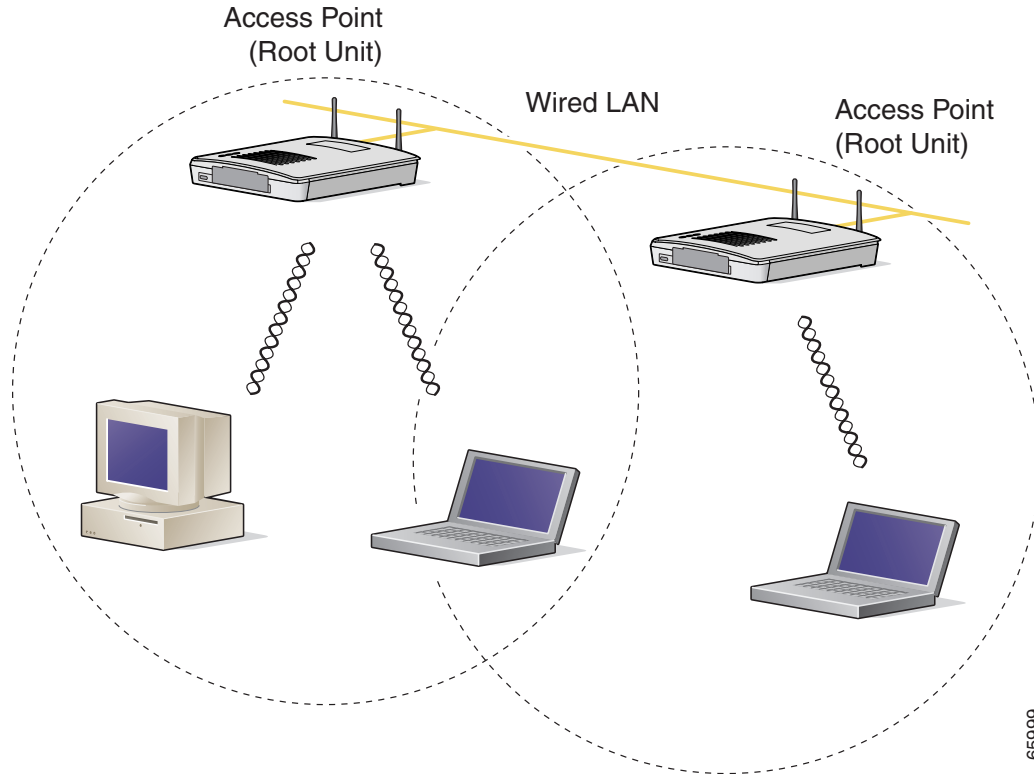
Network Configuration Examples

This section describes the access point’s role in three common wireless network configurations. The access point’s default configuration is as a root unit connected to a wired LAN or as the central unit in an all-wireless network. The repeater role requires a specific configuration.

Root Unit on a Wired LAN

An access point connected directly to a wired LAN provides a connection point for wireless users. If more than one access point is connected to the LAN, users can roam from one area of a facility to another without losing their connection to the network. As users move out of range of one access point, they automatically connect to the network (associate) through another access point. The roaming process is seamless and transparent to the user. [Figure 1-3](#) shows access points acting as root units on a wired LAN.

Figure 1-3 Access Points as Root Units on a Wired LAN



665999

Repeater Unit that Extends Wireless Range

An access point can be configured as a stand-alone repeater to extend the range of your infrastructure or to overcome an obstacle that blocks radio communication. The repeater forwards traffic between wireless users and the wired LAN by sending packets to either another repeater or to an access point connected to the wired LAN. The data is sent through the route that provides the best performance for the client. You can set up either of the radios in your access point as a repeater, but one radio must be set up as a root unit.

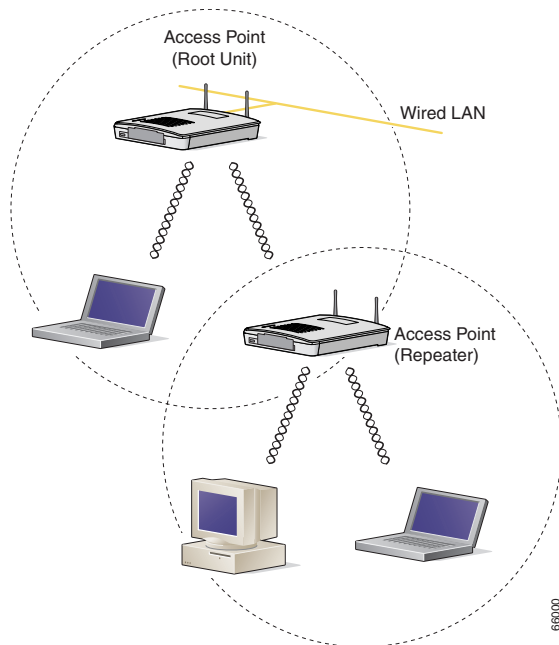
[Figure 1-4](#) shows an access point acting as a repeater. Consult the **Setting Up a Repeater Access Point**, [chp 11](#) for instructions on setting up the access point as a repeater.



Note

Non-Cisco client devices might have difficulty communicating with repeater access points.

Figure 1-4 Access Point as Repeater



Central Unit in an All-Wireless Network

In an all-wireless network, an access point acts as a stand-alone root unit. The access point is not attached to a wired LAN; it functions as a hub linking all stations together. The access point serves as the focal point for communications, increasing the communication range of wireless users. [Figure 1-5](#) shows an access point in an all-wireless network.

Figure 1-5 Access Point as Central Unit in All-Wireless Network

