Cisco Enterprise Distributed Wireless Solutions Reference Network Design

EDCS-466478, Version 2.5

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

Cisco Enterprise Distributed Wireless Solutions Reference Network Design

CONTENTS

CHAPTER 4

CHAPTER 5

CHAPTER 6

CHAPTER 9

CHAPTER 10

Preface

This design guide presents recommendations intended to facilitate Enterprise Wireless Local Area Network (WLAN) solution deployment. The emphasis in this document is with integrating WLAN technology into environments featuring key Enterprise networking elements. Specific chapters address the following topics:

- Chapter 1, "WLAN Solution Overview"—Summarizes the benefits and characteristics of the Cisco secure Enterprise WLAN solution.
- Chapter 2, "WLAN Radio Frequency Design Considerations"—Focuses on radio frequency (RF) considerations in WLAN environments.
- Chapter 3, "WLAN Technology and Product Selection"—Focuses on technology and product assessment and selection in WLAN environments.
- Chapter 4, "WLAN Security Considerations"—Provides details regarding deployment of the Cisco secure Enterprise WLAN solution.
- Chapter 5, "WLAN Deployment Modes"—Focuses on the implementation of virtual local area networks (VLANs) in the context of WLAN environments.
- Chapter 6, "WLAN Quality of Service"—Addresses Quality of Service (QoS) considerations in the context of WLAN implementations.
- Chapter 7, "WLAN Roaming"—Addresses the WLAN design considerations when assessing Layer 2 roaming of wireless LAN clients.
- Chapter 8, "IP Multicast in a Wireless LAN"—Describes the configurations needed to control IP Multicast traffic over a WLAN.
- Chapter 9, "Managing and Deploying WLAN"—Addresses WLAN management and deployment considerations when deploying WLAN across the enterprise.
- Chapter 10, "WLAN Guest Network Access"—Presents the advantages, risks, and proposed configuration for WLAN Guest Network Access.

Where applicable, relevant configuration fragments are included.

Target Audience

This publication provides solution guidelines for large-scale enterprises implementing WLAN networks with Cisco WLAN devices. The intended audiences for this design guide include network architects, network managers, and others concerned with the implementation of secure WLAN solutions, including:

- Cisco sales and support engineers

- Cisco partners
- Cisco customers

Reviewers

Organization	Name and Title	Reviewed	Approved
ITD Systems Design	Lucas Nihart, TSE Mobility, Manager	6/2005	7/2005
	Stephane,	6/2005	7/2005
	Mike Deblauw, Director, ESE	6/2005	7/2005
	Stephane Lamarre, Sr. Manager, TSE	6/2005	7/2005
EAG WNBU Product Marketing	David Stiff, Manager, Technical Marketing	6/2005	7/2005

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

http://www.cisco.com

Translated documentation is available at the following URL:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

http://www.cisco.com/register/

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

CHAPTER 1

WLAN Solution Overview

This chapter summarizes the benefits and characteristics of the Cisco Unified Wireless Network for the Enterprise.

WLAN Introduction

The mobile user requires the same accessibility, security, quality-of-service (QoS), and high availability currently enjoyed by wired users. Whether you are at work, at home, on the road, locally or internationally there is a need to connect. The technological challenges are apparent, but to this end, mobility will play a role in everyone’s life. Companies are deriving business value from mobile and wireless solutions. What was once a vertical market technology is now mainstream, and is an essential tool in getting access to voice, real-time information and critical applications such as e-mail and calendar, enterprise databases, supply chain management, sales force automation, and customer relationship management.

WLAN Solution Benefits

WLANs provide the user with a new way to communicate while accommodating the way business is done now. The benefits achieved by WLANs are:

- *Mobility within building or campus*—Facilitates implementation of applications that require an always-on network and that tend to involve movement within a campus environment.
- *Convenience*— Simplifies networking of large, open people areas.
- *Flexibility*—Allows work to be done at the most appropriate or convenient place rather than where a cable drop terminates. Getting the work done is what is important, not where you are.
- *Easier to set-up temporary spaces*—Promotes quick network setup of meeting rooms, war rooms, or brainstorming rooms tailored to variations in the number of participants.
- *Lower cabling costs*—Reduces the requirement for contingency cable plant installation because the WLAN can be employed to fill the gaps.
- *Easier adds, moves, and changes and lower support and maintenance costs*—Temporary networks become much easier to set up, easing migration issues and costly last-minute fixes.
- *Improved efficiency*—Studies show WLAN users are connected to the network 15 percent longer per day than hard-wired users.
- *Productivity gains*—Promotes easier access to network connectivity, resulting in better utilization of business productivity tools. Productivity studies show a 22 percent increase for WLAN users.

- *Easier to collaborate*—Facilitates access to collaboration tools from any location, such as meeting rooms; files can be shared on the spot and requests for information handled immediately.
- *More efficient use of office space*—Allows greater flexibility for accommodating groups, such as large team meetings.
- *Reduced errors*—Data can be directly entered into systems as it is being collected, rather than when network access is available.
- *Improved efficiency, performance, and security for enterprise partners and guests*—promoted by implementing guest access networks.
- *Improved business resilience*—Increased mobility of the workforce allows rapid redeployment to other locations with WLANs.

Requirements of WLAN Systems

WLAN systems run either as an adjunct to the existing wired enterprise network or as a free-standing network within a campus or branch, individual tele-worker, or tied to applications in the retail, manufacturing or health care industries. WLANs must permit secure, encrypted authorized communication with access to data, communication and business services as if connected to the resources by wire.

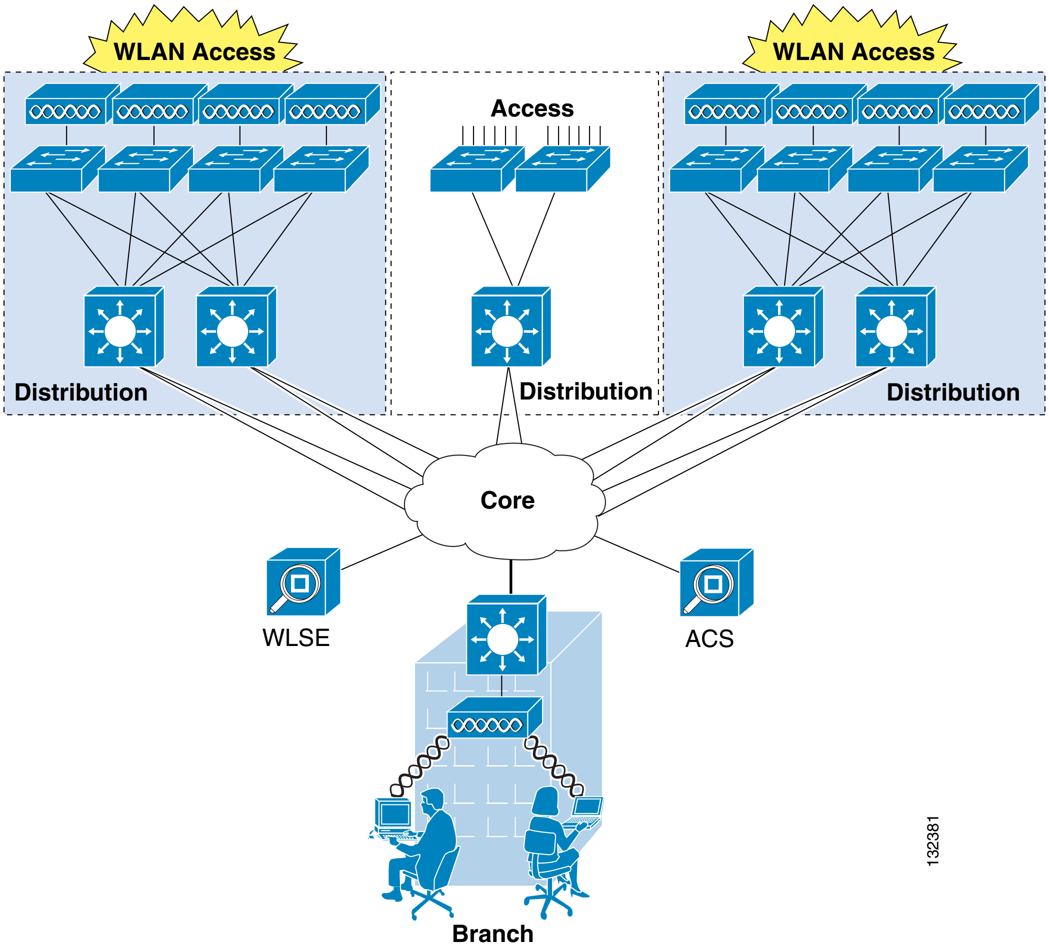
WLANs must be able to:

- *Maintain accessibility to resources while employees are not wired to the network* —This accessibility enables employees to respond more quickly to business needs regardless of whether they are meeting in a conference room with a customer, at lunch with coworkers in the company cafeteria, or collaborating with a teammate in the next building.
- *Secure the enterprise from unauthorized, unsecured, or "rogue," WLAN access points*—IT managers must be able to easily and automatically detect and locate rogue access points and the switch ports to which they are connected, active participation of both access points, and client devices that are providing continuous scanning and monitoring of the RF environment.
- *Extend the full benefits of integrated network services to nomadic users*—IP telephony and IP video-conferencing are supported over the WLAN using QoS, which by giving preferential treatment to real-time traffic, helps ensure that the video and audio information arrives on time. Firewall and Intruder Detection which are part of the enterprise framework are extended to the wireless user.
- *Segment authorized users and block unauthorized users*—Services of the wireless network can be safely extended to guests and vendors. The WLAN must be able to configure support for a separate public network—a guest network.
- *Provide easy, secure network access to visiting employees from other sites*—There is no need to search for an empty cubicle or an available Ethernet port. Users should securely access the network from any WLAN location. Employees are authenticated through IEEE 802.1x and Extensible Authentication Protocol (EAP), and all information sent and received on the WLAN is encrypted.
- *Easily manage central or remote access points*—Network managers must be able to easily deploy, operate, and manage hundreds to thousands of access points within the WLAN campus deployments and branch offices or retail, manufacturing, and health care locations. The desired result is one framework that provides medium-sized to large organizations the same level of security, scalability, reliability, ease of deployment, and management that they have come to expect from their wired LANs.

Wireless LANs in the enterprise have emerged as one of the most effective means for connecting to a network. The design recommendations presented in this document propose a secure WLAN network, not the replacement of wired infrastructure with wireless infrastructure. Figure 1-1 shows WLAN in the Enterprise.

The Cisco Unified Wireless Network cost-effectively addresses the wireless LAN (WLAN) security, deployment, management, and control issues facing enterprises. This framework integrates and extends wired and wireless networks to deliver scalable, manageable and secure WLANs with the lowest total cost of ownership. The Cisco Unified Wireless Network provides the same level of security, scalability, reliability, ease of deployment, and management for wireless LANs that organizations expect from their wired LANs.

Figure 1-1 WLAN in the Enterprise



The Cisco Unified Wireless Network includes two secure, enterprise-class WLAN solutions. Customers can choose to deploy either Autonomous Cisco Aironet Access Points running Cisco IOS® Software or Lightweight Access Points using a controller. The primary difference between these two types of access points lies in their implementation of access point control and management.

The devices are available in two versions; those configured for lightweight operation in conjunction with Cisco Wireless LAN Controllers and the Wireless Control System (WCS) as well as those configured for autonomous operation used independently or in conjunction with the CiscoWorks Wireless LAN Solution Engine (WLSE). Autonomous access points along with the CiscoWorks WLSE deliver a core set of features. Autonomous access points may be field upgraded to lightweight operation and an advanced feature set. Customers can choose the access point that best meets their WLAN deployment needs today knowing that Cisco provides the investment protection and a migration path to evolve their WLAN going forward. For more information about the Cisco Unified Wireless Network, refer to the following URL:

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

Cisco Unified Wireless Network

The core feature set includes autonomous Cisco Aironet access points, the CiscoWorks Wireless LAN Solution Engine (WLSE) or CiscoWorks WLSE Express management platforms and the Cisco Catalyst® 6500 Series Wireless LAN Services Module (WLSM). Cisco Aironet access points that use Cisco IOS Software, are autonomous and do not need a wireless LAN controller. The core feature set is deployable in the following configurations today:

- Access point only deployment for secure WLAN access using Cisco Aironet autonomous access points (1240AG, 1130AG, 1200, 1230AG, 1100 and,1300).
- Autonomous Access points + management capabilities using Cisco Aironet access points and the CiscoWorks WLSE or CiscoWorks WLSE Express.
- Autonomous Access point + management + control through wireless integrated switches using Cisco Aironet access points, the CiscoWorks WLSE or CiscoWorks WLSE Express, and the Cisco Catalyst 6500 Series WLSM with the Cisco Catalyst 6500 Series Supervisor Engine 720.

Adding optional Cisco Aironet or Cisco Compatible Extensions client devices provides additional benefits, including advanced enterprise-class security, extended RF management, and enhanced interoperability.

Enterprise WLAN Design Characteristics

The Enterprise WLAN design solutions presented in this document provide the following assumptions and characteristics:

- WLAN Virtual LANs (VLANs) or Mobility groups allow multiple models to coexist on the same WLAN, allowing a combination of security models based on client requirements or user policies.
- The recommended security model is Wi-Fi Protected Access (WPA) as it creates the optimum network architecture and addresses all known WLAN encryption threats. WPA uses Extensible Authentication Protocol (EAP) for transport of authentication information between client and authentication server.
- Examples of EAP types suitable for use in WLANs are:
  - EAP-Cisco (formerly Lightweight EAP or LEAP)
  - EAP- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST)
  - EAP-Transport Layer Security (EAP-TLS)
  - Protected EAP (PEAP)
  - PEAP- GTC (Generic Token Card)

  If further 802.1x/EAP types are developed to meet business needs, the existing architectures will accommodate them. The 802.1x/EAP type is transparent to the AP, and only has implications for the client software and the Remote Authentication Dial-In User Service (RADIUS) server.

- IPSec VPNs are recommended as an alternative 802.1x/EAP if the customer policy security requires it.
- The design recommendations presented in this publication show a the WPA security model. This model can be combined with other security models within the enterprise implementation using WLAN VLANs or Mobility groups.
- WLANs should be assigned to a dedicated subnet, not one shared with wired LAN users.
- If VLANS for wireless are configured, restrict access to the wireless VLAN. Having a separate VLAN on the switch allows the network administrator to decide who gets access. A separate VLAN (usually referred to as the native VLAN) should be configured for the management of WLAN APs. This VLAN should not have a WLAN appearance (no associated SSID or access from the WLAN).
- Fifteen to 25 users are assumed per AP. This number varies from customer to customer depending on usage profiles and user density.
- For AP-based WDS, fast secure roaming is limited to the same Layer 2 network. Adding Switch based WDS adds Fast secure roaming at Layer 3.
- WLAN QoS tools are used as required.
- IP Multicast for the WLAN is bound to ensure that multicast does not consume excessive bandwidth, and IP multicast applications are tested for their suitability for a WLAN network.

Comparing Wired and WLANs

Just as a network designer must understand how switches and routers handle traffic to design a wired network, the same designer also needs to understand how access points (APs), wireless bridges and workgroup bridges handle traffic in order to design a WLAN.

WLAN devices exhibit network behavior similar to an Ethernet switch combined with a shared Ethernet hub. Ethernet frames passing through an AP, wireless bridge, or workgroup bridge to or from the wireless network undergo changes at Data Link Control (DLC) much as frames can when passing through a Translation Bridge. 802.11, 802.2 DLC, and Subnetwork Access Protocol (SNAP) header information replace Ethernet header information. Where 802.3 framing is used instead of Ethernet, the 802.11 header replaces the 802.3 header. Refer to IEEE 802.1h standards and RFC1042 for further details. Although IP is shown as the Layer 3 protocol, this could just as easily be any protocol able to operate over Ethernet such as IPX, Appletalk, or NetBEUI. However, IP is still required to remotely manage APs, wireless bridges, and workgroup bridges.

Table 1-1 Wired and WLAN DLC Relationships

	Wireless	**Wired (802.3)**	**Wired Ethernet**
Layer-3 Network	**IP**	**IP**	**IP**
Layer 2 DLC	SNAP (0800 = IP)	SNAP (0800 = IP)	Ethernet (0800 = IP)
	IEEE 802.LLC	IEEE 802.LLC	
	IEEE 802.11 MAC	IEEE 802.11 MAC	

Within any one wireless channel, the wireless interface is a shared medium. It operates in a fashion similar to an Ethernet hub. Within any Basic Service Set (BSS), only one station can transmit at any one time. All wireless stations are half-duplex. The same frequency channel is used for transmit and receive. The actual access mechanism used is Carrier Sense Multiple Access with Collision Avoidance

(CSMA/CA). Ethernet uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD). Each station in a CSMA network listens before talking over the air. As collision detection (CD) is difficult in a radio-based environment, a collisions avoidance (CA) mechanism is used instead.

At a detailed level, there are some significant differences between 802.11 and Ethernet, but from a network designer's standpoint, the important idea to remember is the notion of a shared medium. This, differences due to the overheads in the 802.11 protocol, and that some traffic flows may not be occurring at the highest data rate, impact the throughput. Taking overhead and protocol operation into account, the actual aggregate Maximum throughput of a WLAN is approximately half the data rate. Table 1-2 shows the data rates.

Table 1-2 Data Rates

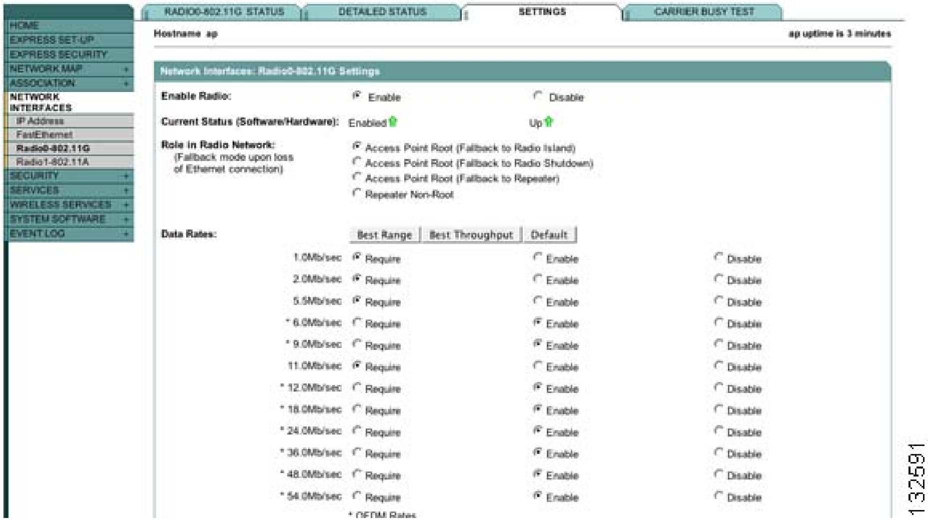
	Data Rate (Mbps)	**Approximate Throughput (Mbps)**
802.11b	11	6
802.11g (802.11b clients in cell)	54	7
802.11g (no 802.11b clients in cell)	54	22
802.11a	54	25

Unicast Traffic

The WLAN device always tries to send data at the highest rate possible. There are many data rates which can be selected. For instance, four rates are possible for 802.11b radio: 1, 2, 5.5, and 11 Mbps. 802.11g adds additional data rate support at 6, 9, 12, 18, 24, 36, 48 and 54 Mbps. 802.11a radio support 6, 9, 12, 18, 24, 36, 48 and 54 Mbps. The data rate used by a WLAN device can normally be configured but standard practice is to configure the required data rates upon the AP, and have the clients automatically adjust their data. Higher rates can be selected as needed to support specific application throughput requirements. Lower data rates can be selected to provide legacy support or to increase the coverage area. Figure 1-2 shows an example of a data rate selection for a 802.11g radio on a Cisco Aironet 1100 Series Access Point.

Note 802.11g and 802.11b devices are compatible. 802.11g and 802.11a devices are not compatible.

Figure 1-2 AP Radio Network Interface:802.11g: Settings Page



Hostname ap

ap uptime is 3 minutes

Network Interfaces: Radio0-802.11G Settings

Enable Radio: ● Enable ○ Disable

Current Status (Software/Hardware): Enabled Up

Role in Radio Network: (Fallback mode upon loss of Ethernet connection)

● Access Point Root (Fallback to Radio Island)
○ Access Point Root (Fallback to Radio Shutdown)
○ Access Point Root (Fallback to Repeater)
○ Repeater Non-Root

Data Rates:

1.0Mb/sec	● Require	○ Enable	○ Disable
2.0Mb/sec	● Require	○ Enable	○ Disable
5.5Mb/sec	● Require	○ Enable	○ Disable
* 6.0Mb/sec	○ Require	● Enable	○ Disable
* 9.0Mb/sec	○ Require	● Enable	○ Disable
11.0Mb/sec	● Require	○ Enable	○ Disable
* 12.0Mb/sec	○ Require	● Enable	○ Disable
* 18.0Mb/sec	○ Require	● Enable	○ Disable
* 24.0Mb/sec	○ Require	● Enable	○ Disable
* 36.0Mb/sec	○ Require	● Enable	○ Disable
* 48.0Mb/sec	○ Require	● Enable	○ Disable
* 54.0Mb/sec	○ Require	● Enable	○ Disable

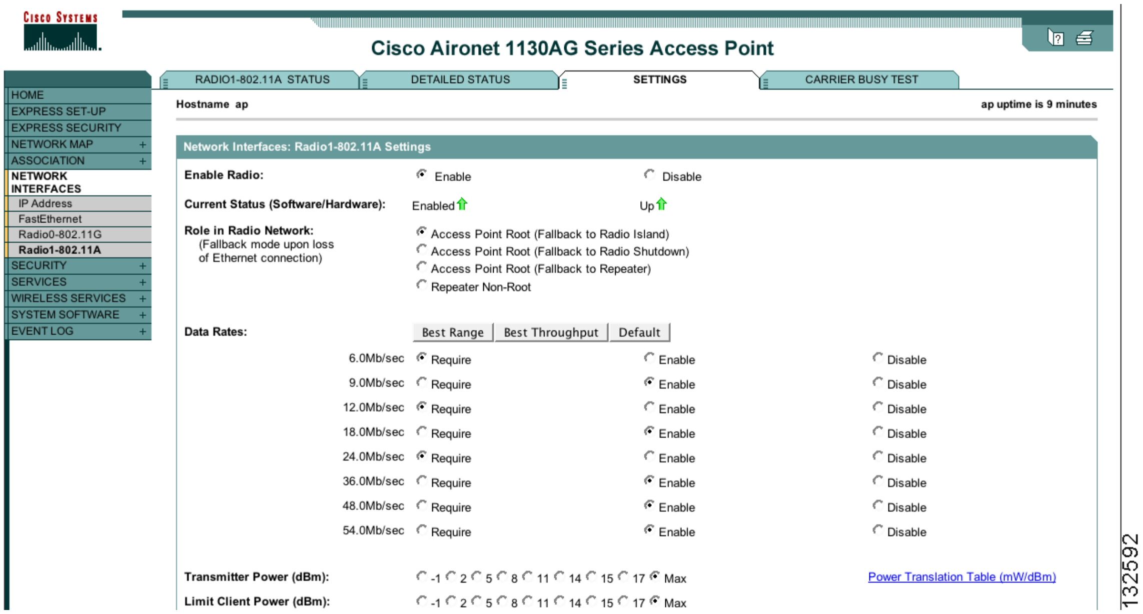
* OFDM Rates

Multicast and Broadcast Traffic

Multicast and broadcast traffic are treated the same within a WLAN network. Multicast traffic is sent at the data rate of the AP client with the lowest data rate. For example, consider an AP configured with data rates as Require, as shown in Figure 1-2, that has clients associated at 11 Mbps and at 5.5 Mbps for 802.11b radio. In this scenario, multicast traffic is sent at 5.5 Mbps to ensure the frames were received by all associated clients. Figure 1-3 shows an 802.11a radio example, which is configured so that multicast packets be transmitted at a specific lower rate by setting a Require value, in this case 24 Mbps maximum, and having unicast transmitted at the higher rate, such as 54Mbps maximum.

Note In Cisco APs, setting a Require rate above 11Mbps prevents 802.11b clients from associating.

Figure 1-3 Configuring Multicast/Broadcast Packets



Hostname ap ap uptime is 9 minutes

Network Interfaces: Radio1-802.11A Settings

Enable Radio:	● Enable	○ Disable	
Current Status (Software/Hardware):	Enabled ⇧	Up ⇧	
Role in Radio Network: (Fallback mode upon loss of Ethernet connection)	● Access Point Root (Fallback to Radio Island) ○ Access Point Root (Fallback to Radio Shutdown) ○ Access Point Root (Fallback to Repeater) ○ Repeater Non-Root		
Data Rates:	Best Range | Best Throughput | Default		
6.0Mb/sec	● Require	○ Enable	○ Disable
9.0Mb/sec	○ Require	● Enable	○ Disable
12.0Mb/sec	● Require	○ Enable	○ Disable
18.0Mb/sec	○ Require	● Enable	○ Disable
24.0Mb/sec	● Require	○ Enable	○ Disable
36.0Mb/sec	○ Require	● Enable	○ Disable
48.0Mb/sec	○ Require	● Enable	○ Disable
54.0Mb/sec	○ Require	● Enable	○ Disable
Transmitter Power (dBm):	○ -1 ○ 2 ○ 5 ○ 8 ○ 11 ○ 14 ○ 15 ○ 17 ● Max		Power Translation Table (mW/dBm)
Limit Client Power (dBm):	○ -1 ○ 2 ○ 5 ○ 8 ○ 11 ○ 14 ○ 15 ○ 17 ● Max		

Infrastructure Mode

The 802.11 standard defines two modes of connection, infrastructure mode and ad-hoc mode.

In infrastructure mode, clients communicate through an AP. The AP is the point at which wireless clients can access the network. Figure 1-4 illustrates a typical WLAN arrangement. The AP provides connectivity to other clients associated with that AP or to the wired LAN.

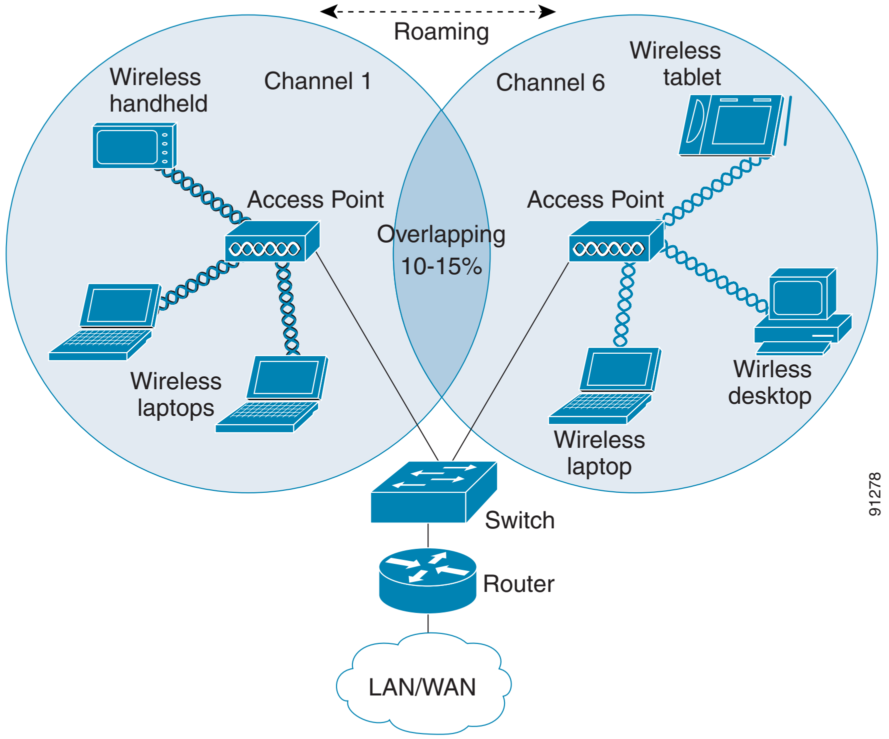
The basic service area (BSA) is the area of RF coverage provided by an AP, also referred to as a *microcell*. To extend the BSA, or to simply add wireless devices and extend the range of an existing wired system, an AP can be added.

The AP attaches to the Ethernet backbone and allows communication between all devices on the Ethernet backbone with all the wireless devices in the cell area. The AP is the master for the cell, and controls traffic flow to and from the network. The remote devices do not communicate directly with each other; they communicate to the AP.

If a single cell does not provide enough coverage, any number of cells can be added to extend the range. This is known as an extended service area (ESA). It is recommended that the ESA cells include 10 to 15 percent overlap to allow remote users to roam without losing RF connections.

Note The recommended amount of overlap between cells is different if VoWLAN is being deployed. Refer to *Cisco Wireless IP Phone 7920 Design and Deployment Guide*.

Figure 1-4 Typical WLAN



Ad-hoc Mode

Ad-hoc mode is used to establish a peer-to-peer network between two or more clients. No AP is used. Security becomes a concern. This mode is selected through the *System Type* section of the *System Parameters* page on the Aironet Client Utility (ACU). This mode is not included in this document, and is generally not recommended for enterprise use due to the security implications.

Links and References

The following documents provide supplemental information about the design and implementation material presented in this SRND. These references fall into several categories:

- General References
- Security References
- IP Multicast References

General References

Cisco Network Solutions and Provisioned Services page:

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

Note Access to specific information varies based on user entitlement at the Cisco Systems web site.

Security References

The Unofficial 802.11 Security Web Page:

http://www.drizzle.com/~aboba/IEEE/

Assessing Wireless Security with AiroPeek and AiroPeek NX:

http://www.wildpackets.com/elements/whitepapers/AiroPeek_Security.pdf

Netstumbler security links:

http://www.netstumbler.com/links.php?op=MostPopular

Organization Unique Identifier —OUI list:

http://standards.ieee.org/regauth/oui/oui.txt

SANS (System Administration, Networking and Security) Institute Wireless page:

http://www.sans.org/rr/whitepapers/wireless/

List of wireless security tools:

http://www.networkintrusion.co.uk/wireless.htm

Cisco Wireless LAN Security Web site

http://www.cisco.com/go/aironet/security

Cisco Aironet Wireless LAN Security Overview

http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm

IP Multicast References

CCO IP Multicast Overview:

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

CHAPTER 2

WLAN Radio Frequency Design Considerations

This chapter focuses on radio frequency (RF) considerations in WLAN environments.

RF Basics

This section provides a summary of regulations and considerations specific to RF implementation.

Regulations

Devices that operate in unlicensed bands do not require any formal licensing process, and equipment produced to operate in these bands must comply with regulatory requirements for these bands. Governing bodies in different parts of the world regulate these bands. WLAN devices must comply to the specifications of the relevant governing regulatory domain. The regulatory requirements do not affect the inter-operability of IEEE 802.11b/g and 802.11a compliant products. It is the responsibility of the vendor to get the product certified from the corresponding regulatory body. Table 2-1 summarizes the current regulatory domains for Wi-Fi products, but do impact the availability of products in different regions, and can impact the choice of technology and how it is deployed. The main regulatory domains are the FCC, ETSI, and TELEC domains.

Table 2-1 Regulatory Domains

Regulatory Domain	Geographic Area
Americas or United States Federal Communication Commission (FCC)	North, South and Central America, Australia and New Zealand, various parts of Asia and Oceania
Europe or European Telecommunications Standards Institute (ETSI)	Europe (both EU and non-EU countries), Middle East, Africa, various parts of Asia and Oceania
Japan (TELEC)	Japan
China	People’s Republic of China (Mainland China)
Israel	Israel
Singapore[1]	Singapore
Taiwan[2]	Republic of China (Taiwan)

1. The regulations of Singapore and Taiwan for wireless LANs are particular to these countries only for operation in the 5 GHz band. Singapore and Taiwan are therefore only regulatory domains for 5 GHz operation, for operation in 2.4 GHz, they fall into the ETSI and FCC domains, respectively.
2. See above.

Note Check the Cisco web site for compliance information and also with your local regulatory authority on what is permitted within your country. The information provided in Table 2-2, Table 2-3, and Table 2-4 on the following pages should be used as a general guideline. For up-to-date information on regional requirements, check http://www.cisco.com/warp/public/779/smbiz/wireless/approvals.html#4.

Table 2-2 Operating Frequency Range for 802.11b and 802.11g

Channel Identifier	Center Frequency	FCC (America)	ESTI (EMEA)	TELEC (Japan)	MOC (Israel)
1	2412	X	X	X	
2	2417	X	X	X	
3	2422	X	X	X	
4	2427	X	X	X	
5	2432	X	X	X	
6	2437	X	X	X	
7	2442	X	X	X	X
8	2447	X	X	X	X
9	2452	X	X	X	X
10	2457	X	X	X	X
11	2462	X	X	X	X
12	2467		X	X	X
13	2472		X	X	
14	2484			X	

Table 2-3 Operating Frequency Range for 802.11a

Channel Identifier	36	40	44	48	52	56	60	64	149	153	157	161
Center Frequency	5180	5200	5220	5240	5260	5280	5300	5320	5745	5765	5785	5805
Band	**UNII-1**				**UNII-2**				**UNII-3**			

Table 2-4 Additional Frequency Bands and Channel Numbers for Other Regulatory Domains

Regulatory Domain	Frequency Band	Channel Number	Center Frequency
Japan	U-NII lower band	34	5.170
		38	5.190
		42	5.210
		|46	5.230
Singapore	U-NII lower band	36	5.180
		40	5.200
		44	5.220
		48	5.240
Taiwan		52	5260
		56	5280
		60	5300
		64	5320
EMEA[1] Australia New Zealand	Same as USA	Same as USA	Same as USA
EMEA	U-NII lower band	36	5.180
		40	5.200
		44	5.220

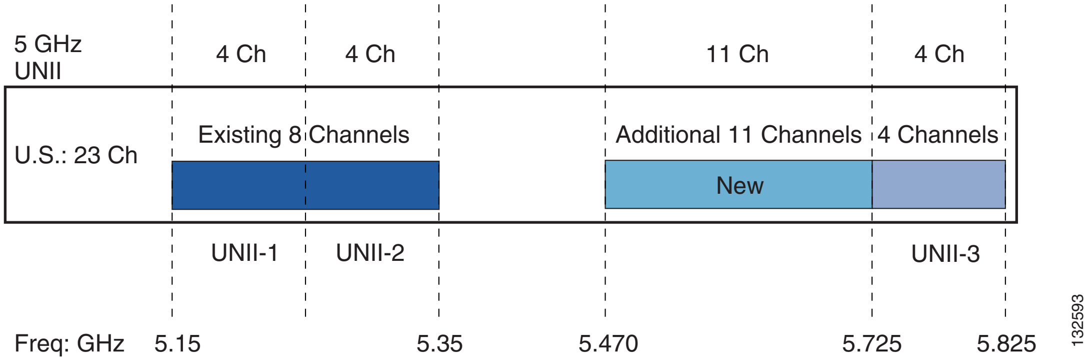
[1] Some EMEA countries, and limited to 20 mW.

Each of the bands presented in Table 2-3 is intended for different uses. The UNII-3 band is intended for long range point-to-point and point-to-multipoint wireless bridging and may only be used outdoors. Please refer to the following URL to find the appropriate WLAN product for your regulatory domain:

http://www.cisco.com/warp/public/779/smbiz/wireless/approvals.html

In February 2004, the FCC released a revision to the regulations covering 5 GHz 802.11a channel usage. This revision added 11 channels, bringing the available channels capacity to 23 (Figure 2-1). In order to use the 11 new channels, however, radios must comply with two features that are part of the 802.11h specification: Transmitter Power Control (TPS) and Dynamic Frequency Selection (DFS).

Figure 2-1 5 GHz 802.11a Channel Capacity



RF Design Planning

A number of factors can affect the WLAN coverage as follows:

- Selected Data Rate
- Power Level
- Antenna type: dipole, omni-directional, or wall mount
- Environment

For a given data rate and location the WLAN designer can alter the power level or elect to use a different antenna to change the coverage area or shape.

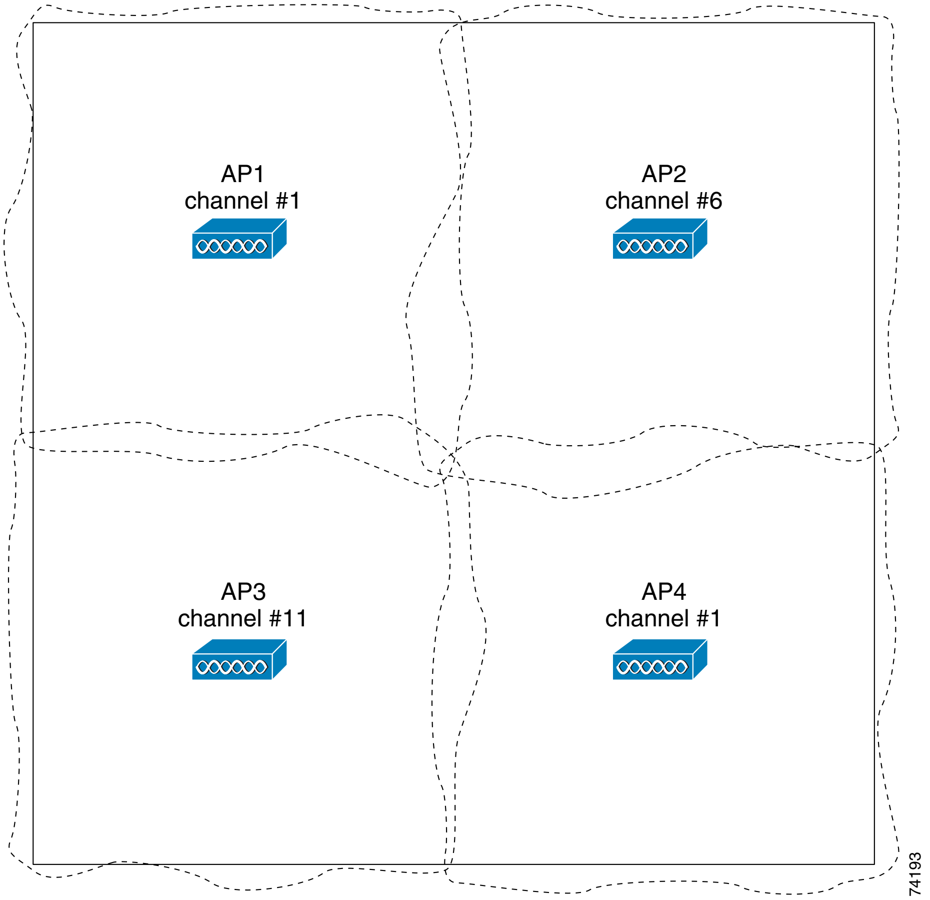
Channel Selection

Channel selection depends on the frequencies that are permitted for a particular region. For example the North American and ETSI 2.4 GHz channel sets permit allocation of three non-overlapping channels1, 6, and 11 while the 5 GHz channel set permits 12 channels.

The channels should be allocated to the coverage cells as follows:

- Overlapping cells should use non-overlapping channels
- Where channels must be used in multiple cells, those cells should have minimal overlap with each other. See Figure 2-2.

Figure 2-2 Channels Allocated to APs



A site survey should be conducted using the same frequency plan as intended for the actual deployment. This facilitates a more accurate estimate of how a particular channel at a particular location will react to the interference and the multi-path.

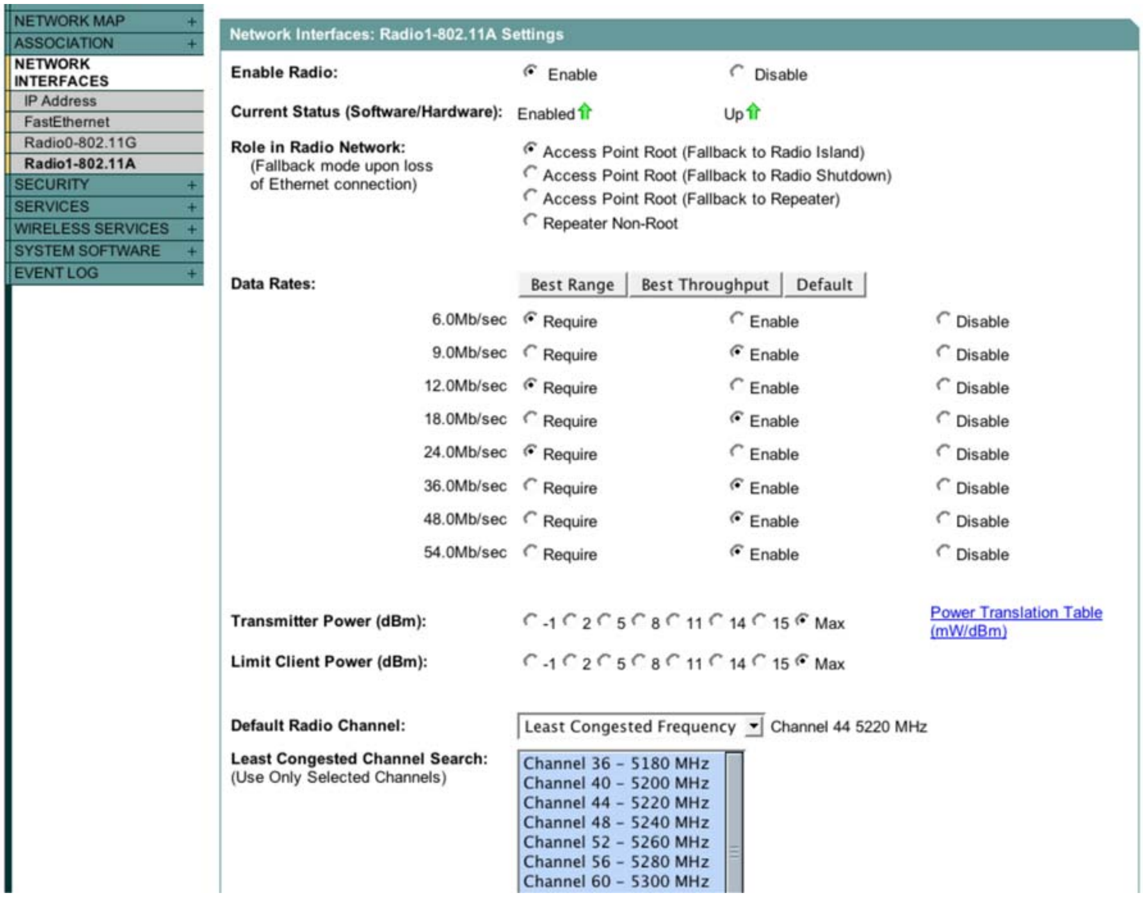
Channel selection also helps in planning for co-channel and the adjacent channel interferences and provides information about where you can reuse a frequency.

In multi-story buildings, such as office towers, hospitals and university classroom buildings, check the cell overlap between floors according to these guidelines. In some cases re-surveying and relocating APs might be required. Multi-story structures introduce a third dimension to coverage planning. The 2.4 GHz waveform of 802.11b and 802.11g can pass through floors, ceilings, and walls. The 5 GHz waveform of 802.11a can also pass through floors, ceilings, and walls, but will do so at a lesser degree due to its higher frequency. With 2.4 GHz Wi-Fi LANs in particular, you must not only avoid overlapping cells on the same floor, but also on adjacent floors. With only three channels, overlapping can be avoided through careful three dimensional planning.

An AP can be configured to automatically search for the best channel when it is powered on. The automatic search is configured from the Network Interfaces window, choosing **802.11x Radio Settings > Least Congested Frequency**. This feature needs to be used with care as the assessment is made when the AP is powered on. For a standalone AP this may be sufficient, but in a multi-AP deployment the assessment that takes place during boot-up is insufficient as the boot-up conditions can be expected to be significantly different from normal operating conditions.

Retest the site using the selected channels and check for any interference. The WLSE can be used to provide assisted site survey through its radio management features.

Figure 2-3 AP Automatic Channel Search



Network Interfaces: Radio1-802.11A Settings

Enable Radio: ● Enable ○ Disable

Current Status (Software/Hardware): Enabled ⇧ Up ⇧

Role in Radio Network:
(Fallback mode upon loss
of Ethernet connection)

● Access Point Root (Fallback to Radio Island)
○ Access Point Root (Fallback to Radio Shutdown)
○ Access Point Root (Fallback to Repeater)
○ Repeater Non-Root

Data Rates:

6.0Mb/sec	● Require	○ Enable	○ Disable
9.0Mb/sec	○ Require	● Enable	○ Disable
12.0Mb/sec	● Require	○ Enable	○ Disable
18.0Mb/sec	○ Require	● Enable	○ Disable
24.0Mb/sec	● Require	○ Enable	○ Disable
36.0Mb/sec	○ Require	● Enable	○ Disable
48.0Mb/sec	○ Require	● Enable	○ Disable
54.0Mb/sec	○ Require	● Enable	○ Disable

Transmitter Power (dBm): ○ -1 ○ 2 ○ 5 ○ 8 ○ 11 ○ 14 ○ 15 ● Max

Limit Client Power (dBm): ○ -1 ○ 2 ○ 5 ○ 8 ○ 11 ○ 14 ○ 15 ● Max

Default Radio Channel: Least Congested Frequency ▾ Channel 44 5220 MHz

Least Congested Channel Search:
(Use Only Selected Channels)

Channel 36 - 5180 MHz
Channel 40 - 5200 MHz
Channel 44 - 5220 MHz
Channel 48 - 5240 MHz
Channel 52 - 5260 MHz
Channel 56 - 5280 MHz
Channel 60 - 5300 MHz

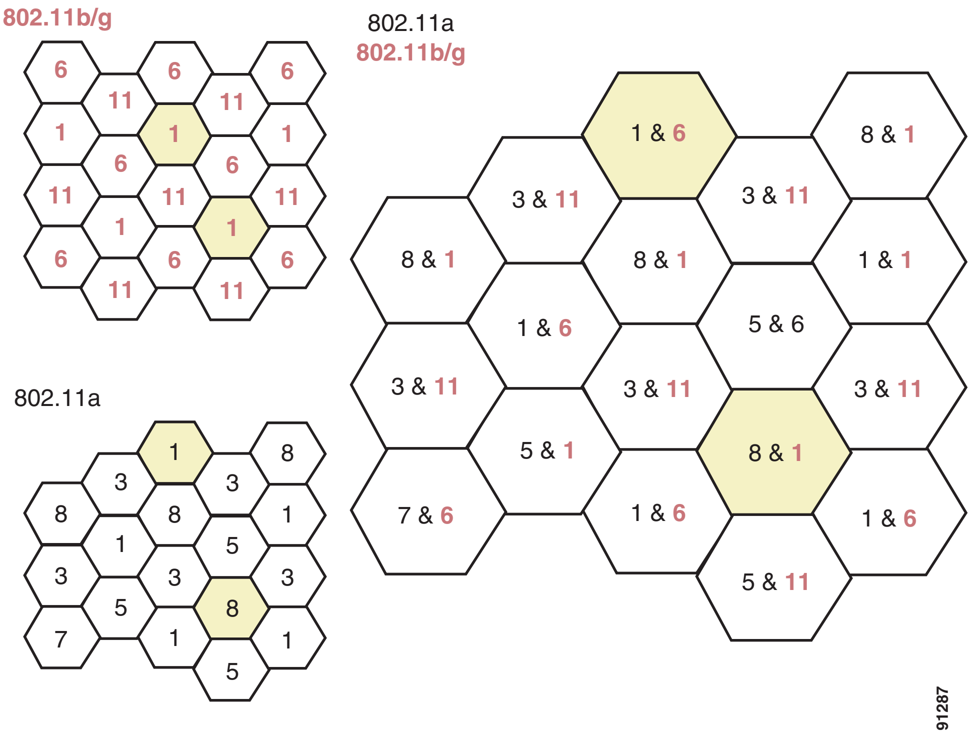
Use the data rate settings to choose the data rates the wireless device uses for data transmission. The rates are expressed in megabits per second. The wireless device always attempts to transmit at the highest possible data rate, also called Require, on the browser-based interface. If RF rates are insufficient to support the highest rate, the wireless device steps down to the highest rate that supports reliable data transmission. You can set each data rate to one of three modes:

- *Require (also known as Basic when using the CLI interface)*—Allows transmission at this rate for all packets, both unicast and multicast. At least one of the wireless device's data rates must be set to Basic, and all associated clients must be able to support this rate. If more than one data rate is set at basic, multicast frames will be sent at the highest rate currently supported by the associated clients.
- *Enabled*—The wireless device transmits only unicast packets at this rate; multicast packets are sent at one of the data rates set to Basic.
- *Disabled*—The wireless device does not transmit data at this rate.

Setting any OFDM rates as “Require (Basic)” disables 802.11b connectivity.

Note It is possible to implement a dual-band deployment scheme as illustrated Table 2-3. Refer to the “Data Rate Considerations” section on page 3-5 for related information about dual-band channel deployment considerations.

Figure 2-4 Dual Band Deployment Diagram



IEEE 802.11 Standards

The IEEE 802.11 standard is the Working Group within the Institute for Electrical and Electronics Engineers (IEEE) responsible for Wireless LAN Standards. Ratified in September 1999, the 802.11b standard operates in the 2.4 Ghz spectrum and supports data rates of 1, 2, 5.5 and 11 Mbps. 802.11b enjoys broad user acceptance and vendor support. 802.11b technology has been deployed by thousands of enterprise organizations, that typically find its speed and performance acceptable for their current applications. 802.11g, ratified in June 2003, operates in the same spectrum as 802.11b and is backward compatible with 802.11b. 802.11g support additional data rates of 6, 9, 12, 18, 24, 36, 48 and 54 Mbps. A third standard, 802.11a operates in the 5 Ghz spectrum and provides data rates of 6, 9, 12, 18, 24, 36, 48 and 54 Mbps. Many vendors manufacture compatible devices, and compatibility is assured through the Wi-Fi certification program. (www.wi-fi.org).

Within the 802.11 Working Group are a number of Task Groups responsible for elements of the 802.11 WLAN Standard. Table 2-5 summarizes some of the Task Group initiatives.

Table 2-5 IEEE 802.11 Task Group Activities

Task Group	Project
MAC	Develop one common MAC for WLANs in conjunction with a physical layer entity (PHY) Task Group
PHY	Develop three WLAN PHYs – Infrared, 2.4 GHz FHSS, 2.4 GHz DSSS
a	Develop PHY for 5 GHz UNII band

Table 2-5 IEEE 802.11 Task Group Activities (continued)

Task Group	Project
b	Develop higher rate PHY in 2.4 GHz band
c	Cover bridge operation with 802.11 MACs (spanning tree)
d	Define physical layer requirements for 802.11 operation in other regulatory domains (countries)
e	Enhance 802.11 MAC for QoS
f	Develop recommended practices for Inter Access Point Protocol (IAPP) for multi-vendor use
g	Develop higher speed PHY extension to 802.11b (54 Mbps)
h	Enhance 802.11 MAC and 802.11a PHY-Dynamic Frequency selection Transmit Power control
i	Enhance 802.11 MAC security and authentication mechanisms
j	Enhance the 802.11 standard and amendments to add channel selection for 4.9 GHz and 5 GHz in Japan
k	Define Radio Resource Measurement enhancements to provide interfaces to higher layers for radio and network measurements
m	To perform editorial maintenance, corrections, improvements, clarifications, and interpretations relevant to documentation for 802.11 family specifications.
n	High throughput extensions (>100MB/s at MAC SAP) in 2.4GHz and/or 5GHz bands
p	Vehicular communications protocol aimed at vehicles, such as toll collection, vehicle safety services, and commerce transactions via cars.
r	To develop a standard specifying fast BSS transitions, fast roaming.
s	To define a MAC and PHY for meshed networks that improve coverage with no single point of failure.
t	To provide a set of performance metrics, measurement methodologies, and test conditions to enable manufacturers, test labs, service providers, and users to measure the performance of 802.11 WLAN devices and networks at the component and application level.

The 802.11a standard delivers a maximum data rate of 54 Mbps and up to 23 non-overlapping frequency channels (in some geographic areas) resulting in increased network capacity, improved scalability, and the ability to create microcellular deployments without interference from adjacent cells.

Note Additional channels have been approved with restrictions. See http://www.cisco.com/en/US/products/hw/wireless/ps469/products_white_paper0900aecd801c4a88.shtml.

Operating in the unlicensed portion of the 5 GHz radio band, 802.11a is also immune to interference from devices that operate in the 2.4 GHz band, such as microwave ovens, cordless phones (5 GHz cordless phones are now on the market), and Bluetooth (a short-range, low-speed, point-to-point, personal-area-network wireless standard). The 802.11a standard is not compatible with existing 802.11b-compliant wireless devices. Equipment at 2.4-GHz and 5-GHz can operate in the same physical environment without interference.

The 802.11g delivers the same 54 Mbps maximum data rate as 802.11a, but operates in the same 2.4 GHz band as 802.11b. The 802.11g also provides backward compatibility with existing 802.11b devices.

Selecting between these technologies is not a one-for-one trade off. They are complementary technologies and will coexist in future enterprise environments. You must be able to make an educated choice between deploying 2.4 GHz-only networks, 5 G Hz-only networks, or a combination of both. Organizations with existing 802.11b networks cannot simply deploy a new 802.11a network on 5 GHz APs and expect to have an 802.11a 54 Mbps data rate coverage similar to 11 Mbps of data rate with 802.11b APs. The technical characteristics of both these bands simply do not allow for this kind of interchangeable coverage.

RF Spectrum Implementation

In the United States, three bands are defined as unlicensed and known as the Industrial, Scientific, and Medical bands (ISM). The ISM bands are as follows:

- 900 MHz (902-to-928 MHz)
- 2.4 GHz (2.4-to-2.4835 GHz) IEEE 802.11
- 5 GHz (5.15-to-5.35 and 5.725-to-5.825 GHz) IEEE 802.11a. These are known as UNII-1 and UNII-2 bands.

Each range has different characteristics. The lower frequencies exhibit better range, but with limited bandwidth and hence lower data rates. The higher frequencies have less range and subject to greater attenuation from solid objects.

Direct Sequence Spread Spectrum

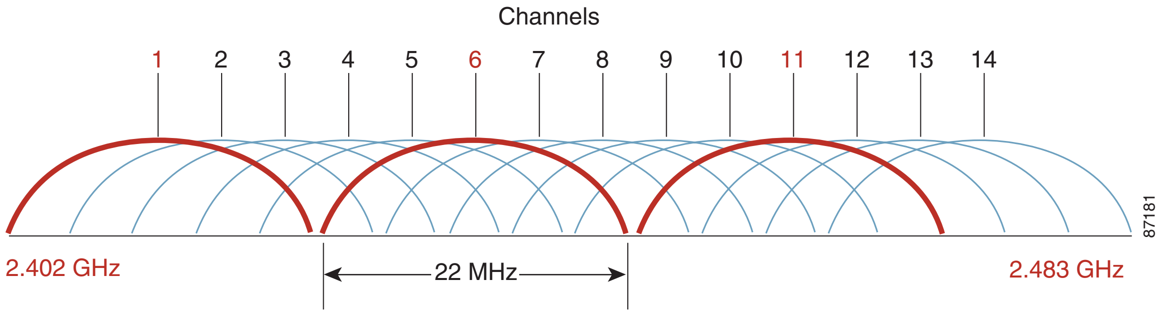
The Direct Sequence Spread Spectrum approach involves encoding redundant information into the RF signal. Every data bit is expanded to a string of chips called a chipping sequence or Barker Sequence. The chipping rate as mandated by the IEEE 802.11 is 11 chips Binary Phase-Shift Keying (BPSK)/Quadrature Phase-Shift Keying (QPSK) at the 1 and 2 Mbps rates and eight chips (CCK) at the 11 and 5.5 Mbps rate. So, at 11 Mbps, 8 bits are transmitted for every one bit of data. The chipping sequence is transmitted in parallel across the spread spectrum frequency range.

IEEE 802.11b Direct Sequence Channels

Fourteen channels are defined in the IEEE 802.11b Direct Sequence (DS) channel set. Each DS channel transmitted is 22 MHz wide, but the channel separation is only 5 MHz. This leads to channel overlap such that signals from neighboring channels can interfere with each other. In a 14-channel DS system, (11 of which are usable in the US), only three non-overlapping (and hence, non-interfering) channels 25 MHz apart are possible, such as Channels 1, 6, and 11.

This channel spacing governs the use and allocation of channels in a multi-AP environment such as an office or campus. APs are usually deployed in *cellular* fashion within an enterprise where adjacent APs are allocated non-overlapping channels. Alternatively, APs can be co-located using Channels 1, 6, and 11 to deliver 33 Mbps bandwidth to a single area, but only 11 Mbps to a single client. The channel allocation scheme is illustrated in Figure 2-5.

Figure 2-5 IEEE 802.11b DSSS Channel Allocations



IEEE 802.11g

The 802.11g provides for a higher aggregate rate (162 Mbps) in the 2.4-Ghz band, the same spectrum as 802.11b. The 802.11g is backward compatible with 802.11b and provides additional data rates of 6, 9, 12, 18, 24, 36, 48 and 54 Mbps. At higher data rates, 802.11g uses the same modulation technique, Orthogonal Frequency Division Multiplexing, (OFDM), as 802.11a. (See "IEEE 802.11a OFDM Physical Layer" on page 10.) Figure 2-6 lists 802.11g modulation and transmission types for the various data rates.

Table 2-6 802.11g Modulation and Transmission types

Modulation	Transmission Type	Bits per Subchannel	Data Rate (Mbps)
BPSK	DSSS	**NA**	1
QPSK	DSSS	NA	2
CCK	DSSS	NA	5.5
BPSK	OFDM	125	6
BPSK	OFDM	187.5	9
CCK	DSSS	NA	11
QPSK	OFDM	250	12
QPSK	OFDM	375	18
16-QAM	OFDM	500	24
16-QAM	OFDM	750	36
64-QAM	OFDM	1000	48
64-QAM	OFDM	1125	54

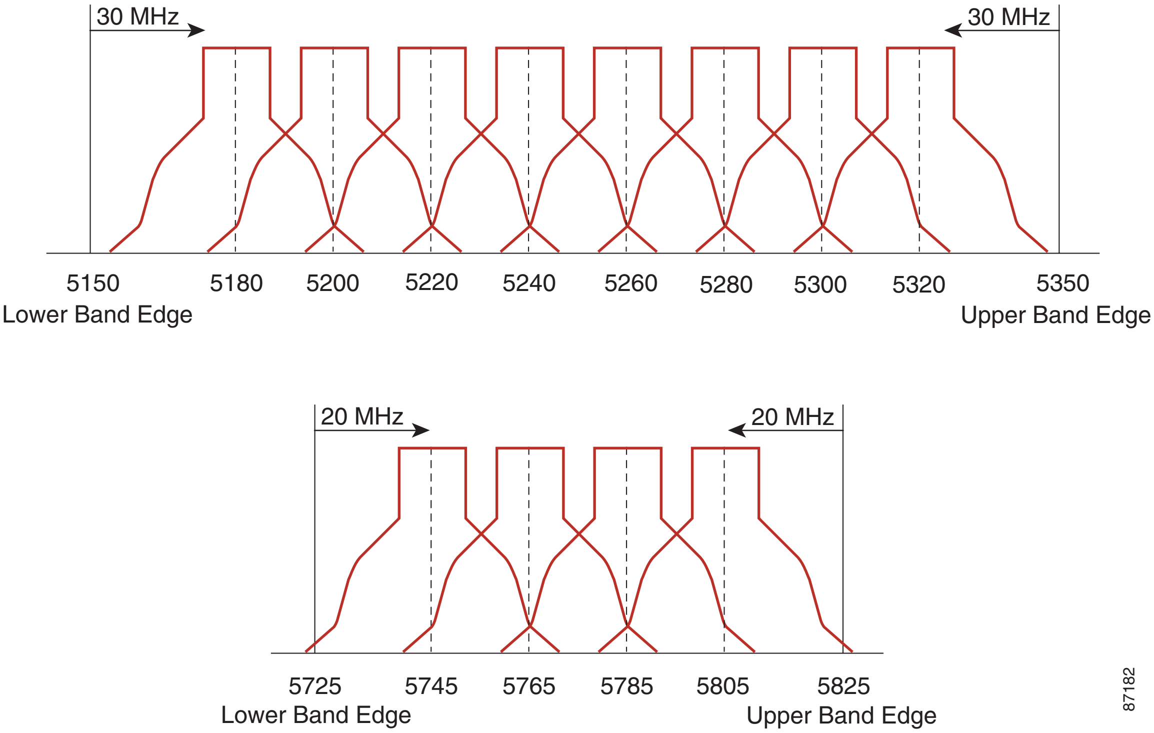
IEEE 802.11a OFDM Physical Layer

The IEEE 802.11 standard defines requirements for PHY operating in the 5.0 GHz U-NII frequency and data rates ranging from 6 Mbps to 54 Mbps. It uses OFDM which is a multi-carrier system (compared to single carrier systems). OFDM allows sub-channels to overlap, providing a high spectral efficiency. The modulation technique allowed in OFDM is more efficient than spread spectrum techniques.

IEEE 802.11a Channels

Figure 2-6 shows the center frequency of the channels. The frequency of the channel is 10 MHz on either side of the dotted line. There is 5 MHz of separation between channels.

Figure 2-6 802.11a Channel Set



For the US-based 802.11a standard, the 5 GHz unlicensed band covers 300 MHz of spectrum and supports 12 channels. As a result, the 5 GHz band is actually a conglomerate of three bands in the USA: 5.150-to-5.250 GHz (UNII 1), 5.250-to-5.350 GHz (UNII 2), and 5.725-to-5.875 GHz (UNII 3).

Planning for RF Deployment

Many of the RF design considerations are interdependent or implementation dependent. As a result there is no one-size-fits-all template for the majority of requirements and environments.

RF Deployment Best Practices

Some considerations can be addressed with general best practice guidelines. The following can be applied to most situations:

- The number of users versus throughput and a given AP. The general recommended number of users per AP is 15 to 25.
- The distance between APs can cause throughput variations for clients based on distance from the AP. The recommendation is to limit the AP data rate to the higher data rates.

- The number of APs depends on coverage and throughput requirements, which might vary. For example Cisco's internal information systems (IS) group currently uses six APs per 38,000 square feet of floor space.

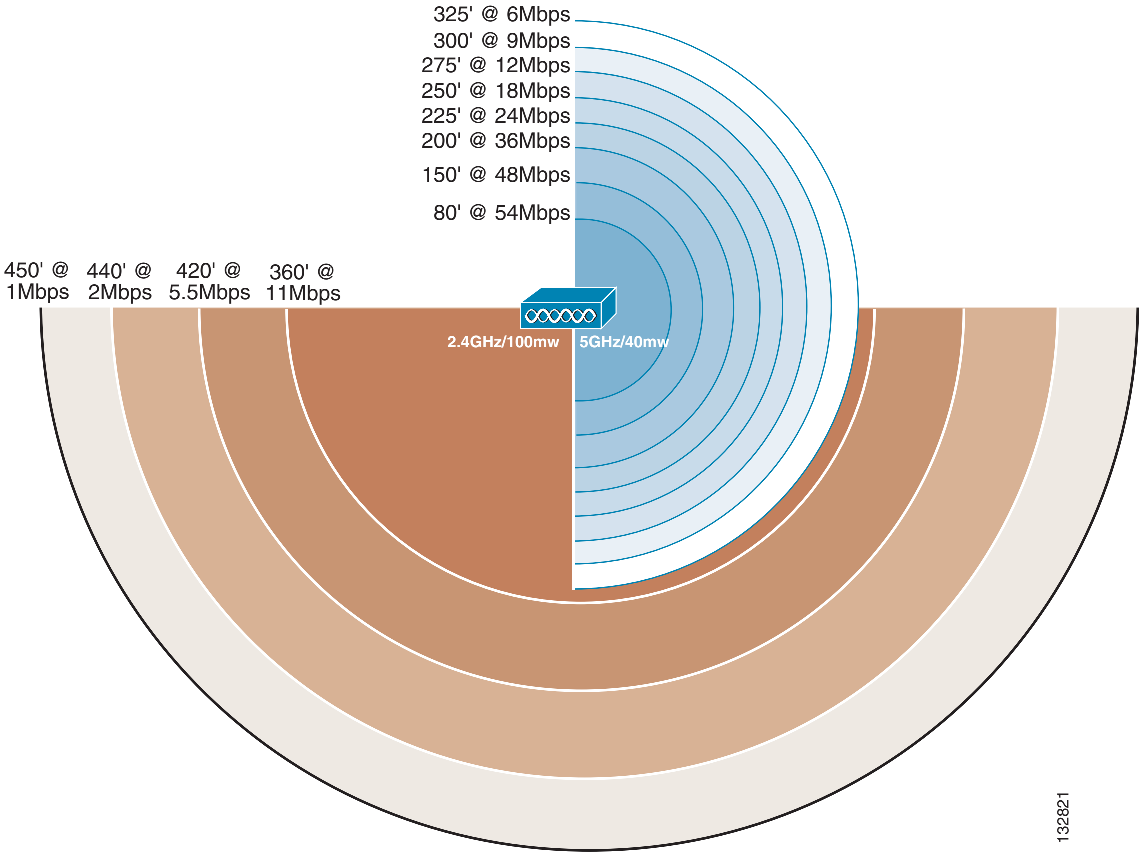
Note Based upon the variability in environments a site survey to determine the number of APs required and their optimal placement is highly recommended.

WLAN Data Rates Required

Data rates affect cell size. Lower data rates (such as 1 Mbps) can extend farther from the AP than can higher data rates (such as 54Mbps). This is illustrated in Figure 2-7 (not to scale). Therefore, the data rate and power level affects cell coverage and consequently the number of APs required, as illustrated in Figure 2-8.

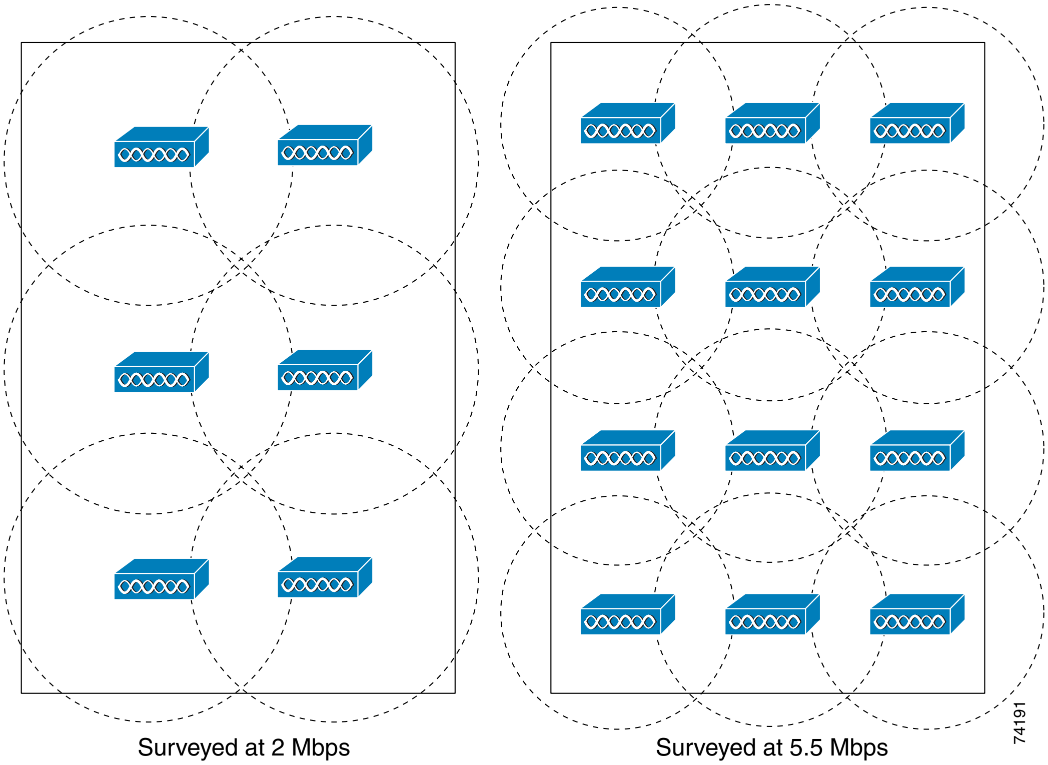
Different data rates are achieved by sending a more *redundant* signal on the wireless link, allowing data to be more easily recovered from noise. The number of symbols sent out for a packet at the 1 Mbps data rate is greater than the number of symbols used for the same packet at 11 Mbps. This means that sending data at the lower bit rates takes more time than sending the equivalent data at a higher bit rate.

Figure 2-7 Data Rate Compared with Coverage



The diameter of the coverage depends upon factors such as environment, power and antenna gain. For example, indoors[1] using the standard antennas on the NIC card and APs, the diameter of the 1 Mbps circle is approximately 700 ft. (210 m), and the diameter of the 11 Mbps circle is about 200 ft. (60 m). Increasing the gain of the antenna can increase the distance and change the shape of the radiation pattern to something more directional.

Figure 2-8 Coverage Comparison and AP density for Different Data Rates



The required data rate has a direct impact upon the number of APs needed in the design. The example in Figure 2-8 illustrates this point. While six APs with a data rate of 2 Mbps might adequately service an area, it might take twice as many APs to support a data rate of 5 Mbps, and more again to support data rates of 11 Mbps.

The data rate chosen is dependent on the type of application to be supported. In a WLAN-LAN extension environment, the higher data rates give maximum throughput and should minimize performance-related support issues. In a WLAN vertical application environment, the data rates selected are determined by the application requirements; some clients might not support the higher data rates and might require the use of lower data rates.

It might seem logical to choose the default configuration of APs and clients, thereby allowing all data rates. However, there are three key reasons for limiting the data rate to the *highest* rate, at which full coverage is obtained:

- Broadcast and multicast are sent at the lowest associated data rate to ensure that all clients can see them. This reduces the WLAN throughput because traffic must wait until frames are processed at the slower rate.

[1] Typically the outdoor range is greater because there are fewer obstacles, and less interference.

- Clients that are farther away, and therefore accessing the network at a lower data rate decrease the overall throughput by causing delays, while the lower bit rates are being serviced. It may be better if the clients roamed to another AP.
- If a 54 Mbps service is specified and provisioned with APs to support *all* data rates, clients at lower rates can associate with APs configured in this way, which can create a coverage area greater than planned, thereby increasing the security exposure and potentially interfering with other WLANs.

Client Density and Throughput Requirements

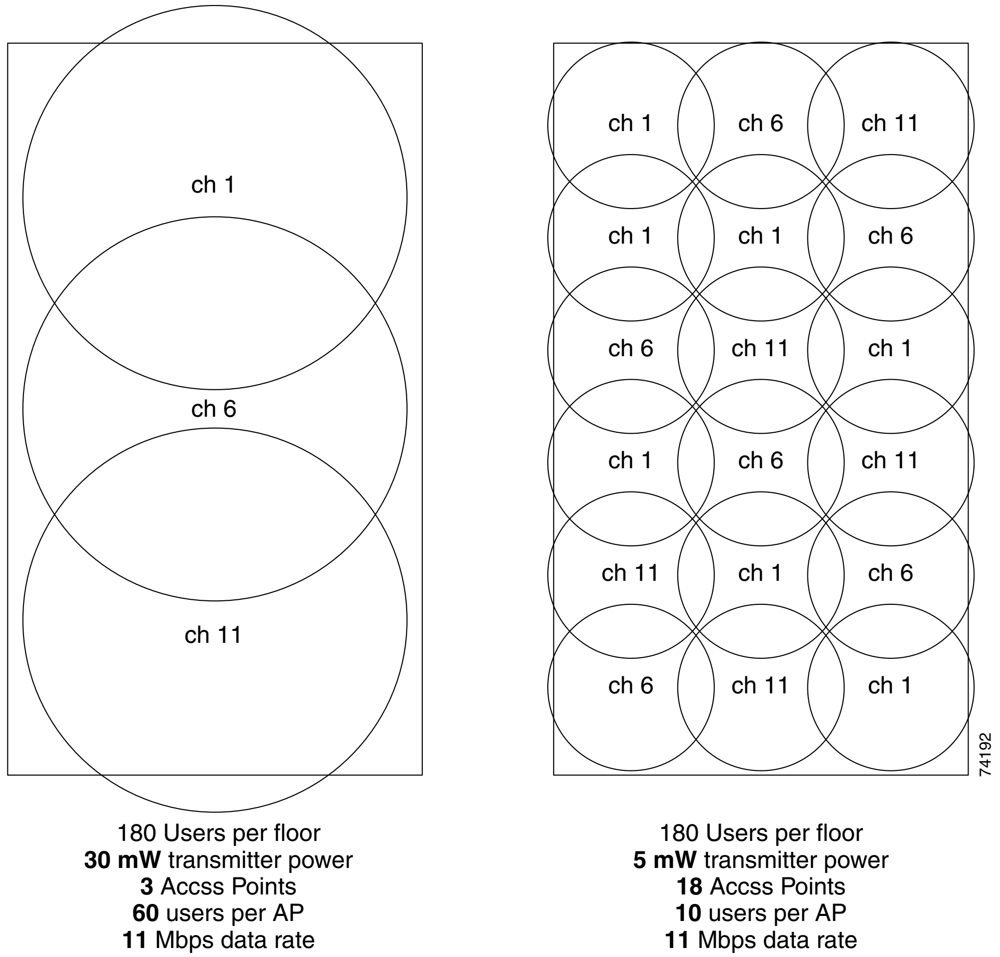
APs are similar to shared hubs and have an aggregate throughput much less than the data rate. With this in mind, you must have an estimate of the maximum number of active associations (active clients). This can be adjusted more or less according to the particular application.

Each cell provides an aggregate amount of throughput that is shared by all the client devices that are within that cell and associated to a given AP. This basically defines a cell as a collision domain. After deciding on the minimum data rate, be sure to consider how much throughput should, on average, be provided to each user of the wireless LAN.

Taking barcode scanners as an example, 25 Kbps may be more than enough bandwidth for such an application. Using a 802.11b AP at 11 Mbps of data rate results in an aggregate throughput of 5 to 6 Mbps, resulting in a maximum number of 200 users. This number could not be achieved due to 802.11 management overhead that is associated with the large number of clients and collision that can be supported satisfactorily. For a 1 Mbps system, 20 users can utilize the same AP for similar bandwidth results. It should be noted that throughput is also greatly impacted by the frame size and, that in calculations such as this, the aggregate throughput of WLAN at the average frame size should be used rather than the stated maximum throughput, which uses 1500 byte frames.

You can increase the potential per-user throughput by decreasing the number of users contending for the aggregate throughput that is provided by a single AP. This can be done by decreasing the size of the coverage cell or adding a second AP on a non-overlapping channel in the same cell area. To reduce the cell size, the AP power or antenna gain can be reduced, resulting in fewer clients in that cell area. This means you will need more APs for the same overall area, increasing the cost of deployment. An example of this is shown in Figure 2-9. Some of the APs do not provide the settings to control transmit power and many have limited or no options

Figure 2-9 Changing the Output Power to Increase Client Performance



Note Client power should be adjusted to match the AP power settings. Maintaining a high setting on the client does not result in higher performance and it can cause interference in nearby cells.

WLAN Coverage Required

Different enterprises have different coverage requirements. Some need a WLAN to cover specific common areas. Others need WLANs to cover each floor of a building, to cover the entire building including stairwells and elevators, or to cover the entire campus including parking lots and roads.

Apart from impacting the number of APs required, the coverage requirements can introduce other issues, such as specialized antennas, outdoor enclosures and lightning protection.

Security Policy

RF design can be used to minimize the RF radiation in coverage areas or in directions where coverage is not required. For example, if WLAN coverage is required only in the buildings, then the amount of RF coverage outside the building can be minimized by AP placement and directional antennas.

RF Environment

The performance of the WLAN and its equipment depends upon its RF environment. The following are some examples of adverse environmental variables:

- 2.4 GHz cordless phones
- Walls fabricated from wire mesh and stucco
- Filing cabinets and metal equipment racks
- Transformers
- Heavy duty electric motors
- Fire walls and fire doors
- Concrete
- Refrigerators
- Sulphur plasma lighting (Fusion 2.4 GHz lighting systems)
- Air conditioning ducts
- Other radio equipment
- Microwave ovens
- Other WLAN equipment

A site survey should be performed to ensure that the required data rates are supported in all the required areas, despite the environmental variables mentioned above.

The site survey should consider the three dimensional space occupied by the WLAN. For example a multi-story building WLAN with different subnets per floor might require a different RF configuration than the same building with a single WLAN subnet per building. In the multiple subnet instance, a client attempting to roam to a different AP on the same floor might acquire an AP from an adjacent floor. Switching APs in a multi-subnet environment changes the roaming activity from a *seamless Layer 2 roam* to a *Layer 3 roam* which in turn disrupts sessions and might require user intervention. The WLSM Layer 3 roaming simplifies this deployment by allowing the client to maintain its IP address even if the AP it roams to is on another subnet.

CHAPTER 3

WLAN Technology and Product Selection

This chapter focuses on technology and product assessment and selection in WLAN environments.

WLAN Technology Selection Considerations

Understanding your environment's requirements and plans for future enhancements are key when choosing a wireless technology.

Comparing WLAN Standards

So, which standard should an organization select? 802.11g delivers the same 54 Mbps maximum data rate as 802.11a, yet it offers the additional advantage of backward compatibility with 802.11b equipment. This means that 802.11b client cards will work with 802.11g APs, and 802.11g client cards will work with 802.11b APs. Because 802.11g and 802.11b operate in the same 2.4 GHz unlicensed band, migrating to 802.11g is be an affordable choice for organizations with existing 802.11b wireless infrastructures. It should be noted that 802.11b products cannot be software upgraded to 802.11g because 802.11g radios use a different chip set than 802.11b. However, much like Ethernet and Fast Ethernet, 802.11g products can be combined with 802.11b products in the same network. Because 802.11g operates in the same unlicensed band as 802.11b, it shares the same three non-overlapping channels. The 802.11a standard can deliver 54Mbps data rate. 802.11a also supports more channels (eight to twenty-two non-overlapping channels) making the RF deployment more flexible. Note that 802.11b/g and 802.11a radios do not inter-work due to spectrum and modulation techniques.

WLAN Data Rate, Throughput and Capacity

Given the flexibility to chose between the various 802.11 standards, a consideration of WLAN data rate, throughput and capacity is warranted.

- Data rate(s) are a matter of standards, environment, and distance. As mentioned, 802.11a provides data rates at in the range of 6 to 54 Mbps, with rates existing at 6, 9,12,18,24,36,48,54 Mbps. 802.11b at 1, 2, 5.5 an 11 Mbps. 802.11g provide 802.11b compatible rates, with additional rates at 6, 9,12,18,24,36,48,54 Mbps
- Throughput is the data rate minus protocol and transmission overhead. Throughput is the net speed. Data rate is the usable, or experienced, data rate.

- Although 802.11a and 802.11g can support the same bit rates, the throughput of 802.11g is slightly less that of 802.11a, due to timing parameters included in 802.11g to provide 802.11b compatibility. If 802.11g and 802.11b clients are using the same AP the maximum throughput of 802.11g clients falls due to the overhead introduced to support the 802.11b clients.
- Per-user throughput is the total throughput for a given frequency (channel) divided by the users on that frequency. This per-user throughput determines the theoretical maximum throughput that an individual application or user could utilize.
- Capacity is throughput multiplied by non-overlapping channels.

Table 3-1 provides an example of data rates, throughput and per-user throughput.

Three non-overlapping channels in the 2.4 GHz band used by 802.11b and 802.11g, represents a challenge that can complicate deployments. 802.11b devices have a maximum capacity of 18Mbps (6 Mbps multiplied by three channels) per given area. 802.11g (no legacy 802.11b support) provide a 66 Mbps capacity (22 Mbps by 3 channels). With eight or more channels, 802.11a systems have a capacity of up to 200Mbps (25 Mbps multiplied by eight channels) in a given area. Figure 3-1 shows the theoretical maximum capacity for the various 802.11 technologies.

The 802.11a standard provides a potential throughput and capacity improvement for a WLAN compared with 802.11b/g-based WLANs implementations. The 802.11a 5 GHz band provides more than three times as much spectrum as the 802.11 b/g 2.4 GHz band. A key advantage for 802.11a deployments is greater flexibility for channel re-use and total enterprise wide capacity. With a greater number of channels (12-23) to select from, it is easier it is to deploy an Enterprise WLAN. Interference in the network is reduced by avoiding two adjacent AP using the same frequency and by increasing the distance between APs with the same frequencies (reducing co-channel interference). That is, the traffic from devices in overlapping cells set to the same channel result in mutual interference, thereby impeding performance.

Given the difference in operating frequencies, 802.11b/g and 802.11a can co exist within the same environment, allowing users to move from one to another by switching clients, or using a dual-band client (combines both radios into a single client). An enterprise must conduct comprehensive site surveys for each technology to guarantee adequate network coverage. Each frequency has different signal strength, interference, and reflection characteristics, and each implementation must be optimized for different requirements.

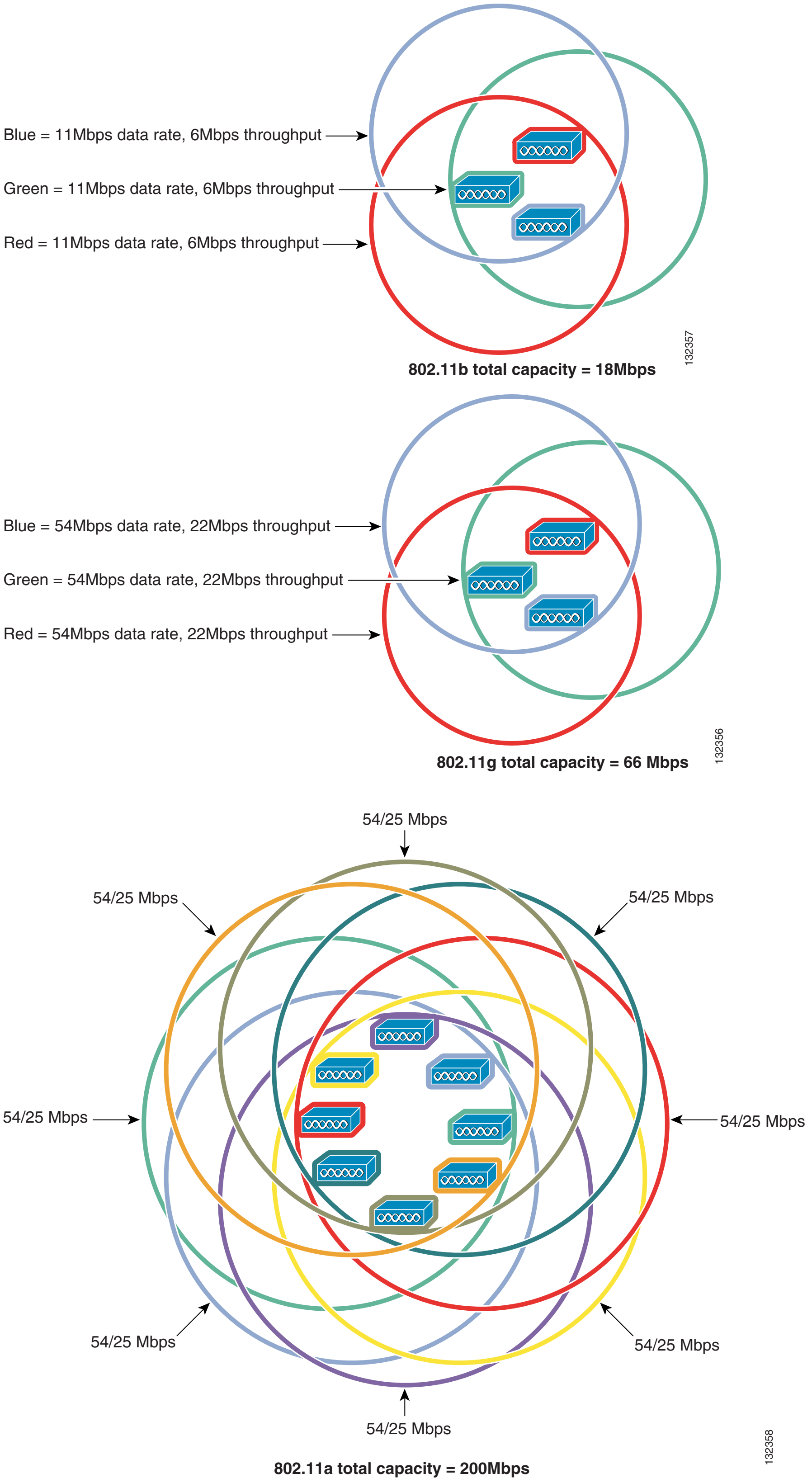
Table 3-1 Throughput Examples

Technology	Data Rate (Mbps)	Aggregate Throughput (Mbps)	Example User Count	Average Per-user Throughput
802.11b	11	6	10	600Kbps
802.11b	11	6	20	300Kbps
802.11b	11	6	30	200Kbps
802.11g*	54	22	10	2.1Mbps
802.11g*	54	22	20	1.1Mbps
802.11g*	54	22	30	760Kbps
802.11a	54	25	10	2.5Mbps
802.11a	54	25	20	1.25Mbps

Table 3-1 Throughput Examples

Technology	Data Rate (Mbps)	Aggregate Throughput (Mbps)	Example User Count	Average Per-user Throughput
802.11a	54	25	30	833Kbps
* No legacy support				

Figure 3-1 Total Capacity (Theoretical)


Blue = 11Mbps data rate, 6Mbps throughput
Green = 11Mbps data rate, 6Mbps throughput
Red = 11Mbps data rate, 6Mbps throughput
132357
802.11b total capacity = 18Mbps
Blue = 54Mbps data rate, 22Mbps throughput
Green = 54Mbps data rate, 22Mbps throughput
Red = 54Mbps data rate, 22Mbps throughput
132356
802.11g total capacity = 66 Mbps
54/25 Mbps
54/25 Mbps
54/25 Mbps
54/25 Mbps
54/25 Mbps
54/25 Mbps
54/25 Mbps
54/25 Mbps
132358
802.11a total capacity = 200Mbps

Data Rate Considerations

Data rates and cell size are intricately tied together. Lower data rates (such as 1 Mbps) can extend further from the AP than can higher data rates (such as 54 Mbps). An example is illustrated in Figure 3-2. Hence the data rate and power level effects cell coverage, and consequently the number of APs required.

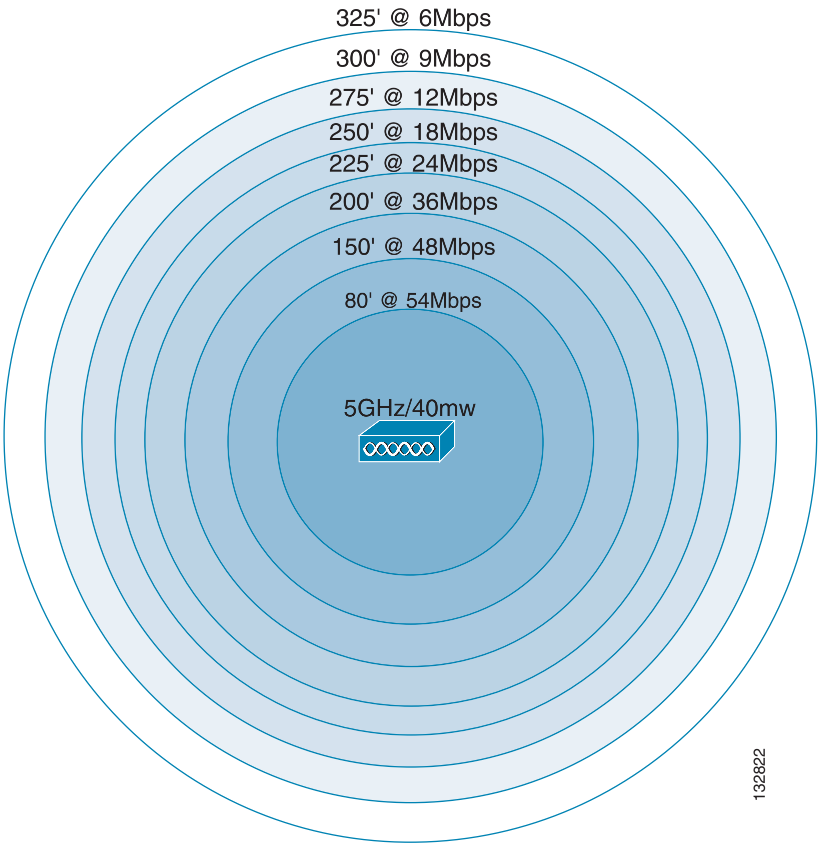
What is considered an acceptable data rate, ultimately depends upon how much bandwidth is required for the application that you want to run at a particular location. Be sure to survey users for the minimum data rate required.

Note The *Cisco Aironet Site Survey Utility* surveys at a given data rate and does not rate shift.

APs offer clients multiple data rates for the wireless link. For 802.11b, the range is from 1 to 11 Mbps in four increments: 1, 2, 5.5 and 11 Mbps, while 802.11a the range is 6 to 54 Mbps in seven increments: 6, 9, 12, 18, 24, 36, 48 and 54 Mbps. Because data rates affect range, selecting data rates during the design stage is extremely important.

The client cards automatically rate shift to the fastest possible rate of the AP; when this is done varies form vendor to vendor. Since each data rate has a unique cell of coverage (the higher the data rate, the smaller the cell), the minimum data rate must be determined at the design stage. Cell sizes at given data rates can be thought of as being nested concentric circles. See Table 3-2 for an example. Selecting only the highest data rate requires a greater number of APs to cover a given area; therefore care must be taken to develop a compromise between required data rates, capacity and overall system cost. The rates/distances in Figure 3-2 are approximate and to be used for example purposes only. Variations of rates/distances will exist based factors such as antenna, radio type, power and environment, to name a few.

Figure 3-2 802.11a Data Rates



Throughput Considerations

Data rate is often confused with the aggregate data throughput. The throughput takes into account the overhead associated with protocol frame structure, collisions, and implementation processing delays associated with frames that are processed by clients and APs. Protocol overhead includes parameters such as RTS, CTS, ACK frames, beacon periods, back off period and propagation delays. The overhead associated with the 802.11b standard exceeds the overhead for 802.3 Ethernet, resulting in better throughput for 10 Mbps Ethernet than 11 Mbps Wi-Fi.

An important purchasing consideration for any networking technology is the amount of bandwidth, data rate, or throughput it provides to each network user, and how well that throughput can support the applications running on the network.

A comparison table of the wireless networks is shown in Table 3-2.

Table 3-2 802.11 Throughput, Capacity Compared (Estimated)

	Data Rate (Mbps)	Max Throughput (Mbps)	Channels	Capacity (Mbps)
802.11b	11	6	3	18
802.11g (mixed mode, RTS/CTS)	54	8	3	24

Table 3-2 802.11 Throughput, Capacity Compared (Estimated)

	Data Rate (Mbps)	Max Throughput (Mbps)	Channels	Capacity (Mbps)
802.11g (mixed mode, CTS to self)	54	14	3	42
802.11g (no legacy support)	54	22	3	66
802.11a (UNII-1 and UNII-2)	54	25	8	200
802.11a (UNII bands)	54	25	12	300
802.11a (with 802.11h support)	54	25	23	575

Note The maximum throughput is achieved when the maximum frame size is used, and therefore typical user traffic can expect lower maximum throughput due to their typically lower average frame size.

For example, 802.11b offers an 11 Mbps data rate, translating into approximately 5 to 7 Mbps of actual throughput per AP. This amount is shared among all network users accessing it at the same time, and is managed through a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) technique modeled on its Ethernet wired equivalent. As most network traffic is “bursty”, and only a few users are on the network simultaneously, Wi-Fi network users generally experience very good connectivity speeds.

Performance Considerations

While unlicensed spectrum is very attractive as there is no licensing fee issue, those using it must factor in the potential performance degradation associated with ambient interference. 802.11a operates in unlicensed bands in exactly the same way as 802.11b and earlier 900 MHz systems operate in unlicensed bands. That is, there are no restrictions on the types of devices that operate in these bands provided that they all conform to a common set of rules. The 900 MHz portion of the spectrum was initially used by WLANs and then, far more commonly, by cordless telephones. Although these devices all complied with applicable regulations, they acted upon each other as interferers, mutually degrading performance and usability. The WLAN industry essentially abandoned the 900 MHz band and migrated to the 2.4 GHz band. Initially, the WLAN industry had this band to themselves (with the exception of microwave oven RF emissions). Eventually, however, the band became more crowded with an increasing number of products, including Bluetooth devices and 2.4 GHz cordless telephones. The attractiveness of the 2.4 GHz band to manufacturers, license-free operation on an international scale and resulting worldwide marketability for 2.4 GHz devices, leads to a central problem for the 2.4 GHz band overcrowding.

This, in turn, leads to a principal advantage of 802.11a because it operates in the relatively interference free 5 GHz band. As of now, it is relatively immune to interference from other devices. 802.11a products are relatively few in number. Bluetooth operates in the 2.4 GHz band and there are very few 5 GHz cordless telephones available in the market. The point is, that today, the 5 GHz band is relatively clean, but there are no restrictions on this band that do not apply equally to 900 MHz and 2.4 GHz. Over time, the 5 GHz band might become equally crowded with interference-causing devices. The amount of spectrum that is available in the 802.11a band is also an advantage as it offers more non-overlapping channels, and therefore offers many opportunities to avoid interference in a particular band.

As the 2.4 GHz band is unlicensed, it is available for anyone to use within limits of maximum Effective Isotropic Radiated Power (EIRP). WLAN interference can come from a number of sources. The main sources are as follows:

- *Microwave Ovens*—The magnetron in household and commercial microwave ovens operates over tens of megahertz in the 2.4 to 2.483 GHz band. While microwave ovens operate at about 700 to 1000 W, the maximum allowed EIRP for WLAN devices is between 0.1 and 4 W. WLAN equipment such as APs should not be located near microwave ovens.
- *Co-channel Interference*—Interference can from radios in adjacent cells on the same frequency. Effective site surveying and WLAN cell planning should minimize the effect of this interference. As WLANs become more prevalent, interference from sources outside enterprise control may become more of an issue, such as in multiple tenancy situations, shopping centers, and apartment blocks. Proper cell planning of the channel frequency and careful layout of the AP can minimize the interference.
- *Bluetooth*—Bluetooth is a Wireless Personal Area Network technology sharing the same 2.4 GHz spectrum as 802.11b. Bluetooth uses Frequency Hopping Spread Spectrum (FHSS) and is a shorter range and lower bandwidth technology than 802.11b. FHSS systems use frequently changing, narrow bands over all channels. It is important to manage the concurrent operation of 802.11b WLANs and Bluetooth within the enterprise. Task Group 2 of the IEEE 802.15 Working Group is looking at the coexistence issues of IEEE 802.11b WLANs and Bluetooth. Multiple companies have researched the issue and concluded that if the two technologies are separated by two meters or more, there is no significant interference.
- *2.4 GHz Cordless Telephones* —Some of the newer household and office cordless telephones operate in the 2.4 GHz range (Direct Sequence Spread Spectrum (DSSS) and FHSS). Depending on the conditions and the manufacturer, degradation to the WLAN can vary from unnoticeable to a total loss of association between the client and the AP. Interference from the WLAN can also impact the voice quality. Users are encouraged to use 900 MHz Cordless Phones in instances where they must coexist with WLANs. If this is not possible, separate the AP from the phone base station as far as possible and perform some rudimentary degradation tests. Note that DSSS cordless phones are more likely to cause degradation than FHSS types.
- *Shared Internet Access*—Wireless local loop (WLL) and systems like Metricom-Ricochet (which is coming back in the market), and T-Mobile all use the same band and can be a source of interference. Interference can also come from other systems such as neighboring DSSS and FHSS WLAN networks.

Range Considerations

Table 3-3 provides a comparison of the relative data rates and ranges associated with 802.11a and 802.11b/g WLANs. These are typical maximum ranges but range varies, normally downward, depending upon the environment. As more obstructions are encountered, such as a metallic building structure, range is reduced.

Table 3-3 802.11 Throughput Capacity Compared, Cisco 1130A/B/G AP (OFDM 50 mW. CCK 100 mW)

	Indoor (Distance across open office environment)		**Outdoor**	
	802.11a	**802.11g**	**802.11a**	**802.11g**
Data Rates and Ranges	80 ft. (24 m) @ 54 Mbps	100 ft. (30 m) @ 54 Mbps	100 ft. (30 m) @ 54 Mbps	120 ft. (37 m) @ 54 Mbps
	150 ft. (45 m) @ 48 Mbps	175 ft. (53 m) @ 48 Mbps	300 ft. (91 m) @ 48 Mbps	350 ft. (107 m) @ 48 Mbps
	200 ft. (60 m) @ 36 Mbps	250 ft. (76 m) @ 36 Mbps	425 ft. (130 m) @ 36 Mbps	550 ft. (168 m) @ 36 Mbps
	225 ft. (69 m) @ 24 Mbps	275 ft. (84 m) @ 24 Mbps	500 ft. (152 m) @ 24 Mbps	650 ft. (198 m) @ 24 Mbps
	250 Ft. (76 m) @ 18 Mbps	325 ft. (100 m) @ 18 Mbps	550 ft. (168 m) @ 18 Mbps	750 ft. (229 m) @ 18 Mbps
	275 ft. (84 m) @ 12 Mbps	350 ft. (107 m) @ 12 Mbps	600 ft. (183 m) @ 12 Mbps	800 ft. (224 m) @ 12 Mbps
	300 ft. (91 m) @ 9 Mbps	360 ft. (110 m) @ 11 Mbps	625 ft. (190 m) @ 9 Mbps	820 ft. (250 m) @ 11 Mbps
	325 ft. (100 m) @ 6 Mbps	375 ft. (114 m) @ 9 Mbps	650 ft. (198 m) @ 6 Mbps	875 ft. (267 m) @ 9 Mbps
		400 ft. (122 m) @ 6 Mbps		900 ft. (274 m) @ 6 Mbps
		420 ft. (128 m) @ 5,5 Mbps		910 ft. (277 m) @ 5,5 Mbps
		440 ft. (134 m) @ 2 Mbps		940 ft. (287 m) @ 2 Mbps
		450 ft. (137 m) @ 1 Mbps		950 ft. (290 m) @ 1 Mbps

Table 3-4 Various Relationships that Relate to Range

Factor	**Example**	**Impact on Range**
Frequency	Higher frequency, e.g. 5GHz (rather than lower frequency, e.g. 2.4GHz)	As frequency increases, range decreases.
Indoor Attenuators	Structural and cubicle walls, elevator shafts, windows, shielding, backing people, etc.	As building material density increases, range decreases.
Outdoor Attenuators	Exterior walls, trees, etc.	As density increases, range decreases.
Means of Transmission	OFDM and DSSS	OFDM increases range relative to DSSS, all else being equal.
Modulation and Data Rate	BPSK, QPSK, CCK, 16-QAM, 64-QAM	As modulation increases in complexity and data rates increase, range decreases.
Transmit Power	100mW(20dBm), 50mW (17dBm)	As transmit power increases, range increases, both the client and AP power must increase. In general, AP and client power levels should close to the same level.

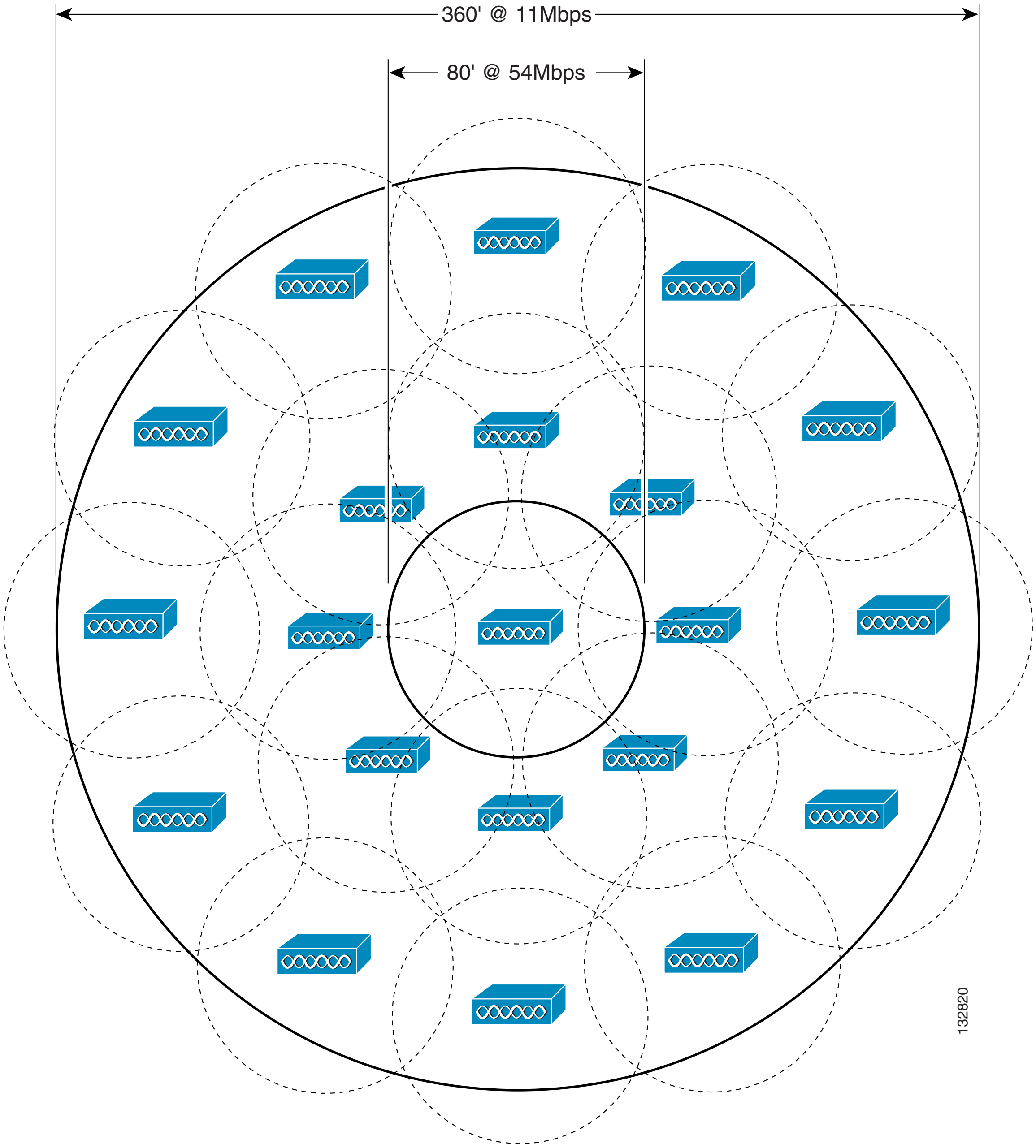
Table 3-4 Various Relationships that Relate to Range

Factor	Example	Impact on Range
Receive Sensitivity	-85dBm, -72dBm, etc.	As receive sensitivity increases in absolute value, range increases.
Antenna Gain	2.2dBi, 5dBi, 20dBi, etc.	As antenna gain increases, range increases while coverage shape changes and coverage area remains constant. Antenna gain is bi-directional, that is, the gain occurs for both transmission and reception.

Figure 3-3 illustrates the coverage area of an 802.11b AP at a maximum bit rate of 11 Mbps, overlaid with 802.11a APs at a maximum bit rate of 54 Mbps. This comparison shows the impact of the different ranges of 802.11b and 802.11a. Ten 802.11a APs are required to cover a similar area as the one 802.11b AP. As of this writing, for 802.11g at 54Mbps data rates, the range extends to approximately to 90 feet from the AP, where as the 802.11a range is approximately 45 feet This approximates to a 3 to 1 coverage advantage of 802.11g over 802.11a.

In summary, more 802.11a APs are required to support a given area in comparison to both 802.11b/g APs, but the capacity of the 802.11a network is significantly greater.

Figure 3-3 Difference in Coverage between 802.11a and 802.11b



Signal Propagation

There is an inverse relationship between wavelength and range. All other things being equal, a signal transmitted at a lower frequency carries farther than a signal transmitted in a higher band. Additionally, a longer waveform from lower in the spectrum will tend to propagate better through solids, like walls and trees, than a shorter waveform. Because 802.11g operates in the same 2.4 GHz portion of the radio frequency spectrum as does 802.11b, it will share its fundamental advantage over the 5 GHz-based 802.11a.

Other factors to consider are transmit power and receive sensitivity. The selection of either DSSS or OFDM transmission type has an effect on the maximum power the transmitter can use, as well as the capability of the receiver, particularly at higher data rates.

Antenna Considerations

An antenna gives the wireless system three fundamental properties—gain, direction, and polarization. Gain is a measure of increase in power. Direction is the shape of the transmission pattern. A good analogy for an antenna is the reflector in a flashlight. The reflector concentrates and intensifies the light beam in a particular direction similar to what a parabolic dish antenna would to a RF source in a radio system.

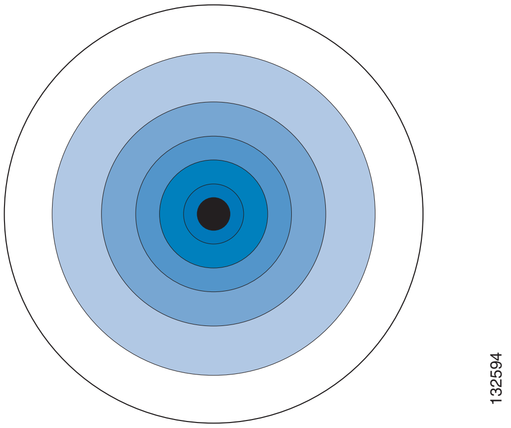
Types of Antennas

There are two basic antennas: omnidirectional and directional.

Omnidirectional Antenna

An omnidirectional antenna is designed to provide a 360-degree radiation pattern in the horizontal plane. This type of antenna is used when coverage in all directions from the antenna is required. The standard 2.2dBi "Rubber Duck" is one style of omnidirectional antenna.

Figure 3-4 Omnidirectional Antenna



Directional Antennas

Directional antennas come in many different styles and shapes. An antenna does not offer any added aggregate power to the signal; it simply concentrates the energy it receives from the transmitter in a particular direction. By redirecting this energy, it has the effect of providing more energy in one direction, and less energy in all other directions. As the gain of a directional antenna increases, the angle of radiation usually decreases, providing a greater coverage distance, but with a reduced coverage angle. Directional antennas include patch antennas (Figure 3-5), YAGI antennas (Figure 3-6), and parabolic dishes. Parabolic dishes have a very narrow RF energy path and the installer must be accurate in aiming these at each other.

Figure 3-5 Directional Patch Antenna

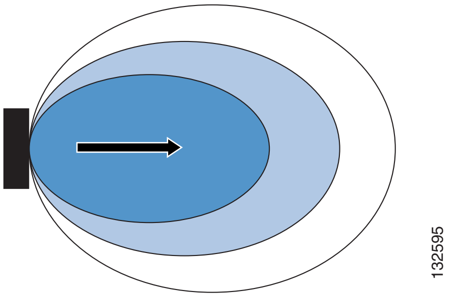
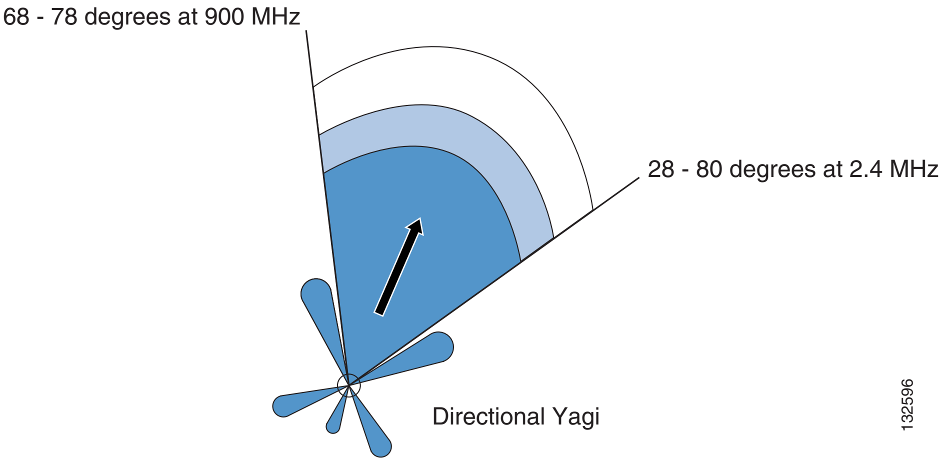


Figure 3-6 YAGI Antenna



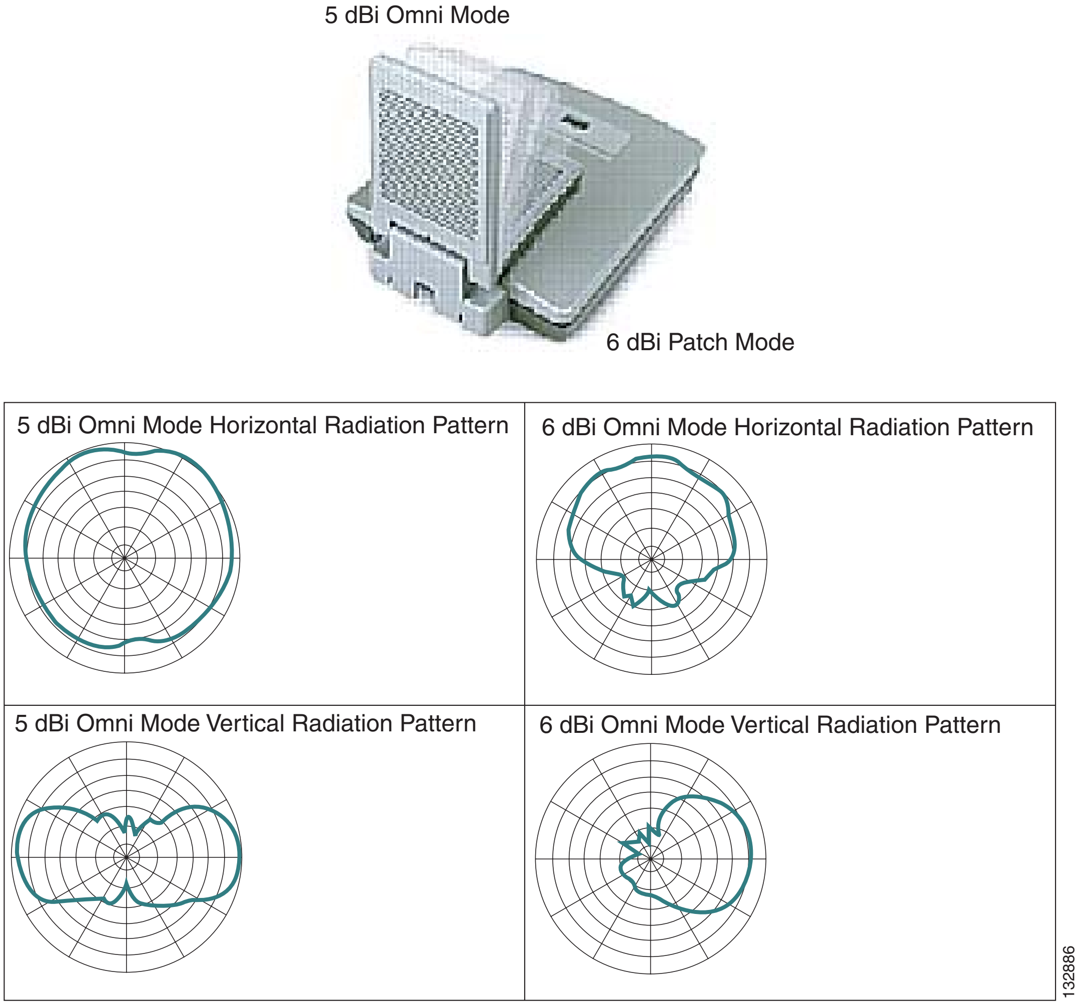
Diversity Antenna Systems

Multi-path interference occurs when an RF signal has more than one path between a receiver and a transmitter. This occurs in sites that have a large amount of metallic or other RF reflective surfaces. Just as light and sound bounce off of objects, so does RF. This means there can be more than one path that RF takes when going from a TX to and RX antenna, and these multiple paths result in different delays. These multiple signals combine in the receiver to cause distortion of the signal Diversity antenna systems are used to overcome multi-path fading. It uses two identical antennas, located a small distance apart, to provide coverage to the same physical area, and the AP chooses the antenna that provide the optimal signal to noise ratio.

Vertical Radiation Patterns of Antennas

Antennas radiated in both the horizontal direction and the vertical direction. The patterns of radiation antennas are typically diagramed by the manufacturer to assist with coverage and deployment. Figure 3-7 shows the coverage for a typical patch antenna. One of the considerations is floor to floor channel overlap and interference that will occur in normal deployments. By knowing the coverage pattern of an integrated antenna or by choosing an antenna with the appropriate coverage pattern the implementation of channel overlap and interference can be minimized.

Figure 3-7 Coverage for a Typical Patch Antenna



WLAN Technology Summary

Organizations must weigh each factor when selecting a wireless technology. In some cases, sheer performance and capacity favor the 802.11a standard implementation. In other cases, vendor support, range and implementation advantages lead to a selection of 802.11a802.11b/g technology. The decision depends on the organization’s type of activity, mission, and plans for the future while weighing cost and function requirements.

These competing wireless standards leave many companies wondering which wireless technology to embrace. The Cisco Aironet 1130/1200 Series and Cisco multi-band clients eliminate this concern. The dual-band design supports both established and emerging wireless standards, letting companies implement WLANs without compromise. With the Cisco Aironet 1130/1200 Series, organizations are assured that they will have the right technology both for today and far into the future.

Cisco WLAN RF Product Selection Considerations

The Cisco Aironet WLAN suite consists of a number of products designed for a variety of WLAN applications.

Note The Cisco Aironet WLAN portfolio is constantly changing. Please refer to the Cisco Product Catalog for up-to-date information.

Different products can be seen on Wireless Network Business Unit web site

http://www.cisco.com/en/US/products/hw/wireless/index.htmll

Access Points

An access point (AP) is typically the center point in a wireless network and the connection point between a wired and wireless network. Multiple APs can be placed throughout an area to provide freedom of movement to users equipped with WLAN client adapters.

Cisco provides access points with either single 802.11g radios for up to 54 Mbps of capacity or dual radio access points supporting both 802.11g and 802.11a for up to 108 Mbps of combined data rate. The Cisco Aironet line includes access points designed for offices and similar facilities, challenging RF environments like factories and warehouses, and the outdoors. These devices can be installed on desktops, on walls, on ceilings, above ceilings, and on top of poles.

Table 3-5 Cisco Aironet Support for 802.11a/b/g

Cisco Aironet Series	802.11b	802.11g	802.11a
1100 Series	Yes	Yes	No
1130AG Series	Yes	Yes	Yes
1200 Series	Yes	Yes	Optional*
1230AG Series	Yes	Yes	Yes
1300 Series	Yes	Yes	No

* With a hardware upgrade module, the Cisco Aironet 1200 Series access point may be field-upgraded to support 802.11a.

Cisco Aironet Series APs offer state of the art features which are very convenient in different deployment scenarios.

Table 3-6 summarizes the current Cisco family of APs.

Table 3-6 Access Points for Offices and Similar Environments

Product	Features/Benefits
Access Points for Offices and Similar Environments	
Cisco Aironet 1130AG Series Access Point Dual-band lightweight or autonomous access point with integrated antennas for easy deployment in offices and similar RF environments	• Two high-performance IEEE 802.11a and 802.11g radios offering 108 Mbps of capacity • 2.4 and 5 GHz integrated diversity omnidirectional antennas for easy deployment without external antennas • Available in either a lightweight version, or an autonomous version that may be field-upgraded to lightweight operation • Low-profile plastic case • 32 MB of memory with 16 MB of storage • Operating temperature range of 32 to 104°F (0 to 40°C) • Inline power support (Cisco pre-standard and 802.3af) • Console port for management • Support for WPA and 802.11i/WPA2 • Integrated and secure mounting system • UL2043-rated for placement in plenum areas
Cisco Aironet 1100 Series Access Point Single-band autonomous access point with integrated antennas for easy deployment in offices and similar environments	• Single 802.11g radio offering 54 Mbps of capacity • 2.4 GHz integrated diversity dipole antennas • Available in an autonomous version only • 16 MB of memory with 8 MB of storage • Operating temperature range of 32 to 104°F (0 to 40°C) • Inline power support (Cisco pre-standard) • Support for WPA and 802.11i/WPA2 • Integrated and secure mounting system • UL2043-rated for placement in plenum areas

Table 3-6 Access Points for Offices and Similar Environments (continued)

Cisco Aironet 1000 Series Lightweight Access Point Model 1010 Dual-band lightweight access point with integrated antennas for easy deployment in offices and similar RF environments	• Two IEEE 802.11a and 802.11g radios offering 108 Mbps of capacity • 2.4 and 5 GHz integrated antennas for easy deployment without external antennas • Available in a lightweight version only • 16 MB of memory with 8 MB of storage • Plastic case • Operating temperature range of 32 to 104°F (0 to 40°C) • Inline power support (802.3af) • Support for WPA and 802.11i/WPA2 • UL2043-rated for placement in plenum areas
Access Points for Challenging Indoor RF Environments	
Cisco Aironet 1240AG Series Access Point Second-generation dual-band lightweight or autonomous access point with dual diversity antenna connectors for challenging RF environments	• Two high-performance IEEE 802.11a and 802.11g radios offering 108 Mbps of capacity • 2.4 and 5 GHz dual-diversity RP-TNC connectors for external antenna support • Available in either a lightweight version, or an autonomous version that may be field-upgraded to lightweight operation • Rugged metal case • 32 MB of memory with 16 MB of storage • Operating temperature range of -4 to 131°F (-20 to 55°C) • Inline power support (Cisco pre-standard and 802.3af) • Console port for management • Support for WPA and 802.11i/WPA2 • Complete with integrated and secure mounting system • UL2043-rated for placement in plenum areas

Table 3-6 Access Points for Offices and Similar Environments (continued)

Cisco Aironet 1230AG Series Access Point First-generation dual-band lightweight or autonomous access point with dual-diversity antenna connectors for challenging RF environments	• Two high-performance IEEE 802.11a and 802.11g radios offering 108 Mbps of capacity • 2.4 and 5 GHz dual-diversity RP-TNC connectors for external antenna support • Available in either a lightweight version, or an autonomous version that may be field-upgraded to lightweight operation • Rugged metal case • 16 MB of memory with 8 MB of storage • Operating temperature range of -4 to 131°F (-20 to 55°C) • Inline power support (Cisco pre-standard) • Console port for management • Support for WPA and 802.11i/WPA2 • Complete with integrated and secure mounting system • UL2043-rated for placement in plenum areas
Cisco Aironet 1200 Series Access Point Single band lightweight or autonomous access point with dual diversity antenna connectors for challenging RF environments.	• Single high performance 802.11g radio offering 54 Mbps of capacity • Field-upgradable to support 802.11a with a hardware upgrade module • 2.4 GHz dual-diversity RP-TNC connectors for external antenna support • Available in either a lightweight version, or an autonomous version that may be field-upgraded to lightweight operation • Rugged metal case • 16 MB of memory with 8 MB of storage • Operating temperature range of -4 to 131°F (-20 to 55°C) • Inline power support (Cisco pre-standard) • Console port for management • Support for WPA and 802.11i/WPA2 • Complete with integrated and secure mounting system • UL2043-rated for placement in plenum areas

Table 3-6 Access Points for Offices and Similar Environments (continued)

Cisco Aironet 1000 Series Lightweight Access Point Model 1020 Dual-band lightweight access point with antenna connectors for challenging RF environments	• Two IEEE 802.11a and 802.11g radios offering 108 Mbps of capacity • 2.4 GHz dual-diversity RP-TNC connectors for external antenna support • 5 GHz non-diversity RP-TNC connector for external antenna support • Available in a lightweight version only • Metal and plastic case • 16 MB of memory with 8 MB of storage • Operating temperature range of 32 to 104°F (0 to 40°C) • Inline power support (802.3af) • Support for WPA and 802.11i/WPA2 • UL2043-rated for placement in plenum areas
Cisco Aironet 1300 Series Outdoor Access Point/Bridge Single-band autonomous access point and wireless bridge with a NEMA-4 compliant case for mounting in outdoor areas	• Single 802.11g radio offering 54 Mbps of capacity • 2.4 GHz dual-diversity RP-TNC connectors for external antenna support • Configurable as an autonomous access point, wireless bridge, or as a workgroup bridge • Support for both point-to-point and point-to-multipoint configurations • Weather resistant NEMA-4 compliant case • Integrated or optional external antennas for flexibility in deployment • 16 MB of memory with 8 MB of storage • Operating temperature range of -22 to 131ºF (-30 to 55ºC) • Inline power support (Cisco pre-standard) • Console port for management • Support for WPA and 802.11i/WPA2 • Complete with Integrated and secure mounting system • UL2043-rated for placement in plenum areas • Integrated or optional external antennas for flexibility in deployment

Note Please see the associated data sheets at http://www.cisco.com for specific product information.

WLAN Client Adapters

Client adapters connect to a variety of devices in a WLAN. Cisco Aironet Wireless LAN Client Adapters connect desktop and mobile computing devices to the wireless LAN in 802.11a, 802.11b or 802.11g-compliant networks.

802.11a Cardbus Client Card

The Cisco Aironet 5 GHz 54 Mbps WLAN client adapter is an IEEE 802.11a-compliant CardBus adapter that operates in the UNII-1 and UNII-2 bands. The integrated 5 dBi gain patch antenna optimizes range.

Enhanced Client Network Management Features with Extended Client Support

The Cisco Aironet 350 Series and 5 GHz 54 Mbps client adapters include the Cisco Aironet Client Utility (ACU), a tool with a graphical user interface for configuring, monitoring, and managing an adapter. The ACU includes site survey tools that produce detailed graphical information, including signal strength, to assist in the correct placement of APs. The ACU provides improved, quantifiable data, including signal-to-noise ratio measured in decibels (dB), and signal level and noise level measured in decibels per milli-watt (dBm). Using the ACU, a user can create a profile of settings for each environment, such as the office or home, making it simple for telecommuters and business travelers to reconfigure the adapter when moving from one environment to another. A user can now configure channel selection, service set identifier (SSID), WEP key, and authentication method for these different locations.

802.11 a/b/g Cardbus Client Card and 802.11 a/b/g PCI Client Card

Both the Cisco Aironet IEEE 802.11a/b/g Wireless CardBus Adapter and the Cisco Aironet IEEE 802.11a/b/g PCI adapters provide 54 Mbps connectivity in the 2.4 and 5 GHz bands. Both adapters can be configured to support single 802.11b coverage, single 802.11g coverage, single 802.11a coverage, dual- mode 802.11a/g coverage or tri-mode 802.11a/b/g coverage. The Cisco Aironet IEEE 802.11a/b/g Wireless CardBus Adapter is suited for use within notebooks and portable devices and has an integrated diversity dual-band 2.4/5 GHz antenna. The Cisco Aironet IEEE 802.11a/b/g PCI adapters provide a low-profile form factor and two-meter cable length for installation in low-profile devices, such as slim desktops and point-of-sale (POS) devices. For versatility, both a low profile and a standard profile bracket frame are included with the adapter. The attached dual-band 2.4/5 GHz 1 dBi effective gain antenna has a 2-meter cable allowing for maximum performance placement.

Both adapters provide superior range and throughput, secure network communications with support for WPA, comprehensive utilities for flexible configuration and management and support for World mode for international roaming.

Enhanced Client Network Management Features with Extended Client Support

Similar in nature to ACU, which is used for Cisco Aironet 350 Series and 5 GHz 54 Mbps client adapters, the 802.11a/b/g client adapters use a utility named Aironet Desktop Utility (ADU). A change in design allows 802.11a/b/g Wireless LAN Client Adapters not to utilize external firmware, rather it is loaded directly through the drivers. The Aironet Configuration and Administration tool (ACAT) which is used on the 350 Series and 5 GHz 54 Mbps client adapters has been renamed Aironet Configuration and Administration Utility (ACAU) for the 802.11a/b/g Wireless LAN Client Adapters. These two utilities are used by an administrator to deploy drivers, utilities, and profiles across the network to large number of end users. Table 8 compares the two utilities naming conventions:

Table 3-7 ACU/DCU Naming

	350 Series and 5 Ghz Client Adapters	802.11a/b/g Client Adapters
Client Utilities	Aironet Client Utility (ACU)	Aironet Desktop Utility (ADU)
Administrative Tool	Aironet Configuration and Administration Tool (ACAT)	Aironet Configuration and Administration Utility (ACAU)
System Tray Icon	Aironet Client Monitor (ACM)	Aironet System Tray Utility (ASTU)

Cisco Compatible Extension Program

The Cisco Compatible Extensions (CCX) program for WLAN clients helps to proliferate WLAN innovations and standards to many different suppliers of mobile computing devices. CCX provide wireless users with a baseline of compatibility for standards, security, VLANs, QoS, performance and management.

Table 3-8 describes the features of the various versions of the CCX program.

Table 3-8 CCX Program Versions

	Version 1.0	Version 2.0	Version 3.0
Standards	• Wired Equivalent Privacy (WEP) • IEEE 802.11 and 802.1x • Wi-Fi compliance • Windows Hardware Quality Labs (WHQL)	• WPA compliance	• WHQL or Wi-Fi (Windows) • WPA and WPA2 advanced encryption
Security	• LEAP • Cisco pre-standard Temporal Key Integrity Protocol (TKIP)	• Protected EAP with Generic Token Card support (PEAP-GTC) • Standard (WPA) TKIP with LEAP and PEAP-GTC	• CCKM with EAP-FAST (migration path for LEAP users) • AES provides 256-bit encryption based on 802.11 TGi

Table 3-8 CCX Program Versions (continued)

	Version 1.0	Version 2.0	Version 3.0
VLANs and QoS	• Inter-operability with access points that support multiple SSIDs and VLANs	• Pre-standard enhanced Distributed Coordination Function (eDCF)	• WME provides standards based QoS based on 802.11 TGi • WiFi QoS WMM (Wi-Fi Multimedia)
Performance and Management		• Access point assisted roaming • Fast 802.1x re-authentication • Radio environment reporting • Access point specified maximum transmit power • Cisco compatible version control	• Cisco compatible version control • Single Sign-on • Proxy ARP

For more information:
http://www.cisco.com/en/US/products/hw/wireless/ps4555/products_data_sheets_list.html

Wireless Phones

The Cisco Wireless IP Phone 7920 is an IEEE 802.11b wireless IP phone that provides comprehensive voice communications in conjunction with Cisco CallManager and Cisco Aironet 1200, 1100, of Wi-Fi (IEEE 802.11b) access points. As a key component of the Cisco IP Communications System Wireless Solution, the Cisco Wireless IP Phone 7920 delivers seamless intelligent services such as security, mobility, quality of service (QoS), and management, across an end-to-end Cisco network.

For more information on the IP Communications portfolio please visit: http://www.cisco.com/go/ipc.

Workgroup Bridges

Workgroup bridges provide wired network connectivity to workgroups through a wireless network connection to an AP site. Cisco 1100 and 1200 series APs can be configured to operate as a workgroup bridge.

The workgroup bridge can be a wireless peer with either an AP or a Cisco wireless bridge. The workgroup bridge to wireless bridge configuration is applicable to outdoor point-to-point campus connections. The workgroup bridge to AP configuration is applicable to shorter range, multi-access solutions where the AP may peer with other workgroup bridges and client adapters.

The various applications of workgroup bridges are illustrated in Figure 3-8 and Figure 3-9.

Figure 3-8 Mobile Ethernet Enabled User

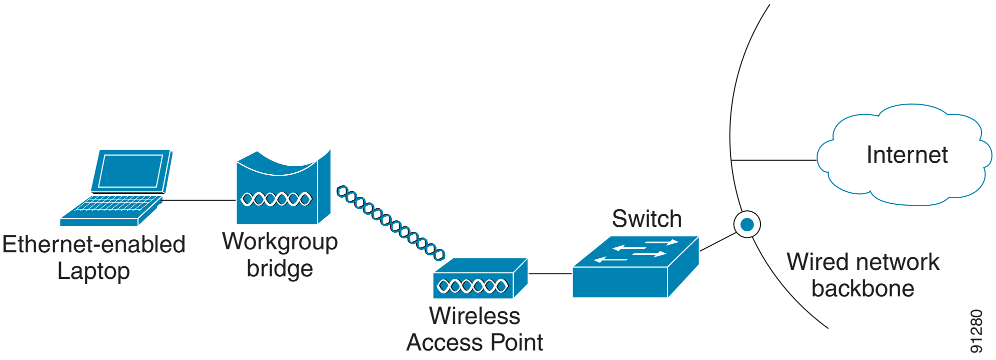
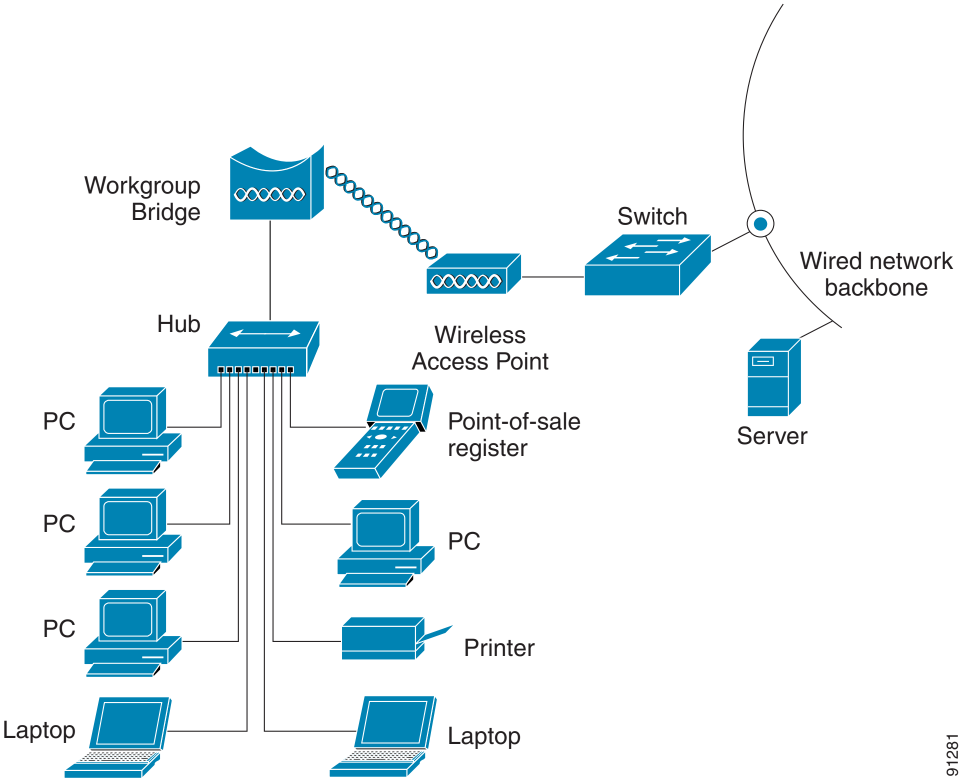


Figure 3-9 Remote Workgroup

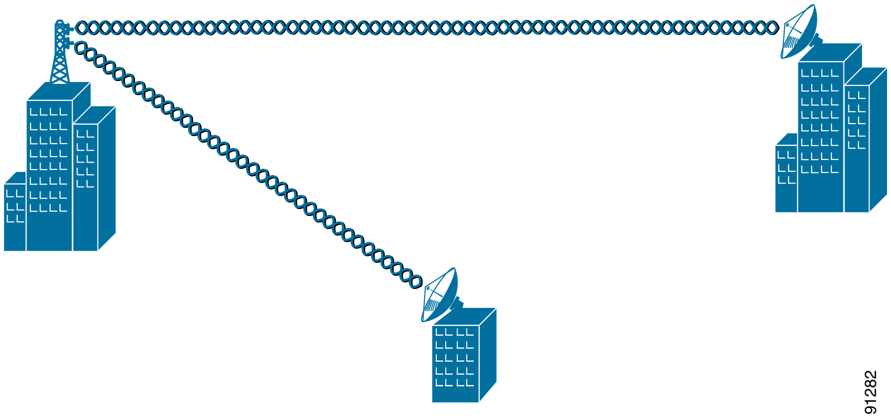


Wireless Bridges

Wireless bridges (or simply *bridges*) are used for wireless connection between two networks, usually in different buildings. With appropriate selection of antennas and clear line of sight, range can extend up to 25 miles at 11 Mbps. It should be noted that only bridges have this extended range capability. The extended range is achieved by operating outside the IEEE 802.11 timing specifications. APs conforming to 802.11b, connected to any client are limited to a one-mile range; irrespective of transmit power, cable, and antenna combinations.

Cisco Aironet Bridges support a superset of AP functionality and can operate in either bridge or AP mode depending upon the requirement.

Figure 3-10 Typical Bridge Application Connecting Buildings Across a Campus or Metro Area



Note APs cannot be used to *bridge* two wired networks.

Cisco Unified Wireless Network

The Cisco Unified Wireless Network provides the framework to integrate and extend wired and wireless networks to deliver the lowest possible total cost of ownership for companies deploying wireless LANs (WLANs). Cisco Unified Wireless Network extends “wireless awareness” into important elements of the network infrastructure, providing the same level of security, scalability, reliability, ease of deployment, and management for wireless LANs that organizations have come to expect from their wired LANs.

This section provides a brief technical synopsis of a Cisco WLAN framework using autonomous access points.

For a detailed review of the Cisco Unified Wireless Network, refer to the brochure at the following URL: http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns337/netbr09186a0080184925.html.

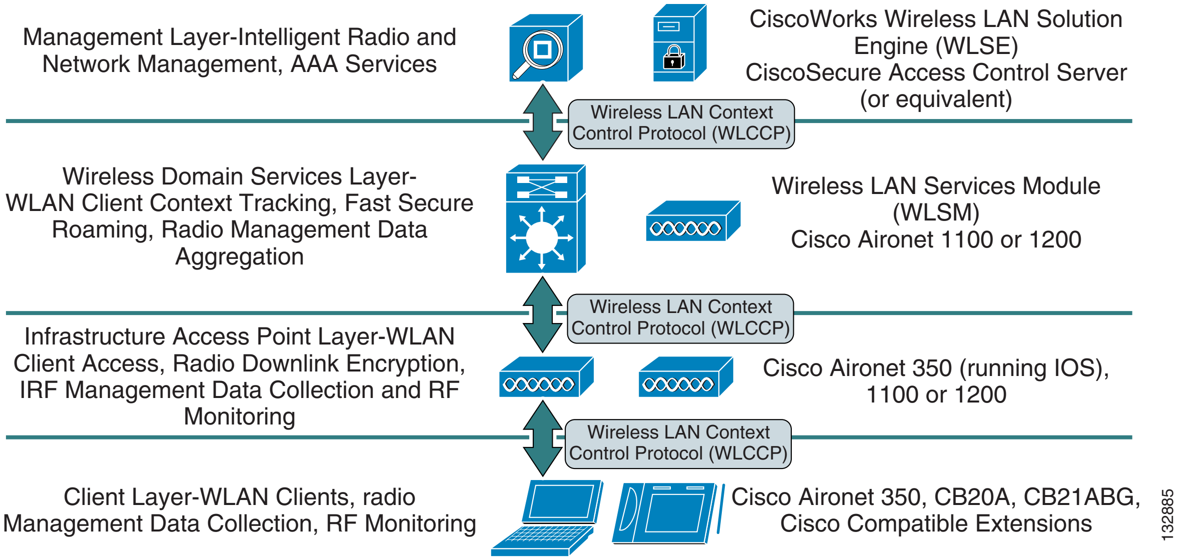
The framework addresses two key issues with managing and operating WLANs: fast secure WLAN client roaming and radio management. Fast secure roaming allows WLAN clients to move association from one access point to another with little or no service disruption. Radio management characterizes the radio transmission environment and responds to the conditions of the environment.

The framework can be visualized as a layered model. The layers are:

- Management Layer
- Wireless Domain Services Layer
- Infrastructure Access Point Layer
- Wireless Client Layer

The framework introduces WLCCP to facilitate control messaging between the framework components. Figure 3-11 illustrates the conceptual model of the framework, including the WLCCP messaging protocol. As shown in Figure 3-11, each layer is implemented in specific Cisco products.

Figure 3-11 Cisco WLAN solution Layers


Management Layer-Intelligent Radio and Network Management, AAA Services
CiscoWorks Wireless LAN Solution Engine (WLSE)
CiscoSecure Access Control Server (or equivalent)
Wireless LAN Context Control Protocol (WLCCP)
Wireless Domain Services Layer-WLAN Client Context Tracking, Fast Secure Roaming, Radio Management Data Aggregation
Wireless LAN Services Module (WLSM)
Cisco Aironet 1100 or 1200
Wireless LAN Context Control Protocol (WLCCP)
Infrastructure Access Point Layer-WLAN Client Access, Radio Downlink Encryption, IRF Management Data Collection and RF Monitoring
Cisco Aironet 350 (running IOS), 1100 or 1200
Wireless LAN Context Control Protocol (WLCCP)
Client Layer-WLAN Clients, radio Management Data Collection, RF Monitoring
Cisco Aironet 350, CB20A, CB21ABG, Cisco Compatible Extensions
132885

The management layer supplies the processing of RM data from the lower layers, controlling and managing the radio coverage environment. This data is also used for securing the radio coverage environment by detecting rogue access points and wireless clients. Authentication, Authorization, and Accounting (AAA) services are also placed in the management layer.

The required management layer component is the CiscoWorks WLSE. An optional component is the CiscoSecure ACS. Other products with functionality equivalent to ACS may be used in the Cisco Unified Wireless Network.

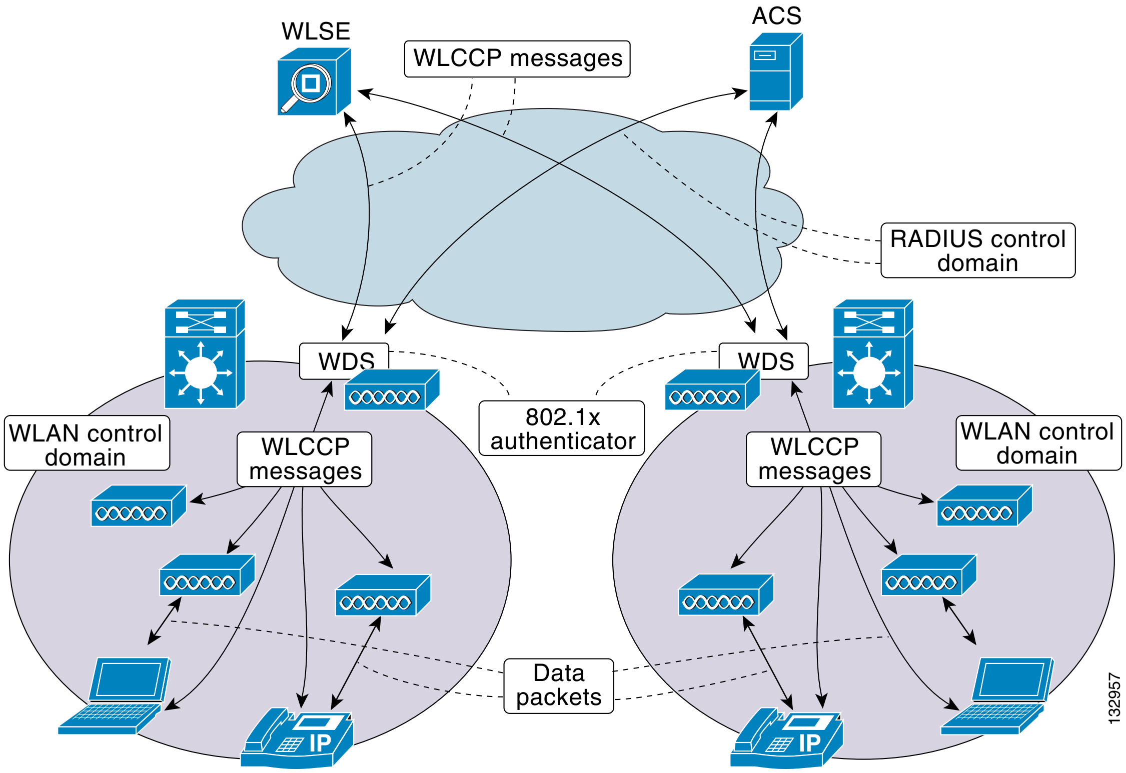
The WDS layer provides critical services: WLAN client context awareness, fast secure roaming, and aggregation of radio management data from the infrastructure access point and client layer. WDS is implemented in supporting versions of Cisco IOS for the Cisco Aironet 1100 and 1200 series access points and on the special Cisco IOS running on the wireless LAN service module for the Catalyst 6500 switch platform. The solution architecture dictates whether to use the WDS access point or the WLSM implementation.

The infrastructure access point layer facilitates WLAN client access to the wired-network, radio downlink encryption, and radio management data collection, including on-going radio monitoring.

The client layer includes all wireless clients. Advanced framework features take advantage of client-side capabilities to allow for radio measurement collection from the WLAN clients and fast secure roaming.

Figure 3-12 represents a logical, hierarchical view of the framework that clearly illustrates the importance of the WDS layer.

Figure 3-12 Cisco Unified Wireless Network Logical View



WDS are configured to run on a supporting device—either a Cisco Aironet 1100 or 1200 for a Layer 2 architectural solution or the WLSM for an switch-based, Layer 3 solution. In both cases, infrastructure access points register with the WDS using special WLCCP messages.

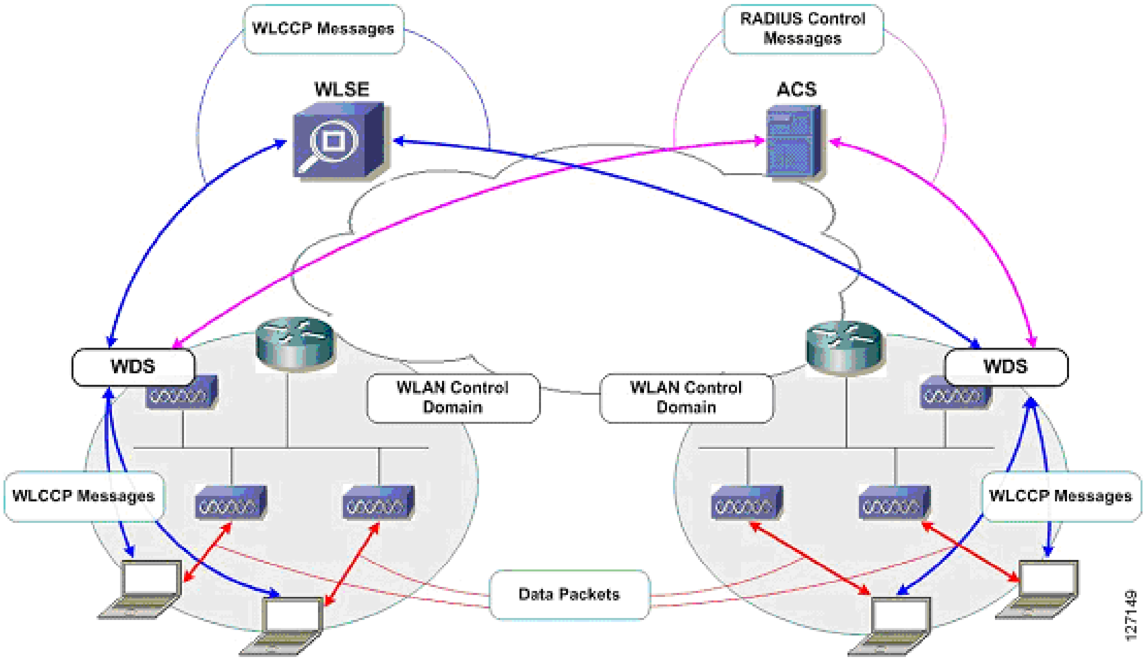
Once registered, the infrastructure access points forward client association, authentication, and roaming information through the WDS via WLCCP MN registration messages, allowing the WDS to control and track wireless clients. If client authentication is implemented via any 802.1x with EAP (such as Cisco LEAP, EAP-FAST, PEAP, EAP-TLS, or EAP-TTLS), the WDS performs an additional important role by acting as the 802.1x authenticator for all wireless clients. In 802.1x authentication transactions, the WDS communicates directly with the RADIUS server. Any valid wireless client associated with an infrastructure access point and registered with the WDS.

A WDS, its registered infrastructure access points, and registered clients make up a WLAN control domain. Wireless clients can seamlessly roam between access points within a WLAN control domain. A WDS also collects radio management data from the infrastructure access points and, potentially, the MNs within the WLAN control domain via special WLCCP radio management (WLCCP-RM) messages. This data is aggregated by the WDS and passed on to the WLSE in WLCCP-RM messages. The WLSE uses this RM data to control and manage the radio coverage environment and to detect rogue access points and clients.

The core feature set of the Cisco Unified Wireless Network offers two basic WLAN architectures: an architecture supporting a Layer 2 WLAN control domain and an architecture supporting a Layer 3 WLAN control domain. The Layer 2 architecture leverages autonomous access point-based WDS. This architecture is called the access point-based WDS solution. The Layer 3 architecture leverages WLSM-based WDS and is called the switch-based WDS solution.

Figure 3-13 shows the autonomous access point-based WDS solution.

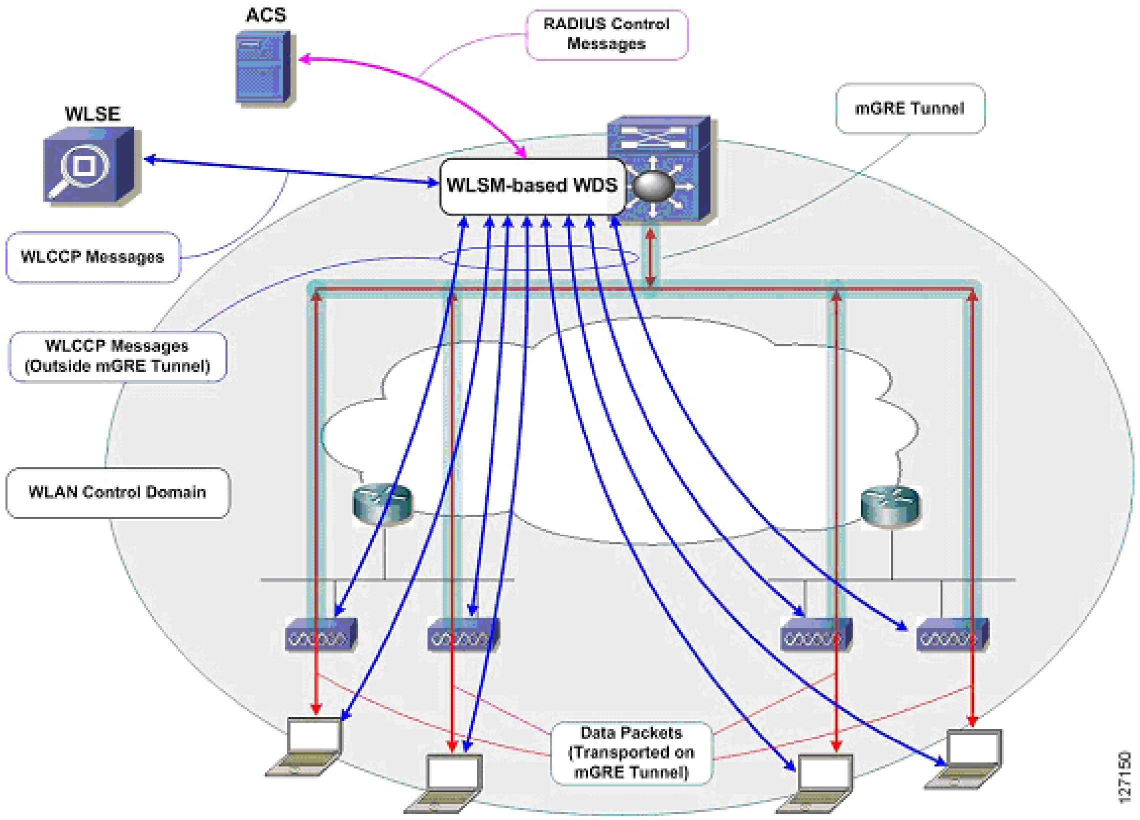
Figure 3-13 Access Point-Based WDS Solution



In the access point-based WDS solution, infrastructure access points discover the WDS via special WLCCP multicast messages. You must have an access point running WDS on each Layer 2 subnet. The solution supports up to 30 infrastructure access points when the WDS-host access point is also serving wireless clients and up to 60 infrastructure access points when the WDS-host access point is not serving wireless clients. The access point-based WDS solution facilitates seamless MN roaming across a Layer 2 WLAN control context.

Figure 3-14 shows the switch-based WDS solution.

Figure 3-14 Switch-Based WDS Solution



In the switch-based WDS solution, mGRE tunnels are built from the Catalyst 6500 switch hosting the WLSM where the WDS is running. Wireless client data is tunneled to the Catalyst 6500 switch where it is forwarded appropriately. The mGRE tunnel legs are built when the infrastructure access points register with the WDS on the WLSM. Wireless client authentication and MN registration WLCCP messages are forwarded to the WLSM for centralized processing. Unlike wireless client data traffic, WLCCP messages are not forwarded on the mGRE tunnel legs. Rather, these messages traverse the network like standard IP packets. The switch-based WDS architecture offers complete control and data plane separation, which are essential elements to true network scalability. The switch-based WDS solution facilitates seamless roaming across a Layer 3 WLAN control context and supports up to 300 registered infrastructure access points and 6000 MNs per WLSM.

CHAPTER 4

WLAN Security Considerations

As network administrators begin to deploy WLANs, they are faced with the challenge of trying to secure these environments while providing maximum flexibility for their users.

WLAN Security Implementation Criteria

For the Wireless network, security is built upon both authentication and encryption. Security mechanisms for wireless networks are:

- Open Authentication, no WEP
- Wired Equivalent Privacy (WEP)
- Cisco WEP Extensions (CKIP +CMIC)
- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access 2 (WPA 2)

The Wi-Fi Alliance is the global Wi-Fi organization that created the Wi-Fi brand. The Alliance certifies inter-operability of IEEE 802.11 products and promotes them as the global, wireless LAN standard across all market segments. The Wi-Fi Alliance has instituted a test suite that defines how member products are tested to certify that they are interoperable with other Wi-Fi Certified products.

The original 802.11 security mechanism, Wired Equivalent Privacy (WEP), was the mechanism for securing wireless networks. Although applying some level of security, WEP is viewed as insufficient for securing business communications. The WEP standard in 802.11 did not address the issue of how to manage encryption keys. The encryption mechanism itself was found to be flawed and the WEP key could be derived from monitoring client traffic. The Cisco Aironet solution addressed these issues by introducing 802.1x authentication and dynamic key generation and by introducing enhancements to WEP encryption, CKIP, and CMIC. 802.11i is the standard introduced by the IEEE to address the security shortcomings of the original 802.11 standard. The time between the original 802.11 standard and the ratification of 802.11i saw the introduction of interim solutions.

Wi-Fi Protected Access (WPA) is an 802.11i based security solution from the Wi-Fi Alliance that addresses the vulnerabilities of WEP. WPA uses Temporal Key Integrity Protocol (TKIP) for encryption and dynamic encryption key generation through either a pre-shared key, or 802.1x authentication. WPA was introduced prior to the ratification of the 802.11i standard to address the weaknesses in WEP. The mechanisms introduced into WPA were designed to address the weakness of the WEP solution without requiring hardware upgrades.

WPA2 is the next generation of Wi-Fi security and is also based upon the 802.11i standard. It is the approved Wi-Fi Alliance interoperable implementation of the ratified IEEE 802.11i standard. WPA 2 offers two classes of certification: Enterprise and Personal. Enterprise requires support for

Radius/802.1x-based authentication and Pre-Shared Key and Personal only requires a common key shared by the client and the AP. The encryption mechanism introduced in WPA2 generally require a hardware upgrade from earlier versions of WLAN clients and APs.

Table 4-1 summarizes the various specifications.

Table 4-1 Wi-Fi Security Comparison

Feature	Static WEP	802.1x WEP	WPA	WPA 2 (Enterprise)
Identity	User and/or machine or WLAN card	User and/or machine	User and/or machine	User and/or machine
Authentication	Shared key	EAP	EAP or pre-shared keys	EAP or pre-shared keys
Integrity	32-bit Integrity Check Value (ICV)	32-bit ICV	64-bit Message Integrity Code (MIC)	CRT/CBC-MAC (Counter mode Cipher Block Chaining Auth Code - CCM)
Encryption	Static Keys	Session Keys	Per Packet Key rotation via TKIP	CCMP (AES)
Key Distribution	One time, Manual	Segment of PMK	Derived from PMK	Derived from PMK
Initialization Vector	Plain text, 24-bits	Plain text, 24-bits	Extended IV-65-bits with selection/sequencing	48-bit Packet Number (PN)
Algorithm	RC4	RC4	RC4	AES
Key Strength	64/128-bit	64/128-bit	128-bit	128-bit
Supporting Infrastructure	None	RADIUS	RADIUS	RADIUS

Cisco Wireless Security Suite provides the user with the options to provide varying security approaches based on the required or pre-existing authentication, privacy and client infrastructure. Cisco Wireless Security Suite supports WPA and WPA2, including:

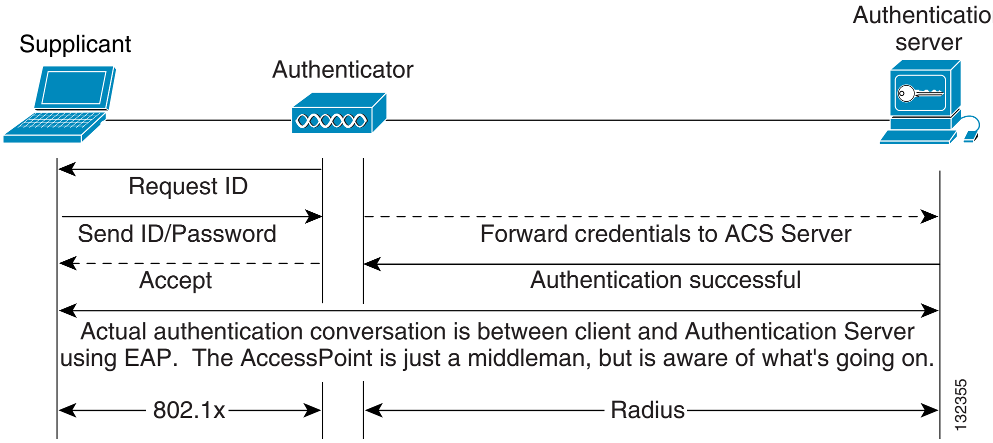
- Authentication providing 802.1X support, including:
  - Cisco LEAP, EAP-Flexible Authentication via Secure Tunneling (EAP-FAST)
  - PEAP- Generic Token Card (PEAP-GTC)
  - PEAP-Microsoft Challenge Authentication Protocol Version 2 (PEAP-MSCHAPv2)
  - EAP-Transport Layer Security (EAP-TLS)
  - EAP-Subscriber Identity Module (EAP-SIM)
- Encryption:
  - AES-CCMP encryption (WPA2)
  - TKIP encryption enhancements: key hashing (per-packet keying), message integrity check (MIC) and broadcast key rotation via WPA TKIP Cisco Key Integrity Protocol (CKIP) and Cisco Message Integrity Check (CMIC)
  - Support for static and dynamic IEEE 802.11 WEP keys of 40 bits and 128 bits

With the Cisco Wireless Security Suite, both Cisco KIP and WPA TKIP algorithms are available on Cisco Aironet access points and Cisco Aironet and Cisco Compatible WLAN client devices. Although Cisco KIP and WPA TKIP do not inter-operate, Cisco Aironet Series access points can run both Cisco KIP and WPA TKIP simultaneously when using multiple VLANs or Mobility groups.When choosing a security mechanism, Cisco recommends the strongest security suite available, whether its WEP, WPA, WPA2 or CKIP/CMIC entirely or in combination, depending upon the client capabilities.

802.1x/EAP Authentication

802.11i specifies the use of 802.1x providing port access on wireless network ports. It uses Extensible Authentication Protocol (EAP) to exchange authentication information. EAP payloads are placed within 802.1x Frames or RADIUS Packets. Access to the network is determined by the success or failure of the EAP authentication. Figure 4-1 diagrams the general authentication flow.

Figure 4-1 Generic EAP over 802.1x Authentication Mode


Supplicant
Authenticator
Authentication server
Request ID
Send ID/Password
Accept
Forward credentials to ACS Server
Authentication successful
Actual authentication conversation is between client and Authentication Server using EAP. The AccessPoint is just a middleman, but is aware of what's going on.
802.1x
Radius
132355

There are a number of different EAP types used in WLAN solutions. Some common EAP types are:

- EAP TLS (Transport Layer Security—very similar to SSL)
- Cisco's Lightweight Extensible Authentication Protocol (LEAP)
- Protected Extensible Authentication Protocol (PEAP)
- Flexible Authentication via Secured Tunnel (FAST)

These EAP types define how the authentication messaging takes place between the client and the authentication server. The Supplicant and the Authentication Server must support the same EAP types. Since the EAP payloads are passed across the Authenticator without being parsed, the Authenticator need not care about the EAP authentication type. EAP payload data of interest to the Authenticator would come from a successful authentication. Such data might include the VLAN ID to apply for the client, ACLs, or controlling QoS parameters.

Table 4-2 provides a brief comparison of various EAP supplicants.

Table 4-2 Comparison of EAP supplicants (LEAP, EAP-FAST, PEAP, EAP-TLS)

	Cisco LEAP	Cisco EAP-FAST	PEAP/MS-CHAPv2	PEAP (EAP-GTC)	EAP-TLS
Single Sign-On (MSFT AD only)	Yes	Yes	Yes	Yes[1]	Yes
Login Scripts Execution (MSFT AD only)	Yes	Yes	Yes	Some	Yes[2]
Password Change (MSFT AD)	No	Yes	Yes	Yes	N/A
Cisco 350 and CB20A Client support for Windows XP, 2000, and Windows CE OS	Yes	Yes	Yes	Yes	Yes
PCI card Client support for Windows XP and Windows 2000	Yes	Yes	Yes	Yes	Yes
Microsoft AD DB support	Yes	Yes	Yes	Yes	Yes
ACS Local DB support	Yes	Yes	Yes	Yes	Yes
LDAP DB support	No	Yes[3]	No	Yes	Yes
OTP authentication support	No	No	No	Yes	No
RADIUS server certificate required?	No	No	Yes	Yes	Yes
Client certificate required?	No	No	No	No	Yes
Susceptible to Dictionary Attacks?	Yes[4]	No	No	No	No
Susceptible to MITM Attacks?	No	No[5]	Yes[6]	Yes[7]	No
Fast Secure Roaming (Cisco CCKM)	Yes	Yes	Yes[1]	Yes[1]	Yes[1]
Local Authentication	Yes	Yes	No	No	No
WPA Support (Windows 2K/XP)	Yes	Yes	Yes	Yes	Yes

[1] Supplicant Dependent

[2] Machine account on Windows AD is required to enable Login Script execution for PEAP and EAP-TLS

[3] Automatic provisioning is not supported for LDAP back-end DBs. Manual provisioning would have to be used for back-end LDAP DBs.

[4] Strong Password policy is required for LEAP deployment to mitigate risks due to offline (i.e. passive) dictionary attacks.

[5] EAP-FAST with automatic provisioning is susceptible to rogue server (reduced MITM) attack during the phase 0 (automatic provisioning stage).

[6] PEAP (specifically PEAPv1) is vulnerable to MITM attacks. This is discussed in http://www.ietf.org/internet-drafts/draft-puthenkulam-eap-binding-04.txt. This MITM vulnerability will be fixed in PEAPv2.

[7] Although Cisco PEAP, as a hybrid authentication type, is theoretically vulnerable to MITM attacks, the Cisco supplicant implementation of PEAPGTC is less vulnerable, as it does not accept the same authentication types inside and outside the TLS tunnel, a requirement for the MiTM exploit publicly detailed.

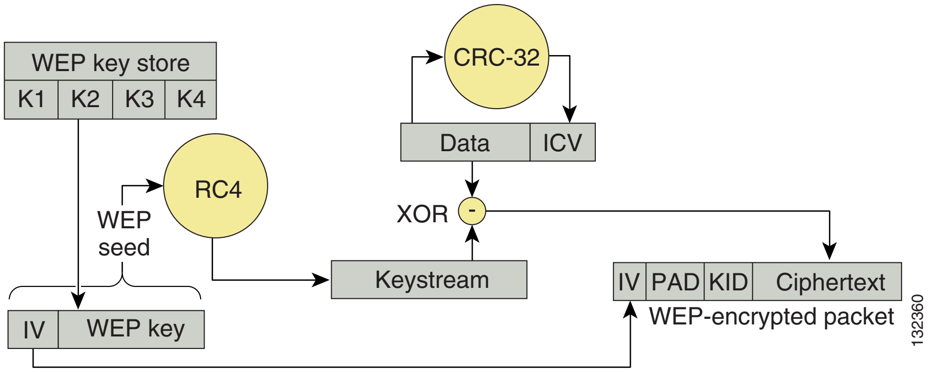
Encryption and Message Integrity

The information in this section is a brief discussion of encryption and message integrity mechanisms. The main goals for encryption and message integrity are preventing disclosure, and modifying and inserting packets in a WLAN. References for sources providing a detailed discussion and analysis of crypto-algorithms, key management and implementations are listed at the end of this section.

Wired Equivalent Privacy

Wired Equivalent Privacy (WEP) was the original encryption method defined in the 802.11 standard. WEP encryption is based on either a 40 or 104-bit key coupled with an initialization factor. WEP uses the RC4 algorithm to prevent disclosure of information. As previously mentioned, WEP was vulnerable to attack and is not recommended for enterprise deployments. Figure 4-2 illustrates the WEP encapsulation process.

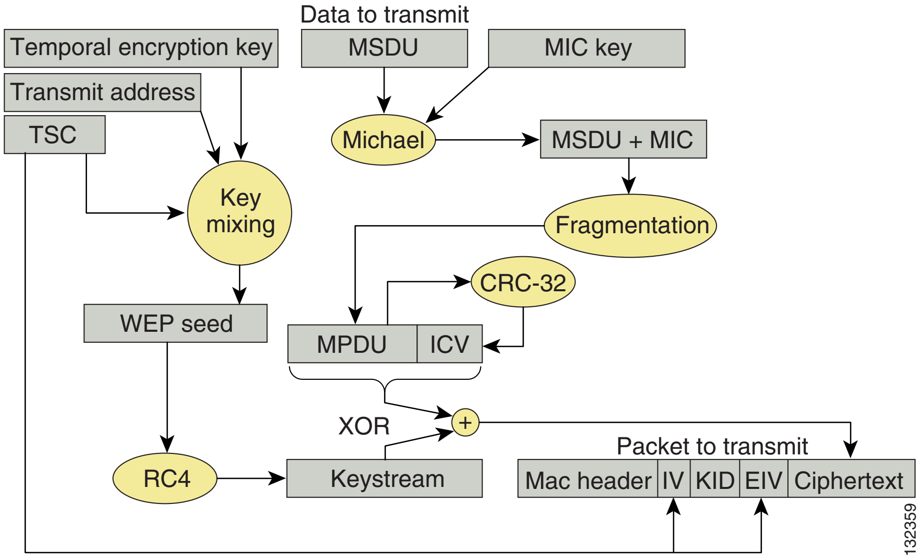
Figure 4-2 WEP Encapsulation Process



Temporal Key Integrity Protocol

With Temporal Key Integrity Protocol (TKIP) the main objective was to address the problems with WEP and to work with legacy hardware. TKIP is a cipher suite that includes key mixing algorithms and a packet counter to protect the keys. It also includes Michael Message Integrity Check (MIC) algorithm that, along with the packet counter, can prevent packet modification and insertion. Figure 4-3 illustrates the TKIP encapsulation process.

Figure 4-3 TKIP Encapsulation Process



Cisco Key Integrity Protocol and Cisco Message Integrity Check

Cisco Key Integrity Protocol (CKIP) and Cisco Message Integrity Check (CMIC) is Cisco's version of TKIP and MIC respectively. CKIP and CMIC were developed to address the WEP vulnerabilities prior to the release of WPA. Combined, CKIP and CMIC provide encryption and message integrity far superior to WEP. Cisco supports both the 802.11i standard as well as CKIP/CMIC.

Counter Mode/CBC-MAC Protocol

Counter Mode/CBC-MAC Protocol (CCMP) is an algorithm based on Advanced Encryption Standard (AES) and provides encryption and data integrity. and is part of the 802.11i spec. It has stronger encryption and message integrity than TKIP, but is not compatible with legacy wireless hardware. Figure 4-4 illustrates the CCMP encapsulation process.

Figure 4-4 CCMP Encapsulation Process

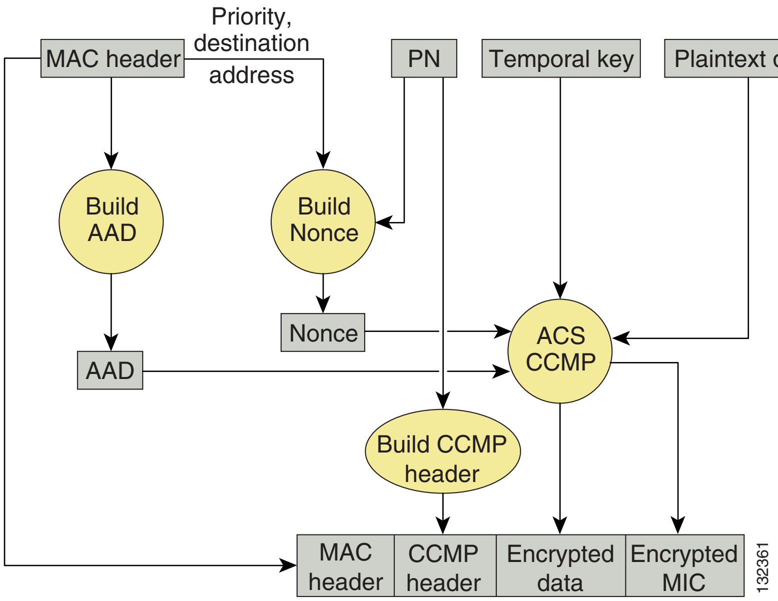
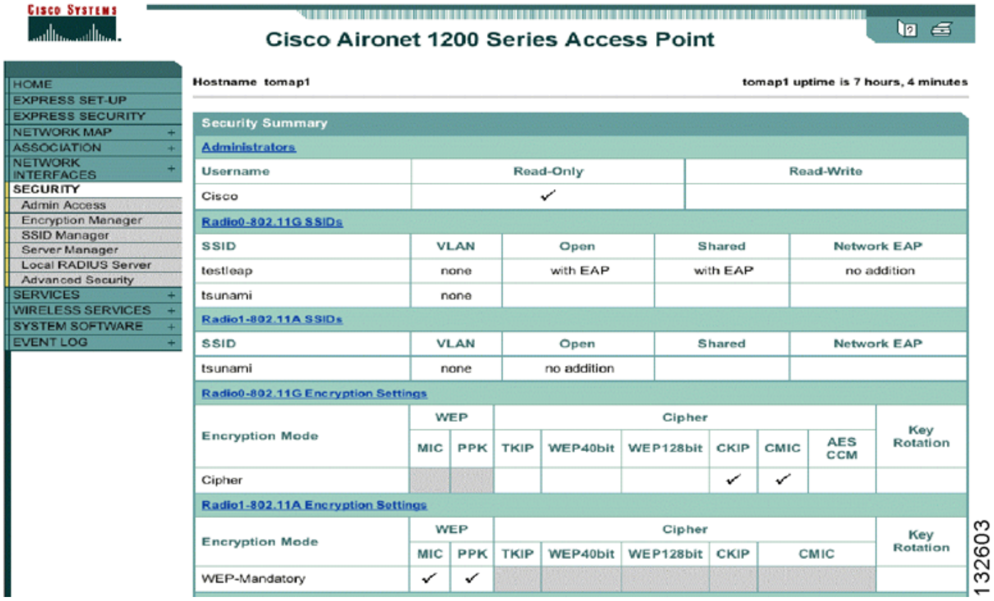


Figure 4-5 show the encryption configuration options available on a Cisco Access point.

Figure 4-5 Cisco Access Point Encryption Configuration Options



Cisco Aironet 1200 Series Access Point

Hostname tomap1 | tomap1 uptime is 7 hours, 4 minutes

Security Summary

Administrators

Username	Read-Only	Read-Write
Cisco	✓	

Radio0-802.11G SSIDs

SSID	VLAN	Open	Shared	Network EAP
testleap	none	with EAP	with EAP	no addition
tsunami	none			

Radio1-802.11A SSIDs

SSID	VLAN	Open	Shared	Network EAP
tsunami	none	no addition		

Radio0-802.11G Encryption Settings

Encryption Mode	WEP		Cipher						Key Rotation
	MIC	PPK	TKIP	WEP40bit	WEP128bit	CKIP	CMIC	AES CCM	
Cipher						✓	✓		

Radio1-802.11A Encryption Settings

Encryption Mode	WEP		Cipher					Key Rotation
	MIC	PPK	TKIP	WEP40bit	WEP128bit	CKIP	CMIC	
WEP-Mandatory	✓	✓						

There are many articles and books that describe security in detail. A few are listed here:

- *Cisco Wireless LAN Security,* by Sankar, Sundaralingam, Balinsky and Miller
- *802.11 Real Security,* by Edney and Arbaugh
- *802.11 Wireless Fundamentals,* by Roshan and Leary

WLAN Security Selection

In selecting and implementing the security standards for WLANs, there are many options. However, in most implementations, the decisions are bound by existing enterprise security practices and clients participating in the wireless LANs, When dealing with clients, you need to know what supplicants are available for those clients, and specifically what authentication/identity framework is used by the enterprise.

Given these options, the decision of what must be implemented can be varied and challenging. Cisco provides the ability to segment various security schemes via VLANs or Mobility groups, which will be discussed in the next chapter.

This section compares and summarizes the following security standards for WLANs:

- Table 4-3 comparing Cisco LEAP, PEAP, and EAP-TLS
- Table 4-4 listing the advantages of using 802.1x EAP for WLAN
- Table 4-5 comparing the advantages of Cisco TKIP with WPA TKIP
- Table 4-5 listing the advantages and disadvantages of using VPN for WLAN

Table 4-3 Comparing Cisco LEAP with PEAP and EAP-TLS

Cisco LEAP	• Supports many operating systems (Windows 95, 98, 2000, XP, Me, NT, Mac OS, Linux, DOS, Windows CE) • Supports many adapters and client devices, including devices with small processors • Supports a variety of wireless LAN devices like Cisco workgroup bridges, wireless bridges, and repeaters • Does not require certificates or a Certificate Authority • Can be configured quickly and easily • Supports a single sign-on with an existing user name and password • Has been field-proven since 2001 • Requires minimal client software overhead • Utilizes minimal authentication messaging • Known security exposure – requires strong passwords
EAP-FAST	• Tunnel establishment is based upon shared secret keys that are unique to users. (Protected Access Credentials (PACs) and may be distributed automatically (Automatic or In-band Provisioning) or manually (Manual or Out-of-band Provisioning) to client devices.) • Single sign-on (SSO) using the user name and password supplied for Windows networking logon • Wi-Fi Protected Access (WPA) support without third party supplicant (Windows 2000 and XP only) • Windows Password Aging (i.e. support for server-based password expiration) • Support for key Cisco Unified Wireless Network features: Fast Secure Roaming (CCKM) and Local • RADIUS Authentication • No reliance on Microsoft 802.1X framework • No certificates authority needed/ No requirement for certificates
PEAP-GTC	• Supports authentication using one-time passwords • Supports NDS and LDAP • Supports password change at expiration • Is defined in a draft RFC • Does not expose the logon user name in the EAP Identity Response • Is not vulnerable to a dictionary attack • Requires a server certificate and CA certificate, but does not require per-user certificates

Table 4-3 Comparing Cisco LEAP with PEAP and EAP-TLS (continued)

EAP-TLS	• Supported natively on Windows XP and Windows 2000 (with service pack) • Supports NDS and LDAP (when appropriately configured) • Uses same PKI mechanism as wired or dial-up access for easy distribution of client certificates • Official EAP type tested with Wi-Fi Protected Access (WPA)– although other EAP types will work with WPA • Exposes user information in the certificate
PEAP-MSCHAP	• Supports password change at expiration • Is defined in a draft RFC • Does not expose the logon user name in the EAP Identity Response • Is not vulnerable to a dictionary attack • Requires a server certificate and CA certificate, but does not require per-user certificates • The authentication protocol is protected by a TLS tunnel but the tunneled authentication protocol is limited to MSCHAPv2 • Supported natively on Windows XP and Windows 2000(with service packs), integrates into Active Directory user
PEAP-MSCHAPv2	•

Table 4-4 Advantages of using 802.1x EAP for WLAN

802.1 EAP Types versus VPNs	The advantages of using 802.1X EAP for WLAN are:· • Included with Wi-Fi certified clients and access points • Minimal client software overhead • Minimal authentication messaging overhead • Minimal management overhead • Natively supported on many operating systems • Layer 3 roaming support • Authentication choice for enterprise deployments

Table 4-5 Comparing the Advantages of Cisco TKIP with WPA TKIP

Cisco TKIP	WPA TKIP
Cisco TKIP is well suited to the following deployments: • Enhanced security is required but a WPA supplicant cannot be supported on the client platform • If 802.1q trunks are supported by the Layer 2 infrastructure and it's possible to use WLAN VLANs to segregate Cisco TKIP users from other WLAN users	WPA TKIP is well suited to the following deployments: • Client devices can support WPA • Cisco Compatible version 2 cards in use • If 802.1q trunks are not supported by the Layer 2 infrastructure WPA and non-WPA clients can operate on the same SSID, via WPA migration modeNative support for wireless devices and authentication protocol is desired (no external supplicant required)

Table 4-6 Advantages and Disadvantages of Using VPN for WLAN

Advantages	Disadvantages
• Uses 3DES or AES encryption • Enforces remote user authentication and polices for Wireless LAN users • Leverages existing VPN if already installed for wired network • Used for remote users accessing the network while on the road at airports, hotels, conference centers	• Client software overhead • Authentication messaging overhead • Management overhead because one VPN application is required per client • Does not support single sign on using Windows log-in • Difficult to integrate existing VPN deployment into a WLAN • Supported user authentication database and server is tied VPN concentrator

WLAN LAN Extension

The goal of a WLAN LAN Extension network is for the WLAN access network to transparently provide the same applications and services as the wired access network. Each WLAN extension discussion that follows addresses the following types of transparency:

- *Security Transparency*—Do the selected security capabilities provide seamless WLAN network security equivalent to wired networks?
- *Application Transparency*—Are the supported WLAN network applications identical to applications on a wired network?
- *Performance Transparency*—Does the WLAN deliver application performance that matches wired network performance?
- *User Transparency*—Are users of the WLAN forced to perform network-specific operations to use the WLAN?

WLAN LAN Extension 802.1x/EAP

This discussion presents WLAN Extension 802.1x/EAP deployment in terms of the following key topics:

- Security Transparency
- Application Transparency
- Performance Transparency
- User Transparency

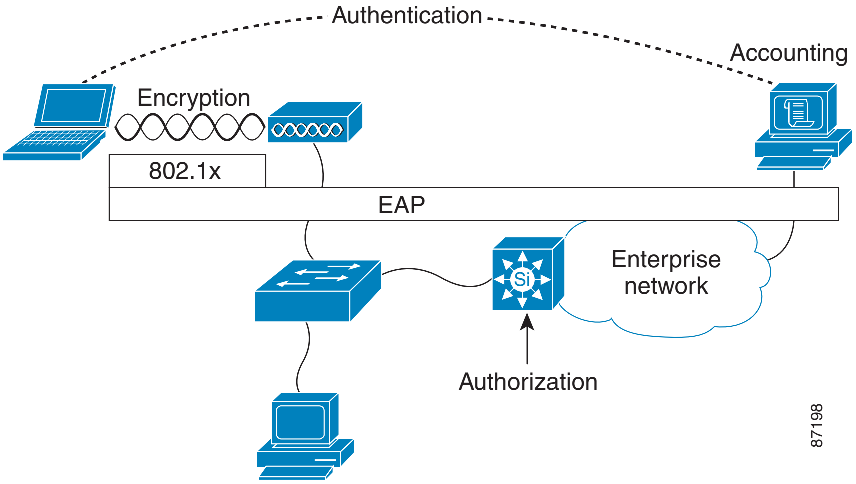
Security Transparency

An 802.1x/EAP implementation of WLAN LAN Extension operates at the Link Layer (Layer 2) to provide authentication, authorization, accounting, and encryption. Figure 4-6 shows a schematic of the 802.1x/EAP WLAN.

The security level provided is beyond that provided on most wired networks, providing link layer encryption and Authentication, Authorization, and Accounting (AAA) access control. This is provided as follows:

- Authentication occurs between the client and the authentication server. Several different EAP types (EAP-Cisco, EAP-FAST, EAP-TLS, PEAP) are supported, allowing the Enterprise to choose the authentication type that best suits its needs.
- Encryption is at the link layer between the WLAN client and the AP. The encryption keys are automatically derived during the authentication process.
- Authorization is controlled by the VLAN or Mobility group membership in combination with the access controls applied at the access router or switch terminating the VLAN or Mobility group.
- Accounting is provided by the RADIUS accounting communicated by the APs to the RADIUS server.

Figure 4-6 WLAN LAN Extension 802.1x/EAP



Application Transparency

As illustrated in Table 4-6, the WLAN connects at the access layer. Once the WLAN client traffic leaves the AP, it is the same as wired traffic—subject to the same access control, queuing, and routing. This achieves the WLAN LAN extension goal of supporting the same applications as the wired network. Any inability to run applications from the wired network over the WLAN network would be the result of policies or the fundamental limitations of the WLAN—not due to the 802.1x/EAP architecture.

Performance Transparency

WLAN has a lower bit rate and a lower throughput than most Enterprise wired LANs. Therefore providing equivalent performance for all applications over the WLAN can be a challenge. The strategy to minimize differences in application performance between the wired and wireless network is to utilize the QoS tools available on the WLAN and the APs. Those applications identified as being sensitive to network throughput and delay can be classified and scheduled as required. Load balancing and admission control tools on the WLAN can optimize the usage of the available WLAN resources. As the user or device has been authenticated there is an opportunity to apply identity based on Q0S features.

User Transparency

The different EAP types in 802.1x/EAP allow enterprises to choose an authentication mechanism that best matches security requirements. This allows the integration of the 802.1x/EAP into existing user behavior. Many organizations enforce stronger authentication mechanisms on WLAN networks (compared to wired networks), due to reduced physical security in the WLAN. Authentication on the wired network is expected to catch up with WLAN networks, with organizations using 802.1x/EAP mechanisms to enhance wired network security.

WLAN LAN Extension IPSec

The use of IPSec VPN tunnels is an alternative to 802.1x/EAP implementation. Network designers might choose this implementation over and 802.1x/EAP solution due to security policy reasons. IPSec is a well-established standard that is endorsed by a number of security organizations. IPSec is a regulatory requirement in some situations.

The primary advantage of an IPSec-based VPN solution is the encryption mechanism. IPSec includes support of Triple Data Encryption Standard (3DES) and AES encryptions, whereas 802.1x/EAP currently relies upon WEP or proprietary WEP plus TKIP and MIC.

A WLAN LAN Extension IPSec solution is considered more difficult to implement than an 802.1x/EAP solution. The network topology up to the VPN concentrator is considered *untrusted* and an appropriate security policy must be created, configured, and maintained at all points that touch this untrusted network.

Security Transparency

WLAN LAN Extension via IPSec provides AAA-equivalent features to 802.1x/EAP solutions. Refer to Figure 4-7. Key elements are as follows:

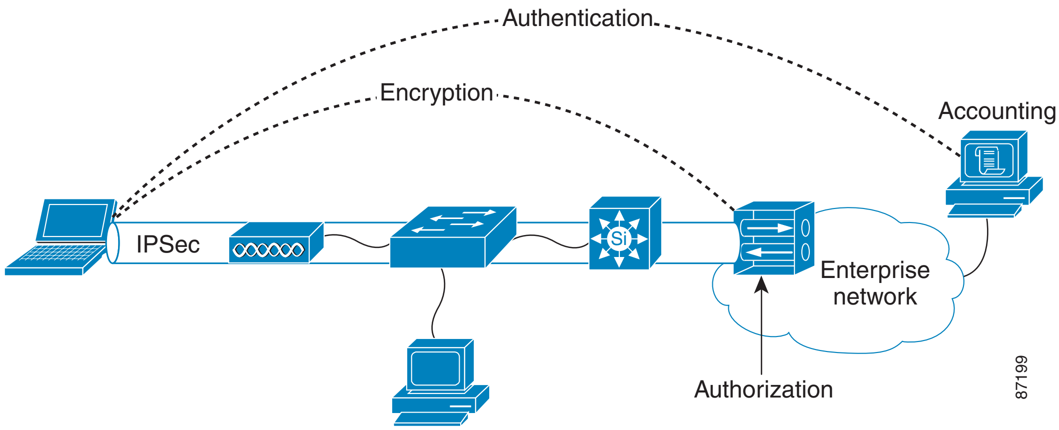
- Authentication occurs between the client and the VPN concentrator. Multiple authentication types are supported with in the IPSec framework.

- Encryption is at the network layer using 3DES or AES, and is negotiated between the client and the VPN concentrator.

In addition to the inherent WLAN LAN Extension IPSec security features associated with this implementation, VPN capabilities provide additional AAA-related security capabilities:

- Authorization is controlled by the VPN concentrator and is determined at the time of authentication. Policy is provided by the authentication server.
- Accounting is provided by RADIUS accounting software on both the VPN concentrator and the authentication server.

Figure 4-7 WLAN LAN Extension IPSec



Application Transparency

As can be seen in Figure 4-7, WLAN traffic is transported over an IPSec tunnel to the VPN concentrator. This can affect application transparency:

- *Protocol Limitations*—Only the IP protocol is supported; the network is not multi-protocol
- *Address Translation*—The IPSec client performs a form of address translation between its local IP address and that allocated by the VPN concentrator. This can impact the operation of some applications.
- *No Multicast*—The connection to the VPN concentrator is point-to-point. Multicast applications are not supported.

Performance Transparency

Providing equivalent performance for all applications over the WLAN can be a challenge, because a WLAN has a lower bit rate and a lower throughput than most Enterprise wired LANs. The use of IPSec VPN tunnels introduces some additional considerations:

- *MTU size*—The MTU size of packets must be adjusted to incorporate IPSec overhead.
- *Processing Overhead*—Clients incur processing overhead from IPSec VPN. However, this should not be noticeable on most target platforms.

- *Traffic Classification and QoS Considerations*—Type of Service (ToS) and differentiated-services-code-point (DSCP) values are projected from client packets into the IPSec packets. As a result, QoS preference can be acted upon, but no classification of traffic is possible while the traffic is IPSec encrypted.
- *Traffic Scheduling*—All queuing at the VPN concentrator is handled on a first-in-first-out basis.

User Transparency

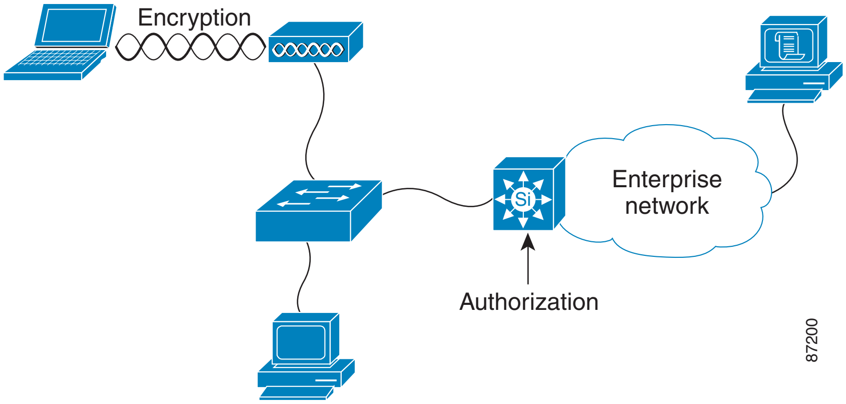
The Cisco IPSec VPN client has a number of features that aid user transparency, thereby providing equivalent services to those available with 802.1x/EAP solutions:

- *Auto Initiation*—The VPN client can be configured to automatically launch for particular address ranges. In an enterprise, this would be configured to launch within the Enterprise WLAN address ranges.
- *OS Integration*—The VPN client can capture user name and password information at login and use these as part of the VPN client login. This is similar to the process used in EAP-Cisco. As an alternative, the VPN client can use stored certificates associated with a specific user, similar to EAP-TLS. These features coupled with Auto Initiation should provide a high level of user transparency.

WLAN Static WEP Keys

Static WEP key implementation is not recommended for general purpose WLAN LAN Extension networks because of known weaknesses in the WEP encryption algorithms—and because of the difficulty in configuring and maintaining of static keys. Certain client devices are only capable of supporting static keys. These clients should be put on a separate WLAN VLAN or mobility group and have their authorization limited to addresses and protocols specific to the application supported by the Static WEP client. If possible, WEP plus TKIP or CKIP and CMIC should be used in preference to WEP, because WEP plus TKIP or CKIP and CMIC provides increased security features.

Figure 4-8 WLAN Static WEP



Security Transparency

Security issues related to static WEP key implementations:

- *Weak Authentication*—Any hardware device with a matching configuration and WEP key may join the network. The Static WEP key authenticates a group of devices—never individual users.
- *Encryption Limitation*—Encryption is at the link layer between the WLAN client and the AP. The current encryption mechanisms available are WEP and WEP plus TKIP or CKIP and CMIC. If possible WEP plus TKIP or CKIP and CMIC should be used.
- *Authorization Limitation*—Authorization is controlled by the VLAN membership associated with the static WEP key.
- *Accounting*—Not available.

Application Transparency

As illustrated in Figure 4-8 the WLAN connects at the access layer. Once the WLAN client traffic leaves the AP, it is the same as wired network traffic and subject to the same access control, queuing, and routing. WLAN Static WEP solutions should be limited to the specialized applications that the Static WEP client supports. The network would appear transparent to this application, but to all other applications access should be blocked.

Performance Transparency

To minimize differences in application performance between the wired and wireless network, utilize the QoS tools available on the WLAN and the APs. Those applications identified as being sensitive to network throughput and delay can be classified and scheduled as required. Load balancing and admission control tools on the WLAN can optimize the usage of the available WLAN resources.

As Static WEP does not perform any user authentication no user based QoS policies can be applied.

User Transparency

Static WEP requires no authentication and should be transparent to the supported applications and users. The static WEP key only becomes an issue for the user if required to change it.

Cisco Unified Wireless Network Considerations

In the Cisco Integrated Wirelss Network, where WDS resides can change the characteristics of transparency. The following section details some of the specific considerations. For further details, refer to the following URL:

Cisco Catalyst 6500 Series Wireless LAN Services Module (WLSM) Deployment Guide: http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_technical_reference09186a0080362bd0.html

Security Transparency

The features enabled by Cisco Unified Wireless Network do not directly impact security transparency as the architecture supports all of the existing security models, while the switch-based WDS solution makes it easier to implement different security solutions through Layer 3 roaming and integration with other Catalyst 6000 modules.

Application Transparency

Fast Secure Roaming (FSR) enables wireless clients to quickly roam between APs. Using Cisco Centralized Key Management (CCKM), the WDS caches session credentials (security keys) derived for a client session and uses them for re-authentication and re-keying when a client roams. Caching this information rather than forcing the client to do a full authentication reduces the authentication time and therefore the total time required for roaming. This can enhance application transparency as the impact of roaming is reduced and less likely to impact either the application or the user.

Performance Transparency

The Cisco Unified Wireless Network architecture was engineered to utilize and maintain the QoS features of the supporting wired network. In a switched-based solution, care must be taken in controlling the MTU size to ensure this does not impact performance.

User Transparency

Cisco Unified Wireless Network is compatible with all other WLAN client solutions, and therefore does not have an adverse impact on user transparency.

EAP Considerations for High Availability ACS Architecture

As a centralized authentication server, Cisco Secure ACS brings in RADIUS based AAA capabilities inside the LAN for both wired and wireless networks.

The ACS redundancy and reliability is meant to address two issues:

- The ACS server should not represent a single point of failure
- A network failure should not impact a user’s ability to log on

The first issue is a good reason to replicate the ACS database to a secondary server, allowing for failover and maintenance. This redundancy configuration should be implemented in almost all cases.

The second issue is an instance in which it is critical to use the local WLAN even in the event of a network failure preventing access to a remote ACS server. Implementation of this second use of replication depends on the application architecture of the enterprise. For example, if the applications that the users want to reach are also remote, little is to be gained by being able to use the WLAN.

The ACS Architecture

The ACS strategy must consider how the entire enterprise will be structured, rather than just the campus. A key consideration is the location of AAA databases. It is essential that—assuming a database that is distributed across the enterprise—the ACS strategy reflect an approach in which the elements of the ACS architecture are carefully analyzed, designed, and implemented for authentication systems associated with file services throughout the enterprise. This assessment should be the starting point for the ACS deployment strategy. In an ideal situation, the existing infrastructure can provide the user names, passwords, and profiles to the ACS servers. The implementation of an ACS architecture-based infrastructure is currently limited to systems that store the password using MS-CHAP, such as Microsoft servers.

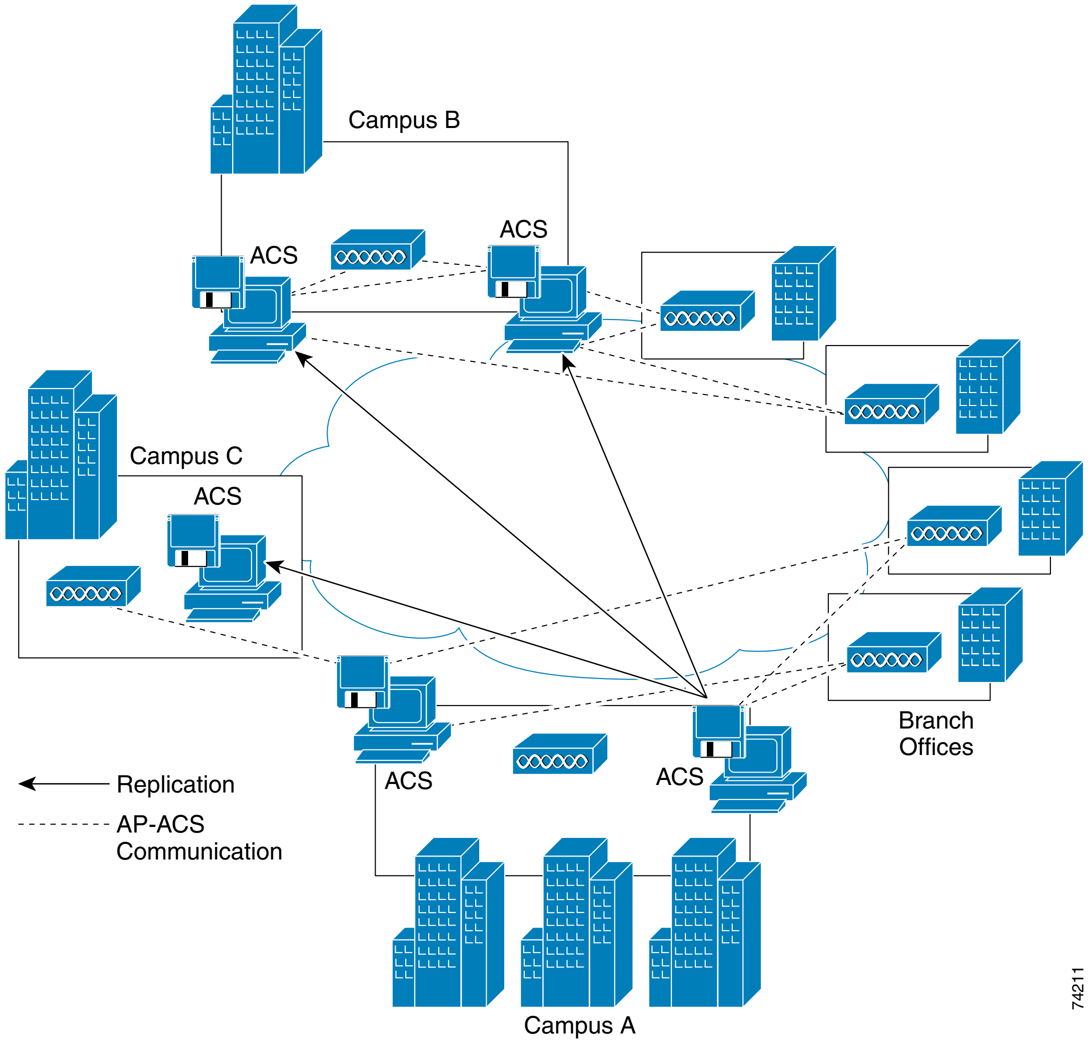
The main point to be aware of in this strategy is that the ACS model is currently a replication model, not a synchronization model. This model might conflict with the administration processes currently in place, as updates must be made on the root server, and administrators on this server have global rights.

Example Architecture

Figure 4-9 shows an example of what ACS architecture might look like. Campus A holds the authoritative ACS database server. This server is replicated to the other Enterprise ACS servers. APs communicate to the two local ACS servers.

Campus B—because of its size and distance from Campus A—has opted for another two ACS servers, thus providing its own backup. Campus C—being smaller and closer to Campus A—has opted to have only one server, and relies on Campus A for backup. The branch offices use the ACS servers that are the shortest network distance from them.

Figure 4-9 Example Enterprises ACS Architecture



CHAPTER 5

WLAN Deployment Modes

This chapter focuses on the Wireless LAN deployment modes.

Cisco WLANs can be deployed in different modes addressing size, complexity, flexibility and mobility considerations of the WLAN environment. There are three basic deployment modes:

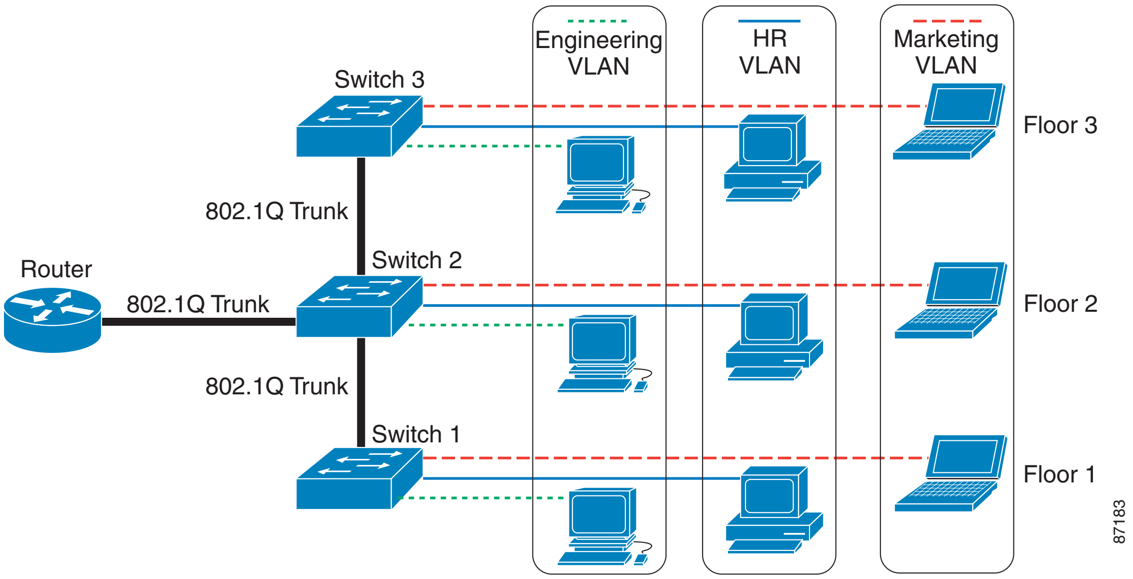
- *Cisco Unified Wireless Network Standalone AP mode*—The AP provides full 802.11 functionality (acting as an 802.11 infrastructure device) along with security, QoS, Layer 2 mobility, and local RADIUS authentication. Wireless VLANs can enable client/SSID segmentation which can include device type, security, key rotation, policy grouping and Class of Service (CoS).
- *Cisco Unified Wireless Network non-switching mode*— The AP provides full 802.11 functionality along with QoS functionality. Wireless Domain Services (WDS) enable functions including Layer 2 Fast Secure Roaming, local RADIUS authentication service, infrastructure authentication and aggregation of radio management information. Wireless VLANs enable client segmentation which can include device type, security, key rotation, policy grouping and CoS.
- *Cisco Unified Wireless Network switch-based mode*—The AP provides full 802.11 functionality along with QoS functionality. Using this deployment mode, switch based WDS adds Layer 3 Fast Secure roaming and Layer 3 roaming (Cisco Central Key Management/CCKM and non-CCKM).

VLAN Background

VLANs define broadcast domains in a Layer 2 network. Legacy networks use routers to define broadcast domain boundaries. Layer-2 switches create broadcast domains based on the configuration of the switch. Switches are multi-port bridges that allow the creation of multiple broadcast domains. Each broadcast domain is a distinct virtual bridge within a switch.

VLANs have the same attributes as physical LANs with the additional capability to group end stations physically to the same LAN segment regardless of the end station’s geographical location. Figure 5-1 shows an example of three wired VLANs in logically defined networks.

Figure 5-1 Example Deployment of Wired VLANs



Single or multiple virtual bridges can be defined within a switch. Each virtual bridge created in the switch defines a new broadcast domain (VLAN). Switch interfaces assigned to VLANs manually are referred to as interface-based or static membership-based VLANs. This type of VLAN is often associated with IP subnetworks. For example, when all of the end stations in a particular IP subnet belong to the same VLAN, traffic cannot pass directly to another VLAN (between broadcast domains) within the switch or between two switches. Traffic between VLANs must be routed.

To interconnect two different VLANs, routers are used. These routers execute inter-VLAN routing or routing of traffic between VLANs. Broadcast traffic is then terminated and isolated by these Layer 3 devices (a router or Layer 3 Switch will not route broadcast traffic from one VLAN to another).

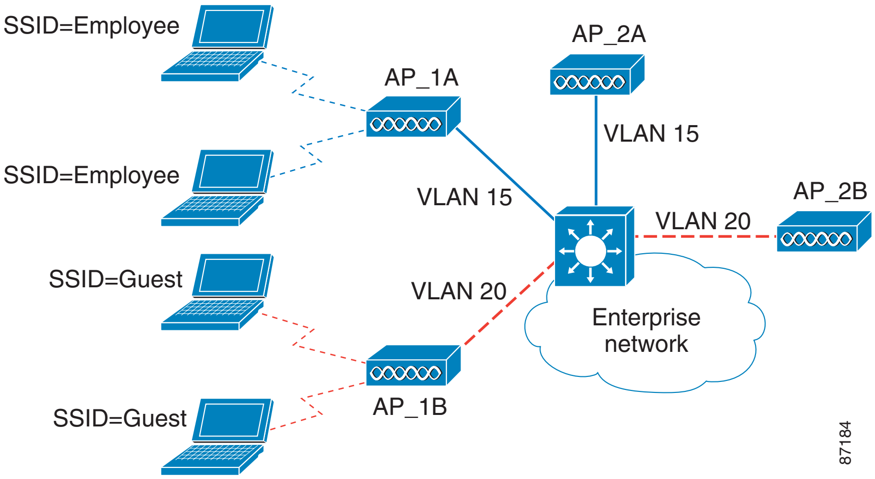
The two most common VLAN trunking protocols used on Cisco switches and routers are Inter-Switch Link (ISL) and IEEE 802.1Q. ISL (Cisco-proprietary protocol) and 802.1Q (IEEE standard) are encapsulation standards used to interconnect multiple switches and routers via trunking. The Cisco AP WLAN solution only supports 802.1q trunking. For more information on these VLAN trunking protocols, please refer to the following URL:

http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Internetworking:Trunking

Wireless VLAN Introduction

For both the Standalone and WDS-based solutions, the concept of Layer 2 wired VLANs is extended to the WLAN with wireless VLANs. As with wired LANS, wireless VLANs define broadcast domains and segregate broadcast/multicast traffic between VLANs. When VLANs are not used, an IT administrator would need to install additional WLAN infrastructure to segment traffic between user groups or device groups. For example, to segment traffic between employee and guest VLANs, an IT administrator must install two APs at each location throughout an Enterprise WLAN network (as shown in Figure 5-2). However, with the use of Wireless VLANs, one AP at each location can be used to provide access to both groups.

Figure 5-2 User Segmentation without Wireless VLANs



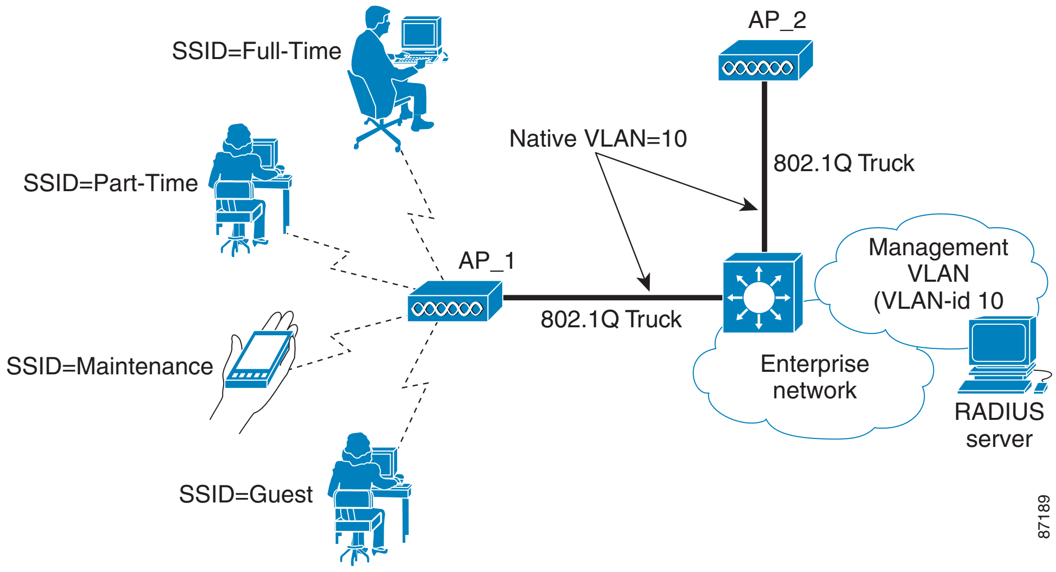
With Cisco APs, an 802.1q trunk can be terminated on an AP, allowing access up to 16 wired VLANs. A unique Service Set Identifier (SSID) defines a wireless VLAN on the AP and the bridge. Each SSID is mapped to a VLAN-id on the wired side (default SSID-to-VLAN-id mapping).

Additionally, with WLANs, a per-VLAN security policy can be defined on the AP and on the bridge by the IT administrator. See "Configuration Parameters per VLAN, page 5-5" for additional information regarding VLAN security configuration. WLAN VLANs are unaffected by the introduction of non-switch-based Cisco Unified Wireless Network. When using switch-based Cisco Unified Wireless Network, Layer 3 roaming removes the requirement for extending wired VLANs from the APs. The concept of a WLAN VLAN is maintained through the concept of a *Mobility Group*. A mobility group maps to an SSID and up to 16 mobility groups can exist on one AP.

Wireless VLAN Deployment Overview

Wireless VLAN deployments are different for indoor and outdoor environments. For indoor deployments see Figure 5-3, the AP is generally configured to map several wired VLANs to the WLAN. Whereas, for outdoor environments (please refer to Figure 5-4), 802.1q trunks are deployed between bridges with each bridge terminating and extending as an 802.1q trunk, and participating in the 802.1d-based spanning-tree protocol (STP) process.

Figure 5-3   Indoor Wireless VLANs Deployment



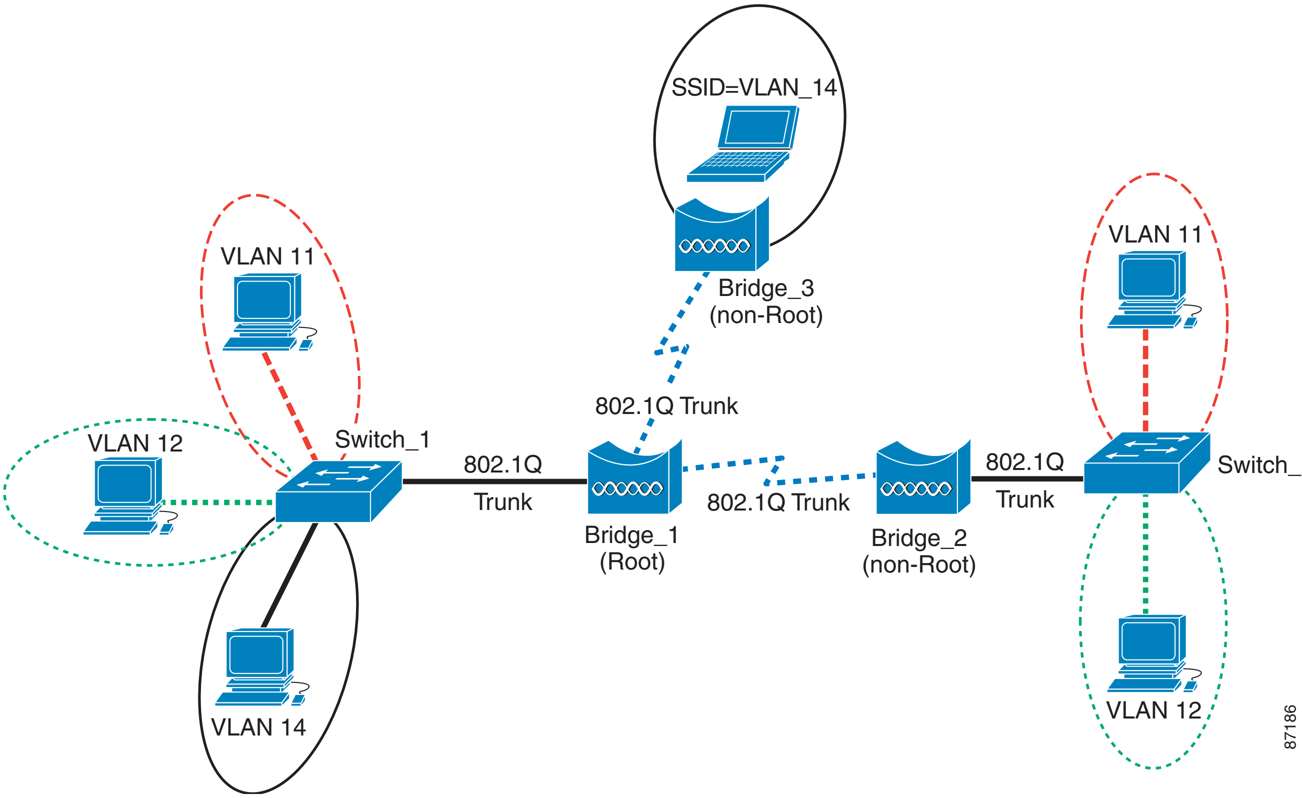
In the indoor WLAN deployment scenario shown in Figure 5-3, four wireless VLANs are provisioned across the campus to provide WLAN access to full-time employees, part-time, maintenance and ^guests. Also, as shown in Figure 5-3, each wireless VLAN is configured with an appropriate security policy and mapped to a wired VLAN. An IT administrator enforces the appropriate security policies within the wired network for these four different user groups.

Table 5-1   Configuration for Wireless VLANs in Figure 5-3

SSID	VLAN-ID	Security Policy
Full-Time	14	EAP Cisco
Part-Time	24	PEAP
Maintenance	34	802.1x with Dynamic WEP + TKIP
Guest	44	Open/no WEP

Note An outdoor WLAN deployment scenario is shown in Figure 5-4. In this example, wireless trunking is used to connect the root bridge to the non-root bridges. The root and non-root bridges terminate the 802.1q trunk and participate in the spanning-tree protocol (STP) process of bridging networks together.

Figure 5-4 Outdoor Wireless VLANs Deployment



Wireless VLANs—Detailed Feature Description

This section details the VLAN features available on Cisco APs. With these features, an 802.1q trunk can be enabled between the AP/bridge and the wired infrastructure allowing up to 16 wired VLANs to be extended to the WLAN.

Configuration Parameters per VLAN

As discussed in the Wireless VLAN Introduction, page 5-2, a per VLAN security policy can be defined on the AP to allow the IT administrator to define appropriate restrictions per VLAN. The following parameters can be configured on the SSID (wireless VLAN):

- *SSID Name*—Configures a unique name per wireless VLAN.
- *Default VLAN ID*—Default VLAN-ID mapping on the wired-side.
- *Authentication Type*s—Open, Shared, and Network-EAP types.
- *Media Access Control (MAC) Authentication*—Under Open, Shared, and Network-EAP.
- *EAP Authentication*—Under Open and Shared authentication types.
- *Maximum Number of Associations*—Ability to limit maximum number of WLAN clients per SSID.

The following parameters can be configured on the wired VLAN side:

- *Encryption Key*—This is the key used for broadcast/multicast traffic segmentation per VLAN. It is also used for static WEP clients (for both unicast and multicast traffic). The IT administrator must define a unique encryption key per VLAN. This is discussed more in detail in Broadcast Domain Segmentation, page 5-6.
- *Enhanced Message Integrity Check (MIC) Verification for WEP*—Enables MIC per VLAN.
- *Temporal Key Integrity Protocol (TKIP)*—Enables per-packet key hashing per VLAN.
- *WEP (Broadcast) Key Rotation Interval*—Enables Broadcast WEP key rotation per VLAN. This is only supported for wireless VLANs with 802.1x protocols enabled (such as EAP-Cisco, EAP-TLS, PEAP, EAP-SIM, and the like.)
- *Default Policy Group*—Applies policy-group (set of Layers 2, 3, and 44 filters) per VLAN. Each filter (within a policy group) can be configured to allow or deny certain type of traffic.
- *Default Priority*—Applies default CoS priority per VLAN.

With an encryption key configured, the VLAN supports standardized WEP. However, TKIP/MIC/Broadcast Key rotation features are optionally configured as noted above. Table 5-2 lists the SSID and VLAN-ID configuration parameters.

Table 5-2 SSID and VLAN-ID Configuration Parameters

Parameter Description	SSID Parameter	VLAN-ID Parameter
Authentication Types	X	
Maximum number of Associations	X	
Encryption key (Broadcast Key)		X
TKIP/MIC		X
WEP (Broadcast) Key rotation Interval		X
Policy Group		X
Default Priority (CoS mapping)		X

Broadcast Domain Segmentation

All Layer 2 broadcast and multicast messages are propagated over the air. Thus, each WLAN client receives broadcast/multicast traffic belonging to different VLANs. This is different from wired VLAN broadcast/multicast traffic. A wired client receives Layer 2 broadcast/multicast traffic only for its own VLAN. Thus, a unique encryption (broadcast/multicast) key per VLAN is used to segment the Layer 2 broadcast domains on the WLAN. This unique encryption key must be configured during initial VLAN setup. If Broadcast Key rotation is enabled, this encryption key is generated dynamically and delivered to WLAN clients in 802.1x messages.

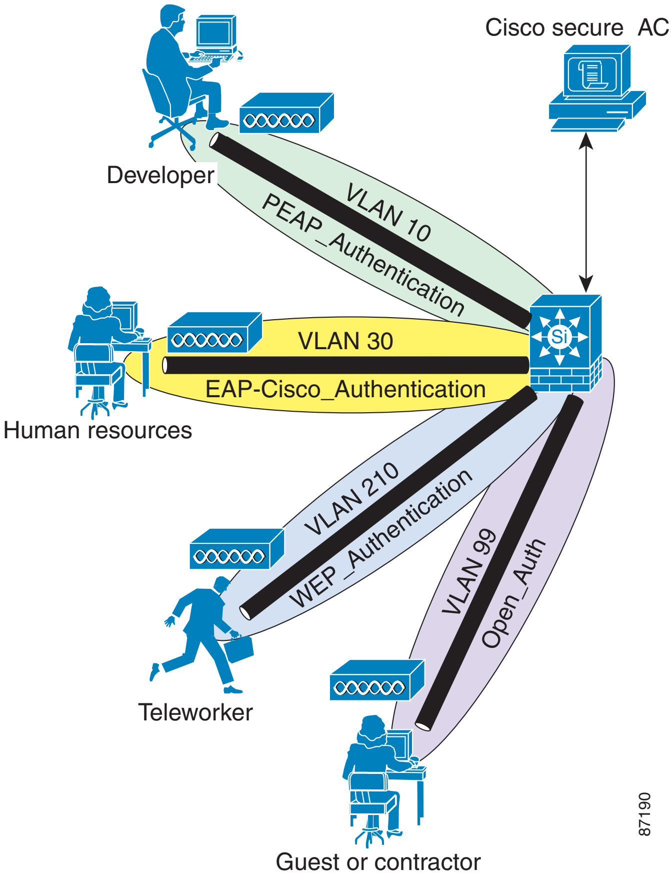
The requirement to segment broadcast domains the wireless side restricts the use of un-encrypted VLAN per WLAN *Extended Sub System* (ESS). A maximum of one VLAN can be un-encrypted per WLAN ESS. Also, the behavior of a WLAN client on an encrypted VLAN should be to discard un-encrypted Layer 2 broadcast/multicast traffic.

IOS firmware release 12.3(4)JA introduced a multiple BSSID feature that allows up to eight unique BSSIDs to be created on the same AP radio. Only the 11g, and later generation 11a radios support this feature. Allowing the unique BSSIDs provides further separation between WLAN VLANs as the clients treat the different BSSIDs as though they are different radios.

Flexible WLAN Security using VLANs

VLAN support on the APs and Catalyst Switches allows multiple WLAN security domains to be created. This allows multiple types of WLAN security to be mixed and matched on the same Cisco AVVID network infrastructure.

Figure 5-5 Using VLANS to Create Multiple WLAN Security Domains



In addition to VLANs having the flexibility to create multiple WLAN security domains for flexible deployments, they also allow flexible migrations from older WLAN security to updated standards or products. This is not only possible because of VLANs, but also because Cisco APs and Cisco Secure ACS support simultaneous WLAN security such as EAP-Cisco, EAP-FAST, EAP-TLS, PEAP and EAP-Subscriber Identity Module (EAP-SIM). In addition, Cisco Aironet 802.11 NICs support multiple types of WLAN security, including EAP-Cisco, EAP-FAST and PEAP.

Native (Default) VLAN Configuration

The AP's, or the bridge's, native VLAN (default VLAN) must be set to the native VLAN of the wired trunk. This allows the AP or bridge to receive and communicate using the Inter-Access Point Protocol (IAPP) with other APs or bridges in the same WLAN ESS. It is a requirement that all APs and bridges in an ESS must use the same native VLAN-ID. All Telnet and Hypertext Transfer Protocol (HTTP) management traffic—as well as the RADIUS and WDS traffic—is routed to the AP via the native

VLAN. Cisco recommends that IT managers restrict user access to the native/default VLAN of the APs and bridges with the use of Layer 3 access control lists (ACLs) and policies on the wired infrastructure side.

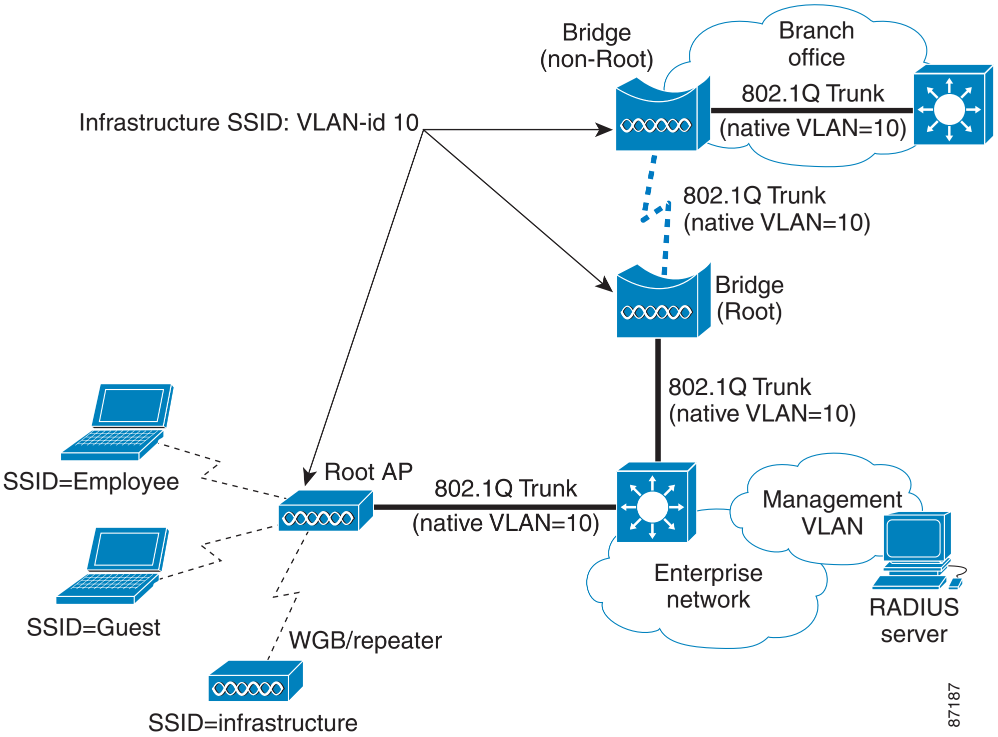
The IT administrator may or may not wish to map the native VLAN of the AP/bridge to an SSID (the WLAN ESS). Scenarios where the native VLAN should be mapped to an SSID include:

- An associated workgroup bridge is treated as an infrastructure device
- Connection of a root bridge to a non-root bridge

In the above scenarios, Cisco recommends configuring an Infrastructure SSID per AP or bridge.

Figure 5-6 illustrates the combined deployment of infrastructure devices (such as workgroup bridges, non-root bridges, and repeaters) along with non-infrastructure devices (such as WLAN clients) in an Enterprise WLAN. The native VLAN of the AP is mapped to the Infrastructure SSID. The highest possible level of encryption should be enabled for the Infrastructure SSID—this would typically be CKIP plus CMIC or TKIP. Configuration of a secondary SSID as the Infrastructure SSID is also recommended. The concepts of primary and secondary SSIDs are explained in the next section.

Figure 5-6 Combined Deployment of Infrastructure and Non-Infrastructure Devices



Primary (Guest) and Secondary SSIDs

When enabling multiple wireless 802.1x VLANs on the AP or bridge, multiple SSIDs are created with each SSID mapping to a default VLAN-ID on the wired side. However, as per the 802.11 specifications, only one SSID can be broadcast in the beacons. The introduction of the MBSSID as mentioned above allows up to eight SSID beacons to be sent out by each AP radio The IT administrator defines the SSIDs that are broadcast in the 802.11 beacon management frames. All other SSIDs are secondary SSIDs and are not broadcast in the 802.11 beacon management frames.

If a client or infrastructure device (such as a workgroup bridge) is to send a probe request with a secondary SSID, the AP or bridge responds with a probe response with that secondary SSID.

An IT administrator can also map the primary SSID to the VLAN-ID on the wired infrastructure in different ways. For example, in an Enterprise rollout scenario, the primary SSID might be mapped to the un-encrypted VLAN on the wired-side to provide guest VLAN access.

RADIUS-based VLAN Access Control

As discussed earlier, each SSID is mapped to a VLAN-ID on the wired side. The IT administrator might wish to impose a RADIUS-based VLAN access control using 802.1x or MAC address authentication mechanisms. For example, if the WLAN is setup such that all VLANs use 802.1x and similar encryption mechanisms for WLAN user access, then a user can hop from one VLAN to another by simply changing the SSID and successfully authenticating to the AP using 802.1x. This may not be preferred if the WLAN user is confined to a particular VLAN.

There are two different ways to implement RADIUS-based VLAN access control methods:

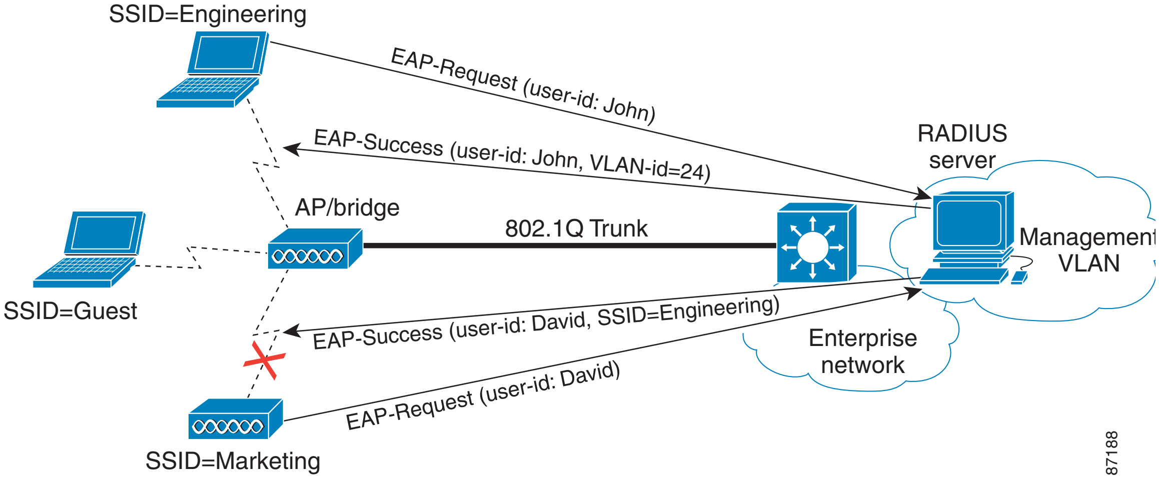
- *RADIUS-based SSID Access Control*—Upon successful 802.1x or MAC address authentication, the RADIUS server passes back the allowed SSID list for the WLAN user to the AP or bridge. If the user used an SSID on the allowed SSID-list, then the user is allowed to associate to the WLAN. Otherwise, the user is disassociated from the AP or bridge.
- *RADIUS-based VLAN Assignment*—Upon successful 802.1x or MAC address authentication, the RADIUS server assigns the user to a pre-determined VLAN-ID on the wired side. The SSID used for WLAN access does not matter because the user is always assigned to this pre-determined VLAN-ID.

Figure 5-7 illustrates both of the RADIUS-based VLAN access control methods. In this diagram, both Engineering and Marketing VLANs are configured to allow only 802.1x authentication (such as EAP-Cisco, EAP-TLS or PEAP).

For RADIUS-based VLAN Assignment, John uses the Engineering SSID to gain access to the WLAN. The RADIUS server maps John to VLAN-ID 24. This may or may not be the default VLAN-ID mapping for the Engineering SSID. Using this method, a user is mapped to a fixed wired VLAN throughout an Enterprise network.

For RADIUS-based SSID access control, David uses the Marketing SSID to gain access to the WLAN. However, the permitted SSID-list sent back by the RADIUS server indicates that David is only allowed access to the Engineering SSID. Upon receipt of this information, the AP disassociates David from the WLAN network. Using this method, a user is given access to only one or pre-determined SSIDs throughout an Enterprise network.

Figure 5-7 RADIUS-based VLAN Access Control


SSID=Engineering
EAP-Request (user-id: John)
EAP-Success (user-id: John, VLAN-id=24)
RADIUS server
AP/bridge
802.1Q Trunk
Management VLAN
SSID=Guest
EAP-Success (user-id: David, SSID=Engineering)
Enterprise network
EAP-Request (user-id: David)
SSID=Marketing
87188

RADIUS user attributes used for VLAN-ID assignment are:

- IETF 64 (Tunnel Type)—Set this to “VLAN”
- IETF 65 (Tunnel Medium Type)—Set this to “802”
- IETF 81 (Tunnel Private Group ID)—Set this to VLAN-ID

RADIUS user attribute used for SSID access control is:

- Cisco IOS/PIX RADIUS Attribute, 009\001 cisco-av-pair

  Example—Configure the above attribute to allow a user to access the WLAN using Engineering and Marketing SSIDs only:

  – ssid=Engineering
  – ssid=Marketing

  With non-switch-based Cisco Unified Wireless Network both VLAN assignments and SSID access control are supported. With switch-based Cisco Unified Wireless Network, only SSID access control is supported. The concept of VLAN assignment for switch-based Cisco Unified Wireless Network is converted to a Mobility Assignment feature.

Guidelines for Deploying Wireless VLANs

In order to properly deploy wireless VLANs, IT administrators should evaluate the need for deploying wireless VLANs in their own environment. Existing wired VLAN deployment rules and policies should also be reviewed. Existing wired VLAN policies can be used as the basis for wireless VLAN deployment policies.

This section is split into three discussions:

- Criteria for Wireless VLAN Deployment—Details selection criteria for wireless VLAN deployment.
- Wireless VLAN Deployment Example—Provides a deployment example, summarizes the of rules for WLAN VLANs deployment.

- Summary of Rules for Wireless VLAN Deployment—Provides best-practices to use on the wired infrastructure when deploying wireless VLANs.

Criteria for Wireless VLAN Deployment

While the full criteria for each wireless VLAN deployment are likely to be unique, some standard criteria exist for most rollouts. These include:

- Common applications used by all WLAN users. The IT administrator should define:
  - Wired network resources (such as servers) commonly accessed by WLAN users
  - Quality of Service (QoS) level needed by each application such as default class of service (CoS) or Voice CoS
- Common devices used to access the WLAN. The IT administrator should define:

  Security mechanisms—Static-WEP, MAC authentication, EAP authentication (such as EAP-Cisco, EAP-TLS, or PEAP), VPN supported by each device type

  Wired network resources, such as Servers, commonly accessed by WLAN device groups

  QoS level needed by each device group, such as default CoS or Voice CoS
- Revise the existing Wired VLAN deployment design guidelines:
  - Existing policies for VLAN access (determine whether specific policies are implemented for different user groups)
  - Localized wired VLANs with Layer-3 core or flat Layer 2 switched network

After the wireless VLAN deployment criteria are defined, the deployment strategy must be determined. Two standard deployment strategies are:

- *Segmentation by User Groups*—Segmentation of the WLAN user community and enforcement of specific security policies per user group. For example, three wired and wireless VLANs in an enterprise environment might be created for full-time employee, part-time employee, and guest access.
- *Segmentation by Device Types*—Segmentation of the WLAN to allow different devices with different security levels to access the WLAN. For example, it is not recommended to have handheld devices that support only 40/128-bit static-WEP co-exist with other WLAN client devices using 802.1x with dynamic WEP in the same VLAN. In this scenario, devices are grouped and isolated with different levels of security into separate VLANs.

Implementation criteria such as those listed below is then defined:

- Use of policy group, such as a set of filters, to map wired policies to the wireless side.
- Use of 802.1x to control user access to VLANs using either RADIUS-based VLAN assignment or RADIUS-based SSID access control.
- Use of separate VLANs to implement different CoS.

Wireless VLAN Deployment Example

A wireless VLAN deployment example is outlined below. The IT administrator of company XYZ determines the need for WLANs in his network. Utilizing the guidelines as described in "Criteria for Wireless VLAN Deployment" his findings are as follows:

- Three different user groups are commonly present across Company XYZ: full-time employees, contract employees, and, guests.
- Full-time and contract employees use company supplied PCs to access the wireless network. These PCs are capable of supporting 802.1x authentication methods for accessing the WLAN.
- Full-time employees need full access to the wired network resources. The IT department has implemented application level privileges for each user via Microsoft Windows NT or Active Directory (AD) mechanisms.
- Part-time employees are not allowed access to certain wired resources (such as human resource servers and data storage servers). Furthermore, the IT department has implemented application level privileges for part-time employees (using Microsoft Windows NT or AD mechanisms).
- Guest users need access to the Internet to launch a VPN tunnel back to their company headquarters.
- Maintenance personal (electrical, facilities, and others) use specialized handheld devices that support static 40 or 128 bit encryption to access trouble ticket information via an application server VLAN.
- Existing wired VLANs deployment:
  - Wired VLANs are localized per building (use of unique VLAN-IDs per building).
  - Layer 3 policies are implemented on all VLANs to prevent users from accessing critical applications such as network management servers).

In the above case, the IT administrator can deploy wireless VLANs by creating four wireless VLANs as follows:

Step 1 For Full-Time and Part-Time VLANs, implement 802.1x with dynamic WEP along with TKIP functionality for WLAN access. Tie user-login on the RADIUS server with Microsoft back-end user database to enable single sign-on for WLAN users.

Implement RADIUS-based SSID access control for both Full-Time and Part-Time employees to access WLAN. This is recommended to prevent part-time employees from VLAN hopping (trying to access the WLAN using Full-Time VLAN).

Note In this deployment scenario, VLANs are localized per building with user group mapping to wired VLAN-IDs different for each building. In order to enable users to access the WLAN from anywhere on campus, SSID access control is recommended rather than fixed VLAN-ID assignments.

Step 2 Create a Guest VLAN. Implement Open/No WEP access with a Broadcast SSID by using the primary SSID for the Guest VLAN. Enforce policies on the wired network side to force all Guest VLAN access to an Internet gateway and deny access into the corporate network.

Step 3 Create a Maintenance VLAN. Implement Open/with WEP plus MAC authentication for this VLAN. Enforce policies on the wired infrastructure to only allow access to the maintenance server on the application server's VLAN.

Figure 5-8 illustrates this sample WLAN deployment scenario. Table 5-3 lists the configuration details for Figure 5-8 VLANs.

Figure 5-8 Wireless VLAN Deployment Example

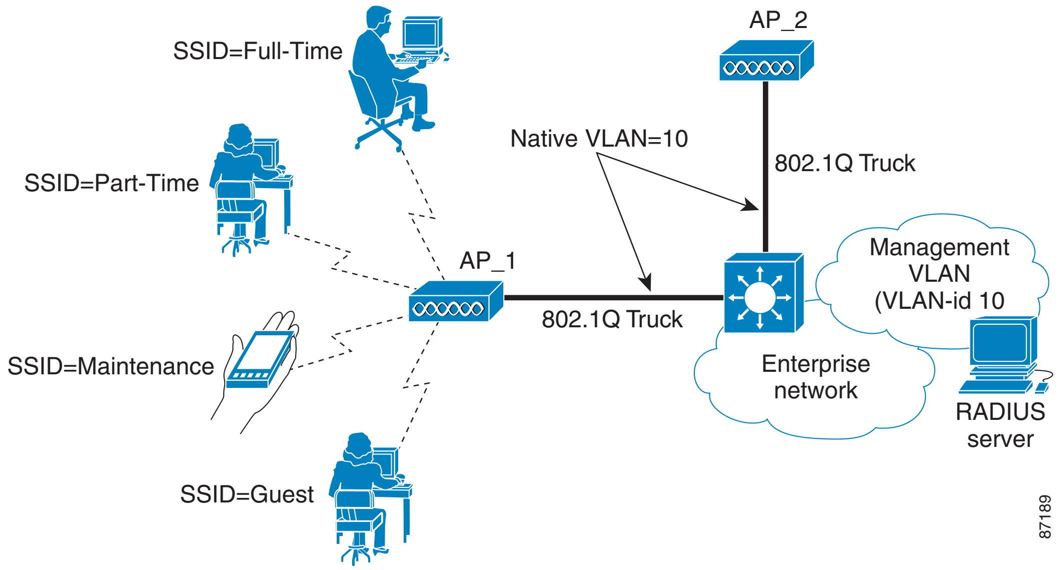


Table 5-3 Configuration for VLANs in Figure 5-8

SSID	VLAN-ID	Security Policy	RADIUS-based VLAN Access Control
Full-time	16	802.1x with Dynamic WEP + TKIP/MIC	Yes
Part-time	26	802.1x with Dynamic WEP + TKIP/MIC	Yes
Maintenance	36	Open/with WEP + MAC authentication	No
Guest	46	Open/no WEP	No

Summary of Rules for Wireless VLAN Deployment

This section summarizes the VLAN rules and guidelines discussed in this document. Key rules to following when deploying wireless VLANs:

- 802.1q VLAN trunking (hybrid mode only) supported between the switch and the AP or bridge.
- A maximum of 16 VLANs per ESS are supported with each wireless VLAN represented with a unique SSID name.
- IT administrator must ensure a unique encryption key per VLAN.
- TKIP, MIC, and Broadcast key rotation can be enabled per VLAN.
- Open, Shared-Key, MAC, network-EAP (EAP-Cisco), and EAP authentication types are supported per SSID.
- One unique policy group (set of Layer 2, Layer 3, and Layer 4 filters) is allowed per VLAN.
- Each SSID is mapped to a default wired VLAN where the ability to override this default SSID to VLAN-ID mapping is provided via RADIUS-based VLAN access control mechanisms.
  - RADIUS-based VLAN-ID assignment per user is supported.
  - RADIUS-based SSID access control per user is supported.

- The ability to assign a CoS mapping per VLAN with eight different levels of priorities is supported.
- The ability to control number of clients per SSID is supported.
- All APs and bridges in the same ESS must use the same native VLAN-ID to facilitate IAPP communication between APs and bridges.
- All WLAN security policies should be mapped to the wired LAN security policies on the switches and routers.

Best-Practices for the Wired Infrastructure

The following best practices are recommended for the wired infrastructure when 802.1q trunking is extended to the APs and bridges:

- Limit broadcast/multicast traffic to the AP and bridge by enabling VLAN filtering and Internet Group Management Protocol (IGMP) snooping on the switch ports. On the 802.1Q trunks to the AP and bridge, filter to allow only active VLANs in the ESS. Enabling IGMP snooping prevents the switch from flooding all switch ports with Layer-3 multicast traffic.
- Map wireless security policies to the wired infrastructure with Access Control Lists (ACLs) and other mechanisms
- The AP does not support the VLAN Trunking Protocol (VTP) or the GARP VLAN Registration Protocol (GVRP) for dynamic management of VLANs because the AP acts as a stub node. The IT administrator must use the wired infrastructure to maintain and manage the wired VLANs.
- Enforce security policies via Layer 3 ACLs on the Guest and Management VLANs (recommended).
  - The IT administrator might implement ACLs on the wired infrastructure to force all Guest VLAN traffic to the Internet Gateway.
  - The IT administrator should restrict user access to the native/default VLAN of the APs and bridges with the use of Layer 3 ACLs and policies on the wired infrastructure.

    Example: Traffic to APs and bridges via the native/default VLAN is only allowed to and from the management VLAN where all the management servers reside—including the RADIUS server.

Note For more details refer to the WLAN VLAN deployment guide.: http://www.cisco.com/en/US/partner/products/hw/wireless/ps430/prod_technical_reference09186a00801444a1.html

CHAPTER 6

WLAN Quality of Service

This chapter addresses quality-of-service (QoS) concerns in the context of WLAN implementations.

QoS Overview

Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic over various network technologies. QoS technologies provide the building blocks for business multimedia and voice applications used in campus, WAN, and service provider networks. QoS allows network managers to establish service level agreements (SLAs) with network users.

QoS enables network resources to be shared more efficiently and expedites the handling of mission-critical applications. QoS manages time-sensitive multimedia and voice application traffic to ensure that this traffic receives higher priority, greater bandwidth and less delay than best-effort data traffic. With QoS, bandwidth can be managed more efficiently across LANs and WANs.

QoS provides enhanced and reliable network service by:

- Supporting dedicated bandwidth for critical users and applications
- Controlling jitter and latency (required by real-time traffic)
- Managing and minimizing network congestion
- Shaping network traffic to smooth the traffic flow
- Setting network traffic priorities

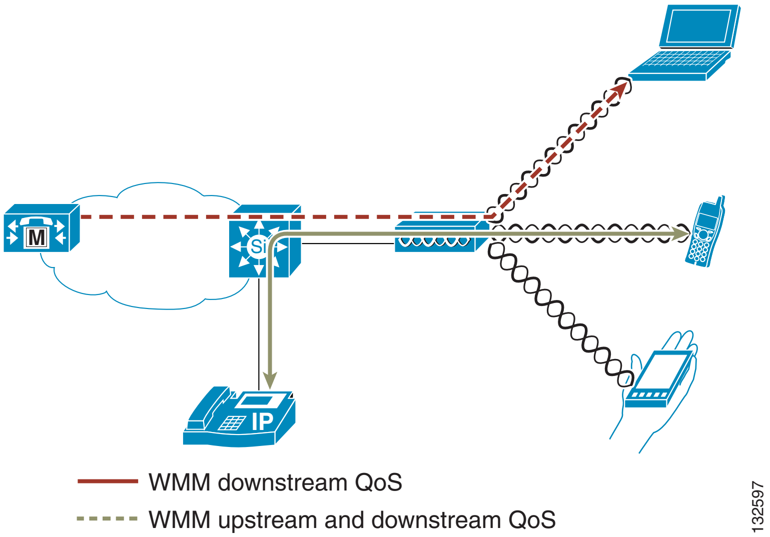
Wireless QoS Deployment Schemes

In the past, WLANs were mainly used to transport low-bandwidth, data-application traffic. Today, with the expansion of WLANs into vertical (such as retail, finance, and education) and Enterprise environments, WLANs are used to transport high-bandwidth, data applications in conjunction with time-sensitive, multi-media applications. This requirement led to the necessity for wireless QoS.

Several vendors, including Cisco, support proprietary wireless QoS schemes for voice applications. To speed up the rate of QoS adoption and to support multi-vendor time-sensitive applications, a unified approach to wireless QoS is necessary. The IEEE 802.11e working group within the IEEE 802.11 standards committee is working on a wireless QoS. Cisco Aironet IOS products support Wi-Fi MultiMedia (WMM), a QoS system based on the IEEE 802.11e Draft that has been published by the Wi-Fi Alliance.

An example deployment of wireless QoS based on Cisco IOS and VxWorks features is shown in Figure 6-1.

Figure 6-1 Wireless QoS Deployment Example



QoS Parameters

QoS is defined as the measure of performance for a transmission system that reflects its transmission quality and service availability. Service availability is a crucial foundational element of QoS. Before QoS can be successfully implemented, the network infrastructure must be highly available. The network transmission quality is determined by latency, jitter, and loss, as described in Table 6-1.

Table 6-1 Definitions for Latency, Jitter, and Loss

Transmission Quality	Description
Latency	Latency (or delay) is the amount of time it takes a packet to reach the receiving endpoint after being transmitted from the sending endpoint. This time period is termed the *end-to-end delay* and can be broken into two areas: fixed network delay and variable network delay. *Fixed network delay* includes encoding/decoding time (for voice and video), as well as the finite amount of time required for the electrical/optical pulses to traverse the media en route to their destination. *Variable network delay* generally refers to network conditions, such as congestion, that may affect the overall time required for transit.

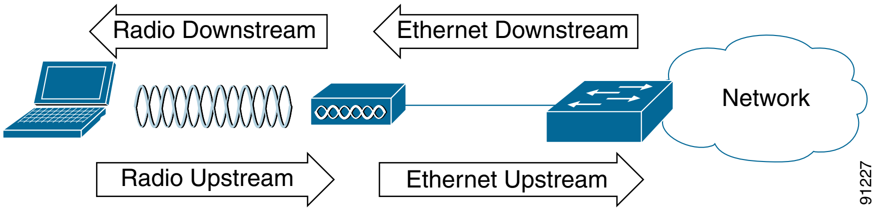
Table 6-1 Definitions for Latency, Jitter, and Loss

Transmission Quality	Description
Jitter	Jitter (or delay-variance) is the difference in the end-to-end latency between packets. For example, if one packet required 100 msec to traverse the network from the source-endpoint to the destination-endpoint and the following packet required 125 msec to make the same trip, then the jitter is calculated as 25 msec.
Loss	Loss (or packet loss) is a comparative measure of packets faithfully transmitted and received to the total number that were transmitted. Loss is expressed as the percentage of packets that were dropped.

Downstream and Upstream QoS

Figure 6-2 illustrates the definition of QoS radio *upstream* and *downstream*.

Figure 6-2 Upstream and Downstream QoS



The notations in Figure 6-2 refers to the following:

- *Radio Downstream* QoS refers to the traffic leaving the AP and traveling to the WLAN clients. Radio Downstream QoS is the primary focus of this deployment guide, as this is still the most common deployment. The client upstream QoS is dependent upon the client implementation.
- *Radio Upstream* QoS refers to traffic leaving the WLAN clients and traveling to the AP. WMM provides upstream QoS for WLAN clients supporting WMM.
- *Ethernet Downstream* refers to traffic leaving the switch/router traveling to the AP. QoS may be applied at this point to prioritize and rate limit traffic to the AP. Configuration of Ethernet downstream QoS is not discussed in this design guide.
- *Ethernet Upstream* refers to traffic leaving the AP traveling to the switch. The AP classifies traffic from the AP to the upstream network according to the traffic classification rules of the AP.

QoS and Network Performance

The application of QoS features may not be easily detected on a lightly loaded network. Indeed, if latency, jitter and loss are noticeable when the media is lightly loaded it is as an indication of a system fault, poor network design or that an application's latency, jitter and loss requirements are not a good match for the network.

QoS features start to impact application performance as the load on the network increases. QoS works to keep latency, jitter and loss for selected traffic types within acceptable bounds.

If providing downstream QoS from the AP, upstream client traffic is treated as best-effort. A client must compete with other clients for upstream transmission as well as competing downstream with best-effort transmission from the AP. Under certain load conditions, a client can experience upstream congestion and the performance of QoS sensitive applications may be unacceptable despite the QoS features on the AP.

Ideally upstream and downstream QoS can be operated either by using WMM on both the AP and WLAN client, or by using WMM and a client's proprietary implementation.

802.11 DCF

Data frames in 802.11 are sent using the *Distributed Coordination Function* (DCF). The DCF is composed of two main components:

- Interframe Spaces (SIFS, PIFS, and DIFS)
- Random Backoff (Contention Window)

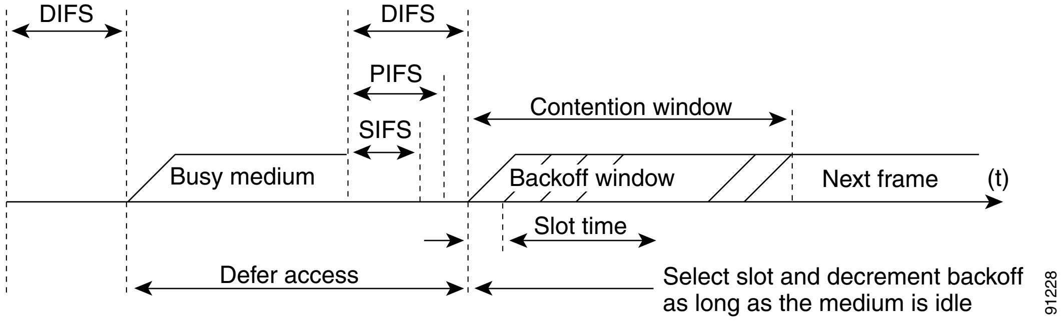
DCF is used in 802.11 networks to manage access to the RF medium. A baseline understanding of DCF is necessary in order to deploy 802.11e based EDCA. Please read the IEEE 802.11 specification for more information on DCF.

DCF is used in 802.11 networks to manage access to the RF medium. A baseline understanding of DCF is necessary in order to deploy 802.11e based EDCA. Please read the IEEE 802.11 specification for more information on DCF.

Interframe Spaces

The Interframe Spaces—SIFS, PIFS, and DIFS—shown in Figure 6-3, allow 802.11 to control which traffic gets first access to the channel once carrier sense declares the channel to be free.

Figure 6-3 Interframe Spaces (IFS)



802.11 currently defines three interframe spaces, as described in Figure 6-3:

- Short Interframe Space (SIFS) 10 µs
- Point Interframe Space (PIFS) SIFS + 1 x slot time = 30 µs
- Distributed Interframe Space (DIFS) 50 µs SIFS + 2 x slot time = 50 µs

Table 6-2 Interframe Spaces

Interframe Space	Description
SIFS	Important frames, such as acknowledgments, wait for the SIFS before transmitting. There is no random backoff when using the SIFS as frames using the SIFS are used in instances where multiple stations would not be trying to send frames at the same time. The SIFS provides a short and deterministic delay for packets that must go through as soon as possible. The SIFS is not available for use by data frames. Only 802.11 management and control frames use SIFS.
PIFS	An optional portion of the 802.11 standard defines priority mechanisms for traffic that uses PIFS. There is no random back mechanism associated with PIFS, as it relies upon a polling mechanism to control which station is transmitting. The option is not widely adopted[1] due to the associated overhead, and lack of flexibility in its application.
DIFS	Data frames wait the DIFS before beginning the random backoff procedure that is part of the Distributed Coordination Function (DCF). This longer wait ensures that traffic using the SIFS or PIFS timing always gets an opportunity to send before any traffic using the DIFS attempts to send.

[1] Figures quoted are for 802.11b; not 802.11a

Random Backoff

When a data frame using Distributed Coordination Function (DCF), shown in Figure 6-4, is ready to be sent, it goes through the following steps:

1. Generate a random backoff number between 0 and a minimum Contention Window (CWmin).
2. Wait until the channel is free for a DIFS interval.
3. If the channel is still free begin to decrement the random backoff number, for every *slot time* (20 µs) the channel remains free.
4. If the channel becomes busy, such as another station getting to 0 before your station, the decrement stops and Steps 2 through 4 are repeated.
5. If the channel remains free until the random backoff number reaches 0 the frame may be sent.

Figure 6-4 Distributed Coordination Function Example

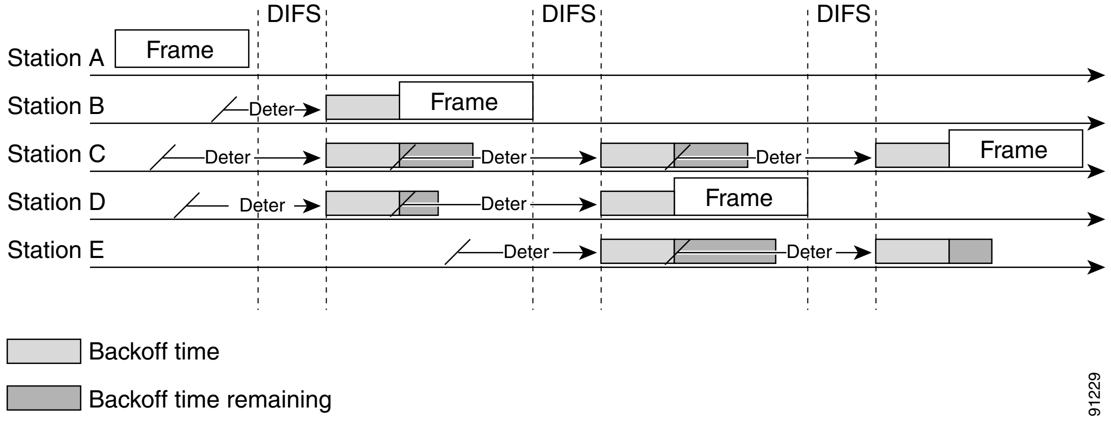


Figure 6-4 shows a simplified example of how the DCF process works. In this simplified DCF process, no acknowledgements are shown and no fragmentation occurs.

The DCF steps illustrated in Figure 6-4 work as follows:

1. Station A successfully sends a frame, and three other stations also wish to send frames but must defer to Station A's traffic.
2. Upon Station A completing the transmission, all the stations must still defer for the DIFS. Once the DIFS is complete, stations wishing to send a frame can begin to decrement the backoff counter, once every slot time, and may send their frame.
3. Station B's backoff counter reaches zero before Stations C and D, and therefore Station B begins transmitting its frame.
4. Once Station C and D detect that Station B is transmitting, they must stop decrementing the backoff counters and defer until the frame is transmitted and a DIFS has passed.
5. During the time that Station B is transmitting a frame, Station E gets a frame to transmit, but as Station B is sending a frame it must defer in the same manner as Stations C and D
6. Once Station B completes transmission and the DIFS has passed, stations with frames to send begin to decrement the backoff counters. In this case, Station D's backoff counter reaches zero first and it begins transmission of its frame.
7. The process continues as traffic arrives on different stations.

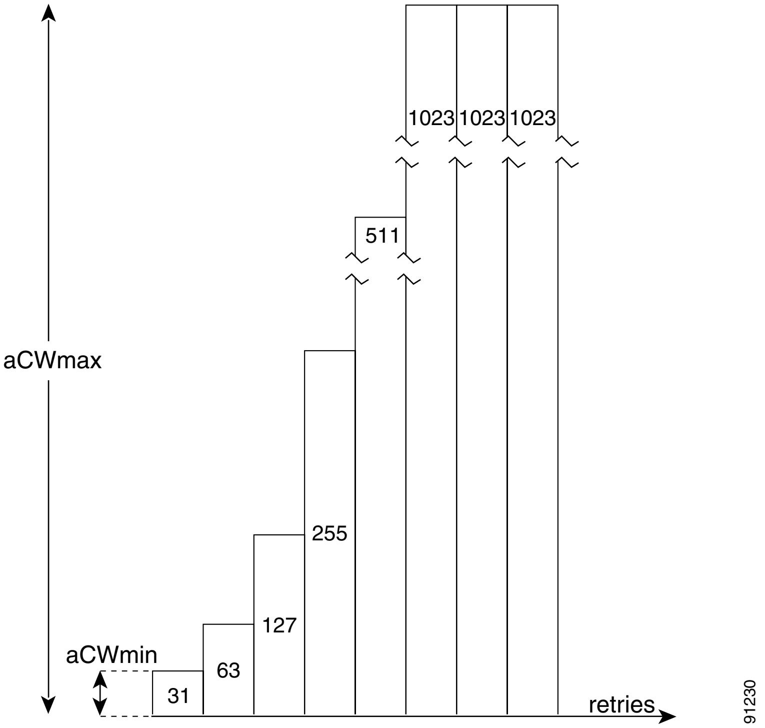
CWmin, CWmax, and Retries

DCF uses a Contention Window (CW) to control the size of the random backoff. The contention window is defined by two parameters:

- aCWmin
- aCWmax

The random number used in the random backoff is initially a number between 0 and aCWmin. If the initial random backoff expires without successfully sending the frame, the station or AP increments the retry counter, and doubles the value random backoff window size. This doubling in size continues until the size equals aCWmax. The retries continue until the maximum retries or Time To Live (TTL) is reached. This process of doubling the backoff window is often referred to as a *binary exponential backoff*, and is illustrated in Figure 6-5.

Figure 6-5 Growth in Random Backoff Range with Retries



Wi-Fi Multimedia

This section discusses two 802.11e implementations for:\

- WMM 802.11a EDCF-based QoS
- QoS Advanced Features for WLAN Infrastructure

Figure 6-7 shows the principle behind different CWmin values per traffic classification. All traffic waits the same DIFS, but the CWmin value used to generate the random backoff number depends upon the traffic classification. High priority traffic has a small CWmin value, giving as short random backoff, whereas best effort traffic has a large CWmin value that on average gives a large random backoff number.

Wi-Fi Multimedia 802.11e based QoS Implementation

Wi-Fi Multimedia (WMM) is a Wi-Fi alliance certification of support for a set of features from the 802.11e draft. This certification is for both clients and APs, and certifies the operation of WMM. WMM is primarily the implementation of the EDCA component of 802.11e. Additional Wi-Fi certifications are planned and will address other components of the 802.11e draft.

WMM Classification

WMM uses the 802.1d classification scheme developed by the IEEE. This has eight different priorities, which WMM maps to four different Access Categories: AC_BK, AC_BE, AC_VI, and AC_VO. These Access Categories map to the four queues required by a WMM device, as shown in Figure 6-3.

Table 6-3 802.1d Priority Mapping to Access Categories

Priority	802.1 Priority (=User Priority)	802.1d Designation	Access Category	WMM Designation
Highest	1	BK Background	AC_BK	Background
	2	-Spare		
Lowest	0	BE Best Effort		
	3	EE Excellent Effort	AC_BE	Best Effort
	4	CL Control Load		
	5	VI Video <100ms	AC_VI	Video
	6	VO Voice <10ms		
	7	NC Network Control “must get there”	AC_VO	Voice

Figure 6-6 WMM Frame Format

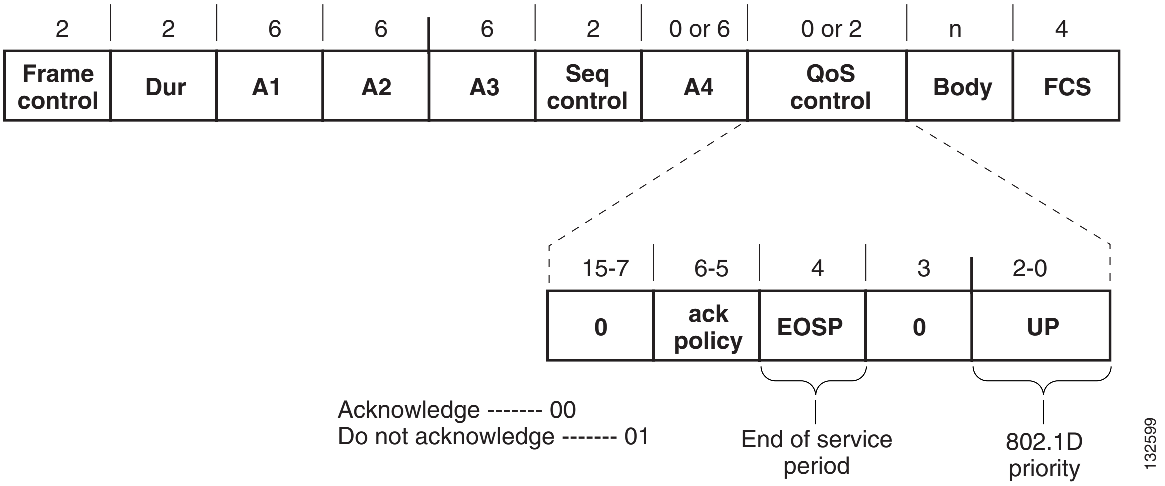


Figure 6-6 shows the 802.11e data frame format. Note that even though WMM maps the eight 802.1D classifications to four access categories, the 802.11D classification is sent in the frame.

WMM Queues

Figure 6-7 WMM Queues

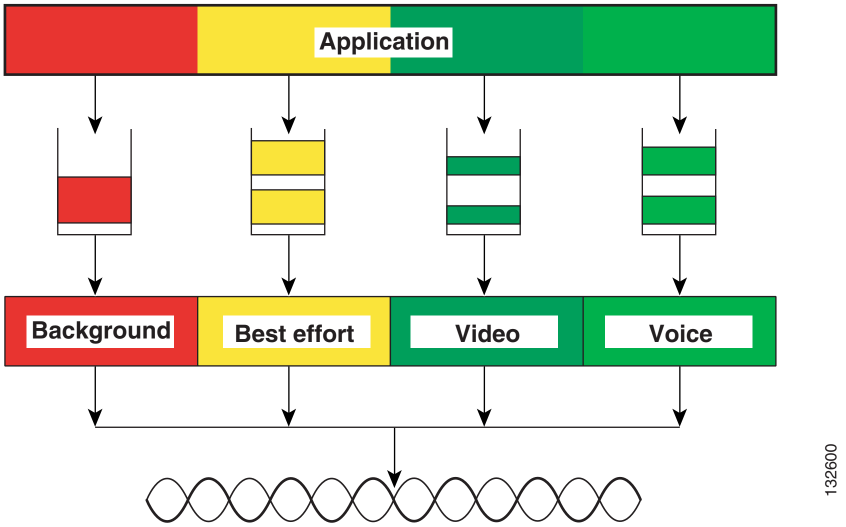


Figure 6-7 shows the queuing performed on a WMM client or AP. There are four separate queues, one for each of the Access Categories. Each of these queues contends for the Wireless channel in a similar manner to the DCF mechanism discussed earlier, with each of the queues using different, Interframe Space, CWmin, and CWmax values. If more than one frame from different Access Categories collide internally, the frame with the higher priority is sent, and the lower priority frame adjusts its backoff parameters as though it had collided with a frame external to the queuing mechanism.

This system is called *Enhanced Distributed Channel Access –EDCA*.

To see the impact of classification, and different access category queues, use the **show controllers dot11Radio *x*** command to view the queue status as shown in Table 6-4. Note that there is a Multicast Queue as well as the Access Categories. This queue is used to hold multicast traffic that is being held due to the power save requests of clients.

Table 6-4 Controllers dot11Radio

```
show controllers dot11Radio 0
...
            Count  Quota  Max  Allow  Count  Quota
Uplink      0      0      0    1      0      0
Voice       0      0      0    1      0      0
Video       0      0      0    1      0      0
BestEffort  0      0      0    1      0      0
Multicast   0      0      0    1      0      0
Backgrouond 0      0      0    1      0      0
```

EDCA

Figure 6-8 EDCA

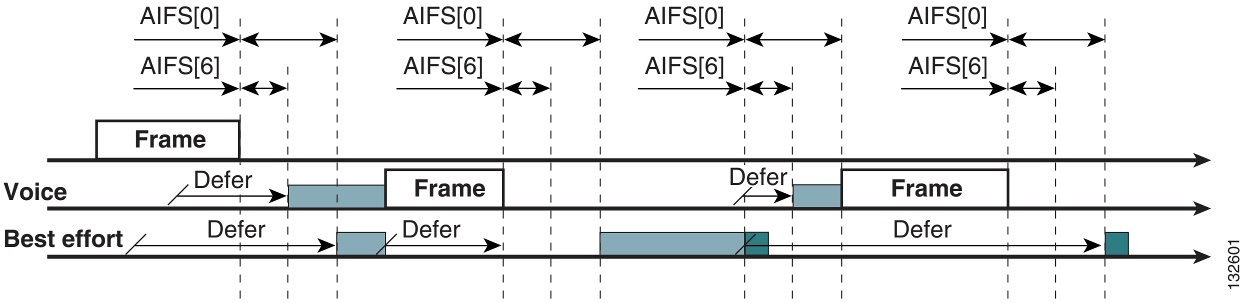
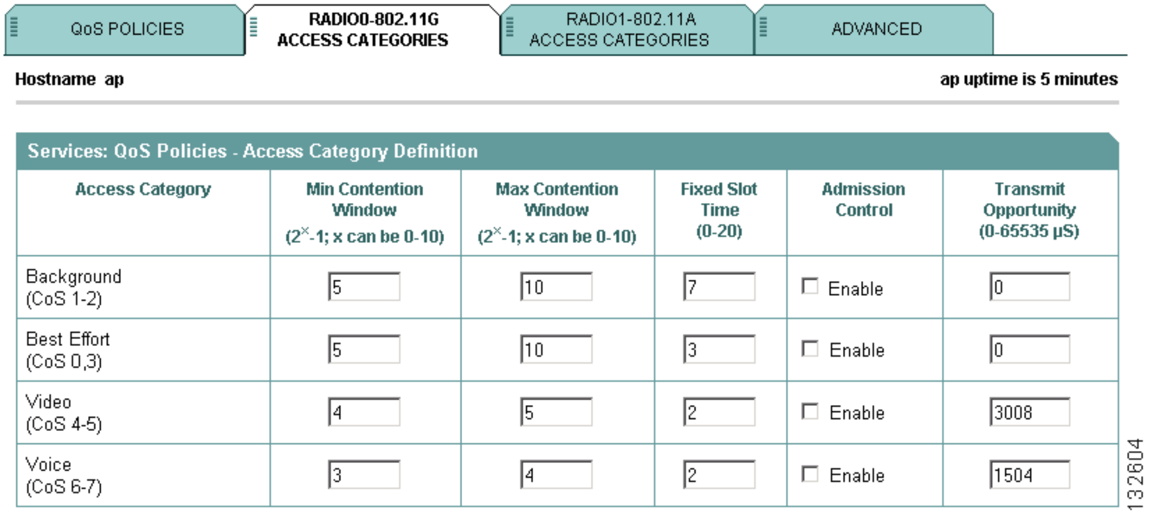


Figure 6-9 Access Categories for 802.11g


QoS POLICIES
RADIO0-802.11G ACCESS CATEGORIES
RADIO1-802.11A ACCESS CATEGORIES
ADVANCED
132604

Hostname ap

ap uptime is 5 minutes

Services: QoS Policies - Access Category Definition

Access Category	Min Contention Window (2^x-1; x can be 0-10)	Max Contention Window (2^x-1; x can be 0-10)	Fixed Slot Time (0-20)	Admission Control	Transmit Opportunity (0-65535 µS)
Background (CoS 1-2)	5	10	7	□ Enable	0
Best Effort (CoS 0,3)	5	10	3	□ Enable	0
Video (CoS 4-5)	4	5	2	□ Enable	3008
Voice (CoS 6-7)	3	4	2	□ Enable	1504

The process illustrated in Figure 6-8, and using data from Figure 6-9, follows this sequence:

1. While Station X is transmitting its frame three other stations determine that they must send a frame. Each station defers as a frame was already being transmitted, and each station generates a random backoff.
2. As station Voice has a traffic classification of voice, it has an arbitrated interframe space (AIFS) of 2, and uses an initial CWmin of 3, and therefore will have to differ the count down of its random backoff for 2 slot times, and will have a short random backoff value.
3. Best Effort has an AIFS of 3 and a longer random backoff time, as its CWmin value is 5.
4. Voice has the shortest random backoff time, and therefore starts transmitting first. When Voice starts transmitting all other stations defer.
5. Once Voice Station finishes transmitting, all stations wait their AIFS, then begin to decrement the random backoff counters again.
6. Best-effort then completes decrementing its random backoff counter and begins transmission. All other stations defer. This can happen even though there may be voice station waiting to transmit. This shows that best effort traffic is not starved by voice traffic as the random backoff decrementing

process eventually brings the best effort backoff down to similar sizes as high priority traffic, and that the random process might, on occasion, generate a small random backoff number for best effort traffic.

7. The process continues as other traffic enters the system.

The access category settings shown in the following tables, are by default the same for an 802.11a radio, and are based upon formulas defined in WMM, as shown in Table 6-5 and Table 6-6.

Note Table 6-6 refers to the parameter settings on a client, and that they are slightly different from that of on AP. This is to take into account that an AP is expected to have multiple clients, and will therefore need to send frames more often.

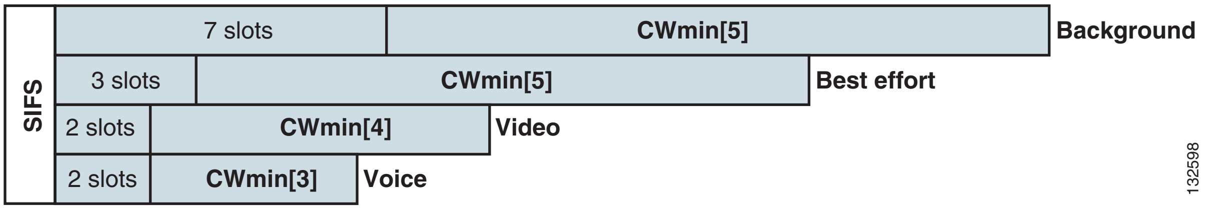
Table 6-5 WMM AP Parameters

AC	CWmin	CWmax	AIFSN	TXOP Limit (802.11b)	TXOP Limit (802.11a/g)
AC_BK	aCWmin	aCWmax	7	0	0
AC_BE	aCWmin	4*(aCQmin+1)-1	3	0	0
AC_VI	(aCWmin+1)/2-1	aCWmin	1	6.016ms	3.008ms
AC_VO	(aCWmin+1)/4-1	(aCWmin+1)/2-1	1	3.264ms	1.504ms

Table 6-6 WMM Station Parameters

Access Category	CWmin	CWmax	AIFSN	TXOP Limit (802.11b)	TXOP Limit (802.11a/g)
AC_BK	aCWmin	aCWmax	7	0	0
AC_BE	aCWmin	4*(aCQmin+1)-1	3	0	0
AC_VI	(aCWmin+1)/2-1	aCWmin	2	6.016ms	3.008ms
AC_VO	(aCWmin+1)/4-1	(aCWmin+1)/2-1	2	3.264ms	1.504ms

Figure 6-10 AIFSs and CWmin for Different Access Categories



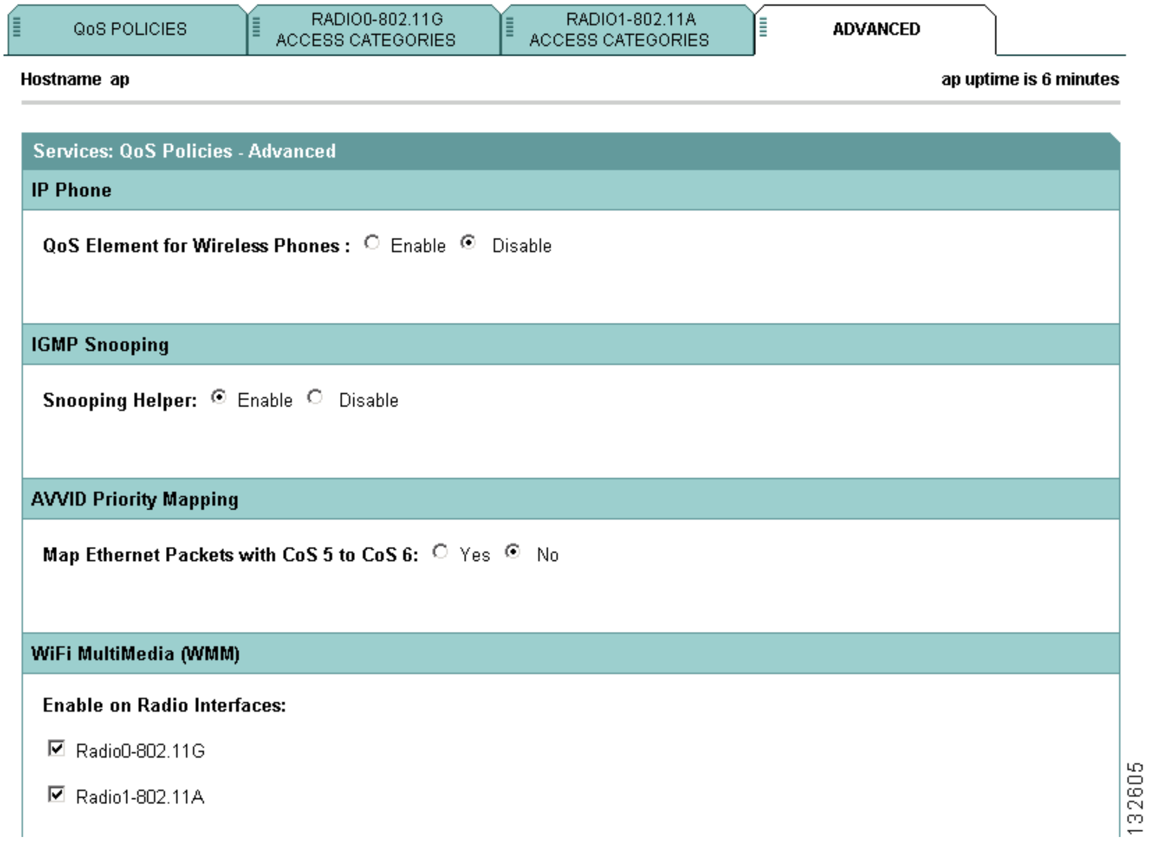
The overall impact of the different AIFS, CWmin and CWmax values is difficult to show well in timing diagrams, as their impact is more statistical in nature. It is simpler to compare the AIFS and the size of the random backoff windows, as shown in Figure 6-10.

If we compare Voice and Background as examples, these traffic categories have CWmin values of 3 (7) and 5 (31), and AIFS of 2 and 7 respectively. This an average delay of 5 slot times before sending a Voice frame, and an average of 22 slot times for Background frame. From this it can be seen that Voice frames are statistically much more likely to be sent before Background frames.

QoS Advanced Features for WLAN Infrastructure

Figure 6-11 shows the advanced configuration page on the Cisco IOS AP, this has a number of configuration options that are used depending upon the particular QoS deployment.

Figure 6-11 Enabling QoS Advanced Features on the AP


QoS POLICIES
RADIO0-802.11G ACCESS CATEGORIES
RADIO1-802.11A ACCESS CATEGORIES
ADVANCED
132605

Hostname ap

ap uptime is 6 minutes

Services: QoS Policies - Advanced

IP Phone

QoS Element for Wireless Phones : ○ Enable ● Disable

IGMP Snooping

Snooping Helper: ● Enable ○ Disable

AVVID Priority Mapping

Map Ethernet Packets with CoS 5 to CoS 6: ○ Yes ● No

WiFi MultiMedia (WMM)

Enable on Radio Interfaces:

☑ Radio0-802.11G

☑ Radio1-802.11A

IP Phone

The “QoS Element for Wireless Phones” enables the AP to include a QBSS element in its beacons. WLAN clients with QoS requirements use these advertised QoS parameters to determine the best AP with which to associate.

Figure 6-7 shows the QBSS Information Element (IE) advertised by a Cisco AP. The Load field indicates the portion of available bandwidth currently used to transport data on that AP.

Table 6-7 Cisco QBSS

1 Octet	1 Octet	4 bytes
Ethernet ID (11)	Length	Load

IGMP Snooping

When Internet Group Membership Protocol (IGMP) snooping is enabled on a switch upstream from the APs, and a client roams from one AP, the client's multicast session may be dropped if there wasn't already a member of that multicast group associated with the new AP. The AP IGMP snooping helper sends a general IGMP query to the network infrastructure on behalf of the client every time the client associates or reassociates to the access point. This allows the IGMP snooping switch to detect the client movement, and forward the multicast traffic to the new AP.

AVVID Priority Mapping

AVVID priority mapping maps Ethernet packets tagged as class of service 5 to class of service 6. This feature enables the AP to apply the Cisco AVVID class of service to voice frames marked with IEEE voice class of service. Cisco AVVID class of service aligns with IEFT classification, that uses the class of service 6 for control packets, order to maintain compatibility between the two difference classification systems the AP converts IEEE to AVVID and AVVID to IEEE.

WiFi MulitMedia

Table 6-8 WMM Parameter Element Field Values

Field		Value
Element ID		221
Length		24
OUI		00:50:f2 (hex)
OUI Type		2
OUI Subtype		1
Version		1
QoS Info Field	Reserved:	Parameter Change Count
Reserved		0
AC Parameters Best Effort		AC Parameters Record AC_BE
AC Parameters Background		AC Parameters Record AC_BK
AC Parameters Video		AC Parameters Record AC_VI
AC Parameters Voice		AC Parameters Record AC_VO

Enabling WiFi Multimedia on radio interfaces enables support for WiFi MultiMedia, makes a number of changes:

- Advertise WMM parameters in the Beacons, shown in Table 6-8. These parameters are also sent or exchanged in probe requests, probe responses, association requests, and association response.
- Control of access categories through the Access Control features shown in Figure 6-9, such as checking an access category, prevents clients from using this Access Category.
- Send, receive, and pass through CoS marking for WMM associated clients, as per the WMM frame format shown in Figure 6-6.

Deploying EDCF on Cisco IOS-based APs

When deploying WLAN QoS on the APs the following should be remembered:

- APs do not classify packets; they prioritize packets based on DSCP value, client type (such as a wireless phone), or the priority value in the 802.1q or 802.1p tag. The APs only support MQC policy-map **set cos** action (i.e the AP), can set or change the CoS value of frames
- APs do not construct internal DSCP values; they only support mapping by assigning IP DSCP, Precedence, or Protocol values to Layer 2 COS values.
- APs carry out EDCF like queuing on the radio egress port only.
- APs only do FIFO queueing on the Ethernet egress port.
- APs support only 802.1Q/P tagged packets.
- APs prioritize the traffic from voice clients, such as Symbol phones, over traffic from other clients when the QoS Element for Wireless Phones feature is enabled.
- APs support:
  - Symbol Technologies, Inc. Extensions (*Symbol*® NetVision handsets only)
  - QoS Basis Service Set (QBSS)—Based on IEEE 802.11e DRAFT version 3.3

In situations when different mechanisms for frame classification my be in use, the classification takes the following priority:

1. *Packets already classified*—When the access point receives packets from a QoS-enabled switch or router that has already classified the packets with non-zero 802.1q/p user_priority values, the access point uses that classification and does not apply other QoS policy rules to the packets. An existing classification takes precedence over all other policies on the access point. Even if you have not configured a QoS policy, the access point always honors tagged 802.1p packets that it receives over the radio interface.
2. *QoS Element for Wireless Phones* setting—If you enable the *QoS Element for Wireless Phones* setting, traffic from voice clients takes priority over other traffic regardless of other policy settings. The *QoS Element for Wireless Phones* setting takes precedence over other policies, second only to previously assigned packet classifications.
3. Policies you create on the access point—QoS Policies that you create and apply to VLANs or to the access point interfaces are third in precedence after previously classified packets and the *QoS Element for Wireless Phones* setting.
4. Default classification for all packets on VLAN—If you set a default classification for all packets on a VLAN, that policy is fourth in the precedence list.

Guidelines for Deploying Wireless QoS

The same rules for Deploying QoS in a wired network apply to deploying QoS in a wireless network. The first and most important guideline in QoS deployment is: *know your traffic*. Know your protocols, your application's sensitivity to delay, and traffic bandwidth. QoS does not create additional bandwidth it simply gives more control of where the bandwidth is allocated.

Throughput

An important consideration in deploying 802.11 QoS is understanding the offered traffic, not only in terms of bit rate, but also in terms of frame size, as 802.11 throughput is sensitive to the frame size of the offered traffic.

Table 6-9 Throughput Compared to Frame Size

	300	**600**	**900**	**1200**	**1500**	**Frame Size (Bytes)**
11g - 54Mbps	11.4	19.2	24.6	28.4	31.4	Throughput bps
11b - 11Mbps	2.2	3.6	4.7	5.4	6	Throughput bps

Table 6-9 shows the impact frame size has upon throughput, as packet size decreases so does throughput.

For example, if an application offering traffic at a rate of 3Mbps was to be deployed on an 11Mbps 802.11b network, but used an average frame size of 300 bytes, no QoS setting on the AP would allow the application to achieve its throughput requirements. This is because 802.11b cannot support the required throughput for that throughput and frame size combination. The same amount of offered traffic, but with a frame size of 1500 bytes does not have this issue.

WLAN Voice and the Cisco 7920

The Cisco 7920 is a Cisco 802.11b VoIP handset, and it's use would be one of the most common reasons for deploying QoS on a WLAN.

Deploying Voice over WLAN infrastructure involves more than simply providing QoS on WLAN. A Voice WLAN, needs to consider site survey coverage requirements, user behavior, roaming requirements, and admission control. This is covered in the *Cisco Wireless IP Phone 7920 Design and Deployment Guide*, which can be found at:

http://www.cisco.com/en/US/products/hw/phones/ps379/products_implementation_design_guide_book09186a00802a029a.html

CHAPTER 7

WLAN Roaming

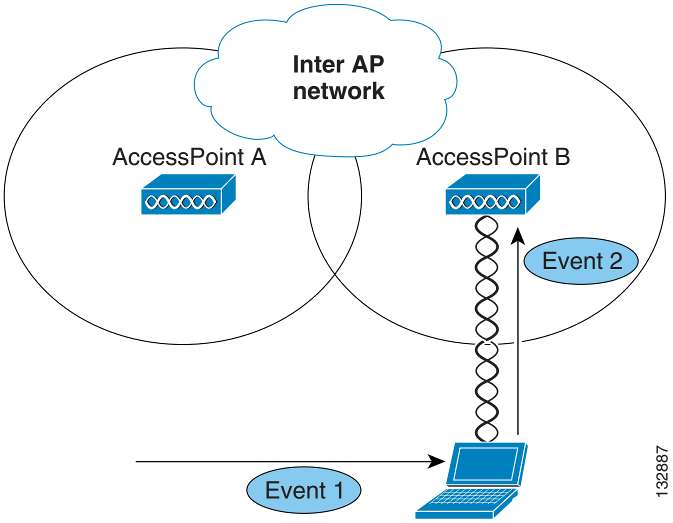
This chapter addresses the WLAN design considerations for WLAN client roaming. It discusses client roaming requirements, Cisco Fast Secure Roaming, Layer 2 and Layer 3 design recommendations.

Roaming Technical Overview

The 802.11 standards define very little about WLAN client roaming, other than the client sends the BSSID of the previous AP to the new AP. The standards do not define what causes a client to roam, and how a client determines which AP to access. Therefore, these discussions of client behavior are specific to Cisco and CCX compatible clients.

A WLAN client roam occurs when a WLAN station moves from one AP to another. Figure 7-1 illustrates the sequence of events associated with a WLAN roam.

Figure 7-1 Sequence of Events for Layer 2 Roam



The arrows in Figure 7-1 indicate the following events:

Event 1 A Client moves from AP "A" coverage area into AP "B" coverage area. As the client moves out of AP "A" range a "Roaming Event" will be triggered (such as Max Retries). Event 1, and the events that cause a client to initiate the roam process are discussed in more detail in Roaming Events, page 7-2.

Event 2 The client then scans all 802.11 channels for alternative APs. In this case, the client discovers AP "B" and re-authenticates and re-associates to it. Event 2, and the process of discovering, evaluating, and roaming to an alternative A Pis covered in the The Roam Process, page 7-5.

The main focus in this chapter is on Events 1 and 2 in Figure 7-1. Events that occur after are part of post-roam actions taken as part of Cisco's proprietary *Inter Access Point Protocol* (IAPP), or the Cisco WLCCP Protocol, which are discussed in Switch Roaming, page 7-6 and WLSM Roaming, page 7-8. It is important to note that roaming is always a client station decision. The client station is responsible for detecting, evaluating, and roaming to an alternative AP.

Roaming Events

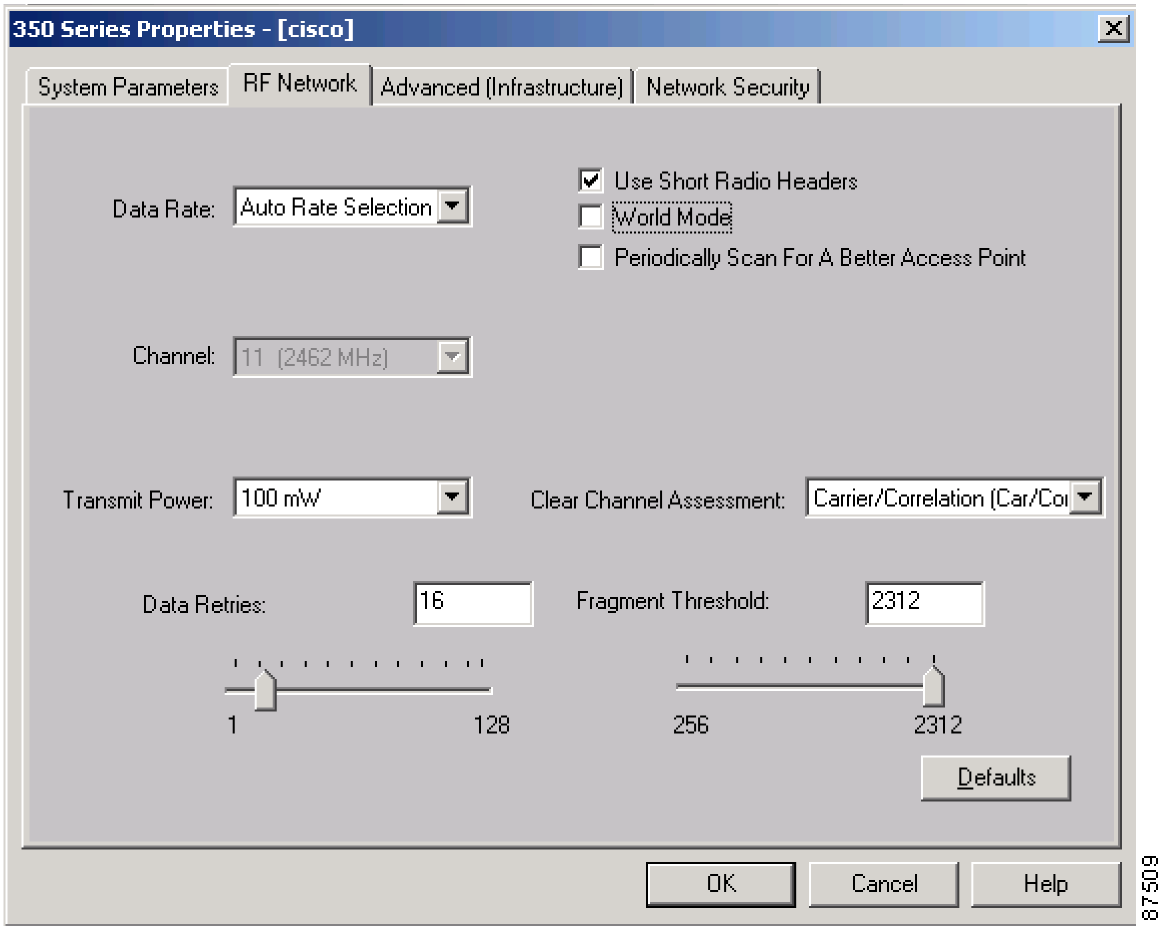
This section details the events that cause a client to roam. The roam process itself is described in The Roam Process, page 7-5. Roaming is always initiated by the client and is caused by one of the following events, each described in subsequent sections:

- Max Data Retry Count Exceeded
- Missed Too Many Beacons
- Data Rate Shift
- Periodic Client Interval
- Initial Client Startup

Max Data Retry Count Exceeded

When a client station retries a packet more than the value entered for *Max Data Retry Count*, the client initiates a roam. The *Max Data Retry Count* defaults to 16, and is configured in the Aironet Client Utility (ACU) under the *RF Network* tab for the currently active profile. A sample screen is shown in Figure 7-2.

Figure 7-2 Setting Max Data Retries in the ACU



Data Rate: Auto Rate Selection

☑ Use Short Radio Headers

☐ World Mode

☐ Periodically Scan For A Better Access Point

Channel: 11 (2462 MHz)

Transmit Power: 100 mW

Clear Channel Assessment: Carrier/Correlation (Car/Co

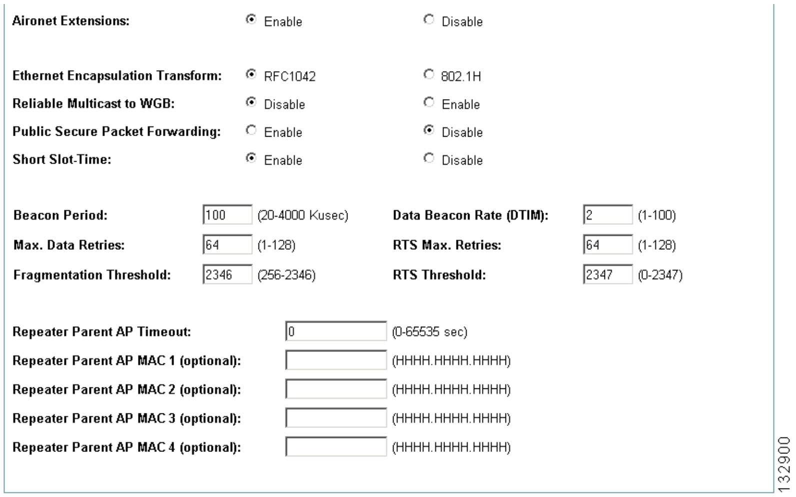
Data Retries: 16 (1 – 128)

Fragment Threshold: 2312 (256 – 2312)

Missed Too Many Beacons

All clients associated with an AP should receive a periodic beacon. By default, APs send a beacon every 100 msec. The beacon period setting on an AP is shown in Figure 7-3.

Figure 7-3 Max Data Retries, Beacon Period and Data Rate Settings



Aironet Extensions:	● Enable	○ Disable
Ethernet Encapsulation Transform:	● RFC1042	○ 802.1H
Reliable Multicast to WGB:	● Disable	○ Enable
Public Secure Packet Forwarding:	○ Enable	● Disable
Short Slot-Time:	● Enable	○ Disable

Beacon Period:	100 (20-4000 Kusec)	Data Beacon Rate (DTIM):	2 (1-100)
Max. Data Retries:	64 (1-128)	RTS Max. Retries:	64 (1-128)
Fragmentation Threshold:	2346 (256-2346)	RTS Threshold:	2347 (0-2347)

Repeater Parent AP Timeout:	0 (0-65535 sec)
Repeater Parent AP MAC 1 (optional):	(HHHH.HHHH.HHHH)
Repeater Parent AP MAC 2 (optional):	(HHHH.HHHH.HHHH)
Repeater Parent AP MAC 3 (optional):	(HHHH.HHHH.HHHH)
Repeater Parent AP MAC 4 (optional):	(HHHH.HHHH.HHHH)

Clients learn the AP’s beacon interval from an element in the beacon. If a client misses eight consecutive beacons, a roaming event is deemed to have occurred and the roam process, detailed in the The Roam Process, page 7-5, is initiated. By continuously monitoring for received beacons, even an otherwise idle client is able to detect a loss of wireless link quality and is able to initiate a roam.

Data Rate Shift

Packets are normally transmitted at the AP’s default rate. The default rate is the highest rate set to *basic* or *yes* on the AP. Configuring a data rate on an AP is shown in Figure 7-3. A rate-shift occurs when a frame is retransmitted three times and RTS/CTS is used to send the last two retransmissions.

Every time a packet must be retransmitted at a lower rate, a count is increased by 3. For each packet successfully transmitted at the default rate, the count is decreased by 1 until it is 0. If the count reaches 12 one of the following occurs:

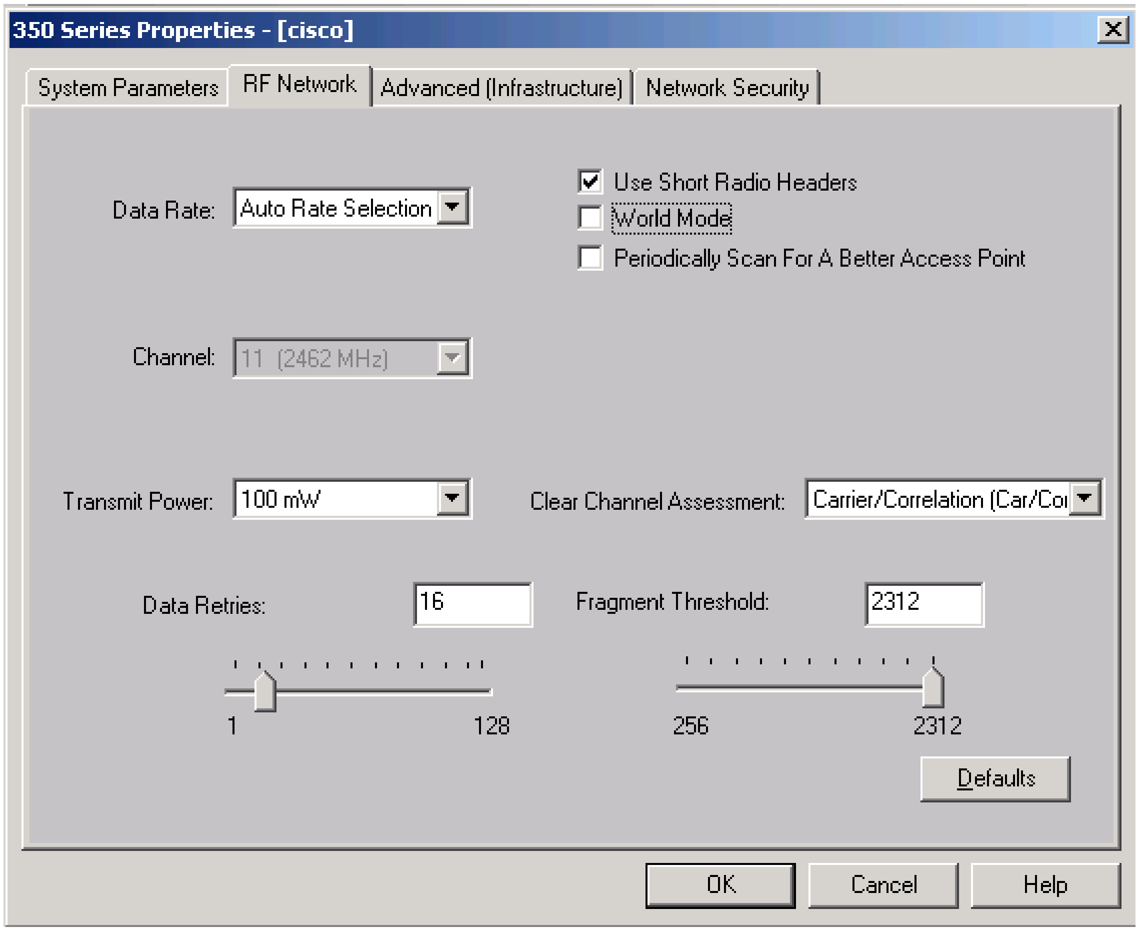
- If the client has not attempted to roam in the last 30 seconds then the roam process as described in the The Roam Process, page 7-5 occurs.
- If the client has already attempted to roam in the last 30 seconds, the data rate for that client is set to the next lower rate.

A client transmitting at less than the default rate increases the data rate back to the next-higher rate after a short time interval, if transmissions are successful.

Periodic Client Interval

If it is configured to do so, the latest version of ACU, client driver, and firmware allow the client to periodically scan for a better AP when its AP signal strength gets low. This capability is configured in the ACU for the selected profile under the *RF Network* tab as shown in Figure 7-4. The periodic scan is a roaming event that initiates the roam process described in The Roam Process, page 7-5.

Figure 7-4 ACU Configuration—Periodic Scan for a Better AP



Data Rate: Auto Rate Selection

☑ Use Short Radio Headers

□ World Mode

□ Periodically Scan For A Better Access Point

Channel: 11 (2462 MHz)

Transmit Power: 100 mW

Clear Channel Assessment: Carrier/Correlation (Car/Co

Data Retries: 16

Fragment Threshold: 2312

Initial Client Startup

When a client starts up it goes through the roam process described in the The Roam Process, page 7-5, to scan for, and associate with the most appropriate AP.

The Roam Process

Roaming Events described the events that can cause a client to decide that it needs to roam. This section addresses the actions taken by a client station when it roams.

When a roaming event occurs the client station scans each 802.11 channel that is valid in the country in which the client is operating. On each channel, the client station sends a probe and waits for a response or beacon from APs on that channel. The probe responses and beacons received from other APs are discarded unless the conditions list in Table 7-1 are met. If the conditions in Table 7-1 are satisfied, then a client roams to a new AP that best meets one of the conditions specified in Table 7-2.

Table 7-1 AP Conditions Required to be Considered as a Roam Target

Client Station with Aironet Extensions Enabled[1]	Client Station without Aironet Extensions
APs signal strength is: • Greater than 20 percent • If 20+ percent weaker than current AP, then absolute signal strength must be at least 50 percent	Unknown—Implementation dependent
If the AP is in repeater mode and is more radio hops from the backbone than the current AP, its signal strength must be more than 20 percent greater than the current AP	Not Applicable—Radio hop information is Cisco proprietary element in beacons
The new AP must not have more than a 10 percent worse transmitter load than the current AP	Not Applicable—AP transmitter load information is Cisco proprietary element in beacons

[1] Probe-responses/beacons must satisfy all conditions.

Table 7-2 Choosing from Eligible Roam Targets

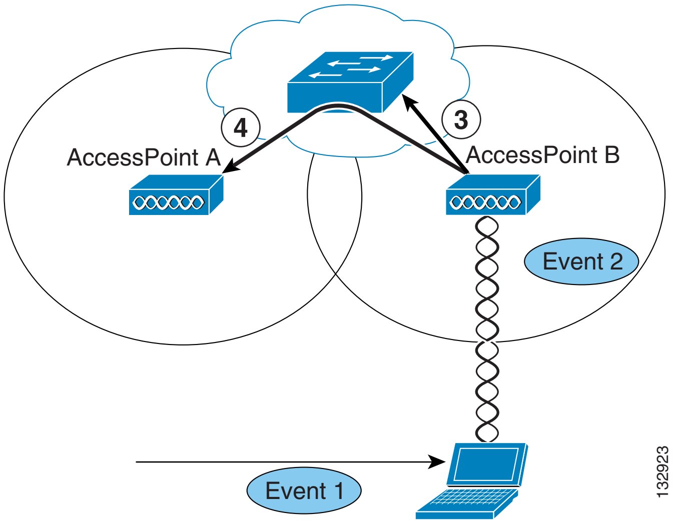
Client Station with Aironet Extensions Enabled (AP Must satisfy Any Condition)	Client Station without Aironet Extensions (AP must Satisfy All Conditions)
Signal strength is more than 20 percent stronger	Unknown—Implementation dependent
Fewer hops to the backbone	Not Applicable—Backbone hops information is Cisco proprietary element in beacons
Four (or more) less clients associated to it	Not Applicable—AP client association load information is Cisco proprietary element in beacons
Twenty+ percent less transmitter load[1]	Not Applicable —AP transmitter load information is Cisco proprietary element in beacons

[1] Transmitter load is an indication of whether an AP radio is busy sending frames.

Switch Roaming

Figure 7-5 shows a schematic examining the roaming events that occur on a switch network behind WLAN APs when a client roams from one AP to another.

Figure 7-5 WLAN client roaming in a switched network



Event 1 AP “B” sends a null MAC multicast using the source address of the client. This updates the Content Addressable Memory (CAM) tables in upstream switches and directs further LAN traffic for the client to AP “B”, and not AP “A”.

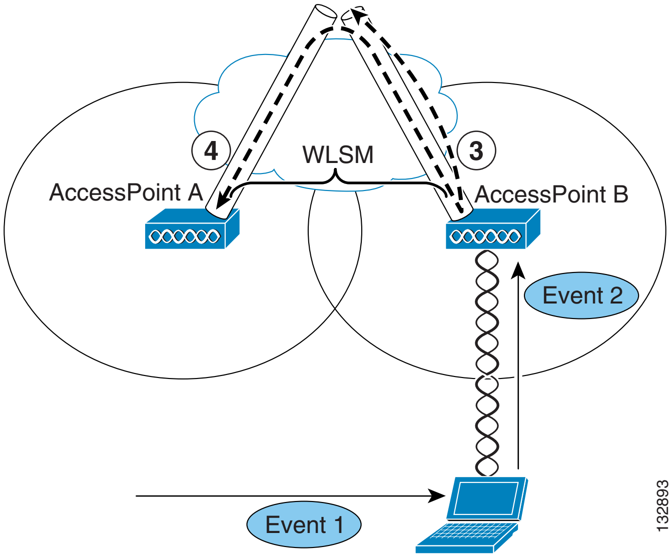
Event 2 AP “B” sends a MAC multicast using its own source address telling the “old” AP that AP “B” now has the client associated to it. AP “A” receives this multicast and removes the client MAC address from its association table.

It should be noted that VLANs are used with APs the messages described about are sent on the same VLAN as the roaming client.

WLSM Roaming

Figure 7-6 shows a schematic examining the roaming events that occur with a switch-based WDS roam.

Figure 7-6 WLSM Client Roaming



Event 1 AP “B” sends a WLLCP message containing the source address of the client updating the WDS of the client’s change of location. The actual updating of the roaming table depends on the mobility group configuration

Event 2 AP “B” sends a WLLCP message, via the WDS, using its own source address telling the “old” AP that AP “B” now has the client associated to it. AP “A” receives this message and removes the client MAC address from its association table.

It should be noted CAM tables do not need to be updated in the WLSM solution, as client traffic is tunneled by through mGRE to the sup720.

Fast Secure Roaming

The Cisco fast secure roaming implementation in Cisco IOS Software release 12.2(11)JA is comprised of two main enhancements:

- Improved 802.11 channel scanning during physical roaming
- Improved re-authentication using advanced key management

The improved 802.11 channel scanning during physical roaming enhancements speeds up all L2 roaming, regardless of the security method used. The improved re-authentication, using advanced key management enhancements, speeds up EAP authentication to provide fast secure roaming.

Improved 802.11 Channel Scanning

Improved channel scanning is enabled by default on Cisco clients and APs and can not be configured. The fast secure roaming enhancements to channel scanning require communication between the client and AP. Improved channel scanning has the following software dependencies:

- Cisco IOS Software release 12.2(11)JA or greater
- Cisco Aironet Client Utility, firmware, and driver software, which is included in Cisco Aironet Client Adaptor Installation Wizard version 1.1 or greater, or third party client cards at the appropriate CCX level for the EAP type to be used.

Channel Scanning Prior to Fast Secure Roaming

Before the release of Cisco IOS Software 12.2(11)JA, Cisco Aironet clients took 37ms to scan for each of the eleven 802.11 channels in the United States, for a total scan time of ~400ms. (Different regulatory domains, or countries, use different channel sets. Eleven are used in the United States.)

For each of the 802.11 channels valid in a specific regulatory domain, the client performs the following steps:

1. Radio hardware physically moves to a specific WLAN channel
2. Client listens to avoid a collision
3. Client transmits a probe frame
4. Client waits for probe responses or beacon frames

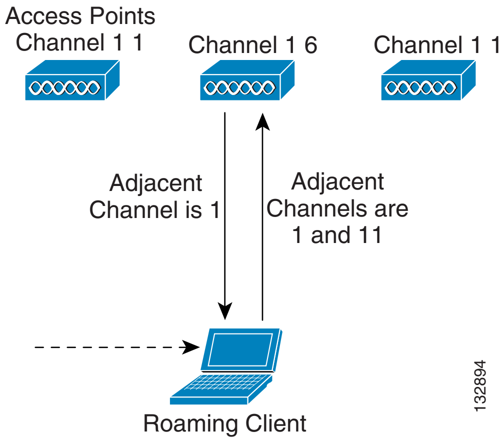
Fast Secure Roaming Channel Scanning Improvements

Improvements to the Cisco channel scanning algorithm that were introduced with Cisco IOS Software release 12.2(11)JA include:

- Clients that are re-associating now communicate information to the new AP, such as the length of time since they lost association with the previous AP, channel number, and SSID.
- Using the information from client associations, an AP builds a list of adjacent APs and the channels these APs were using. If the client reporting an adjacent AP was disassociated from its previous AP for more than 10 seconds its information is not added to the new access point list.
- Access points store a maximum list of 30 adjacent APs. This list is aged out over a one-day period.
- When a client associates to an AP, the associated AP sends the adjacent access point list to the client as a directed unicast packet.

The communication between client and AP is shown in Figure 7-7.

Figure 7-7 Client and Access Point Communication During Association



When a client needs to roam, it uses the adjacent access point list it received from its current AP to reduce the number of channels it needs to scan. How the client uses the adjacent access point list depends upon how busy the client is. There are three types of client roams:

- Normal Roam: The client has not sent or received a unicast packet in the last 500ms.
  - The client does not use the adjacent AP list obtained from the previous AP. Instead it scans all channels valid for the operating regulatory domain.
- Fast Roam: The client has sent or received a unicast packet in the last 500ms.
  - The client scans the channels on which it has been told there is an adjacent AP.
  - If no new APs are found after scanning the adjacent access point list, the client reverts to scanning all channels.
  - The client limits its scan time to 75ms if it is able to find at least one better access point.
- Very Fast Roam: the client has sent or received a unicast packet in the last 500ms, and the client is contributing a non-zero percentage to the load of the cell.
  - Identical to a Fast Roam except the scan is ended as soon as a better access point is found.

If the client did not receive an adjacent access point list from its previous AP, and it wants to fast roam or very fast roam, then it will use the list of channels on which APs were found during its last full scan.

Improved Cisco EAP Authentication

Besides fast 802.11 channel scanning, the fast secure roaming feature provides a fast rekey capability for clients using EAP/802.1x authentication protocols.

Improved EAP authentication introduces the new CCKM protocol that is a component of the Cisco Wireless Security Suite.

EAP Authentication Prior to Fast Secure Roaming

A Cisco LEAP client using Cisco IOS Software version 12.2(8)JA or earlier needs to perform a full Cisco LEAP re-authentication each time it roams. A Cisco LEAP re-authentication requires:

- A minimum of 100ms

- An average of ~600ms
- Up to 1.2seconds +

The time frames above are in addition to the channel-scanning portion of the L2 roam. Cisco LEAP authentication takes this much time because it requires three round trips to a Remote Authentication Dial-In User Service (RADIUS) server using the following process:

Step 1 Client sends identity, Cisco Secure Access Control Server (ACS) or RADIUS Server sends challenge

Step 2 Client sends challenge response, Cisco Secure ACS sends success

Step 3 Client sends challenge, Cisco Secure ACS sends challenge response

In addition to network transit times, each of these round trip transactions requires time-consuming cryptographic calculations, hence the total times quoted above.

Improved Re-authentication Using Fast Secure Roaming Advanced Key Management

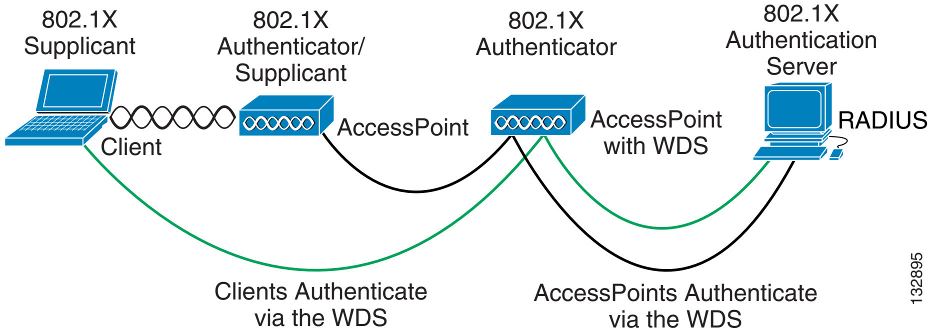
Industry standards such as Wi-Fi Protected Access and 802.11i require 802.1x and also introduce a new key hierarchy to WLAN security. Cisco fast secure roaming is based on this new key hierarchy. Cisco fast secure roaming is a WDS feature.

Cisco fast secure roaming requires 802.1x authentication of APs and clients to a RADIUS server. This authentication uses either a dedicated RADIUS server or the local authentication service running on a Cisco Aironet AP.

About Wireless Domain Services

Wireless Domain Services act as a central authentication entity that supports a fast client rekey rather than requiring a full RADIUS re-authentication each time the client roams. All APs and clients in a WDS domain 802.1x authenticate to a RADIUS server via the WDS that performs the role of 802.1x authenticator. Because all clients and APs authenticate via the WDS, the WDS is able to establish shared keys between itself and every other entity in the WDS domain. These shared keys enable CCKM fast secure roaming. Figure 7-8 illustrates APs and clients authenticating to WDS.

Figure 7-8 Access Points and Clients Authenticating to WDS



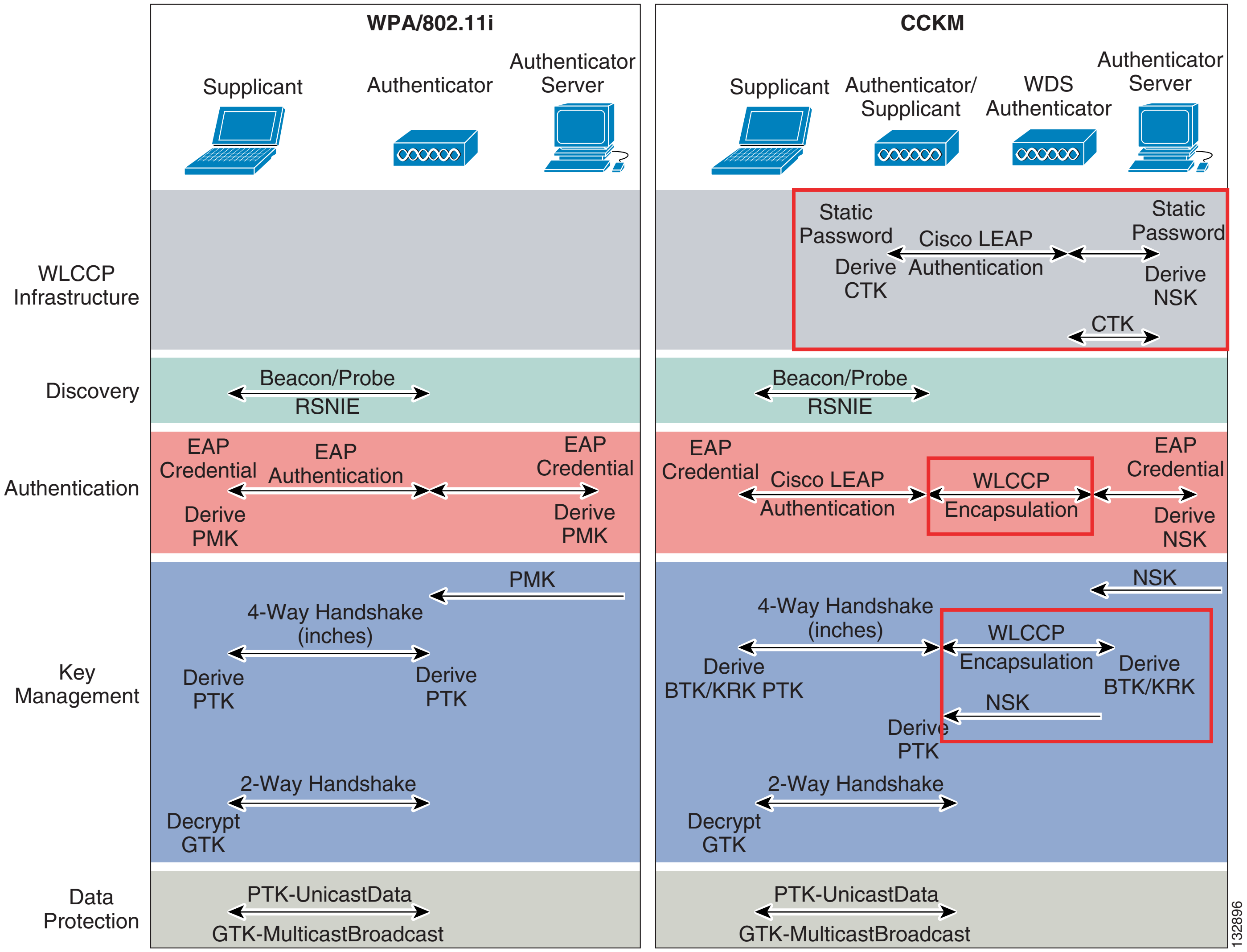
At least one WDS is required per WDS domain. The CCKM architecture supports WDS redundancy via a MAC-layer multicast primary WDS election process, on a Layer 2 WDS domain, or a Hot Standby protocol between WLSMs on switch based WDS.

Comparing Cisco Fast Secure Roaming with 802.11i or WPA Security Protocols

While the CCKM protocol is very closely aligned to the 802.11i and WPA security specifications, it adds additional steps to perform fast secure roaming. Currently, 802.11i and WPA have no equivalent fast secure roaming capability.

Cisco APs support both WPA and CCKM concurrently. However, only CCKM clients can perform fast secure roaming. Figure 7-9 provides a high-level overview of the differences between 802.11i or WPA key management schemes and CCKM. The additional steps performed only during initial client authentication by CCKM are circled. CCKM derives different, additional keys and introduces WDS between the APs and the RADIUS server.

Figure 7-9 Comparing CCKM Initial Key Establishment with Industry Standard WPA/802.11i Key Management



Fast Secure Roaming Stages

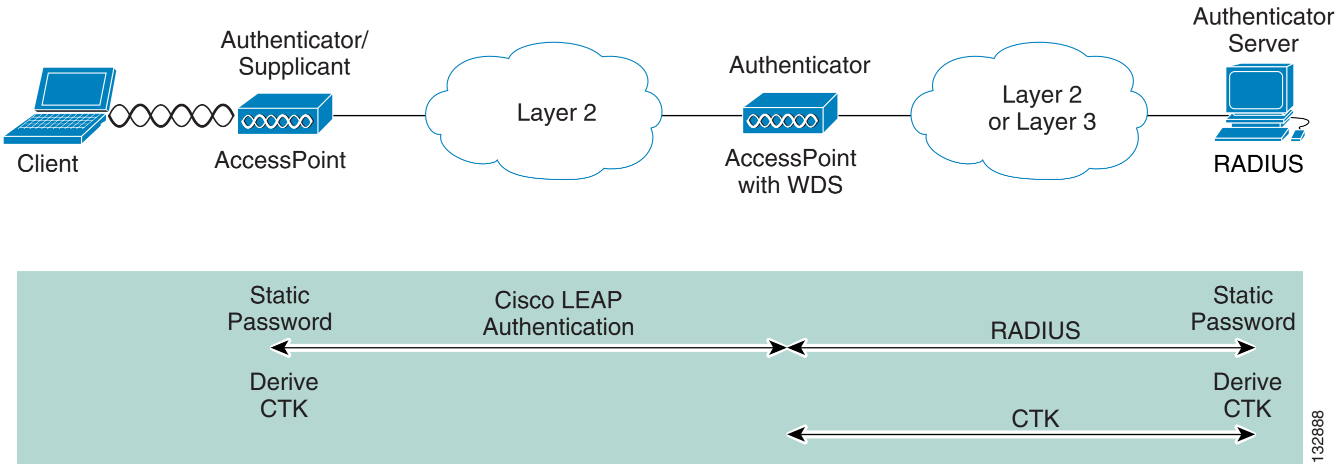
There are three stages in Cisco fast secure roaming:

1. *Infrastructure authentication*—All of the APs in a L2 domain 802.1x authenticate, via the WDS, to a RADIUS server.
2. *Initial authentication*—When a WLAN client first associates to an AP in a new WDS domain, it performs a full 802.1x authentication, via the WDS, to the RADIUS server. This initial authentication has the same latency characteristics as non-CCKM (EAP) authentication. Fast secure roaming applies when the client moves to subsequent APs in the same WDS domain.
3. *Fast secure roaming*—When a client roams to another AP in the same WDS domain, it uses CCKM to perform fast rekeying, without contacting the RADIUS server.

Infrastructure Authentication

During infrastructure authentication, all Cisco Aironet APs, including any that are running WDS, authenticate using Cisco LEAP7 via the WDS, to a RADIUS server as shown in Figure 7-10.

Figure 7-10 Infrastructure Authentication Phase



The AP advertises its security capabilities via the Robust Security Network Information Element (RSNIE) in the AP's beacons and probe responses.

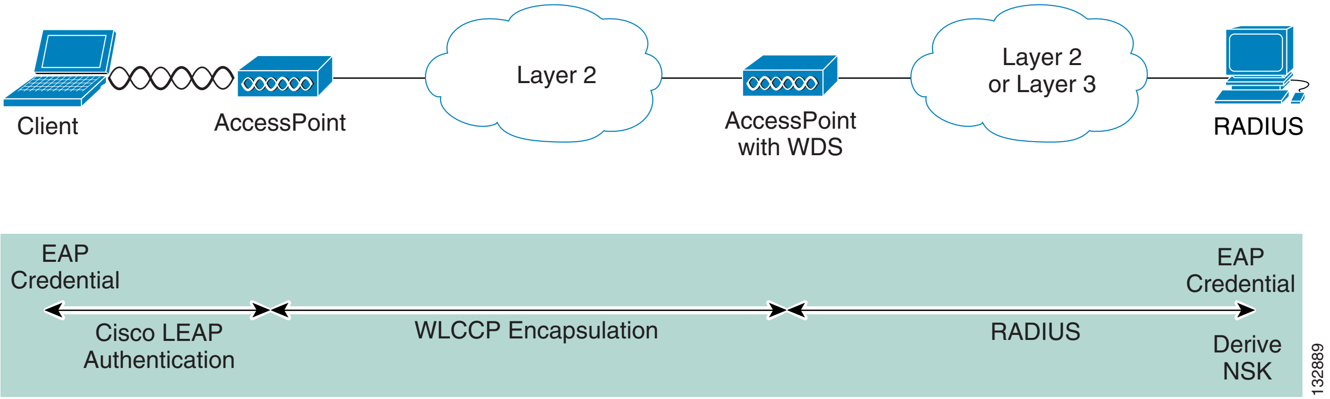
CCKM capability is communicated by a MAC organizationally unique identifier (OUI) value of 00:40:96 and a type value of 0 in the Authenticated Key Management (AKM) suite selector of the RSNIE.

Initial Authentication — Authentication Stage

In CCKM, 802.1x EAP authentication is split between the AP to which the client is associated and the WDS. The AP the client is authenticating to blocks all client data traffic until EAP authentication is complete according to the standard authentication process. Instead of communicating directly with the RADIUS server to perform the EAP authentication, the AP puts a wireless LAN context control protocol (WLCCP) header on the packets, and sends them to the WDS. The WDS communicates with the RADIUS server to complete the EAP authentication.

A network session key (NSK) is mutually derived on the RADIUS server and the client following successful authentication, as shown in Figure 7-11.

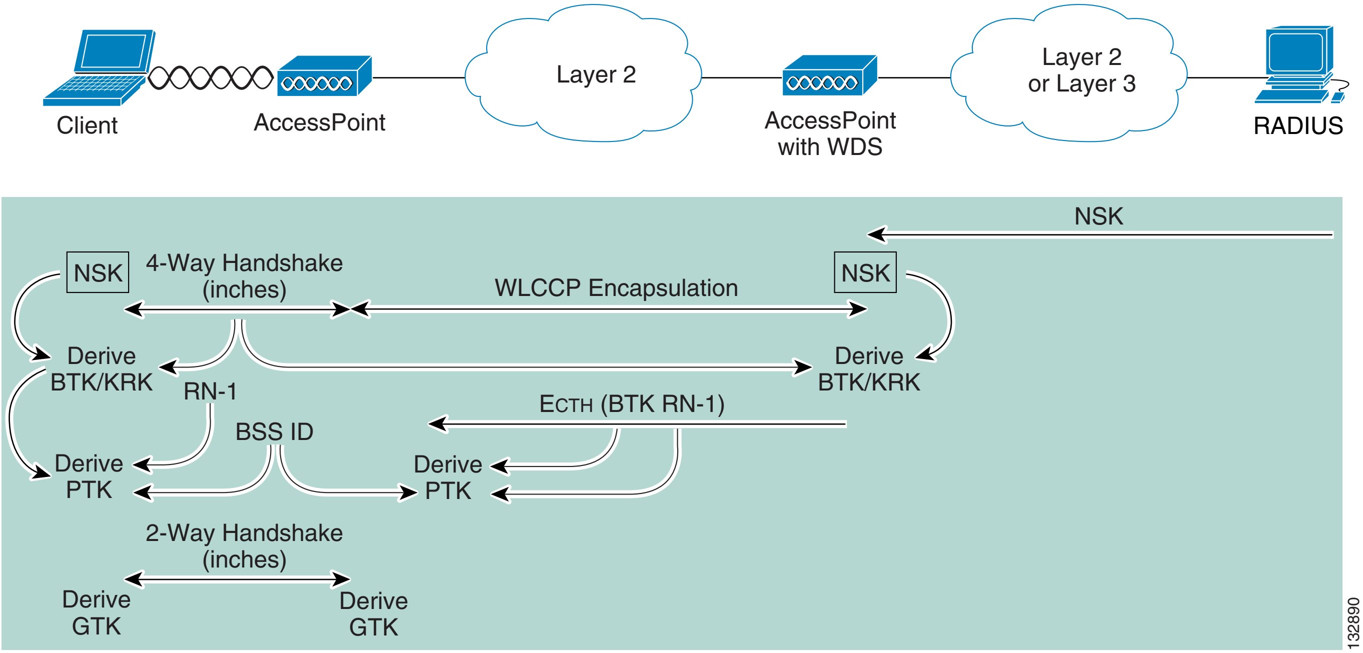
Figure 7-11 Initial Authentication



Initial Authentication—Key Management Stage

In the key management stage, the process for CCKM authentication differs significantly from WPA/802.11i authentication. In this stage, an additional key—the base transient key (BTK)—is established on the WDS. In the CCKM scheme, the BTK is used for fast secure roaming. For WPA/802.11i, the BTK does not exist and a full re-authentication is required for roaming WPA/802.11i clients, as shown in Figure 7-12.

Figure 7-12 Initial Authentication - Key Management Stage



For CCKM clients, the RADIUS server forwards the NSK it derived from the EAP authentication process to the WDS, because from the RADIUS server's viewpoint, the WDS was the 802.1x authenticator. The NSK is used as the basis for deriving all subsequent keys for the lifetime of the client's association with this extended basic service set (EBSS), or until the RADIUS server's rekey interval changes it.

The WDS and the client derive a BTK and a key request key (KRK) by combining the NSK with random numbers (nonces) obtained via a process known as the four-way handshake. The four-way handshake appears to the client to be between the client and the AP it is authenticating to, but the AP puts a WLCCP header on the frames in the four-way handshake, and forwards them to the WDS.

After the four-way handshake is complete, WDS forwards the BTK, and a rekey number (RN) to the AP to which the client is authenticating (since this is the initial authentication the WDS sets the RN to one). The AP the client is authenticating to uses the BTK, RN, and basic service set identifier (BSSID) to derive a pair wise transient key (PTK) which includes a shared session key for unicast traffic.

After the PTK has been successfully derived, the AP sends the group transient key (GTK) that is used for multicast and broadcast traffic to the client, encrypted by an element of the PTK. The process of sending the GTK to the client is called the two-way handshake. The BTK and KRK are used when the client roams to quickly establish a new PTK.

Fast Secure Roaming

The third stage, fast secure roaming, occurs after the client has performed its initial EAP authentication. Any subsequent roams to an AP in the same L2 domain will utilize the preestablished key hierarchy to perform a very fast rekey.

Comparing a WPA/802.11i Roam with a CCKM Roam

The advantage of CCKM becomes apparent when the WLAN client roams. In Figure 7-13, the roaming WPA client is shown completing a re-authentication, including 802.1x re-authentication to a central RADIUS server. In contrast, the CCKM client sends a single reassociate-request frame to the AP, which sends a single frame to a local WDS and receives a single frame reply. Table 7-3 compares the process of re-establishing a CCKM roam with industry standard key management.

Figure 7-13 Comparing a CCKM Roam Establishment with Industry Standard

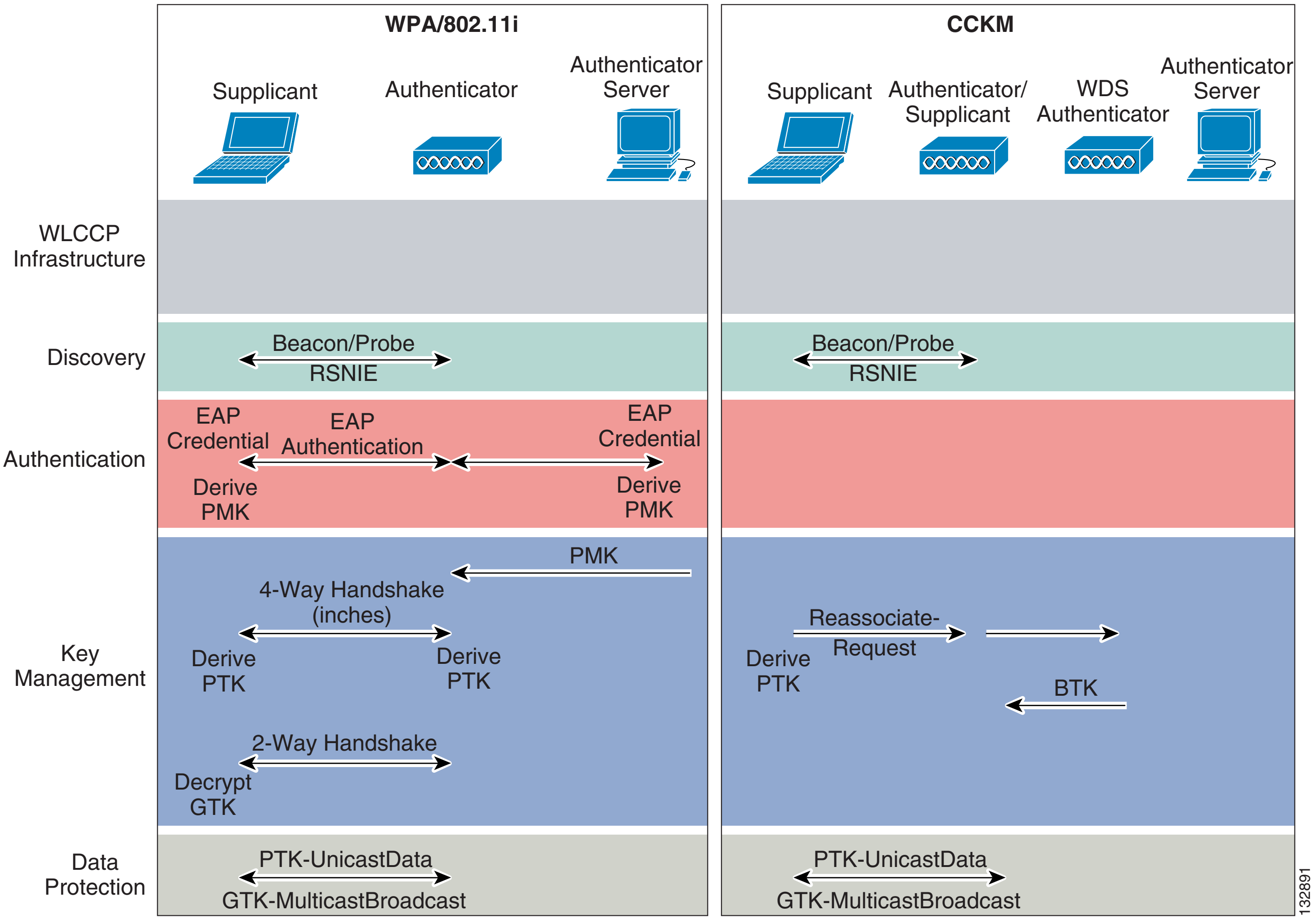


Table 7-3 Comparing a CCKM Roam Establishment with Industry Standard Key Management

WPA/802.11i	Cisco CCKM
When a WPA/802.11i client roams, it completes a full re-authentication, just as it did in the initial authentication. This includes: • A full Cisco LEAP re-authentication with a central RADIUS server • The complete four-way handshake to derive the PTK • The complete two-way handshake to determine the GTK	When a CCKM client roams, it sends a reassociate request to its new AP. • The new AP forwards the reassociate request to the WDS • The WDS sends the new AP the client's BTK • The new AP and the client mutually derive a new PTK • The GTK, encrypted by the PTK, is sent to the client

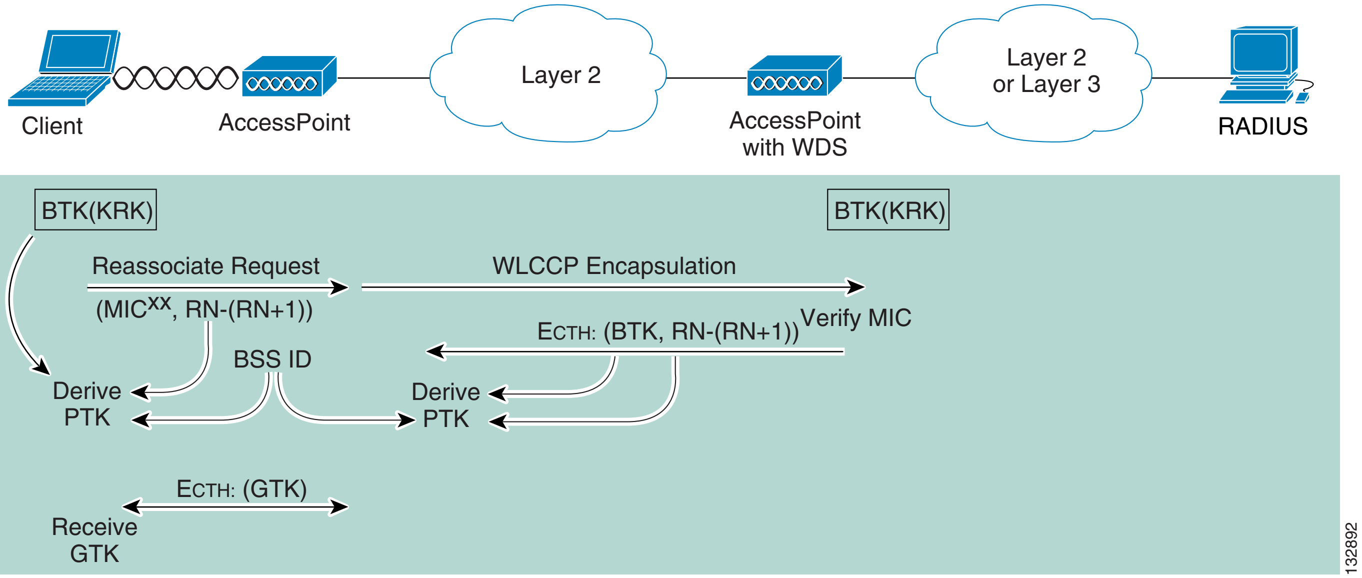
When a CCKM client roams, it sends a re-association request message to the new AP. The re-association request includes:

- A message integrity check (MIC) using the KRK
- A sequentially incrementing RN

Immediately after sending the re-association request, the client is able to calculate its next PTK. It does this by performing a cryptographic hash of the BTK, the RN, and the BSSID. Figure 7-14 shows the CCKM key management phase in more detail.

The AP passes the re-association request to the WDS by encapsulating it in the WLCCP protocol. The WDS verifies the MIC. The WDS then encrypts the BTK and the RN with the CTK shared by the WDS and the new AP, and passes the encrypted message to the new AP. The new AP then hashes the BTK, RN and BSSID to calculate the same new PTK as the client. After the PTK has been mutually derived by the AP and the client, the AP uses an element of the PTK to encrypt the GTK. The AP then passes the GTK to the client.

Figure 7-14 CCKM Fast Rekey



IP Multicast in a Wireless LAN

This chapter describes the configurations needed to control IP Multicast traffic over a WLAN.

For information about IP multicast theory, deployment, and configuration, please see one of the many multicast documents including: *IPmc SRND: Overview Chapter IP Multicast Overview.*

Note This chapter uses MoH and IP/TV in the examples. It does not, however, provide configurations and designs for MoH and IP/TV. Also, other types of IP multicast implementations, such as IP multicast for financial deployments, are not covered.

Multicast WLAN Deployment Recommendations

By default, IP multicast traffic is permitted to stream across a WLAN. However, because WLANs use shared bandwidth, certain measures should be taken to prevent saturation of the available bandwidth. If IP multicast traffic is not required on the wireless network, it is recommended that a boundary be configured to block the multicast traffic. The best place to control IP Multicast traffic is on the routers and switches that connect to the APs and bridges.

Note Filters on the AP and bridge do not provide the flexibility needed for true multicast control.

If IP Multicast is to be deployed and streamed across the wireless network, then the following recommendations should be implemented:

- Prevent unwanted multicast traffic from being sent on the air interface.
  - Place the WLAN in its own subnet.
  - Control which multicast groups are allowed by implementing multicast boundaries on the egress Layer 3 interface connecting to the VLAN or interface to the AP or bridge.
- To gain the highest AP/bridge performance for multicast traffic and data traffic, configure the APs and bridges to run at the highest possible fixed data rate. This removes the requirement for multicast to clock out at a slower rate, which can impact the range of the AP/bridge and must be taken into account in the site survey.
- If multicast reliability is a problem (seen as dropped packets), ignore the preceding recommendation and use a slower data rate (base rate) for multicast. This gives the multicast a better signal-to-noise ratio and can reduce the number of dropped packets.

- Test the multicast application for suitability in the WLAN environment. Determine the application and user performance effects when packet loss is higher than that seen on wired networks.

IP Multicast WLAN Configuration

The **ip multicast boundary** command configures an administratively scoped boundary on an interface for multicast group addresses found in the range defined by an access list. No multicast packets are allowed to flow across the boundary from either direction, except those packets explicitly allowed by the access list.

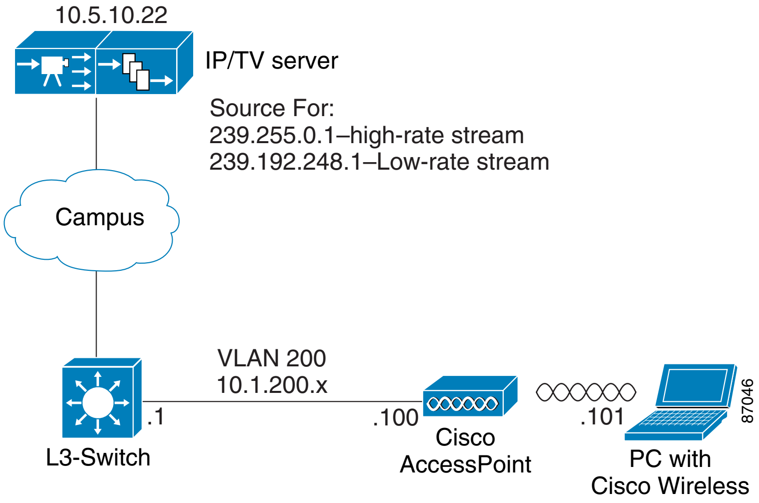
Controlling IP Multicast in a WLAN with APs

Figure 8-1 shows the topology for a WLAN using an AP. The IP multicast source is the IP/TV server (10.5.10.22). There are two multicast streams being sourced from the IP/TV server.

- 239.255.0.1 is a high-rate (1.4 Mbps) video stream.
- 239.192.248.1 is a low-rate (100 Kbps) video stream.

The low-rate stream is allowed and the high-rate stream is disallowed on the WLAN link. A multicast boundary is used to control multicast forwarding and IGMP packets.

Figure 8-1 Testbed for Wireless LAN using an Access Point



In this configuration:

- L3-SWITCH connects to the campus network and the Cisco Access Point (10.1.200.100).
- The VLAN 200 interface on L3-SWITCH has the IP address of 10.1.200.1 and is the interface that provides the boundary for IP multicast.
- The laptop computer (10.1.200.101) has a Cisco PC Card and is running the IP/TV Viewer software.

Below is the configuration is for L3-SWITCH.

```
interface Vlan200
 description WLAN VLAN
 ip address 10.1.200.1 255.255.255.0
 ip pim sparse-mode                          Enables PIM on the interface.
 ip multicast boundary IPMC-WLAN             Boundary refers to named ACL "IPMC-WLAN" and controls
!                                            multicast forwarding AND IGMP packets.
ip access-list standard IPMC-WLAN
 permit 239.192.248.1                       Permits low-rate stream (239.192.248.1).
```

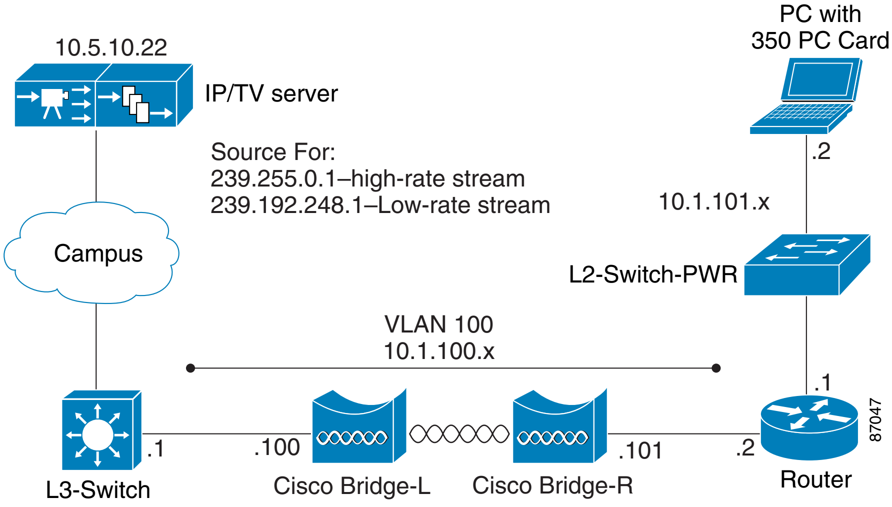
Controlling IP Multicast in a P2P WLAN using Bridges

The same boundary that was deployed in the AP scenario is used with the bridge scenario. Figure 8-2 shows the topology for a WLAN using a bridge for a Point-to-Point (P2P) connection. The IP/TV server (10.5.10.22) is sourcing the same groups as in the previous example:

- 239.255.0.1 is a high-rate (1.4 Mbps) video stream.
- 239.192.248.1 is a low-rate (100 Kbps) video stream.

The low-rate stream is allowed and the high-rate stream is disallowed on the P2P wireless link. To control what multicast traffic passes over the P2P link, only the **ip multicast boundary** configuration on ROUTER is needed. Because the multicast boundary prevents hosts from joining unwanted groups, the network never knows to forward unwanted traffic over the P2P link.

Figure 8-2 Testbed for Point-to-Point Wireless Network using Bridges



In this configuration:

- L3-SWITCH (VLAN 100-10.1.100.1) connects to the campus network and the P2P wireless network.
- The P2P wireless link is made possible by two Cisco Aironet Bridges, CiscoBridge-L (10.1.100.100) and CiscoBridge-R (10.1.100.101).
- ROUTER (10.1.100.2) connects to the P2P wireless network and the remote site network (10.1.101.1) via L2-SWITCH-PWR.
- The laptop computer (10.1.101.2) is running the IP/TV Viewer software.

If the remote side of the P2P link has a Layer 2 switch and no Layer 3 switch or router, then a boundary can be placed on the VLAN 100 interface of L3-SWITCH2. Also, in a Point-to-Multipoint (P2MP) deployment, a mix of both may be needed. Both configurations are shown here for reference.

Following is the configuration for L3-SWITCH.

```
interface Vlan100
 description VLAN for P2P Bridge
 ip address 10.1.100.1 255.255.255.0
 ip pim sparse-mode                           Enables PIM on the interface.
 ip multicast boundary IPMC-BRIDGE            Boundary refers to named ACL "IPMC-BRIDGE."
!
ip access-list standard IPMC-BRIDGE
 permit 239.192.248.1                        Permits low-rate stream (239.192.248.1).
```

To prevent unwanted IGMP messaging and multicast traffic from traversing the P2P wireless link on the receiver side (remote LAN - 10.1.101.x), an **ip multicast boundary** is configured on the Fast Ethernet 0/1 interface of ROUTER.

Following is the configuration for ROUTER.

```
interface FastEthernet 0/1
 description Local LAN in Remote Site
 ip address 10.1.101.1 255.255.255.0
 ip pim sparse-mode                           Enables PIM on the interface.
 ip multicast boundary IPMC-BRIDGE            Boundary refers to named ACL "IPMC-BRIDGE."

ip access-list standard IPMC-BRIDGE
 permit 239.192.248.1                        Permits low-rate stream (239.192.248.1).
```

Other Considerations

The following additional considerations apply to deploying IP multicast in a WLAN environment:

- The WLAN LAN extension via EAP and WLAN static WEP solutions can support multicast traffic on the WLAN; the WLAN LAN extension via IPSec solution cannot.
- The WLAN has an 11 Mbps or 54 Mbps available bit rate that must be shared by all clients of an AP. If the AP is configured to operate at multiple bit-rates, multicasts and broadcasts are sent at the lowest rate to ensure that all clients receive them. This reduces the available throughput of the network because traffic must queue behind traffic that is being clocked out at a slower rate.
- Cisco Group Management Protocol (CGMP) or Internet Group Management Protocol (IGMP) should be used to limit the multicast traffic on each AP to the traffic required by associated clients. If a client roams with these features configured on an upstream switch, the multicast stream might not be delivered to the new AP. To address this, the Cisco AP can be configured to generate a general IGMP query when a client associates or disassociates. This allows the upstream switch to learn which multicast groups are required on that AP.
- Multicast and broadcast from the AP are sent without requiring link-layer acknowledgement. Every unicast packet is acknowledged and retransmitted if unacknowledged. The purpose of the acknowledgement is to overcome the inherent unreliable nature of wireless links. Broadcasts and

multicasts are unacknowledged due to the difficulty in managing and scaling the acknowledgements. This means that a network that is seen as operating well for unicast applications, can experience degraded performance in multicast applications.

- Enterprise customers who are using WLAN in laptops would normally use Constant Awake Mode (CAM) as the Power-Save Mode. If delay-sensitive multicast traffic is being sent over the WLAN, customers should ensure that only the CAM configuration is used on their WLAN clients. Based on the 802.11 standard, if the client is in power-save mode, then the AP will buffer broadcast and multicast traffic until the next beacon period that contains a delivery traffic information map (DTIM) transmission. The default period is 200ms. Enterprises that use WLAN on small handheld devices will most likely need to use the WLAN power-save features (Max or Fast) and should not attempt to run delay-sensitive multicast traffic over the same WLAN.

IP Multicast Traffic Considerations in Cisco Unified Wireless Network Switch-Based Mode

The introduction of Layer 3 roaming through the use of the switch-based WDS and mGRE tunnels changes how the multicast traffic is managed. This section discusses these changes and how they impact the WLAN network design.

IP Multicast Traffic Overview

Cisco Unified Wireless Network switched-based mode changes how the AP manages IP multicast traffic and has important consequences for the design of a multicast-enabled wireless network solution.

All the multicast traffic generated from a wireless client belonging to a certain mobility group is received by the AP and forwarded into the corresponding GRE tunnel to the central switch. Thus, all the IP multicast traffic enters the wired network through a single point, which is the mGRE tunnel interface on the Sup720. This makes it easy for a network administrator to control and manage this traffic with the use of ACLs and QoS policies.

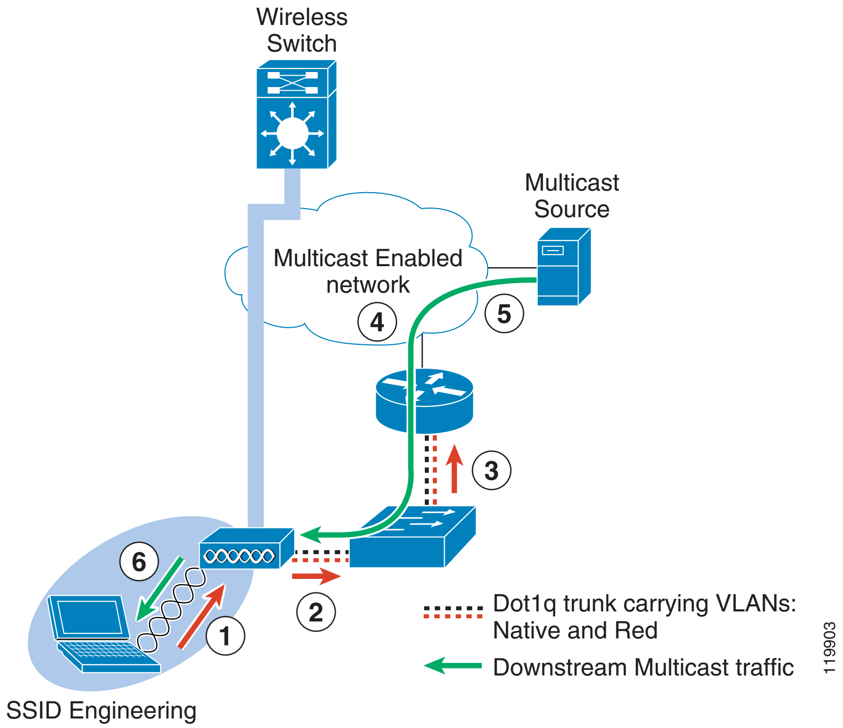
Downstream multicast traffic is delivered in the same way for wireless and wired clients. This means that traffic originating from a wired multicast source and directed to a mobile node is not delivered through the GRE tunnel, but instead is forwarded using the native VLAN infrastructure.

The reason for this asymmetric behavior is in the unicast nature of GRE. For example, consider a mobility group that consists of 300 APs, each configured with a wireless client that requests the same multicast stream. When the traffic gets to the wireless switch from the wired source, the supervisor must duplicate the multicast stream to as many GRE tunnels as there are APs with a client interested in that multicast program.

Delivering Downstream Multicast Traffic

In a Cisco Unified Wireless Network switch-based deployment with the WLSM, the IP multicast traffic downstream from a wired source to a wireless client is delivered outside the GRE tunnel leveraging the existing network infrastructure shows how the AP processes the Internet Group Management Protocol (IGMP) join message received from the client. A similar behavior is applied to the IGMP leave message.

Figure 8-3 AP Processing of the IGMP Join Message


Wireless Switch
Multicast Source
Multicast Enabled network
4
5
3
6
2
1
Dot1q trunk carrying VLANs: Native and Red
Downstream Multicast traffic
119903
SSID Engineering

The AP has been configured with SSID = Engineering, which has been mapped to a certain network ID and also to a local VLAN: VLAN = Red. The connection between the AP and the access switch has also been configured as a 802.1q trunk. VLAN Red is carried to the switch and then to a first hop router.

The step-by-step process is as follows:

1. The wireless client sends an IGMP join request for a certain multicast group.
2. After recognizing this particular type of frame, the AP bridges it onto VLAN Red.
3. Through the access switch, the packet reaches the first hop router (usually the distribution switch) where the VLAN Red interface is defined.
4. The router sends the Protocol Independent Multicast (PIM) join upstream and the multicast trees are built.
5. The multicast traffic starts flowing back to the AP.
6. The AP receives the traffic on VLAN Red, and based on the VLAN/SSID mapping, the AP is able to determine which broadcast encryption key to use to forward the frame into the air to the wireless client.

Note As implemented in the Cisco Aironet access point, the broadcast key is derived from the VLAN associated to a particular SSID. If no VLAN is specified during the mobility group configuration (SSID and Network ID configuration), all the SSIDs are associated to the same default or native VLAN, and they share the same broadcast key.

The following additional configuration is required to enable multicast traffic with the WLSM when compared to a unicast-only solution:

- First, you must configure the connection between the AP and the access switch as an 802.1q trunk to carry multiple VLANs (the native VLAN and an additional multicast VLAN for each mobility group that is multicast-enabled). Remember that for unicast traffic, only the native VLAN is required.
- The multicast VLAN has to be carried to the first hop router, where you must define a L3 interface.

You must assign an IP address to this L3 interface, and you must enable a multicast routing protocol for the router to forward the multicast traffic.

An important consequence of the multicast implementation with the WLSM, and in particular the fact that the traffic is delivered outside the tunnel, is that wireless multicast traffic cannot take advantage of the L3 seamless roaming provided by the mGRE infrastructure. As the client roams to a different AP in the same mobility group, it has to allow the time for the multicast network to re-converge before it can resume receiving the multicast traffic. This results in an interruption of traffic, and thus not in seamless roaming.

For further information on multicast in a Cisco Unified Wireless Network switch-based mode, please see

Cisco Catalyst 6500 Series Wireless LAN Services Module (WLSM) Deployment Guide: http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_technical_reference09186a0080362bd0.html

Summary

In summary, when using IP multicast in the WLAN, follow these recommendations.

- Place the WLAN AP or bridge on a separate VLAN or Layer 3 interface so multicast boundaries can be implemented.
- Use the **ip multicast boundary** command to prevent IGMP joins and multicast forwarding on denied multicast groups.
- In a WLAN using AP, the boundary should be placed on the VLAN or Layer 3 interface connecting to the AP.
- In a WLAN using bridges, the boundary is placed on the VLAN or Layer 3 interface connecting to the remote receiver side. If no Layer 3 capable device is used at the remote site, the boundary is placed on the VLAN or Layer 3 interface connecting to the bridge at the main site. Also, a combination of a boundary at the receiver side and bridge connection at the main site, may be needed in a P2MP deployment.
- Set the highest possible fixed data rate on the APs and bridges to ensure the best possible performance for multicast and data traffic.
- If dropped packets occur and impact the performance of the application, the fixed data rate on the APs and bridges may need to be reduced to ensure a better signal-to-noise ratio, which can reduce dropped packets.

CHAPTER 9

Managing and Deploying WLAN

This chapter addresses WLAN management and deployment considerations when deploying WLAN across your enterprise. It discusses common WLAN management requirements; including configuration, image, security and radio management.

Management Solution Overview

The Wireless LAN Solution Engine (WLSE) plays a critical role as the high-level management interface to a wireless network with autonomous access points. The goal of the WLSE is to provide integration into one device as well as the configuration and management of the various components that compromise a complete WLAN solution.

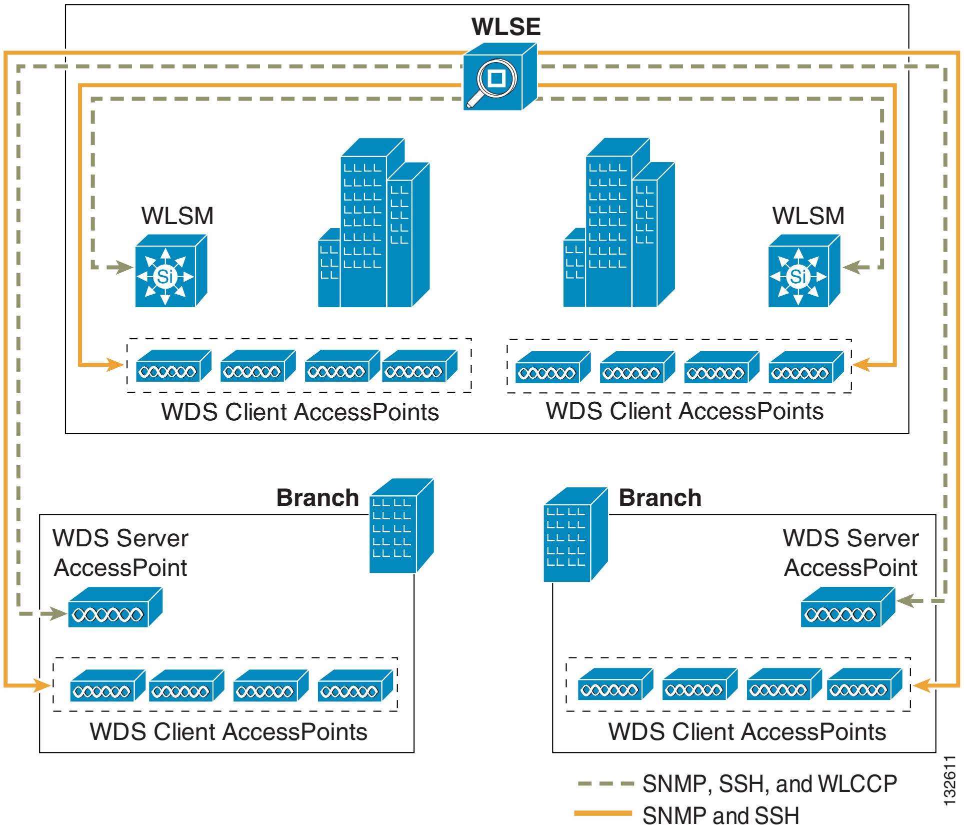
The key functionality of the WLSE can be broken down into the following functional areas;

- Configuration and Image Management
  - Managing the configuration and software images of Access Points and other devices
  - Providing a repository of historical configurations and images
- Radio and Security Management
  - Collecting and analyzing raw 802.11 information received from clients and WLAN Access Points via WLCCP
  - Providing radio configuration guidance through site survey process
  - Securing the WLAN from rogue Access Points and clients
- Reporting
  - Consolidating the wealth of information available in WLSE to management reports
  - Northbound reporting of critical events via SNMP traps or email

Architecture

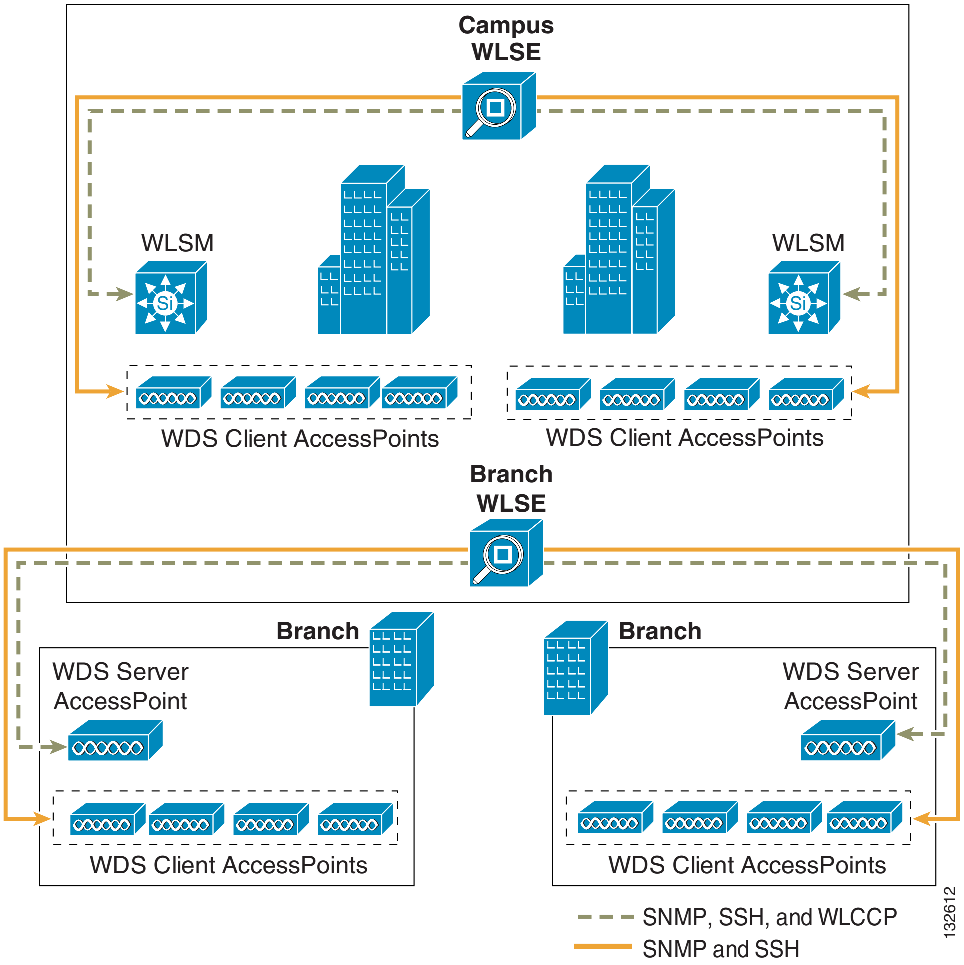
A typical WLSE deployment is shown in Figure 9-1. In this deployment one centralized WLSE manages access points on the Campus and the Branch networks simultaneously. The WLSE also maintains WLCCP connections to the WLSM WDS servers on the campus and the AP WDS servers in the branch, as detailed by the dotted lines connecting the devices.

Figure 9-1 Typical WLSE Deployment in the Enterprise



AWLSE can manage up to 2500 autonomous access points, so most enterprises choose this deployment model. However with large branch and campus networks you can exceed this threshold. When this occurs the best model is to distribute the management and deploy multiple WLSEs. In Figure 9-2 there are two separate WLSE devices managing the large campus network and a separate WLSE managing the branch devices. While this management strategy does not provide a single point for management of all WLAN devices, it does allow you to scale your wireless deployment far beyond 2500 access points.

Figure 9-2 Optional Deployment of Multiple WLSEs to Manage Large Number of Access Points



Another option especially useful in a large branch environment is the deployment of a WLSE Express in each branch. The WLSE Express integrates the functionality of the WLSE with a Radius AAA server, and supports up to 100 Access Points. A separate design guide will be published covering the implementation model for the WLSE Express.

Initial configuration

Before an access point can be managed by the WLSE, both devices must share a configuration that allows the two to communicate securely. Several methods exist of configuring an access point to communicate with the management system and are detailed below.

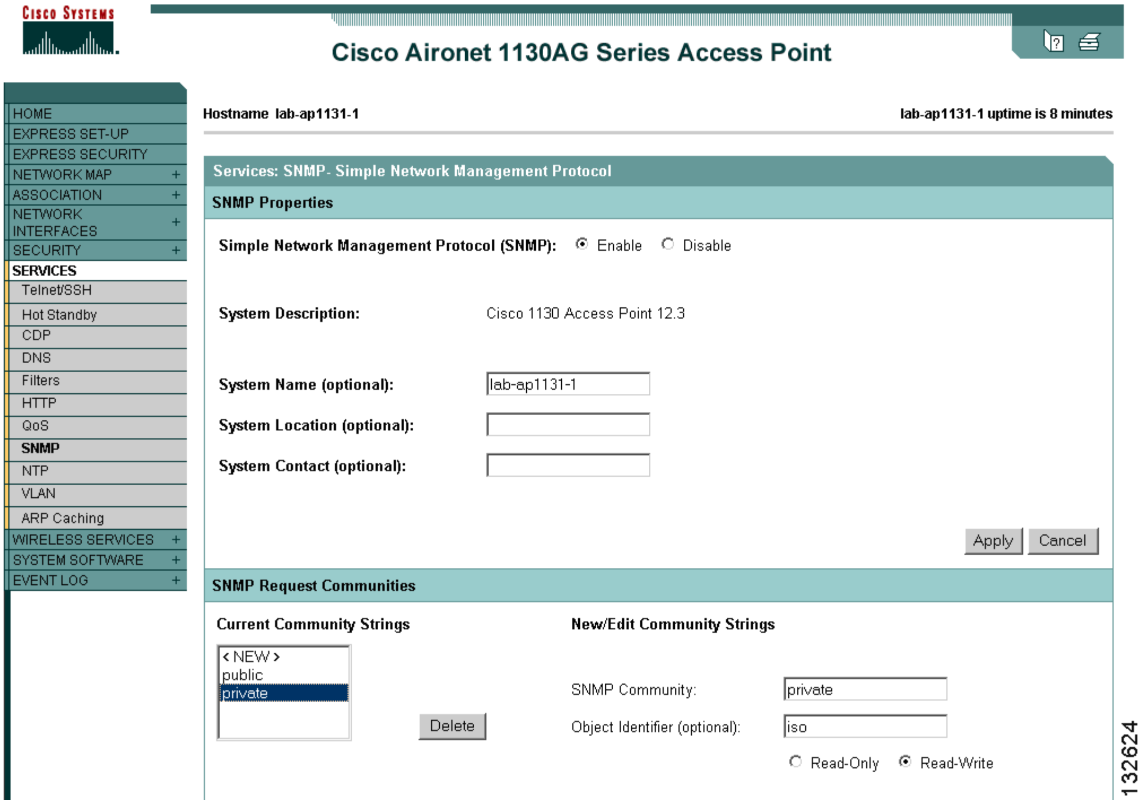
- Directed discovery of the Access Point
- Automatic discovery of the Access Point
- DHCP auto-registration of the Access Point

Directed discovery is the most common and is covered in detail in this section. Directed discovery involves the administrator entering the IP address of Access Points to be discovered into the WLSE GUI, along with the correct SNMP string of the access point. While this method is the most manual of the above methods, it relies on few other variables and is highly repeatable.

The following assumes that the access point has been configured with static IP address information and a unique host name. After that the first step of directed discovery is to ensure that the access point has been configured for SNMP Management.

As you can see below in Figure 9-3 you can enable SNMP management through the access point's web GUI, by choosing **Services > SNMP.** After this you will need to configure both public and private SNMP strings which will act as the trusted secrets between the AP and the WLSE. When you configure these strings, ensure that the object identifier is **ISO**.

Figure 9-3   Configuring an Access Point for SNMP



Cisco Aironet 1130AG Series Access Point

Hostname lab-ap1131-1   lab-ap1131-1 uptime is 8 minutes

Services: SNMP- Simple Network Management Protocol

SNMP Properties

Simple Network Management Protocol (SNMP): ● Enable ○ Disable

System Description: Cisco 1130 Access Point 12.3

System Name (optional): lab-ap1131-1

System Location (optional):

System Contact (optional):

SNMP Request Communities

Current Community Strings: < NEW >
public
private

New/Edit Community Strings

SNMP Community: private

Object Identifier (optional): iso

○ Read-Only ● Read-Write

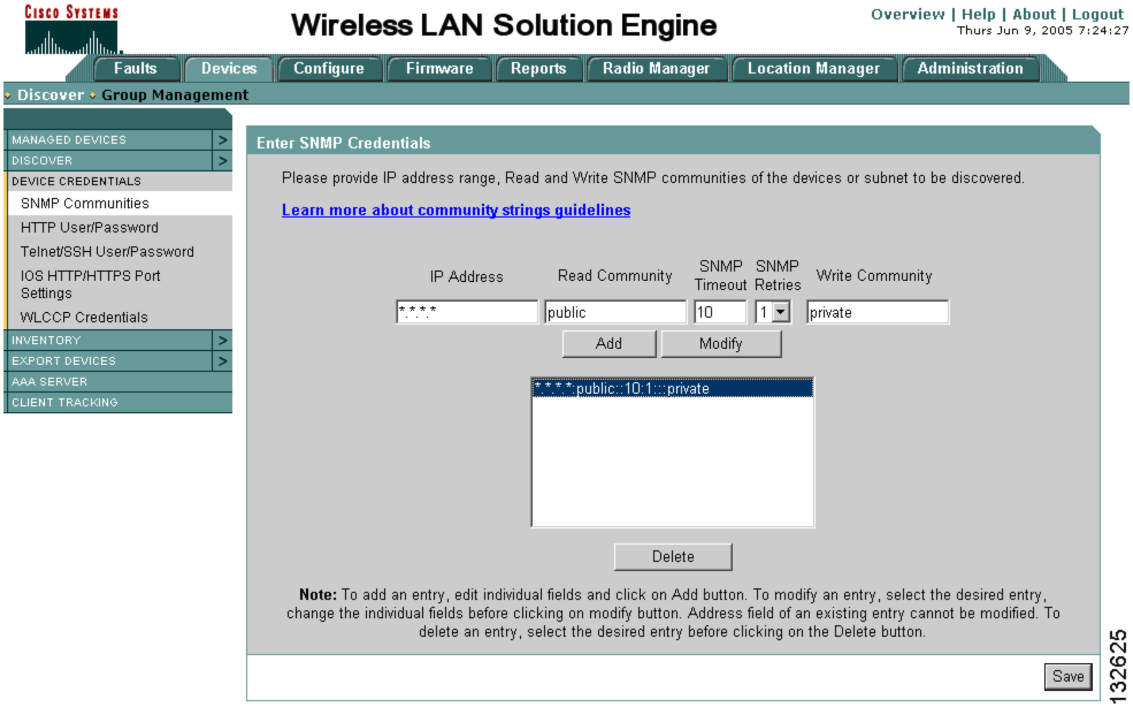
At this point, the access point is ready to be managed by the WLSE. This guide assumes that the WLSE has been configured with a static IP address and SSL access has been enabled to the WLSE appliance

Access your WLSE at https://x.x.x.x or http://x.x.x.x:1741 (where x represents the URL) and log in to the appliance. Before starting the discovery process it is important the WLSE is configured with proper credentials to access the devices configured in the previous steps. You need to configure the following credentials on the WLSE by choosing **Devices > Discover > Device Credentials**.

- SNMP Credentials
- Telnet / SSH User / Password

To configure the SNMP Credentials enter the SNMP community strings that you entered in the previous step. Since different devices may have varying community strings, the WLSE provides the option to provide different strings for different networks and devices. A properly configured SNMP string that applies to all networks and devices is shown in Figure 9-4.

Figure 9-4 Entering SNMP Device Credentials



Enter SNMP Credentials

Please provide IP address range, Read and Write SNMP communities of the devices or subnet to be discovered.

Learn more about community strings guidelines

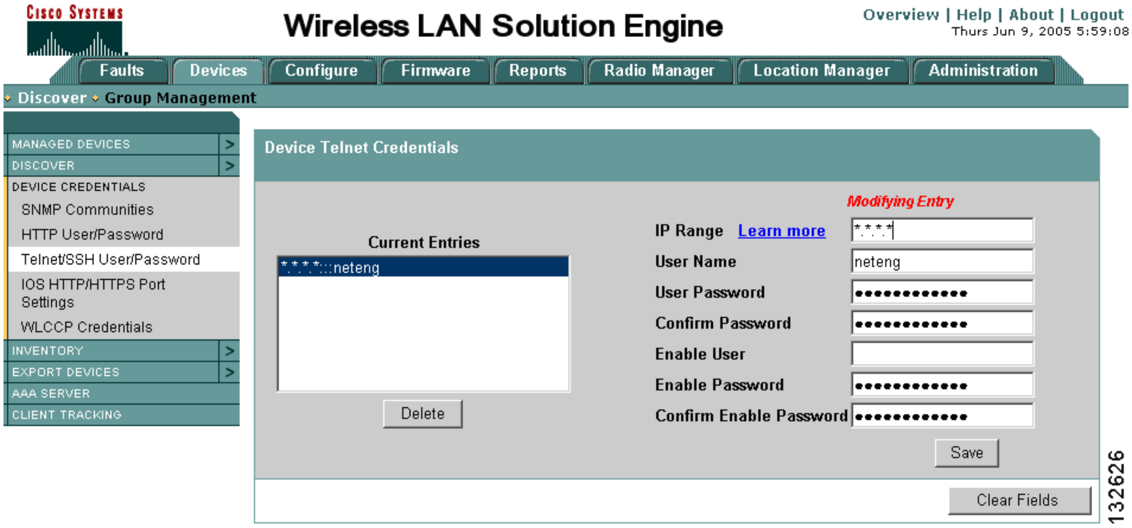
IP Address	Read Community	SNMP Timeout	SNMP Retries	Write Community
..*.*	public	10	1	private

..*.*:public::10:1:::private

Note: To add an entry, edit individual fields and click on Add button. To modify an entry, select the desired entry, change the individual fields before clicking on modify button. Address field of an existing entry cannot be modified. To delete an entry, select the desired entry before clicking on the Delete button.

After the SNMP device credentials have been entered it is also required that Telnet and SSH credentials are configured. Where as SNMP is used for image management and monitoring, Telnet and SSH can be utilized to deploy complex configurations to Access Points and, once again, the WLSE provides the capability to have different credentials on a per network or device basis. In this example we use the "neteng" account with the password "Cisco". For reference the default user name and password is "Cisco" and "Cisco". Figure 9-5 shows the configured credentials.

Figure 9-5 Entering Telnet/SSH Device Credentials



Device Telnet Credentials

Current Entries

..*.*:::neteng

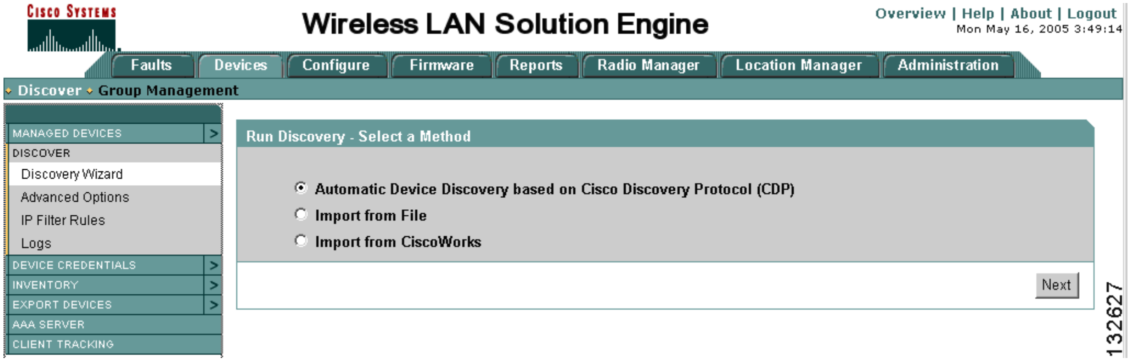
Modifying Entry

IP Range Learn more	*.*.*.*
User Name	neteng
User Password	●●●●●●●●●●●●
Confirm Password	●●●●●●●●●●●●
Enable User	
Enable Password	●●●●●●●●●●●●
Confirm Enable Password	●●●●●●●●●●●●

At this point you are ready to start the Discovery process. To start, choose **Devices>Discover>Discovery Wizard**. The Discovery Wizard guides you through the steps to manage an Access Point.

On the first page you are presented with several options, which allow you import seed files from CiscoWorks or a flat file. Since in this example, we are directly seeding values, choose **Automatic Discovery based on Cisco Discovery Protocol (CDP)** as shown in Figure 9-6. In the next window choose **Run Now** to perform the discovery process immediately after completing the wizard.

Figure 9-6 Starting the WLSE Discovery Process



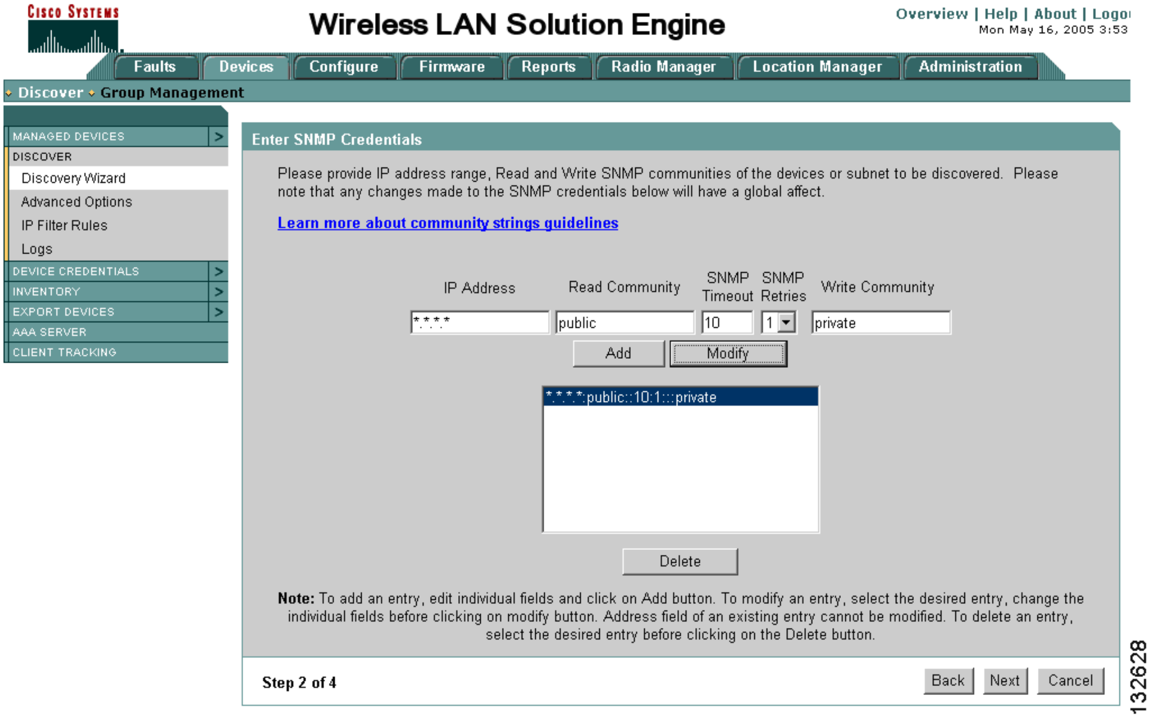
Mon May 16, 2005 3:49:14

Run Discovery - Select a Method

● Automatic Device Discovery based on Cisco Discovery Protocol (CDP)
○ Import from File
○ Import from CiscoWorks

On the next window you are presented the opportunity to adjust the SNMP values that the WLSE has configured. The SNMP strings are configured correctly for the example in Figure 9-7. Also note that any changes made to the SNMP strings in this wizard update the SNMP credentials for the whole appliance, so adjust carefully.

Figure 9-7 Option to modify SNMP Credentials on the WLSE



Mon May 16, 2005 3:53

Enter SNMP Credentials

Please provide IP address range, Read and Write SNMP communities of the devices or subnet to be discovered. Please note that any changes made to the SNMP credentials below will have a global affect.

IP Address	Read Community	SNMP Timeout	SNMP Retries	Write Community
..*.*	public	10	1	private

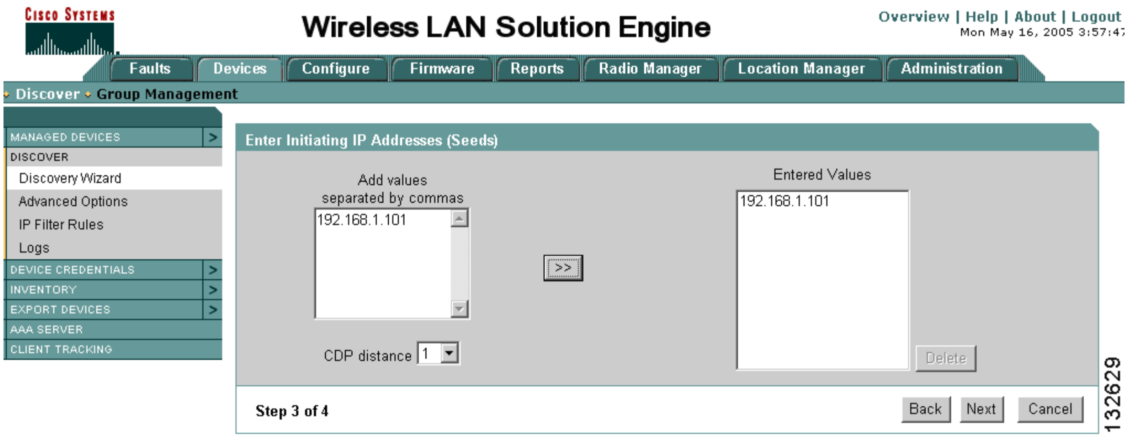
..*.*:public::10:1:::private

Note: To add an entry, edit individual fields and click on Add button. To modify an entry, select the desired entry, change the individual fields before clicking on modify button. Address field of an existing entry cannot be modified. To delete an entry, select the desired entry before clicking on the Delete button.

Step 2 of 4

On the next screen enter the IP addresses of the Access Points to be managed into the Seed Values area, if you wish to discover additional access points you can alternatively increase the CDP distance that the WLSE will search beyond the initial device.Once you have completed entering values, choose **Next** and the discovery job is created. When increasing the CDP distance to discover more devices the WLSE needs to know if the SNMP read strings of upstream devices such as switches and routers. Increasing the CDP distance allows more discoveries to be made from an initial starting point, but at the cost of increased time required to discover devices. It is often more efficient to perform multiple targeted discoveries with a smaller CDP distance than attempting to discover all APs with one discovery. The discovery process does not have to begin with an AP; it can start at a more centralized location in the network, and this can also aid in discovery efficiency.

Figure 9-8 Entering Seed Discovery Values



Enter Initiating IP Addresses (Seeds)

Add values separated by commas: 192.168.1.101

Entered Values: 192.168.1.101

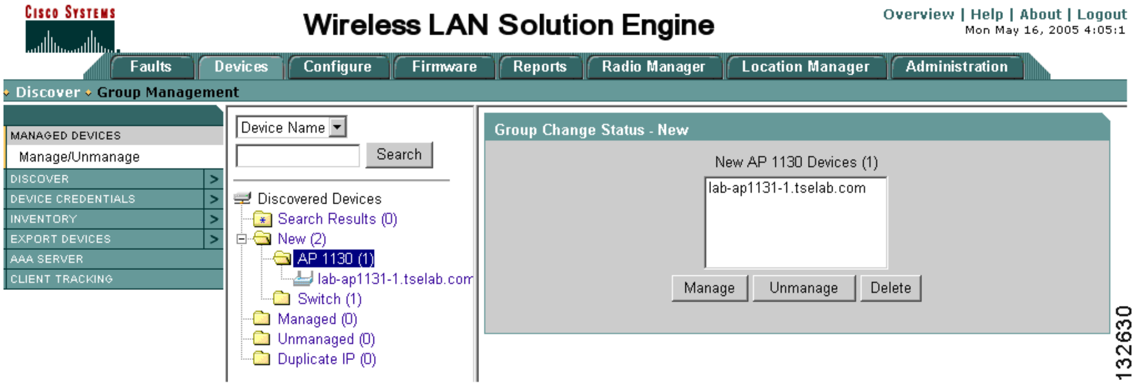
CDP distance: 1

Step 3 of 4

After the discovery job has completed you can now manage the access point by choosing **Managed Devices>Manage/Unmanage** and selecting the appropriate access points, as shown in Figure 9-9. As you manage the access points they move from the New list to the Managed AP list.

While there is an option to automatically manage newly discovered devices, generally it is recommended that the manual process be followed because allows an audit of what has been discovered against what is expected.

Figure 9-9 Managing a discovered device



Discovered Devices
- Search Results (0)
- New (2)
  - AP 1130 (1)
    - lab-ap1131-1.tselab.com
  - Switch (1)
- Managed (0)
- Unmanaged (0)
- Duplicate IP (0)

Group Change Status - New

New AP 1130 Devices (1): lab-ap1131-1.tselab.com

Once you have configured your WLSE to manage your access points, you can now begin to centrally manage your WLAN infrastructure.

Another mechanism of managing individual access points is DHCP discovery, in which DHCP option 66 is set on your corporate DHCP server. And as the access points boot up for the first time, they are directed to register and receive their start-up configuration from the WLSE specified by option 66.

Once the device has been discovered and the decision has been made to manage the device, the WLSE performs an inventory of the device to determine its details. After this inventory is completed the device is available for management by the WLSE, and will appear in the difference navigation trees, of the other WLSE menus.

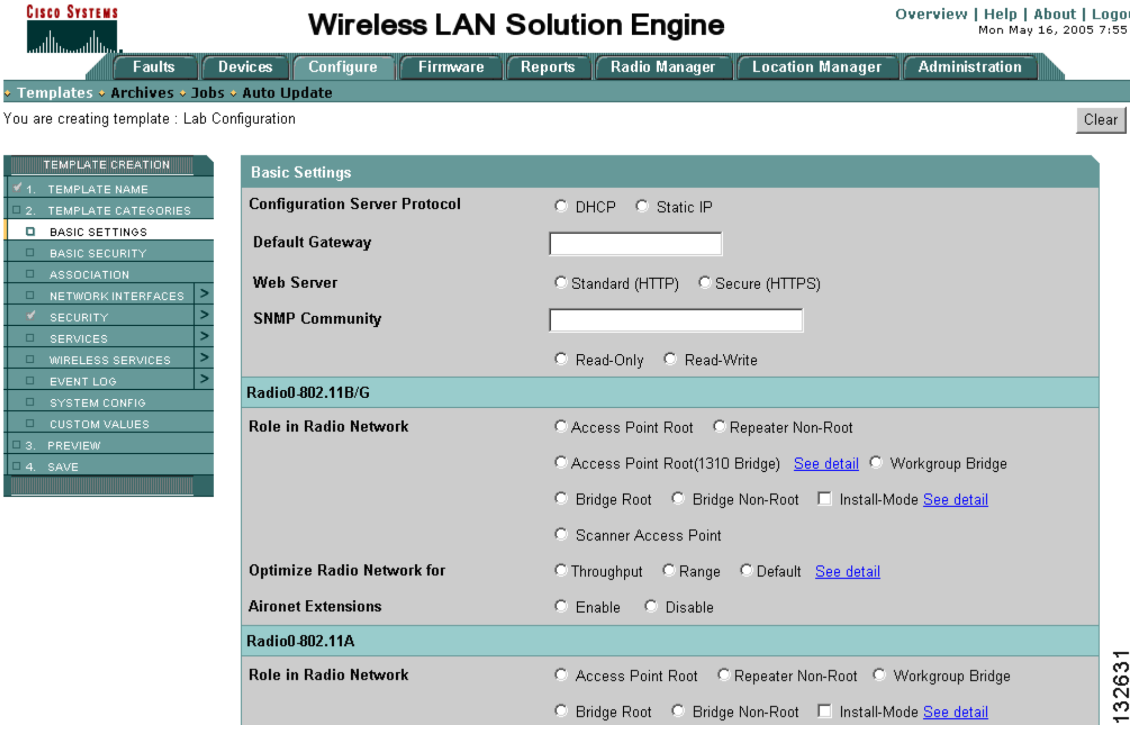
Configuration and Image Management

Configuration and image management are tasks that take a small amount of time over the lifetime of the solution product, but are often the first major challenge encounter in a WLAN deployment. This is due to the large number of devices, their location, and the possible security implications of an incorrectly configured WLAN device. Thus, the WLSE was designed to assist in managing these devices in a systematic fashion.

Creating and deploying configurations

The WLSE supplies a configuration template tool, shown in Figure 9-10, which provides a GUI interface to create a configuration that may be pushed out to multiple devices. The GUI interface is augmented by a custom commands option that allows commands to be entered as device CLI statements. The advantage of the GUI portion of the template creation is that parses the entries to determine which software versions support these commands, and this is checked when a configuration job is run. Configuration templates are accessed by choosing **Configure>Templates**. Templates are then used by configuration jobs to push a common configuration to all selected APs.

Figure 9-10 Configuration Template



You are creating template : Lab Configuration

Basic Settings

Configuration Server Protocol ○ DHCP ○ Static IP

Default Gateway

Web Server ○ Standard (HTTP) ○ Secure (HTTPS)

SNMP Community

○ Read-Only ○ Read-Write

Radio0-802.11B/G

Role in Radio Network ○ Access Point Root ○ Repeater Non-Root

○ Access Point Root(1310 Bridge) See detail ○ Workgroup Bridge

○ Bridge Root ○ Bridge Non-Root □ Install-Mode See detail

○ Scanner Access Point

Optimize Radio Network for ○ Throughput ○ Range ○ Default See detail

Aironet Extensions ○ Enable ○ Disable

Radio0-802.11A

Role in Radio Network ○ Access Point Root ○ Repeater Non-Root ○ Workgroup Bridge

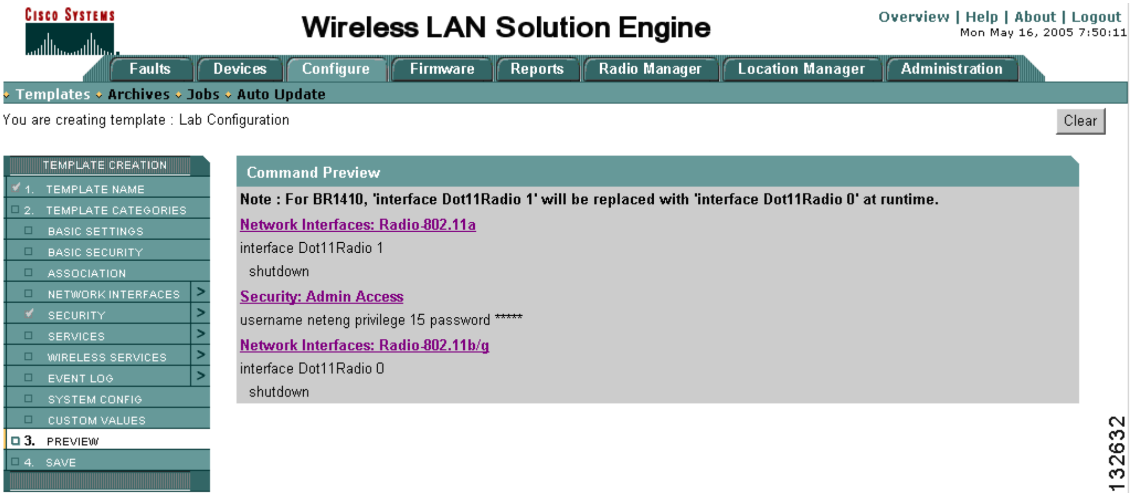
○ Bridge Root ○ Bridge Non-Root □ Install-Mode See detail

You can configure templates in much the same way as you would configure an individual access point. However take caution in configuring device specific attributes, such as IP address, host name, and radio channel in a template since they are applied to multiple devices. Device specific templates may also be created for application to an Access Point based on the MAC address, serial number, or switch port the access point is plugged into.

After you have entered the configuration items you wish to change, you can preview the IOS commands which are issued to the access points to affect the necessary changes. In the example in Figure 9-11, you can see that we have disabled both 802.11a and 802.11g radios and created a new administrative user in the local authentication database.

One often overlooked short cut involves the custom values setting show in Figure 9-11. Using the custom values entry method, you can directly create or remove IOS commands from selected access points. This allows you to be creative in removing or adding configuration using the WLSE, but it also bypasses rule-checking that prevents configuration missteps.

Figure 9-11 Configuration Template preview



You are creating template : Lab Configuration

Note : For BR1410, 'interface Dot11Radio 1' will be replaced with 'interface Dot11Radio 0' at runtime.

Network Interfaces: Radio-802.11a

```
interface Dot11Radio 1
 shutdown
```

Security: Admin Access

```
username neteng privilege 15 password *****
```

Network Interfaces: Radio-802.11b/g

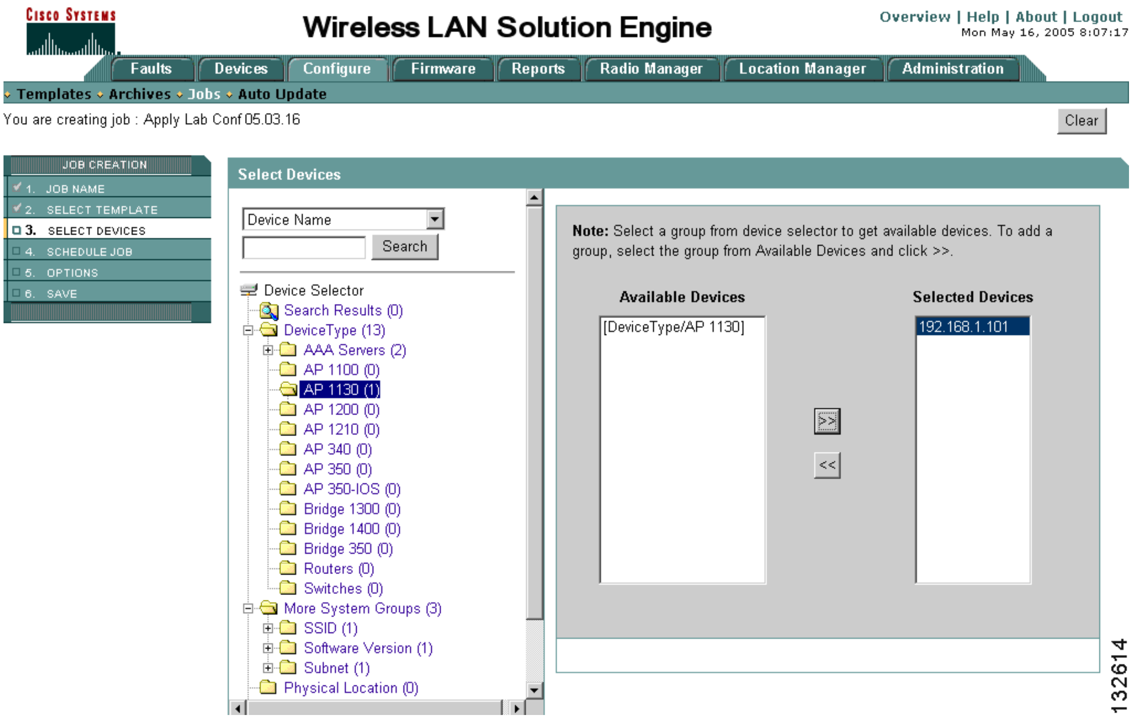
```
interface Dot11Radio 0
 shutdown
```

After creating the configuration template and giving it a name, you can create configuration job to deploy the template to a group of access points, a single access point, or your entire WLAN network. To create a configuration job, from the main WLSE menu, choose **Configuration>Jobs**.

On this window you are asked to name the configuration job; common name schemes include the date and a brief description of the task involved.

After choosing **Create Config Job** you are prompted to select a template to apply and, additionally, which devices you want to deploy the template against. Device selection is detailed below in Figure 9-12.

Figure 9-12 Selecting Devices to be Configured



You are creating job : Apply Lab Conf 05.03.16

Note: Select a group from device selector to get available devices. To add a group, select the group from Available Devices and click >>.

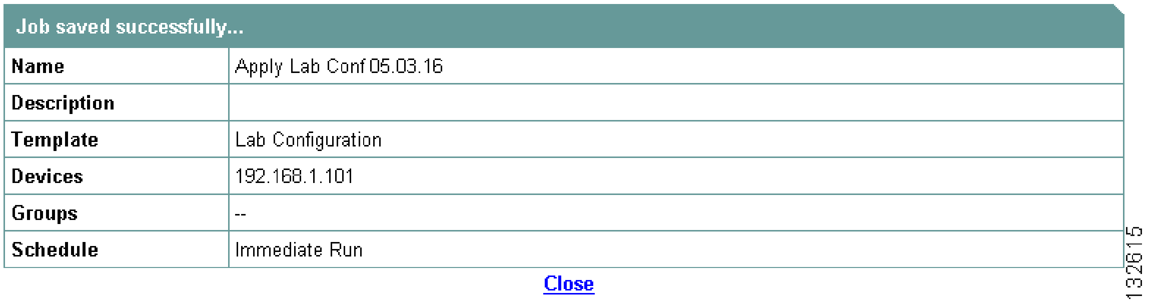
Available Devices	Selected Devices
[DeviceType/AP 1130]	192.168.1.101

Selecting Devices to be configured

At this point you need to select a time to execute the configuration job, this allows you to schedule job execution in the future or to run now.

After you select run now and finish the configuration job, you are presented with options to notify you via email when the job completes. After you enter your notification information and click the Save Job button, you are presented with the Job Save Summary window shown in Figure 9-13.

Figure 9-13 Configuration job summary page

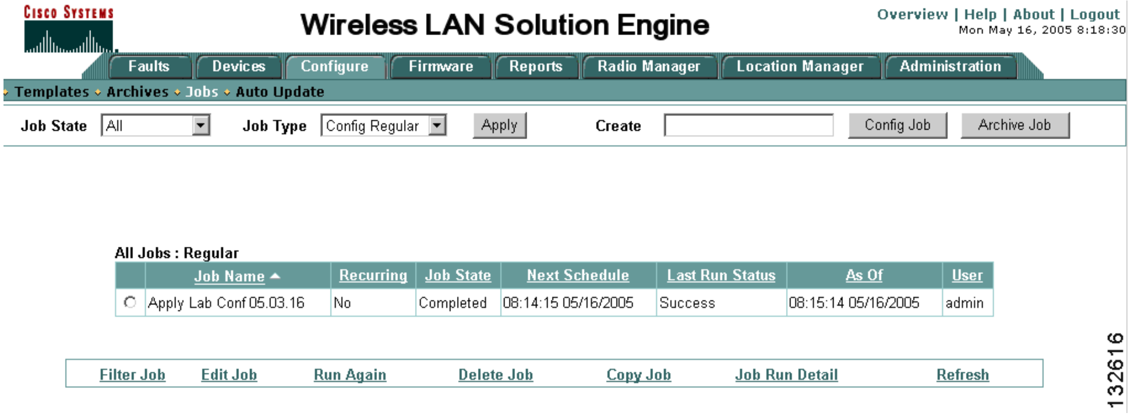


Job saved successfully...

Name	Apply Lab Conf 05.03.16
Description	
Template	Lab Configuration
Devices	192.168.1.101
Groups	--
Schedule	Immediate Run

Clicking on the Close button brings you back to the main job creation window where you can verify the status of current queued jobs. When the job completes you see a summary screen similar to Figure 9-14.

Figure 9-14 Configuration Job Summary screen showing successful configuration deployment



Job State: All   Job Type: Config Regular

All Jobs : Regular

	Job Name	Recurring	Job State	Next Schedule	Last Run Status	As Of	User
○	Apply Lab Conf 05.03.16	No	Completed	08:14:15 05/16/2005	Success	08:15:14 05/16/2005	admin

While this is not a complete discussion of the configuration management capabilities of the WLSE it gives you a general framework from which you can further manage your WLAN Access Points' configuration.

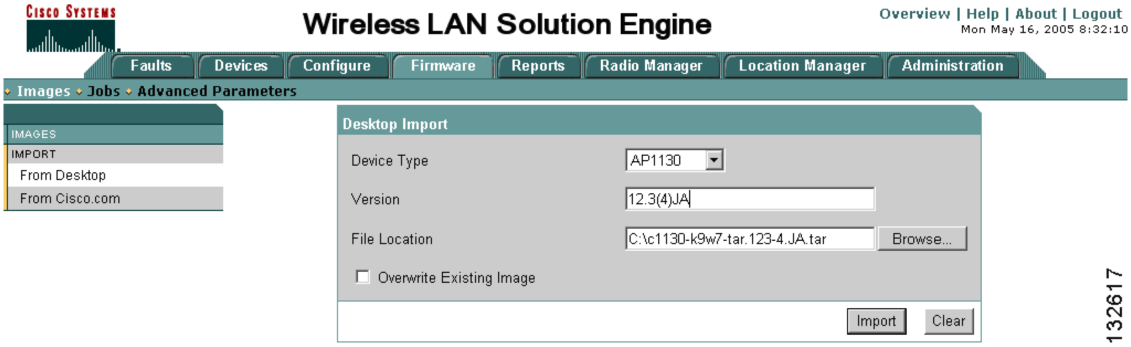
Importing and deploying images

The WLSE can also be utilized to update software on individual access points from the Firmware tab on the main WLSE menu.

The first step to deploying new firmware to your WLAN is to import the images to the WLSE. The easiest way to do this is to download the appropriate image to your desktop from CCO and import it to the WLSE. In previous versions you were able to download directly from CCO, but this has been disabled.

To import from your desktop, choose **Import >From Desktop**. At this point you are prompted to select the hardware platform, version, and the actual file from your desktop system to upload. Be careful to follow the IOS numbering scheme very carefully, the proper format is 12.X(Y)JAz where X represents the major release, Y the minor release and JAz is the release number z. In Figure 9-15 we are importing release 12.3(4)JA for the AP1130 platform to the WLSE from our desktop.

Figure 9-15 Importing an image into the Firmware repository



Device Type: AP1130

Version: 12.3(4)JA

File Location: C:\c1130-k9w7-tar.123-4.JA.tar

□ Overwrite Existing Image

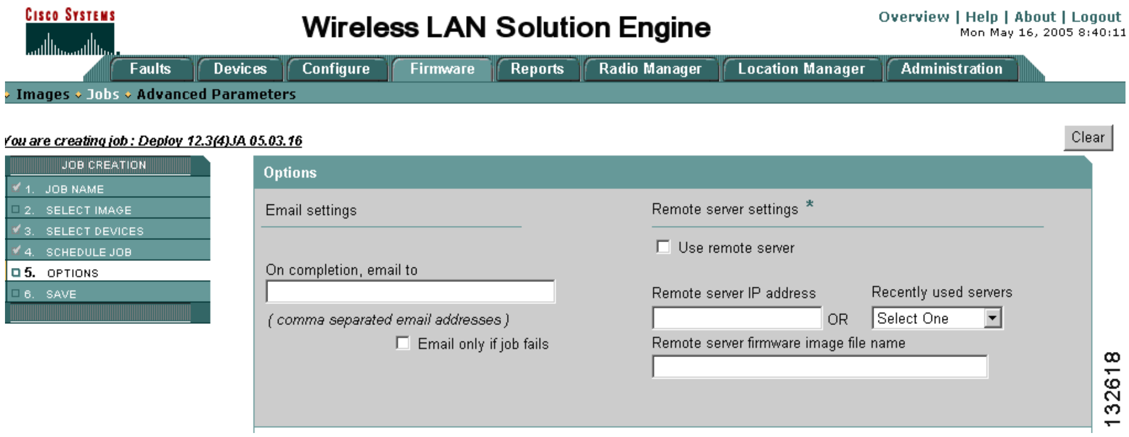
After the import has completed, the image is available for deployment via a configuration job.

To create a configuration job, click on **Firmware->Jobs**. After creating a descriptive name for the job select SNMP for the deployment method. While HTTP is also available as an option, SNMP is the preferred method as it utilizes memory more efficiently and increases the download speed.

Select the image uploaded in the previous example and select the appropriate device or group of devices to deploy the images. On the schedule job page, you can elect to run the firmware job now or at a later date.

As seen in Figure 9-16 you can enable an email to be generated at the completion of the firmware job. You can also specify a remote TFTP server for remote access points to download their images from. This can reduce WAN bandwidth utilization when upgrading a large number of remote access points across bandwidth limited connections, and also greatly decrease the time taken to convert images.

Figure 9-16 Firmware job options screen



You are creating job : Deploy 12.3(4)JA 05.03.16

Options

Email settings

On completion, email to

(comma separated email addresses)

□ Email only if job fails

Remote server settings *

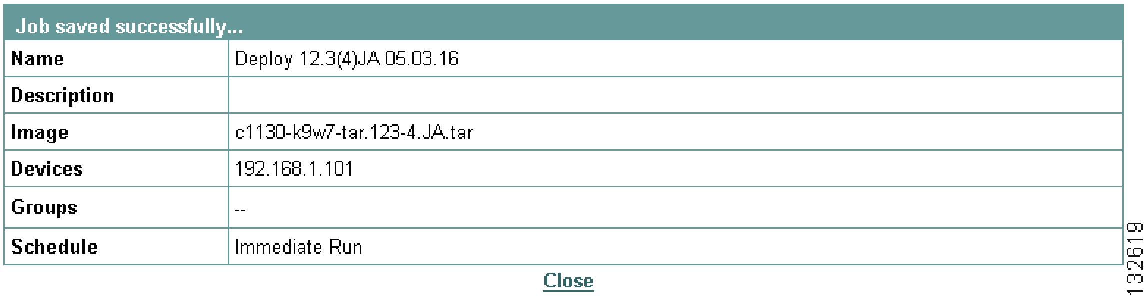
□ Use remote server

Remote server IP address OR Recently used servers: Select One

Remote server firmware image file name

After creating the job you are presented with a job save summary window which details the firmware deployment job that was just created, as shown in Figure 9-17. After closing this screen you are directed towards the main Firmware Jobs screen where you can monitor the firmware job.

Figure 9-17 Firmware job summary screen

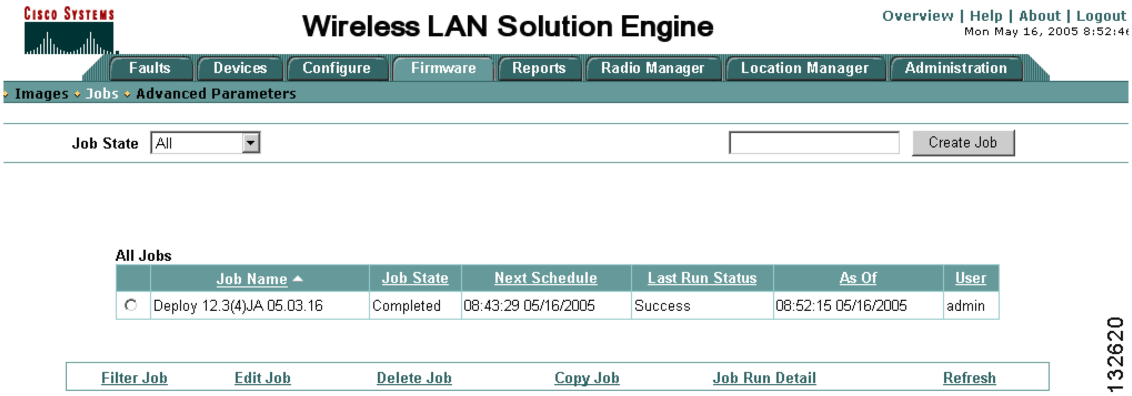


Job saved successfully...

Name	Deploy 12.3(4)JA 05.03.16
Description	
Image	c1130-k9w7-tar.123-4.JA.tar
Devices	192.168.1.101
Groups	--
Schedule	Immediate Run

Depending on the number of devices and the complexity, firmware upgrades can take anywhere from five minutes to several hours to complete. Do not be alarmed that the job is not complete by the time you access the Firmware Jobs screen. When the job is complete you are presented with a screen similar to Figure 9-18.

Figure 9-18 Firmware Job Summary screen showing successful firmware deployment



Job State: All

All Jobs

	Job Name ▲	Job State	Next Schedule	Last Run Status	As Of	User
○	Deploy 12.3(4)JA 05.03.16	Completed	08:43:29 05/16/2005	Success	08:52:15 05/16/2005	admin

Other firmware capabilities include tracking the version of firmware historically deployed to a given access point. This allows detailed asset and version tracking down to the individual AP.

Configuration and Image Management Summary

With the combination of Configuration and Image management you can easily manage large number of Access Points and WLAN devices without having to make configuration changes on each individually. While the configuration examples presented herein are simplistic in nature they are meant to give a general overview of a much larger reference, the WLSE 2.11 Documentation, which can be found at:

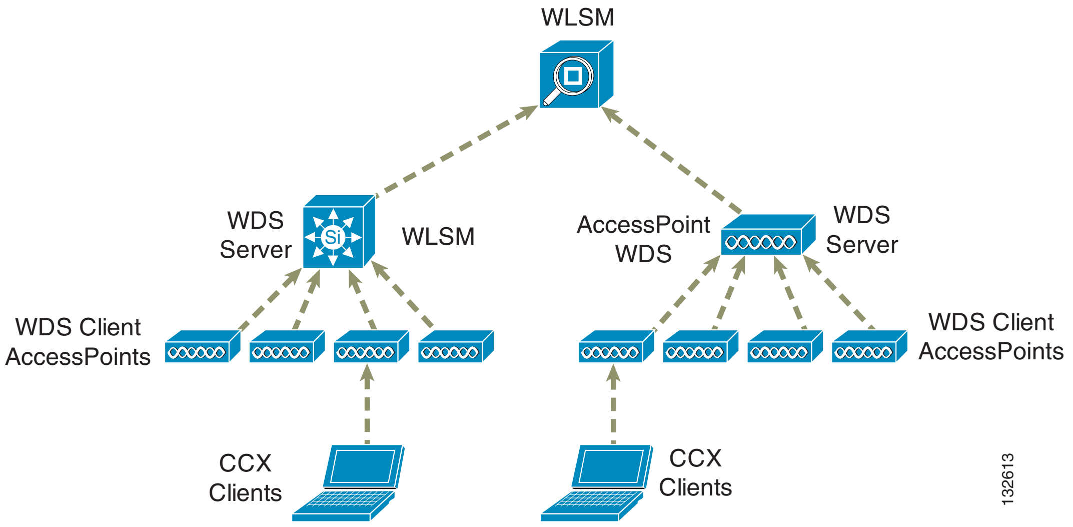
Managing Device Configuration
http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_user_guide_chapter09186a0080364097.html

Managing Device Firmware
http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_user_guide_chapter09186a0080364082.html

Radio and Security Management

At the highest level, radio and security management are related because they involve the in-depth analysis of raw radio information. In the case of radio management the WLSE is analyzing the strength of received packets from Clients and Access Points. With security management the WLSE is analyzing packets looking for suspicious activity, such as an unknown access point or a high number of association attempts form a single client. To facilitate this access to raw information the Wireless LAN Context Control Protocol (WLCCP) was created. WLCCP Packets flow from Wireless LAN Clients and WDS Client access points to Wireless Domain Services (WDS) Servers where they are aggregated and reported to the WLSE. The flow of WLCCP information is shown below in Figure 9-19.

Figure 9-19 High level overview of WLCCP Data in a Cisco Unified Wireless Network



Several options exist for the choice of WDS Server in the Cisco Unified Wireless Network architecture are detailed below:

- Access Point acting as WDS Server (L2) - Provide dual purpose, AP simultaneously serves clients and acts as the WDS for Client Access Points.
- Dedicated Access Point acting as WDS Server (L2) - Access Point only acts as a WDS Server for Client Access Points, in this mode the WDS can handle additional Client Access Points
- Wireless Lan Services Module (WLSM) (L3) - Dedicated Catalyst 6500 module providing high capacity WDS Server and ability to provide WDS services beyond L2 boundaries

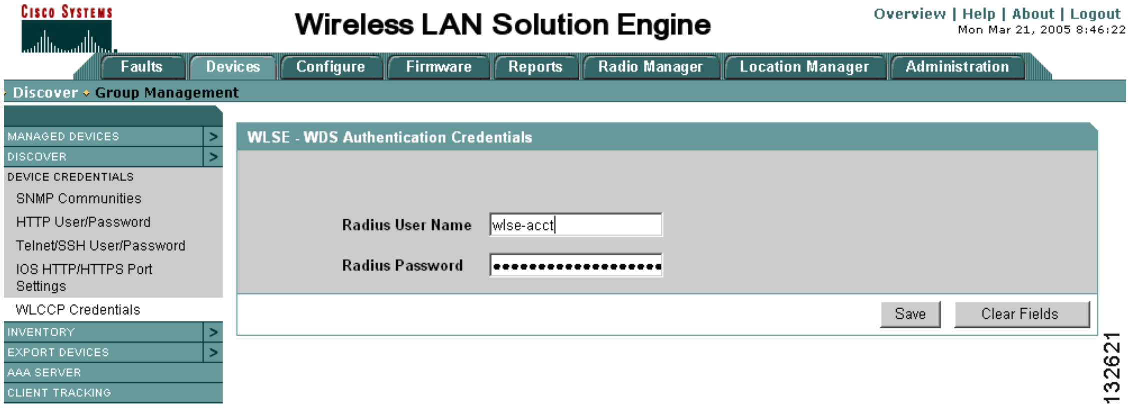
In L2 WDS mode the communication between Access Points and the WDS server is accomplished using multicast, so it is important that the underlying network support multicast. In L3 environments WLCCP communication TCP and UDP on port 2887 for communication, the same port is also utilized for communication between the WDS Servers and the WLSE.

Initial Configuration

Just like the WLSE and Access Point had to be configured for initial management, the WLSE, WDS Server Access Points and WDS Client Access Points must all be configured to communicate radio information.

The first step of configuring WLCCP in your environment is to configure WLCCP credentials on the WLSE. To configure WLCCP credentials go to **Devices > Device Credentials > WLCCP** Credentials. The user name and password entered in Figure 9-20 will be used to authenticate the WLSE to each WDS Server Access Point. Also note that a radius user account matching this name and password must exist in your environment.

Figure 9-20 Entering WLCCP Credentials in WLSE



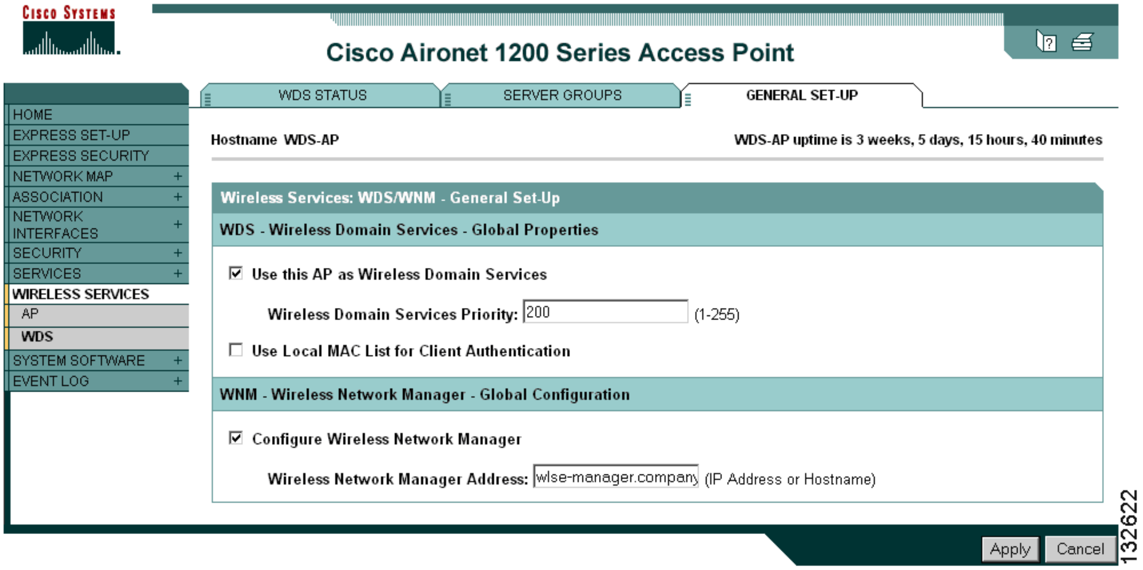
WLSE - WDS Authentication Credentials

Radius User Name: wlse-acct

Radius Password: ••••••••••••••••••••

After configuring the WLSE you must configure each WDS Server Access Point to communicate with the WLSE. For simplification the configuration screen is shown on an individual access point, however this could alternatively be deployed by the WLSE as a template. To point the WDS Server AP to the WLSE enter the IP address or Domain name of the WLSE into the Wireless Network Manager Address field on the Wireless Services -> WDS -> General Setup Screen of the Access Point. A sample configuration is shown below in Figure 9-21.

Figure 9-21 Configuring an Access Point to communicate with the WLSE via WLCCP



Hostname WDS-AP

WDS-AP uptime is 3 weeks, 5 days, 15 hours, 40 minutes

Wireless Services: WDS/WNM - General Set-Up

WDS - Wireless Domain Services - Global Properties

☑ Use this AP as Wireless Domain Services

Wireless Domain Services Priority: 200 (1-255)

□ Use Local MAC List for Client Authentication

WNM - Wireless Network Manager - Global Configuration

☑ Configure Wireless Network Manager

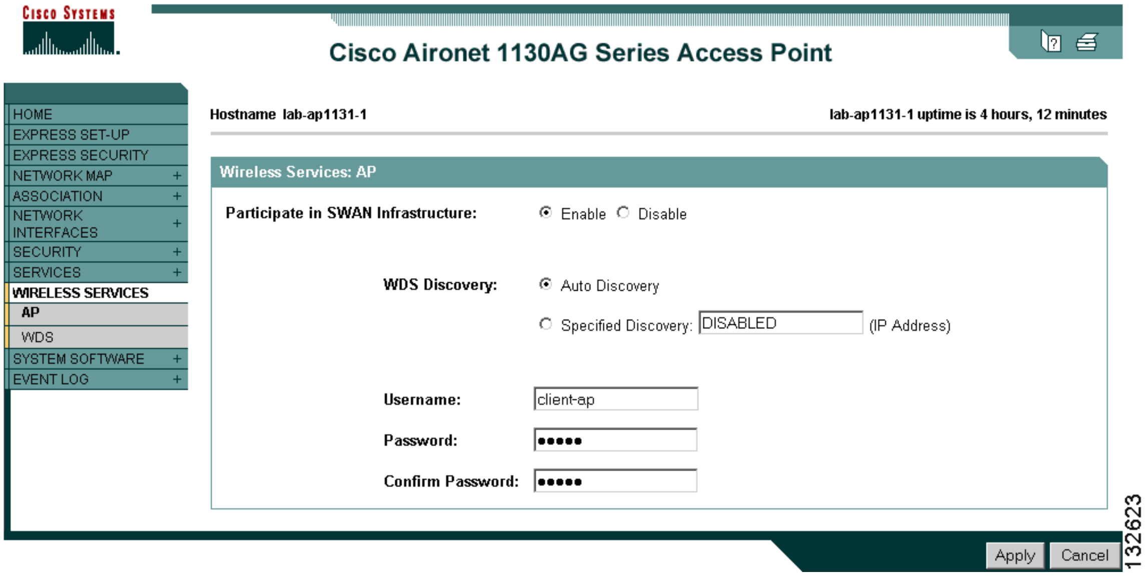
Wireless Network Manager Address: wlse-manager.company (IP Address or Hostname)

Your WDS Access Point should now be able to communicate via WLCCP with the WLSE. You can verify this by issuing the following command line on a WDS Server Access Point;

```
wds-ap# show wlccp wnm status
WNM IP Address: wlse-manager.company.com Status: SECURITY KEYS SETUP
```

After the WDS Server Access Point or WLSM is configured you must configure WDS Client Access points to register with the WDS Server. To configure a client access point in a L2 environment, enable participation in the Cisco Unified Wireless Network infrastructure with Auto Discover, and specify a valid radius user name and password, a sample configuration is shown below in Figure 9-22. In a L3 WLSM environment select Specified Discovery and enter the IP address of the WLSM control interface.

Figure 9-22 Configuring WDS Client Access Point to register with WDS Server



Hostname lab-ap1131-1

lab-ap1131-1 uptime is 4 hours, 12 minutes

Wireless Services: AP

Participate in SWAN Infrastructure: ● Enable ○ Disable

WDS Discovery: ● Auto Discovery

○ Specified Discovery: DISABLED (IP Address)

Username: client-ap

Password: •••••

Confirm Password: •••••

After this has been configured you can verify that the Client AP has registered with the WDS Server AP by clicking on the Wireless Services tab and verifying that the AP has registered. The wireless infrastructure has now been configured to pass Radio and Security management information to the WLSE.

As of WLSE version 2.11 a wizard has been created to simplify the initial deployment of Radio and Security Management. This wizard is covered in more detail in the WLSE 2.11 Configuration and Management guide at the following URL: http://www.cisco.com/en/US/partner/products/sw/cscowork/ps3915/products_user_guide_chapter09186a008037cc1d.html

Radio Management

Radio Management provides configuration guidance and real-time performance information on your Wireless LAN. Radio management is an essential component of WLAN deployments to account for the dynamic nature of RF environments.

Key configuration guidance is provided by the following features;

- *Assisted Site Survey*—Provides guidance on channel selection and power selection of Access Points
- *Assisted Re-Site Survey*—Gathers performance data from Access Points and provides report on actual WLAN performance
- *Interference Detection*—Detects interference in the RF environment
- *Provide Location Maps*—RF Coverage Maps

While this configuration guide will not cover Radio Management in great detail, Table 9-1 shows the configuration steps for a typical Radio Management deployment.

Table 9-1 Radio Management Configuration Steps

Configuration Step	Command
Enable Radio Monitoring	**Radio Manager>Radio Monitoring**
Add building floor plans to the WLSE Location Manager	**Location Manager**
Place Access Points in correct locations on the respective floor plans	**Location Manager**
Perform an assisted site survey	**Location Manager>Wizard>Assisted Site Survey**
Configure a floor to self-heal in the event of radio failure or RF interference	**Radio Manager>Self Healing**

Radio monitoring can be enabled to monitor the serving channel or monitor all radio channels. Note that when Access Points are configured to monitor all radio channels, the radio will go off channel for a brief interval (~40 ms) so in critical environments with high traffic loads you may want to only monitor the serving channel.

After the environment has stabilized and the WLSE has gathered sufficient performance information from the WLAN you can perform an Assisted Re-Site Survey to get a feeling for the performance characteristics of the current RF environment.

Additional details on radio management can be found in the detailed WLSE Radio Management guide at;
http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_user_guide_chapter09186a00803a241d.html

Security Management

The configuration for Radio Management also enables Security Management on the WLSE. Since the inception of Wireless LANs security has been an issue as all communication is transacted on an RF medium that is susceptible to a variety of attacks. These attacks include capture, insertion, client spoofing, determining encryption key, disassociation, and RF interference. A brief summary of some of the detected signatures is shown below;

Security Management on the WLSE detects and reports the following events;

- *Rogue Access Points*—Rogue access point detection scans for beacons from access points not managed by the WLSE. Each access point sends out a beacon on a regular interval (often 100ms) so clients can discover the AP and attempt to associate. To find access points the WLSE listens for beacons looks for BSSIDs that are not managed by the WLSE.
- *RF Interference*—RF Interference can come from both benign sources—microwaves, cordless phones, and other RF emitting equipment—and intentional sources which are directed to be a denial of service on the radio environment. Often this aimed at disrupting the existing WLAN.
- *Ad-hoc Networks*—Since ad-hoc networks are between clients there is no inherent requirement for encryption or security, and as such present a vulnerability because anyone can attempt to associate to an ad-hoc network
- *Unregistered Clients*—Unregistered clients are clients that unsuccessfully attempt to authenticate to the WLAN a specified number of times
- *Authentication Failures*—Detects attempted replay and insertion attacks on the WLAN
- *Wireless MAC Spoofing*—Detects client attempting to spoof another clients wireless MAC Address
- *EAPOL Flood Detection*—This detects a user that is generating an abnormal number of EAP requests to the radius server. This is often an attempt at brute forcing user passwords or a denial of service on the radius server.

Depending on the layout of your RF environment you must carefully select whether you will scan on non-serving channels or restrict your scans to serving channel. If you opt to only scan on the serving channel you can easily miss security events on other channels which would be detected otherwise.

When the WLSE detects a security event you can configure the action for WLSE to take. It can generate a fault on the WLSE, send an SNMP trap to a northbound management system, or send an email to a configured address.

Once you are alerted to the security event additional detail can be viewed through the Faults tab on the WLSE. And on the location manager you can also display the location of the fault.

The WLSE can also be configured to respond automatically to certain security events—such as a rogue access point—and automatically suppress the rogue device. Rogue devices can only be suppressed on your trusted infrastructure and rely on a correlation between the Rogue BSSID and the Rogue’s Ethernet MAC address (BSSID = Ethernet MAC +- 1). While this relationship holds true for most “Home” class access points, it does not hold true for many enterprise class products. For these devices it is recommended to locate them via triangulation in the location manager.

Additional details on Security Management can be found in the WLSE 2.11 IDS configuration guide at; http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_user_guide_chapter09186a0080365135.html

Reporting Overview

The WLSE has the ability to generate a wealth of reports on either an ad-hoc basis or automatically generated and sent via email. These reports are grouped into several classes listed below;

- *Device Report*s—Generates reports on individual devices, including configuration, fault, and firmware history. Can also generate reports on managed WDS Registered Access Points and a summary reports on all managed access points.
- *Radio Management Reports*—Radio Management reports are focused on the RF environment and can provide reports on RF path loss, channel loading, and radar detection (802.11h) events.
- *Client Reports*—Detailed reports on clients, including client association/authentication, client roaming events, and client authentication failures.
- *Trend Reports*—Providing historical information to gauge the utilization of your WLAN. Can provide statistics on RF Utilization, Top N Client, Top N Associations, and other capacity related reports.
- *Real-Time Reports*—These reports are most useful in troubleshooting issues on a specific access point, they detail the CPU, Memory, Association Attempts, and Utilization in Real-Time.
- *Current Report*s—Current reports can return configuration or status reports on groups of Access Points. These reports can summarize the configuration of a building, or alternatively, report a list of clients associated to a group of Access Points. By applying reporting capability to the groups created by the WLSE and WLAN administrator you can generate many customized reports.

To view a more detailed summary of the reporting capabilities of the WLSE, you can access the "Using Reports" section of the WLSE 2.11 User Guide. http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_user_guide_chapter09186a00803640b5.htm

Management Summary

The WLSE is a powerful tool in deploying and maintaining Wireless LAN deployments. In terms of functionality this overview has served to cover the product at a very high level, with the intention of giving the administrator a quick tour of the functionality.

Several key functions of the WLSE, such as fault management were not covered in detail, and are left to the comprehensive product guide located at; http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_user_guide_book09186a0080363fb0.html

CHAPTER 10

WLAN Guest Network Access

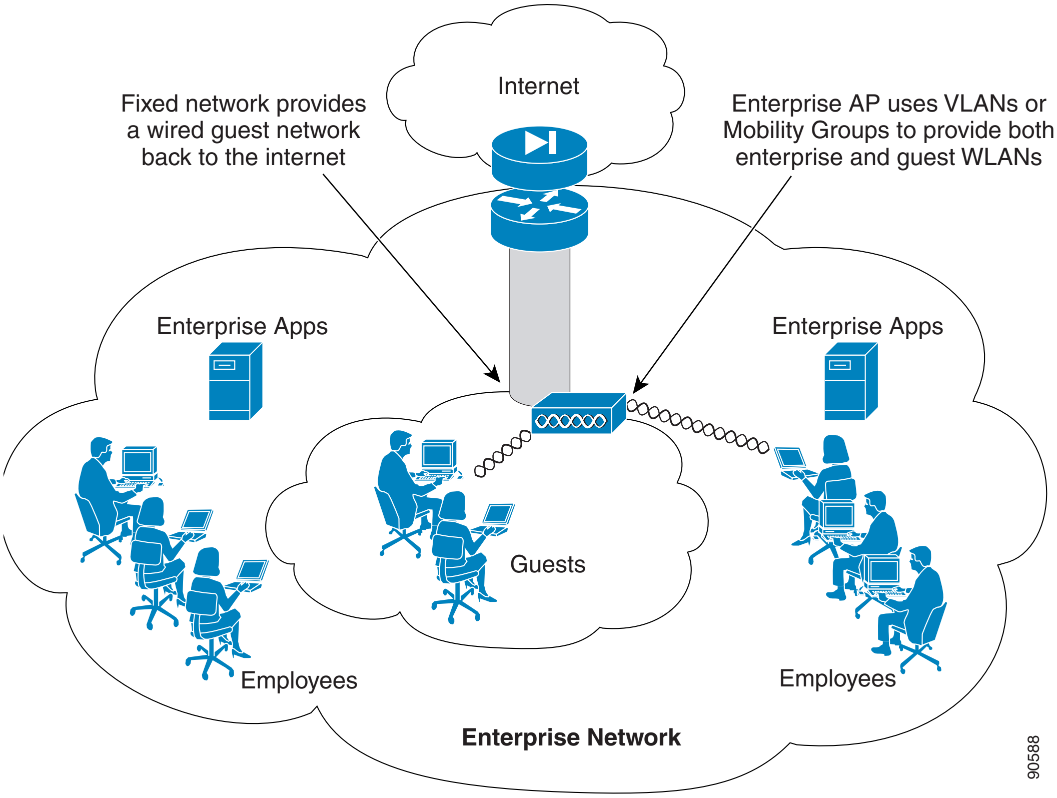
This chapter presents the advantages, considerations, and proposed configuration for a *WLAN Guest Network* access and addresses the following key topics:

- Reasons for providing Guest Network access
- WLAN as one of the best mechanisms for providing Guest Network access
- Considerations in a WLAN Guest Network implementation

The need for guest access has evolved as the needs of guests have evolved. Once it was sufficient to provide guests a chair and a phone. Today, with laptops, networked application, and digital phone lines, a guest visiting your enterprise is *disconnected and disempowered* without access to these technologies.

Guest Networks are network connections provided by an enterprise to allow their guest to gain access to the Internet, and the guest's own enterprise without compromising the security of the host enterprise. Figure 10-1 illustrates the Guess Access Network concept. Guests are within the Enterprise Network, but are only able to access the Internet; enterprise employees have full access to the enterprise applications and the Internet.

Figure 10-1 Guess Access Network


Internet
Fixed network provides a wired guest network back to the internet
Enterprise AP uses VLANs or Mobility Groups to provide both enterprise and guest WLANs
Enterprise Apps
Enterprise Apps
Guests
Employees
Employees
Enterprise Network
90588

Benefits of Guest Network Access

Initially, the lack of network access for guests may not seem to be an issue, but we need to remember that we have guests because we want them. A guest may be a business partner, a technician, or salesperson who has been brought to the enterprise to perform a task, and without Guest Network access their performance is degraded. As businesses become more networked, with outsourcing of non-core activities, this degradation increases if the network access is not provided.

Increased Security

It may appear counter-intuitive that Guest Network access increases security, but the reality is that Guest Network access does occur in Enterprise Networks now, but in an uncontrolled manner. These guests are not hackers; they are simply motivated people trying to get their job done. The main concern with these guests is that they are a potential source of viruses, worms, and Trojans. The PC with which they connect to the Enterprise Network might not have the security systems that exist on the local enterprise PCs.

Guest Network access provides guests of this type with a way to connect to an Enterprise Network in order to be more productive, while limiting the risk to the host organization. Why risk violating policy and risk the relationship with the host when there is a credible solution?

Increased Productivity

The guest of an enterprise is there for a reason, because the enterprise wants them to perform a task. The more efficiently this task is performed the better it is for both enterprises. If a service technician is visiting the enterprise, it is in the enterprise's interest for that service/repair to happen within the minimum amount of time and with the least amount of disruption

If a salesperson is visiting the enterprise, it is in the enterprise's interest that the information be accurate and up-to-date. By having immediate access to information, the salesperson is able to position products appropriately and answer as many questions as possible while at the enterprise. This immediate responsiveness could potentially lead to orders being placed while on-site.

Benefits of WLAN Guest Network Access

WLAN technology can provide Guest Network access because of the following characteristics:

- Provides wide coverage, including areas such as lobby and waiting rooms that may not traditionally have cabling
- Removes the need to have a dedicated location for guest access
- Allows partners to access their network resources while in meeting rooms, offices, giving them the productivity benefits that WLAN gives the enterprise employees.
- Provide authorization, agreement and disclaimer notification to the guest user.
- Provide an audit mechanism for guest users.

Deployment Considerations and Caveats

The greater range of WLANs, which is an advantage in deploying Guest Networks, also introduces issues:

- *User Authentication*—People who are not guests may access the Guest Network through their physical proximity to the WLAN Guest Network. This is not an issue in a wired network, as the guest has to be brought past the physical security. This means that the WLAN Guest Network requires user authentication, authorization and accounting, above that required for the wired network.
- *Authentication Options*—There are several models for authenticating guests:
  - The use of a web interface such as Cisco Building Broadband Service Manager (BBSM), Cisco Clean Access or Cisco IOS Authentication Proxy.
- *Web Authentication*—Web interface authentication relies on the ubiquity of HTML browsers. Prior to using the Guest Network, users must launch their HTML browser, and try to access a web site. The user's HTML browser is forced to an authentication page, and the users must enter their authentication details before access is granted. The HTML browser authentication does not generate dynamic per session encryption keys and in order to make the WLAN easy to use and easy to support no static encryption is used on the WLAN link. This means that authenticated users are only distinguishable from unauthenticated users through their IP addresses and MAC addresses (if on the same Layer-2 network). As the IP address and MAC address are sent in clear text they are open to exploitation through IP address and MAC address spoofing.

Note As of this writing, the BBSM is specifically designed for guest access applications, and apart from providing a sophisticated HTML controlled user interface, it provides MAC-level verification if the client is on the same Layer-2 network as the BBSM, and uses switch and AP management interfaces to control where and when a client can use the network. Cisco Clean Access is another software solution that can be used for guest access. A typical Clean Access deployment consists of a Clean Access Server that initiates device assessment and enforces access privileges based on endpoint compliance and a Clean Access Manager used to establish roles, checks, rules and policies.

- *Cisco IOS Authentication Proxy*—Included in the Cisco IOS firewall feature set; provides a simple HTML interface; and controls access based upon a clients IP address.
- *Specialized Clients*—Ideally guests should use 802.1x/EAP to authenticate to the Enterprise Network, and generate a dynamic encryption key for their wireless session. This would be the preferred solution as it provides authentication, authorization and privacy. Given that different enterprises are at different stages in their 802.1x/EAP maturity, guests cannot (yet) be expected to have compatible 802.1x/EAP clients on their PCs.
- *IPSec VPN Clients*—Another client that offers strong authentication, authorization and privacy and could potentially be used as a Guest Network access client. The major barrier in this case would be the installation of an appropriate client on guest machines, and the interaction of two IPSec VPN clients, one client providing guest access and the other client providing secured access across the Internet to the guest’s home network.
- *Time of Day Control*—Just as physical security can control who has access to the wired network, it can also control who is present at a particular time of day. As WLAN cannot rely upon physical security to control users it cannot stop users from accessing the network outside of permitted hours. This means that the WLAN Guest Network must provide time of day control over when the service is made available.
- *Additional Security*—Given the weakness described above, the WLAN Guest Network could not be considered as secure as the wired network and might require additional policies, processes, configuration, and equipment to ensure that an attack on the Enterprise Network through the WLAN Guest Network is not successful.
- *Wired Network*—The wired network contains the key components that control the Guest Network. Guests get authenticated access to the Internet, while ensuring that guests are not able to access the host enterprise’s systems. There are three primary configurations in the wired network:
  - VLAN controlled access, where the wired Guest VLAN is extended all the way to the authentication device and the Internet. This applies to the non-switched mode of Cisco Unified Wireless Network.
  - Mobility group controlled access, where guest data is GRE encapsulated to the supervisor of the 6500 switch, and then extended potentially via VRF to the authentication device and the Internet. This applies to the switch-based mode of Cisco Unified Wireless Network.
  - ACL controlled access, where guest traffic shares the same Layer-3 network as enterprise traffic to get to the internet, but is prevented from accessing the Enterprise Network through the use of ACLs routing table and separation (where Guest Network traffic uses separate routing tables on the Enterprise Network to prevent access to the Enterprise Network).

  The choice of which wired-network configuration is best depends on the existing Enterprise Network. The configuration of the wired Enterprise Network to provide Guest Network access and the transport of Guest Network traffic is discussed in Chapter 5.

- *Other Considerations from Wired Network*—Even though the WLAN Guest Network is primarily a WLAN extension of a wired Guest Network, the lack of control of physical access and the possible spoofing legitimate users to gain access heighten the security risk associated with Guest Networks. Therefore additional tools—such as Intrusion Detection Systems (IDS) should be considered to detect suspicious behavior.

Guest WLAN Recommendations

The following actions are key Guest WLAN setup recommendations:

1. Create a Guest WLAN VLAN (non-switched mode) or Mobility group (switch-based mode) with no encryption, open authentication, and a broadcast "guest" SSID. MBSSID (Multiple Basic Service Set Identifier) is a new feature in IOS 12.3(4) JA. MBSSID allows an AP to broadcast multiple SSIDs each with their own MAC addresses. MBSSID will be discussed later in this chapter.
2. Choose a Wired Guest Network model that best fits your Enterprise Network.
3. Choose an HTML authentication service that best fits your needs and topology.
4. Add application filters, time of day controls and IDS as required.

Recommended 802.11 Configuration for WLAN Guest Network

The biggest challenge in WLAN Guest Network access is to support the widest number of possible guests without having to provide IT support for the guests. It is recommended that WLAN Guest Network access use:

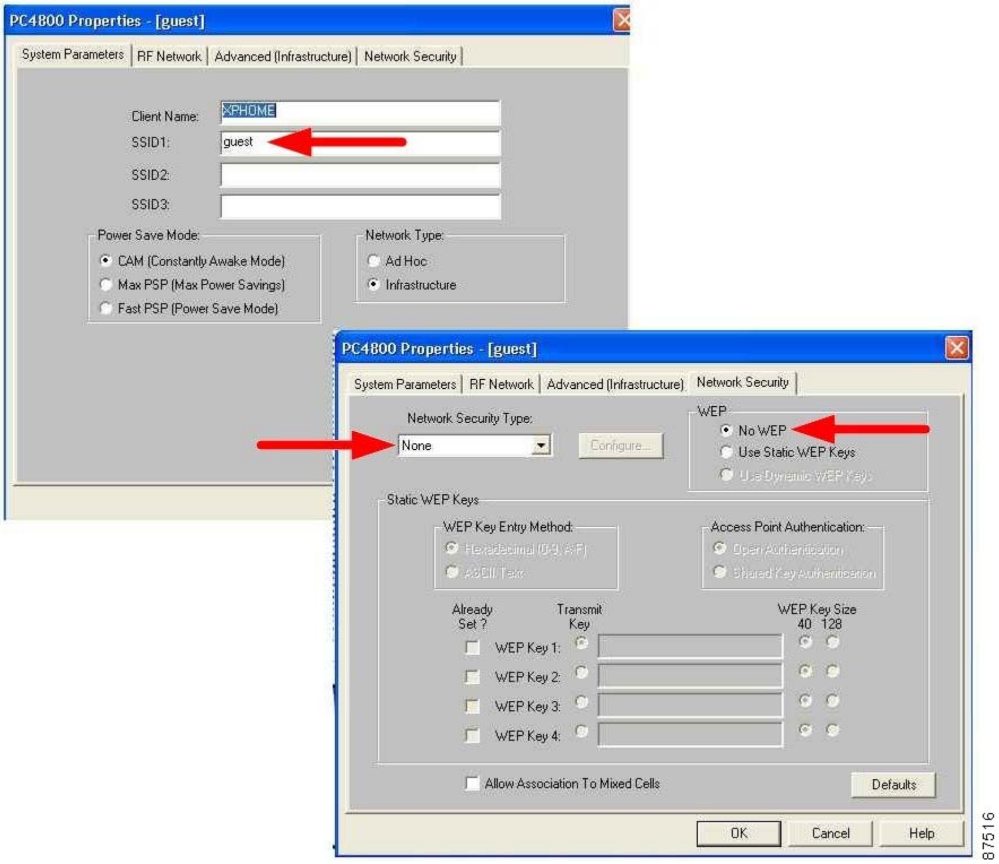
- *A Broadcast SSID*—Some WLAN clients only operate with a broadcast SSID.
- *Open Authentication*—The default configuration.
- *No Encryption*—The entry and format of the WEP key varies from client to client, users can easily incorrectly enter the WEP key, and the WEP key would quickly become compromised as it is being distributed in an uncontrolled manner.

This allows the Guest Access WLAN to adopt the minimum configuration while serving the widest range of WLAN clients. It also matches the configuration most used in WLAN hotspots today.

Figure 10-2 shows the Aironet Client Utility (ACU) configuration that would be used to gain access to the Guest Network. The key features of this setup are as follows:

- The SSID ID is configured to match the SSID that is broadcast by the enterprise WLAN Guest Network, a blank entry would also suffice if the AP is configured as recommended in this document.
- Network Security Type is none; this is "Open Authentication".
- No WEP is selected.

Figure 10-2 ACU Configuration



PC4800 Properties - [guest]

System Parameters | RF Network | Advanced (Infrastructure) | Network Security

Client Name: XPHOME
SSID1: guest
SSID2:
SSID3:

Power Save Mode:
- ● CAM (Constantly Awake Mode)
- ○ Max PSP (Max Power Savings)
- ○ Fast PSP (Power Save Mode)

Network Type:
- ○ Ad Hoc
- ● Infrastructure

PC4800 Properties - [guest]

System Parameters | RF Network | Advanced (Infrastructure) | Network Security

Network Security Type: None

WEP
- ● No WEP
- ○ Use Static WEP Keys
- ○ Use Dynamic WEP Keys

Static WEP Keys

WEP Key Entry Method:
- ○ Hexadecimal (0-9, A-F)
- ○ ASCII Text

Access Point Authentication:
- ○ Open Authentication
- ○ Shared Key Authentication

Already Set ?		Transmit Key		WEP Key Size 40	128
□	WEP Key 1:	○		○	○
□	WEP Key 2:	○		○	○
□	WEP Key 3:	○		○	○
□	WEP Key 4:	○		○	○

□ Allow Association To Mixed Cells

Configuring Guest WLANs

This section presents the following discussions addressing Guest WLAN configuration:

Network Topology

Figure 10-1 shows a general schematic illustrating how Guest Network traffic is tunneled across the Enterprise Network. This tunnel can be achieved via multiple technologies depending on the Enterprise Network architecture and requirements.

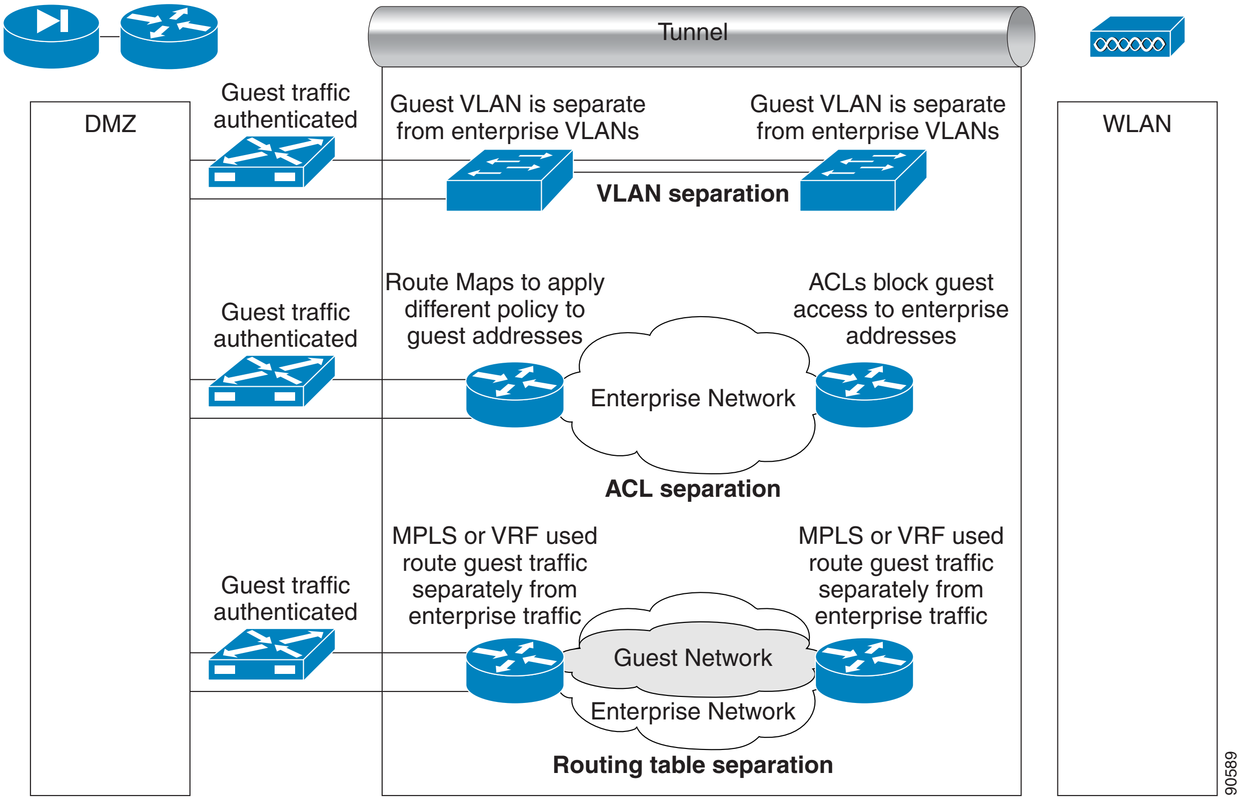
Figure 10-3 shows a schematic of three different tunnel possibilities:

- *VLAN Separation*—The Guest VLAN is extended all the way to DMZ. This is normally implemented with non-switched mode Cisco Unified Wireless Network.
- *ACL Separation*—The Guest VLAN is terminated at an access router; ACLs are used to ensure that Guest Network traffic is unable to go to enterprise addresses.
- *Routing Table Separation*—The Guest VLAN terminate at the access router and separate routing tables ensure that Guest Network traffic is able to go nowhere but the DMZ. As part of Cisco Unified Wireless Network switch-based mode the guest Mobility group is terminated at the central switch. The guest data can then be forwarded via separate routing tables (VRF).

In this example, for each of the tunneling possibilities Guest Network users are authenticated by a BBSM before gaining access to the DMZ. Authentication of users of the Guest Network is needed to prevent the Guest Network being used for non-authorized purposes. The BBSM is an example of a Cisco Product designed for this purpose, but other tools such as, Cisco Clean Access, Cisco IOS and PIX authentication proxy may be used.

In the following sections we will describe VLAN separation in non-switched mode Cisco Unified Wireless Network and switch-based mode Routing Table (VRF) separation for Guest Access.

Figure 10-3 General Guest Network Topology


Tunnel
DMZ
WLAN
Guest traffic authenticated
Guest VLAN is separate from enterprise VLANs
Guest VLAN is separate from enterprise VLANs
VLAN separation
Guest traffic authenticated
Route Maps to apply different policy to guest addresses
ACLs block guest access to enterprise addresses
Enterprise Network
ACL separation
Guest traffic authenticated
MPLS or VRF used route guest traffic separately from enterprise traffic
MPLS or VRF used route guest traffic separately from enterprise traffic
Guest Network
Enterprise Network
Routing table separation
90589

AP and Switch Configuration

For the purpose of this example, these configurations deal with the configuration of a Guest Network access WLAN VLAN on an AP that also supports three other WLAN VLANs named *PEAP*, *IPSec* and *LEAP* (with the VLAN name *LEAP* used here representing an EAP-Cisco implementation) that map to VLANs on the Ethernet interface of the AP.

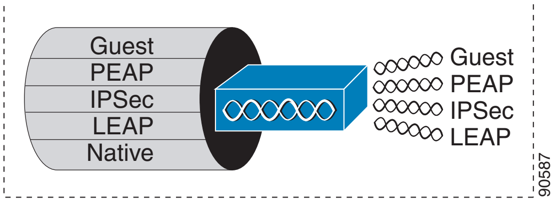
The configuration of *PEAP*, *IPSec*, and *LEAP* is not discussed in this chapter, and for information on WLAN AP and Client configuration refer to:

http://www.cisco.com/en/US/products/hw/wireless/ps458/prod_instructions_guides.html

Figure 10-4 shows a schematic of the example configuration used in this chapter that has four WLAN VLANs and five VLANs on the AP. The difference in number of VLANs is due to the addition of a *native* VLAN for the administration of the AP.

http://www.cisco.com/en/US/products/hw/wireless/ps458/prod_instructions_guides.html

Figure 10-4 Multiple VLANs including a Guest Network VLAN



The configuration fragment below shows an example configuration for the switch connecting the AP to the Enterprise Network. Points to note include:

- VLAN 1 which is the native VLAN
- The VLANs allowed for the AP connection are limited to the mandatory VLANs (1, 1002-1005) and the VLANs used on the AP (1,10, 20, 30, 40).

```
interface FastEthernet0/3
     switchport trunk encapsulation dot1q
     switchport trunk native vlan 1
     switchport trunk allowed vlan 1,10,20,30,40
     switchport mode trunk
```

WLAN Guest VLAN Filtering

When applying network access control filters, a general rule is that these filters should be placed as close as possible to the users whose access is being controlled.

In the case of WLAN guest networking, the closest point at which access control filters can be placed is the WLAN VLAN on the AP.

Although the filtering that can be applied is limited by the need to support the applications accessible by guests, there are simple filters that can be applied:

- *Protocol Filters*—Guests would be expected to use specific protocols, such as ARP and IP; all other protocols on the WLAN guest VLAN can be blocked.
- *Source Address*—The users on the WLAN guest VLAN will have IP addresses assigned through DHCP, and the AP (Cisco IOS APs only); as a result, network administrators can apply address filters to permit access by specific network addresses, while block others.

Terminology Notes

The introduction of VLANs to the APs introduces a number of new definitions such as:

- *Default VLAN*—This is the VLAN associated by default with an SSID, the name allows for the RADIUS server to provide a different VLAN number based on the group membership of a user.
- *Primary SSID*—The AP is only capable of sending one set of information in its beacons; the information that is sent in the beacons is that of the VLAN associated with the Primary SSID.
- *Guest SSID*—The AP can only have a single VLAN that accepts traffic that is not encrypted. The SSID associated with this VLAN is called the Guest SSID.
- *Infrastructure SSID*—Infrastructure such as repeaters and workgroup bridges can be associated with the AP on one particular VLAN. The SSID associated with this VLAN is called the *Infrastructure SSID*.

- *Native VLAN*—802.1q allows for one of the VLANs in the trunk to be native thereby not requiring 802.1q encapsulation and making it possible to remain connected with the AP when trunking is enabled on the switch before it is on the AP, or visa versa. The VLAN that is given this capability is called the Native VLAN.

AP Configuration

The key AP configuration processes are presented in the following sections.

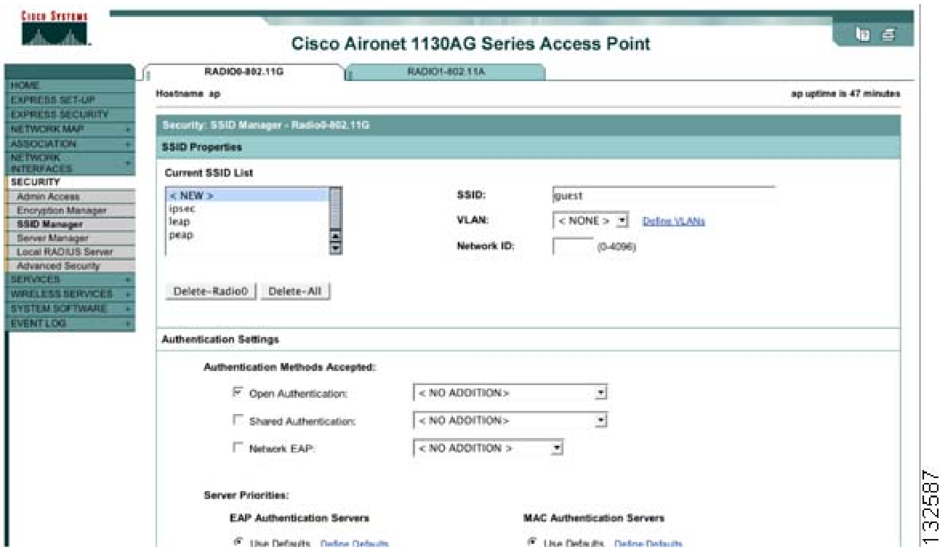
Configuring SSIDs

Figure 10-5 shows the Security: SSID Manager screen. It shows that three SSIDS have been setup. Guest access SSID name is “guest,” but the SSID can be anything the enterprise feels appropriate. When an SSID is added or edited the authentication mechanism for the SSID can be set For “guest,” the authentication settings are set for “open” allowing the broadest range for connectivity among a diverse set of clients. Once the “guest” SSID is created, the Security:SSID Manager Global Radio Properties: Set Guest Mode SSID should be set for guest access on either or both radios. As a note, with dual radio Access points, SSIDs (both guest and others) and be applied to either or both of the radios by “applying radio-0” or “apply both” buttons. Figure 10-6 shows the screen for the dual mode AP 1130 802.11 G radio.

Note The Primary SSID is the one advertised in beacons. Since a broadcast SSID is recommended for guest use, this is the SSID that should be made primary. To ensure successful configuration this should be the first SSID configuration made, because ownership of the Primary SSID cannot be transferred to another SSID.

Cisco Enterprise Distributed Wireless Solutions Reference Network DesignThe Guest VLAN should not be used for *Infrastructure Stations*, and therefore another VLAN must be chosen and *Infrastructure Stations* on other VLANs disallowed.

Figure 10-5 The Security: SSID Manager Screen



Hostname ap

ap uptime is 47 minutes

Security: SSID Manager - Radio0-802.11G

SSID Properties

Current SSID List

< NEW >
ipsec
leap
peap

SSID: guest

VLAN: < NONE >

Network ID: (0-4096)

Authentication Settings

Authentication Methods Accepted:

☑ Open Authentication: < NO ADDITION>

□ Shared Authentication: < NO ADDITION>

□ Network EAP: < NO ADDITION >

Server Priorities:

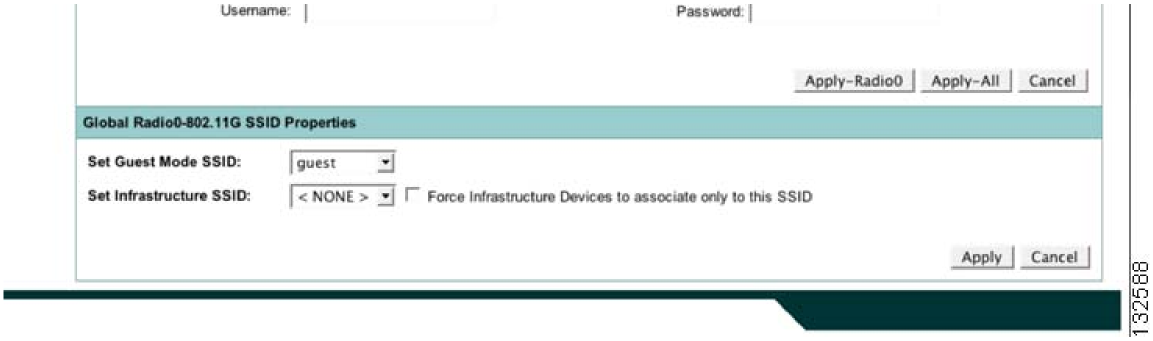
EAP Authentication Servers

● Use Defaults

MAC Authentication Servers

● Use Defaults

Figure 10-6 Dual Mode AP 1130 802.11 G Radio Screen



Username:

Password:

Global Radio0-802.11G SSID Properties

Set Guest Mode SSID: guest

Set Infrastructure SSID: < NONE > □ Force Infrastructure Devices to associate only to this SSID

Multiple Broadcasts Service Set Indentifiers (MBSSID)

Access points are identifiable by their Ethernet MAC address. The MAC address is used as the source address for 802.11 MAC layer operations and data frames. Subsequent to IOS release 12.3(4), multiple SSIDs were advertised by a single AP using a single MAC address, MBSSID allows eight different MAC addresses per radio and up to 16 per AP (on a dual radio). Each MAC address can be used as a source address for the broadcast SSID. MAC addresses are assigned sequentially from the base MAC address (ending in zero). With the ability to broadcast multiple SSIDs and the case of despots (such as airports and coffee shops) allows different services (even potentially different service providers) to be offered by each SSID. Also with these multiple broadcasts increased accessibility is provided for those client cards who cannot provide “active scanning” for APs. MBSSID also provides the ability to uniquely configure per SSID Delivery Traffic Indication Message (DTIM). This is important for devices whose battery life is limited and implement PSP (power saving mode). PSP clients “go to sleep” and must wake up based on the DTIM interval to check for buffered data. With MBSSIDs, DTIM intervals can be uniquely set for specific device types such as bar code readers per specific SSIDs.

Note Not all radios support MBSSIDs. To check for MBSSID support:

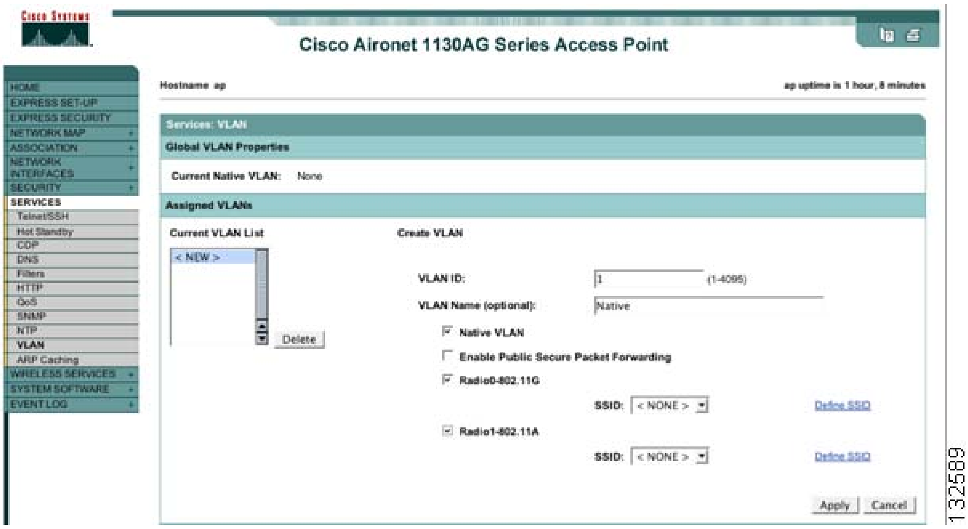
```
ap#show cont dot 0
!
interface Dot11Radio0
Radio AIR-AP1131G, Base Address 0012.44b3.a0c0, BBlock version 0.00, Software version
5.70.5
Serial number: GAM09071XWX
Number of supported simultaneous BSSID on Dot11Radio0: 8
Carrier Set: Americas (US )
ap#show cont dot 1
!
interface Dot11Radio1
Radio AIR-AP1131A, Base Address 0012.44b7.a0a0, BBlock version 0.00, Software version
5.70.5
Serial number: ALP09071XWX
Number of supported simultaneous BSSID on Dot11Radio1: 8
Carrier Set: Americas (UNI2ML OFDM) (US )
```

Configuring VLANs

To ensure contiguous communication with the AP, care should be taken to have a Native VLAN configured before 802.1q tagging is enabled. Figure 10-7 shows the *Sevices:VLAN* screen, this allows individual VLANs to be created or removed, and the Native VLAN, and Unencrypted VLAN (Guest VLAN) to be set. In this example:

- Configurations for this example are identical for both A and G radios
- VLANs are enabled by selecting 802.1Q tagging.The Native VLAN (VLAN1) is the VLAN that will have the AP's IP interface. The Native VLAN has no associated SSIDs.

Figure 10-7 Creating the Native VLAN



Cisco Aironet 1130AG Series Access Point

Hostname ap
ap uptime is 1 hour, 8 minutes

Services: VLAN

Global VLAN Properties

Current Native VLAN: None

Assigned VLANs

Current VLAN List: < NEW >

Create VLAN

VLAN ID: 1 (1-4095)

VLAN Name (optional): Native

☑ Native VLAN

□ Enable Public Secure Packet Forwarding

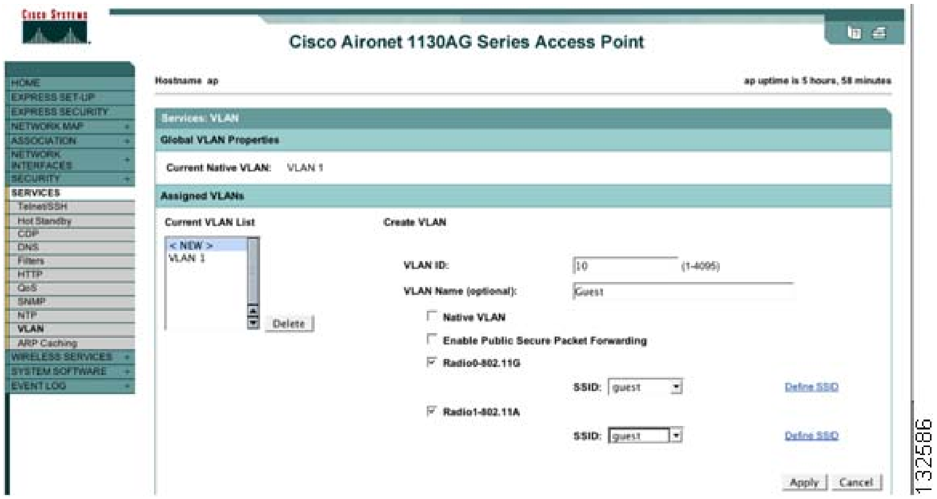
☑ Radio0-802.11G

SSID: < NONE >

☑ Radio1-802.11A

SSID: < NONE >

Figure 10-8 Creating the Guest VLAN



Cisco Aironet 1130AG Series Access Point

Hostname ap
ap uptime is 5 hours, 58 minutes

Services: VLAN

Global VLAN Properties

Current Native VLAN: VLAN 1

Assigned VLANs

Current VLAN List: < NEW >
VLAN 1

Create VLAN

VLAN ID: 10 (1-4095)

VLAN Name (optional): Guest

□ Native VLAN

□ Enable Public Secure Packet Forwarding

☑ Radio0-802.11G

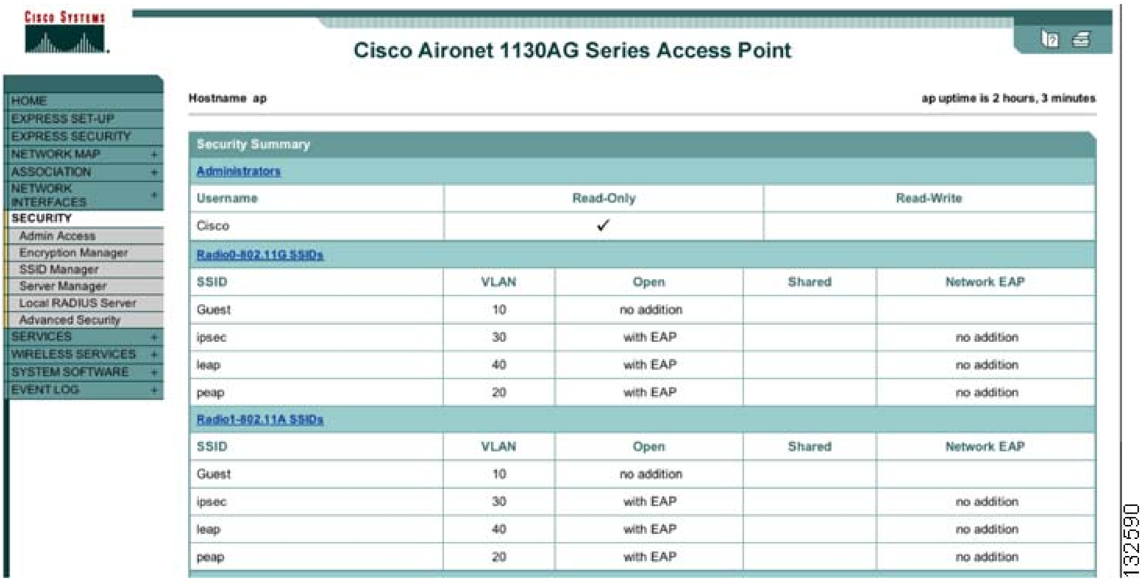
SSID: guest

☑ Radio1-802.11A

SSID: guest

When the Apply button creates a new VLAN, the screen automatically changes to reflect the updated information. Figure 10-9 show the summary screen for SSIDs.

Figure 10-9 SSID Summary Screen



Cisco Aironet 1130AG Series Access Point

Hostname ap

ap uptime is 2 hours, 3 minutes

Security Summary

Administrators

Username	Read-Only	Read-Write
Cisco	✓	

Radio0-802.11G SSIDs

SSID	VLAN	Open	Shared	Network EAP
Guest	10	no addition		
ipsec	30	with EAP		no addition
leap	40	with EAP		no addition
peap	20	with EAP		no addition

Radio1-802.11A SSIDs

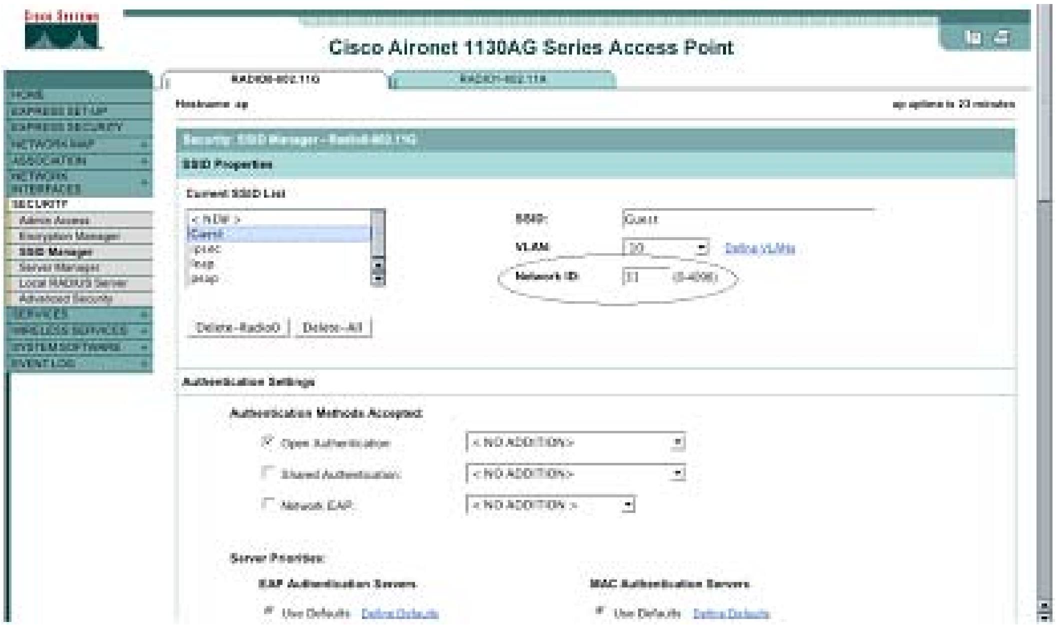
SSID	VLAN	Open	Shared	Network EAP
Guest	10	no addition		
ipsec	30	with EAP		no addition
leap	40	with EAP		no addition
peap	20	with EAP		no addition

Creating Guest Mobility Groups

For switched-based WLAN solution, data from autonomous access point is tunneled using mGRE to the supervisor module of the 6500 Catalyst switch. To enable that, the autonomous access point must be configured with an authentication, key management and Network ID, and identifying the mobility group belonging to the guest's SSID. Figure 10-10 shows the assignment of the Network ID to the guest access SSID. Note VLANs play a different role in switch-based mode AP configuration versus non-switched. VLANs in switch-based mode are of local significance to the AP point only providing a mechanism allowing a specific encryption type per SSID. Also VLANs do not need to be created on the switch since the VLANs are local to the AP. When using the switch-based mode and WLSM there will always be a Layer 3 hop between the wireless clients and the authentication server. One way to force the guest wireless traffic to the authentication server through the switch is to use VRF to establish a completely separate routing table where a default route is configured to point to the location of the authentication server's network.

Note In this Layer 3 mode, the client's MAC address is not carried as part of the IP packet

Figure 10-10 Assigning Network ID to Guest SSID



Hostname ap

ap uptime is 23 minutes

Security: SSID Manager - Radio0-802.11G

SSID Properties

Current SSID List

< NEW >
Guest
ipsec
leap
peap

SSID: Guest

VLAN: 20 Define VLANs

Network ID: 31 (0-4096)

Authentication Settings

Authentication Methods Accepted:

☑ Open Authentication: < NO ADDITION>

☐ Shared Authentication: < NO ADDITION>

☐ Network EAP: < NO ADDITION >

Server Priorities:

EAP Authentication Servers

● Use Defaults Define Defaults

MAC Authentication Servers

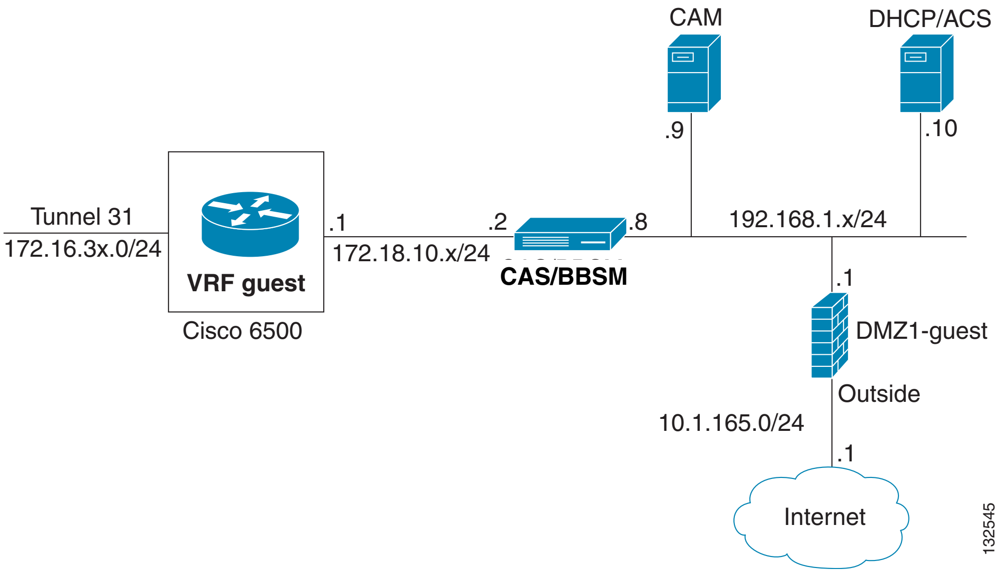
● Use Defaults Define Defaults

The following 6500 switch configuration examples show how to provide the VRF routing separation for guest access traffic.

```
description Establish guest VRF and a unique route descriptor
ip vrf guest
 rd 100:3
description Establish loopback number and address
interface Loopback3x
 description  Guest
  ip address 10.3.103.x 255.255.255.255 (example address)
!
description Establish  Tunnel number and source address, vrf forwarding, helper address,
and mobility network ID (same as configured on AP)
interface Tunnel3
description  Guest
 ip vrf forwarding guest
 ip address 172.16.3x.1 255.255.255.0 (example address)
 ip helper-address 192.168.1.10 (example address)
 no ip redirects
 ip dhcp snooping packets
 tunnel source Loopback3x
 tunnel mode gre multipoint
 mobility network-id 31

description Install a default route in the VRF guest and the IP address where the
authenication server resides
ip route vrf guest 0.0.0.0 0.0.0.0 172.18.10.2 (example address)
```

Figure 10-11 Logical Topology for Guest Access



For further details on BBSM or Cisco Clean Access see:

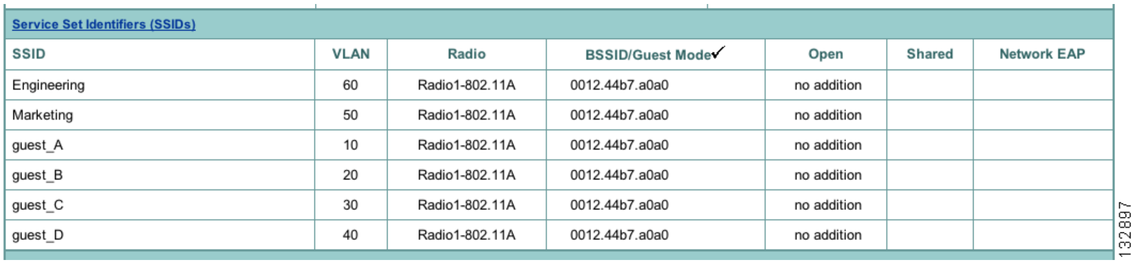
BBSM:
http://www.cisco.com/en/US/partner/products/sw/netmgtsw/ps533/products_user_guide_chapter09186a008019228c.html

Cisco Clean Access:
http://www.cisco.com/en/US/partner/products/ps6128/products_user_guide_list.html

Configuring MBSSID

To configure MBSSIDs create the desired SSIDs and tie them to VLANs or Mobility group (Network ID). Figure 10-12 show an example of SSIDs and VLANs.

Figure 10-12 SSID and VLANs Display

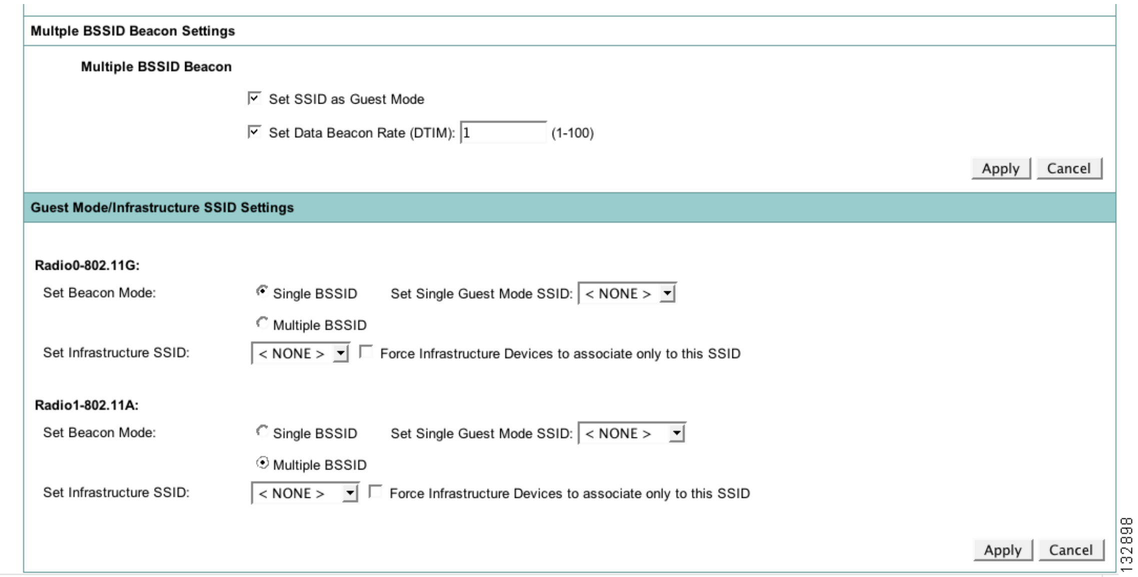


Service Set Identifiers (SSIDs)

SSID	VLAN	Radio	BSSID/Guest Mode✓	Open	Shared	Network EAP
Engineering	60	Radio1-802.11A	0012.44b7.a0a0	no addition		
Marketing	50	Radio1-802.11A	0012.44b7.a0a0	no addition		
guest_A	10	Radio1-802.11A	0012.44b7.a0a0	no addition		
guest_B	20	Radio1-802.11A	0012.44b7.a0a0	no addition		
guest_C	30	Radio1-802.11A	0012.44b7.a0a0	no addition		
guest_D	40	Radio1-802.11A	0012.44b7.a0a0	no addition		

As part of the SSID definition to configure MBSSIDs under Guest Mode/Infrastructure SSID settings, “Set Beacon Mode” must be set to “Multiple BSSID” as displayed in Figure 10-13.

Figure 10-13 Configuring MBSSIDs Under Guest Mode/Infrastructure SSID Settings



Multple BSSID Beacon Settings

Multiple BSSID Beacon

☑ Set SSID as Guest Mode

☑ Set Data Beacon Rate (DTIM): 1 (1-100)

Guest Mode/Infrastructure SSID Settings

Radio0-802.11G:

Set Beacon Mode: ● Single BSSID Set Single Guest Mode SSID: < NONE >
○ Multiple BSSID

Set Infrastructure SSID: < NONE > □ Force Infrastructure Devices to associate only to this SSID

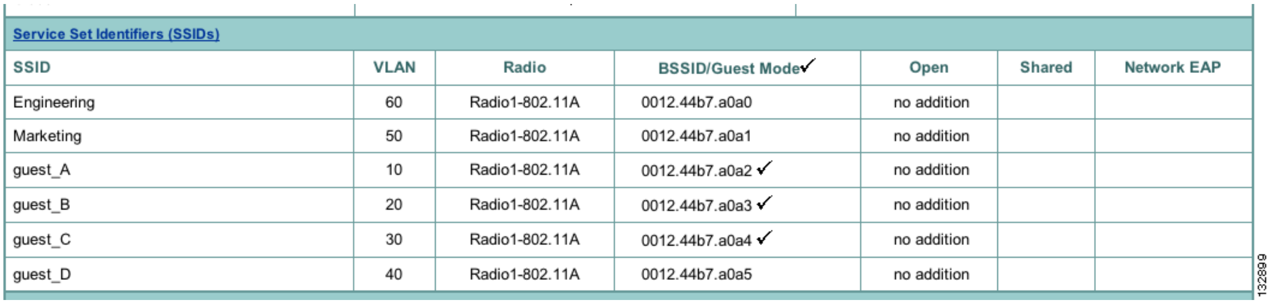
Radio1-802.11A:

Set Beacon Mode: ○ Single BSSID Set Single Guest Mode SSID: < NONE >
● Multiple BSSID

Set Infrastructure SSID: < NONE > □ Force Infrastructure Devices to associate only to this SSID

Under SSID settings, “Multiple BSSID Beacon Settings” there are two check boxes, one for setting the SSID as Guest Mode which allows the SSID to be broadcast with a unique MAC address and the second check box is the “Set Data Beacon Rate (DTIM), which allows setting the rate that will determine the number of beacons sent before a DTIM beacon. Figure 10-14 shows what the SSIDs look like once configured for MBSSID.

Figure 10-14 SSIDs Configured for MBSSID



Service Set Identifiers (SSIDs)

SSID	VLAN	Radio	BSSID/Guest Mode✓	Open	Shared	Network EAP
Engineering	60	Radio1-802.11A	0012.44b7.a0a0	no addition		
Marketing	50	Radio1-802.11A	0012.44b7.a0a1	no addition		
guest_A	10	Radio1-802.11A	0012.44b7.a0a2 ✓	no addition		
guest_B	20	Radio1-802.11A	0012.44b7.a0a3 ✓	no addition		
guest_C	30	Radio1-802.11A	0012.44b7.a0a4 ✓	no addition		
guest_D	40	Radio1-802.11A	0012.44b7.a0a5	no addition		

INDEX