AWLF

Aironet Wireless LAN Fundamentals

Volume 1

Version 3.1

Student Guide

Text Part Number: 67-1688-01

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia •
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary
India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands
New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia
Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine •
United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Table of Contents

Volume 1

Volume 2

Module 1

Introduction

Overview

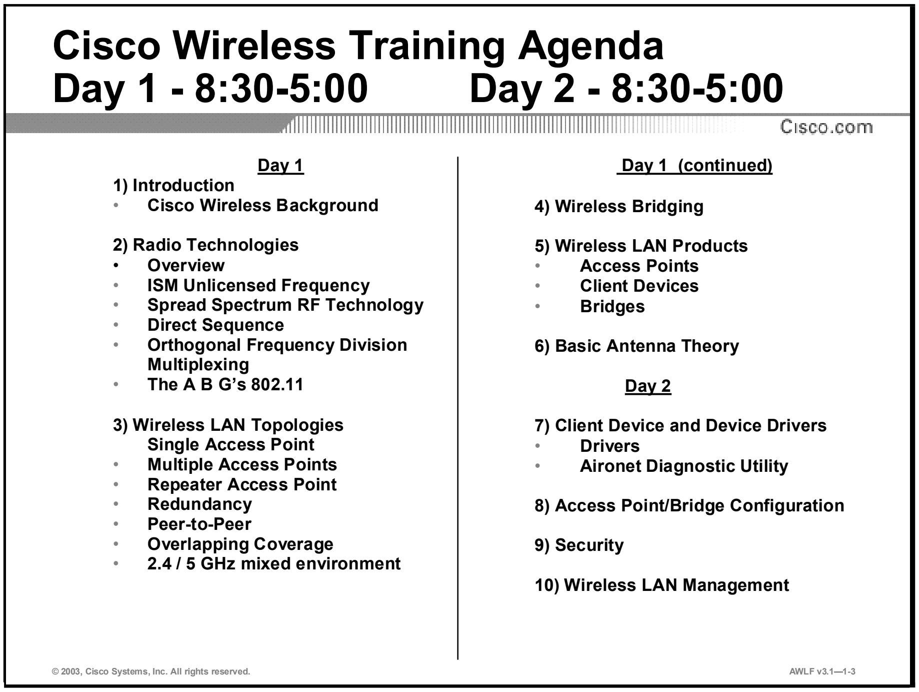
This module introduces the Wireless LAN (WLAN) industry.

It is designed to give the student a brief overview of the history of WLAN products and the evolution of those products, as well as to help the learner understand the development history of Cisco Aironet® wireless product set.

It includes the following topics:

- Agenda
- Cisco Wireless
- Wireless Data Networks
- WLAN Evolution
- Cisco Wireless Advantages

Agenda



Cisco Wireless Training Agenda
Day 1 - 8:30-5:00 Day 2 - 8:30-5:00

Day 1

1) Introduction
- Cisco Wireless Background

2) Radio Technologies
- Overview
- ISM Unlicensed Frequency
- Spread Spectrum RF Technology
- Direct Sequence
- Orthogonal Frequency Division Multiplexing
- The A B G's 802.11

3) Wireless LAN Topologies
Single Access Point
- Multiple Access Points
- Repeater Access Point
- Redundancy
- Peer-to-Peer
- Overlapping Coverage
- 2.4 / 5 GHz mixed environment

Day 1 (continued)

4) Wireless Bridging

5) Wireless LAN Products
- Access Points
- Client Devices
- Bridges

6) Basic Antenna Theory

Day 2

7) Client Device and Device Drivers
- Drivers
- Aironet Diagnostic Utility

8) Access Point/Bridge Configuration

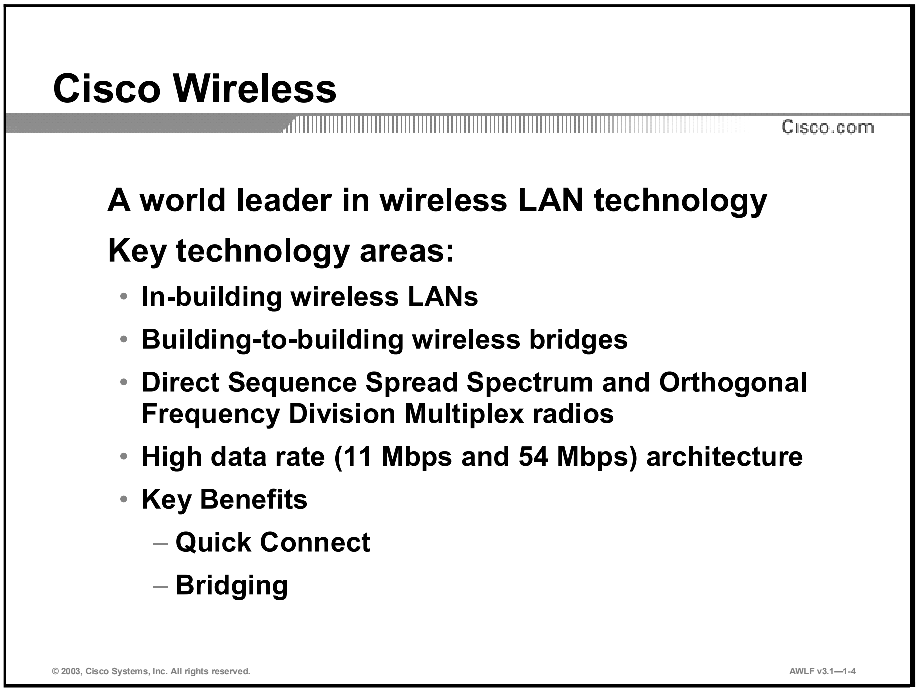
9) Security

10) Wireless LAN Management

AWLF v3.1—1-3

With its acquisition of Aironet in 1999, Cisco now has the experience of building Direct Sequence Spread Spectrum (DSSS) radios for the commercial market longer than any other company. In addition, Cisco now offers wireless equipment that uses Orthogonal Frequency Division Multiplex (OFDM) technology.

Cisco Wireless



Cisco Wireless

Cisco.com

A world leader in wireless LAN technology

Key technology areas:

- **In-building wireless LANs**
- **Building-to-building wireless bridges**
- **Direct Sequence Spread Spectrum and Orthogonal Frequency Division Multiplex radios**
- **High data rate (11 Mbps and 54 Mbps) architecture**
- **Key Benefits**
  - **Quick Connect**
  - **Bridging**

AWLF v3.1—1-4

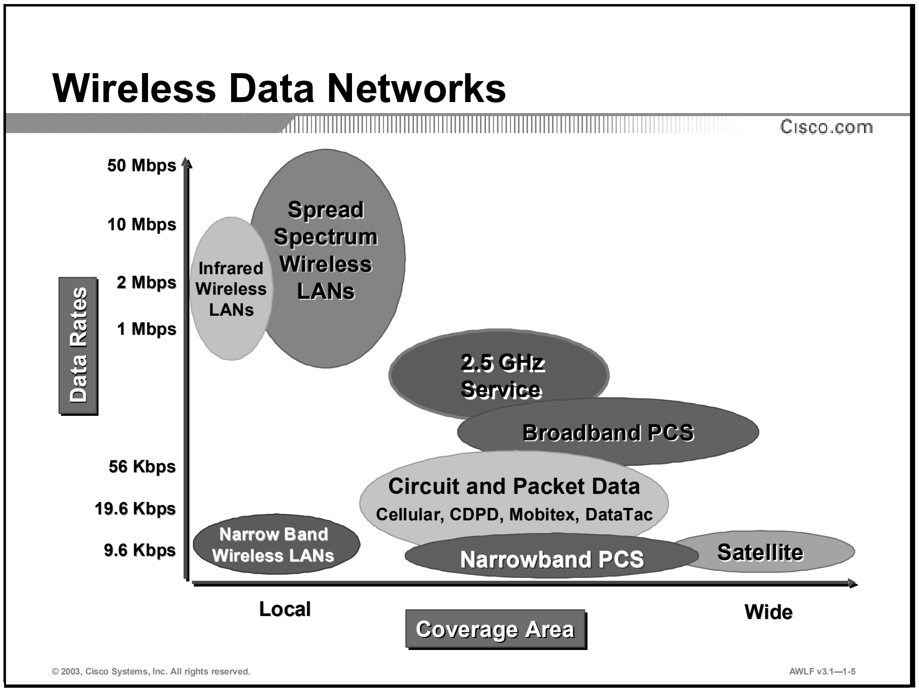
Organizations around the world are deploying overlay and freestanding wireless networks to increase employee productivity, reduce costs, and overcome obstacles to traditional wired connections.

A November 2001 study by NOP World—one of the world's largest research and business information companies—found that wireless LANs boosted employee productivity by an average of 22%.

Those gains are the result of being able to check e-mail, schedule meetings, and access files and applications from conference rooms, classrooms, coworkers' desks, and virtually anywhere else within a building or campus environment.

Many times, wireless LANs also offer a simpler and more cost-effective alternative to traditional wired connections. In some cases, such as in historic buildings or areas where asbestos poses an environmental hazard, it may be the only viable means of extending high-speed network access.

Wireless Data Networks



Wireless Data Networks

Cisco.com

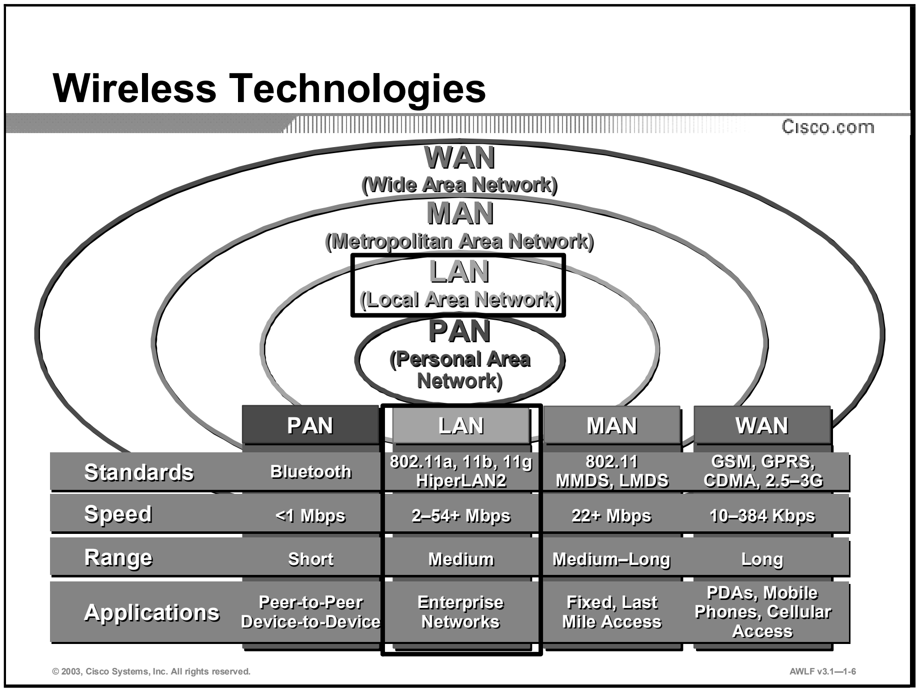
© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—1-5

There are many different types of wireless data communications, with each having its advantages and drawbacks.

- **Infrared (IR):** Very high data rates, lower cost, and very short distance.
- **Narrowband**: Low data rates, medium cost, license required, limited distance.
- **Spread Spectrum**: Limited to campus coverage, medium cost, and high data rates.
- **Personal communication service (PCS):** Low data rates, medium cost, citywide coverage.
- **2.5 GHz service, T-Mobile:** Global System for Mobile Communication (GSM), medium cost, and worldwide coverage.
- **Cellular, Cellular digital packet data (CDPD), Mobitex, DataTac**: Low data rates, flat monthly rate, and national coverage.

WLAN Evolution



Wireless Technologies

Cisco.com

WAN
(Wide Area Network)

MAN
(Metropolitan Area Network)

LAN
(Local Area Network)

PAN
(Personal Area Network)

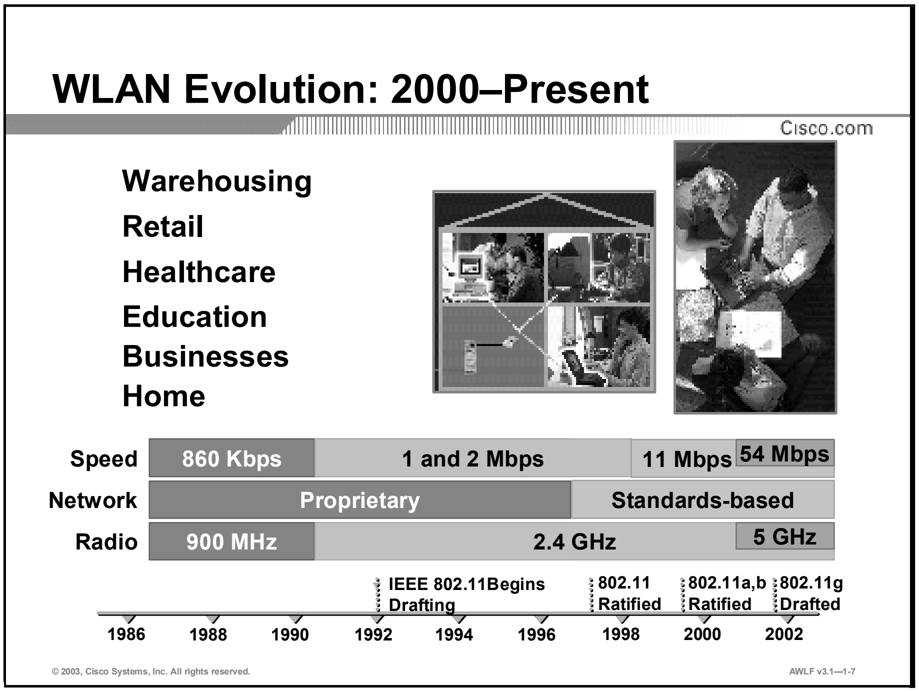
	PAN	LAN	MAN	WAN
Standards	Bluetooth	802.11a, 11b, 11g HiperLAN2	802.11 MMDS, LMDS	GSM, GPRS, CDMA, 2.5–3G
Speed	<1 Mbps	2–54+ Mbps	22+ Mbps	10–384 Kbps
Range	Short	Medium	Medium–Long	Long
Applications	Peer-to-Peer Device-to-Device	Enterprise Networks	Fixed, Last Mile Access	PDAs, Mobile Phones, Cellular Access

AWLF v3.1—1-6

In today's wireless world, there are many different types of networks offered. Each of these different networks are designed to give different coverage areas. Starting with the smallest coverage area, they are as follows:

- Personal Area Network (PAN) – Typically designed to cover your personal workspace. Radios are typically very low powered and do not deliver options in antenna selection thus limiting the size of coverage area (typically less than 20 feet of radius). One such PAN network is Bluetooth. Good applications of this technology are communications between PC and peripheral or between wireless phone and headset. In the PAN wireless network, the customer owns 100% of the network; therefore no airtime charges are incurred.
- Local Area Network (LAN) – Designed to be enterprise based wireless networks allowing for complete enterprise applications to be utilized without wires. Typically delivers Ethernet capable speeds (up to 54 Mbps). In the LAN wireless network, the customer owns 100% of the network; therefore no airtime charges are incurred.
- Metropolitan Area Networks (MAN) – These wireless networks are deployed inside a metropolitan area allowing wireless connectivity throughout an urban area. The MAN networks typically deliver up to broadband speeds (similar to DSL) but are not capable of Ethernet speeds. In the MAN wireless network, the wireless networks can either be a licensed carrier requiring the customer to purchase airtime or may be built out and supported by one entity such as a police department.
- Wide Area Networks (WAN) – The WAN wireless networks are typically slower in speeds but have more coverage, sometimes covering rural areas. Due to the vast deployment, all WAN wireless networks will require a customer purchase airtime for data transmission.

Note The Cisco Aironet wireless products are considered Local Area Network wireless products.



WLAN Evolution: 2000–Present

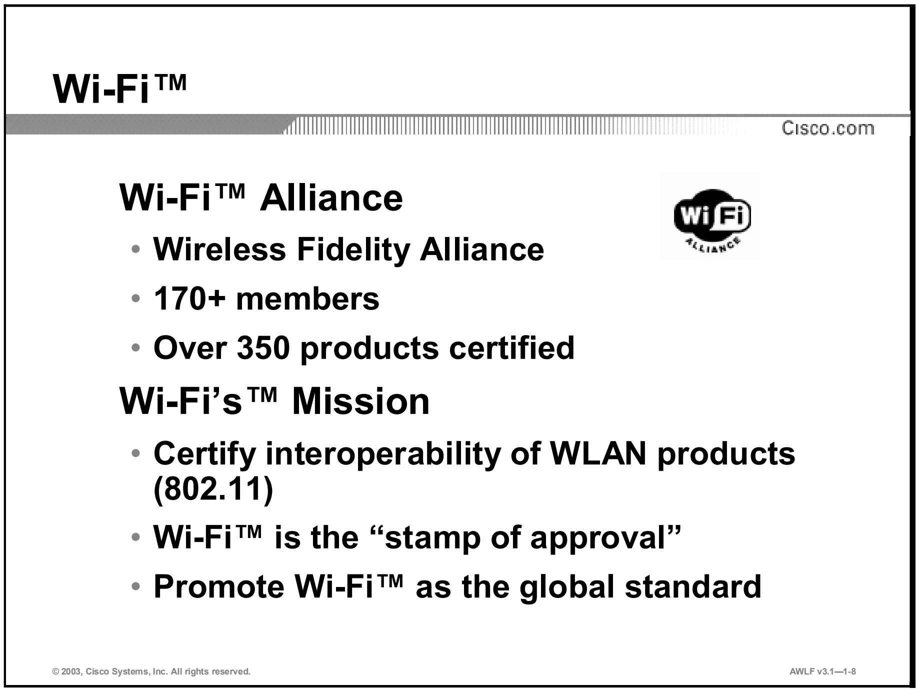
Cisco.com

- Warehousing
- Retail
- Healthcare
- Education
- Businesses
- Home

AWLF v3.1—1-7

The WLAN Evolution started in the 1980’s using 900 MHz Direct Sequence Spread Spectrum (DSSS) technology. The 900 MHz systems were fairly easy to deploy because one access point could cover large areas and no licenses were required in the approved countries. One problem for 900 MHz technology was that only a few countries allowed the technology. As time progressed the need for faster speeds, open standards, and global acceptance forced the manufactures of WLAN products to engineer new products to use the 2.4 GHz band.

The move to 2.4 GHz in the 1990’s put WLAN products into a “cleaner” RF environment making it possible to deploy data collection system without the worries of 900 MHz interference. 2.4 GHz was also well received because the throughput grew from 860 Kbps to 1 Mbps and 2 Mbps. When the frequency and speeds are increased the distances are decreased. The new data collection opportunities that the faster throughput helped to create, justified the extra access points that were needed. End users were still concerned about using a proprietary system and that is when the IEEE became involved. In 1992 the IEEE 802.11 draft began and the group’s focus was to eliminate the proprietary issue and design an open standard for WLAN.



Wi-Fi™

Cisco.com

Wi-Fi™ Alliance

- Wireless Fidelity Alliance
- 170+ members
- Over 350 products certified

Wi-Fi's™ Mission

- Certify interoperability of WLAN products (802.11)
- Wi-Fi™ is the "stamp of approval"
- Promote Wi-Fi™ as the global standard

AWLF v3.1—1-8

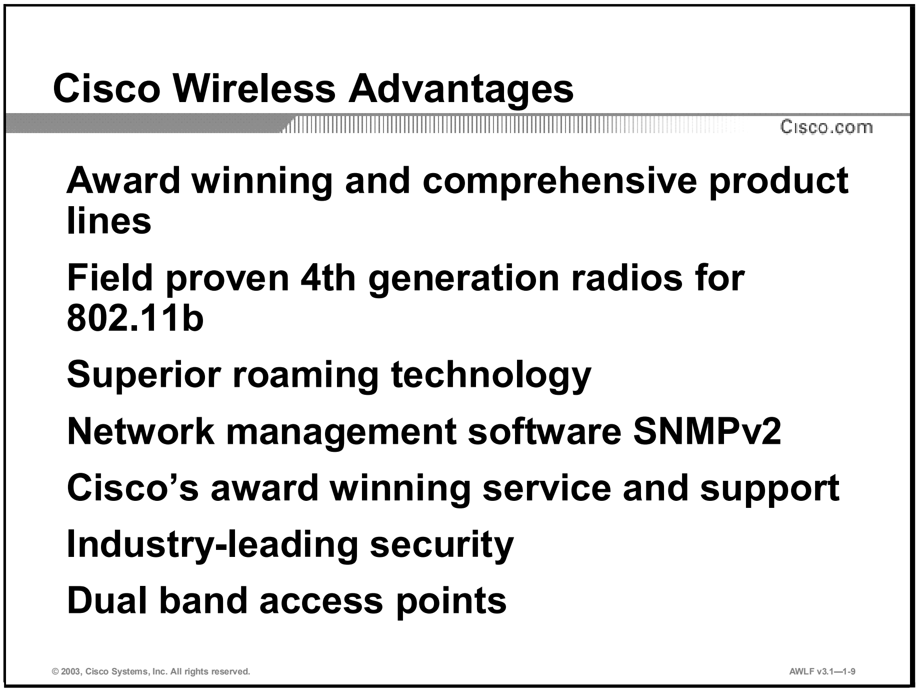
With the recent growth of the WLAN industry, a greater need for interoperability between WLAN vendors, better testing and certification is needed.

Wireless Fidelity Alliance or Wi-Fi™ is the new name for Wireless Ethernet Compatibility Alliance (WECA). The Wireless Fidelity Alliance is a nonprofit organization formed in 1999 to certify interoperability of Wi-Fi™ products and to promote Wi-Fi™ as the global, wireless LAN standard across all market segments. Cisco Systems is a founding member and one of the first companies to be certified interoperable by Wi-Fi™.Wi-Fi™ has over 170+ members and certified 350+ products. These members are concerned with the current standards as well as the need for further standards. For better interoperability there are many standards that still need to be addressed. Some of these include:

- Quality of Service (QOS)
- Security

For more information on the Wi-Fi™ standard, visit their web page at www.wi-fi.org

Cisco Wireless Advantages



Cisco Wireless Advantages

Award winning and comprehensive product lines

Field proven 4th generation radios for 802.11b

Superior roaming technology

Network management software SNMPv2

Cisco's award winning service and support

Industry-leading security

Dual band access points

AWLF v3.1—1-9

Why Cisco?

There are many reasons that you should choose Cisco Aironet Wireless:

- Patented roaming and communications software
- 11 and 54 Mbps-Ethernet speed wireless solution
- Best price/performance ratio in the wireless LAN and wireless bridge markets
- Global approvals and focus
- Commitment to wireless LAN industry
- Available for full SNMP v2 support
- Experienced--world's largest installed base

In short, Cisco Aironet Wireless has many features that cannot be matched by the competition.

Module 2

Radio Frequency Spread Spectrum Technology

Overview

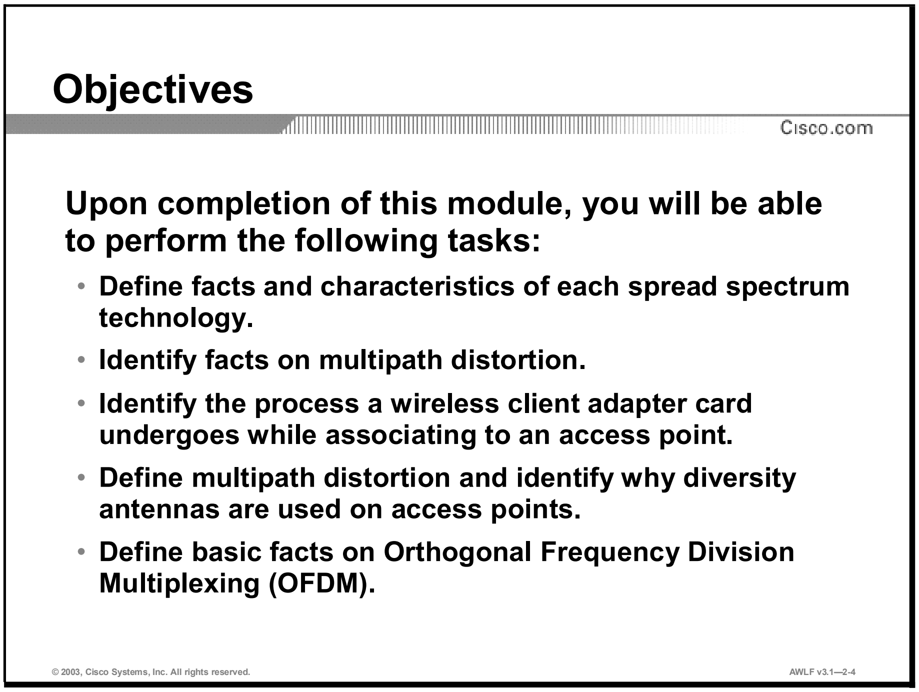
This module explores the basics of Radio Frequency Technology, modulation techniques, sources of interference, and association processes for WLAN client adapter cards.

It includes the following topics:

- Objectives
- ISM Unlicensed Frequencies
- Spread Spectrum RF Technology
- 802.11b Modulation
- 802.11a Modulation
- 802.11 Authentication
- Multipath
- Summary
- Review Questions

Objectives

This section lists the module's objectives.



Objectives

Upon completion of this module, you will be able to perform the following tasks:

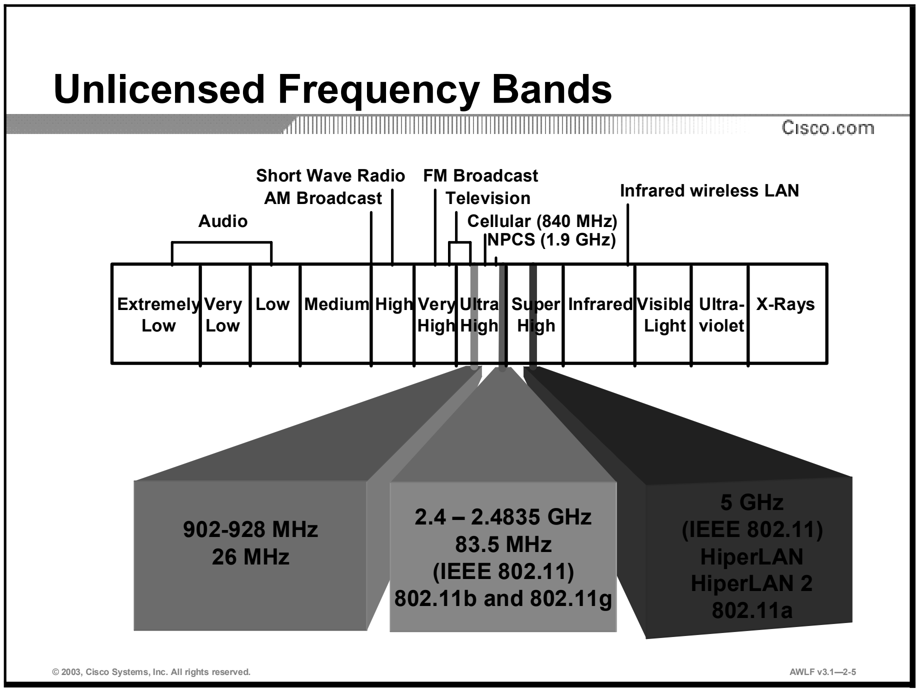
- **Define facts and characteristics of each spread spectrum technology.**
- **Identify facts on multipath distortion.**
- **Identify the process a wireless client adapter card undergoes while associating to an access point.**
- **Define multipath distortion and identify why diversity antennas are used on access points.**
- **Define basic facts on Orthogonal Frequency Division Multiplexing (OFDM).**

AWLF v3.1—2-4

Upon completion of this module, you will be able to perform the following tasks:

- Define facts and characteristics of each spread spectrum technology.
- Identify facts on multipath distortion.
- Identify the process a wireless client adapter card undergoes while associating to an access point.
- Define multipath distortion and identify why diversity antennas are used on access points.
- Define basic facts on Orthogonal Frequency Division Multiplexing (OFDM).

ISM Unlicensed Frequencies



Unlicensed Frequency Bands

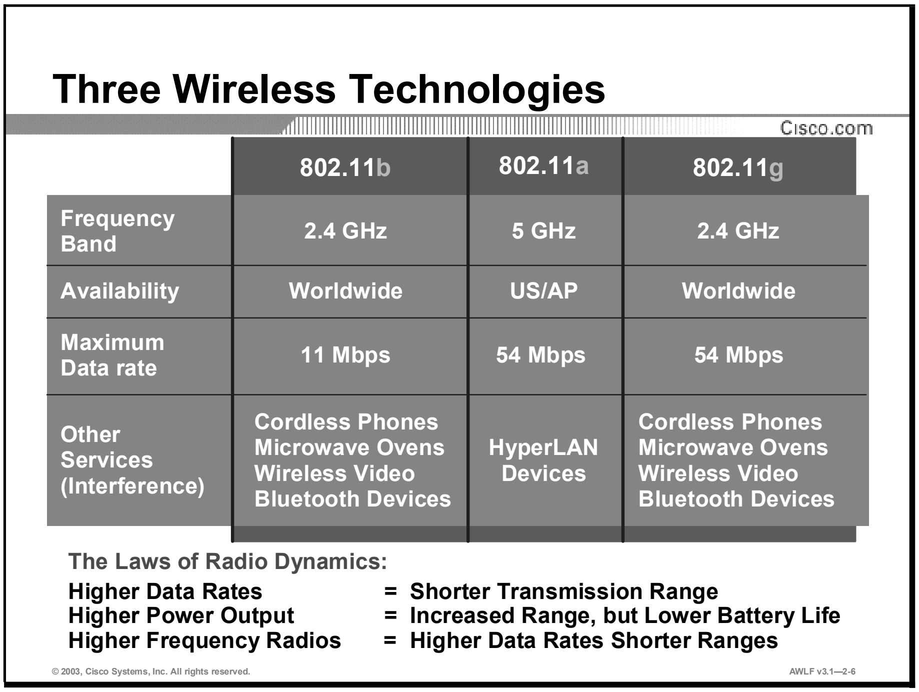
AWLF v3.1—2-5

There are three unlicensed bands, at 900 MHz, 2.4 GHz, and 5.7 GHz. These bands are referred to as the Industrial, Scientific, and Medical (ISM) frequencies.

The focus of this module is on 2.4 and 5 GHz bands. Cisco Aironet ® products utilize these bands today as well as adhere to the Institute of Electrical and Electronics Engineers (IEEE) 802.11a and 802.11b standards.

Recently, the Federal Communications Commission (FCC) also opened up the 5.2 GHz band for unlicensed use by high-speed data communications devices. 5.2 GHz is the same band that is used for the European Telecommunications Standards Institute (ETSI) HiperLAN specifications in Europe.

A nearby neighbor of the 900 MHz band is the cellular phone system. This helped the early development of the wireless LAN (WLAN) industry in the 900 MHz band because of the availability of inexpensive, small RF components developed for use in that band. The 2.4 GHz band has a neighbor in the PCS/GSM (cellular) system. That helps with component costs too.



Three Wireless Technologies

Cisco.com

	802.11b	802.11a	802.11g
Frequency Band	2.4 GHz	5 GHz	2.4 GHz
Availability	Worldwide	US/AP	Worldwide
Maximum Data rate	11 Mbps	54 Mbps	54 Mbps
Other Services (Interference)	Cordless Phones Microwave Ovens Wireless Video Bluetooth Devices	HyperLAN Devices	Cordless Phones Microwave Ovens Wireless Video Bluetooth Devices

The Laws of Radio Dynamics:

Higher Data Rates	=	Shorter Transmission Range
Higher Power Output	=	Increased Range, but Lower Battery Life
Higher Frequency Radios	=	Higher Data Rates Shorter Ranges

AWLF v3.1—2-6

2.4 GHz (802.11b)

The 802.11b standard, most widely deployed wireless standard, operates in the 2.4 GHz unlicensed radio band and delivers a maximum data rate of 11 Mbps. The 802.11b standard has been widely adopted by vendors and customers who find its 11 Mbps data rate more than adequate for their applications. Interoperability between many of the products on the market is ensured through the Wi-Fi™ certification program. Therefore, if your network requirements include supporting a wide variety of devices from different vendors, 802.11b is probably your best choice.

5 GHz (802.11a)

The IEEE ratified the 802.11a standard in 1999, but the first 802.11a-compliant products did not begin appearing on the market until December 2001.The 802.11a standard delivers a maximum data rate of 54 Mbps and eight nonoverlapping frequency channels—resulting in increased network capacity, improved scalability, and the ability to create microcellular deployments without interference from adjacent cells. 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, and Bluetooth (a short-range, low-speed, point-to-point, personal-area-network wireless standard). The 802.11a standard is not, however, compatible with existing 802.11b-compliant wireless devices. Organizations with 802.11b equipment that want the extra channels and network speed offered by 802.11a technology must install an entirely new wireless infrastructure with 802.11a access points and client adapters. It is important to note that 2.4- and 5-GHz equipment can operate in the same physical environment without interference.

2.4 GHz (802.11g)

The 802.11g standard has been in draft form since November 2001 and is unlikely to be finalized until 2003. 802.11g will deliver the same 54 Mbps maximum data rate as 802.11a, yet it offers an additional and compelling advantage—backward compatibility with 802.11b equipment. This means that 802.11b client cards will work with 802.11g access points, and 802.11g client cards will work with 802.11b access points. Because 802.11g and 802.11b operate in the same 2.4 GHz unlicensed band, migrating to 802.11g will 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 will use a different chipset than 802.11b in order to deliver the higher data rate. However, much like Ethernet and Fast Ethernet, 802.11g products can be commingled with 802.11b products in the same network. Because 802.11g operate in the same unlicensed band as 802.11b, it shares the same three channels, which can limit wireless capacity and scalability.

Worldwide Availability

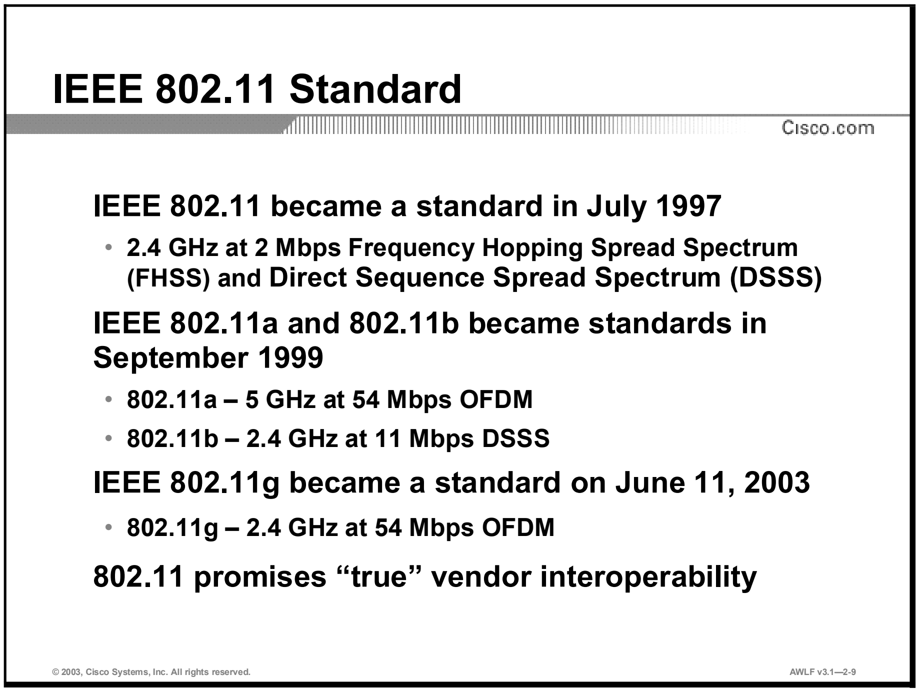
www.cisco.com/go/aironet/compliance

AWLF v3.1—2-8

One of the reasons Cisco has focused on the 2.4 GHz band for WLAN products is that this is the only band that is available with virtually the same technical rules for use worldwide. In most parts of the world Cisco products can be deployed without a user license (i.e., it's unlicensed). In most countries there is over 80 MHz of available spectrum. 5 GHz WLAN technology is also gaining popularity worldwide as more products become available in the UNII-1, UNII-2 and UNII-3 frequency bands. The operating frequency range varies worldwide from 5.170 GHz to 5.725 GHz as well as the maximum power, which is determined by the local regulating country.

http://www.cisco.com/go/aironet/compliance lists the Cisco Aironet products and the specific countries each product is currently certified in for order and shipment. If there is not an "X" in the matrix box that corresponds to the country and product, then that product is not certified to ship to this country. Please take note of the Country SKU Suffix in the column adjacent to your country. You will need this specific SKU Suffix to ensure you order the product with the proper power and channel settings required for each country. If you have any questions regarding this information, please contract your Cisco Account Manager or Cisco Reseller for more information. Each country has its own set of rules governing the installation and use of RF products. Be aware that these rules may affect which products you use and may require you to obtain a site-specific license.

Spread Spectrum RF Technology



IEEE 802.11 Standard

IEEE 802.11 became a standard in July 1997

- 2.4 GHz at 2 Mbps Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS)

IEEE 802.11a and 802.11b became standards in September 1999

- 802.11a – 5 GHz at 54 Mbps OFDM
- 802.11b – 2.4 GHz at 11 Mbps DSSS

IEEE 802.11g became a standard on June 11, 2003

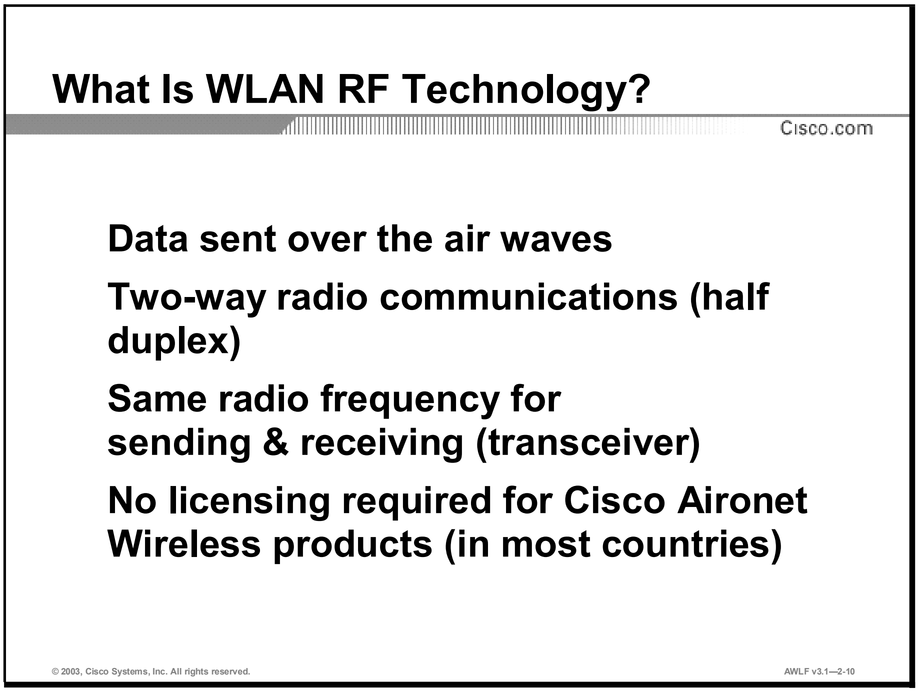
- 802.11g – 2.4 GHz at 54 Mbps OFDM

802.11 promises “true” vendor interoperability

AWLF v3.1—2-9

Any time an IEEE committee works on a standard, they invite the top engineers from all appropriate companies in the field to participate in the development of the specification. The 802.11 Committee was formed in the same manner. Top engineers from many different wireless data companies (and some wired data LAN companies) together developed a standard that they all believed would deliver a high quality, high performance product.

For this reason, an 802.11 radio will be a better product than any of the older proprietary products. 802.11 define such things as receiver sensitivity, Media Access control (MAC) layer performance and modulation schemes.



What Is WLAN RF Technology?

Data sent over the air waves

Two-way radio communications (half duplex)

Same radio frequency for sending & receiving (transceiver)

No licensing required for Cisco Aironet Wireless products (in most countries)

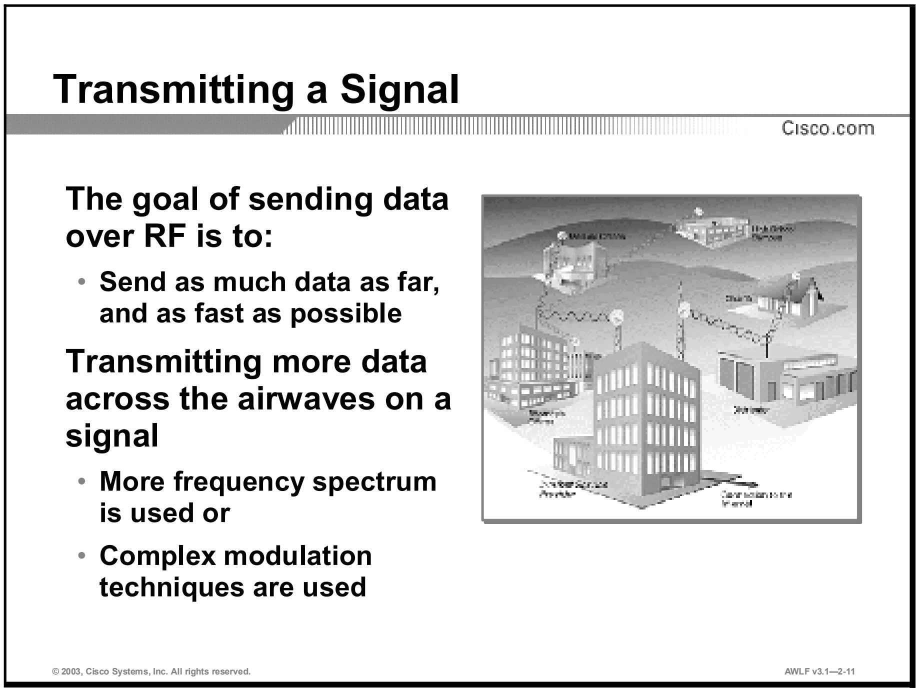
AWLF v3.1—2-10

Spread Spectrum is a type of emission designed to be somewhat immune to interference, difficult to detect, and hard to intercept.

Actress Hedy Lamarr and music composer George Antheil patented the concept of Spread Spectrum in 1942. The idea was a method for guiding a torpedo without interference from a jamming signal.

In 1986, the FCC agreed to allow the use of Spread Spectrum in the commercial market under the ISM bands.

Just as the radio in your car has AM (Amplitude Modulation) and FM (Frequency Modulation) bands, other radios use different bands and types of modulation.



Transmitting a Signal

The goal of sending data over RF is to:

- **Send as much data as far, and as fast as possible**

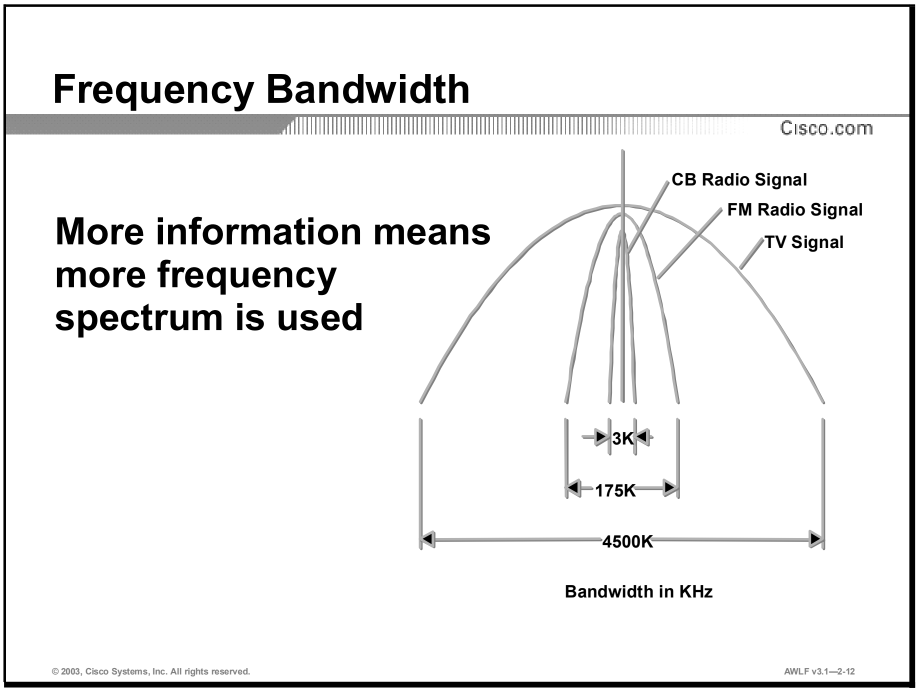
Transmitting more data across the airwaves on a signal

- **More frequency spectrum is used or**
- **Complex modulation techniques are used**

When transmitting a signal in data format, three questions come to mind:

- How fast: What data rate can be achieved?
- How far: How far apart can the units be that are transmitting or receiving and still get the maximum data rate?
- How many: How many users can be on the system without slowing the data rate to an unacceptable level? Cisco products operate as a shared medium and can be thought of much the same way as a wired 10 Mbps Ethernet segment.

These factors all relate to the ability to receive a good signal as far away as possible. Increasing the amount of data requires the use of more frequency spectrum or a different method of placing the data on the RF signal (modulation technique).



Frequency Bandwidth

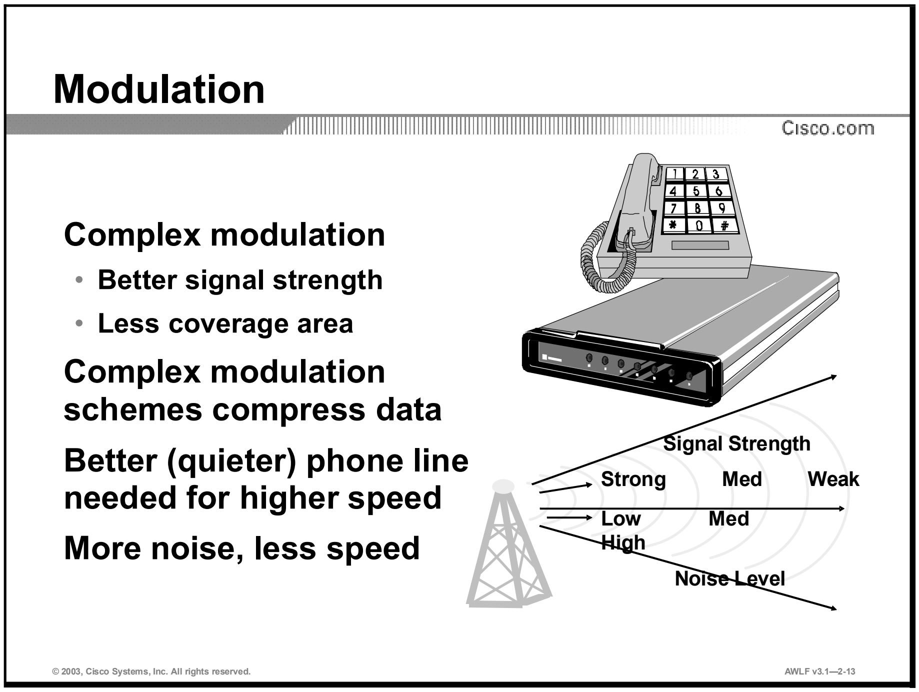
More information means more frequency spectrum is used

AWLF v3.1—2-12

As more information is placed on a radio signal, more frequency spectrum (or bandwidth) is used.

- A CB signal has very low quality audio, and requires about 3 KHz of bandwidth.
- A FM radio signal provides high quality audio, which consumes about 175 KHz of bandwidth.
- A TV signal, which contains both audio and video, utilizes almost 4500 KHz (4.5 MHz) of bandwidth.

MORE INFORMATION = MORE FREQUENCY SPECTRUM USED



Modulation

Cisco.com

Complex modulation

- **Better signal strength**
- **Less coverage area**

Complex modulation schemes compress data

Better (quieter) phone line needed for higher speed

More noise, less speed

Signal Strength
Strong
Med
Weak
Low
Med
High
Noise Level

© 2003, Cisco Systems, Inc. All rights reserved.

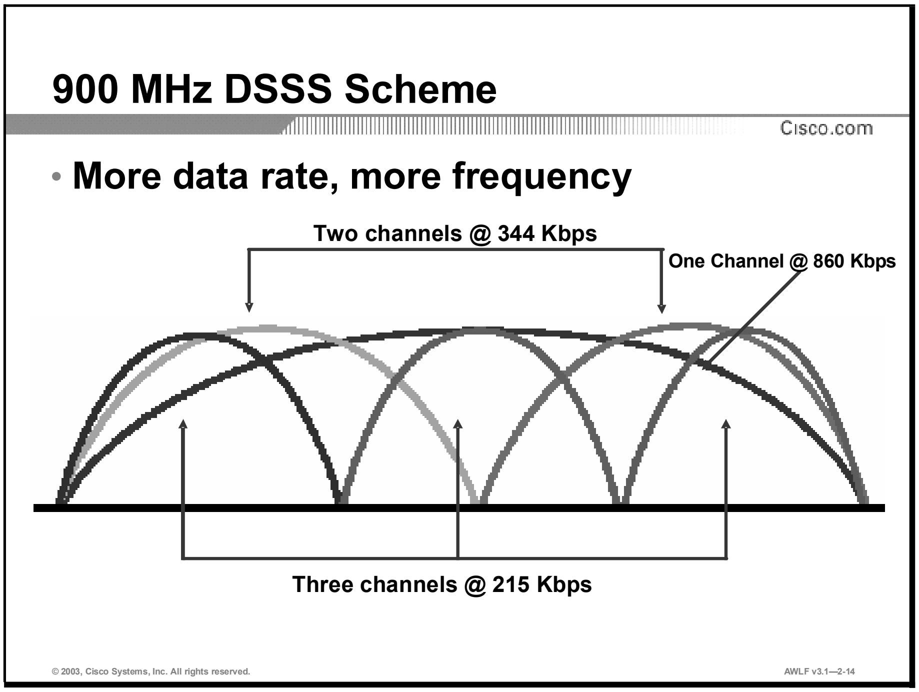
AWLF v3.1—2-13

Years ago, a modem was able to communicate at 300-baud. Today, a 56K modem gets much higher speeds over the same wire as the 300-baud modem. This increase in speed is due to the modem compressing the data into a smaller space, and using the same bandwidth of the phone line as the 300-baud modem used.

One problem that may arise is that if there is noise on the phone line, the modem speed will be reduced. As the data is further compressed, it requires a stronger signal as compared to the noise level. More noise means slower speed for the data to be received correctly.

The same is true in radio. As a receiver moves farther from a transmitter the signal gets weaker, and the difference between the signal and noise decreases. At some point, the signal cannot be distinguished from the noise and loss of communication occurs. The amount of compression (or modulation type) at which the signal is transmitted determines the amount of signal needed to be clearly received through the noise.

As transmission or modulation schemes (compression) become more complex and data rate goes up, immunity to noise decreases, and coverage goes down.



900 MHz DSSS Scheme

Cisco.com

- **More data rate, more frequency**

Two channels @ 344 Kbps

One Channel @ 860 Kbps

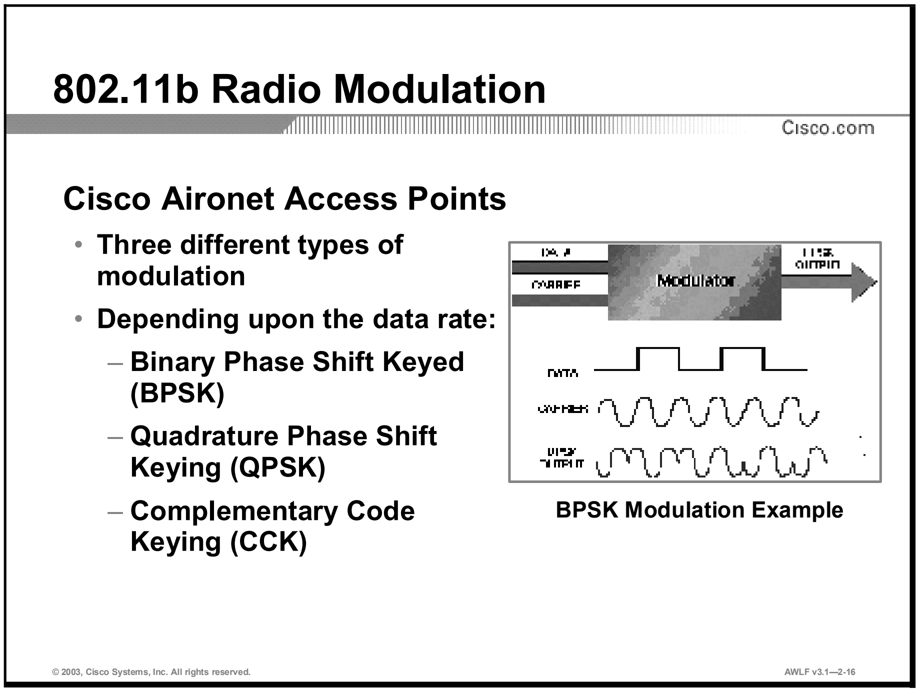
Three channels @ 215 Kbps

AWLF v3.1—2-14

Early on in the development of 900 MHz Direct Sequence Spread Spectrum (DSSS) technology, a special scheme was used to achieve the higher data rates. At that time there wasn't a standard in place to design your 900 MHz DSSS system. The basic concept of this scheme was use all of the channel to produce one fast channel 860 Kbps or you could break the channel into smaller sections to produce more channels but those channels performed at slower speeds e.g. three channels at 215 Kbps or two channels at 344 Kbps.

Now that the 802.11 standards are in place, an RF engineer has to follow the rules to make his/her hardware 802.11 compliant. So the practice of using more of the channel could no longer be used to achieve higher data rates. The new scheme for 802.11 is to use very advanced modulation techniques to achieve higher data rates. The remainder of this module will address the modulation techniques for 802.11b and 802.11a.

802.11b Modulation



802.11b Radio Modulation

Cisco.com

Cisco Aironet Access Points

- Three different types of modulation
- Depending upon the data rate:
  - Binary Phase Shift Keyed (BPSK)
  - Quadrature Phase Shift Keying (QPSK)
  - Complementary Code Keying (CCK)

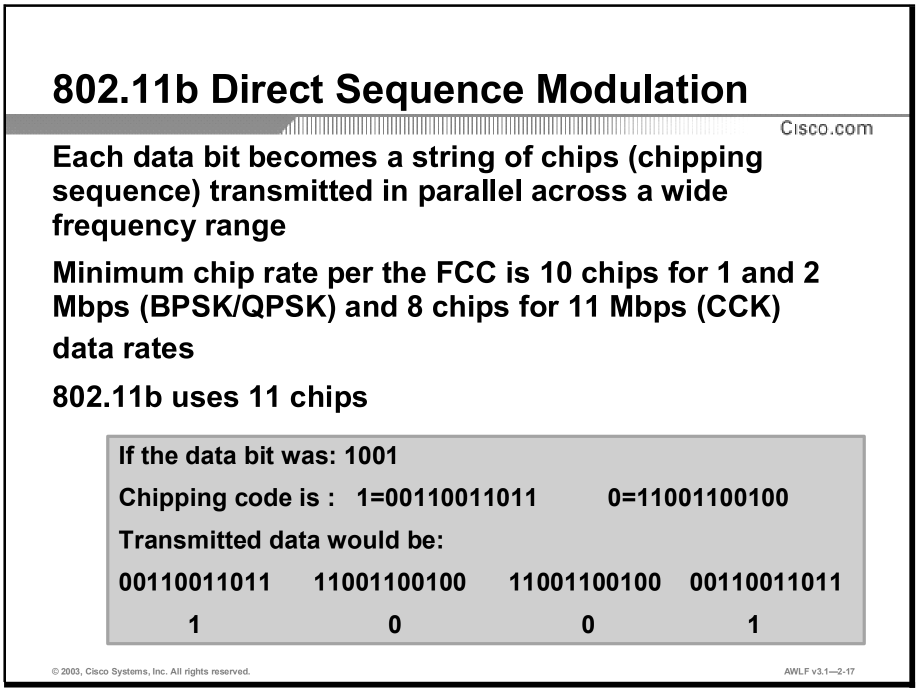
DATA
CARRIER
Modulator
BPSK OUTPUT
DATA
CARRIER
BPSK OUTPUT

BPSK Modulation Example

AWLF v3.1—2-16

Cisco Aironet Access Points use three different types of modulation, depending upon the data rate used. The types of modulation include:

- **Binary phase shift keyed (BPSK):** BPSK uses one phase to represent a binary 1 and another to represent a binary 0 for a total of two bits of binary data. This is utilized to transmit data at 1 Mbps.
- **Quadrature phase shift keying (QPSK):** With QPSK, the carrier undergoes four changes in phase and can thus represent four binary bits of data. This is utilized to transmit data at 2 Mbps.
- **Complementary code keying (CCK):** CCK uses a complex set of functions know as complementary codes to send more data. One of the advantages of CCK over similar modulation techniques is that it suffers less from multipath distortion. This is utilized to transmit data at 5.5 and 11 Mbps.



802.11b Direct Sequence Modulation

Cisco.com

- Each data bit becomes a string of chips (chipping sequence) transmitted in parallel across a wide frequency range
- Minimum chip rate per the FCC is 10 chips for 1 and 2 Mbps (BPSK/QPSK) and 8 chips for 11 Mbps (CCK) data rates
- 802.11b uses 11 chips

If the data bit was: 1001

Chipping code is : 1=00110011011 0=11001100100

Transmitted data would be:

00110011011	11001100100	11001100100	00110011011
1	0	0	1

© 2003, Cisco Systems, Inc. All rights reserved.

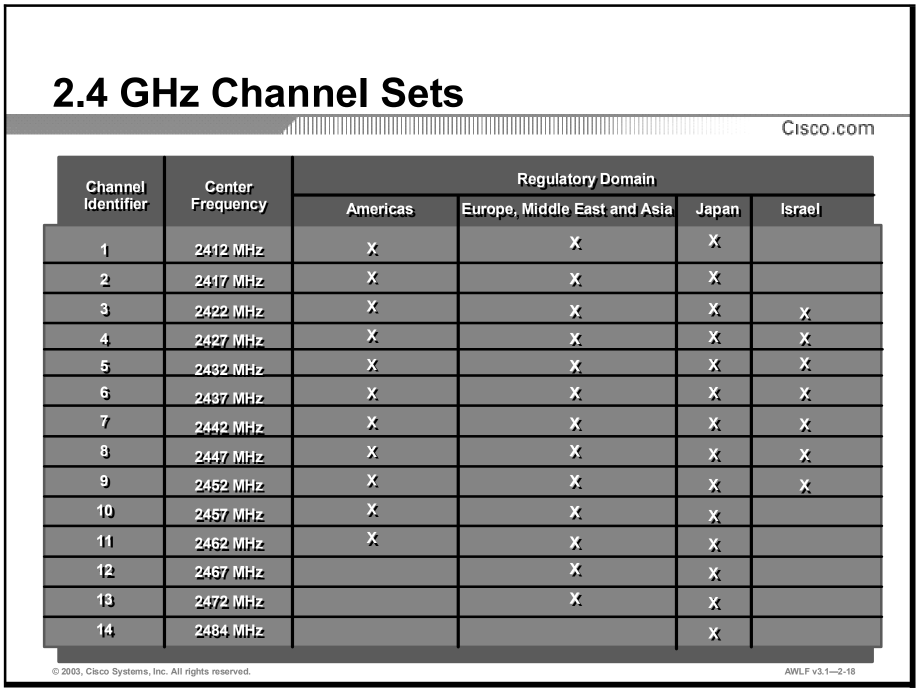
AWLF v3.1—2-17

Direct Sequence

By using these codes, the receiver could actually miss several bits and the software would be able to still identify that the code was intended to be a 1 or a 0. If there were an interfering signal, the unit would still be able to get the data through without loss of data or reduction in throughput or performance.

Example

If a bit was received that was a 01111011011, when compared to a 1, there would be two bits different. Comparing it to a 0, there would be 9 bits different. Therefore, that received bit should represent a 1. More than 5 data bits would have to be inverted to change the value, which translates to over half of the signal lost before the original message cannot be reconstructed.



2.4 GHz Channel Sets

Cisco.com

Channel Identifier	Center Frequency	Regulatory Domain			
		Americas	Europe, Middle East and Asia	Japan	Israel
1	2412 MHz	X	X	X	
2	2417 MHz	X	X	X	
3	2422 MHz	X	X	X	X
4	2427 MHz	X	X	X	X
5	2432 MHz	X	X	X	X
6	2437 MHz	X	X	X	X
7	2442 MHz	X	X	X	X
8	2447 MHz	X	X	X	X
9	2452 MHz	X	X	X	X
10	2457 MHz	X	X	X	
11	2462 MHz	X	X	X	
12	2467 MHz		X	X	
13	2472 MHz		X	X	
14	2484 MHz			X	

AWLF v3.1—2-18

Different countries have different regulatory bodies and may have as many as 14 channel sets available. In some countries, this may mean that the number of non-overlapping channels is reduced to one, and an aggregate data rate of 33 Mbps may not be possible.

The following list the countries that belong to each regulatory domain. Regulatory Domain information is subject to change weekly. An up-to-date listing of the countries that correspond to theses Regulatory Domains is available at: http://www.cisco.com/go/aironet/compliance.

Americas

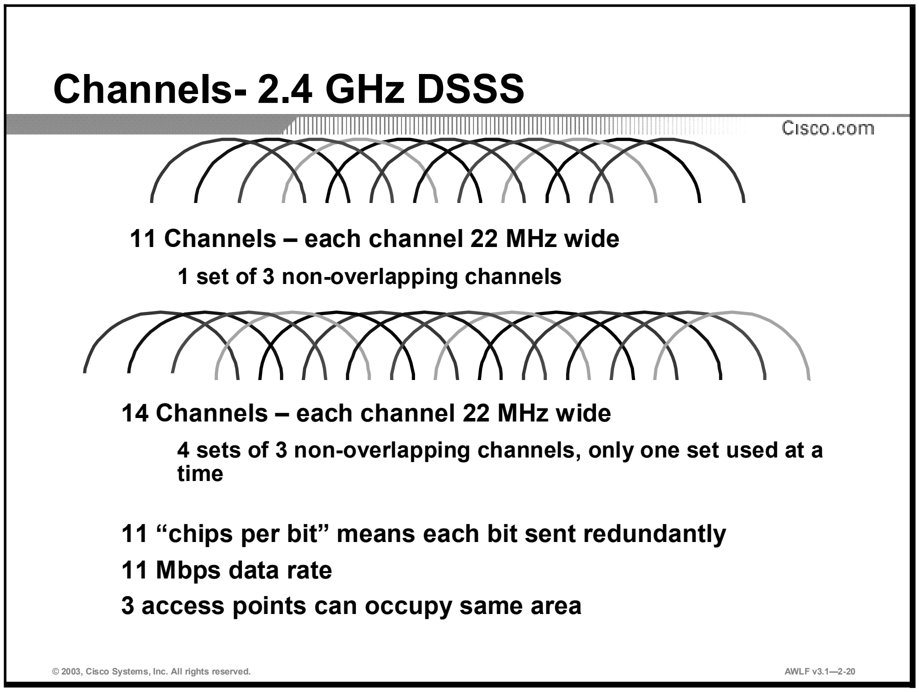
United States, Canada, Mexico, America Samoa, Antigua and Barbuda, Argentina, Aruba, Ashmore and Cartier Islands, Australia, Bahamas, Baker Island, Barbados, Bermuda, Bolivia, Bouvet Island, Brazil, Cameroon, Central African Republic, Chad, Chile, China, Christmas Island, Clipperton Island, Cocos Island, Colombia, Cook Island, Coral Sea Islands, Costa Rica, Ecuador, El Salvador, Europa Island, Faroe Islands, Fiji, Glorioso Islands, Grenada, Guadeloupe, Guam, Guatemala, Guyana, Haiti, Heard Island, Honduras, Hong Kong, Jamaica, Kingman Reef, Malawi, Malaysia, Mali, Marshall Islands, Midway Islands, Navassa Island, New Caledonia, New Guinea, New Zealand, Nicaragua, Niger, Nigeria, Norfolk Island, Northern Mariana Islands, Palau, Palmyra Atoll, Panama, Papua New Guinea, Paracel Islands, Paraguay, Peru, Phillippines, Pitcairn Islands, Puerto Rico, Russia, Saint Kitts and Nevis, Saint Lucia, Saint Pierre and Miquelon, Saint Vincent and the Grenadines, Samoa, Saudi Arabia, Solomon Islands, South Korea, Taiwan, India, Spratly Islands, Togo, Tonga, Trinidad and Tobago, Tromelin Island, Turks and Caicos Islands, Uruguay, US Virgin Islands, Venezuela, Wake Island, Western Sahara

Note Mexico is included in the Americas regulatory domain; however, channels 1 through 8 are for indoor use only while channels 9 through 11 can be used indoors and outdoors. Users are responsible for ensuring that the channel set configuration complies with the regulatory standards of Mexico.

Europe, Middle East and Asia (EMEA)

Afghanistan, Albania, Algeria, Andorra, Angola, Angullia, Armenia, Austria, Azerbaijan, Bahrain, Bangladesh, Bassas da India, Belarus, Belgium, Belize, Benin, Bhutan, Bosnia, Botswana, British Indian Ocean, Territory, British Virgin Islands, Brunei, Bulgaria, Burkina Faso, Burma, Burundi, Cambodia, Cape Verde, Cayman Islands, Comoros, Cote d'Ivoire, Croatia, Cyprus, Czech Republic, Democratic Republic of the Congo, Denmark, Djibouti, Dominica, Egypt, Equatorial Guinea, Eritrea, Estonia, Ethiopia, Falkland Islands, Finland, France, French Guiana, French Polynesia, French Southern and Antarctic Lands, Gabon, Gambia, Georgia, Germany, Ghana, Gilbraltar, Greece, Greenland, Guernsey, Guinea, Guinea-Bissau, Hungary, Iceland, Indonesia, Ireland, Isle of Man, Italy, Ivory Coast, Jan Mayan, Jarvis Island, Jersey, Johnston Atoll, Jordan, Juan de Nova Island, Kazakhstan, Kenya, Kiribati, Kuwait, Kyrgyzstan, Laos, Latvia, Lebanon, Lesotho, Liberia, Liechtenstein, Lithuania, Luxembourg, Macau, Macedonia, Madagascar, Maldives, Malta, Martinique, Mauritania, Mauritius, Mayotte, Micronesia, Moldova, Monaco, Mongolia, Montserrat, Morocco, Mozambique, Namibia, Nauru, Nepal, Netherlands, Niue, Norway, Oman, Pakistan, Poland, Portugal, Qatar, Republic of the Congo, Reunion, Romania, Rwanda, Saint Helena, San Marino, Sao Tome and Principe, Senegal, Serbia, Seychelles, Sierra Leone, Slovak Republic, Slovenia, Somalia, South Africa, South Georgia, Spain, Sri Lanka, Sudan, Suriname, Svalbard, Swaziland, Sweden, Switzerland, Syria, Tajikistan, Tanzania, Thailand, Tokelau, Tunisia, Turkey, Turkmenistan, Tuvalu, Uganda, Ukraine, United Arab Emirates, United Kingdom, Uzbekistan, Vanuatu, Vatican City, Vietnam, Wallis and Futuna, Yemen, Zaire, Zambia, Zimbabwe.

Note France is included in the EMEA regulatory domain; however, only channels 10 through 13 can be used in France. Users are responsible for ensuring that the channel set configuration complies with the regulatory standards of France.



Channels- 2.4 GHz DSSS

11 Channels – each channel 22 MHz wide

- 1 set of 3 non-overlapping channels

14 Channels – each channel 22 MHz wide

- 4 sets of 3 non-overlapping channels, only one set used at a time

11 “chips per bit” means each bit sent redundantly

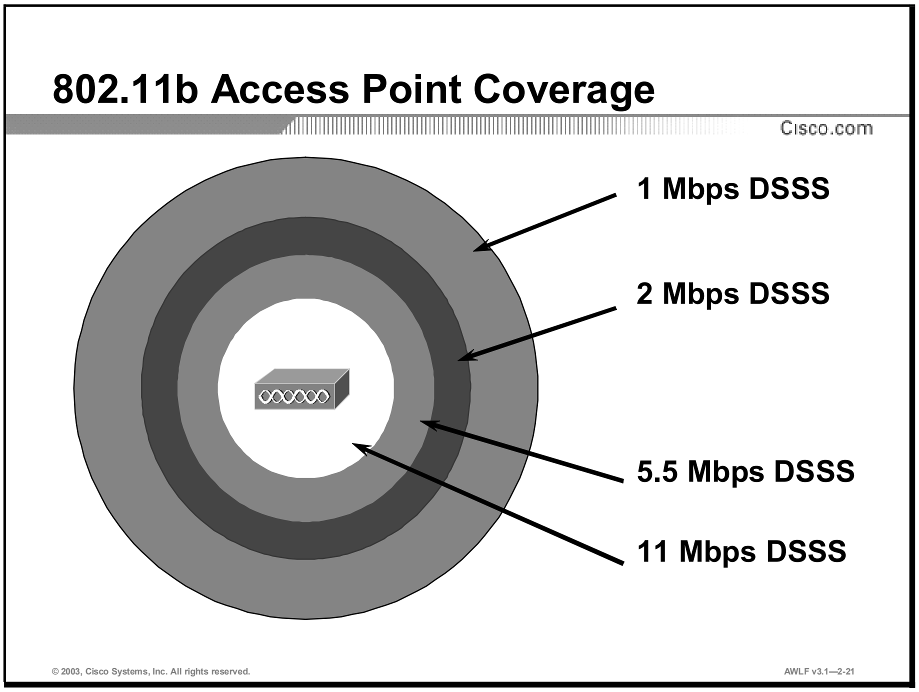
11 Mbps data rate

3 access points can occupy same area

AWLF v3.1—2-20

With direct sequence (DS), the energy is spread out over a wide area of the band. With Cisco products, the 802.11 channels have a bandwidth of 22 MHz. This will allow 3 non-overlapping, non-interfering channels to be used in the same area. This is also the 802.11 channel scheme.

If there is severe signal interference in one area, it is possible to change to another channel and totally avoid the interference. Normally, changing channels does not happen automatically in DS, and must be done with re-configuration to the access point. Cisco firmware will allow an access point to search for the “less congested” channel.



802.11b Access Point Coverage

1 Mbps DSSS

2 Mbps DSSS

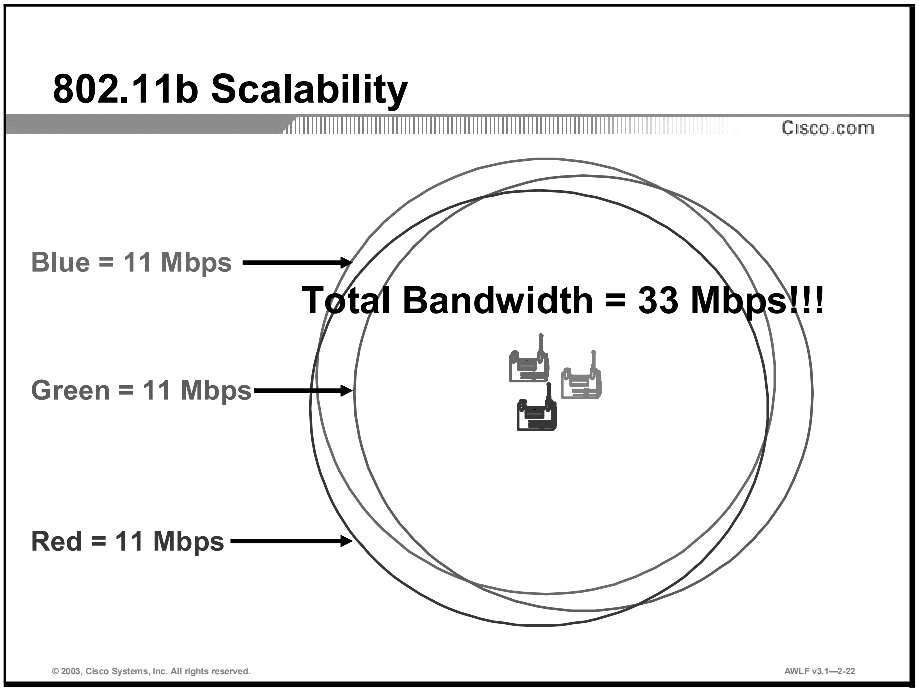
5.5 Mbps DSSS

11 Mbps DSSS

AWLF v3.1—2-21

With 802.11b products, coverage at 1 Mbps and 2 Mbps are identical to 802.11, 1 and 2 Mbps products with the added benefit of support for 5.5 Mbps and 11 Mbps.

All 802.11b products also have the ability to data rate shift while moving, allowing the same person operating at 11 Mbps, to shift to 5.5 Mbps, 2 Mbps, and finally still communicate at the outside ring at 1 Mbps. This rate shifting happens without losing connection and without any interaction from the user. Rate shifting also happens on a transmission-by-transmission basis; therefore the access point has the ability to support multiple clients at multiple speeds depending upon the location of each client.



802.11b Scalability

Cisco.com

Blue = 11 Mbps

Green = 11 Mbps

Red = 11 Mbps

Total Bandwidth = 33 Mbps!!!

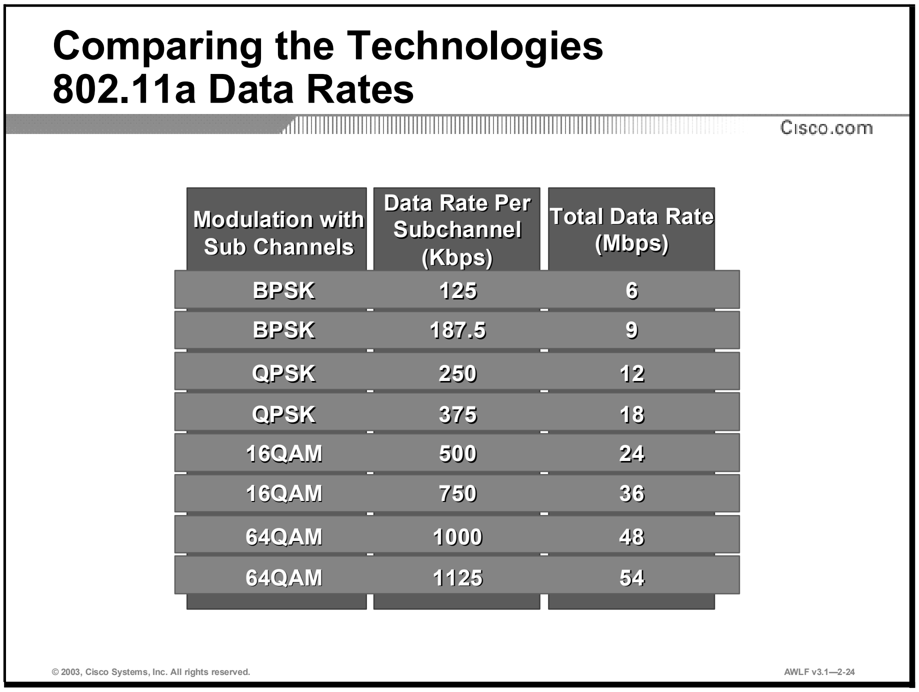
AWLF v3.1—2-22

Scalability is the ability to locate more than one access point in the same area, increasing the bandwidth of that area for all users local to that access point.

Since 802.11b Americas, EMEA and Japan channel sets have 3 non-overlapping channels, three discrete systems can reside in the same area with no interference. If more than three systems are required in the same area, they must time share the frequency. Therefore, the highest aggregate (total combined) data rate for an 802.11b system is 33 Mbps for a given cell area.

Using the ability to scale throughput and add access points in the same cell area increases the overall available bandwidth of any cell.

802.11a Modulation



Comparing the Technologies 802.11a Data Rates

Cisco.com

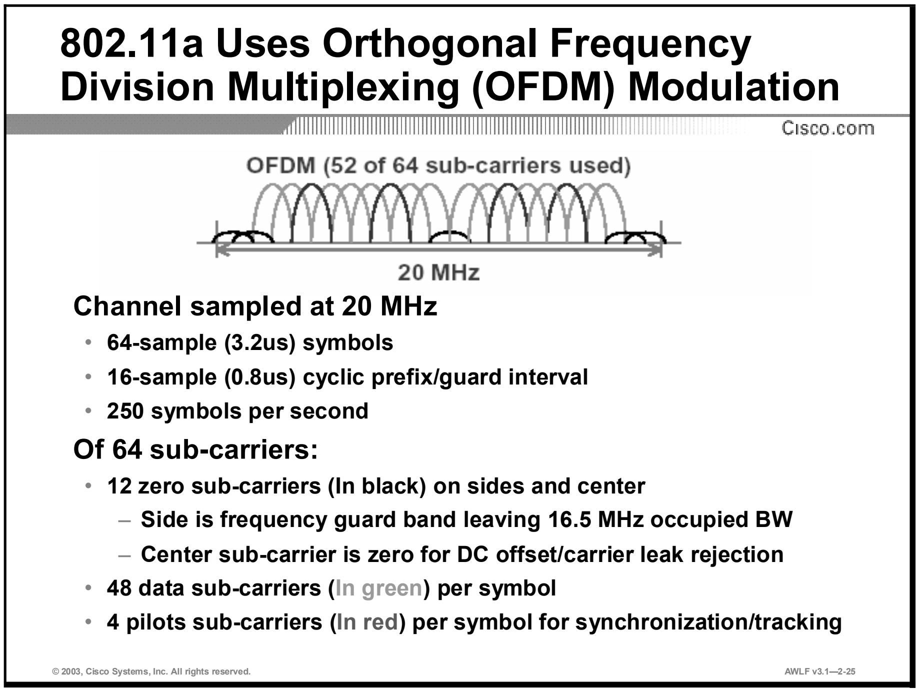
Modulation with Sub Channels	Data Rate Per Subchannel (Kbps)	Total Data Rate (Mbps)
BPSK	125	6
BPSK	187.5	9
QPSK	250	12
QPSK	375	18
16QAM	500	24
16QAM	750	36
64QAM	1000	48
64QAM	1125	54

AWLF v3.1—2-24

Orthogonal Frequency Division Multiplexing (OFDM)

OFDM works by breaking one high-speed data carrier into several lower-speed subcarriers, which are then transmitted in parallel. Each high-speed carrier is 20 MHz wide and is broken up into 52 subchannels, each approximately 300 KHz wide. OFDM uses 48 of these subchannels for data, while the remaining four are used for error correction. Coded orthogonal frequency division multiplexing (COFDM) delivers higher data rates and a high degree of multipath reflection recovery, thanks to its encoding scheme and error correction.

Each subchannel in the OFDM implementation is about 300 KHz wide. At the low end of the speed gradient, Binary Phase Shift Keying (BPSK) is used to encode 125 Kbps of data per channel, resulting in a 6,000-Kbps, or 6 Mbps, data rate. Using Quadrature Phase Shift Keying (QPSK), you can double the amount of data encoded to 250 Kbps per channel, yielding a 12-Mbps data rate. And by using 16-level Quadrature Amplitude Modulation (16-QAM) encoding 4 bits per hertz, you can achieve a data rate of 24 Mbps. The 802.11a standard specifies that all 802.11a-compliant products must support these basic data rates. The standard also lets the vendor extend the modulation scheme beyond 24 Mbps. Data rates of 54 Mbps are achieved by using 64-level Quadrature Amplitude Modulation (64-QAM), which yields 8 bits per cycle or 10 bits per cycle, for a total of up to 1.125 Mbps per 300-KHz channel. With 48 channels, this results in a 54 Mbps data rate. Remember, the more bits per cycle (hertz) that are encoded, the more susceptible the signal will be to interference and fading, and ultimately, the shorter the range, unless power output is increased.



802.11a Uses Orthogonal Frequency Division Multiplexing (OFDM) Modulation

Channel sampled at 20 MHz

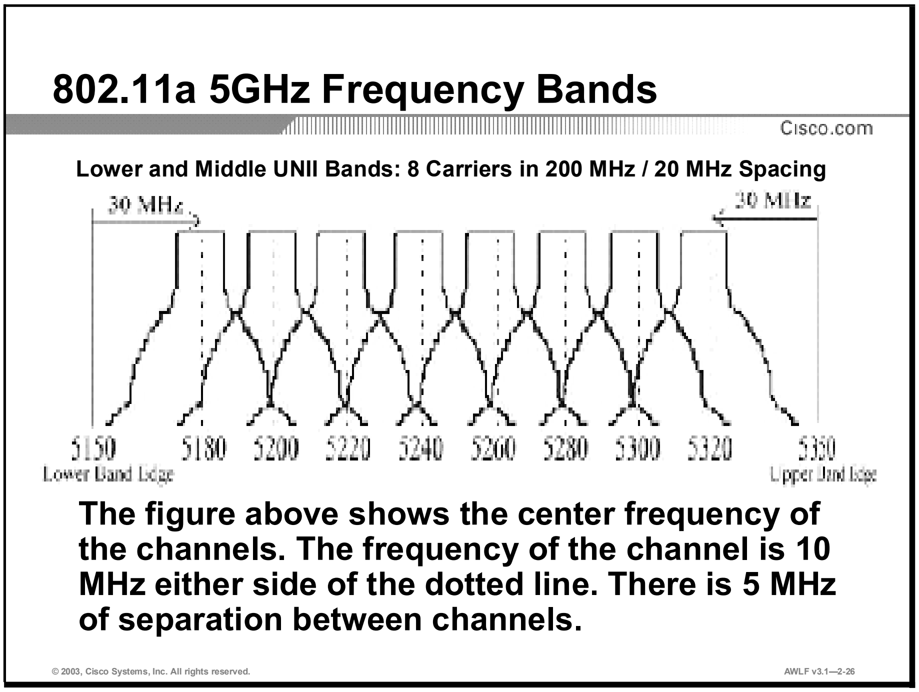
- 64-sample (3.2us) symbols
- 16-sample (0.8us) cyclic prefix/guard interval
- 250 symbols per second

Of 64 sub-carriers:

- 12 zero sub-carriers (In black) on sides and center
  - Side is frequency guard band leaving 16.5 MHz occupied BW
  - Center sub-carrier is zero for DC offset/carrier leak rejection
- 48 data sub-carriers (In green) per symbol
- 4 pilots sub-carriers (In red) per symbol for synchronization/tracking

AWLF v3.1—2-25

Orthogonal Frequency Division Multiplexing (OFDM) is the modulation technique used by 802.11a. The OFDM encoding scheme works by splitting the 20 MHz radio channel into 52 smaller sub-carriers. 48 of the 52 sub-carriers are used to transmit data. The remaining 4 sub-carriers are used as pilot carriers for monitoring path shifts and Inter Carrier Interference (ICI). These sub-carriers are then transmitted simultaneously at different frequencies to the receiver.



802.11a 5GHz Frequency Bands

Cisco.com

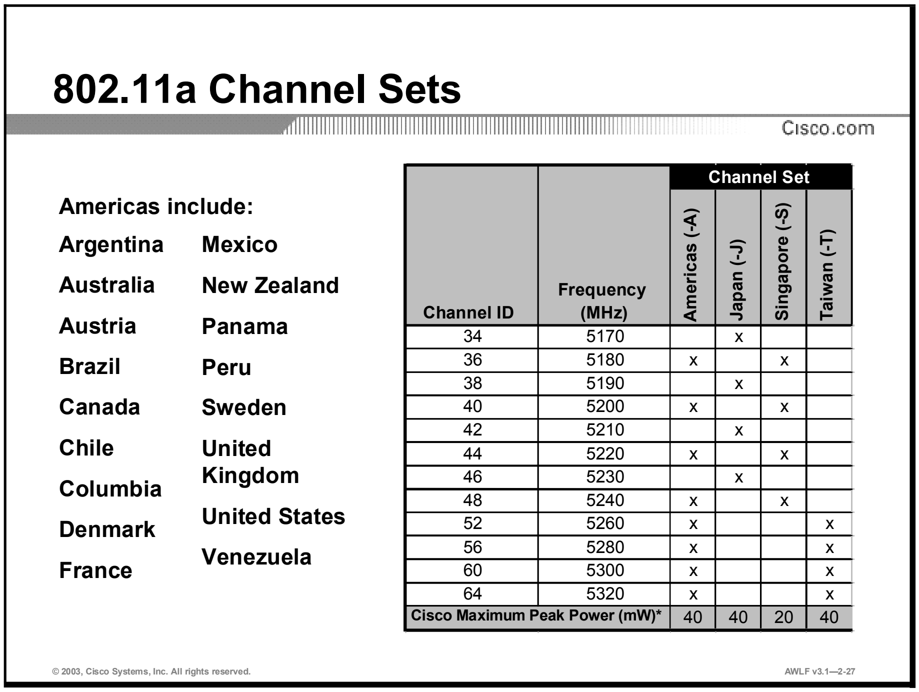
Lower and Middle UNII Bands: 8 Carriers in 200 MHz / 20 MHz Spacing

The figure above shows the center frequency of the channels. The frequency of the channel is 10 MHz either side of the dotted line. There is 5 MHz of separation between channels.

AWLF v3.1—2-26

This chart shows the lower and middle Unlicensed National Information Infrastructure (UNII) US channels. 802.11a has eight channels without overlap of frequency. 802.11b has 11 channels with only three channels that do not overlap in frequency. UNII-1 uses the first 4 channels and UNII-2 uses the last 4 channels.

- **UNII-1 – 5.15 GHz to 5.25 GHz**
  - Indoor only, 40 mW max with 6 dBi integrated antenna
  - Four 802.11a Channels
- **UNII-2 – 5.25 GHz to 5.35 GHz**
  - When the radio is capable of transmitting on UNII-1 and UNII-2 it must follow UNII-1 rules for transmit power and antenna gain.
  - If the radio is UNII-2 only the radio can transmit at 200 mW and use removable antennas.
  - Four 802.11a Channels
- **UNII-3 – 5.725 GHz to 5.825 GHz**
  - Outdoor only, 1 W max with 6 dBi antenna for point-to-multipoint and 23 dBi antenna for point-to-point.
  - Four 802.11a Channels



802.11a Channel Sets

Cisco.com

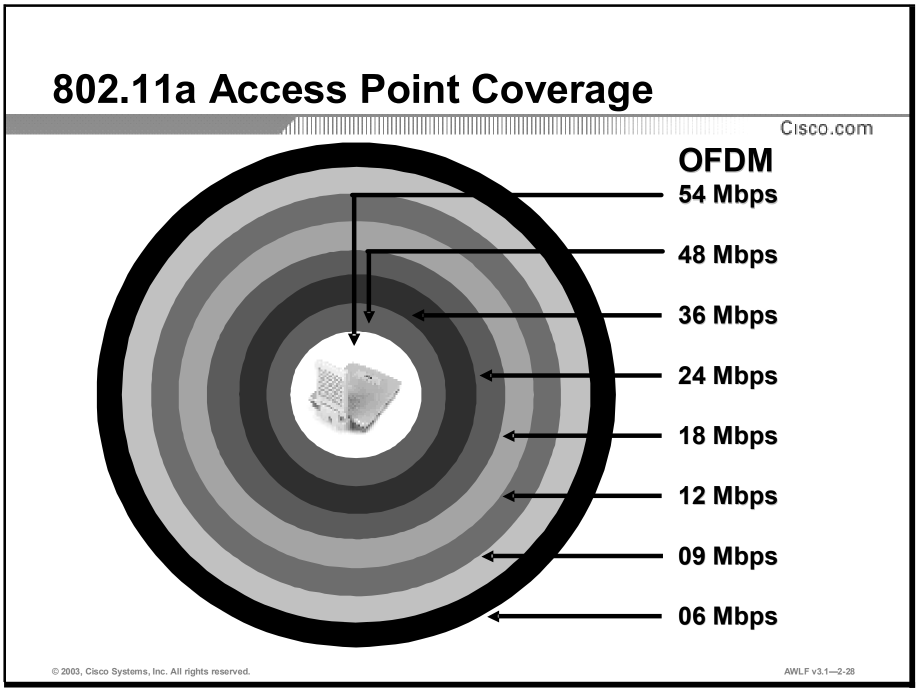
Americas include:

Argentina
Australia
Austria
Brazil
Canada
Chile
Columbia
Denmark
France
Mexico
New Zealand
Panama
Peru
Sweden
United Kingdom
United States
Venezuela

		Channel Set			
Channel ID	Frequency (MHz)	Americas (-A)	Japan (-J)	Singapore (-S)	Taiwan (-T)
34	5170		x		
36	5180	x		x	
38	5190		x		
40	5200	x		x	
42	5210		x		
44	5220	x		x	
46	5230		x		
48	5240	x		x	
52	5260	x			x
56	5280	x			x
60	5300	x			x
64	5320	x			x
Cisco Maximum Peak Power (mW)*		40	40	20	40

Assuming a 6 dBi antenna (The radiated power is):

- UNII-1 – 50 mW in the US/Japan, 200 mW in Europe, 4 Channels (5.15-5.25), Indoor Access- Fixed Antenna
- UNII-2 – 250 mW in US, 4 Channels (5.25-5.35)- Indoor/Outdoor Use – Flexible Antenna
- UNII-3 – 1 W in the US, 4 Channels (5.725-5.825) – Outdoor Bridging only
- HiperLAN – 200 mW in Europe, 8 Channels (5.25-5.35) – Indoor Use only
- HiperLAN– 1W in Europe, 11 channels (5.470-5.725) – Indoor/Outdoor Use –Flexible Antenna



802.11a Access Point Coverage

Cisco.com

OFDM

54 Mbps

48 Mbps

36 Mbps

24 Mbps

18 Mbps

12 Mbps

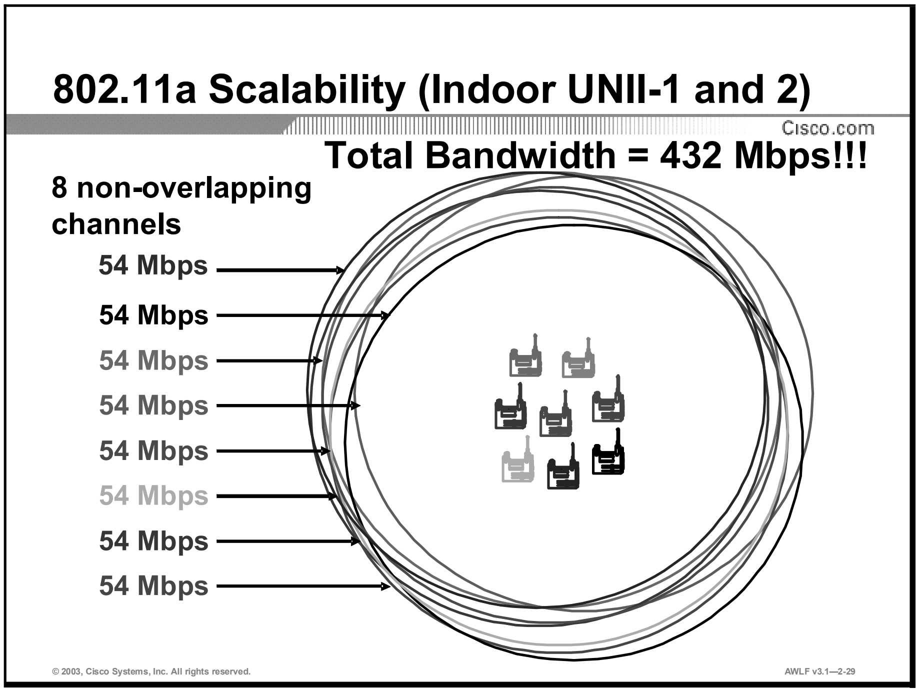
09 Mbps

06 Mbps

AWLF v3.1—2-28

Like the 802.11b products, the 802.11a products also support multiple data rate cells. Unlike the 4 data rates supported by 802.11b radios, the 802.11a radios support 8 different data rates.

Similar to the 802.11b radios, all 802.11a products also have the ability to data rate shift while moving. The 802.11a products allow the same person operating at 54 Mbps, to shift to 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, 9 Mbps and finally still communicate at the outside ring at 6 Mbps. This rate shifting happens without losing connection, and without any interaction from the user. Rate shifting also happens on a transmission-by-transmission basis; therefore the access point has the ability to support multiple clients at multiple speeds depending upon the location of each client.



802.11a Scalability (Indoor UNII-1 and 2)

Cisco.com

Total Bandwidth = 432 Mbps!!!

8 non-overlapping channels

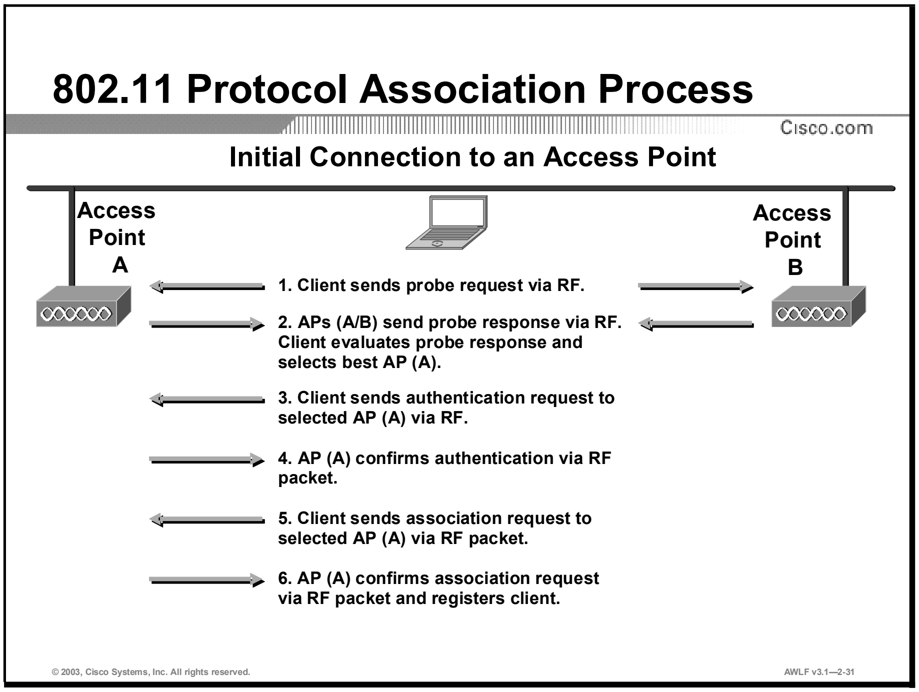
AWLF v3.1—2-29

Scalability is the ability to locate more than one access point in the same area, increasing the bandwidth of that area for all users local to that access point.

Since 802.11a has 8 non-overlapping channels, eight discrete systems can reside in the same area with no interference. If more than eight systems are required in the same area, they must time share the frequency. Therefore, the highest aggregate (total combined using both UNII-1 and 2 bands, indoor only) data rate for an 802.11a system is 432 Mbps for a given cell area.

Using the ability to scale throughput and add access points in the same cell area increases the overall available bandwidth of any cell.

802.11 Authentication



802.11 Protocol Association Process

Initial Connection to an Access Point

1. Client sends probe request via RF.
2. APs (A/B) send probe response via RF. Client evaluates probe response and selects best AP (A).
3. Client sends authentication request to selected AP (A) via RF.
4. AP (A) confirms authentication via RF packet.
5. Client sends association request to selected AP (A) via RF packet.
6. AP (A) confirms association request via RF packet and registers client.

AWLF v3.1—2-31

Association Process

While trying to connect to a WLAN, the client adapter card undergoes a two-step process, Authentication and Association. Authentication is the process of verifying the credentials of a client adapter card desiring to join a WLAN. Association is the process of associating a client adapter card with a given access point in the WLAN.

Step 1 When a client adapter card comes on line, it will broadcast a Probe Request.

Step 2 An access point that hears this will respond with details.

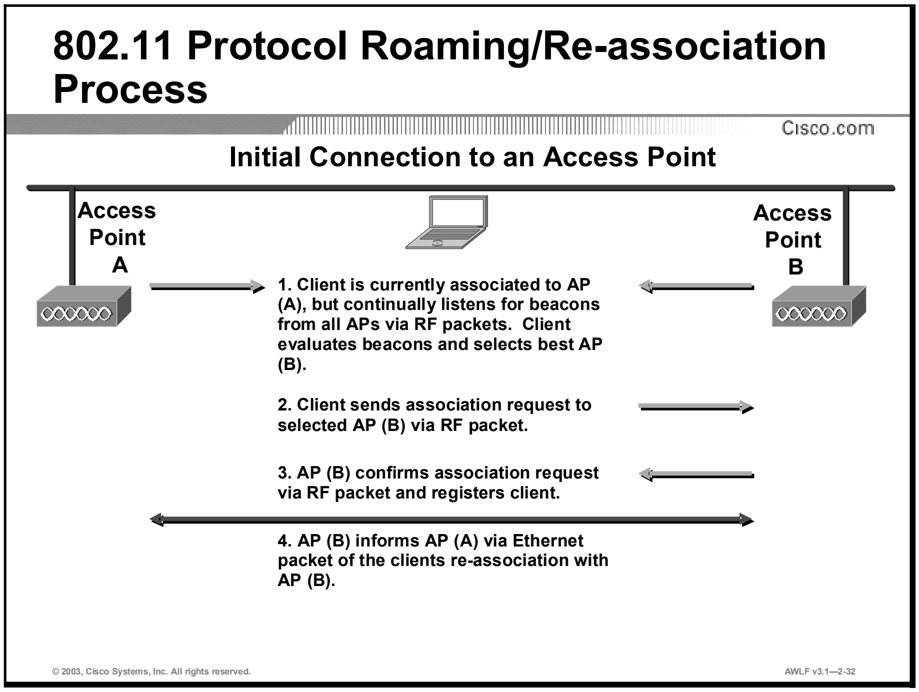
Step 3 The client adapter card makes a decision about which access point to associate with based on the information returned from the access point. Then the client adapter card will send an authentication request to the desired access point.

Step 4 The access point authenticates the client adapter card, and sends an acknowledgement back.

Step 5 Next the client adapter card sends up an association request to that access point.

Step 6 The access point then puts the client adapter card into the table, and sends back an association response. From that point forward, the network acts like the client adapter card is located at the access point. The access point acts like an Ethernet hub.

The access points broadcast a beacon at predetermined (and programmable) intervals. This broadcast contains information about the access point, such as RF hops to the backbone, load, hopping pattern, etc. The client adapter card always listens to ALL access points that it can hear (beacons received). It builds an information table about each one and enters the information the access points sends during beacons, including the signal strength of the access points.



802.11 Protocol Roaming/Re-association Process

Cisco.com

Initial Connection to an Access Point

1. Client is currently associated to AP (A), but continually listens for beacons from all APs via RF packets. Client evaluates beacons and selects best AP (B).

2. Client sends association request to selected AP (B) via RF packet.

3. AP (B) confirms association request via RF packet and registers client.

4. AP (B) informs AP (A) via Ethernet packet of the clients re-association with AP (B).

AWLF v3.1—2-32

As the client is moving out of range of his associated access point, the signal strength will start to drop off. At the same time, the strength of another access point will begin to increase and the following steps will occur.

Step 1 Client is currently associated to Access Point (A), but listens for the beacons from all Access Points. The Client evaluates the beacons received from Access Point (A) and (B) and selects the best Access Point to connect to.

Step 2 The Client selects Access Point (B) over (A) and sends an association request to the Access Point (B).

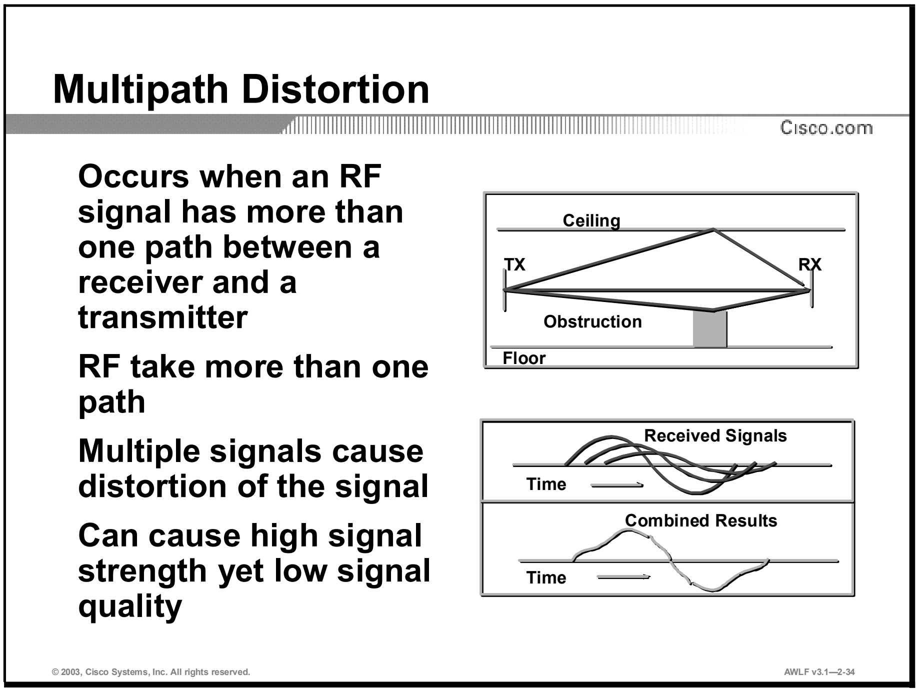
Step 3 Access Point (B) confirms the Clients association and registers the Client.

Step 4 Access Point (B) communicates with Access Point (A) by Ethernet backbone_to inform Access Point (A) of the re-association with Access Point (B).

This same process will occur for load balancing reasons.

Due to the Inter Access Point Protocol (IAPP) traffic not being fully covered in the 802.11 specifications, it is critical to keep the backbone all one vendor.

Multipath



Multipath Distortion

Cisco.com

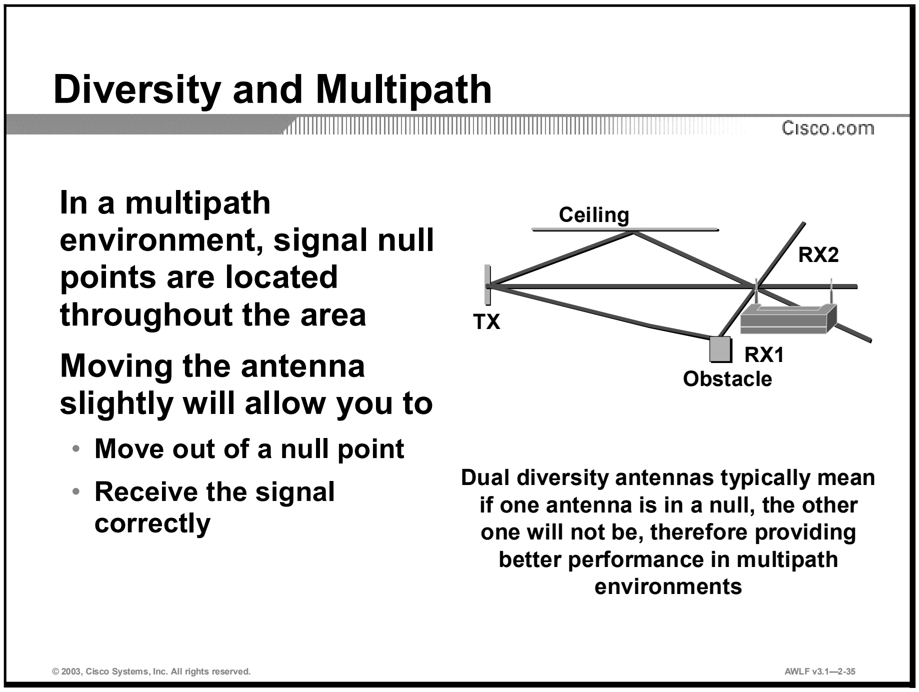
- Occurs when an RF signal has more than one path between a receiver and a transmitter
- RF take more than one path
- Multiple signals cause distortion of the signal
- Can cause high signal strength yet low signal quality

AWLF v3.1—2-34

Multipath interference occurs when an RF signal has more than one path between a receiver and a transmitter. 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 an RX antenna. These multiple signals combine in the RX antenna and receiver to cause distortion of the signal.

Multipath interference can cause high signal strength yet low signal quality, whereby the data would be unreadable.

You can relate this to a common occurrence in your car. As you pull up to a stop, you may notice static on the radio. But as you move forward a few inches or feet, the station starts to come in more clearly. By rolling forward, you move the antenna slightly, out of the point where the multiple signals converge.



Diversity and Multipath

Cisco.com

In a multipath environment, signal null points are located throughout the area

Moving the antenna slightly will allow you to

- Move out of a null point
- Receive the signal correctly

Ceiling
RX2
TX
RX1
Obstacle

Dual diversity antennas typically mean if one antenna is in a null, the other one will not be, therefore providing better performance in multipath environments

AWLF v3.1—2-35

When a radio wave bounces back on itself 180 degrees out of phase, a dead spot or "null" is created. Null points are a fact of life with RF and will be located throughout the coverage area.

Two things can change the multipath null point:

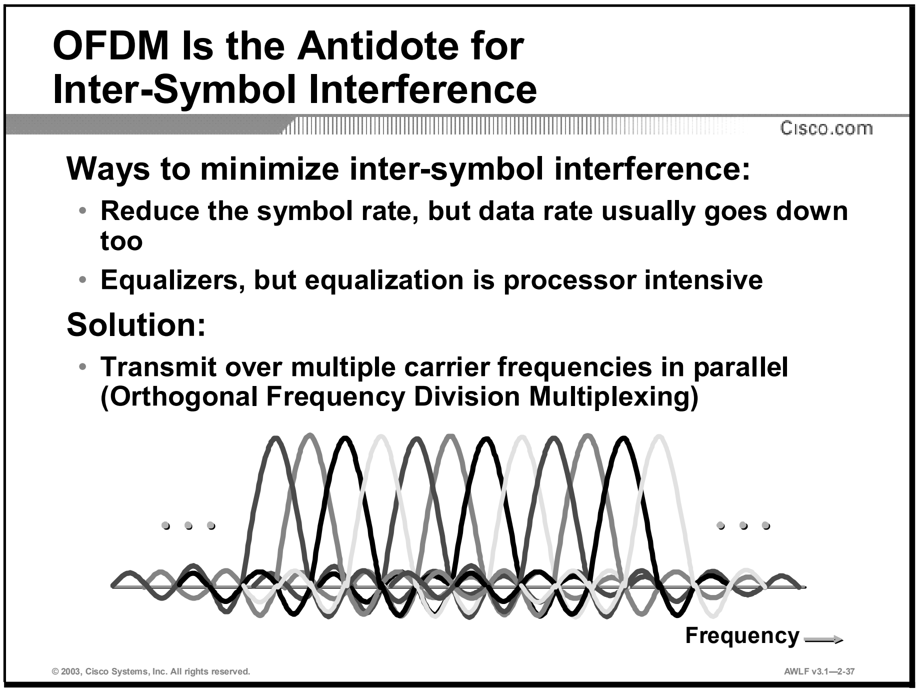
- Change the location of the antenna.
- Change the type of antenna, moving the main lobe of energy and affecting the reflected energy.

A diversity antenna system can be compared to a switch that selects one antenna or another, never both at the same time. The radio in receive mode will continually switch between antennas listening for a valid radio packet. After the beginning sync of a valid packet is heard, the radio will evaluate the sync signal of the packet, on one antenna, then switch to the other antenna and evaluate. Then the radio will select the best antenna, and use only that antenna for the remaining portion of that packet.

On transmit, the radio will select the same antenna it used the last time it communicated to that given radio. If a packet fails, it will switch to the other antenna and retry the packet.

Changing the type of antenna and/or the location of the antenna can eliminate multipath interference. The shortest distance between two points is a straight line. As other signals take longer paths, they will arrive later and weaker. All of the signals will combine in the RX to form a single received signal, and the result is distorted.

Caution: Diversity is *not* designed for using two antennas, covering two *different* coverage cells. The problem in using it this way, is that if antenna #1 is communicating to device #1, while device #2 (which is in the antenna #2 cell) tries to communicate, antenna #2 is not connected (due to the position of the switch), and the communication fails. Diversity antennas should cover the same area, from only a slightly different location.



OFDM Is the Antidote for Inter-Symbol Interference

Ways to minimize inter-symbol interference:

- Reduce the symbol rate, but data rate usually goes down too
- Equalizers, but equalization is processor intensive

Solution:

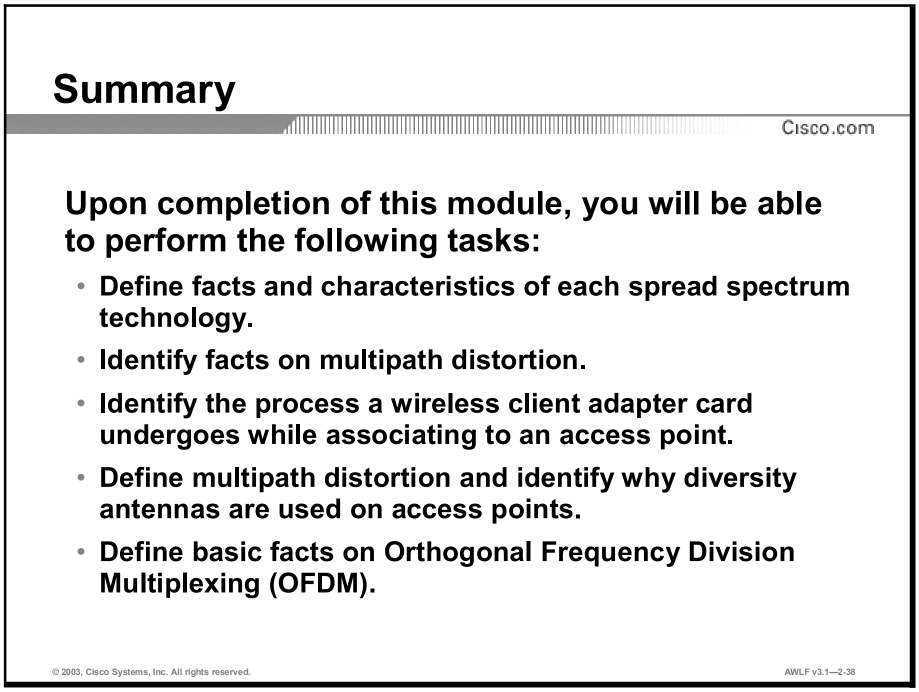
- Transmit over multiple carrier frequencies in parallel (Orthogonal Frequency Division Multiplexing)

AWLF v3.1—2-37

Multipath fading is a special case of inter-symbol interference. Most 802.11 wireless communication equipment use omni-directional antennas, so the RF energy is distributed in every direction. The radio waves will take different paths from the transmitter to the receiver, because the radio waves are reflected by surfaces in the area. The different paths will result in the RF energy being delayed with respects to each other. When the delayed radio waves are combined in the receiver the resulting out-of-phase signals may cancel each other's energy. OFDM signal is not affected by inter-symbol interference because the data is sent on the multiple frequencies instead of single frequency so it is very unlikely that two frequencies will fade at the same time in the same environment. Fourier transform has an added advantage of making the circuitry simple, because of the Fourier transform you have to use only one pair of modulator and demodulator instead of using many modulators/demodulators as we are using multiple frequencies.

Summary

This section summarizes the concepts you learned in this module.



Summary

Upon completion of this module, you will be able to perform the following tasks:

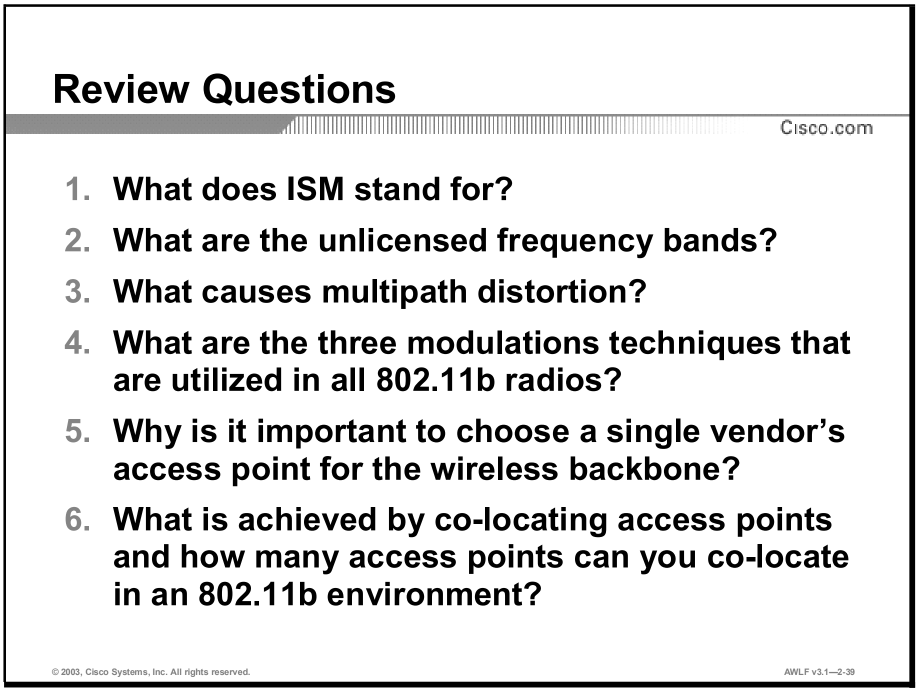
- **Define facts and characteristics of each spread spectrum technology.**
- **Identify facts on multipath distortion.**
- **Identify the process a wireless client adapter card undergoes while associating to an access point.**
- **Define multipath distortion and identify why diversity antennas are used on access points.**
- **Define basic facts on Orthogonal Frequency Division Multiplexing (OFDM).**

AWLF v3.1—2-38

Upon completion of this module, you will be able to perform the following tasks:

- Define facts and characteristics of each spread spectrum technology.
- Identify facts on multipath distortion.
- Identify the process a wireless client adapter card undergoes while associating to an access point.
- Define multipath distortion and identify why diversity antennas are used on access points.
- Define basic facts on Orthogonal Frequency Division Multiplexing (OFDM).

Review Questions



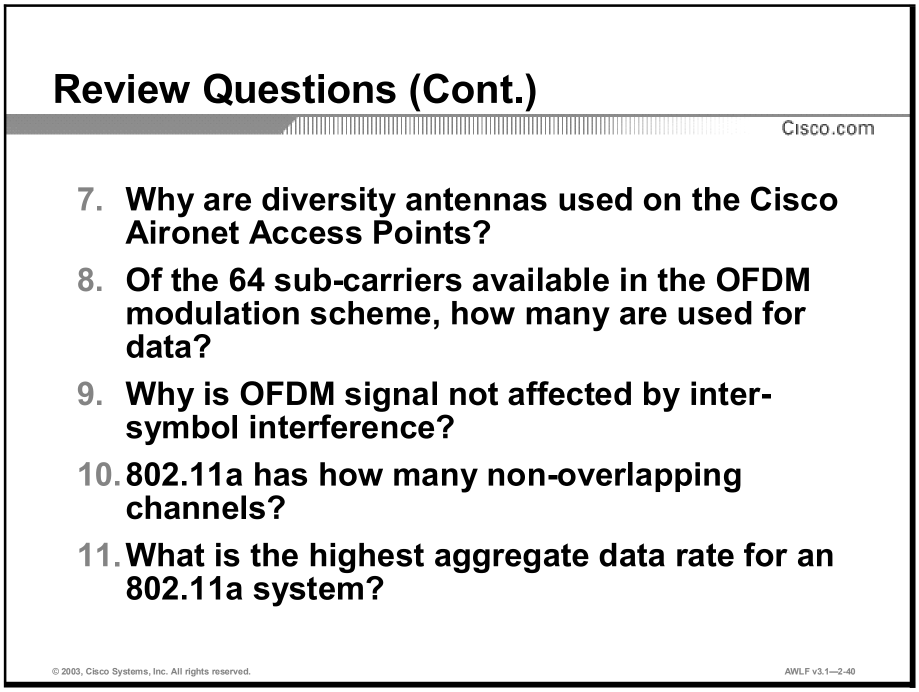
Review Questions

Cisco.com

1. What does ISM stand for?
2. What are the unlicensed frequency bands?
3. What causes multipath distortion?
4. What are the three modulations techniques that are utilized in all 802.11b radios?
5. Why is it important to choose a single vendor's access point for the wireless backbone?
6. What is achieved by co-locating access points and how many access points can you co-locate in an 802.11b environment?

AWLF v3.1—2-39

Answer these review questions.



Review Questions (Cont.)

Cisco.com

7. Why are diversity antennas used on the Cisco Aironet Access Points?
8. Of the 64 sub-carriers available in the OFDM modulation scheme, how many are used for data?
9. Why is OFDM signal not affected by inter-symbol interference?
10. 802.11a has how many non-overlapping channels?
11. What is the highest aggregate data rate for an 802.11a system?

AWLF v3.1—2-40

Answer these review questions.

Module 3

Wireless LAN Topologies

Overview

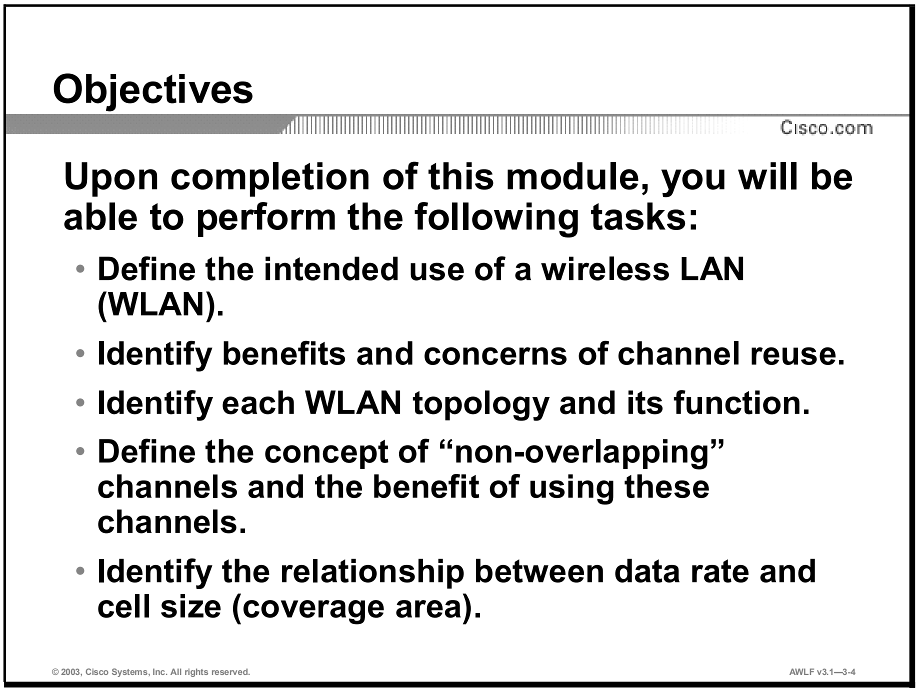
This module explores typical topologies associated with wireless LANs (WLANs).

It includes the following topics:

- Objectives
- WLAN Topology
- Enterprise Topologies, Channel Reuse and Multi-Rate Shifting
- Inline Power
- Cisco Aironet Access Point VLAN Feature
- Cisco Aironet Access Point Quality of Service Feature
- Cisco Aironet Access Point Proxy Mobile IP
- Cisco Aironet Structured Wireless Aware Network (SWAN)
- Summary
- Review Question

Objectives

This section lists the module's objectives.



Objectives

Cisco.com

Upon completion of this module, you will be able to perform the following tasks:

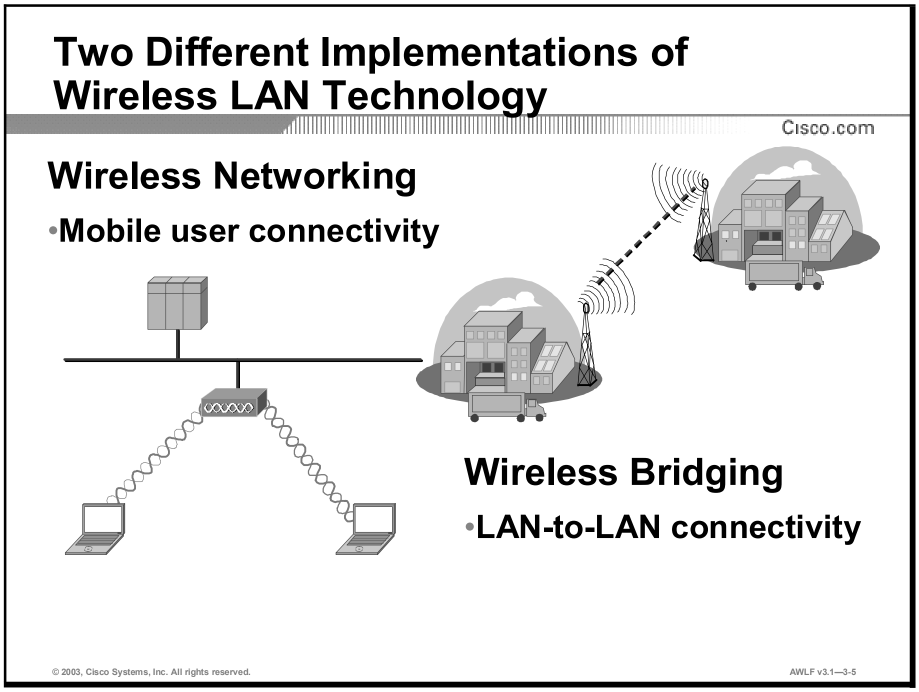
- **Define the intended use of a wireless LAN (WLAN).**
- **Identify benefits and concerns of channel reuse.**
- **Identify each WLAN topology and its function.**
- **Define the concept of "non-overlapping" channels and the benefit of using these channels.**
- **Identify the relationship between data rate and cell size (coverage area).**

© 2003, Cisco Systems, Inc. All rights reserved. AWLF v3.1—3-4

Upon completion of this module, you will be able to perform the following tasks:

- Define the intended use of a wireless LAN (WLAN).
- Identify benefits and concerns of channel reuse.
- Identify each WLAN topology and its function.
- Define the concept of "non-overlapping" channels and the benefit of using these channels.
- Identify the relationship between data rate and cell size (coverage area).

WLAN Topology



Two Different Implementations of Wireless LAN Technology

Cisco.com

Wireless Networking

- Mobile user connectivity

Wireless Bridging

- LAN-to-LAN connectivity

© 2003, Cisco Systems, Inc. All rights reserved.

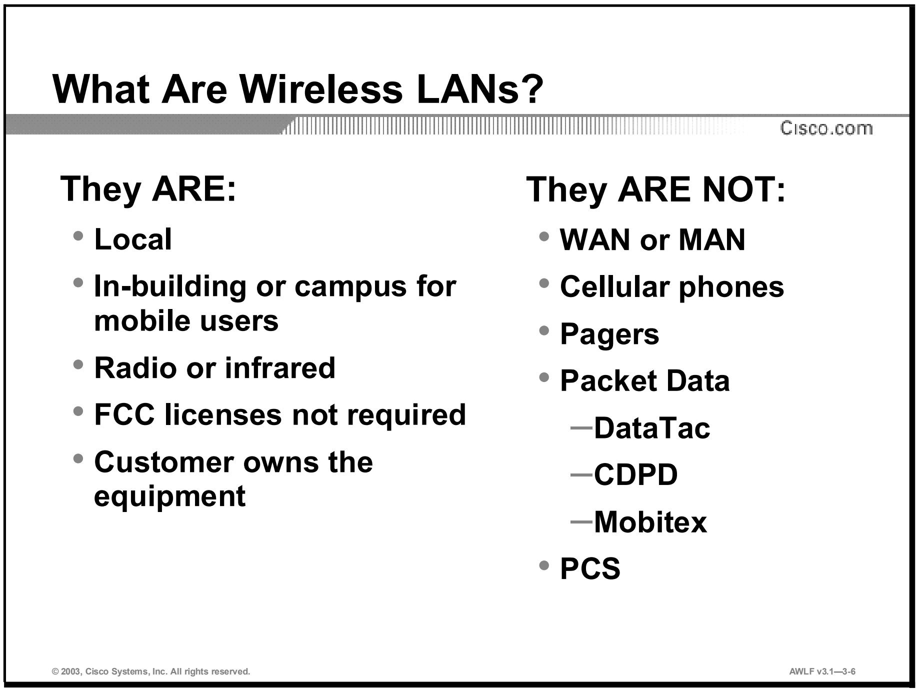
AWLF v3.1—3-5

Cisco Aironet® Wireless products fit into two main categories: wireless in-building LANs and wireless building-to-building bridges. Wireless LANs replace the layer one transmission medium of a traditional wired network (usually Cat 5 cable) with radio transmission over the air.

Cisco Aironet WLAN products can plug into a wired network and function as an overlay to traditional or wired LANs, or can be deployed as a standalone LAN where wired networking isn't feasible. Wireless LANs permit the use of desktop and/or portable computers or specialty devices in a system where connection to the network is essential. WLANs are typically within a building, and for distances up to 1000 feet.

Properly deployed WLANs can provide instant access to the network from anywhere in facility. Users can roam without losing network connection.

The Cisco Aironet WLAN provides complete flexibility. Wireless bridges allow two or more networks that are physically separated to be connected on one LAN, without the time or expense of dedicated cable or T1 lines.



What Are Wireless LANs?

Cisco.com

They ARE:

- Local
- In-building or campus for mobile users
- Radio or infrared
- FCC licenses not required
- Customer owns the equipment

They ARE NOT:

- WAN or MAN
- Cellular phones
- Pagers
- Packet Data
  - —DataTac
  - —CDPD
  - —Mobitex
- PCS

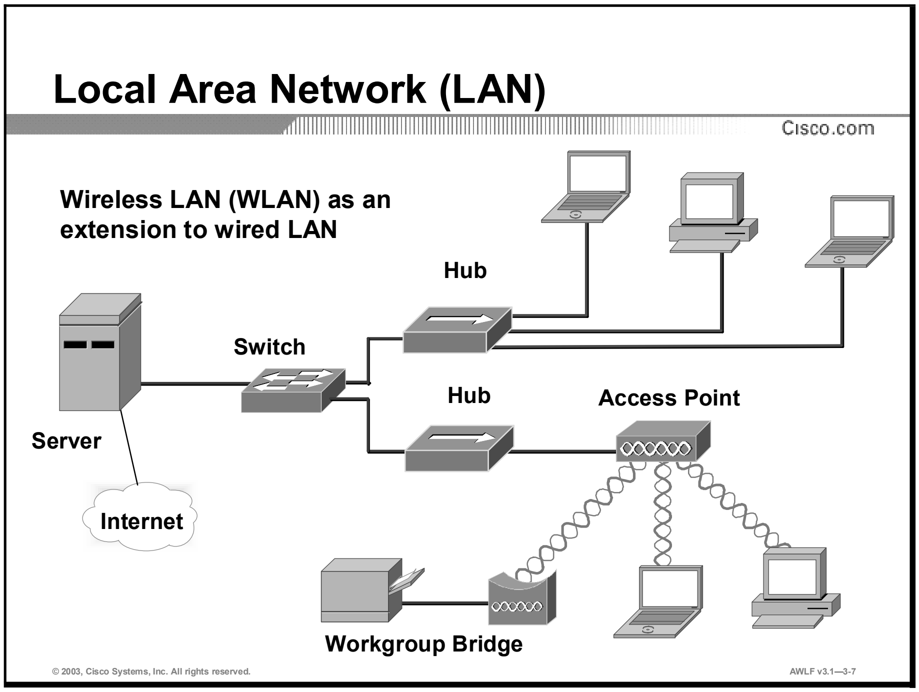
AWLF v3.1—3-6

Cisco Aironet Wireless LANS are designed for a LOCAL not a Wide Area Network. They are intended for in-building wireless networks, or line-of-site outdoor bridging applications.

No license is required for the spread spectrum and OFDM devices from Cisco Aironet in most countries.

They are NOT designed for city wide wireless network.

There is no rental, ongoing, or licensing fees for the usage of Cisco Aironet wireless devices.



Local Area Network (LAN)

Cisco.com

Wireless LAN (WLAN) as an extension to wired LAN

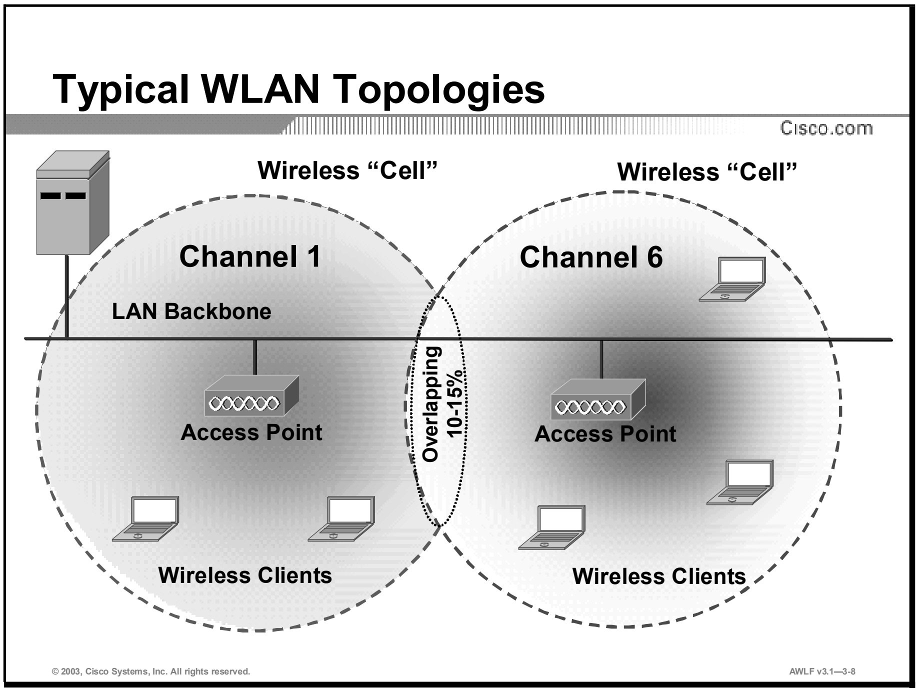
© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—3-7

Wired LANs require that users to locate themselves to one spot and stay there. WLANs are an extension to the wired LAN network. WLANs can be an overlay to or substitute for traditional wired LAN networks.

With Cisco Aironet Wireless LANs, mobile users can:

- Move freely around a facility.
- Enjoy real time access to the wired LAN, at wired Ethernet speeds.
- Access ALL the resources of wired LANs.



Typical WLAN Topologies

AWLF v3.1—3-8

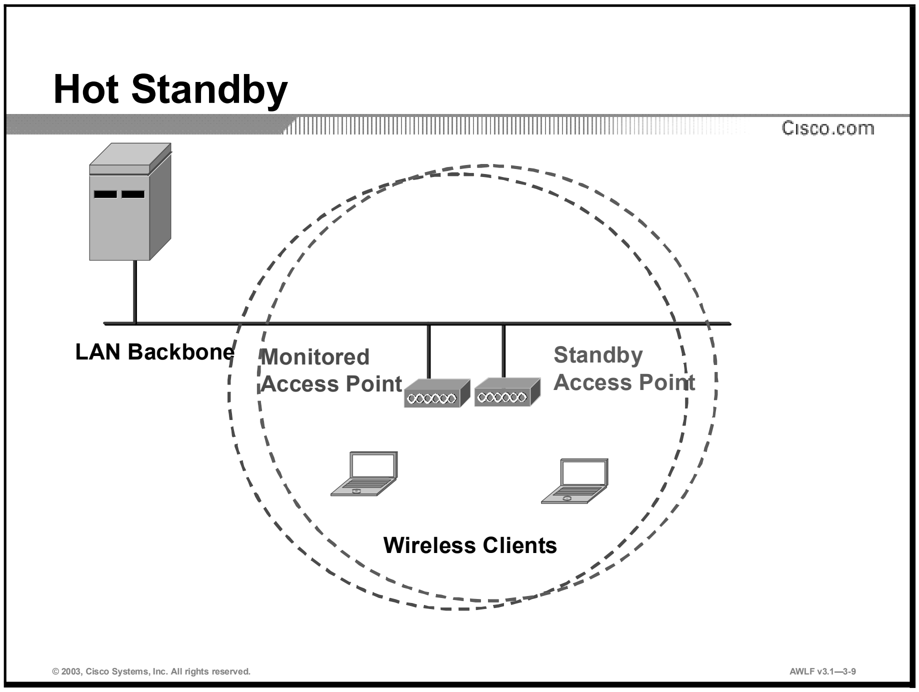
The basic service area (BSA) is the area of RF coverage provided by an access point, also referred to as a "microcell." To extend the BSA, or to simply add wireless devices and extend range of an existing wired system, an access point can be added. (As the name "access point" indicates, this unit is the point at which wireless clients can access the network.)

The access point attaches to the Ethernet backbone and communicates with all the wireless devices in the cell area. The access point 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 access point.

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 have 10-15% overlap to allow remote users to roam without losing RF connections.

Bordering cells should be set to different non-overlapping channels for best performance.



Hot Standby

Cisco.com

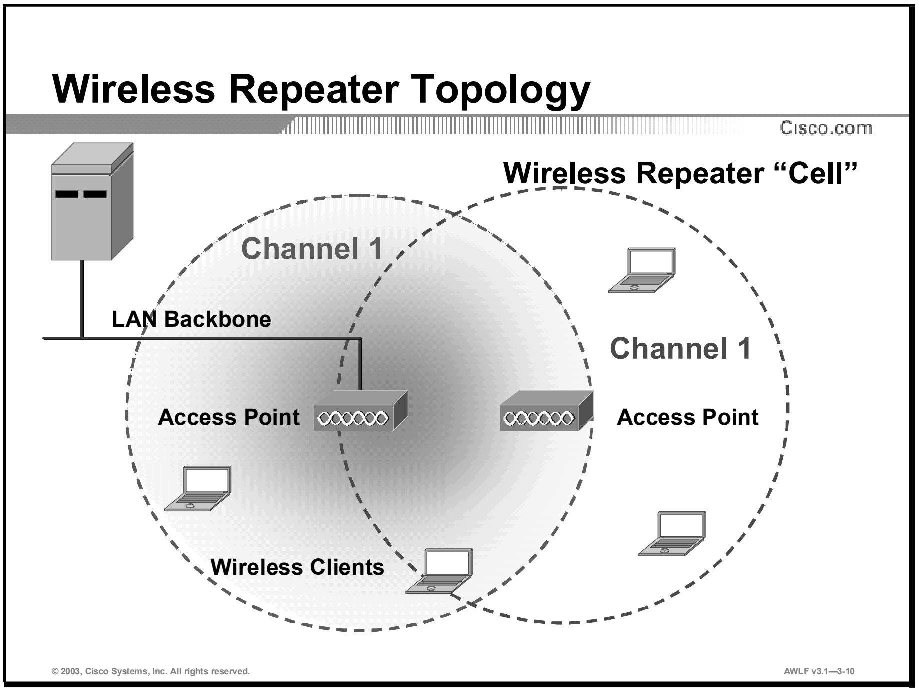
AWLF v3.1—3-9

In a system where it is essential to have communications, some customers will require redundancy. The Cisco Aironet wireless products work well in this environment.

With some other vendors' direct sequence products, both access point units will be set to the same frequency and data rate. Since they timeshare the frequency, only one unit can be talking at a time. If that one unit goes down for some reason, the remote clients will hand off to the other active unit. While this does provide redundancy, it does not provide any more throughput than a single access point.

Utilizing the hot standby mode, the redundant access point can be set to monitor the main access point. This monitoring is done via both the RF and the Ethernet connection. In the event that either fails, the redundant access point will take over.

In the hot standby mode, the redundant access point becomes a client (will not accept associations from clients) of the monitored access point and therefore does not interfere with the monitored access point.

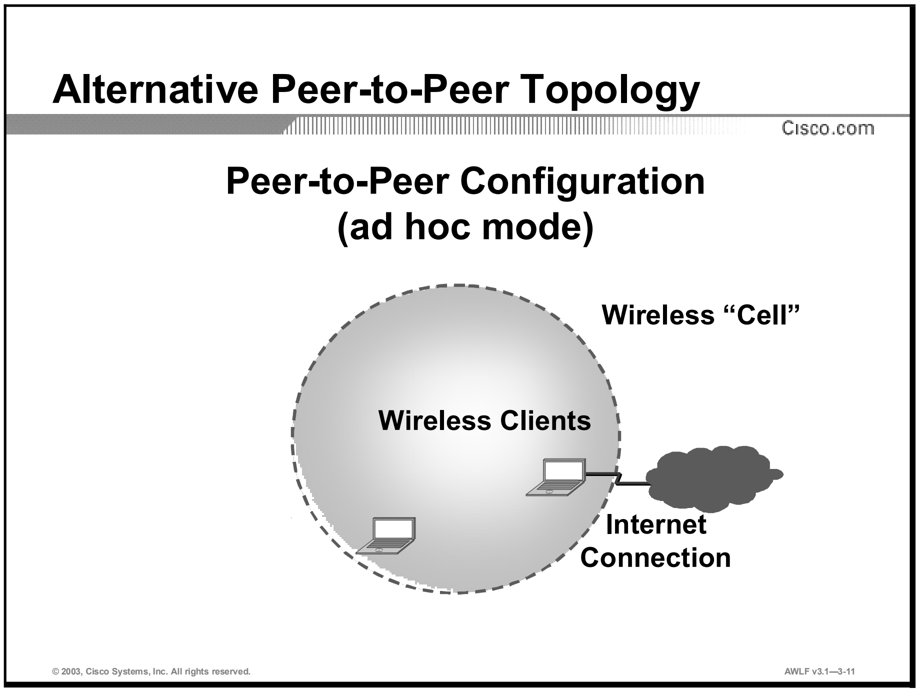


Wireless Repeater Topology

Cisco.com

AWLF v3.1—3-10

In an environment where extended coverage is needed, but access to the backbone is not practical or available, a wireless repeater can be used. A wireless repeater is simply an access point that is not connected to the wired backbone. This requires a 50% overlap of the access point on the backbone and the wireless repeater. Receive and re-transmit time involved will decrease due to data rates.



Alternative Peer-to-Peer Topology

Cisco.com

Peer-to-Peer Configuration (ad hoc mode)

Wireless “Cell”

Wireless Clients

Internet Connection

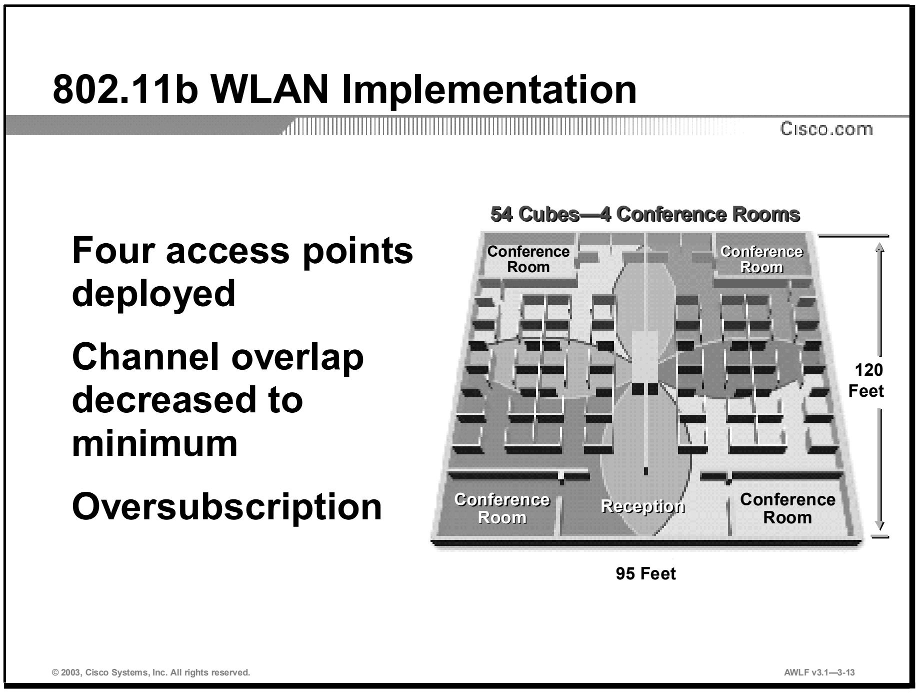
AWLF v3.1—3-11

The BSA can consist of nothing more than two or more wireless PCs with a wireless network card. Operating systems such as Windows 95, 98, Windows NT/2000/XP and Me have made this type of network very easy to setup.

This can be used for a small office (or home office) to allow a laptop to be connected to the main PC, or for several people to simply share files.

This type of network has one drawback- coverage limitation. Everyone must be able to hear everyone else.

Enterprise Topologies, Channel Reuse and Multi-Rate Shifting



802.11b WLAN Implementation

Cisco.com

- Four access points deployed
- Channel overlap decreased to minimum
- Oversubscription

AWLF v3.1—3-13

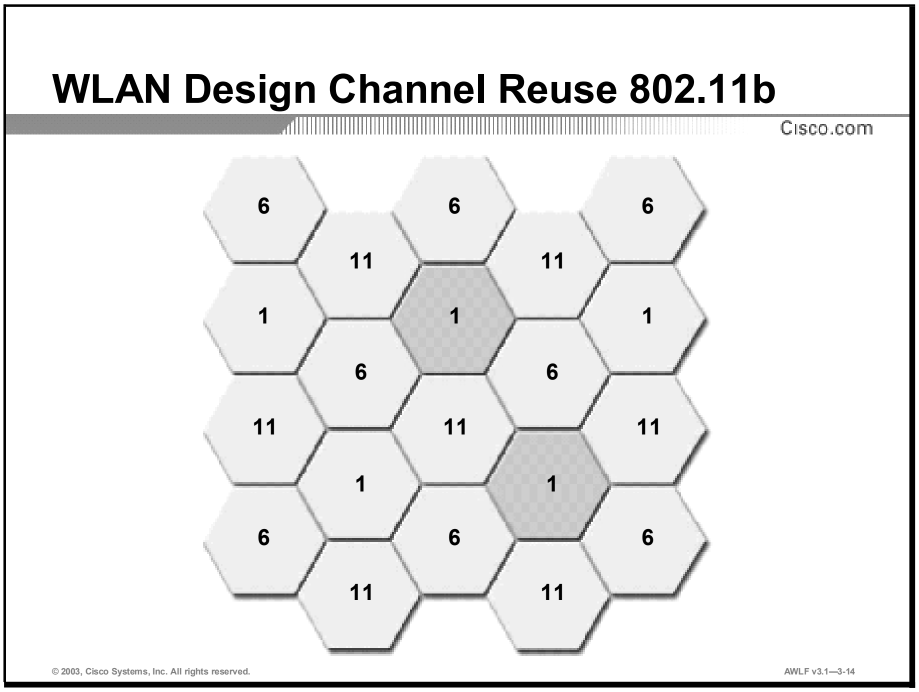
In this particular example the goal was to cover the whole office area with wireless coverage.

Some items to note:

- Full 11 Mbps coverage due to the density of users
- Cell size can be controlled by the use of radio power settings
- Since there are only three non-overlapping channels, access point placement was made to reduce the overlap of same channel
- 14 users per access points with no conference rooms provides .48 Mbps per users
- 14 users + 1 conference room
  (10 users) = 24 total users provides .28 Mbps per user

Oversubscription is an Internet Service Provider (ISP) buzzword that simply means to over sell your bandwidth. How much you oversubscribe depends on your customer base and your customer usage patterns. Typically ISP's will over subscribe somewhere between 5 and 20 to 1 for broadband cable/DSL access. What that means is that if you have 128 kbps of bandwidth you should be able to sell somewhere between 5 and 20 times that much bandwidth on to people.

The same concept of oversubscription can be applied to WLAN designs. In a typical office environment, not all of the WLAN user will be using the WLAN resources at the same exact time. For example, some users will be surfing the internet, some will be their reading e-mail they just downloaded and some will be saving files to the corporate sever. With this usage pattern in mind it is possible use oversubscribe in a typical office environment without the risk of end users complaining about performance issues.



WLAN Design Channel Reuse 802.11b

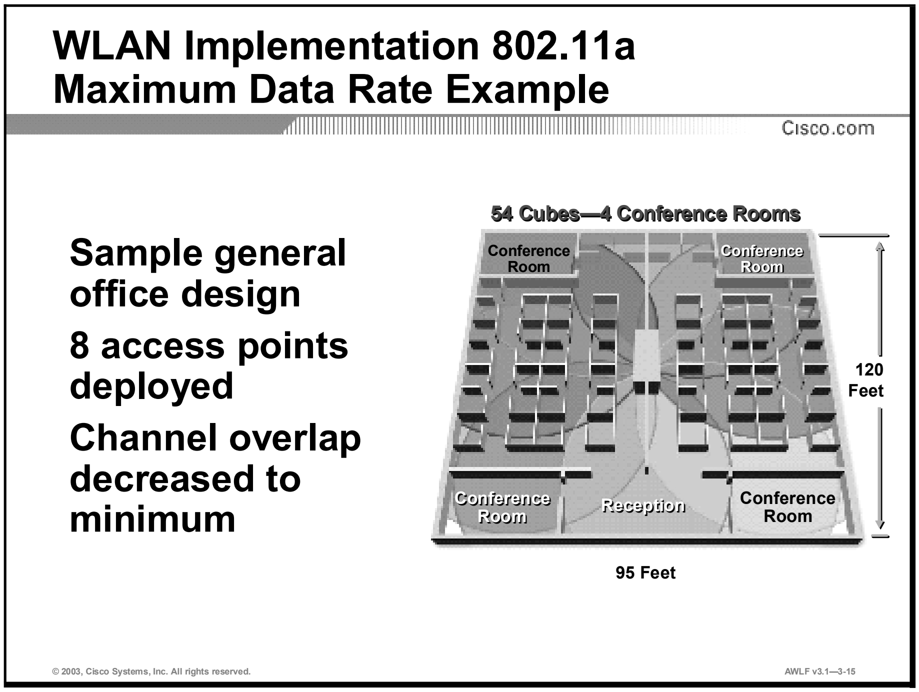
Cisco.com

AWLF v3.1—3-14

This particular diagram indicates the 3 non-overlapping channels that are available within 802.11b.

The goal of access point/cell placement is to reduce the overlapping of cells that are on the same channel.

You can correlate this concept to the placement of FM radio stations throughout the country. You will never see two radio stations in the same geographic area on the exact same channel. The same concept exists in this particular case.



WLAN Implementation 802.11a Maximum Data Rate Example

Cisco.com

- Sample general office design
- 8 access points deployed
- Channel overlap decreased to minimum

AWLF v3.1—3-15

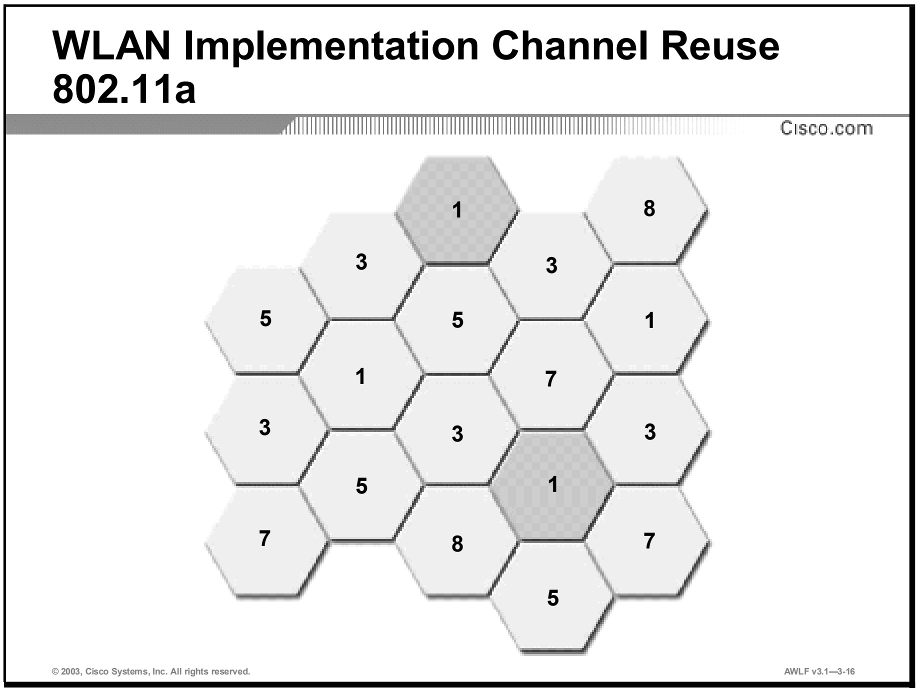
Using the same diagram as on the 802.11b example you will see that by using 802.11a products you have the capability of increasing the throughput of any individual user due to the data rate of each cell increasing to 54 Mbps.

With 802.11a products you have 8 non-overlapping channels and can thus have more cells on a per area basis.

This particular example uses 8 cells utilizing 8 different channels. With this deployment is not as important to worry about the co-channel interference.

Note 7 users per access points with no conference rooms provide 4.5 Mbps per users.

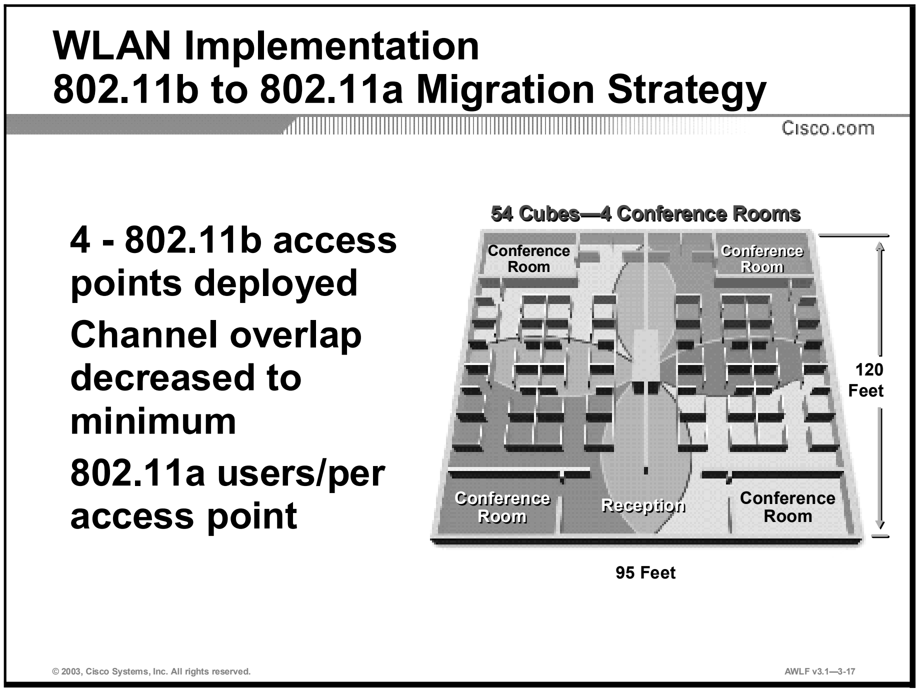
Note 7 users + 1 conference room (10 users) = 17 total users provides 1.8 Mbps per user.



WLAN Implementation Channel Reuse 802.11a

AWLF v3.1—3-16

This particular diagram illustrates the channel deployment of 802.11a products throughout a given area. As you can see the cells are easier to deploy due to there being 8 different channels to work with. It is recommended for neighboring cells to be at least 2 channels apart as illustrated above.



WLAN Implementation
802.11b to 802.11a Migration Strategy

- 4 - 802.11b access points deployed
- Channel overlap decreased to minimum
- 802.11a users/per access point

AWLF v3.1—3-17

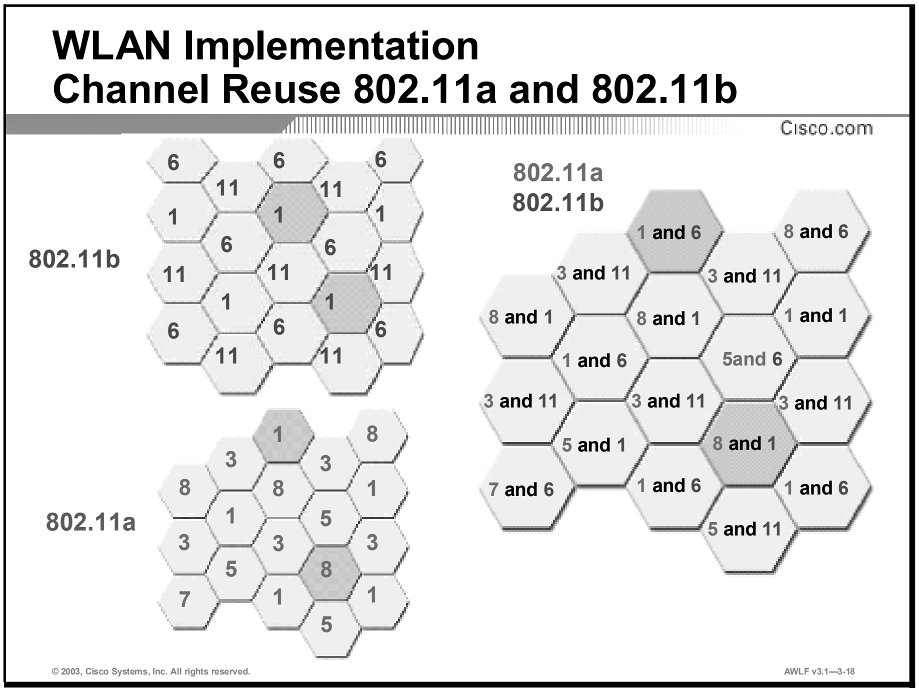
When using the same layout for this example 802.11b access points are already installed and can be upgraded by installing the 802.11a modules into the existing Cisco Aironet Access Point's.

When this has been completed there will more than likely be some 802.11a holes of coverage due to the fact 802.11b will cover more area than 802.11a.

In this case to fill these holes of coverage 802.11a "ONLY" access point's can be used and deployed on the same backbone infrastructure.

Some items to note:

- 14 users per access point and Range <40 feet = 2.3 Mbps
- Range >40–120 feet = .71 Mbps
- Max users = 24 = .41 Mbps
- 802.11b users/per access point
- Range 0–120 feet
  - Max users = 14 = .48 Mbps
  - Max users = 24 = .28 Mbps



WLAN Implementation
Channel Reuse 802.11a and 802.11b

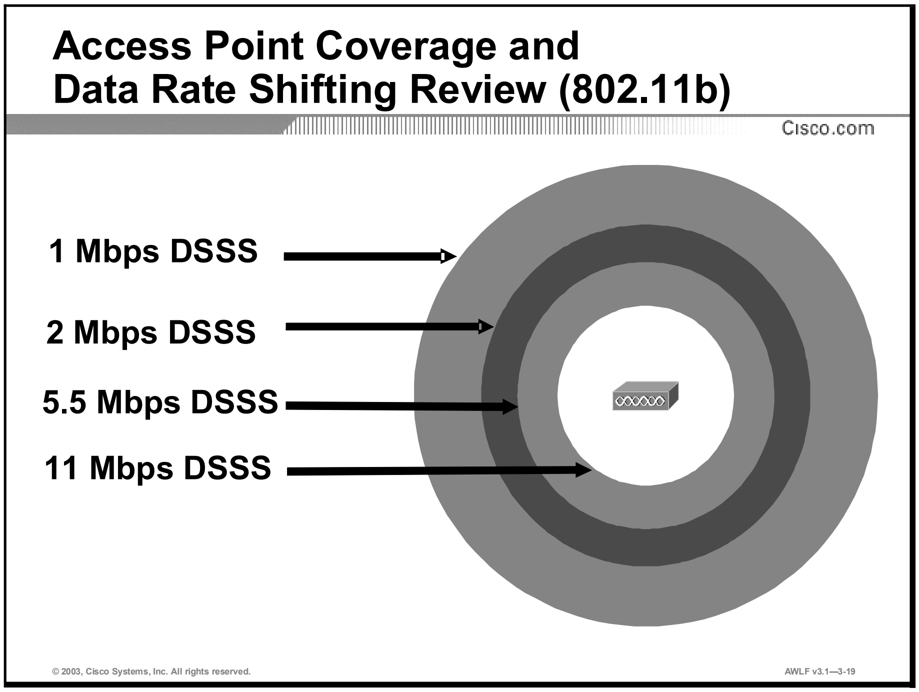
Cisco.com

AWLF v3.1—3-18

When implementing a mixed environment with 802.11a and 802.11b access points be careful to separate the 802.11b access points so they do not overlap.

In the example above, each cell has 2 access points. The number on the left represents the channel for the 802.11a cell; the number on the right represents the channel for the 802.11b cell.

Well planned channel deployment guarantees a productive and optimized installation.



Access Point Coverage and Data Rate Shifting Review (802.11b)

Cisco.com

1 Mbps DSSS

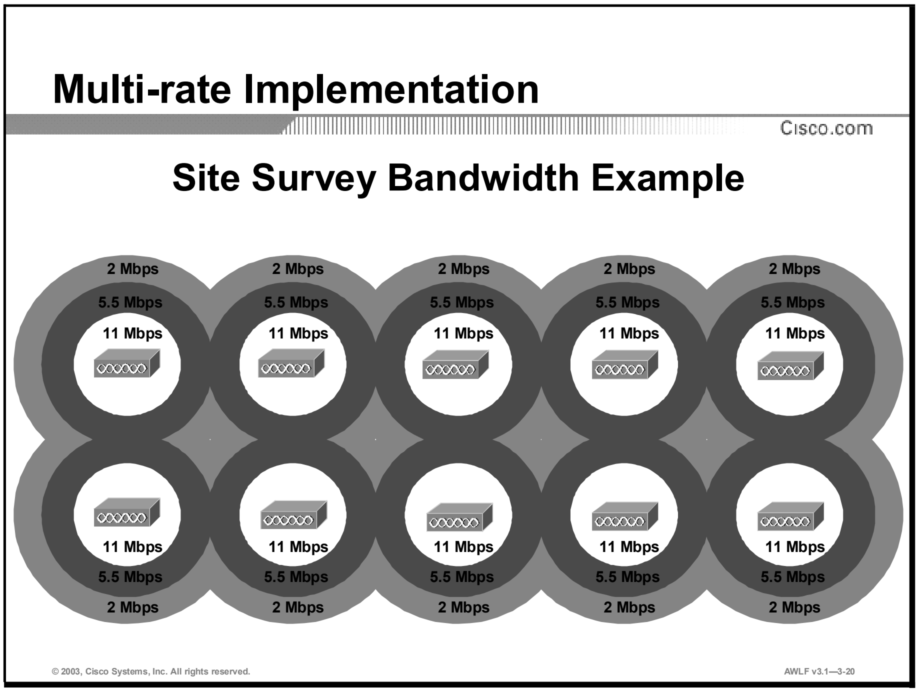
2 Mbps DSSS

5.5 Mbps DSSS

11 Mbps DSSS

AWLF v3.1—3-19

As a client roams away from the access point, the transmission between the two attenuates. Rather than decreasing reliability, the Cisco Aironet Access Point shifts to a slower data rate, which gives more accurate throughput. This is called data rate or multi-rate shifting. As a client moves away from an access point, its data rate will go from 11 Mbps, to 5.5 Mbps, 2 Mbps, and finally to 1 Mbps, as shown in this illustration. This happens without losing connection, and without any interaction from the user. This also happens on a transmission-by-transmission basis; therefore if other clients remain in the 11 Mbps cell, they will still communicate at 11 Mbps.



Multi-rate Implementation

Cisco.com

Site Survey Bandwidth Example

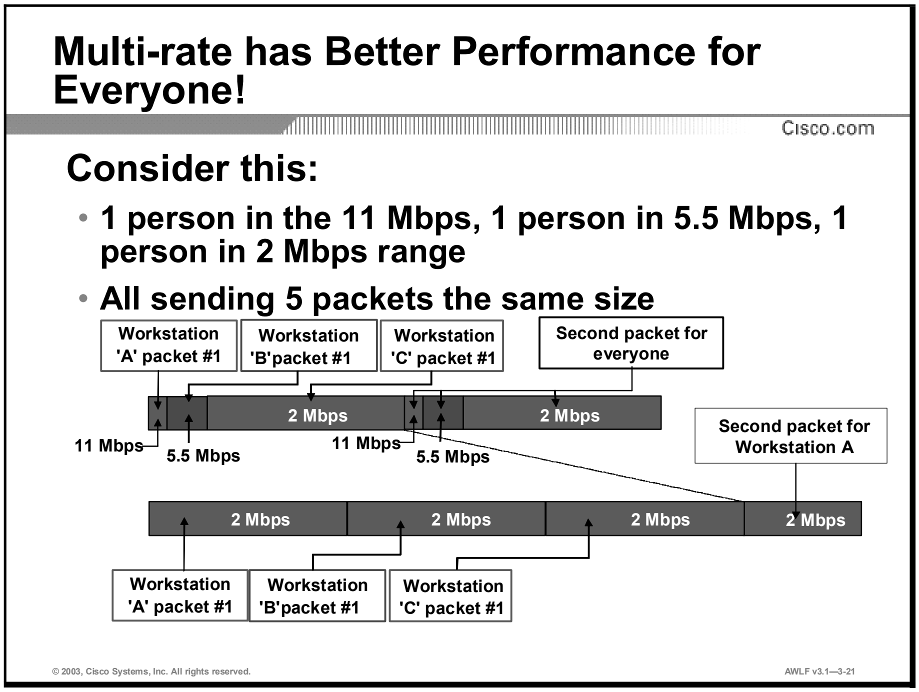
© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—3-20

Multi-rate Implementation

Bandwidth requirements factor into coverage mappings, since the distance from an access point affects the available bandwidth. The above example provides for seamless roaming, but not at a constant speed. To take advantage of the multi-rate technology a client can step down in bandwidth in order to gain greater coverage distances with a single access point. On the other hand, if 11 Mbps is required everywhere, the access points would need to be relocated so that ONLY the 11 Mbps circles were touching each other. This would require a greater amount of access points but consistent bandwidth would be achieved.

Notice that the data rate decreases as the coverage distance increases.



Multi-rate has Better Performance for Everyone!

Cisco.com

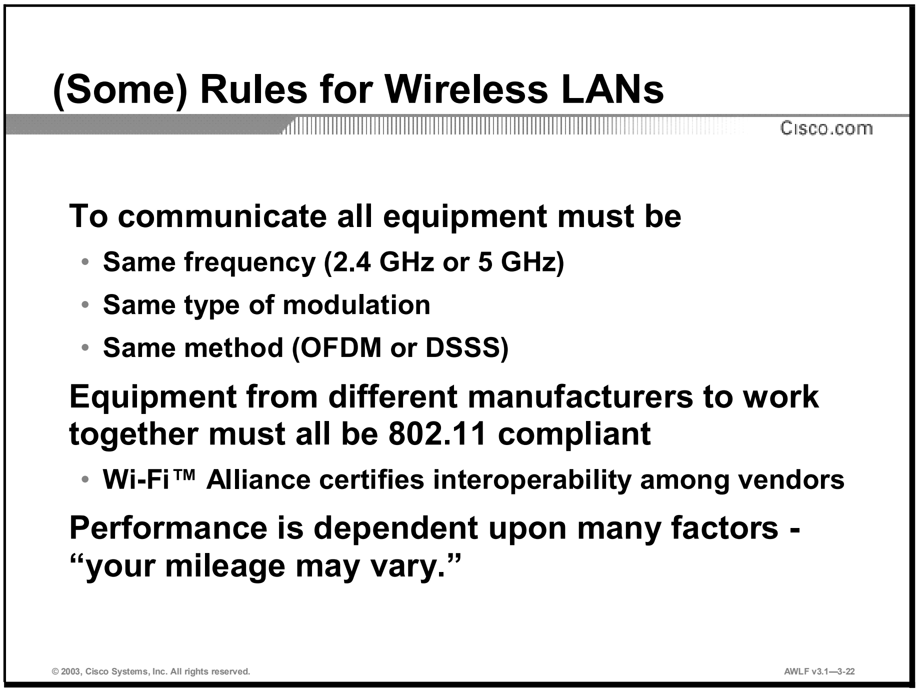
Consider this:

- 1 person in the 11 Mbps, 1 person in 5.5 Mbps, 1 person in 2 Mbps range
- All sending 5 packets the same size

Workstation 'A' packet #1
Workstation 'B'packet #1
Workstation 'C' packet #1
Second packet for everyone
2 Mbps
2 Mbps
11 Mbps
5.5 Mbps
11 Mbps
5.5 Mbps
Second packet for Workstation A
2 Mbps
2 Mbps
2 Mbps
2 Mbps
Workstation 'A' packet #1
Workstation 'B'packet #1
Workstation 'C' packet #1

AWLF v3.1—3-21

If everyone is operating at the same data rate, they will all take the same amount of time to send the same size packets. If some people are operating at higher speeds, then they will transmit the packet faster, which will allow the RF to be available more quickly for the next person waiting to transmit. For this reason, multi-rate systems will allow faster performance for all users, even those operating at lower speeds.



(Some) Rules for Wireless LANs

To communicate all equipment must be

- **Same frequency (2.4 GHz or 5 GHz)**
- **Same type of modulation**
- **Same method (OFDM or DSSS)**

Equipment from different manufacturers to work together must all be 802.11 compliant

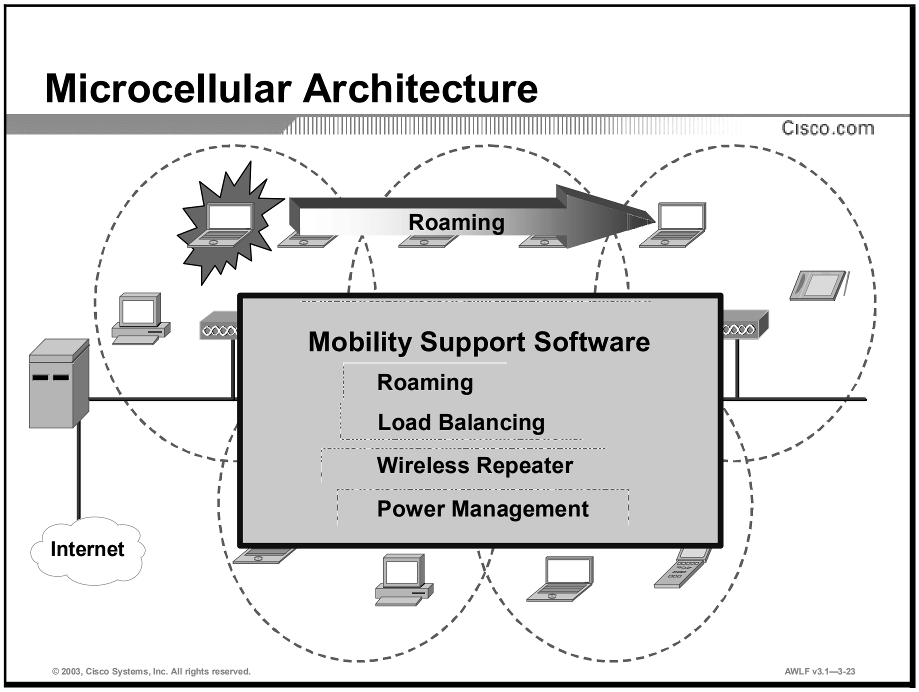
- **Wi-Fi™ Alliance certifies interoperability among vendors**

Performance is dependent upon many factors - “your mileage may vary.”

AWLF v3.1—3-22

In a wireless LAN, there are several things to take into account when selecting a new system or adding to an existing system. First, all equipment MUST be the same frequency and modulation type.

With the 802.11 specifications complete, and vendor cooperation taking place in the Wi-Fi™ Alliance, any 802.11 radio should talk to any other 802.11 radio that is Wi-Fi™ certified, provided they follow the same specifications (with 802.11a and with 802.11b). Vendors are working together to ensure that all units will interoperate. (Please note that “vendor” applies only to RF vendors, NOT terminal or computer vendors).



Microcellular Architecture

Cisco.com

Roaming

Mobility Support Software

Roaming

Load Balancing

Wireless Repeater

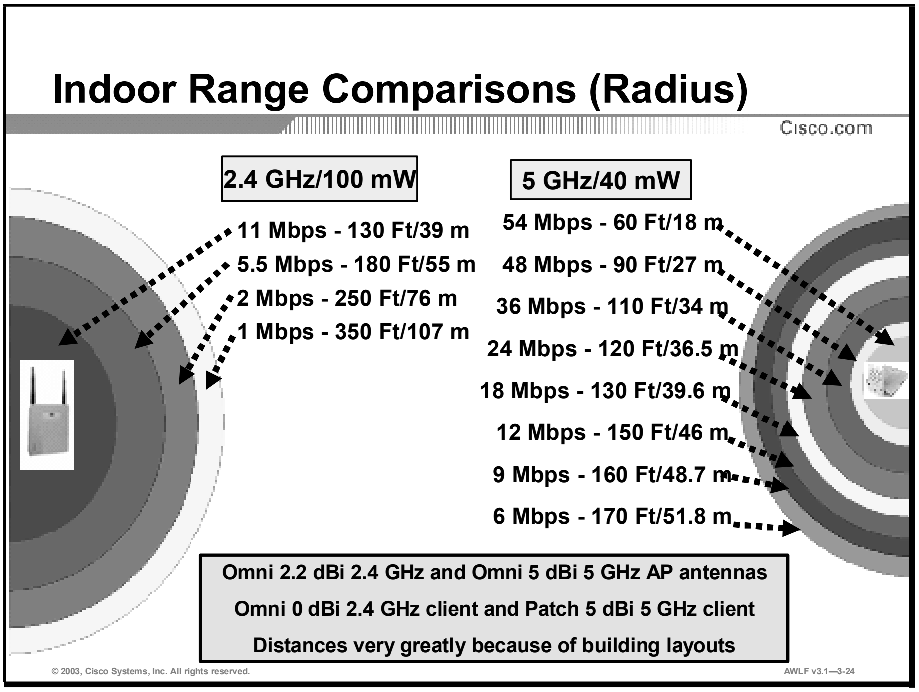
Power Management

AWLF v3.1—3-23

A typical WLAN can include PCs, laptop computers, pen-based computers, printers, and any other device that is normally found on a typical wired network. The WLAN consists of microcells, and the user has the ability to move freely anywhere the RF coverage permits.

Benefits of Cisco Aironet's WLAN products:

- Seamless roaming across access points allows users to maintain connection while moving around the facility.
- Superior power management results in better battery life for portable devices.
- Dynamic load balancing distributes users among access points to increase the throughput of each user.
- Cisco Aironet Access Points have the capability to be a backbone-connected access point or a wireless repeater, via a simple configuration parameter. Wireless repeaters can be used to connect access points throughout a facility without incurring the expense of running wires.
- Fault-tolerant wireless LAN backbones can be provided with the use of access points with overlapping coverage cells.



Indoor Range Comparisons (Radius)

Cisco.com

2.4 GHz/100 mW

11 Mbps - 130 Ft/39 m
5.5 Mbps - 180 Ft/55 m
2 Mbps - 250 Ft/76 m
1 Mbps - 350 Ft/107 m

5 GHz/40 mW

54 Mbps - 60 Ft/18 m
48 Mbps - 90 Ft/27 m
36 Mbps - 110 Ft/34 m
24 Mbps - 120 Ft/36.5 m
18 Mbps - 130 Ft/39.6 m
12 Mbps - 150 Ft/46 m
9 Mbps - 160 Ft/48.7 m
6 Mbps - 170 Ft/51.8 m

Omni 2.2 dBi 2.4 GHz and Omni 5 dBi 5 GHz AP antennas
Omni 0 dBi 2.4 GHz client and Patch 5 dBi 5 GHz client
Distances very greatly because of building layouts

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—3-24

Cisco's 2.4 GHz Radios

Cisco's 2.4 GHz radio delivers 100 mW output and offers a high degree of receive sensitivity delivering competitive range and reliability for in building WLAN applications. Customers however want more power to extend range per access point and increase WLAN reliability. It's important to note that to realize the full capability of range enhancements for the 100 mW radio both the infrastructure device and the client device must have 100 mW capabilities. Otherwise, the least powerful radio will be the determining factor for range/reliability.

2.4 GHz technology uses a 100 mW (+20 dBm) radio. Other supported power levels will include:

- 50 mW
- 30 mW
- 20 mW
- 5 mW
- 1 mW

The receiver has the following sensitivity (@ 10 BER)

- -85 dBm @ 11 Mbps
- -89 dBm @ 5.5 Mbps
- -91 dBm @ 2 Mbps
- -94 dBm @ 1 Mbps

Cisco's 5 GHz Radios

Data from actual tests conducted by Cisco Aironet engineers.

The Radius for 54 Mbps data is shown to vary from 40 feet to 60 feet. The results of measures in standard office spaces. But a cell maybe as small as 25 feet or as large as 100 feet depending on objects in the cell area.

The 5 GHz client has a 20 mW transmit power and the 5 GHz access point has a 40 mW transmit power.

Other available transmit powers on the AP are as follows:20 mW

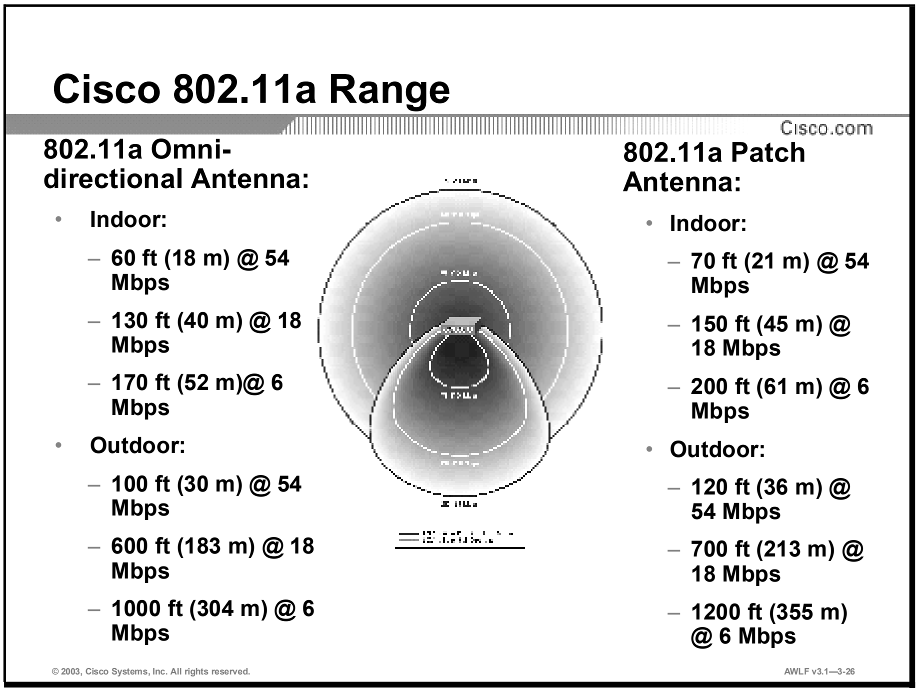
- 10 mW
- 5 mW

Other available transmit powers on the 5 GHz client are as follows:

- 10 mW
- 5 mW

Cisco's 5 GHz receiver sensitivities:

- 6 Mbps: -85 dBm
- 9 Mbps: -84 dBm
- 12 Mbps: -82 dBm
- 18 Mbps: -80 dBm
- 24 Mbps: -77 dBm
- 36 Mbps: -73 dBm
- 48 Mbps: -69 dBm
- 54 Mbps: -68 dBm



Cisco 802.11a Range

Cisco.com

802.11a Omni-directional Antenna:

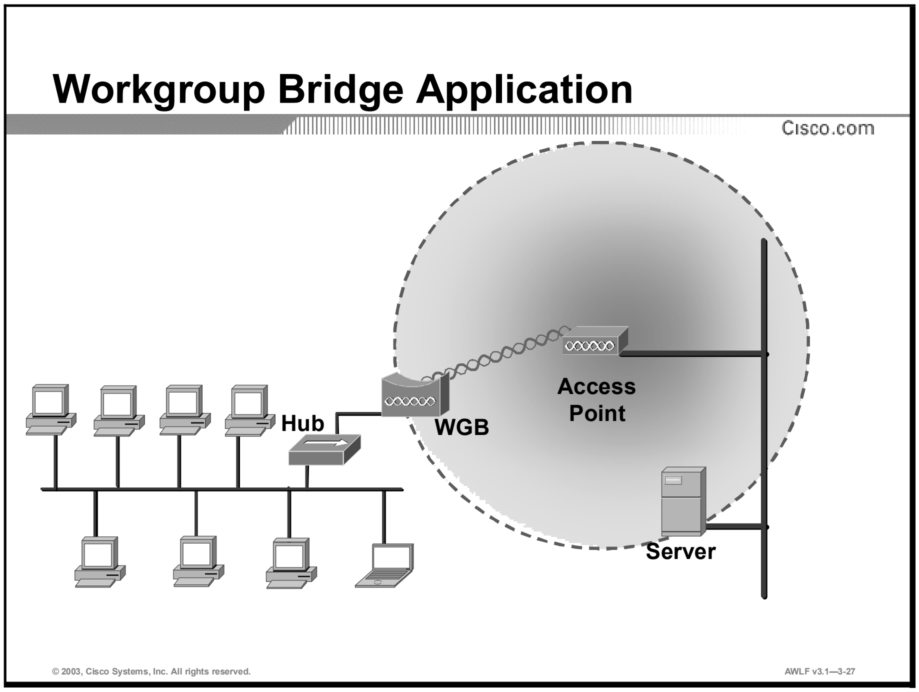
- **Indoor:**
  - **60 ft (18 m) @ 54 Mbps**
  - **130 ft (40 m) @ 18 Mbps**
  - **170 ft (52 m)@ 6 Mbps**
- **Outdoor:**
  - **100 ft (30 m) @ 54 Mbps**
  - **600 ft (183 m) @ 18 Mbps**
  - **1000 ft (304 m) @ 6 Mbps**

802.11a Patch Antenna:

- **Indoor:**
  - **70 ft (21 m) @ 54 Mbps**
  - **150 ft (45 m) @ 18 Mbps**
  - **200 ft (61 m) @ 6 Mbps**
- **Outdoor:**
  - **120 ft (36 m) @ 54 Mbps**
  - **700 ft (213 m) @ 18 Mbps**
  - **1200 ft (355 m) @ 6 Mbps**

AWLF v3.1—3-26

Ranges vary according to application and cell size. Cell size is greatly affected by density of objects. Site surveys are recommended for optimal WLAN operation.



Workgroup Bridge Application

Cisco.com

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—3-27

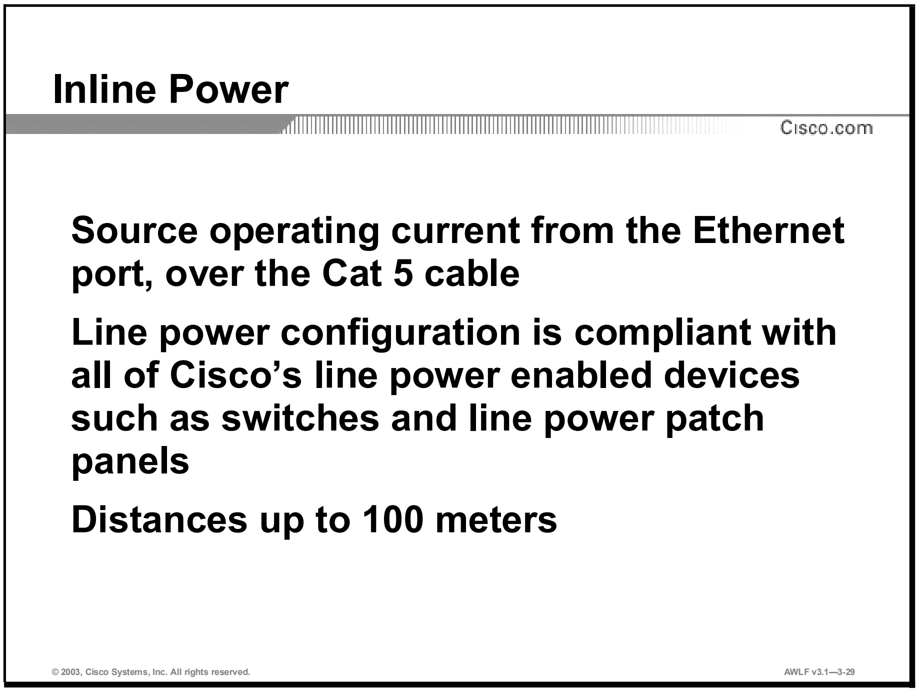
The Cisco Aironet Workgroup Bridge (WGB) product connects to the Ethernet port of a device that does not have a PCI or PCMCIA slot available. It provides a single MAC address connection into an access point, and onto the LAN backbone. It cannot be used in a peer-to-peer mode connection, and must communicate to a Cisco Aironet Access Point or Cisco Aironet Bridge in access point mode. The Cisco Aironet WGB will not operate with other vendors' access points.

Another configuration of the Workgroup Bridge will allow up to 8 wired machines to be attached to the same radio device. It is ideal for connecting remote workgroups to a wired LAN.

In order to use a WGB with multiple MAC addresses, the WGB must be connected to a hub. All users must connect to the hub. The unit will automatically select the first 8 MAC addresses it hears on the Ethernet, or the addresses may be entered manually into a table. These 8 MAC addresses are static.

In the case where there are more than 8 MAC devices on the Ethernet, it will ONLY use the first 8 it heard. All others MAC address packets will not be acknowledged. If a "smart" hub is used, it may take one of the available MAC address entries. This MAC address may be removed from the table manually to allow the eight clients to use the WGB.

Inline Power



Inline Power

Cisco.com

Source operating current from the Ethernet port, over the Cat 5 cable

Line power configuration is compliant with all of Cisco’s line power enabled devices such as switches and line power patch panels

Distances up to 100 meters

© 2003, Cisco Systems, Inc. All rights reserved.

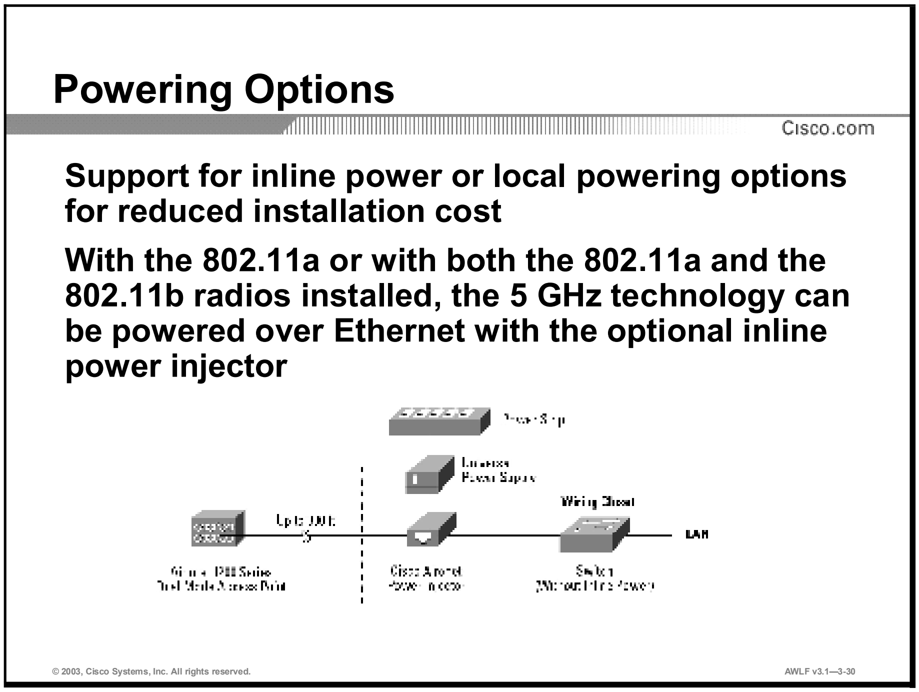
AWLF v3.1—3-29

To decrease the cost and complexity of the installation, the Cisco Aironet 1200 can be powered over an Ethernet cable, eliminating the need to run expensive AC power to remote access point installation locations. Some items to note about Cisco Aironet 1200 Series power options. The Cisco Aironet 1200 Access Point ships with a 110-220V wall transformer (at no extra charge). An optional power injector may be configured (at an additional cost) instead of a power supply. For 802.11a and dual radio 802.11b/802.11a configurations, a power injector is required, line power enabled switches and patch panels do not provide the wattage required for those configurations yet. For 802.11b only configurations, Cisco line power-enabled devices like switches and patch panels may be used instead of power injector. Remember the standard Cat 5 cable requirements still apply (maximum 328 feet or 100 meters).

Inline power further reduces the installation costs, as an electrician is not required. Anyone qualified to run Cat 5 cable could install the cabling required to power Cisco Aironet Access Point.

A Power Injection module is shipped with every 350 Series Access Point. The 350 Series Access Point can ONLY receive power via the RJ-45 port. There is no other means of powering the access point.

Note The new C3550-24PWR inline power switch (15W per port) can supply power for Cisco Aironet 1200 Series dual-mode access point.



Powering Options

Cisco.com

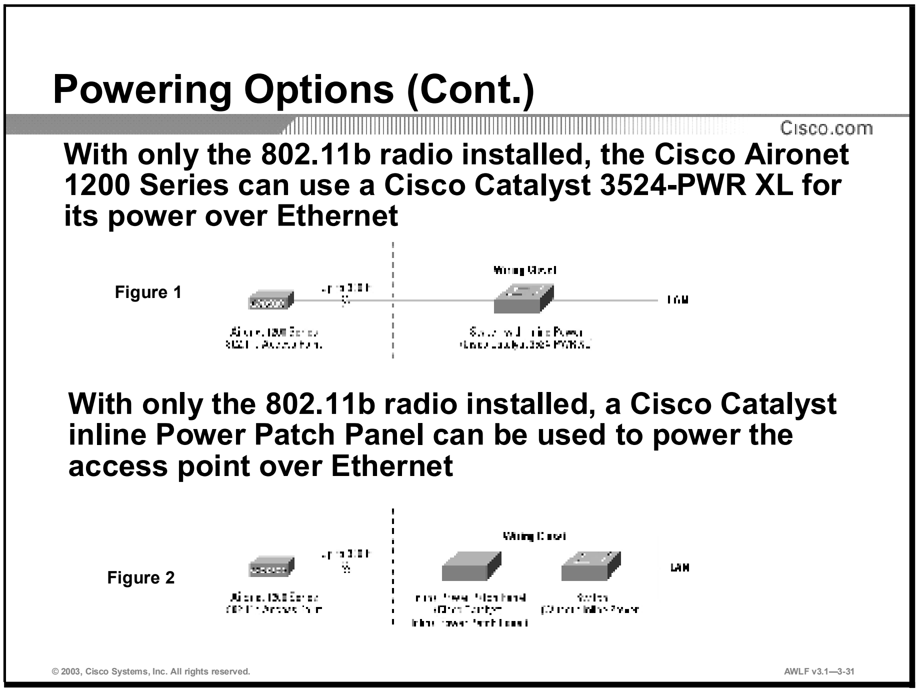
- Support for inline power or local powering options for reduced installation cost
- With the 802.11a or with both the 802.11a and the 802.11b radios installed, the 5 GHz technology can be powered over Ethernet with the optional inline power injector

Power Strip
Universal Power Supply
Wiring Closet
Up to 100 ft
LAN
Aironet 1200 Series Dual Mode Access Point
Cisco Aironet Power Injector
Switch (Without Inline Power)

AWLF v3.1—3-30

Caution Cisco Aironet power injectors are designed for use with 350 series access points and bridges only. Using the power injector with other Ethernet-ready devices can damage the equipment. The operational voltage range for Cisco Aironet 350 Series Access Points and Bridges is 24 to 60 VDC. Higher voltage can damage the equipment.

With the 802.11a, or with both the 802.11a and 802.11b radios installed, the Cisco Aironet 1200 Series can be powered over Ethernet with the optional inline power injector.



Powering Options (Cont.)

Cisco.com

With only the 802.11b radio installed, the Cisco Aironet 1200 Series can use a Cisco Catalyst 3524-PWR XL for its power over Ethernet

Figure 1

With only the 802.11b radio installed, a Cisco Catalyst inline Power Patch Panel can be used to power the access point over Ethernet

Figure 2

AWLF v3.1—3-31

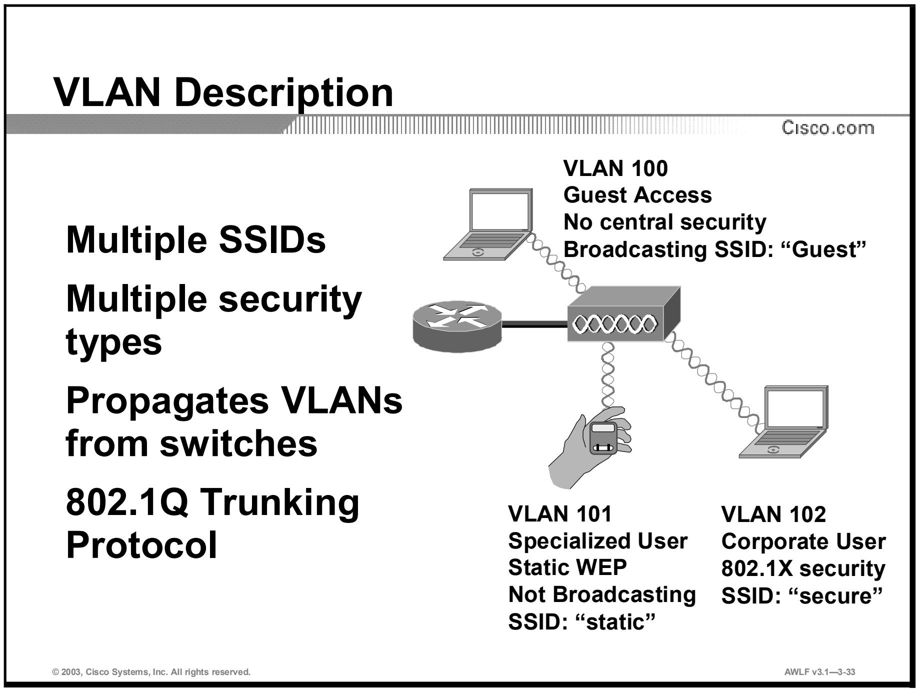
Figure 1

With only the 802.11b radio installed, the Cisco Aironet 1200 can use a Cisco Catalyst 3524-PWR XL for its power over Ethernet.

Figure 2

With only the 802.11b radio installed, a Cisco Catalyst Inline Power Patch Panel can be used to power the access point over Ethernet.

Cisco Aironet Access Point VLAN Feature



VLAN Description

Cisco.com

- Multiple SSIDs
- Multiple security types
- Propagates VLANs from switches
- 802.1Q Trunking Protocol

VLAN 100
Guest Access
No central security
Broadcasting SSID: "Guest"

VLAN 101
Specialized User
Static WEP
Not Broadcasting
SSID: "static"

VLAN 102
Corporate User
802.1X security
SSID: "secure"

AWLF v3.1—3-33

VLAN Feature

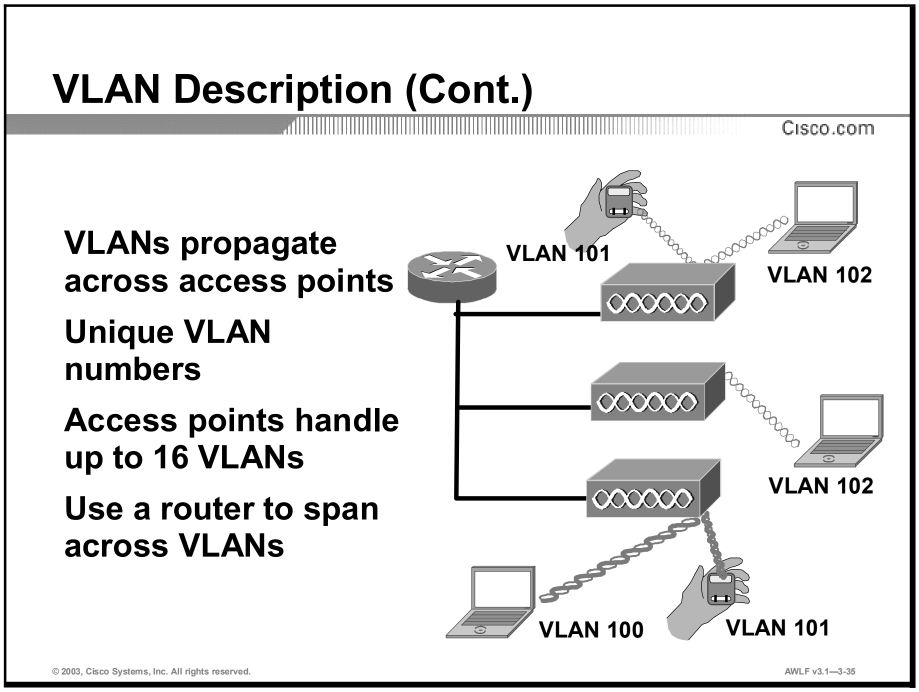
LAN networks are increasingly being divided into workgroups connected via common backbones to form virtual LAN (VLAN) topologies. VLANs enable efficient traffic separation, provide better bandwidth utilization, and alleviate scaling issues by logically segmenting the physical local-area network (LAN) infrastructure into different subnets so that packets are switched only between ports within the same VLAN. When combined with central configuration management support, VLANs facilitate workgroups and client/server additions and changes. Some common reasons why a company might have VLANs:

- **Security** - Separating systems that have sensitive data from the rest of the network decreases the chances that people will gain access to information they are not authorized to see.
- **Departments/Specific job types** - Companies may want VLANs set up for departments that are heavy network users (such as multimedia or engineering), or a VLAN across departments that is dedicated to specific types of employees (such as managers or sales people).
- **Broadcasts/Traffic flow** - Since a principle element of a VLAN is the fact that it does not pass broadcast traffic to nodes that are not part of the VLAN, it automatically reduces broadcasts. **Access lists** (ACL) provide the network administrator with a way to control who sees what network traffic. An access list is a table the network administrator creates that lists which addresses have access to that network.

The following number schemes can be used as an example to different VLANs.

- **VLAN100** allows guest who come into you Enterprise environment to connect directly to the Internet without having access to your Enterprise Servers. Without the VLANs function it would require two access points to provide isolated connectivity for the Guest users and Enterprise users. VLAN100 would be configured with no security and broadcast its SSID. An Access Control List on the Router could also be configured to ensure that traffic with VLAN100 tags go straight out the firewall.
- **VLAN101** allows specialized users (shipping/receiving clerk) to use a barcode scanner with static WEP security since the barcode scanner cannot support dynamic security. VLAN101 would be configured with static WEP security and not to broadcast its SSID.
- **VLAN102** allows Enterprise users to take advantage of 802.1X Extensible Authentication Protocol (EAP-LEAP / EAP-TLS / EAP-PEAP). VLAN102 would be configured to support 802.1X EAP securities.

Note The Cisco Aironet Access Points only supports the 802.1Q Trunking protocol standard. Cisco Switches and Routers support both the pre-standard Inter-Switch Link (ISL) protocol and 802.1Q.



VLAN Description (Cont.)

Cisco.com

- VLANs propagate across access points
- Unique VLAN numbers
- Access points handle up to 16 VLANs
- Use a router to span across VLANs

AWLF v3.1—3-35

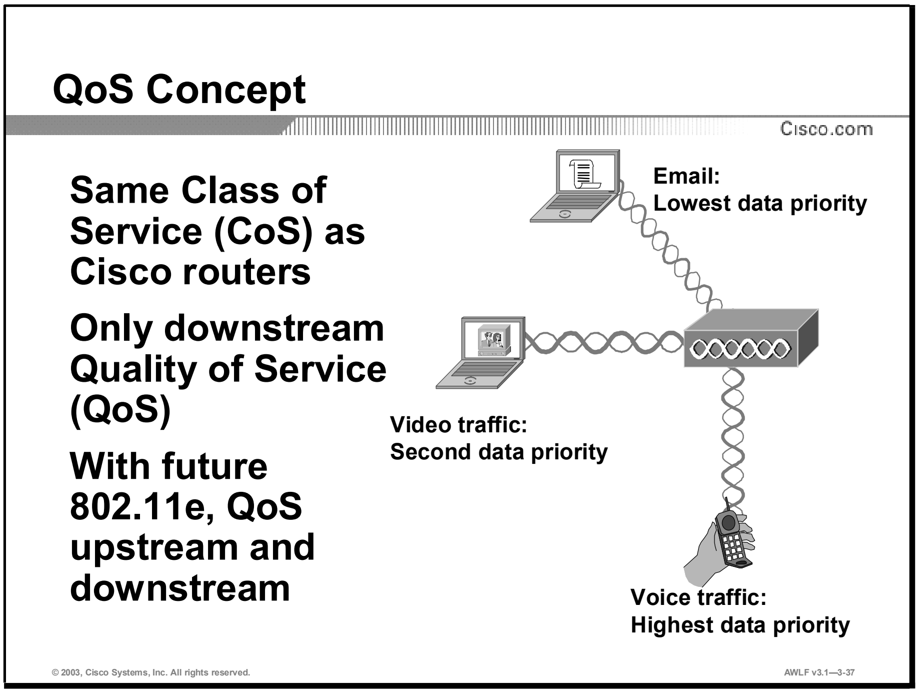
WLAN can now fit nicely into the larger network because VLANs have been enabled on the Access Points. This allows WLAN users to roam from access point to access point maintaining connectivity to the proper VLAN.

In the example above, the barcode scanner user is able to maintain access to the proper VLAN (VLAN101) and communicate to the Router when roaming from access point to access point.

Note Switches will not allow different VLANs to talk to one another. A Router will be needed to allow different VLANs to communicate to each other.

Note The Cisco Aironet Access Points can be configured with 16 different VLANs for system design flexibility.

Cisco Aironet Access Point Quality of Service Feature



QoS Concept

Cisco.com

Same Class of Service (CoS) as Cisco routers

Only downstream Quality of Service (QoS)

With future 802.11e, QoS upstream and downstream

Email:
Lowest data priority

Video traffic:
Second data priority

Voice traffic:
Highest data priority

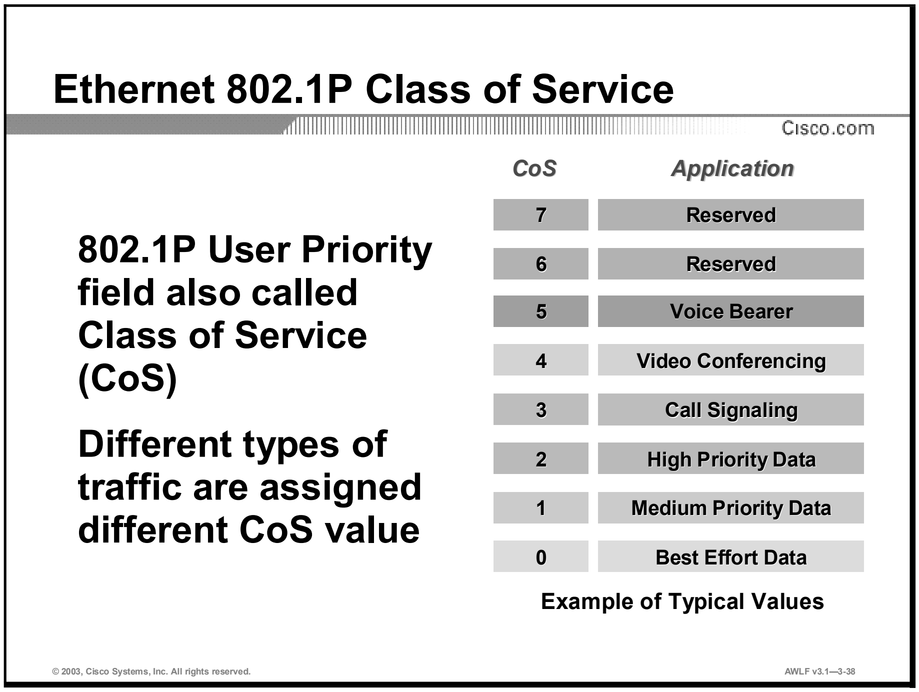
© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—3-37

QoS Feature

Time critical data like voice and video benefit from Quality of Service (QoS) because the QoS feature can be configured to give voice and video higher priority. This allows for smooth voice communication, jitter free video and reliable delivery of E-Mail configured with a lower priority.

Cisco uses the same Class of Service (CoS) used on Cisco Routers. At this time Cisco can only support downstream (Access Point to Client) QoS. When 802.11e QoS becomes ratified, Cisco will also support upstream (Client to Access Point) QoS as well by simply upgrading the firmware.



Ethernet 802.1P Class of Service

Cisco.com

802.1P User Priority field also called Class of Service (CoS)

Different types of traffic are assigned different CoS value

CoS	Application
7	Reserved
6	Reserved
5	Voice Bearer
4	Video Conferencing
3	Call Signaling
2	High Priority Data
1	Medium Priority Data
0	Best Effort Data

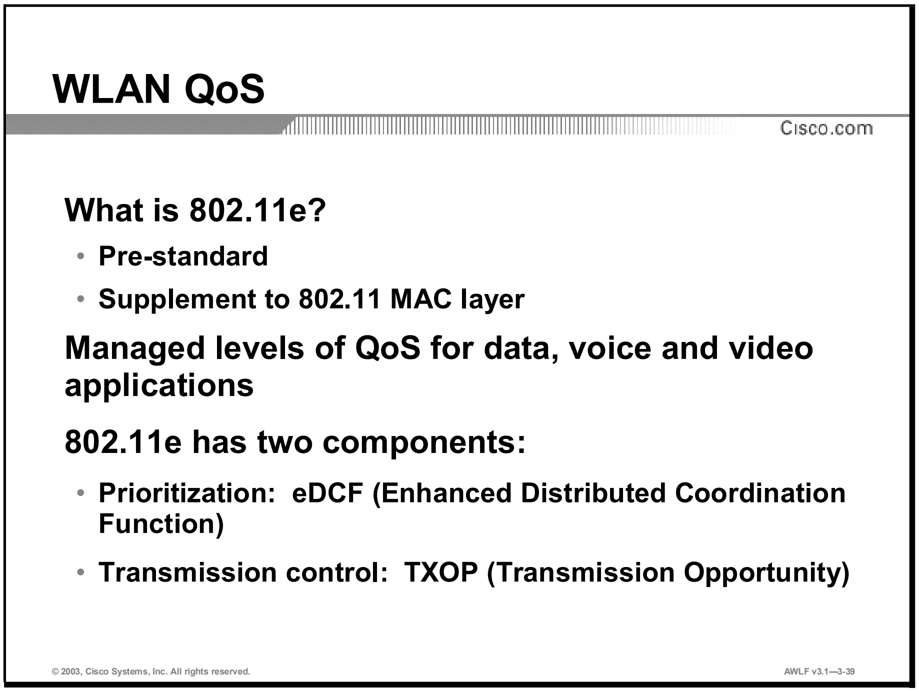
Example of Typical Values

AWLF v3.1—3-38

Class of Service (CoS) uses the 802.1P standard to set priority field to network traffic. There are eight different types of CoS traffic values that can be assigned different network traffic.

Priority Level of these Values:

- 7 and 6 are reserved for network traffic
- 5 is used for most time sensitive traffic. (e.g.) Voice/IP
- 4 is used for the second most time sensitive traffic. (e.g.) Video
- 3 is used for call signaling
- 2 is used for high priority data. (e.g.) Enterprise Application
- 1 is used for medium priority data. (e.g.) Email
- 0 is used for best effort data. (e.g.) Web Browsing



WLAN QoS

What is 802.11e?

- **Pre-standard**
- **Supplement to 802.11 MAC layer**

Managed levels of QoS for data, voice and video applications

802.11e has two components:

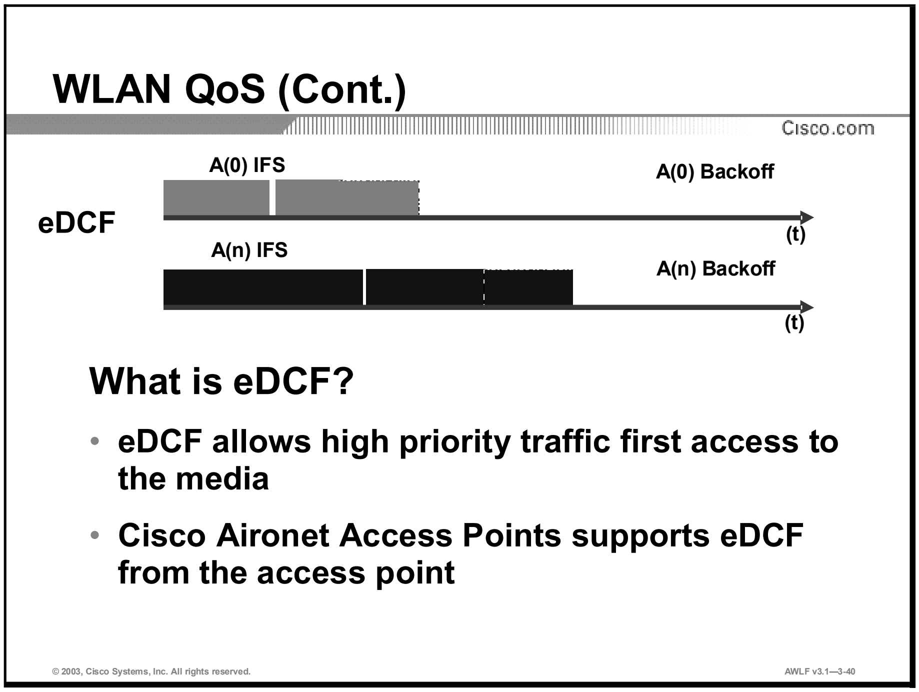
- **Prioritization: eDCF (Enhanced Distributed Coordination Function)**
- **Transmission control: TXOP (Transmission Opportunity)**

AWLF v3.1—3-39

802.11e is supplementary to the MAC layer to provide QoS support for LAN applications. It will apply to 802.11 physical standards a, b and g. The purpose is to provide classes of service with managed levels of QoS for data, voice and video applications.

802.11e has two components:

- Enhanced Distributed Coordination Function (eDCF) which is responsible for prioritization.
- Transmission Opportunity (TXOP) which is responsible for transmission control.



WLAN QoS (Cont.)

What is eDCF?

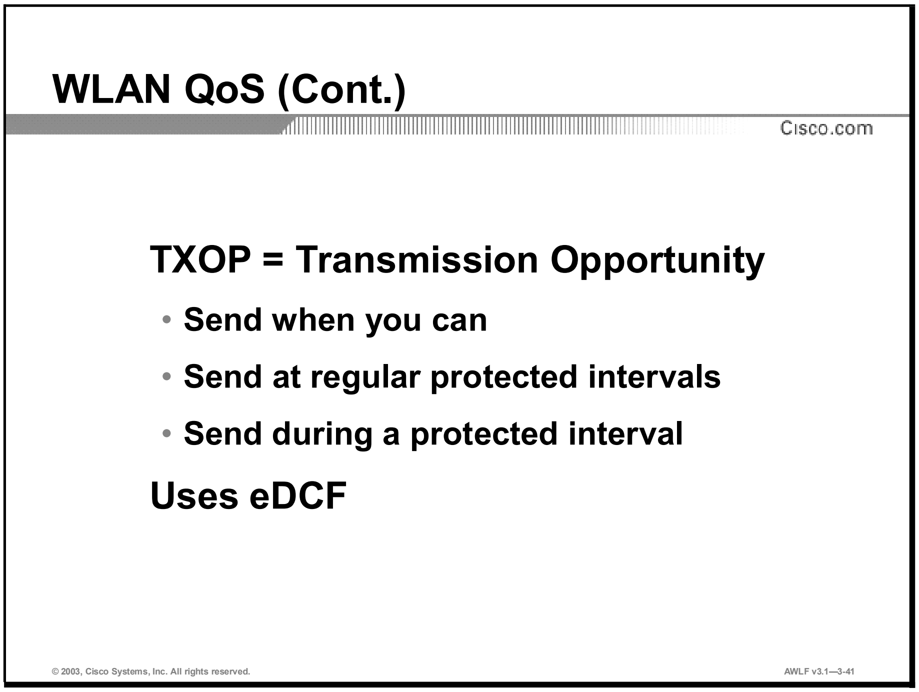
- eDCF allows high priority traffic first access to the media
- Cisco Aironet Access Points supports eDCF from the access point

AWLF v3.1—3-40

There is bound to be network collisions when sharing the WLAN. Clients communicating on the WLAN at the exact same time cause these collisions. This causes both packets to back off for a random period of time before sending the packets again. Collisions cannot be entirely eliminated but keeping them to a minimum will help to preserve your WLAN bandwidth.

To help maintain the bandwidth QoS uses eDCF to allow higher priority traffic first access to the WLAN media. With QoS, instead of backing off for a random period of time they will back of for variable amount of time depending on the packets priority. eDCF allows the higher priority traffic to pass through the access points interfaces before lower priority traffic.

In the example above you we see that A (0) IFS (Inter-Frame Space) has a shorter back off time (e.g.) voice packet. A (n) IFS has a longer back off time (e.g.) email packet.



WLAN QoS (Cont.)

Cisco.com

TXOP = Transmission Opportunity

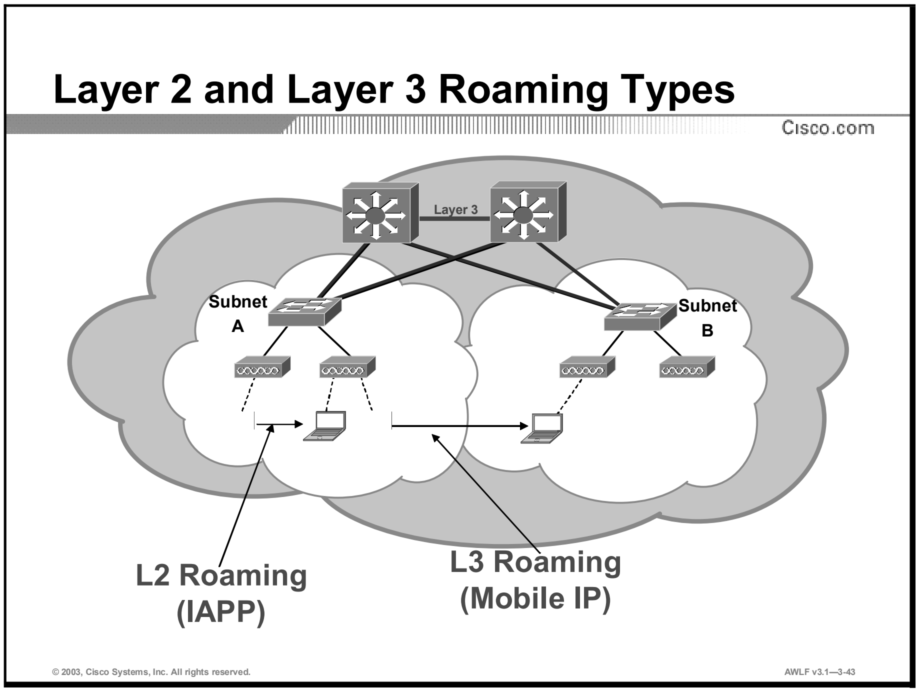
- Send when you can
- Send at regular protected intervals
- Send during a protected interval

Uses eDCF

AWLF v3.1—3-41

TXOP is for environments that have a large amount of WLAN traffic going through the access point. High priority packets will only wait a few second to retransmit and if the traffic volume is still high the high priority packet will continue to resend and resend. TXOP will always reserve a place in line for the high priority packets by reserving the first couple seconds for high priority packets. This will guarantee higher priority packet handling and if there is not a high priority packet in the queue that access point addresses the next packet in line. eDCF is also used to assist the process of handling high priority packets.

Cisco Aironet Access Point Proxy Mobile IP



Layer 2 and Layer 3 Roaming Types

Cisco.com

L2 Roaming (IAPP)

L3 Roaming (Mobile IP)

© 2003, Cisco Systems, Inc. All rights reserved.

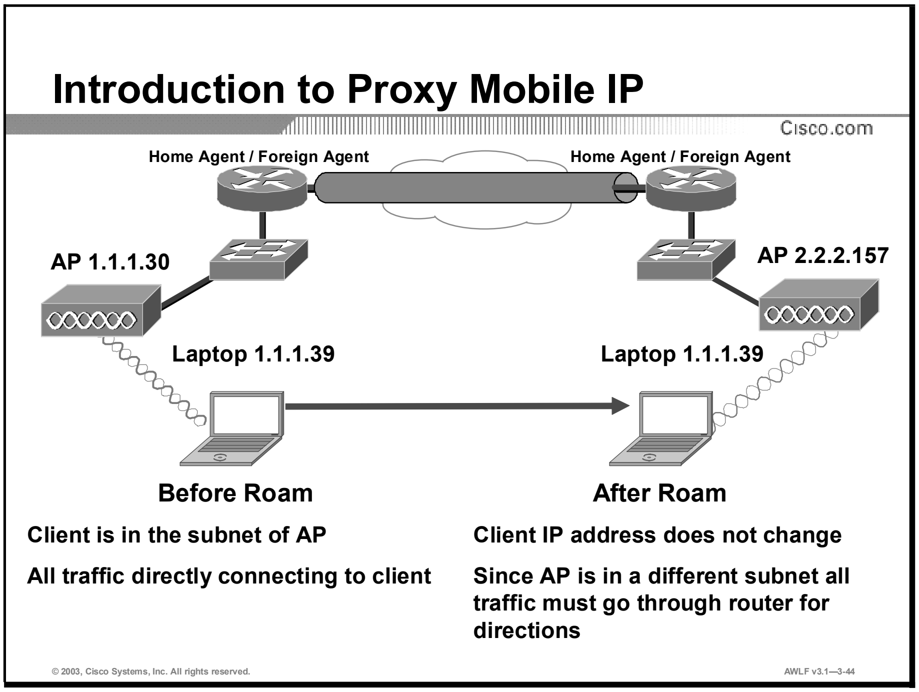
AWLF v3.1—3-43

Proxy Mobile IP

- **Layer 2 Roaming / IAPP:** Network designers working with mobile users in a large area will often find it necessary to deploy more than one access point. The 802.11 standard does not define how access points track moving users or how to negotiate a handoff from one access point to the next, a process referred to as *roaming*. Several companies have introduced proprietary Inter-Access Point Protocols (IAPP) to support roaming. IAPP accomplishes roaming within a subnet; however, it does not address how the wireless system tracks users moving from one subnet to another when the same session must be maintained, as in the case of voice calls.

- **Layer 3 Roaming / Mobile IP:** Where wireless is being deployed across multiple subnets, there are options to achieve seamless roaming. Wireless client adapters can contain proprietary client IP stacks that understand mobility and allow roaming between subnets.
  - All mobile users on the network must have this software installed.

- **Layer 3 Roaming / Proxy Mobile IP:** Another option is to have the wireless infrastructure contain the intelligence to perform the task. Cisco’s Proxy Mobile IP delivers this functionality. Mobile IP is designed for use in even the most complex network environments. As the wireless station leaves one area and enters the next, the new access point informs the home agent of its new association and the home agent is responsible for maintaining a record of this association location.



Introduction to Proxy Mobile IP

Before Roam

Client is in the subnet of AP

All traffic directly connecting to client

After Roam

Client IP address does not change

Since AP is in a different subnet all traffic must go through router for directions

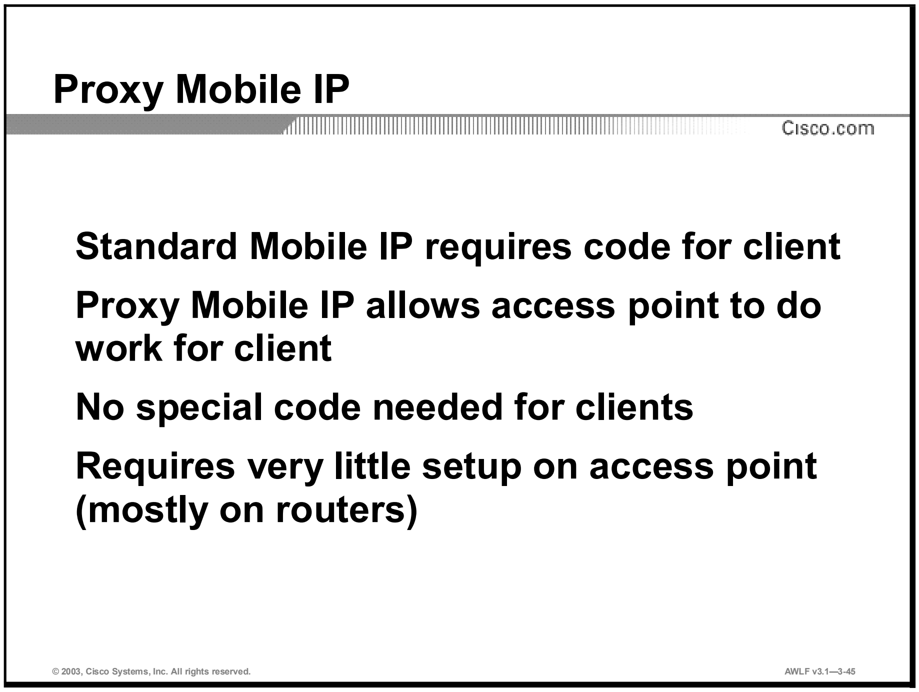
AWLF v3.1—3-44

Before Roaming

The laptop (1.1.1.39) and the access point (1.1.1.30) belong to the same subnet and all network traffic between the access point and the laptop is directed by the switch.

After Roaming

The laptop (1.1.1.39) and the access point (2.2.2.157) belong to different subnets and all network traffic between the access point and the laptop now requires assistance from the router. The router must have firmware on it that supports the Home Agent/Foreign Agent (HA/FA) function. The HA/FA function allows the router to create a tunnel between the two access points on different subnets and manage the whereabouts of roaming clients. So when the access point (1.1.1.30) has data to deliver to the laptop the data is sent through the tunnel to the access point (2.2.2.157) and the data is delivered to the laptop (1.1.1.39).



Proxy Mobile IP

Cisco.com

- Standard Mobile IP requires code for client
- Proxy Mobile IP allows access point to do work for client
- No special code needed for clients
- Requires very little setup on access point (mostly on routers)

© 2003, Cisco Systems, Inc. All rights reserved. AWLF v3.1—3-45

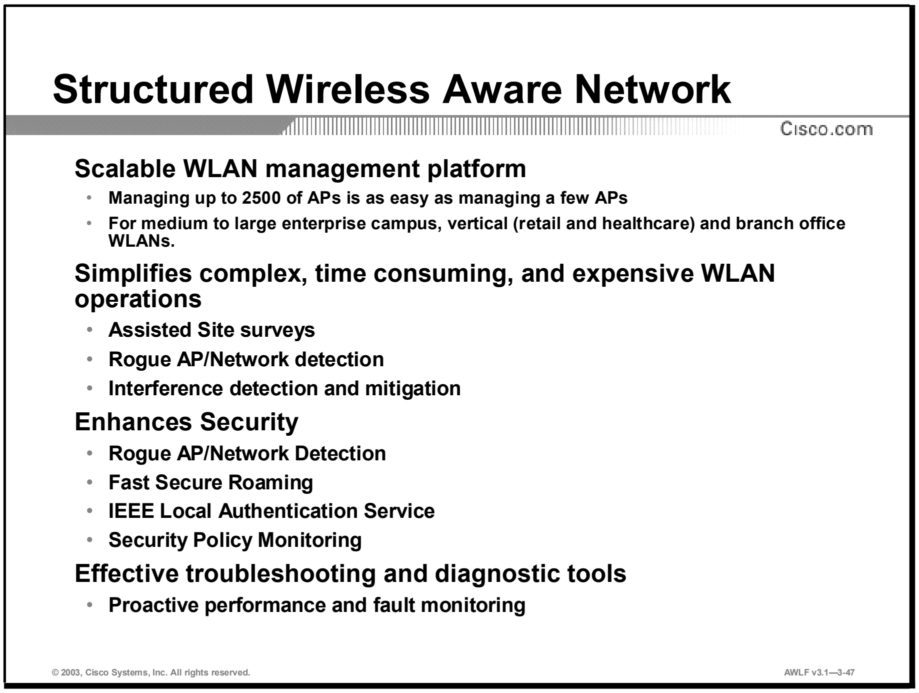
Standard Mobile IP

Standard Mobile IP requires IT personnel to install Mobile IP client software on all clients.

Proxy Mobile IP

Proxy Mobile IP does not require IT personnel to install client software on every client. However it does require firmware to be installed and configured on the Routers to support the Home Agent / Forwarding Agent function. The access points will also need to be configured to support Proxy Mobile IP. Addresses of wireless clients authorized for Mobile IP operation must be entered into Security Association table or access point must have a RADIUS server authorize Security Associations.

Cisco Aironet Structured Wireless Aware Network (SWAN)



Structured Wireless Aware Network

Cisco.com

Scalable WLAN management platform

- Managing up to 2500 of APs is as easy as managing a few APs
- For medium to large enterprise campus, vertical (retail and healthcare) and branch office WLANs.

Simplifies complex, time consuming, and expensive WLAN operations

- Assisted Site surveys
- Rogue AP/Network detection
- Interference detection and mitigation

Enhances Security

- Rogue AP/Network Detection
- Fast Secure Roaming
- IEEE Local Authentication Service
- Security Policy Monitoring

Effective troubleshooting and diagnostic tools

- Proactive performance and fault monitoring

AWLF v3.1—3-47

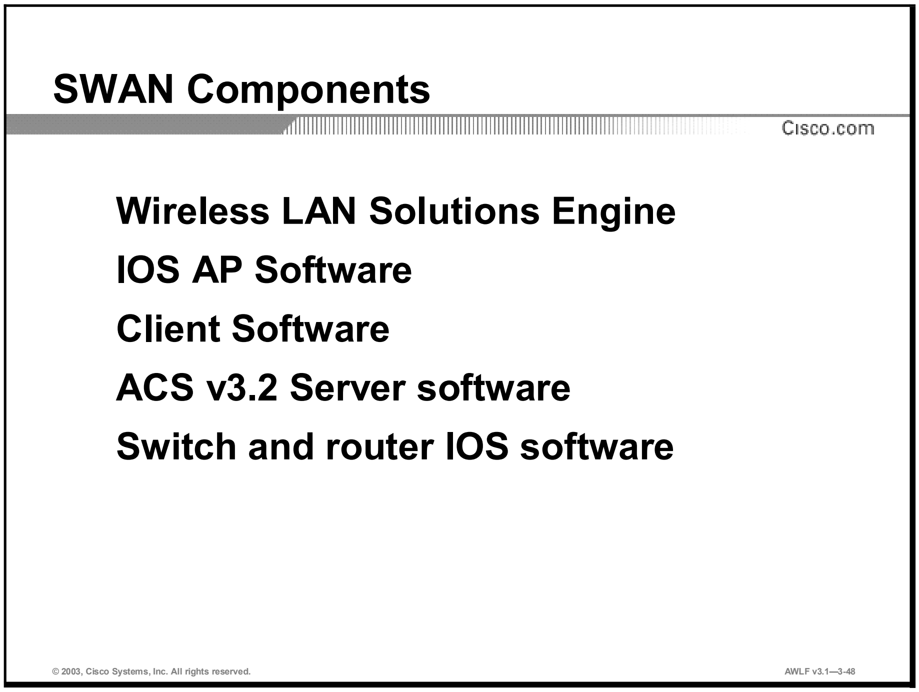
The Cisco Structured Wireless Aware Network (SWAN) is a solution composed of multiple components to enhance the manageability and security of Cisco WLAN’s.

SWAN incorporates “intelligent” AP’s which participate in the management and control aspects of the network, contributing to the scalability of the solution.

Because of this granular scalability, the expense for WLAN management and expansion is minimized.

SWAN incorporates both management and diagnostic aids to consolidate fault detection and correction resources.

SWAN improves alarm, monitoring, and fault correction capabilities of existing WLAN infrastructures by bringing together wired and wireless monitoring to allow fault detection and network adaptability to compensate for interference or outage.



SWAN Components

Cisco.com

Wireless LAN Solutions Engine

IOS AP Software

Client Software

ACS v3.2 Server software

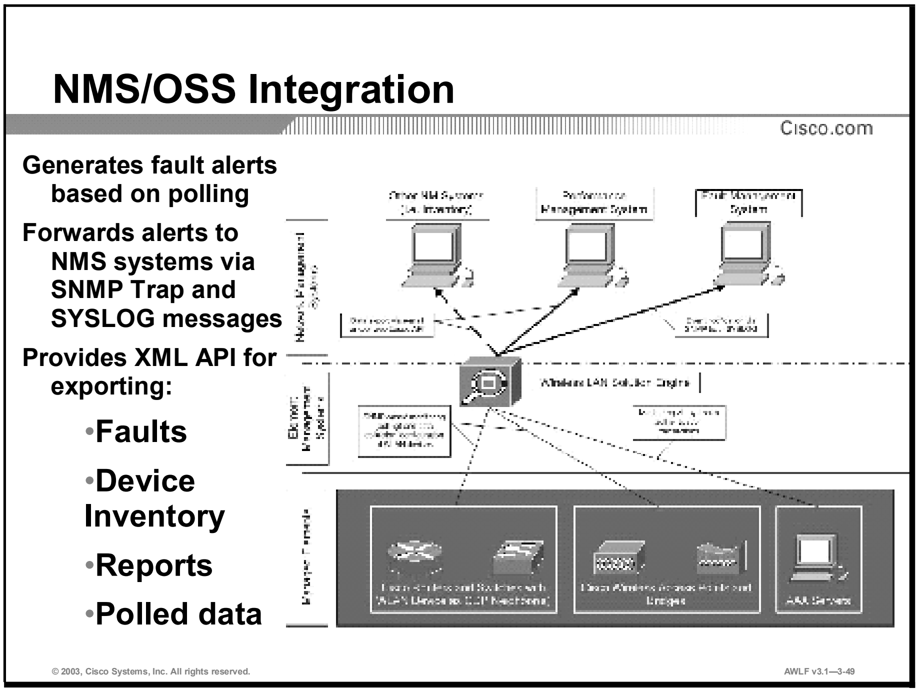
Switch and router IOS software

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—3-48

Components of the SWAN solution include the following:

- Wireless LAN Solution Engine (WLSE) provides configuration, fault/performance monitoring, and NMS integration to aid in managing WLAN networks. In addition, WLSE provides the processing resource to provide the site survey and rogue AP detection/location functions of SWAN.
- IOS AP Software provides Wireless Domain Service, which is critical to SWAN functionality. Wireless Domain Service allows Fast Secure roaming by 802.1X authenticating each AP in a “wireless domain” prior to the clients roaming between the AP’s. This permits the AP’s to securely share keying information, thus permitting the clients to obtain keys without re-authenticating to the RADIUS server. WDS function will also permit the collection and aggregation of Radio Monitoring information from clients and AP’s for submission to the WLSE These functions will become available on select Cisco Router and Switch platforms in early 2004.
- Software in the Cisco Aironet client (and Cisco Compatible Extensions clients) provides Radio Monitoring function—whereby the client devices report on AP’s detected over RF & report to WLSE via WDS to aid in interference and rogue AP detection.
- ACS version 3.2 software provides the RADIUS authentication resource for client and infrastructure devices which participate in the WDS/Fast secure roaming operation.



NMS/OSS Integration

Cisco.com

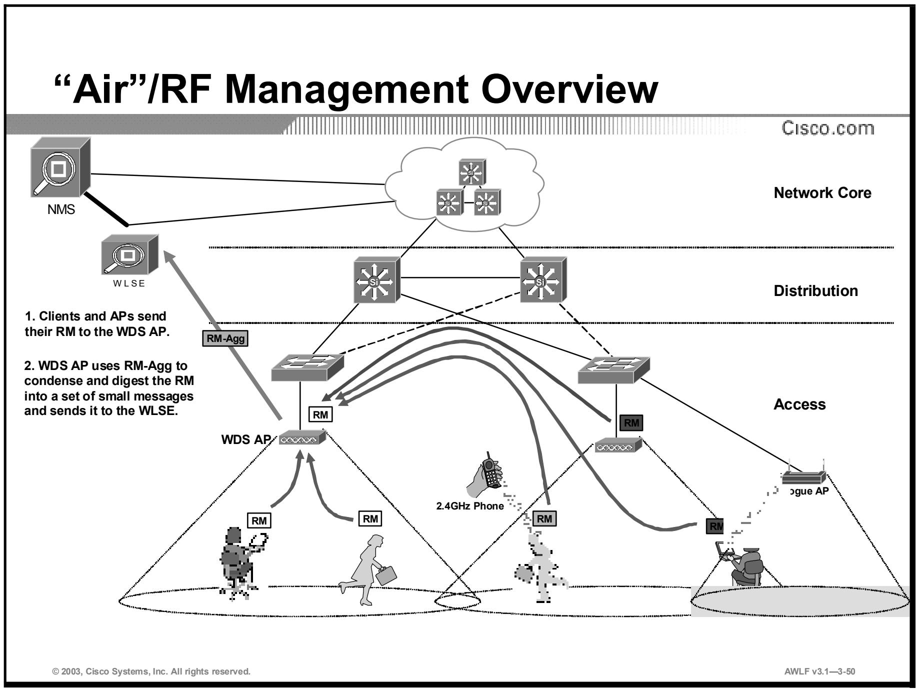
- Generates fault alerts based on polling
- Forwards alerts to NMS systems via SNMP Trap and SYSLOG messages
- Provides XML API for exporting:
  - •Faults
  - •Device Inventory
  - •Reports
  - •Polled data

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—3-49

The Network Management functions of the SWAN/ CiscoWorks WLSE solution provide the capability to extend all features of the wired network to the 802.11 wireless infrastructure, including management and fault monitoring. The following are the specific functions of SWAN provide integration with an Enterprise Network Management system.

- Integration with existing network management infrastructure (SOAP/XML interface, Simple Network Management Protocol (SNMP) traps and Syslog messages)
- Integration with CiscoWorks LMS
- Configuration archival/ monitoring of wireless device configuration templates
- Distribution of firmware/ firmware checking for WLAN infrastructure devices



“Air”/RF Management Overview

1. Clients and APs send their RM to the WDS AP.

2. WDS AP uses RM-Agg to condense and digest the RM into a set of small messages and sends it to the WLSE.

AWLF v3.1—3-50

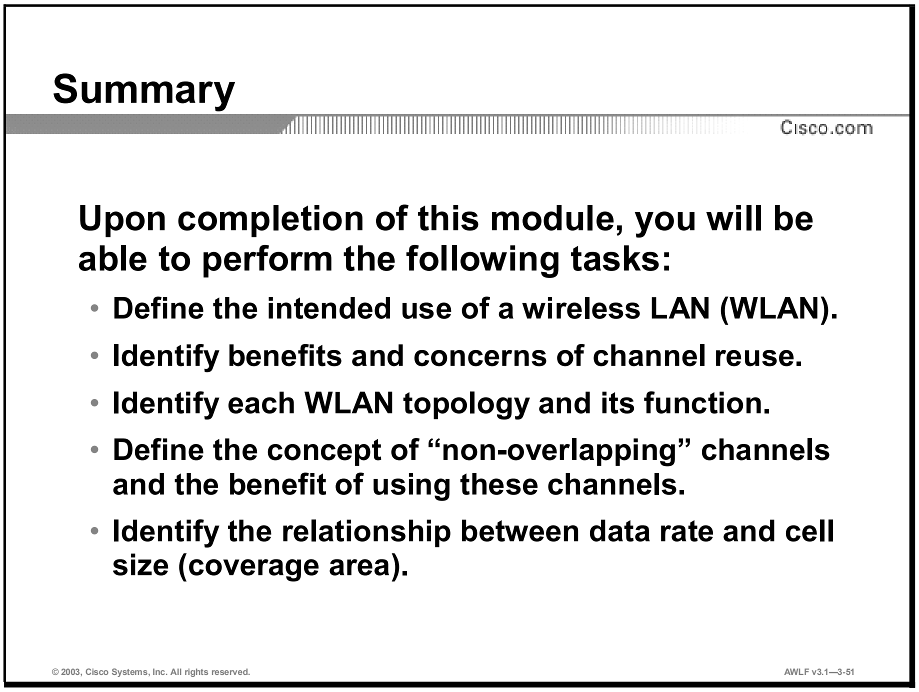
With the Cisco Structured Wireless-Aware Network, Cisco clients and Cisco Compatible clients detect and report on obscure and potentially dangerous rogue access point deployments using client assisted rogue access point detection.

Since WLAN clients can potentially move through a large physical area, the addition of client-assisted rogue access point scanning and monitoring into the framework greatly increases the RF coverage area. Client air management provides 10 to 20 times more RF measurement data than access point RF measurements alone. This extends RF monitoring to areas most likely to contain rogue access points and allows for more accurate rogue access point detection.

All data captured from the access points and client devices is compiled by WDS and sent to the CiscoWorks WLSE. The CiscoWorks WLSE processes these received samples, calling out those that indicate the presence of rogue access points in the CiscoWorks WLSE 2.5 Location Manager and CiscoWorks WLSE 2.0 Fault Summary.

Summary

This section summarized the concepts you learned in this module.



Summary

Cisco.com

Upon completion of this module, you will be able to perform the following tasks:

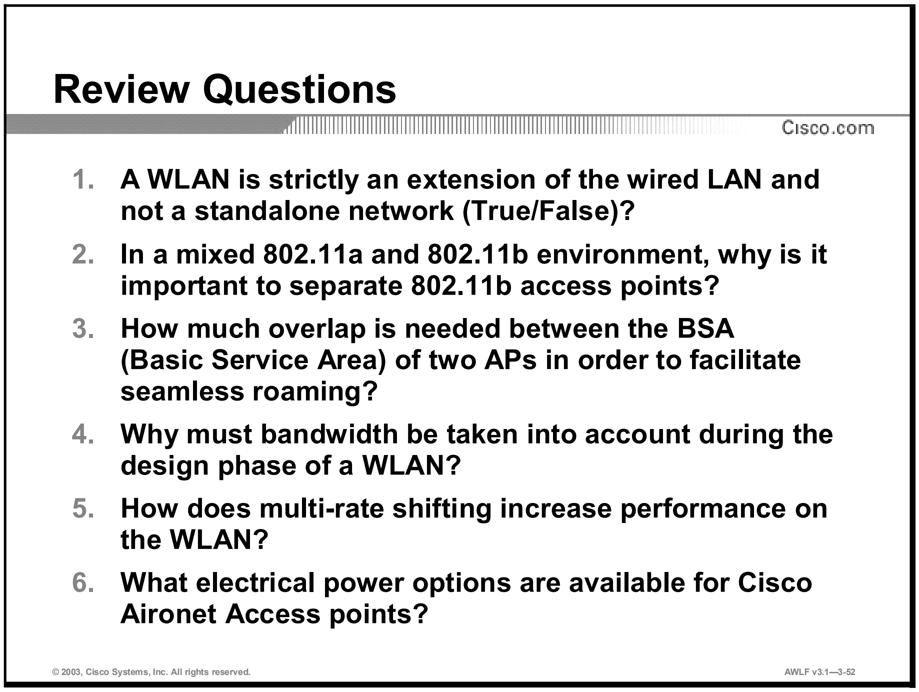
- **Define the intended use of a wireless LAN (WLAN).**
- **Identify benefits and concerns of channel reuse.**
- **Identify each WLAN topology and its function.**
- **Define the concept of “non-overlapping” channels and the benefit of using these channels.**
- **Identify the relationship between data rate and cell size (coverage area).**

© 2003, Cisco Systems, Inc. All rights reserved. AWLF v3.1—3-51

Upon completion of this module, you will be able to perform the following tasks:

- Define the intended use of a wireless LAN (WLAN).
- Identify benefits and concerns of channel reuse.
- Identify each WLAN topology and its function.
- Define the concept of “non-overlapping” channels and the benefit of using these channels.
- Identify the relationship between data rate and cell size (coverage area).

Review Questions



Review Questions

Cisco.com

1. A WLAN is strictly an extension of the wired LAN and not a standalone network (True/False)?
2. In a mixed 802.11a and 802.11b environment, why is it important to separate 802.11b access points?
3. How much overlap is needed between the BSA (Basic Service Area) of two APs in order to facilitate seamless roaming?
4. Why must bandwidth be taken into account during the design phase of a WLAN?
5. How does multi-rate shifting increase performance on the WLAN?
6. What electrical power options are available for Cisco Aironet Access points?

AWLF v3.1—3-52

Answer these review questions.

Module 4

Wireless Bridging

Overview

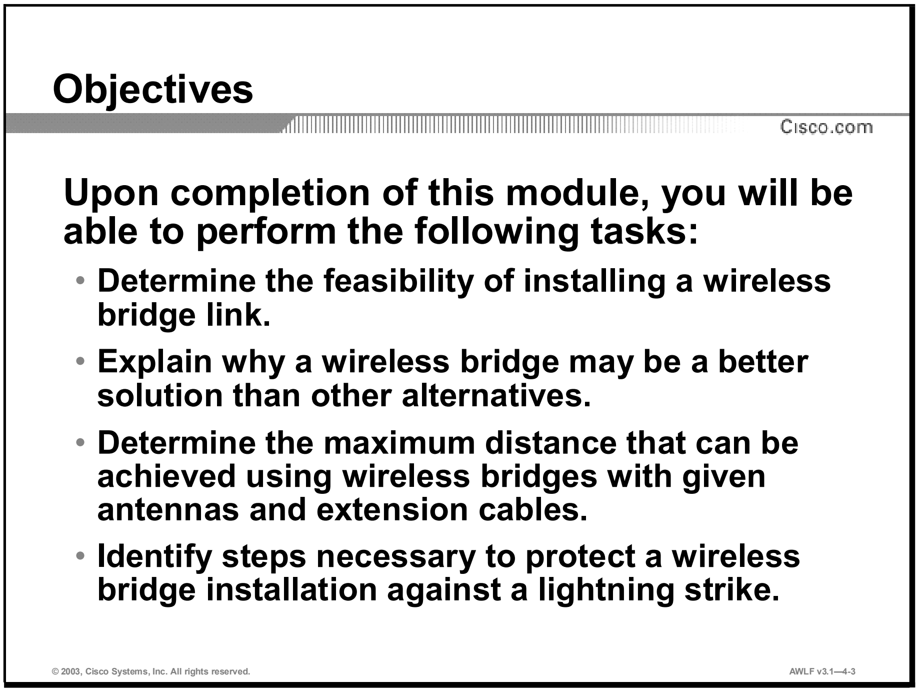
This module explores the concept of using a wireless device to create a layer-2 bridge.

It includes the following topics:

- Objectives
- Wireless Bridge Alternatives
- Role in Radio Network
- Installation Considerations
- Path Loss Considerations
- Common Questions and Misconceptions
- Summary
- Review Questions

Objectives

This section lists the module's objectives.



Objectives

Cisco.com

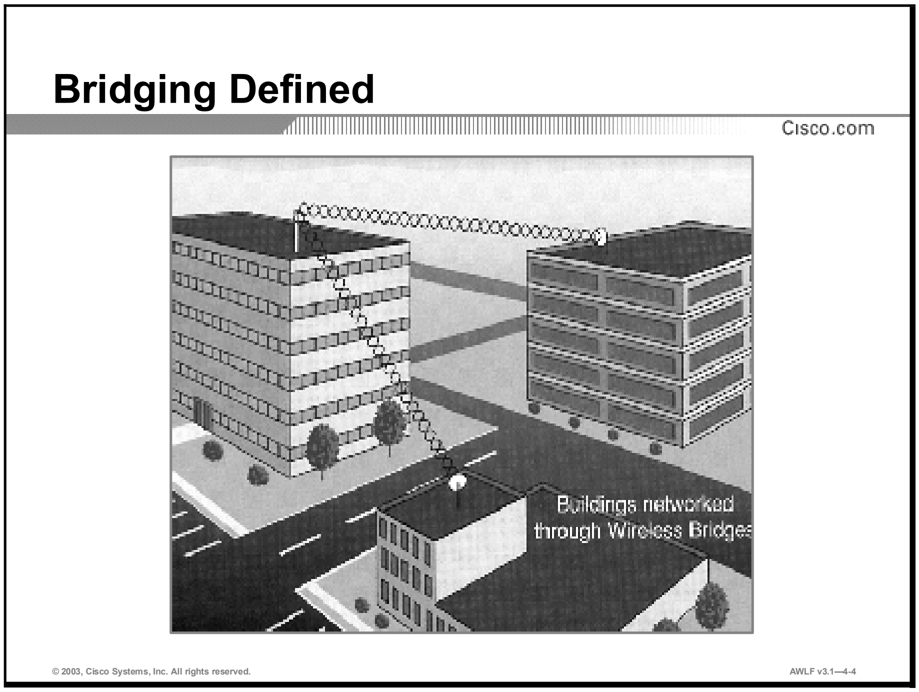
Upon completion of this module, you will be able to perform the following tasks:

- **Determine the feasibility of installing a wireless bridge link.**
- **Explain why a wireless bridge may be a better solution than other alternatives.**
- **Determine the maximum distance that can be achieved using wireless bridges with given antennas and extension cables.**
- **Identify steps necessary to protect a wireless bridge installation against a lightning strike.**

AWLF v3.1—4-3

Upon completion of this module, you will be able to perform the following tasks:

- Determine the feasibility of installing a wireless bridge link.
- Explain why a wireless bridge may be a better solution than other alternatives.
- Determine the maximum distance that can be achieved using wireless bridges with given antennas and extension cables.
- Identify steps necessary to protect a wireless bridge installation against a lightning strike.



Bridging Defined

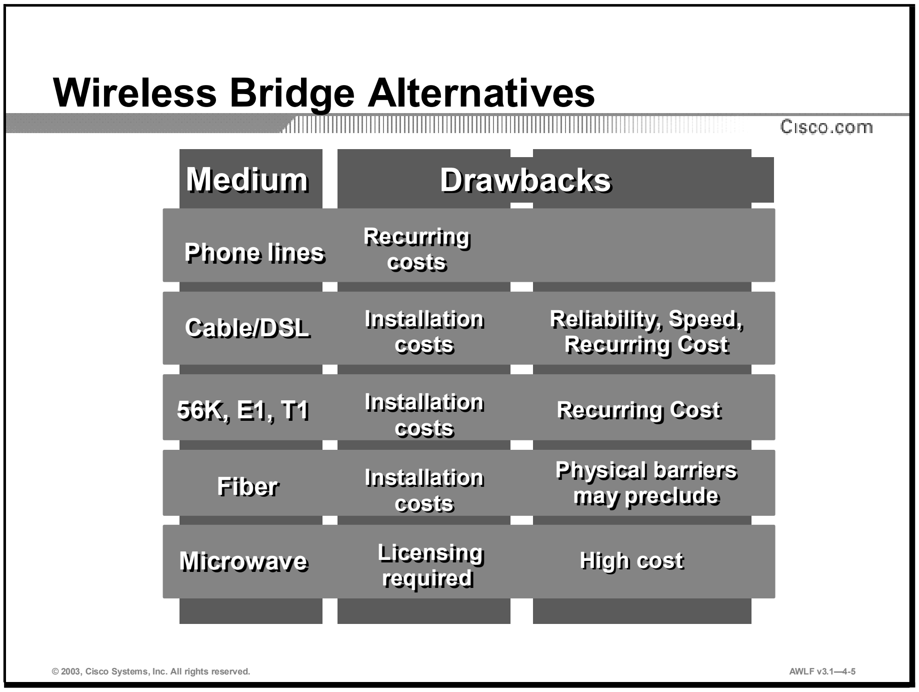
Cisco.com

AWLF v3.1—4-4

Bridges are used to connect two or more wired LAN's, usually located within separate buildings, to create one large LAN. A Cisco Aironet 350 Series bridge can act as an access point in some applications by communicating with clients at the remote sites. This is accomplished with the Cisco Workgroup Bridge, PC Card and PCI products. The Cisco Aironet 1400 Series Bridge is used for bridging purposes only. It does not communicate with clients.

Cisco Aironet® bridges operate at the MAC address layer (Data Link Layer), which means they have no routing capabilities. A router must be put in place if IP subnetting is needed within the network.

Wireless Bridge Alternatives



Wireless Bridge Alternatives

Cisco.com

Medium	Drawbacks	
Phone lines	Recurring costs	
Cable/DSL	Installation costs	Reliability, Speed, Recurring Cost
56K, E1, T1	Installation costs	Recurring Cost
Fiber	Installation costs	Physical barriers may preclude
Microwave	Licensing required	High cost

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—4-5

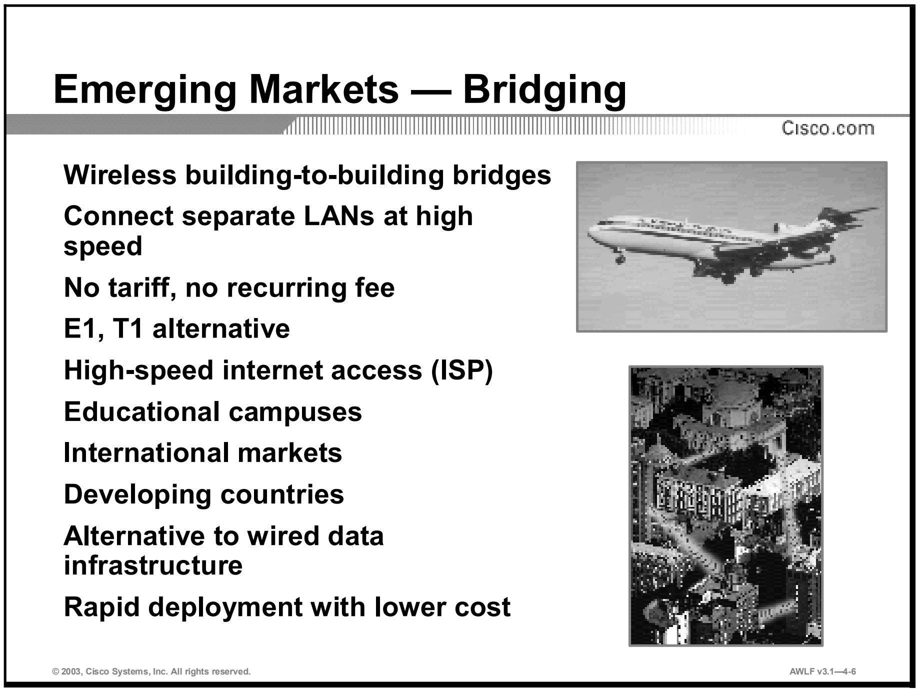
Cisco Aironet Bridges offer many advantages over other more costly alternative connections. Some alternatives include T1 lines, cabling, and microwave connections.

A T-1 line typically costs between $200 to over $1,000 per month. For a site with four buildings, that could cost anywhere from $10,000 to $36,000 per year. If such sites were connected via Cisco Aironet Bridges the payback for the hardware costs incurred could actually be realized in less than a single year.

In some cases where T-I is not available, or the buildings are located on the same property, an underground cable could be put in place. Trenching today can cost over $100/foot, depending upon the task. To connect three buildings located 1000 feet apart from each other, the cost could exceed $200,000.

Another popular option for smaller businesses may be a cable/DSL modem. This solution sometimes offers faster download speeds, but slower upload speeds. Reliability is often an issue. Users are often forced to “share” connections with other nearby businesses, sometimes causing a sacrifice in speed.

Microwave is a solution for some sites where distance is close, reliability is not critical, and money is not an issue. With microwave, an FCC license is required. The cost of the equipment is typically over $10,000 per site, not including installation items. In the event of heavy fog, rain or snow, performance is questionable. Multipoint connections are usually not possible.



Emerging Markets — Bridging

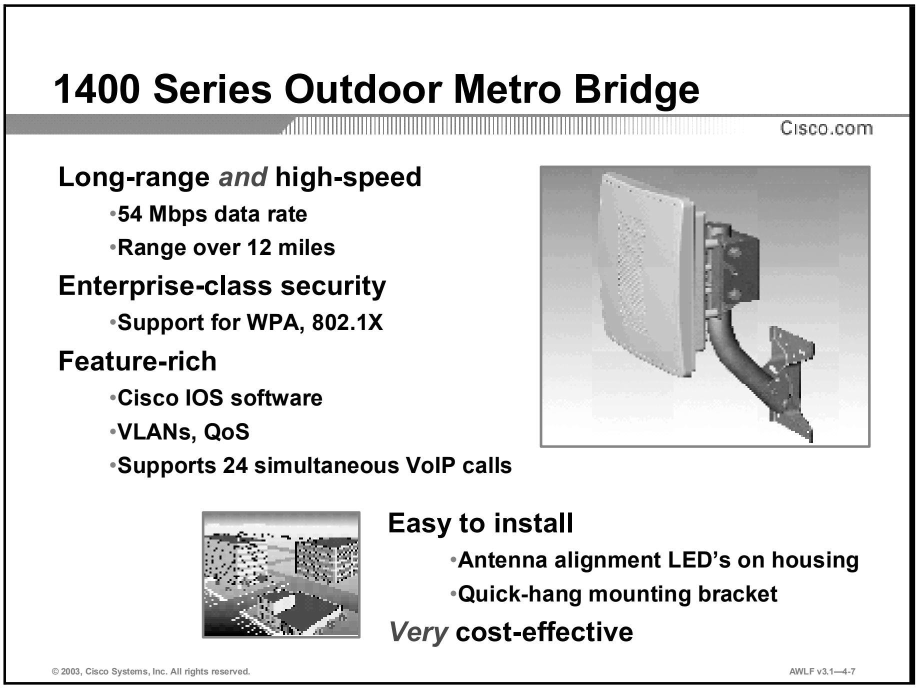
Cisco.com

- Wireless building-to-building bridges
- Connect separate LANs at high speed
- No tariff, no recurring fee
- E1, T1 alternative
- High-speed internet access (ISP)
- Educational campuses
- International markets
- Developing countries
- Alternative to wired data infrastructure
- Rapid deployment with lower cost

© 2003, Cisco Systems, Inc. All rights reserved. AWLF v3.1—4-6

Bridging has quickly become one of the most popular uses of wireless networks. This is in part due to the ease of installation and setup. But it is also due to the variety of emerging markets where WLAN bridging can be applied. Some of these markets include:

- Campus environments, such as hospitals, schools, universities, and corporations
- Areas where geography may exclude other solutions
- Temporary network installations
- Internet Service Providers
- Backup of alternative connections
- Developing countries, where alternative solutions may not be available
- International markets



1400 Series Outdoor Metro Bridge

Cisco.com

Long-range *and* high-speed

- **54 Mbps data rate**
- **Range over 12 miles**

Enterprise-class security

- **Support for WPA, 802.1X**

Feature-rich

- **Cisco IOS software**
- **VLANs, QoS**
- **Supports 24 simultaneous VoIP calls**

Easy to install

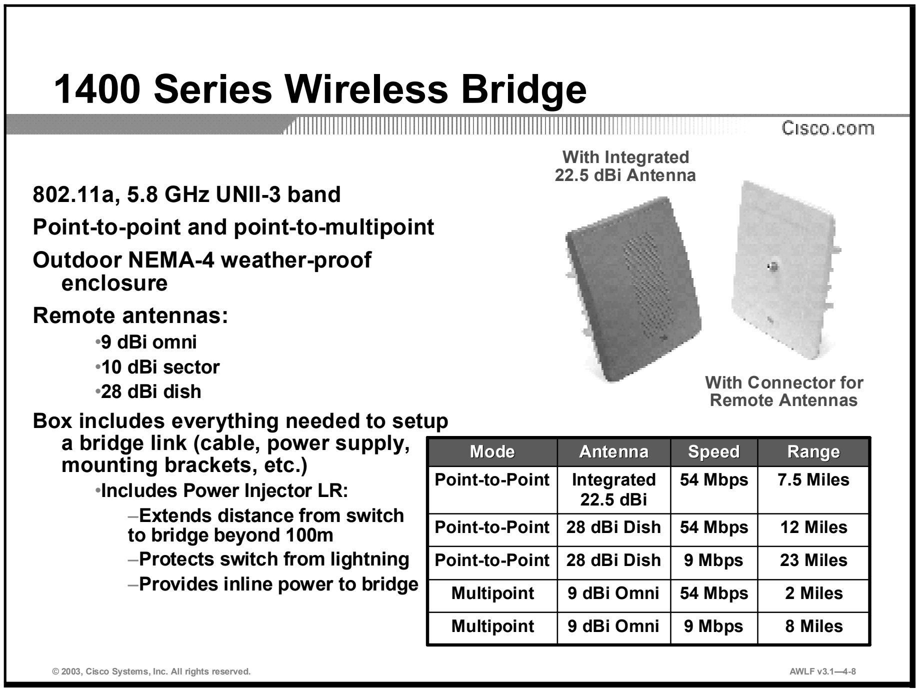
- **Antenna alignment LED's on housing**
- **Quick-hang mounting bracket**

***Very* cost-effective**

AWLF v3.1—4-7

The Cisco Aironet® 1400 Series Wireless Bridge provides a high-performance and feature-rich solution for connecting multiple LANs in a metropolitan area. Designed to be a cost-effective alternative to leased lines, it is engineered specifically for harsh outdoor environments, yet also works well in indoor deployments. The Cisco Aironet 1400 Series Wireless Bridge is the premier high-speed, high-performance outdoor bridging solution for line-of-sight applications, providing features such as:

- Support for both point-to-point or point-to-multipoint configurations
- Industry leading range and throughput, supporting data rates up to 54 Mbps
- Enhanced security mechanisms based on 802.11 standards
- Ruggedized enclosure optimized for harsh outdoor environments with extended operating temperature range
- Integrated or optional external antennas for flexibility in deployment
- Designed specifically for ease-of-installation and operation



1400 Series Wireless Bridge

Cisco.com

- 802.11a, 5.8 GHz UNII-3 band
- Point-to-point and point-to-multipoint
- Outdoor NEMA-4 weather-proof enclosure
- Remote antennas:
  - 9 dBi omni
  - 10 dBi sector
  - 28 dBi dish
- Box includes everything needed to setup a bridge link (cable, power supply, mounting brackets, etc.)
  - Includes Power Injector LR:
    - Extends distance from switch to bridge beyond 100m
    - Protects switch from lightning
    - Provides inline power to bridge

With Integrated 22.5 dBi Antenna

With Connector for Remote Antennas

Mode	Antenna	Speed	Range
Point-to-Point	Integrated 22.5 dBi	54 Mbps	7.5 Miles
Point-to-Point	28 dBi Dish	54 Mbps	12 Miles
Point-to-Point	28 dBi Dish	9 Mbps	23 Miles
Multipoint	9 dBi Omni	54 Mbps	2 Miles
Multipoint	9 dBi Omni	9 Mbps	8 Miles

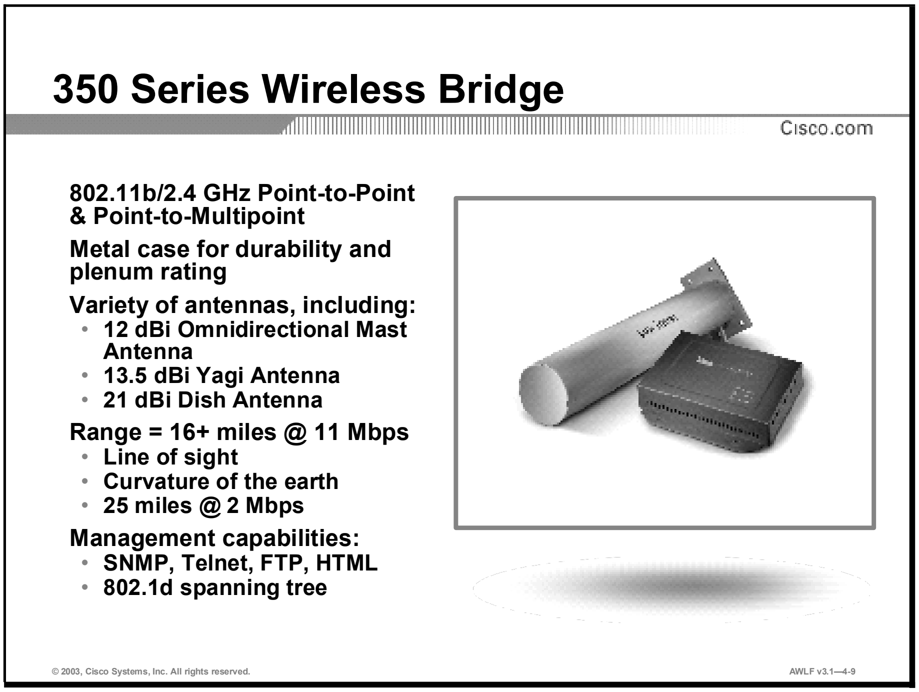
AWLF v3.1—4-8

Operating in the unlicensed 5.8 GHz band, the Cisco Aironet 1400 Series Wireless Bridge sets a new standard for performance, combining powerful 250 mW radios, industry-leading receive sensitivity, installation tools to assist in bridge placement, delay spread capabilities, and a choice of integrated or connectorized high gain antennas, Cisco provides a complete solution for a wide variety of fixed wireless applications.

Data rates of 54 Mbps can be enabled for point-to-point links up to 7.5 miles, and for point-to-multipoint links up to 2 miles. Aggregate throughput can be obtained in excess of 28 Mbps. Also, by using higher gain antennas or lower data rates, ranges in excess of 20 miles point-to-point can be covered.

Rapid deployment and redeployment can be achieved with no reliance upon telecommunications providers nor a lengthy license or trenching process. The Cisco Aironet 1400 Series Wireless Bridge allows placement in an outdoor environment without the use of an expensive additional National Electrical Manufacturers Association (NEMA) enclosure. Further flexibility is achieved by enabling point-to-point or point-to-multipoint networks with a single product line. The mounting bracket has been designed to allow installation on poles, walls, and roofs, while also providing a mechanism for choosing the desired polarization. The Cisco Aironet 1400 Series Wireless Bridge offers an outdoor wireless bridging solution in two product SKUs. The captured antenna version features an integrated radio and high-gain integrated antenna for user installations of point-to-point links and the non-root nodes of point-to-multipoint networks. The connectorized version provides professional installers with an N-Type connector that allows the deployment of the root nodes of point-to-multipoint networks with omni-directional or sector antennas, or of high gain dish antennas for longer links. The external antenna options are:

- 9.0 dBi vertically polarized omni antenna
- 9.5 dBi sector antenna with support for vertical or horizontal linear polarization
- 28.0 dBi dish antenna with support for vertical or horizontal linear polarization



350 Series Wireless Bridge

802.11b/2.4 GHz Point-to-Point & Point-to-Multipoint

Metal case for durability and plenum rating

Variety of antennas, including:

- **12 dBi Omnidirectional Mast Antenna**
- **13.5 dBi Yagi Antenna**
- **21 dBi Dish Antenna**

Range = 16+ miles @ 11 Mbps

- **Line of sight**
- **Curvature of the earth**
- **25 miles @ 2 Mbps**

Management capabilities:

- **SNMP, Telnet, FTP, HTML**
- **802.1d spanning tree**

AWLF v3.1—4-9

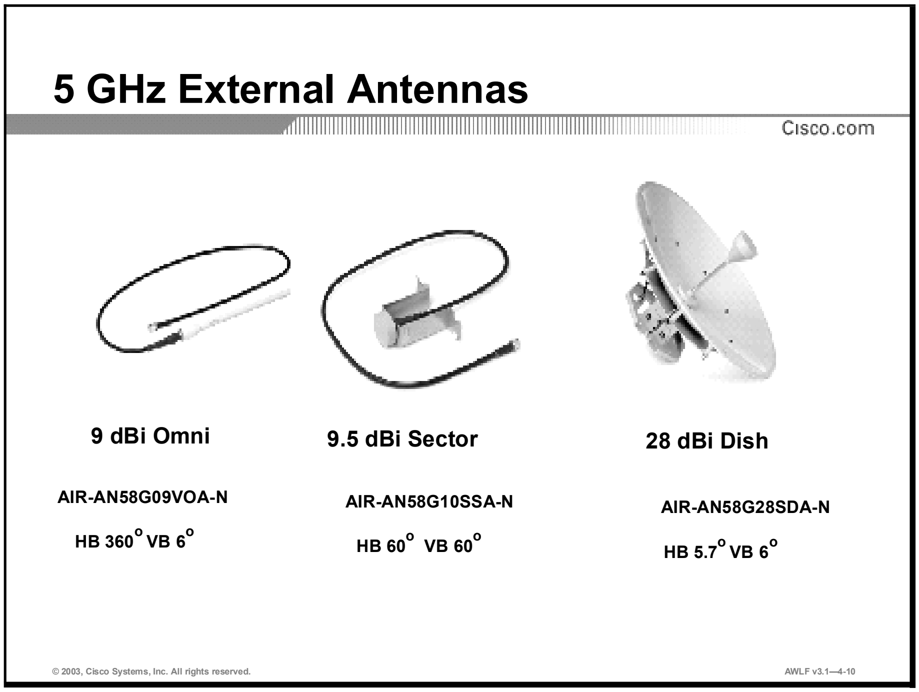
Cisco Aironet 350 Series Wireless Bridges enable high-speed building-to-building links of up to 25 miles (40 km) in FCC regulated areas, or 6.5 miles (10.5 km) in Europe. Delivering throughput several times greater than T1/E1 lines at a fraction of the cost, wireless bridges are ideal for data-intensive, line-of-sight applications, such as connecting hard-to-wire sites, campus settings, satellite offices, and temporary networks. They can be configured for point-to-point or point-to-multi-point applications, allowing two or more sites to connect into a single LAN and/or share a single high-speed Internet connection.

Some of the outstanding features include:

- 802.1D Spanning Tree capabilities
- Full SNMP capability
- FTP
- Bootstrap Protocol (BOOTP) and Telnet capabilities
- Flexibility of configuration with non-volatile Flash ROM
- Inline power
- Same security options available on the Cisco Aironet 350 Series Access Point

The Cisco Aironet 350 Series Bridge is also UL 2043 certified, and designed to achieve plenum rating as defined by various municipal fire codes.

Perhaps the most outstanding feature is the price. The Cisco bridge products are priced as one of the lowest in the industry, while still maintaining highest possible performance.



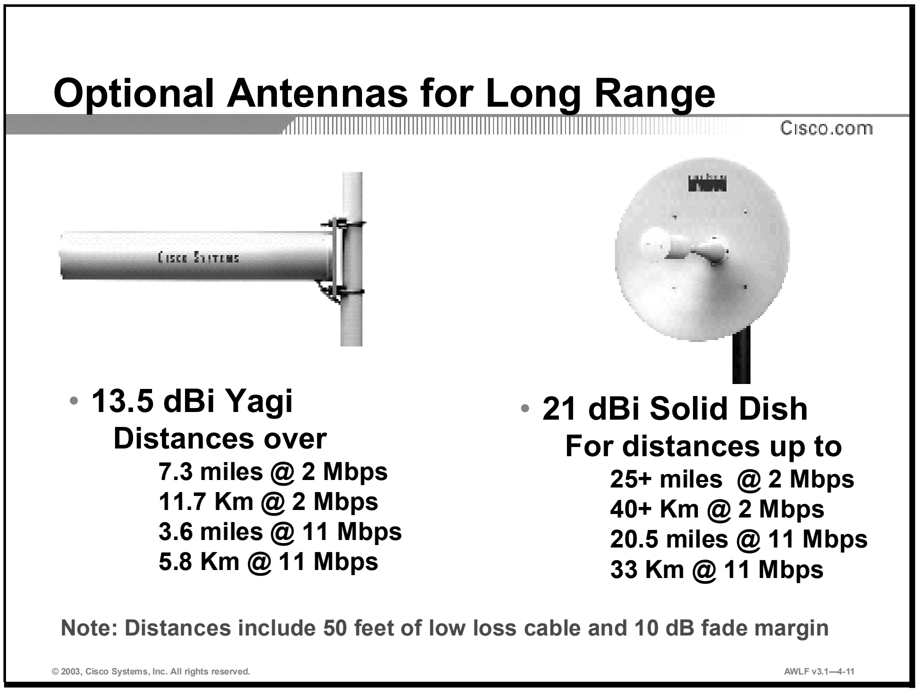
5 GHz External Antennas

9 dBi Omni	9.5 dBi Sector	28 dBi Dish
AIR-AN58G09VOA-N	AIR-AN58G10SSA-N	AIR-AN58G28SDA-N
HB 360° VB 6°	HB 60° VB 60°	HB 5.7° VB 6°

AWLF v3.1—4-10

Cisco Aironet bridge antennas allow for extraordinary transmission distances between two or more buildings. Available in directional configurations for point-to-point transmission and sector or omni-directional configurations for point-to-multipoint implementations, Cisco has a bridge antenna for every application.

The antennas are available with different gain and range capabilities, beam widths, and form factors.



Cisco Systems

Optional Antennas for Long Range

Cisco.com

- 13.5 dBi Yagi
  - Distances over
    - 7.3 miles @ 2 Mbps
    - 11.7 Km @ 2 Mbps
    - 3.6 miles @ 11 Mbps
    - 5.8 Km @ 11 Mbps
- 21 dBi Solid Dish
  - For distances up to
    - 25+ miles @ 2 Mbps
    - 40+ Km @ 2 Mbps
    - 20.5 miles @ 11 Mbps
    - 33 Km @ 11 Mbps

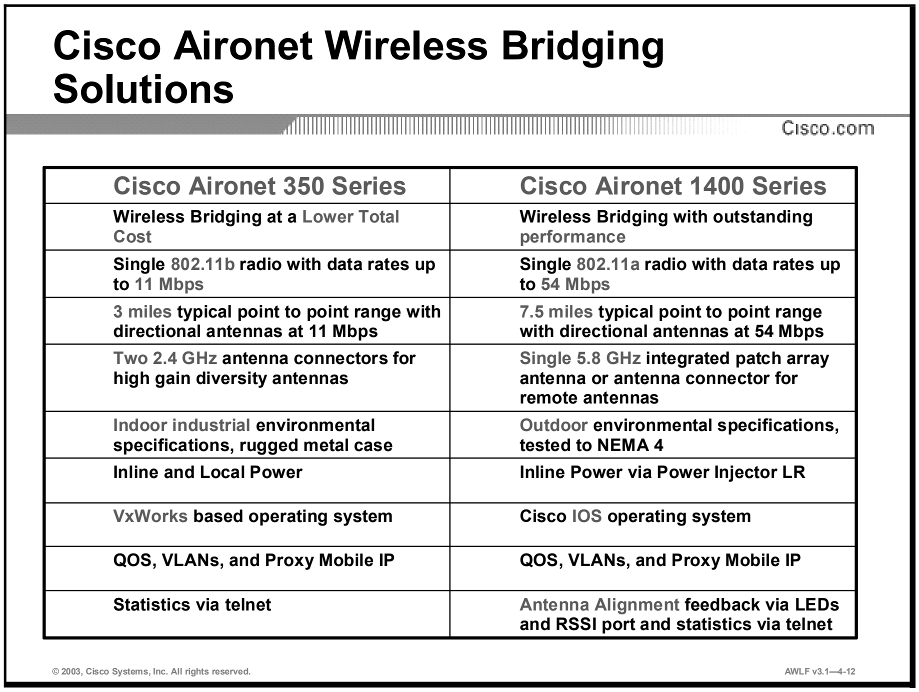
Note: Distances include 50 feet of low loss cable and 10 dB fade margin

AWLF v3.1—4-11

Cisco offers several directional long-range antennas.

- The Yagi is a small (18” x 3”), lightweight (1.5 lbs) antenna that can be used for ranges up to 7.62 miles (11.7 Km) at 2 Mbps, and 3.63 miles (5.8 Km) at 11 Mbps.
- The solid dish is the best structural dish antenna on the market. It will withstand icing and winds over 110 MPH. It will allow 2 Mbps operation up to 25 miles (40 Km) and 11 Mbps operation up to 20.52 miles (33 Km).

Note All distances shown in the illustration are theoretical and may actually be shorter, dependant upon the country of installation, governing bodies, and allowable EIRP levels.



Cisco Aironet Wireless Bridging Solutions

Cisco.com

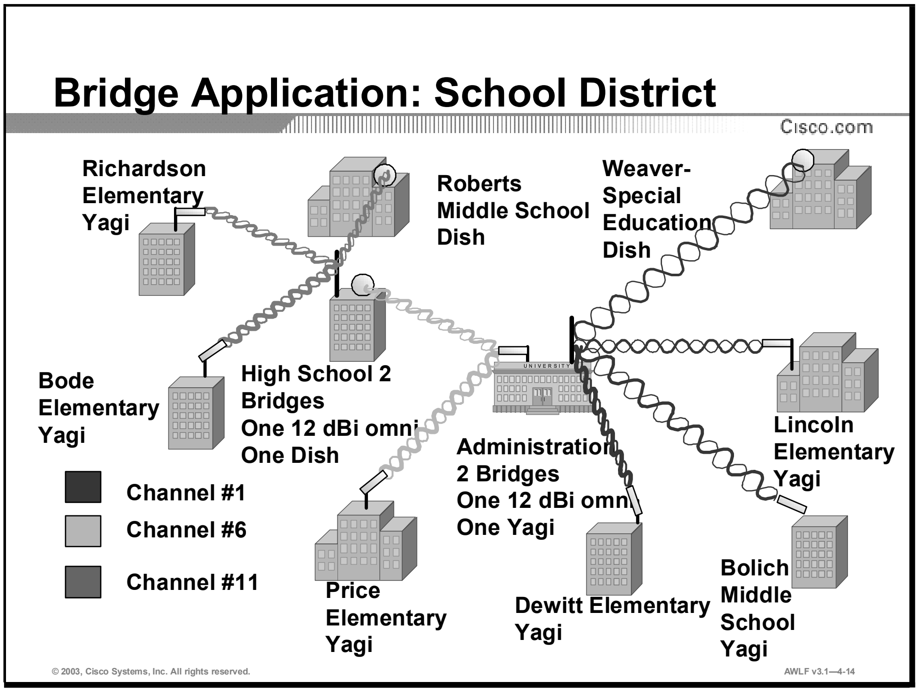
Cisco Aironet 350 Series	Cisco Aironet 1400 Series
Wireless Bridging at a Lower Total Cost	Wireless Bridging with outstanding performance
Single 802.11b radio with data rates up to 11 Mbps	Single 802.11a radio with data rates up to 54 Mbps
3 miles typical point to point range with directional antennas at 11 Mbps	7.5 miles typical point to point range with directional antennas at 54 Mbps
Two 2.4 GHz antenna connectors for high gain diversity antennas	Single 5.8 GHz integrated patch array antenna or antenna connector for remote antennas
Indoor industrial environmental specifications, rugged metal case	Outdoor environmental specifications, tested to NEMA 4
Inline and Local Power	Inline Power via Power Injector LR
VxWorks based operating system	Cisco IOS operating system
QOS, VLANs, and Proxy Mobile IP	QOS, VLANs, and Proxy Mobile IP
Statistics via telnet	Antenna Alignment feedback via LEDs and RSSI port and statistics via telnet

AWLF v3.1—4-12

Difference between the 350 Series and the 1400 Series Bridges

The BR1410 operates in a different frequency band (5.8GHz) than the BR350 (2.4GHz). The BR1410 supports higher data rates, up to 54Mbps, compared to the BR350, which supports data rates up to 11Mbps. The entire unit was designed specifically for harsh outdoor environments, with extended operating temperature range, and ability to withstand humidity and extreme weather conditions. Unlike the BR350, the BR1410 only supports the Root and Non-Root Bridge roles in the radio network.

Role in Radio Network



Bridge Application: School District

Richardson Elementary Yagi

Roberts Middle School Dish

Weaver-Special Education Dish

Bode Elementary Yagi

High School 2 Bridges
One 12 dBi omni
One Dish

Administration 2 Bridges
One 12 dBi omni
One Yagi

Lincoln Elementary Yagi

Price Elementary Yagi

Dewitt Elementary Yagi

Bolich Middle School Yagi

■ Channel #1

□ Channel #6

▨ Channel #11

AWLF v3.1—4-14

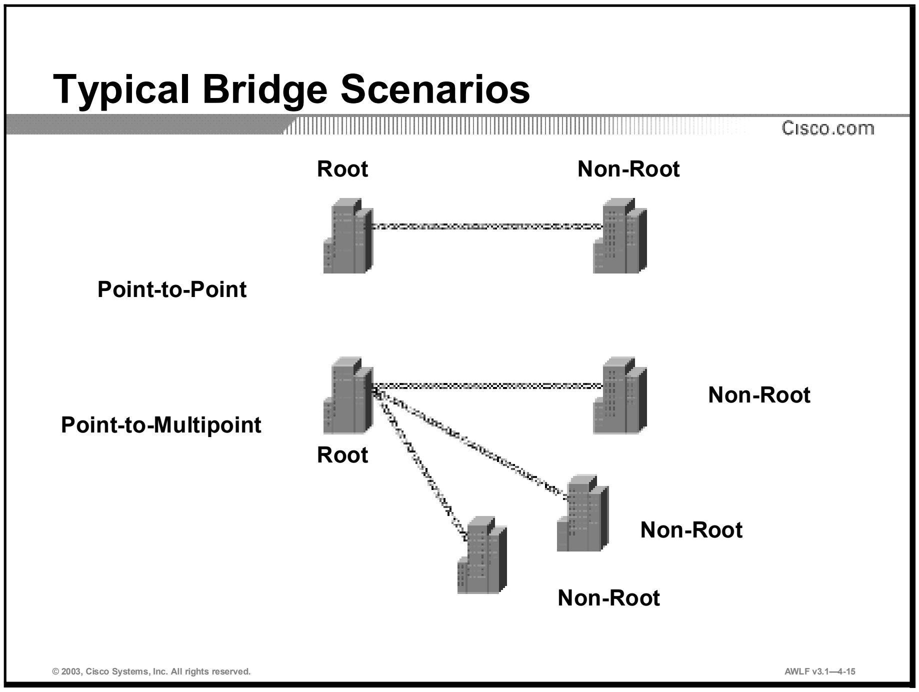
Illustrated in the slide above is a typical school environment based on a 2.4 GHz bridging solution; faster speeds may be obtained using a 5 GHz bridging solution. The Internet line comes into the Administration building. At that site, the network spans in two directions.

Assume 5.5 Mbps of throughput for the 11 Mbps bridges. Weaver, Lincoln, Bolich, and Dewitt schools all communicate to the administration building with channel 1, providing a minimum of 1.3 Mbps throughput connection to each school. (That is T1 speed!)

Richardson, Roberts and Bode all communicate to the High School using Channel 11, providing at least 1.8 Mbps throughput to the High School. The data is then passed on to another bridge that uses Channel 6 to communicate to the Administration building. Price school is also tied in on this same channel. In this manner we have 5 schools sharing Channel 6, which still provides over 1.1 Mbps to all 5 schools.

Over all, the worst case for ANY school is over 1 Mbps of throughput. And payback for the cost of the bridges averages about 1 year. No need to spend taxpayer's money year after year.

Cisco Aironet = LESS MONEY & MORE PERFORMANCE



Typical Bridge Scenarios

Cisco.com

Root

Non-Root

Point-to-Point

Point-to-Multipoint

Root

Non-Root

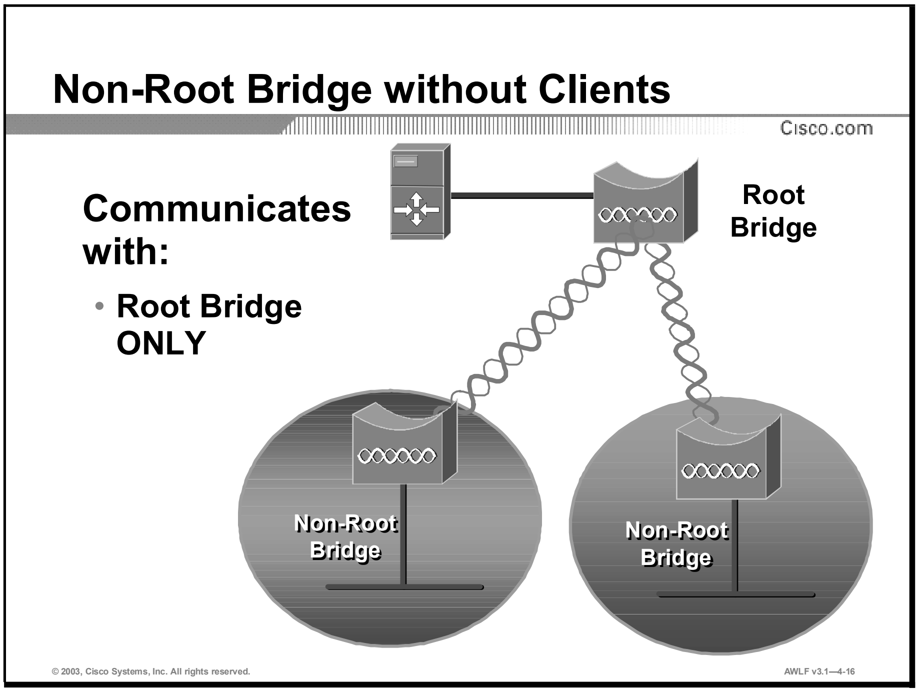
Non-Root

Non-Root

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—4-15

Cisco Aironet Bridges can be configured to operate in many different modes. This is the function of the Role in Radio Network parameter. Note in each scenario there is only one Root Bridge.



Non-Root Bridge without Clients

Communicates with:

- Root Bridge ONLY

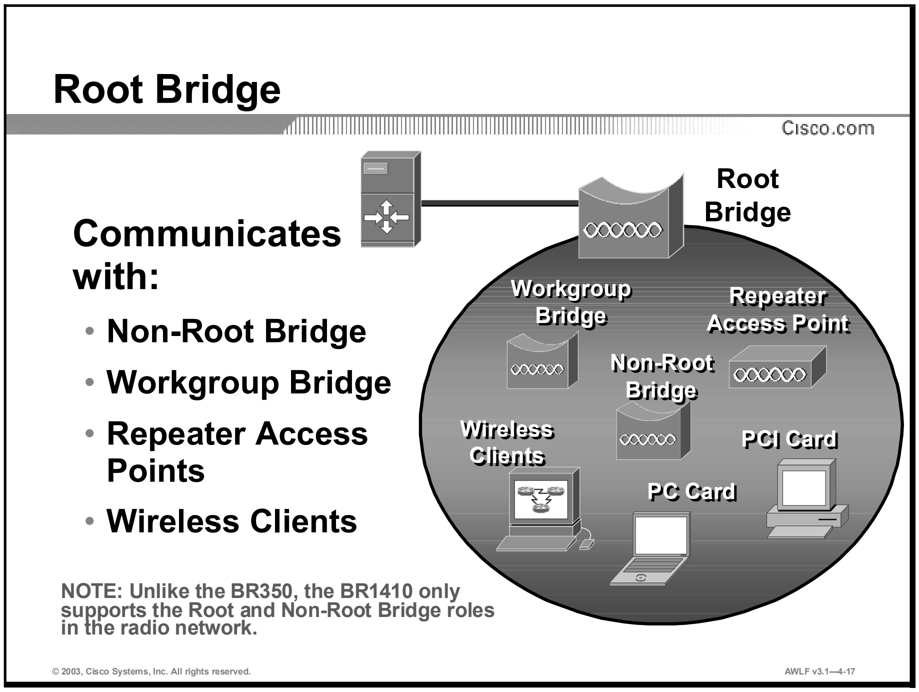
Root Bridge

Non-Root Bridge

Non-Root Bridge

AWLF v3.1—4-16

This mode would be used for a bridge that is used to connect a remote wired LAN and will only communicate with another Root Bridge. In this mode the bridge will refuse associations from wireless clients.



Root Bridge

Communicates with:

- **Non-Root Bridge**
- **Workgroup Bridge**
- **Repeater Access Points**
- **Wireless Clients**

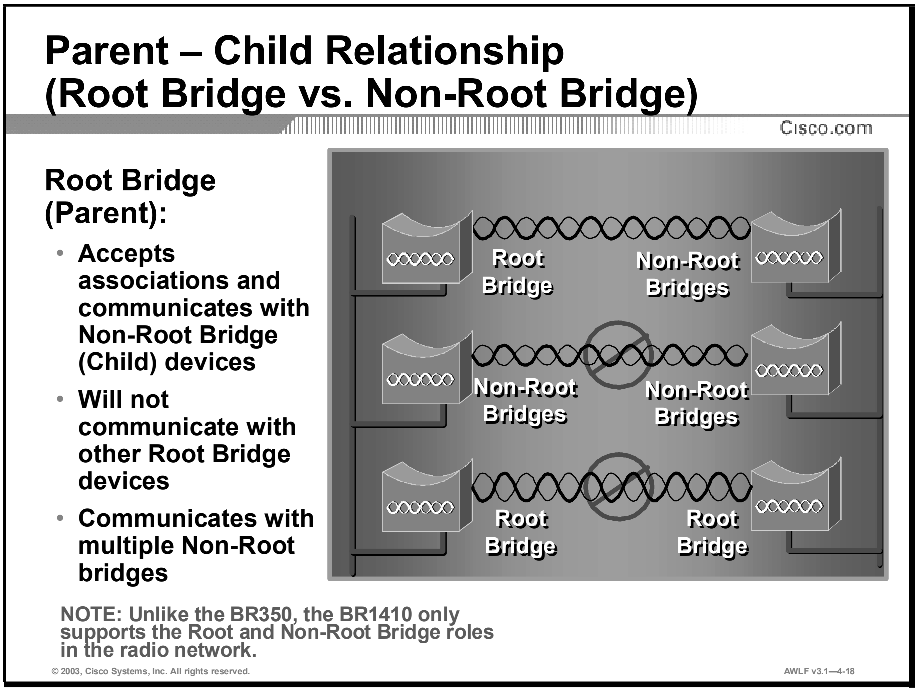
NOTE: Unlike the BR350, the BR1410 only supports the Root and Non-Root Bridge roles in the radio network.

AWLF v3.1—4-17

This setting is normally used for the “main” bridge – in other words, the bridge that is connected to the main network. This bridge would be used to provide connectivity to the main LAN for other wireless clients or wired clients that are being connected wirelessly. In this mode the bridge will support the following client types by default:

- Non-Root Bridges
- Wireless Client Cards (PC Card, PCI Card)
- Workgroup Bridges (WGB)
- Access points configured as Repeaters

Only one bridge in a WLAN can be set as the root bridge. This is the default setting for Cisco Aironet Bridges.



Parent – Child Relationship (Root Bridge vs. Non-Root Bridge)

Cisco.com

Root Bridge (Parent):

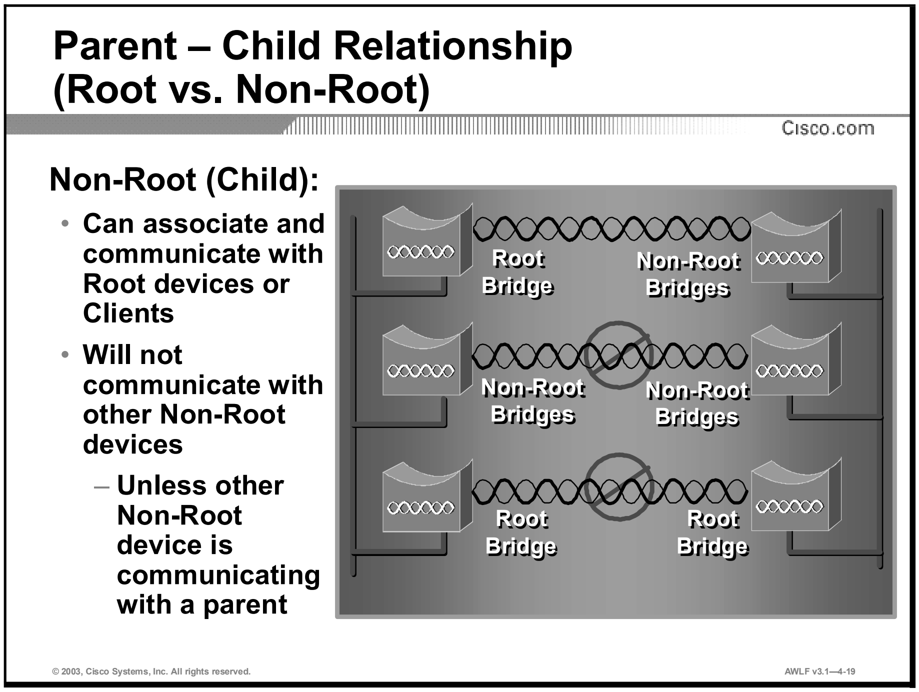
- Accepts associations and communicates with Non-Root Bridge (Child) devices
- Will not communicate with other Root Bridge devices
- Communicates with multiple Non-Root bridges

Root Bridge
Non-Root Bridges
Non-Root Bridges
Non-Root Bridges
Root Bridge
Root Bridge

NOTE: Unlike the BR350, the BR1410 only supports the Root and Non-Root Bridge roles in the radio network.

AWLF v3.1—4-18

Unlike Cisco Aironet Access Points, bridges require some configuration prior to installation. A parent-child relationship must be established between bridges before they can communicate. This is the function of the “Root Bridge” mode on Cisco Aironet bridges. A bridge that is configured as a “Root Bridge” device is considered a parent bridge. A bridge that is configured as a “Non-Root Bridge” device is considered a child. The child bridge will learn many of the configurable parameters from the parent bridge.



Parent – Child Relationship (Root vs. Non-Root)

Cisco.com

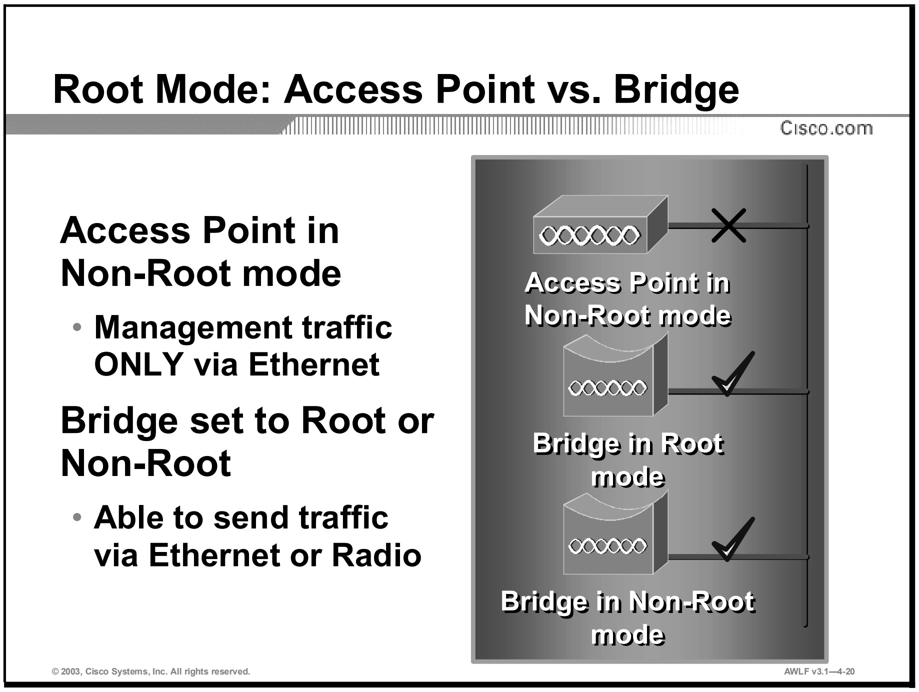
Non-Root (Child):

- **Can associate and communicate with Root devices or Clients**
- **Will not communicate with other Non-Root devices**
  - **Unless other Non-Root device is communicating with a parent**

AWLF v3.1—4-19

A single parent bridge can support numerous child bridges. How many child bridges should actually be attached to a parent bridge will be determined by usage and throughput needs.

Only exception: Non-Root Bridge will communicate to another Non-Root Bridge as long as one of the Non-Root Bridges has a Root Bridge in its uplink.



Root Mode: Access Point vs. Bridge

Cisco.com

Access Point in Non-Root mode

- Management traffic ONLY via Ethernet

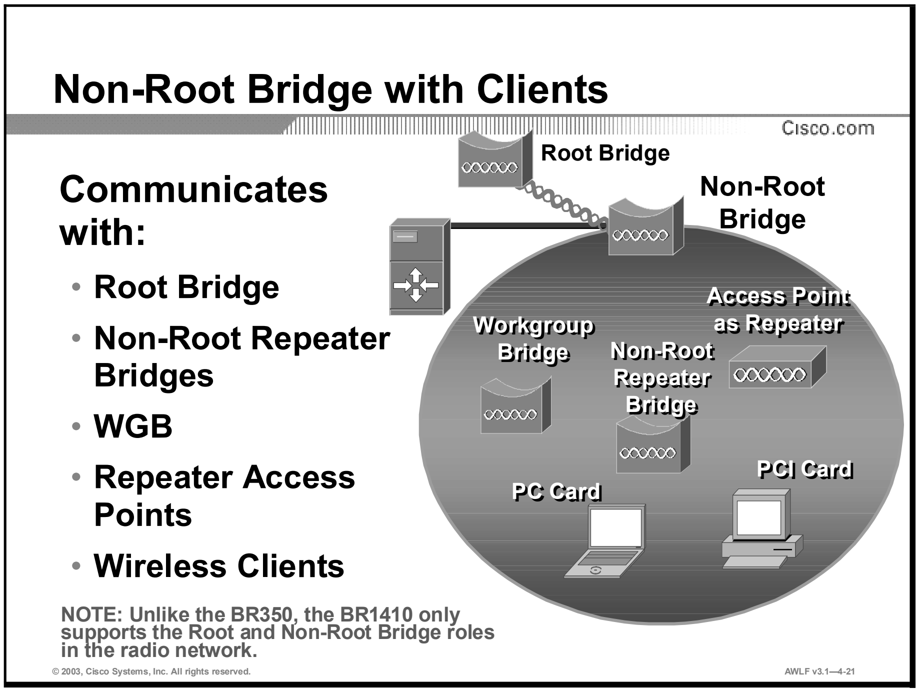
Bridge set to Root or Non-Root

- Able to send traffic via Ethernet or Radio

AWLF v3.1—4-20

Whether configured as a "Root" or "Non-Root" device, a bridge can always communicate with other bridges via the RF, and the wired network via the Ethernet port. Even when configured to operate in access point mode, the bridge can still pass network traffic via both the RF and Ethernet ports. This is one of the main differences between a Cisco Aironet Bridge and Access Point.

Cisco Aironet Access Points and Bridges use the same radio. The Cisco Aironet Bridge has the same receiver sensitivity, power levels, and capabilities as the Cisco Aironet Access Point. This means that while operating in access point mode, the Cisco Aironet Bridge can be configured as a fully IEEE 802.11 compliant access point that will support Cisco Aironet wireless clients.



Non-Root Bridge with Clients

Cisco.com

Communicates with:

- **Root Bridge**
- **Non-Root Repeater Bridges**
- **WGB**
- **Repeater Access Points**
- **Wireless Clients**

NOTE: Unlike the BR350, the BR1410 only supports the Root and Non-Root Bridge roles in the radio network.

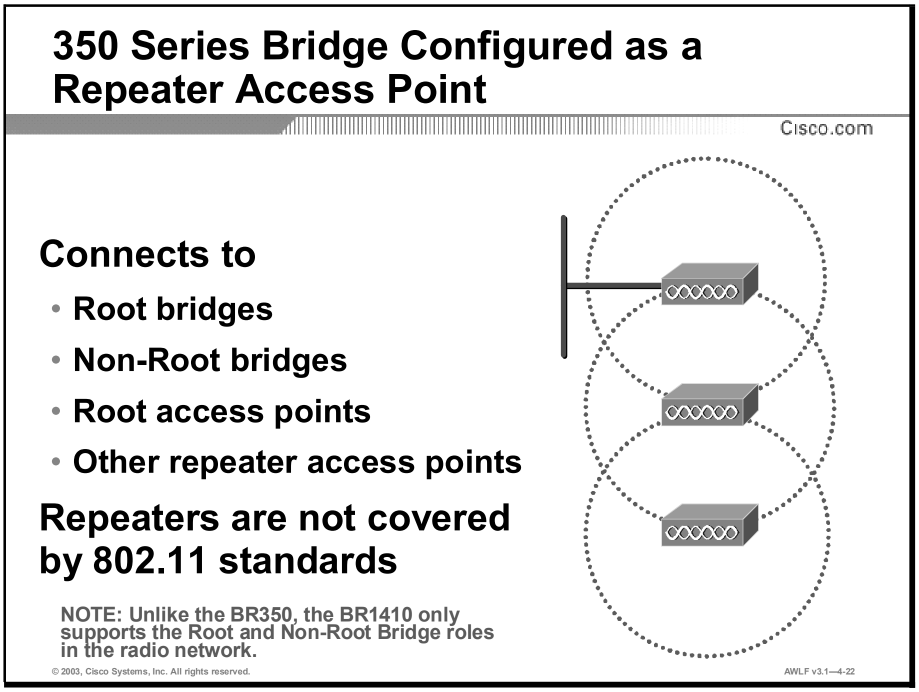
AWLF v3.1—4-21

This setting is used for any bridges in the WLAN that will be connecting to a Root bridge. In this mode, a bridge will perform bridging functions (connect to a Root bridge) and will also support the following clients by default:

- Wireless Clients (PC Card, PCI Card)
- Workgroup Bridge
- Access points configured as a Repeater
- Other Non-Root Bridges

In this mode the bridge may connect to a remote wired LAN or may be used as a repeater bridge. When used as a repeater bridge, the bridge would not be connected to a remote wired LAN and would simply pass traffic from associated wireless clients to another Non-Root bridge or a Root bridge.

In order for wireless clients to attach to a Non-Root bridge, the bridge must be associated with a Root bridge, or another Non-Root bridge that is associated to a Root bridge.



350 Series Bridge Configured as a Repeater Access Point

Cisco.com

Connects to

- **Root bridges**
- **Non-Root bridges**
- **Root access points**
- **Other repeater access points**

Repeaters are not covered by 802.11 standards

NOTE: Unlike the BR350, the BR1410 only supports the Root and Non-Root Bridge roles in the radio network.

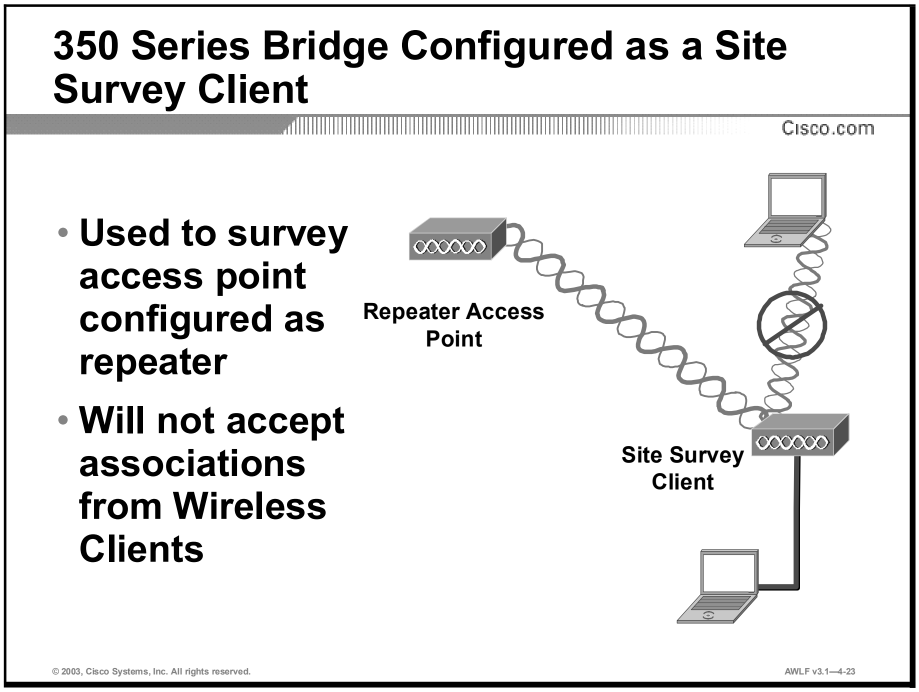
AWLF v3.1—4-22

When in this mode the bridge will operate with the same functionality as a Cisco Aironet Access Point in repeater mode. The bridge will repeat wireless client traffic to any of the following:

- Access point connected to LAN
- Another Repeater Access Point
- Root Bridge connected to LAN
- Non-Root Bridge connected to LAN
- Bridge in access point mode connected to LAN

The bridge will only pass management traffic (no WLAN client traffic) via the Ethernet port.

Due to the fact that repeaters are not covered by 802.11 standards non-Cisco clients may or may not work with Cisco repeaters.



350 Series Bridge Configured as a Site Survey Client

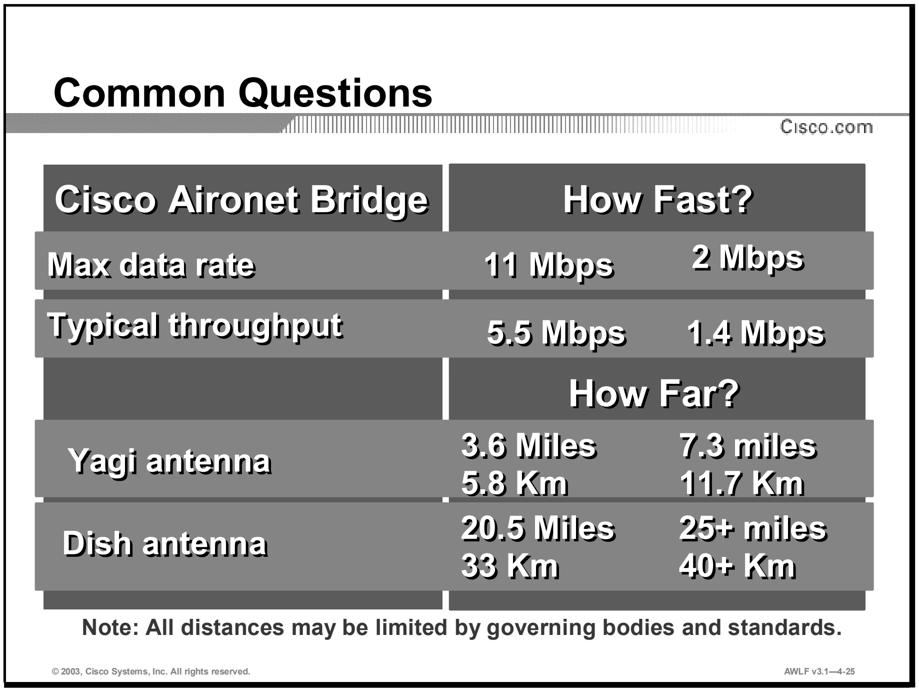
Cisco.com

- Used to survey access point configured as repeater
- Will not accept associations from Wireless Clients

AWLF v3.1—4-23

The bridge can be configured as a Site Survey Client for surveying a repeater access point. While in this mode the bridge can connect to another bridge or access point, but will not accept associations from wireless clients. The Site Survey Client can then be used to perform linktests with other bridges or access points.

Installation Considerations



Common Questions

Cisco Aironet Bridge	How Fast?	
Max data rate	11 Mbps	2 Mbps
Typical throughput	5.5 Mbps	1.4 Mbps
	How Far?	
Yagi antenna	3.6 Miles 5.8 Km	7.3 miles 11.7 Km
Dish antenna	20.5 Miles 33 Km	25+ miles 40+ Km

Note: All distances may be limited by governing bodies and standards.

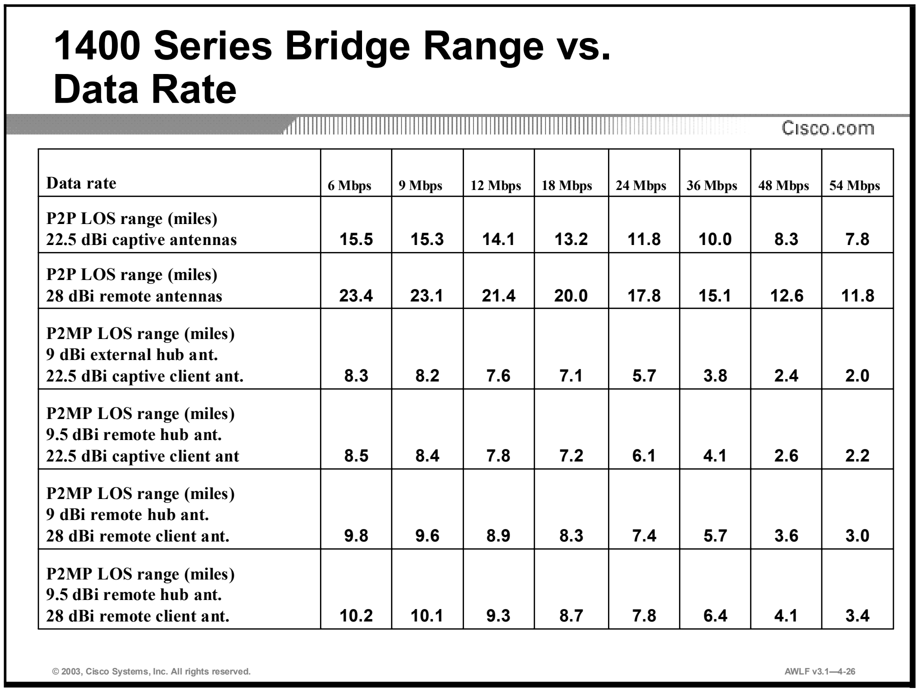
AWLF v3.1—4-25

Typical questions for bridges include how far will it go, how fast will it go, and how many users can it support.

How fast: One item that is very deceiving is data rate - what does it really mean? As with the LAN systems, data rate indicates how fast the RF passes data. This RF data includes the radio system overhead, plus the network data. The real item that should be discussed is throughput. This is the actual amount of network data that gets passed from one LAN to another. Remember higher data rates do not mean higher throughput. Some 1.6 Mbps systems achieve as little as 500 Kbps throughput.

With a 2.4 GHz bridge, the data rate can be set to various speeds (1, 2, 5.5, 11 Mbps). Reducing the speed increases the maximum distances that can be obtained. The same concept applies to 5 GHz bridges.

Adding filtering in the configuration can increase actual performance by eliminating unnecessary traffic over the RF. This has the same effect as increasing throughput. How many users the bridge can support is a question of what type of traffic is being handled. Throughput is the real limiting factor.



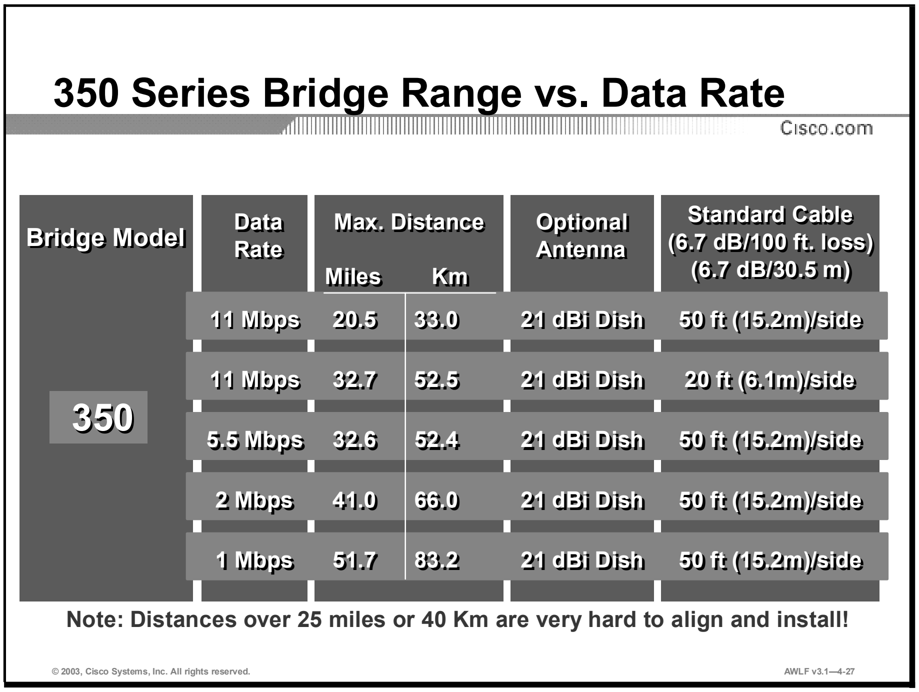
1400 Series Bridge Range vs. Data Rate

Data rate	6 Mbps	9 Mbps	12 Mbps	18 Mbps	24 Mbps	36 Mbps	48 Mbps	54 Mbps
P2P LOS range (miles) 22.5 dBi captive antennas	15.5	15.3	14.1	13.2	11.8	10.0	8.3	7.8
P2P LOS range (miles) 28 dBi remote antennas	23.4	23.1	21.4	20.0	17.8	15.1	12.6	11.8
P2MP LOS range (miles) 9 dBi external hub ant. 22.5 dBi captive client ant.	8.3	8.2	7.6	7.1	5.7	3.8	2.4	2.0
P2MP LOS range (miles) 9.5 dBi remote hub ant. 22.5 dBi captive client ant	8.5	8.4	7.8	7.2	6.1	4.1	2.6	2.2
P2MP LOS range (miles) 9 dBi remote hub ant. 28 dBi remote client ant.	9.8	9.6	8.9	8.3	7.4	5.7	3.6	3.0
P2MP LOS range (miles) 9.5 dBi remote hub ant. 28 dBi remote client ant.	10.2	10.1	9.3	8.7	7.8	6.4	4.1	3.4

AWLF v3.1—4-26

The 5.8 GHz radio in the Cisco Aironet 1400 Series offers superior radio performance that results in industry-leading range. The greater the range, the higher the supported data rate or the more reliable the link at a given data rate.

- **Point-to-point range** 7.5 miles (13 km) @ 54 Mbps16 miles (26 km) @ 9 Mbps 12 miles (19 km) @ 54 Mbps23 miles (37 km) @ 9 Mbps(Antennas are 28 dBi dish)
- **Point-to-multipoint range (sector antenna at root)** 2 miles (3 km) @ 54 Mbps8 miles (13 km) @ 9 Mbps4 miles (7 km) @ 54 Mbps11 miles (18 km) @ 9 Mbps(Non-root antenna is 28 dBi dish)



350 Series Bridge Range vs. Data Rate

Cisco.com

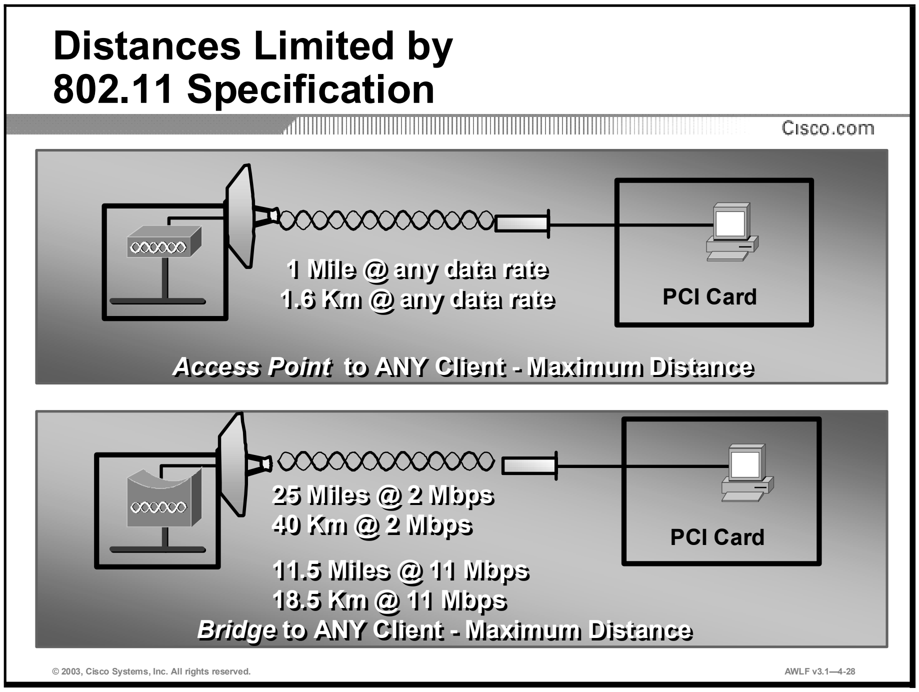
Bridge Model	Data Rate	Max. Distance Miles	Max. Distance Km	Optional Antenna	Standard Cable (6.7 dB/100 ft. loss) (6.7 dB/30.5 m)
350	11 Mbps	20.5	33.0	21 dBi Dish	50 ft (15.2m)/side
	11 Mbps	32.7	52.5	21 dBi Dish	20 ft (6.1m)/side
	5.5 Mbps	32.6	52.4	21 dBi Dish	50 ft (15.2m)/side
	2 Mbps	41.0	66.0	21 dBi Dish	50 ft (15.2m)/side
	1 Mbps	51.7	83.2	21 dBi Dish	50 ft (15.2m)/side

Note: Distances over 25 miles or 40 Km are very hard to align and install!

AWLF v3.1—4-27

At 11 Mbps, using a 21-dBi dish and 50 feet of cable on each side, the 350 Series Bridge will have a range exceeding 20 miles or 33 kilometers. Reducing the loss in the cables by reducing cable length whenever possible or changing to a lower data rate allows this range to extend even further.

Note All distances shown in the illustration are theoretical and may actually be shorter, dependant upon the country of installation, governing bodies, and allowable EIRP levels.



Distances Limited by 802.11 Specification

Cisco.com

1 Mile @ any data rate
1.6 Km @ any data rate

PCI Card

Access Point to ANY Client - Maximum Distance

25 Miles @ 2 Mbps
40 Km @ 2 Mbps

11.5 Miles @ 11 Mbps
18.5 Km @ 11 Mbps

PCI Card

Bridge to ANY Client - Maximum Distance

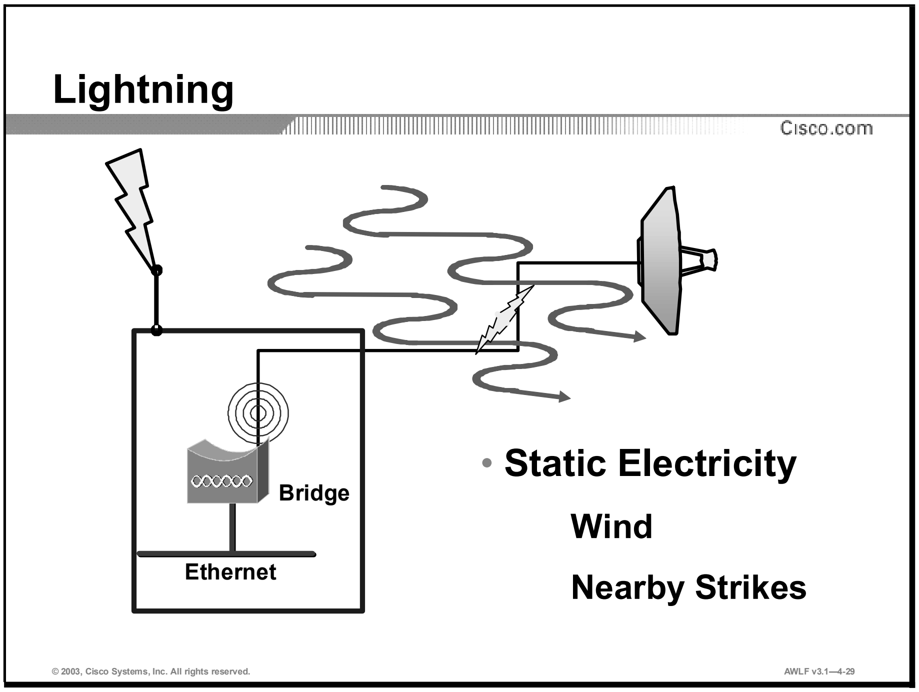
© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—4-28

Customers may want to save money and use the workgroup bridge and access point in place of a bridge. If the distance is less than 1 mile and remote end (WGB) has less than 8 end devices, this can be done. However, if the distance is greater than 1 mile, it is recommended that a bridge be used instead of the access point. Using an access point at more than 1 mile will not provide reliable communications. This is due to timing constraints that the 802.11 standard puts on the return times for packets acknowledgements. Remember, 802.11 defines a **LAN** - *Local Area Network* - which is typically a wireless range of up to 1000 feet.

The bridge product has a parameter that stretches this timing (which violates 802.11) and allows the Cisco Aironet devices to operate at greater distances. (All bridges that support distances over 1 mile violate 802.11.)

It also means other 802.11 vendors' radios may not work with the Cisco Aironet bridge at distances greater than 1 mile.



Lightning

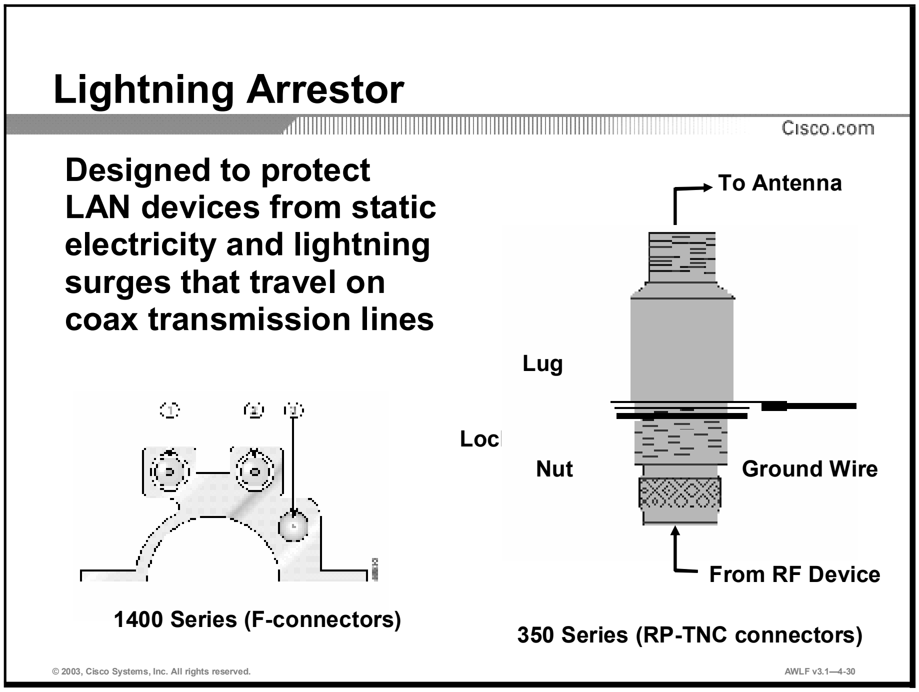
Cisco.com

- Static Electricity
  - Wind
  - Nearby Strikes

AWLF v3.1—4-29

The Cisco Lightning Arrestor is designed to protect Cisco Spread Spectrum Wireless LAN devices from static electricity and lightning surges that travel on coaxial transmission lines. The Cisco Aironet lightning arrestor complies with FCC and DOC regulations.

Lightning does not need a direct hit to cause problems. An indirect hit can induce enough energy into the cable and antennas to cause damage to the bridge and other network devices.



Lightning Arrestor

Cisco.com

Designed to protect LAN devices from static electricity and lightning surges that travel on coax transmission lines

1400 Series (F-connectors)

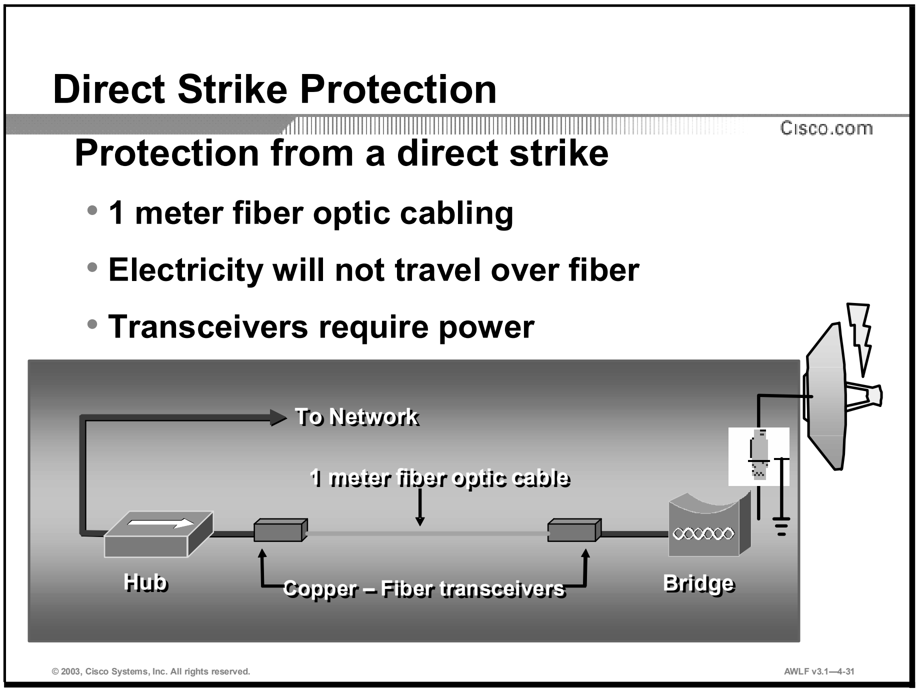
350 Series (RP-TNC connectors)

AWLF v3.1—4-30

Theory of Operation

The Cisco Lightning Arrestor prevents energy surges from reaching the RF equipment through the shunting effect of the device. Surges are limited to less than 50 volts, in about .0000001 seconds (100 nano seconds). A typical lightning surge is about .000002 (2 microseconds). The accepted IEEE transient (surge) suppression is .000008 seconds (8 microseconds).

A lightning arrestor has two main purposes. One is to bleed off any high static charges that collect on the antenna, which will prevent the antenna from attracting a lightning hit. The second purpose is to dissipate any energy that gets induced into the antenna or coax from a near lightning strike.



Direct Strike Protection

Cisco.com

Protection from a direct strike

- 1 meter fiber optic cabling
- Electricity will not travel over fiber
- Transceivers require power

© 2003, Cisco Systems, Inc. All rights reserved.

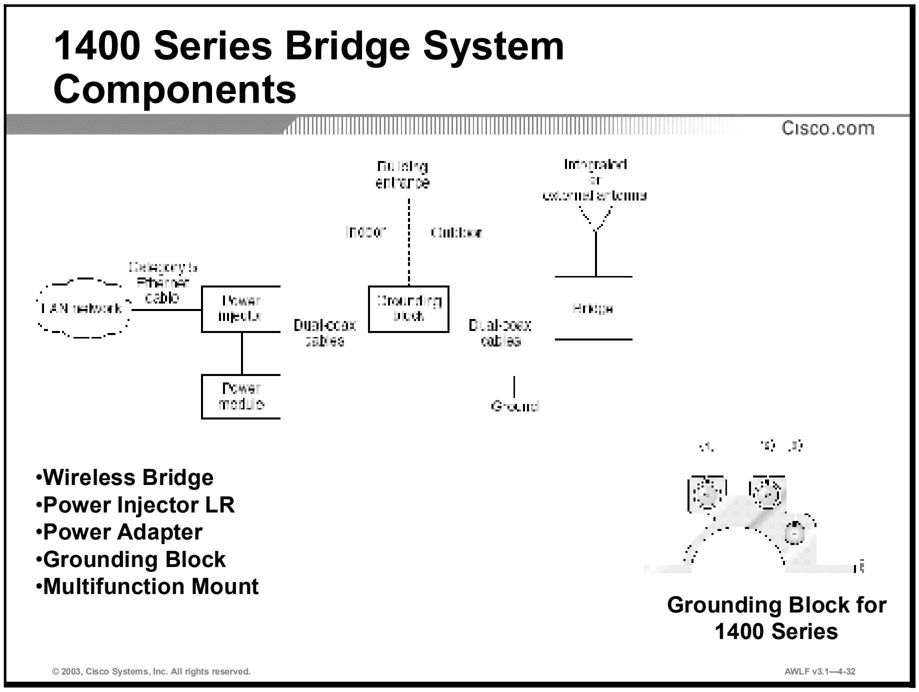
AWLF v3.1—4-31

When an antenna is installed outside of the building, there is a chance that it could be struck by lightning. Because of the extreme voltage associated with a lightning strike, the current could travel into the network, using the antenna, extension cable, and then the Cat 5 cable as a path. Once the current is on the Cat 5 cable, it could travel throughout the entire network and damage any equipment connected to the Cat 5.

The best protection against a direct strike is fiber optic cabling. The Cisco Aironet lightning arrestor will not stop a direct strike. Because the conductor in fiber optic cabling is glass, the current cannot travel over the fiber, and the energy is dissipated as heat, melting the fiber optic cabling.

In order to use this method, one meter of fiber optic cabling is needed, and two copper-fiber transceivers. The transceivers will require power.

Note	Note: Do not plug both transceivers into the same electrical outlet as this may provide a path for the current to bypass the fiber optic cabling.



1400 Series Bridge System Components

Cisco.com

- •Wireless Bridge
- •Power Injector LR
- •Power Adapter
- •Grounding Block
- •Multifunction Mount

Grounding Block for 1400 Series

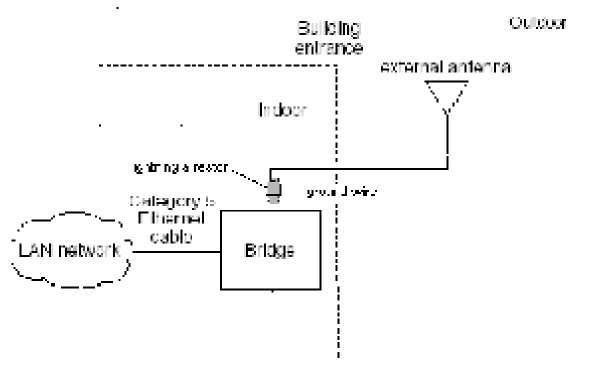
AWLF v3.1—4-32

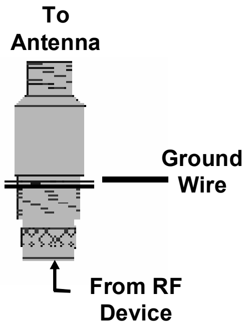
This diagram depicts the 1400 Series bridge installed outdoors. Typically the duel cables coming from the bridge are routed through a grounding block just before the cable enters the building.

The grounding block ensures that the cables are taken to a ground source to prevent lightning damage.

350 Series Bridge System Components

Cisco.com



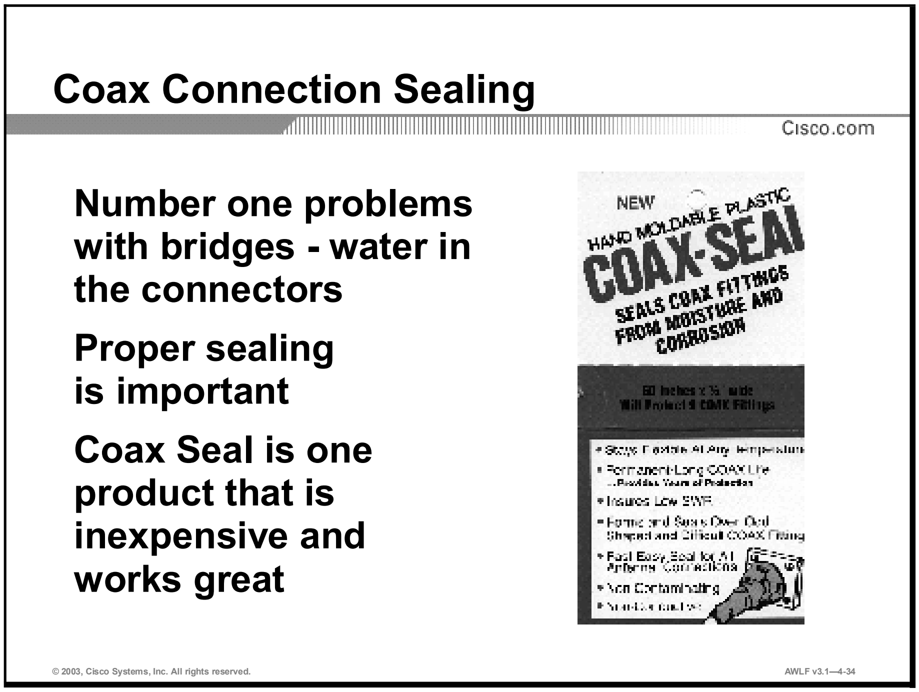


350 Series Lightning Arrestor

AWLF v3.1—4-33

The 350 Series Bridge is typically installed indoors with the antenna deployed outside. A lightning arrestor is attached inline with the bridge and a wire from the lightning arrestor connects to a good ground source.

Sources of ground include but are not limited to, a conductive ground rod, electrical panel ground or building structural steel. Try to locate the bridge close to one of these sources of ground.



Coax Connection Sealing

Cisco.com

- Number one problems with bridges - water in the connectors
- Proper sealing is important
- Coax Seal is one product that is inexpensive and works great

NEW
HAND MOLDABLE PLASTIC
COAX-SEAL
SEALS COAX FITTINGS FROM MOISTURE AND CORROSION
Stays Flexible At Any Temperature
Permanent-Long COAX Life ...Provides Years of Protection
Insures Low SWR
Forms and Seals Over Odd Shaped and Difficult COAX Fitting
Fast Easy Seal for All Antenna Connections
Non Contaminating

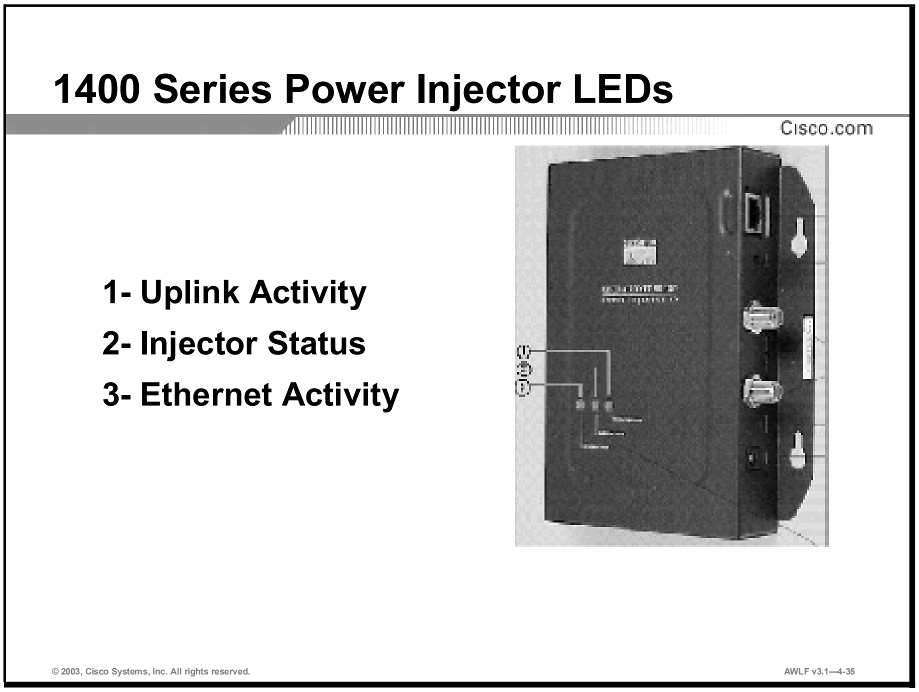
AWLF v3.1—4-34

You will need to seal the coax connectors to prevent water intrusion into the connectors. If water gets into the connectors, it will work its way up the coax, contaminating it and rendering the coax unusable.

The only way to prevent this from happening is to use a sealant. Room Temperature Vulcanized (or RTV) is not a good sealant, as many variations of this material contain a curing agent that is actually corrosive to metal and can cause bad connections.

Coax Seal is one of the best products that are available to seal connectors. It is available from most ham radio stores and may two-way radio shops. Typical cost is $3.00 per roll (or about 33 cents per connection).

The Cisco Aironet 1400 Series provides standard N-Type and F-Type coaxial cable connectors for easy and reliable weather sealing and grounding. A coaxial sealant is provided with each system, along with a standard grounding block to allow the installer to meet National Electric Code guidelines.



1400 Series Power Injector LEDs

Cisco.com

1- Uplink Activity

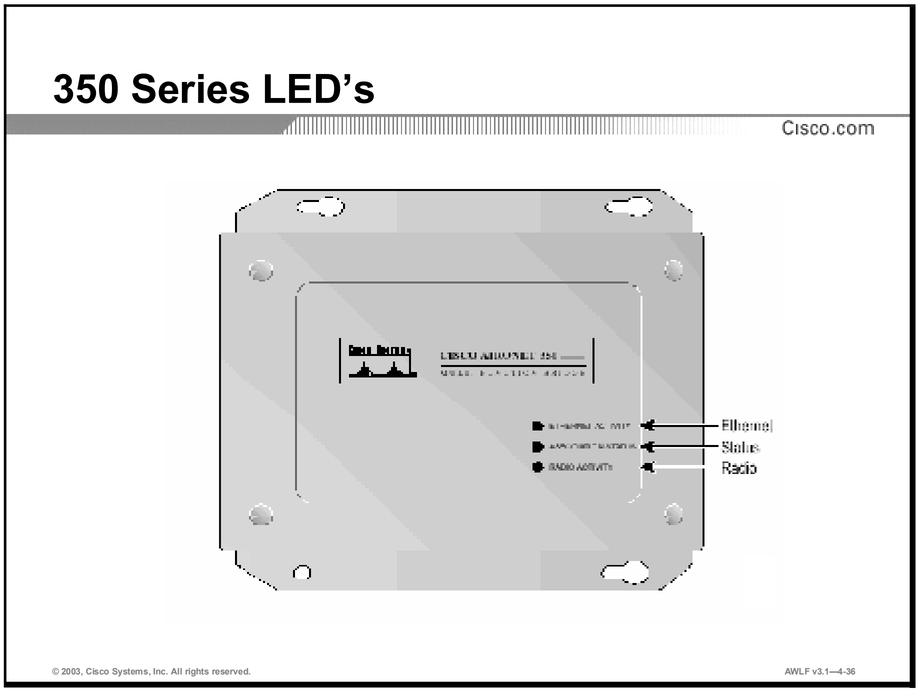
2- Injector Status

3- Ethernet Activity

AWLF v3.1—4-35

1. Uplink Activity, Green, Link between power injector and bridge is operational
2. Injector Status, Green, Bridge successfully passed Power On Self Test (POST) and loaded the IOS image
3. Ethernet Activity, Green, Wired LAN Ethernet link is operational

For more details please view the 1400 Series Bridge Installation guide: http://www.cisco.com/en/US/products/hw/wireless/ps5279/products_installation_guide_chapter09186a0080184a70.html#1049273



350 Series LED’s

Cisco.com

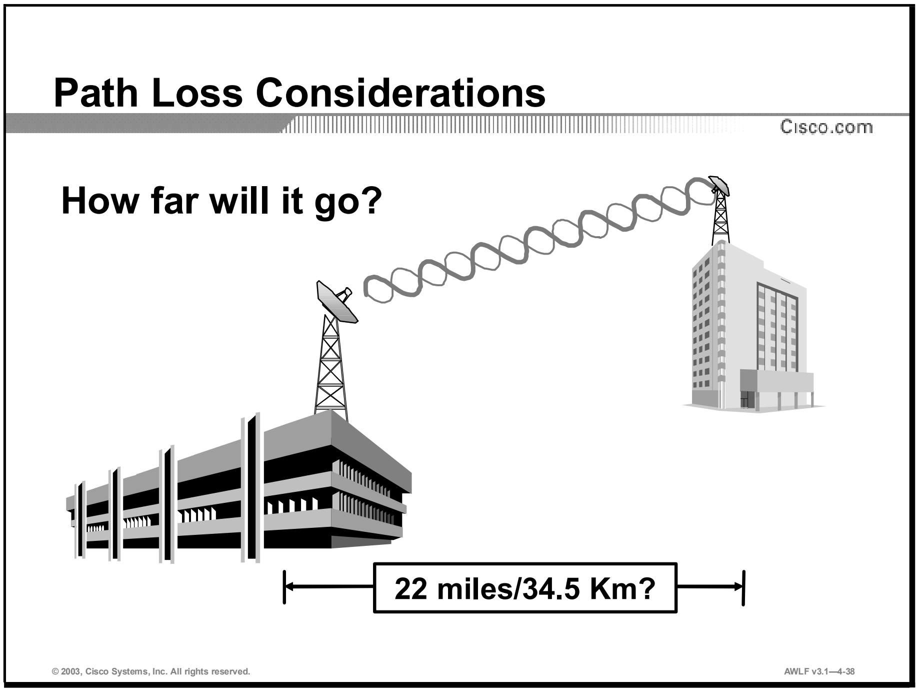
AWLF v3.1—4-36

The Status light provides updates on the operation of the unit itself. The most important feature of the light is the ability to determine if there are any remote devices communicating with the bridge. If the light is solid green, there is at least one other RF device connected. If it is blinking consistently (on/off equally at about ½ second rate) there are no devices communicating. In the Non-Root mode, the light is solid with a very short off blink occurring about every second.

The status light may also flash red or amber anytime the system has an error occur. This would prompt you to look into the history logs for a review of errors that have been reported.

The Radio and Ethernet LED indicate activity (transmit or receive) over these medias. Typically the Ethernet will blink much faster than the RF since there will be more traffic on the Ethernet side than the RF side. If the RF LED is blinking much more that the Ethernet, this is an indication there is a lot or radio traffic going on, without corresponding Ethernet traffic. This could be from a RF test routine, or poor communication causing RF retries.

Path Loss Consideration



Path Loss Considerations

Cisco.com

How far will it go?

22 miles/34.5 Km?

AWLF v3.1—4-38

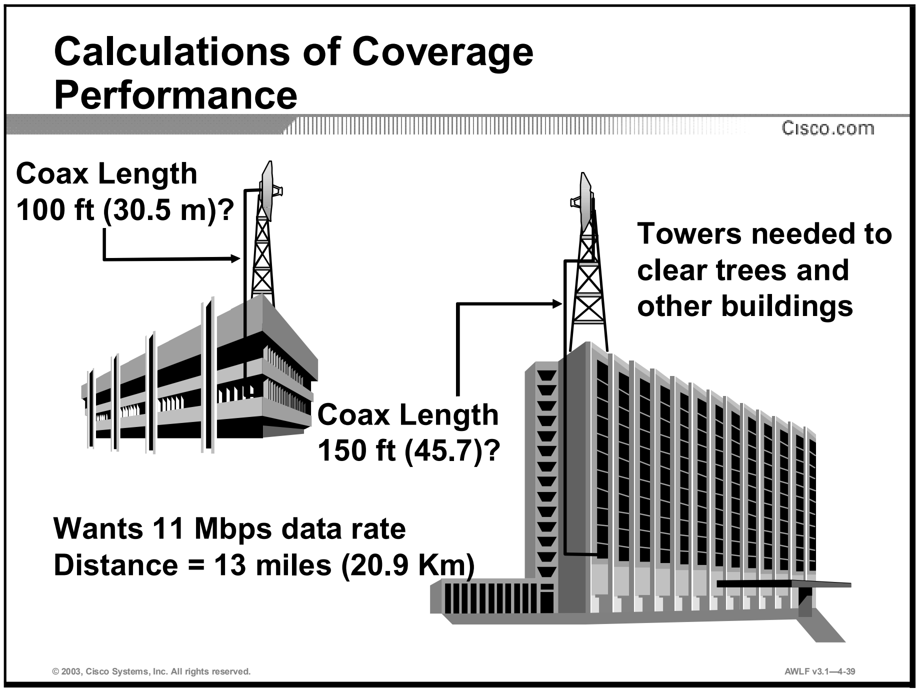
Calculations can be done to provide accurate information on performance and distance.

The following are included in calculations for determining coverage performance:

- Antenna Gain
- Transmitter Power
- Receiver Performance
- Cable Losses
- Environmental Structures

Path Loss determines how far a signal will travel and still provide reliable communications. Calculations are done in dB, and can be derived from the theoretical model.

Margin determines how much path interference can be inserted and still maintains communications. A 10 dB fade margin is required for dependable communications in all weather conditions.



Calculations of Coverage Performance

Coax Length
100 ft (30.5 m)?

Towers needed to clear trees and other buildings

Coax Length
150 ft (45.7)?

Wants 11 Mbps data rate
Distance = 13 miles (20.9 Km)

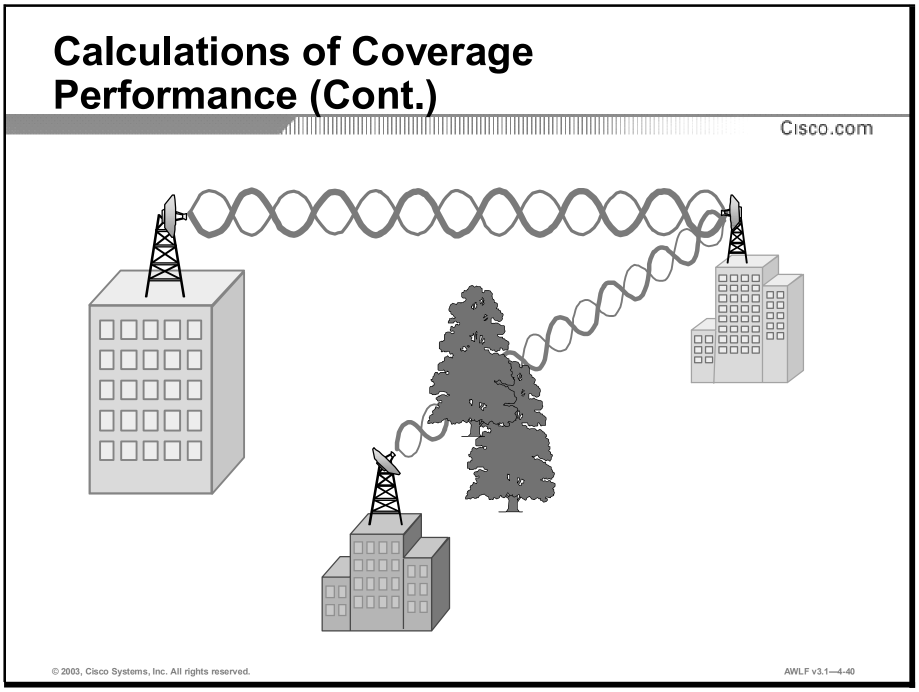
Suppose the customer is attempting to install the system as depicted in the slide above. Will the system work and meet their needs?

Using path loss calculations, antenna gains, and cable lengths, the distances can be theoretically checked.

Changes to the design can be made BEFORE attempting to install based upon these calculations.

Some level of comfort can be obtained for a system when using these calculations.

You can use the Antenna Calculation Utility to find out if the above situation is feasible. Later in this module the Antenna Calculation Utility will be discussed as well as how to use it to determine maximum distances possible while using various cables and antennae at different speeds.



Calculations of Coverage Performance (Cont.)

Cisco.com

AWLF v3.1—4-40

Rain, fog, and snow have little effect on path loss. The effect that it does have can be offset by having a path margin of at least 10 dB, as provided by the Cisco Antenna Calculation spreadsheet.

Line of sight is required between sites for long distances.

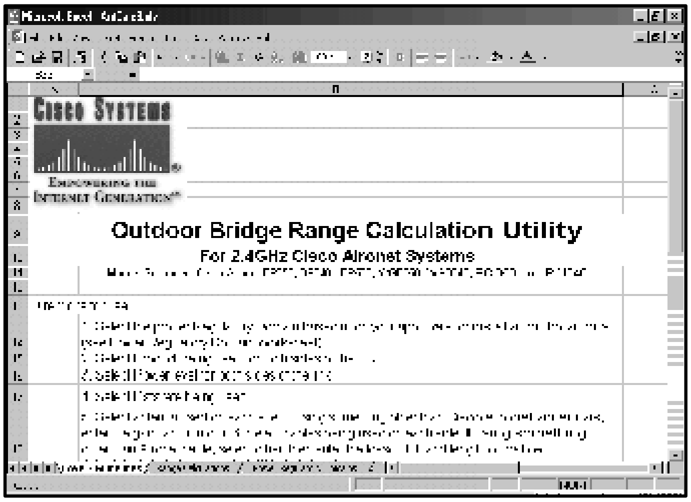
Because trees are mostly water, they can have a major effect on loss. Microwave ovens use the 2.4 GHz band because of how well water absorbs this particular frequency; therefore, the RF signal in the 2.4 GHz band will not get through trees because their high water content means the trees will absorb the signal. The same concept applies to 5 GHz.

Other considerations:

- Long distance signals will not travel through most building structures.
- Line-Of -Site is generally required between sites for long distances.

Bridge Distance Calculations

Cisco.com



Outdoor Bridge Range Calculation Utility

For 2.4GHz Cisco Aironet Systems

AWLF v3.1—4-41

For distance calculations, the following rules apply:

- Antenna gains are given in dBi (based upon a theoretical isotropic antenna) not dBd (based upon a dipole antenna).
- To convert from dBd to dBi, add 2.14 to the dBd
  - 0 dBd=2.14 dBi
- Cable lengths are a loss and are subtracted.

The antenna and radio parameters include cable losses at the receiver and transmitter sites, the antennas used at both sites, and the performance of the receiver and transmitter. Receiver gain changes with data rate. Always use maximum data rate values needed by the customer.

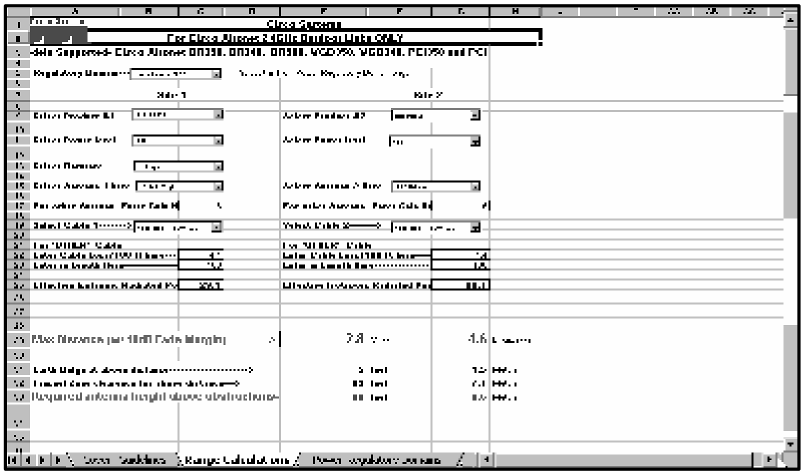
Distances for these formulas are calculated in miles and kilometers. For any given frequency, the atmosphere causes losses. This loss is a standard for any radio at that frequency.

Cisco Aironet offers the Cisco Aironet Outdoor Bridge Range Calculation utility. This utility is a spreadsheet that contains the necessary formulas to allow you to calculate how far a proposed bridge link can go. When using the Cisco Aironet Outdoor Bridge Range Calculation utility, follow these basic steps.

Select the product line being used. If you are trying to use access points outdoors, you can follow the same procedures.

Bridge Distance Calculations (Cont.)

Cisco.com



Cisco Systems

For Cisco Aironet 2.4GHz Outdoor Links ONLY

Side 1

Side 2

Max Distance (per 10dB Fade Margin)

Required antenna height above obstructions

AWLF v3.1—4-42

Select the configuration for your theoretical bridge link. Options include:

- Regulatory Domain
- Wireless Client (Bridge, Access Point, Workgroup Bridge, Client Card)
- Power Level
- Data Rate
- Antennas
- Antenna Extension Cable

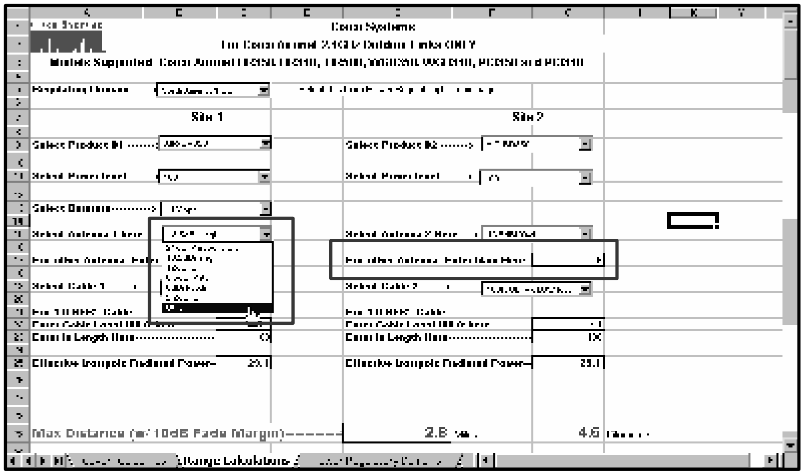
The utility will then show at what distance the selected components could connect.

Note	Your instructor will demonstrate the Outdoor Bridge Range Calculation (OBRC) utility live in class.

Note	The ORBC can be downloaded from Cisco Connection Online (CCO).

Bridge Distance Calculations (Cont.)

Cisco.com



Cisco Systems

Models Supported

Site 1

Site 2

Select Product #1

Select Product #2

Select Power level

Select Antenna 1 Here

Select Antenna 2 Here

Select Cable 1

Select Cable 2

Cable Length Here

Effective Isotropic Radiated Power 29.1

Max Distance (w/ 10dB Fade Margin) 2.8 4.6

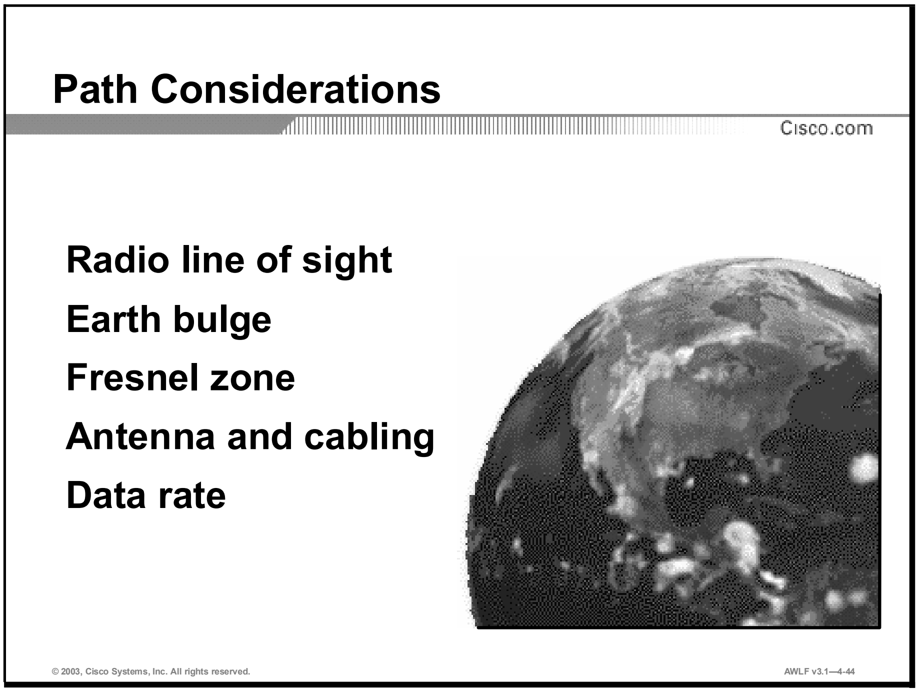
Range Calculations

AWLF v3.1—4-43

By selecting **Other Antenna** under the antenna selection, other losses can be added, if needed due to splitters, connectors, etc. Simply add then subtract the losses from the antenna gain and enter the result into the into the **Other Antenna Gain** box.

Remember these are theoretical values, but should provide a very good comfort level for proper operation.

These values provide a 10 dB fade margin.



Path Considerations

Cisco.com

Radio line of sight

Earth bulge

Fresnel zone

Antenna and cabling

Data rate

© 2003, Cisco Systems, Inc. All rights reserved.

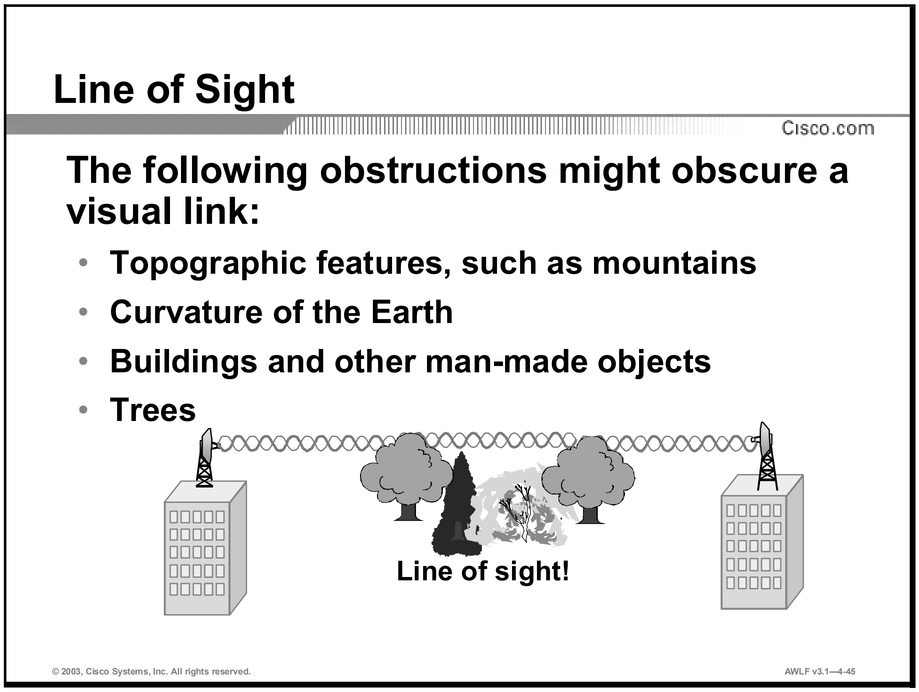
AWLF v3.1—4-44

Radio line of sight

There should be a clear visible path between the two antennas (you may need binoculars to see from one to the other). There should be no obstructions between the antennas themselves. These include trees, buildings, hills etc. Also, you need to take into account other line of sight factors including the Earth Bulge and the Fresnel Zone.

Earth Bulge

Takes into account the curvature of the earth and atmospheric refraction. Typically, at distances below 7 miles (11.26 Km), earth bulge can be ignored.



Line of Sight

The following obstructions might obscure a visual link:

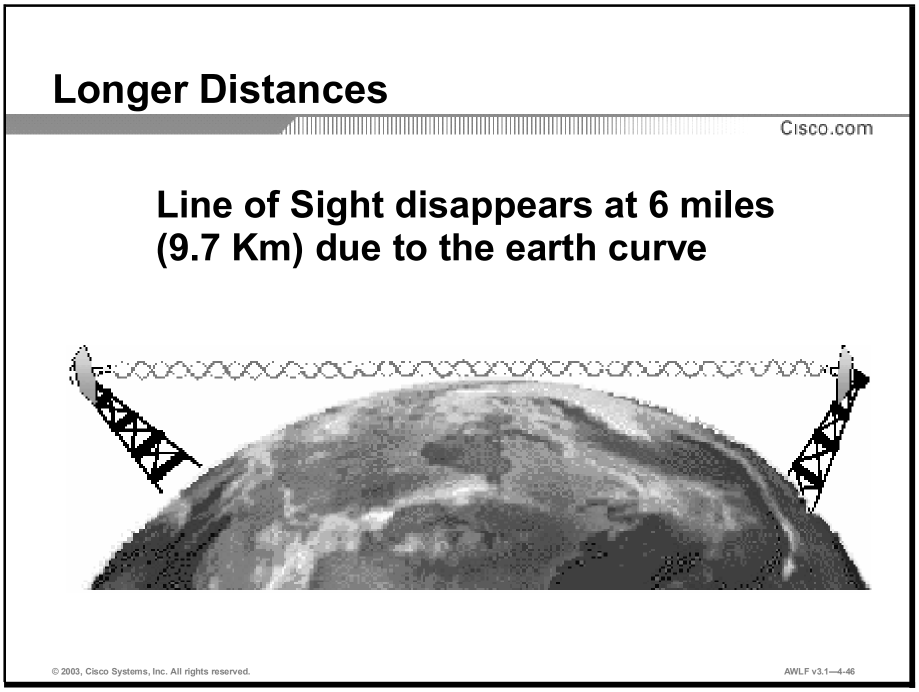
- **Topographic features, such as mountains**
- **Curvature of the Earth**
- **Buildings and other man-made objects**
- **Trees**

Line of sight!

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—4-45

One of the most important concepts for installing Cisco Aironet Bridges is *line of sight*. Cisco Aironet Bridges are unlicensed devices and are not designed to penetrate objects such as mountains, trees, or buildings. The signal will be either absorbed or reflected, and the end result will be that the bridges are unable to connect.

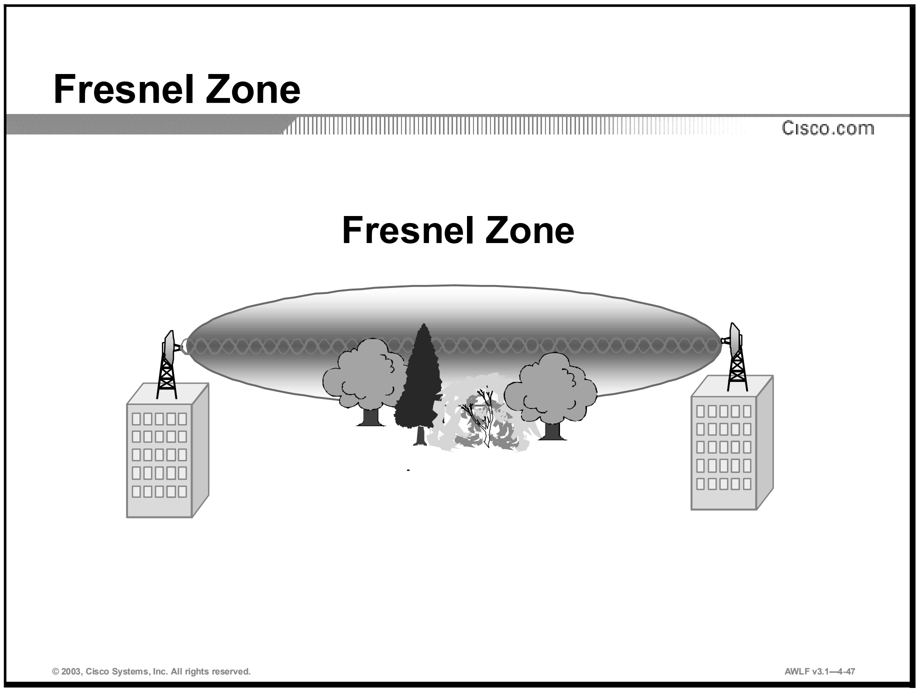


Longer Distances

Line of Sight disappears at 6 miles (9.7 Km) due to the earth curve

AWLF v3.1—4-46

For a typical 6’ (183 cm) person, the horizon appears at about 6 miles (9.7 Km). Disappearance is determined by the height of the observer. If you have two 10’ (305 cm) structures, the top of one will have line of sight to the other at about 16 miles 26 Km), but it will have minimum clearance at the horizon point.



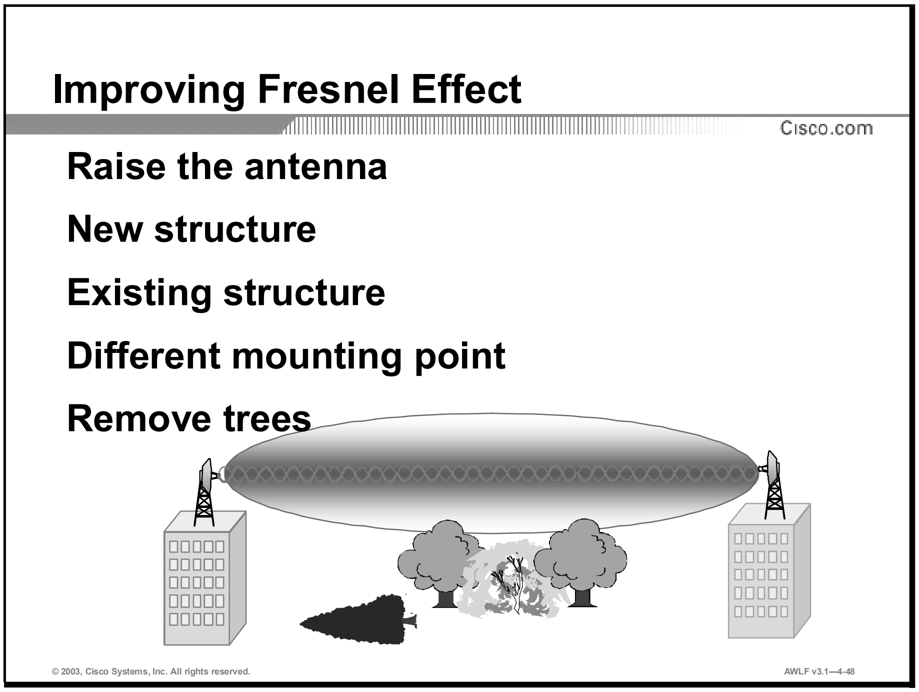
Fresnel Zone

Cisco.com

Fresnel Zone

AWLF v3.1—4-47

The Fresnel zone is an elliptical area immediately surrounding the visual path. It varies depending on the length of the signal path and the frequency of the signal. The Fresnel zone can be calculated, and it must be taken into account when designing a wireless link. If the Fresnel zone is obstructed then there is not the clear line of sight that is required and the link may be unreliable.



Improving Fresnel Effect

Cisco.com

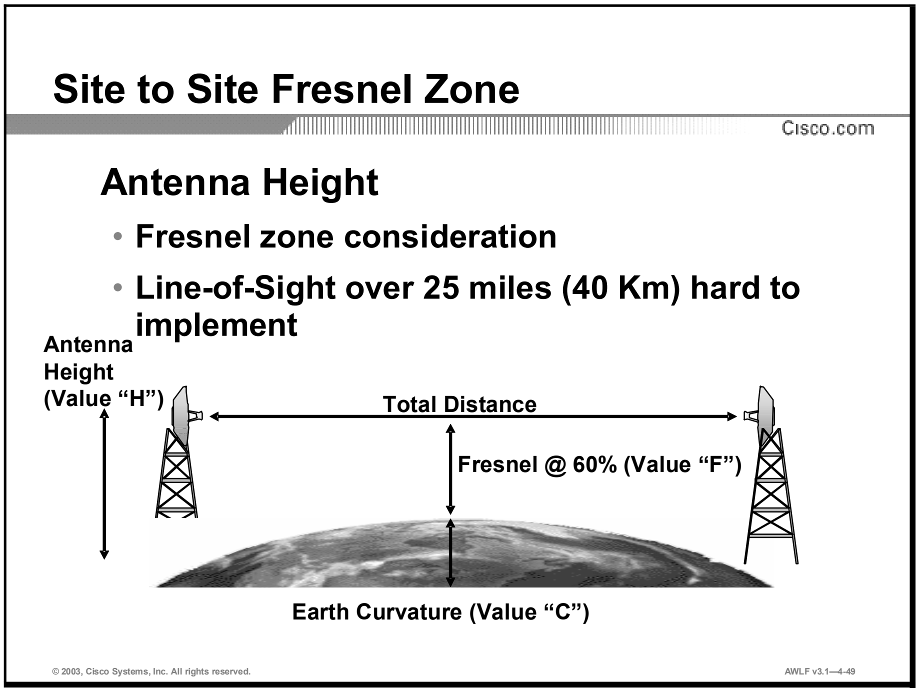
- Raise the antenna
- New structure
- Existing structure
- Different mounting point
- Remove trees

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—4-48

There are a variety of things that can be done to keep the Fresnel zone clear. They include the following:

- Raise the antenna mounting point on the existing structure.
- Build a new structure. For example, a radio tower that is tall enough to mount the antenna.
- Increase the height of an existing tower.
- Locate a different mounting point, for the antenna.
- Cut down problem trees.



Site to Site Fresnel Zone

Cisco.com

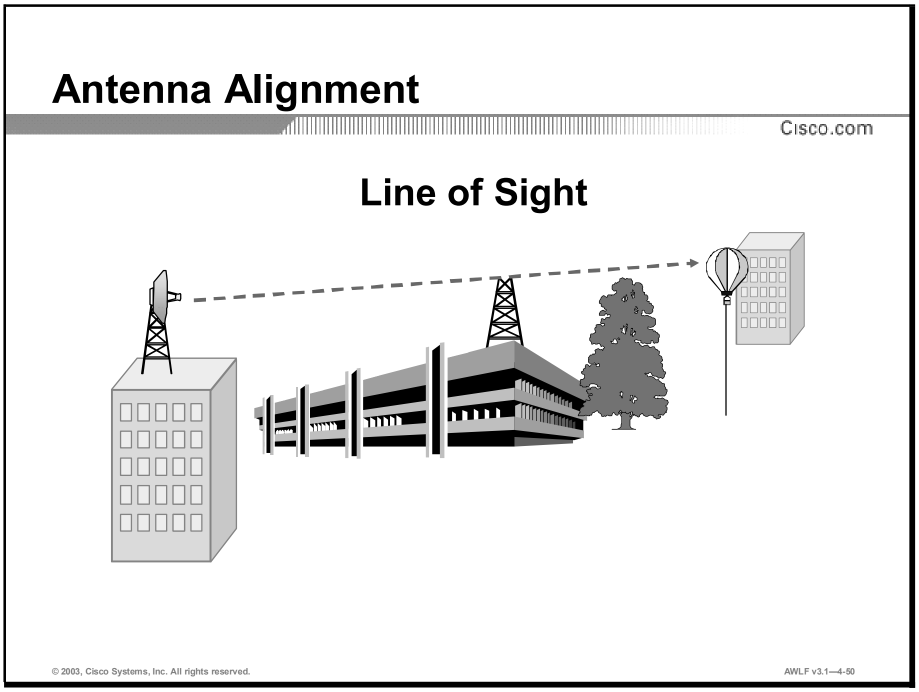
Antenna Height

- Fresnel zone consideration
- Line-of-Sight over 25 miles (40 Km) hard to implement

AWLF v3.1—4-49

The following example illustrates 2.4 GHz bridging. The same concept applies to 5 GHz bridging solutions. In order to determine the antenna mounting height, take the mid-path Fresnel zone width (at 60%) for 2.4 GHz and add it to the curvature of the earth. 60% unobstructed Fresnel Zone clearance is the commonly accepted RF link design coverage. In order to get these measurements, refer to Fresnel Calculation Table below.

Cisco Aironet utility software, Outdoor Bridge Range Calculation Utility, can be found at this link: http://www.cisco.com/application/vnd.ms-excel/en/us/guest/products/ps458/c1225/ccmigration_09186a00800a912a.xls



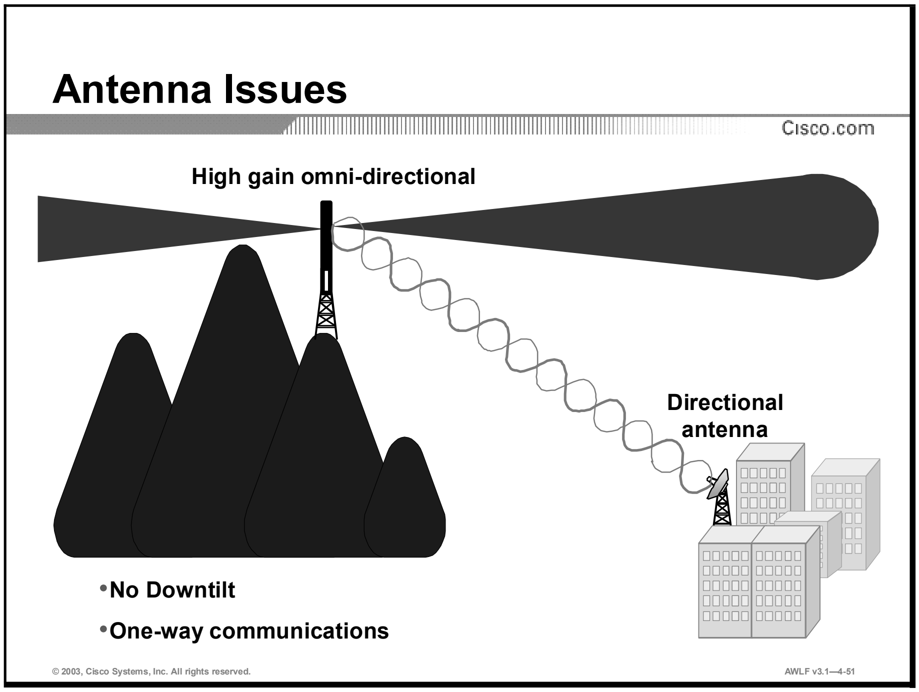
Antenna Alignment

Line of Sight

Verify the radio line of sight, which was previously discussed.

Alignment suggestions:

- Balloon: Attached to a rope marked at ten feet intervals so a height can be established. This figure will determine the overall height of the tower or mast needed.
- Binoculars/telescope: These are needed for the more distant links. Remember the balloon must be visible from the remote site.
- GPS: Used for very distant radio links. This is a tool that will allow the installer to aim the antennas in the correct direction.
- Strobe light: This is used in lieu of the balloon. Use this at night to determine where to align the antenna and at what height.



Antenna Issues

Cisco.com

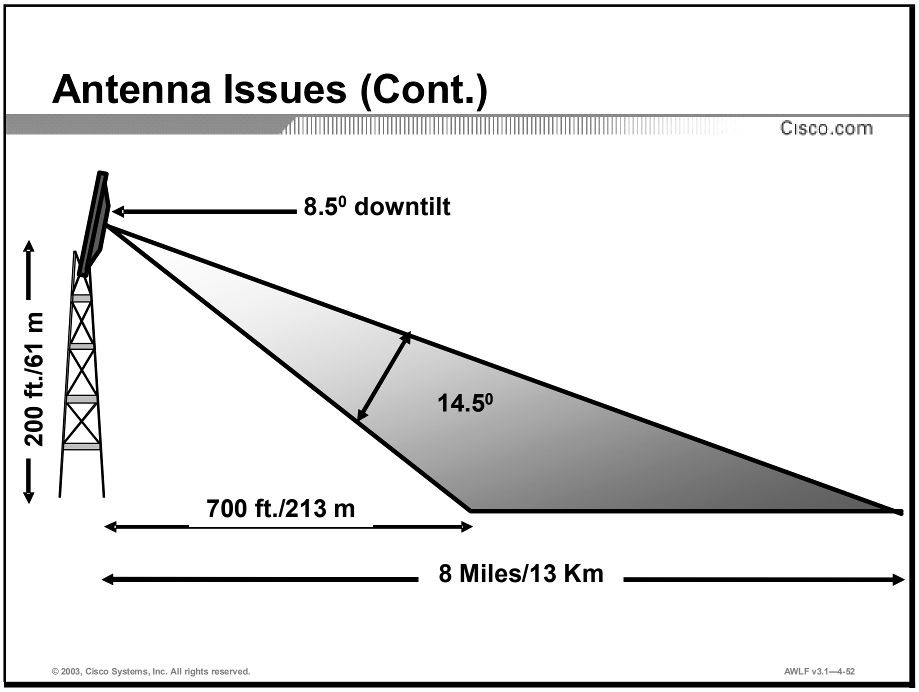
- No Downtilt
- One-way communications

AWLF v3.1—4-51

A common mistake is to use a high-gain omni-directional antenna to try and coverage a large area from a high point. Unfortunately, a high-gain omni-directional antenna may not have any downtilt.

As shown in the figure above, this can result in all of the RF energy being propagated above the desired target, in this case the directional antenna.

This situation is often complicated further by using a directional antenna to establish a link with the high-gain omni-directional antenna. The directional antenna is capable of sending RF traffic to the high-gain omni-directional antenna, but responses cannot be returned to the directional antenna. This results in what appears to be one-way communications.

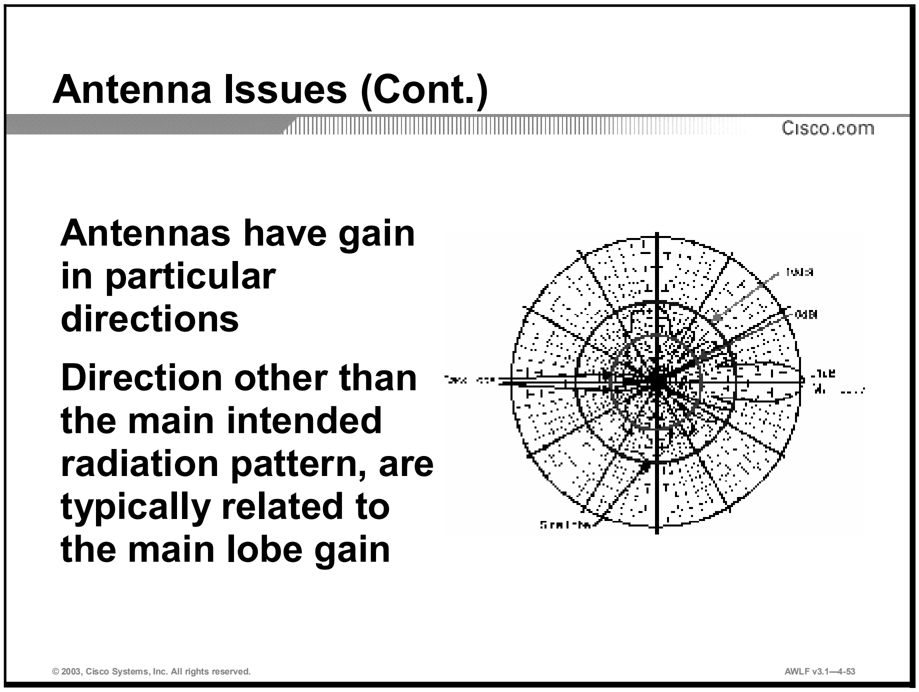


Antenna Issues (Cont.)

AWLF v3.1—4-52

Antennas have both a horizontal and a vertical beamwidths. Some antennas have what is called a “downtilt”, meaning that the beamwidths are manipulated to provide more coverage below the antenna than above the antenna. This can be particularly important in an outdoor installation.

Even though the antenna in the diagram provides some downtilt, there will still potentially be a “dead spot” with no coverage below the tower. The higher the antenna is mounted, the larger this “dead spot” becomes.



Antenna Issues (Cont.)

Cisco.com

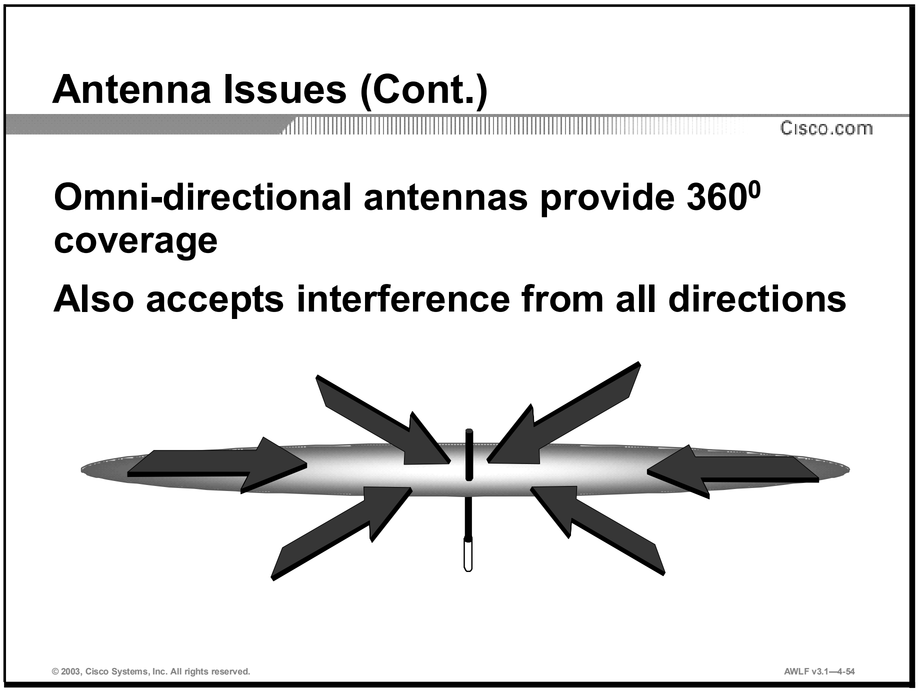
Antennas have gain in particular directions

Direction other than the main intended radiation pattern, are typically related to the main lobe gain

AWLF v3.1—4-53

An antenna may have a gain of 21 dBi, a Front to back ratio of 20 dB or a front to side ratio of 15 dB. This means the gain in the backward direction is 1 dBi, and gain off the side is 6 dBi.

This measurement needs to be taken into account when locating systems on the same channel. There must be sufficient separation of the antennas to insure that the two will not interfere with each other.



Antenna Issues (Cont.)

Cisco.com

Omni-directional antennas provide 360^0 coverage

Also accepts interference from all directions

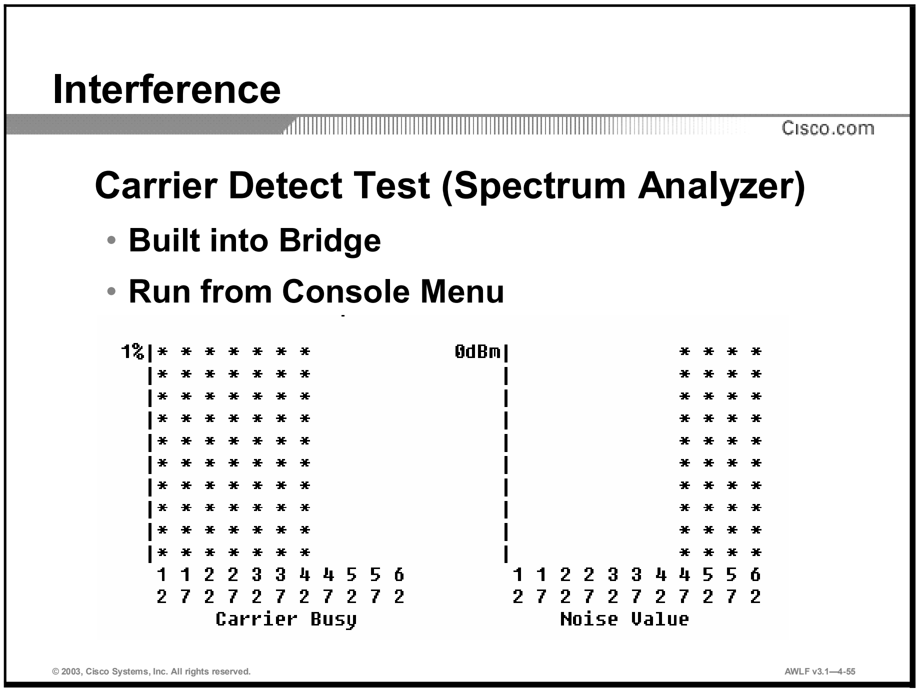
AWLF v3.1—4-54

When deciding which antenna to use as the center antenna (typically the antenna attached to the Root ON device) remembers that antennas will provide coverage in certain directions, but will also receive interference in those directions. This is a much larger issue with an outdoor bridge link because there may be many sources of interference than cannot be removed. More control over interference is afforded in an in-building WLAN installation, where the customer can remove or limit the amount of interference.

Because the bridges are FCC Part 15 products, they must receive all traffic. They cannot block out any traffic. Traffic that is not meant for the bridge will be discarded, but can slow down the bridge.

Often omni directional antennas are chosen for a center site in a point-to-multipoint installation. If 360-coverage is not needed, a more directional antenna (such as a patch antenna) may be a better choice. First, determine the maximum beamwidth that the antenna will need to produce a coverage cell that will contain all of the other devices. An antenna should then be chosen that would match this beamwidth as closely as possible. This will minimize the amount of interference received and maximize bridge performance.

Remember that even directional antennas will have some back and side lobes that will be susceptible to interference as well.



Interference

Cisco.com

Carrier Detect Test (Spectrum Analyzer)

- Built into Bridge
- Run from Console Menu

```
1%|* * * * * * *             0dBm|              * * * *
  |* * * * * * *                 |              * * * *
  |* * * * * * *                 |              * * * *
  |* * * * * * *                 |              * * * *
  |* * * * * * *                 |              * * * *
  |* * * * * * *                 |              * * * *
  |* * * * * * *                 |              * * * *
  |* * * * * * *                 |              * * * *
  |* * * * * * *                 |              * * * *
  |* * * * * * *                 |              * * * *
   1 1 2 2 3 3 4 4 5 5 6          1 1 2 2 3 3 4 4 5 5 6
   2 7 2 7 2 7 2 7 2 7 2          2 7 2 7 2 7 2 7 2 7 2
        Carrier Busy                  Noise Value
```

AWLF v3.1—4-55

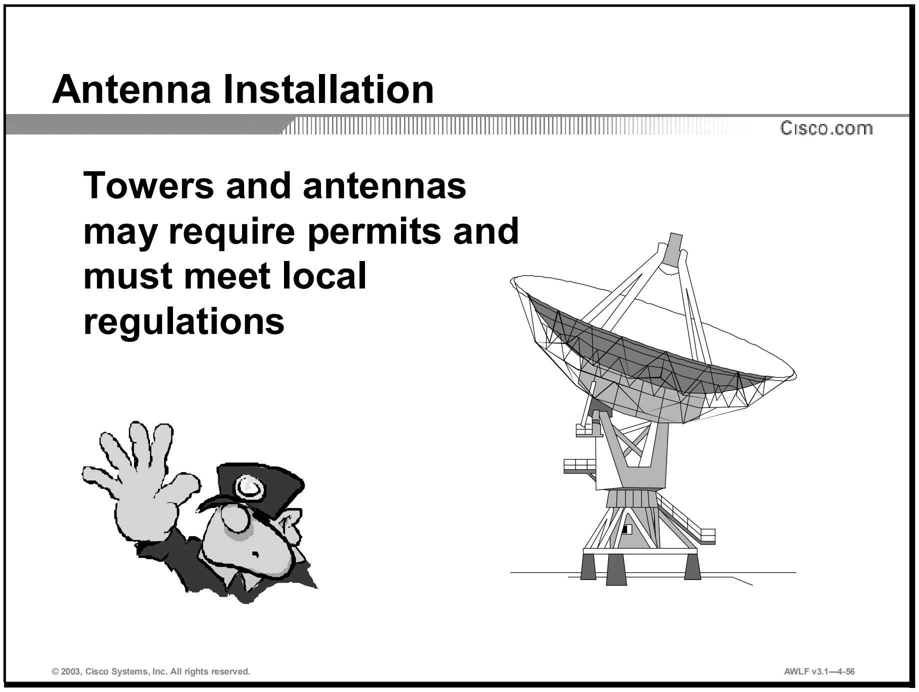
When trying to evaluate the interference you can use the Carrier Detect Test on the bridge. This function is built into both the access points and bridges. This utility will listen for RF energy throughout the 2.4 GHz band. The results are then displayed on the screen as shown in the figure.

The Carrier Busy shows percent usage on each of the available channels and is read vertically. Each set of numbers (12, 17, 22, etc.) represents a channel. For example, 12 represent the center frequency of channel 1, 2412 MHz, or 2.412 GHz.

The Carrier Busy value is read by observing the highest value (represented by asterisks) on the chart. To the left of the chart will be a percentage value. This percentage value represents the highest percentage usage of any channel. All other channels are in relation to this percentage. In the diagram, the percentage is 1%. Therefore all other values are less than 1%.

The Noise Value chart is read in the same manner. The highest asterisk value represents that maximum noise level, and all other are read in relation to that value. In the diagram, this value is 0 dBm.

Note The access point or bridge will not support clients while in this mode. Any clients connected to the access point when the test begins will be disconnected.



Antenna Installation

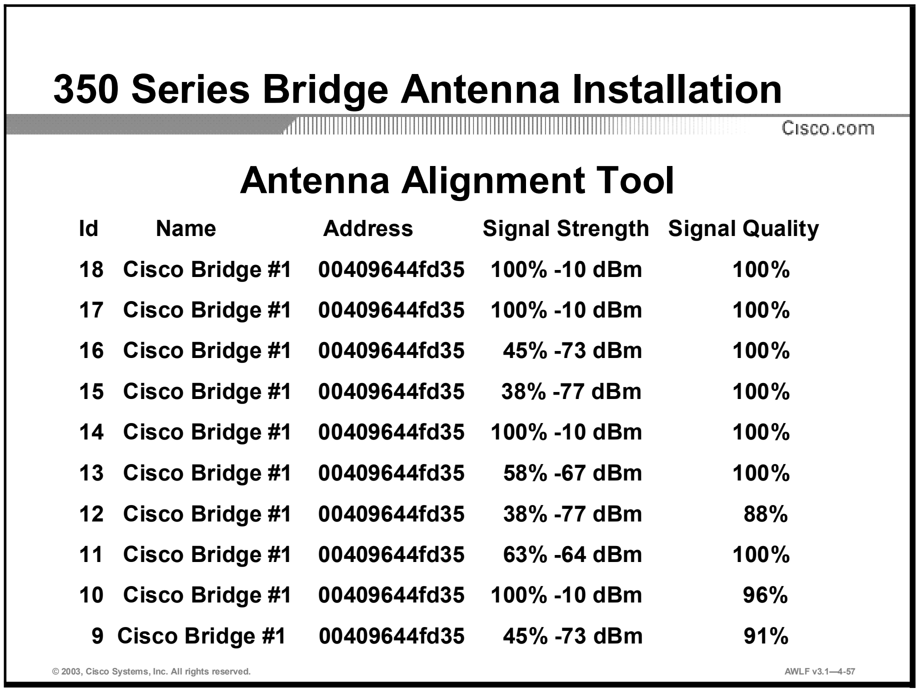
Cisco.com

Towers and antennas may require permits and must meet local regulations

AWLF v3.1—4-56

Restrictions

When dealing with tall structures and tower installations, the codes and laws of each city/municipality may vary. A building permit to install towers or masts may be required depending upon height.



350 Series Bridge Antenna Installation

Cisco.com

Antenna Alignment Tool

Id	Name	Address	Signal Strength	Signal Quality
18	Cisco Bridge #1	00409644fd35	100% -10 dBm	100%
17	Cisco Bridge #1	00409644fd35	100% -10 dBm	100%
16	Cisco Bridge #1	00409644fd35	45% -73 dBm	100%
15	Cisco Bridge #1	00409644fd35	38% -77 dBm	100%
14	Cisco Bridge #1	00409644fd35	100% -10 dBm	100%
13	Cisco Bridge #1	00409644fd35	58% -67 dBm	100%
12	Cisco Bridge #1	00409644fd35	38% -77 dBm	88%
11	Cisco Bridge #1	00409644fd35	63% -64 dBm	100%
10	Cisco Bridge #1	00409644fd35	100% -10 dBm	96%
9	Cisco Bridge #1	00409644fd35	45% -73 dBm	91%

AWLF v3.1—4-57

The Cisco Aironet Bridge also contains a utility to assist in the alignment of the antennas between two bridges. The antenna alignment utility will report back the following results:

- Bridge Name
- MAC Address
- Signal Strength
- Signal Quality

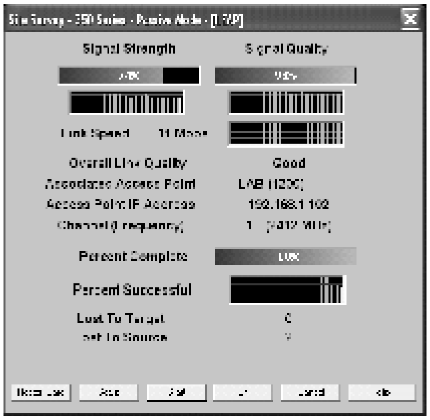
This allows the installer to connect to a bridge, start the utility, and then make adjustments to the antenna to obtain the best results and the best link possible. The installer should be connected to the bridge via serial cable or Ethernet while running this test.

350 Series Bridge Antenna Installation (Cont.)

Cisco.com

Aironet Client Utility

Site Survey Utility for antenna alignment



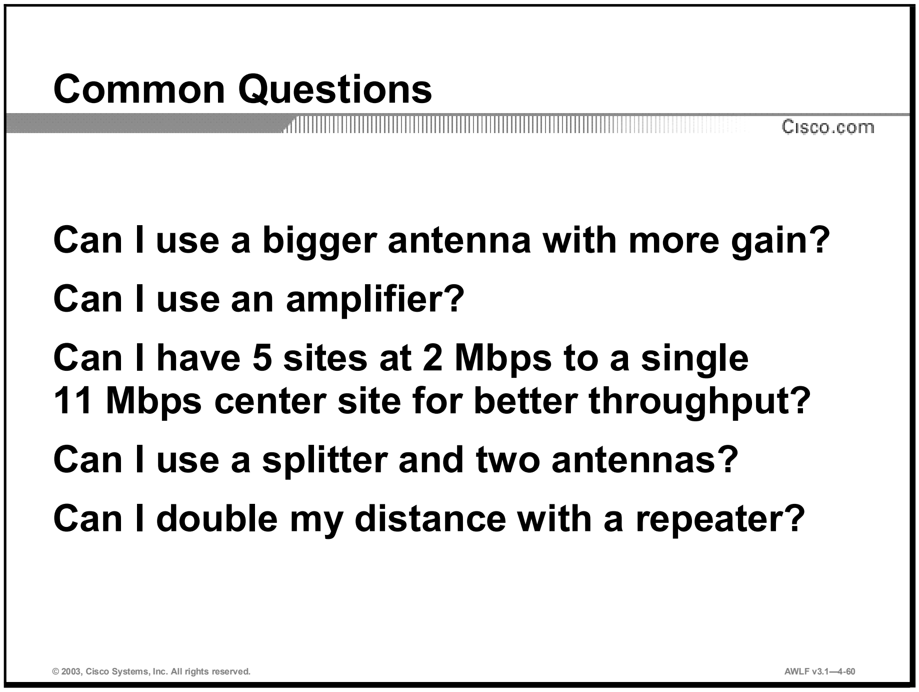
Link Speed 11 Mbps
Overall Link Quality Good
Associated Access Point LAB (1200)
Access Point IP Address 192.168.1.102
Channel (Frequency) 1 (2412 MHz)
Lost To Target 0
Lost To Source 0

AWLF v3.1—4-58

Another method of alignment is to use a laptop configured with a PC card and attached to the same antenna that the bridge will be using (a Yagi for example). Included with every client card is Cisco’s Aironet Client Utility, software that can be used to monitor the link between a client card and an access point or bridge. Because the radio in the client card is the exact same as the radio in the bridge, the utility can be used to assess the link and align bridge antennas.

The Aironet Client Utility will be examined and explained in a later module.

Common Questions and Misconceptions



Common Questions

Cisco.com

Can I use a bigger antenna with more gain?

Can I use an amplifier?

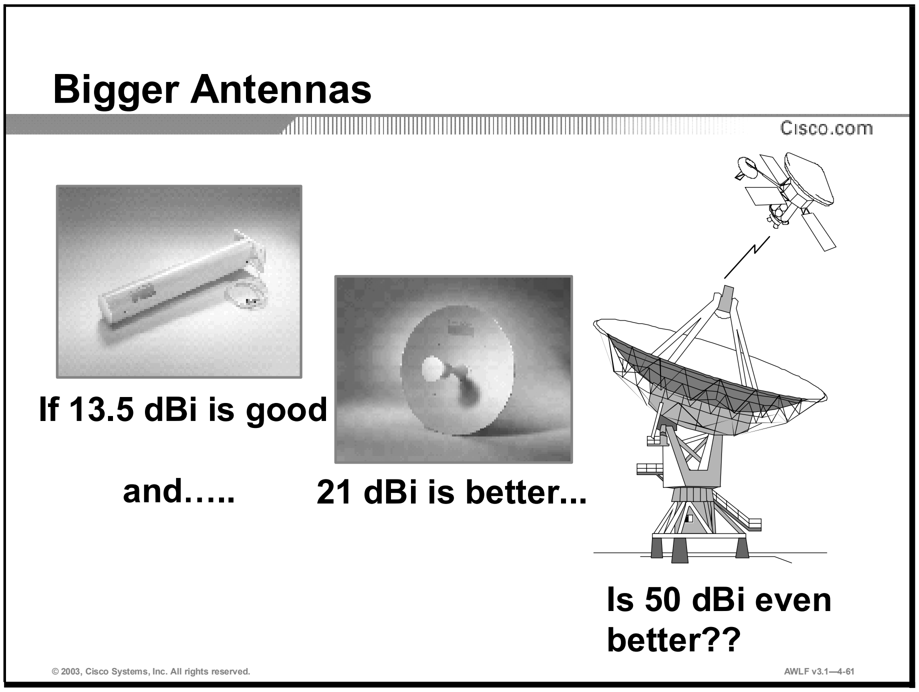
Can I have 5 sites at 2 Mbps to a single
11 Mbps center site for better throughput?

Can I use a splitter and two antennas?

Can I double my distance with a repeater?

AWLF v3.1—4-60

Listed in the slide are the most common questions when it comes to obtaining more coverage distance. The answers require a small explanation of the advantages or drawbacks of each.



Bigger Antennas

Cisco.com

If 13.5 dBi is good

and…..

21 dBi is better...

Is 50 dBi even better??

AWLF v3.1—4-61

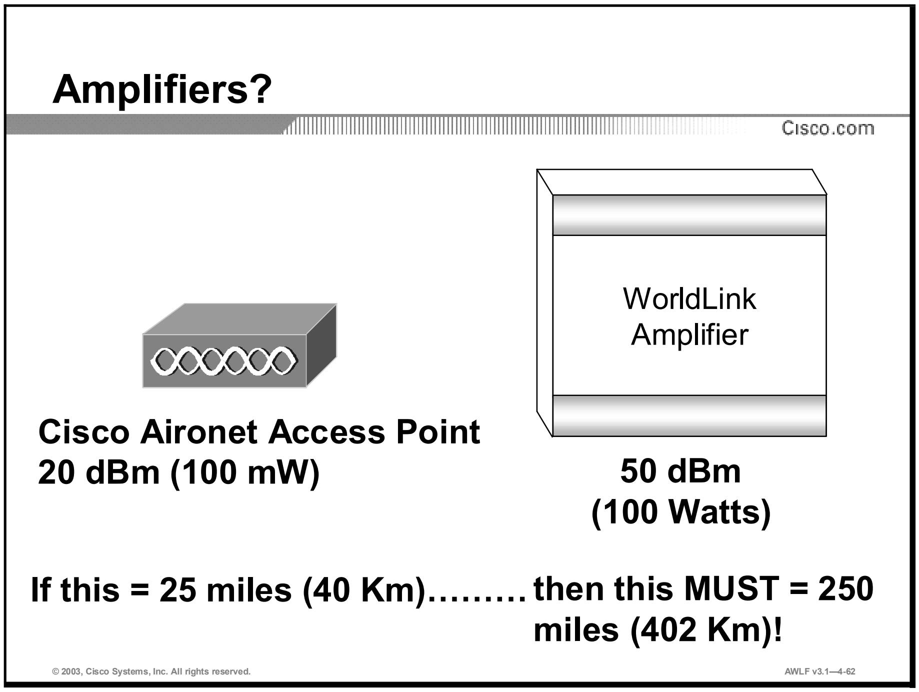
In Point-to-Multipoint systems, the FCC has limited the maximum EIRP (effective radiated power) in the 900 MHz, 2.4 GHz and 5.7 GHz spread spectrum bands to 36 dBm.

EIRP = transmit power + antenna gain.

At 2.4 GHz, Cisco Aironet’s transmitter power is 20 dBm, so the largest antenna gain allowable is 16 dBi.

Under the “Professional Installer” clause, a trained installer may attach antennas with higher gain, if it is verified that the system is operating within the FCC rules and guidelines, but only if:

- Antenna gain + transmitter power + cable losses is greater than or equal to 36 dBm.
- In Point-to-Point system for 2.4 GHz system, using directional antennas the rules are changed. It has a 3:1 ratio for additional antenna gain (over 6 dBi) compared to TX power reduction.
- At 30 dBm TX power, a 6-dBi antenna is still the max.
- At 27 dBm TX power, (-3 dB) the antenna can be 9 dB above the initial 6, or 15 dBi.
- At 24 dBm TX power, it would be possible to use a 24 dBi antenna.



Amplifiers?

WorldLink
Amplifier

Cisco Aironet Access Point
20 dBm (100 mW)

50 dBm
(100 Watts)

If this = 25 miles (40 Km)……… then this MUST = 250 miles (402 Km)!

AWLF v3.1—4-62

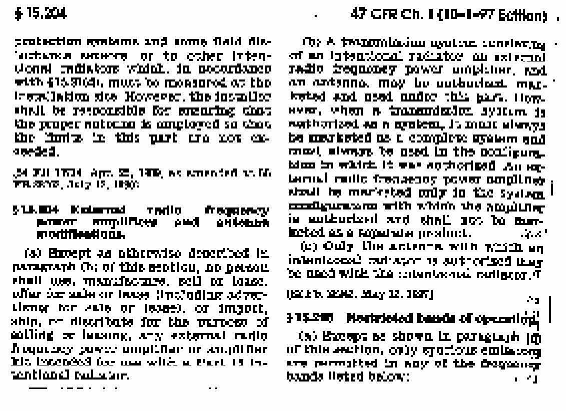
Under the FCC’s rules, amplifiers are typically not permitted.

Remember, each country will have its own maximum EIRP value. For the US, this is 36 dBm. Below is a list of the equivalent dBm (decibels per milliwatt) for each of the available power levels on the Cisco Aironet Bridges:

- 100 mW = 20 dBm
- 50 mW = 17 dBm
- 30 mW = 15 dBm
- 20 mW = 13 dBm
- 15 mW = 12 dBm
- 5 mW = 7 dBm
- 1 mW = 0 dBm

Amplifiers and the FCC

Cisco.com



§ 15.204 47 CFR Ch. I (10–1–97 Edition)

protection systems and some field disturbance sensors, or to other intentional radiators which, in accordance with §15.31(d), must be measured at the installation site. However, the installer shall be responsible for ensuring that the proper antenna is employed so that the limits in this part are not exceeded.

[54 FR 17714, Apr. 25, 1989, as amended at 55 FR 28762, July 13, 1990]

§15.204 External radio frequency power amplifiers and antenna modifications.

(a) Except as otherwise described in paragraph (b) of this section, no person shall use, manufacture, sell or lease, offer for sale or lease (including advertising for sale or lease), or import, ship, or distribute for the purpose of selling or leasing, any external radio frequency power amplifier or amplifier kit intended for use with a Part 15 intentional radiator.

(b) A transmission system consisting of an intentional radiator, an external radio frequency power amplifier, and an antenna, may be authorized, marketed and used under this part. However, when a transmission system is authorized as a system, it must always be marketed as a complete system and must always be used in the configuration in which it was authorized. An external radio frequency power amplifier shall be marketed only in the system configuration with which the amplifier is authorized and shall not be marketed as a separate product.

(c) Only the antenna with which an intentional radiator is authorized may be used with the intentional radiator.

[62 FR 26242, May 12, 1997]

§15.205 Restricted bands of operation.

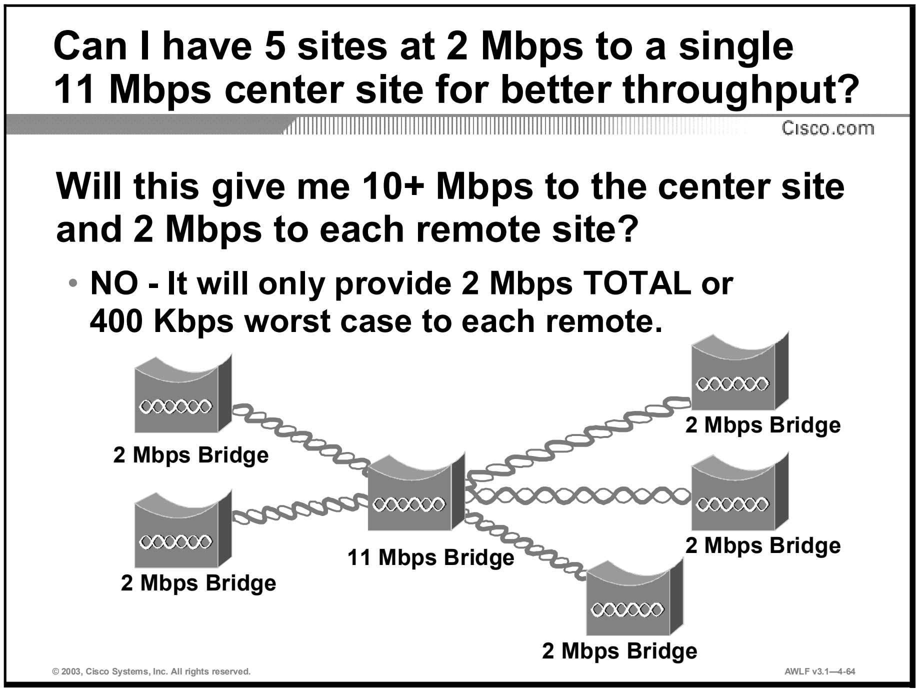
(a) Except as shown in paragraph (d) of this section, only spurious emissions are permitted in any of the frequency bands listed below:

AWLF v3.1—4-63

The FCC rules state:

- **Section 15.204(b):** External radio frequency power amplifiers shall not be marketed as separate products.
- **Section 15.204(c):** Only the antenna with which an intentional radiator (transmitter) is originally authorized may be used with the intentional radiator.

This means that unless the amplifier manufacturer submits the amplifier for testing with the radio and antenna, is not allowed to be sold in the US.



Can I have 5 sites at 2 Mbps to a single 11 Mbps center site for better throughput?

Will this give me 10+ Mbps to the center site and 2 Mbps to each remote site?

- **NO - It will only provide 2 Mbps TOTAL or 400 Kbps worst case to each remote.**

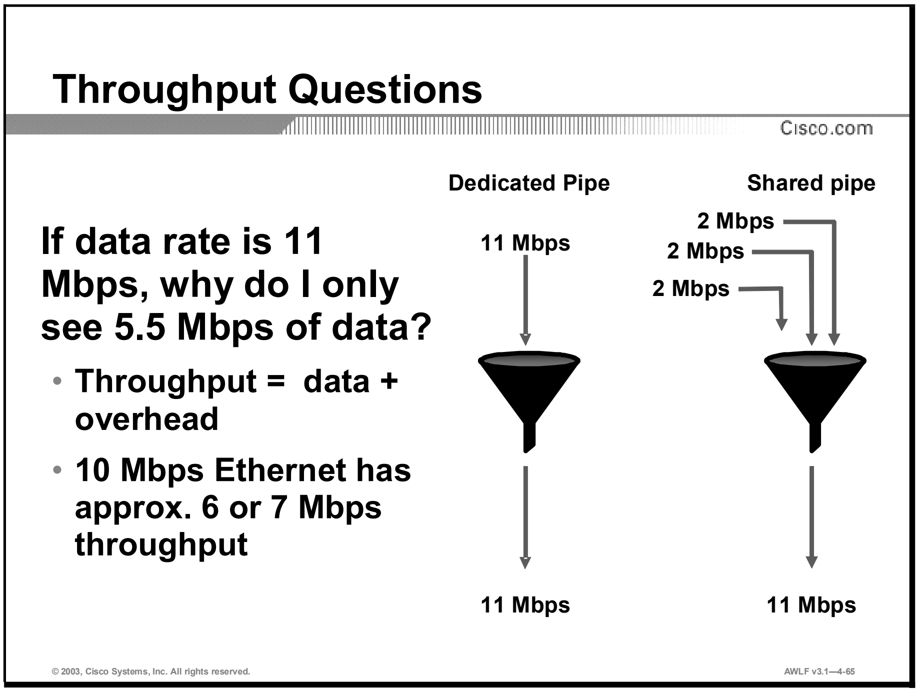
AWLF v3.1—4-64

Many people think that the 11 Mbps product will support many 2 Mbps radios and provide a total (aggregate) data rate of 11 Mbps, with each unit getting a full 2 Mbps. The problem is that the 2 Mbps units transmit at 2 Mbps, taking 5 times as long to transmit the same data as an 11 Mbps product would. This means the data rate is only 2 Mbps for any given remote, and the total the 11 Mbps unit sees is still 2 Mbps.

In order to achieve a total aggregate 11 Mbps data rate, everyone will have to be set to 11 Mbps. If a single unit is less than 11 Mbps, the overall rate will be somewhat less than 11, as the base or central unit has to service the slower remote.

As a reminder:

- If everyone is operating at the same data rate, they will all take the same amount of time to send the same size packets.
- If some people are operating at higher speeds, then they will transmit the packet faster, which will allow the RF to be available quicker for the next person waiting to send some data.
- But if in an attempt to REDUCE throughput to a given party by lowering the bridge speed, this will also affect the high-speed bridges!



Throughput Questions

Cisco.com

If data rate is 11 Mbps, why do I only see 5.5 Mbps of data?

- Throughput = data + overhead
- 10 Mbps Ethernet has approx. 6 or 7 Mbps throughput

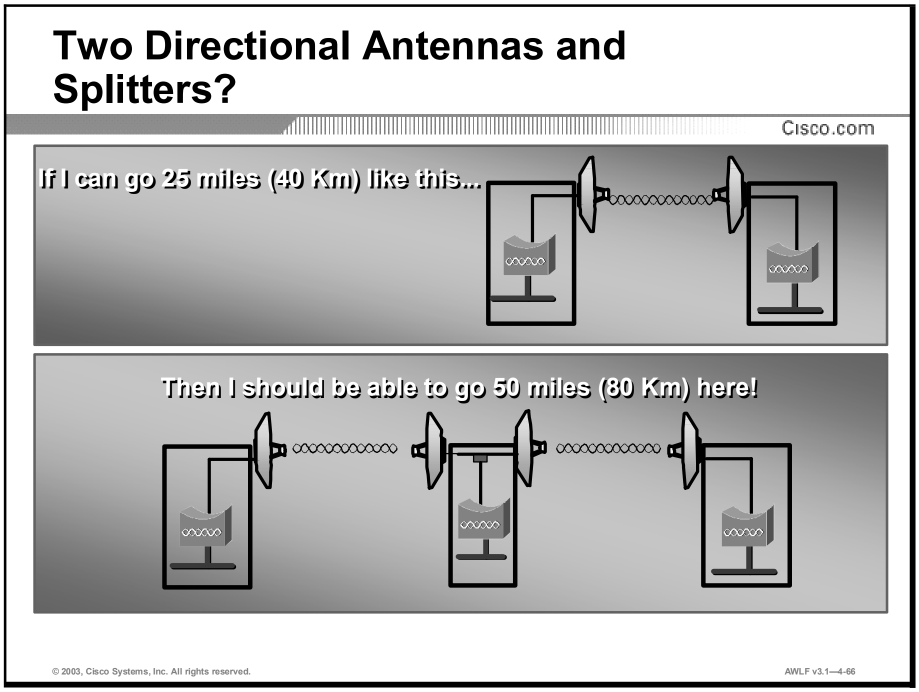
Dedicated Pipe
11 Mbps
11 Mbps
Shared pipe
2 Mbps
2 Mbps
2 Mbps
11 Mbps

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—4-65

- **Throughput:** The amount of USER data correctly transported, by the media, over a data network per unit of time, in this case, the wireless devices.
- **True throughput vs. pipe itself:** Data rate is the amount of all data that the media can pass. This includes overhead packets such as ACKs, association packets, retries, etc. Throughput is typically 50 to 60% of the data rate for a wireless system.
- **Dedicated pipes vs. shared pipes:** A point-to-point bridge configuration is an example of a dedicated pipe. If the RF link is set to 11 Mbps then the data throughput between those sites is 11 Mbps.

A shared pipe consists of a point-to-multipoint RF network. If the RF link is set to 11 Mbps, all the remote sites share that 11 Mbps pipe. This sharing can be compared to the sharing of an Ethernet segment. When there are multiple Ethernet devices on a wired segment they share the pipe they reside on. The more you add to the pipe the slower the overall throughput.



Two Directional Antennas and Splitters?

Cisco.com

If I can go 25 miles (40 Km) like this...

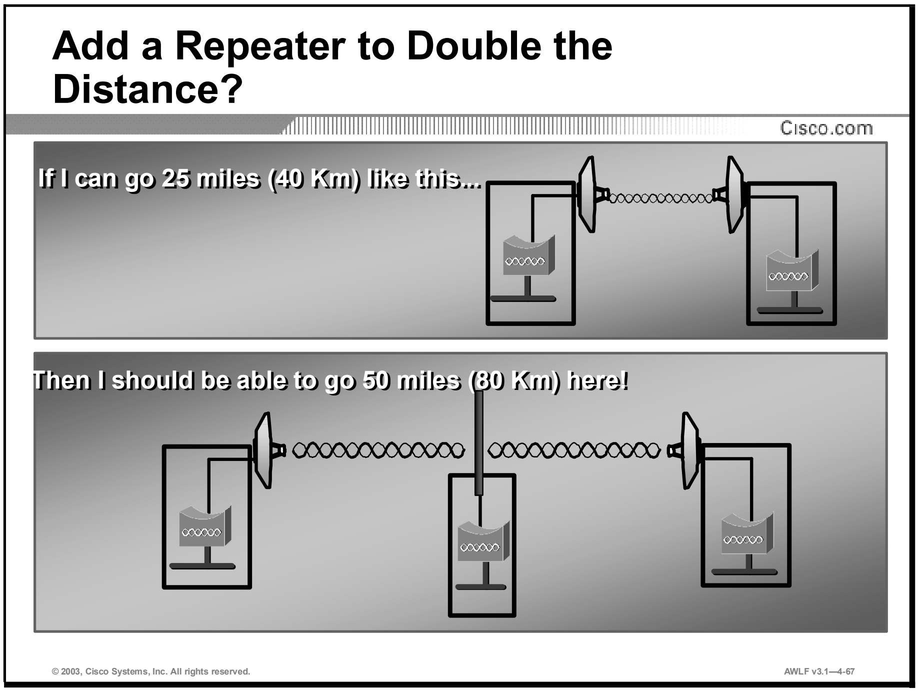
Then I should be able to go 50 miles (80 Km) here!

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—4-66

The use of splitters usually adds a loss of about 4 dB (for a good quality splitter) to the system. This loss is seen at both antennas (each antenna suffers a 4 dB loss). At 2.4 GHz, it reduces the gain of a dish from 21 to 17 dBi providing some distance advantage, but not double. By reducing the gain on one antenna to 17 dBi, the distance drops from 20.5 miles, or 33 Km (at 11 Mbps) to approximately 13 miles, or 21 Km.

A second drawback is that the throughput is reduced by approximately 50% because the repeater must receive, buffer, and transmit the data.



Add a Repeater to Double the Distance?

If I can go 25 miles (40 Km) like this...

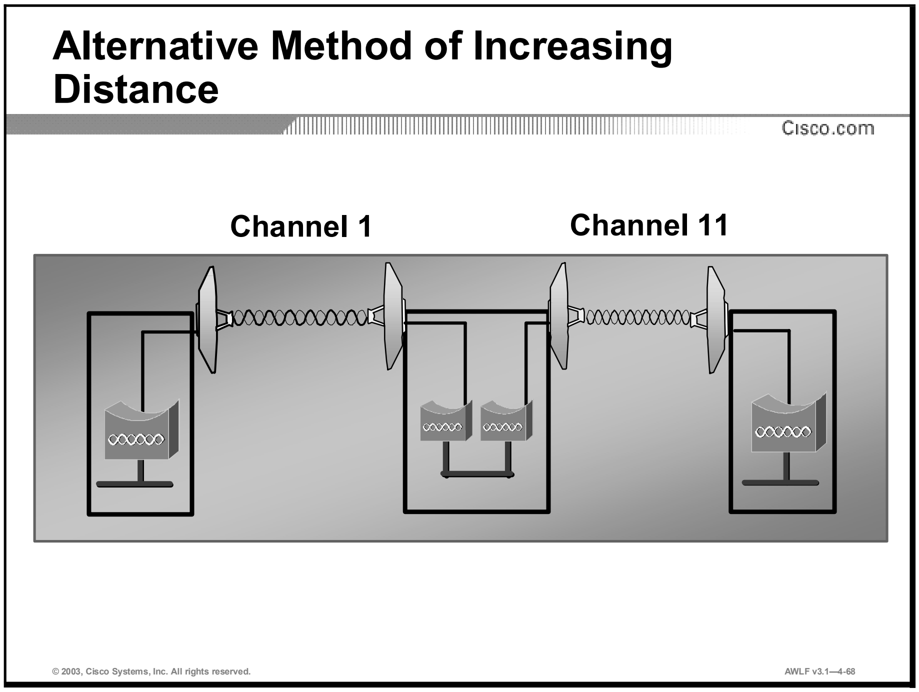
Then I should be able to go 50 miles (80 Km) here!

AWLF v3.1—4-67

A repeater can be added to extend the range of a bridge, but not double it. As a repeater, it needs to receive and transmit in more than one direction. Therefore, Yagis typically cannot be used. In such a situation an omni-directional or semi-directional (panel or patch) antenna would be employed, and they are less effective than a link using two directional antennas.

Using the high-gain omni-directional antenna shown in the figure above would only result in a link of just over seven miles.

And again, the throughput is reduced by approximately 50% because the repeater must receive, buffer, and transmit the data.



Alternative Method of Increasing Distance

Cisco.com

Channel 1

Channel 11

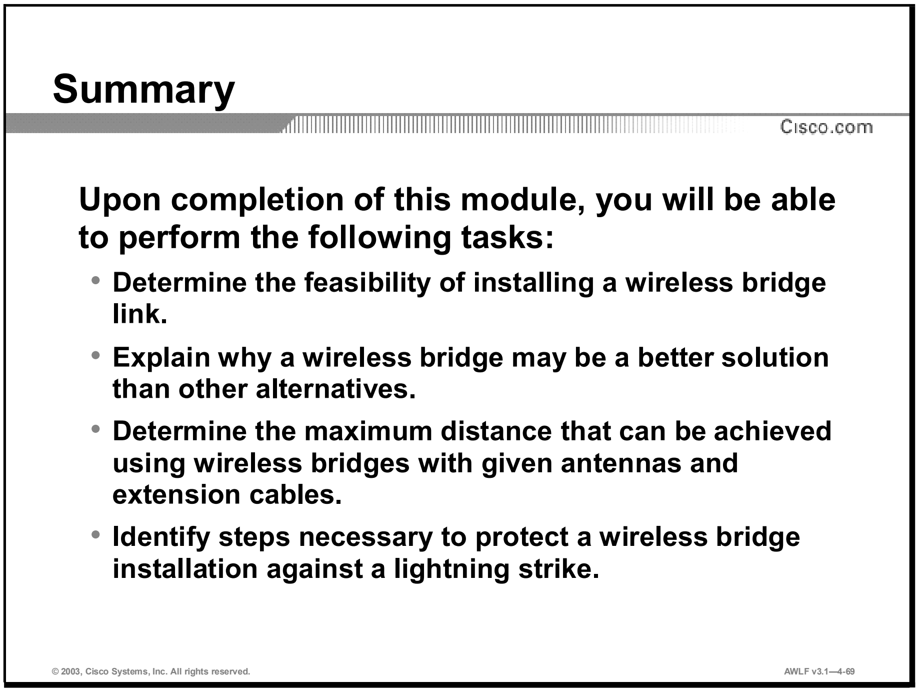
AWLF v3.1—4-68

A better way to increase distance is through the use of a linked repeater site. This site consists of two bridges and two antennas, operating on two different channels and system set identifiers (SSID). This allows both sides to the link to operate simultaneously at full gain and full throughput.

The drawback to this is that it requires one extra bridge and antenna, and a loss in throughput of about 15% due to Ethernet latency.

Summary

This section summarizes the concepts you learned in this module.



Summary

Cisco.com

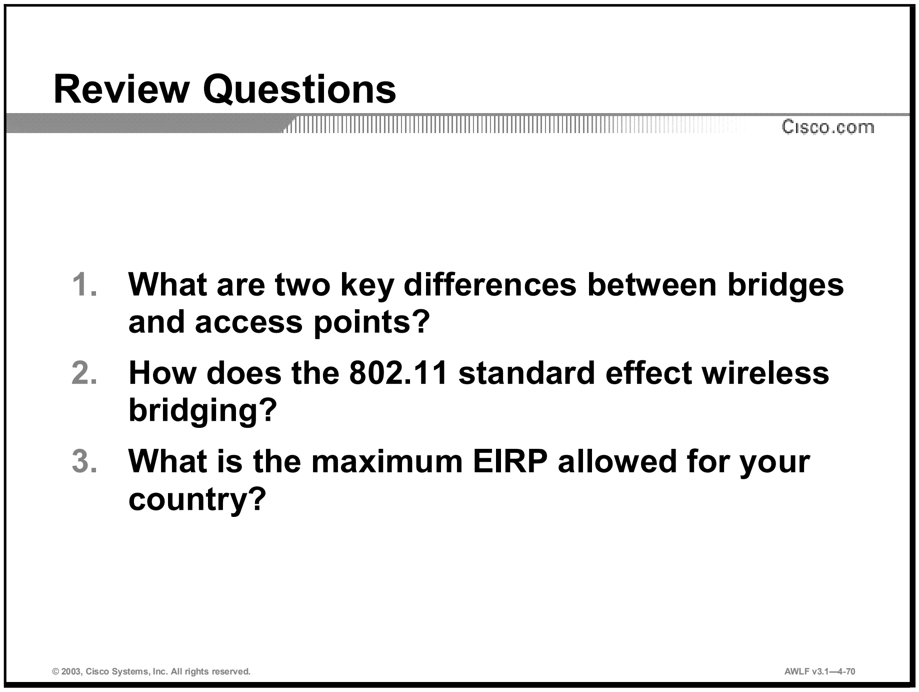
Upon completion of this module, you will be able to perform the following tasks:

- **Determine the feasibility of installing a wireless bridge link.**
- **Explain why a wireless bridge may be a better solution than other alternatives.**
- **Determine the maximum distance that can be achieved using wireless bridges with given antennas and extension cables.**
- **Identify steps necessary to protect a wireless bridge installation against a lightning strike.**

Upon completion of this module, you will be able to perform the following tasks:

- Determine the feasibility of installing a wireless bridge link.
- Explain why a wireless bridge may be a better solution than other alternatives.
- Determine the maximum distance that can be achieved using wireless bridges with given antennas and extension cables.
- Identify steps necessary to protect a wireless bridge installation against a lightning strike.

Review Questions



Review Questions

1. What are two key differences between bridges and access points?
2. How does the 802.11 standard effect wireless bridging?
3. What is the maximum EIRP allowed for your country?

AWLF v3.1—4-70

Answer these review questions.

Module 5

Cisco Aironet Wireless LAN Products

Overview

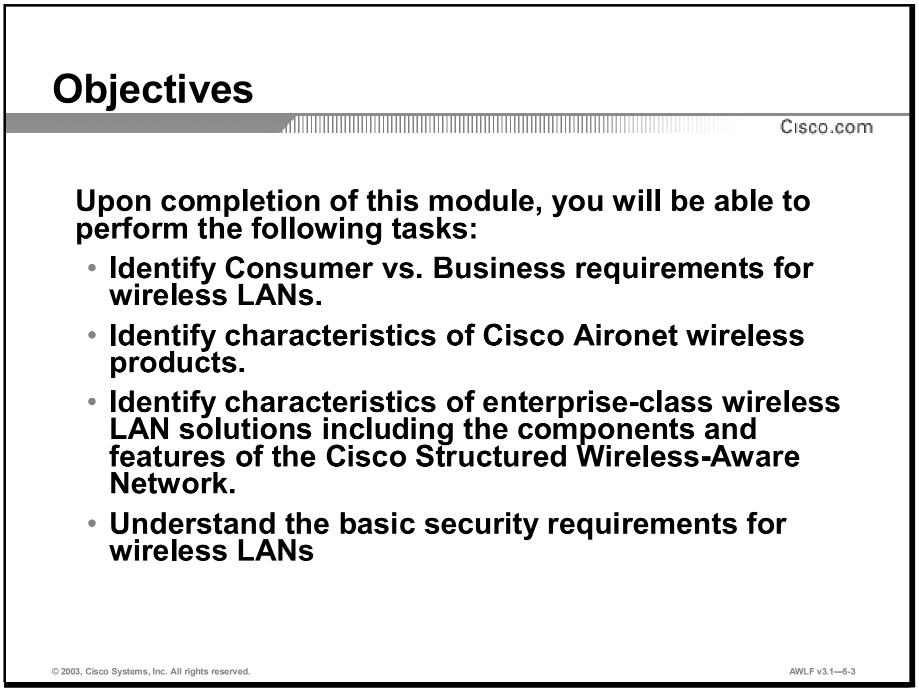
This module is an overview of the Cisco Aironet Wireless product offerings.

It includes the following topics:

- Objectives
- WLAN Products
- Cisco Aironet WLAN Product Line
- Structured Wireless-Aware Network
- Enterprise-Class WLAN Security
- Summary
- Review Questions

Objectives

This section lists the module's objectives.



Objectives

Upon completion of this module, you will be able to perform the following tasks:

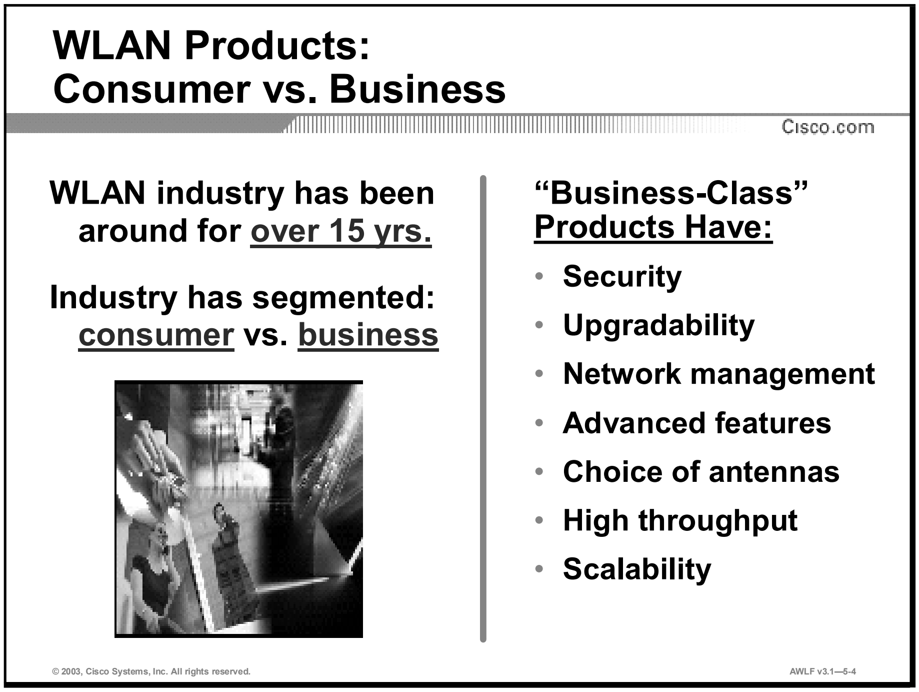
- **Identify Consumer vs. Business requirements for wireless LANs.**
- **Identify characteristics of Cisco Aironet wireless products.**
- **Identify characteristics of enterprise-class wireless LAN solutions including the components and features of the Cisco Structured Wireless-Aware Network.**
- **Understand the basic security requirements for wireless LANs**

AWLF v3.1—5-3

Upon completion of this module, you will be able to perform the following tasks:

- Identify Consumer vs. Business requirements for wireless LANs.
- Identify characteristics of Cisco Aironet products including Access Points, Clients, Bridges, Workgroup Bridges, Antennas, and Power Injectors.
- Identify characteristics of an Enterprise-Class WLAN Solutions including the components and features of the Cisco Structured Wireless-Aware Network.
- Understand the basic security requirements for wireless LANs

WLAN Products



WLAN Products: Consumer vs. Business

Cisco.com

WLAN industry has been around for over 15 yrs.

Industry has segmented: consumer vs. business

"Business-Class" Products Have:

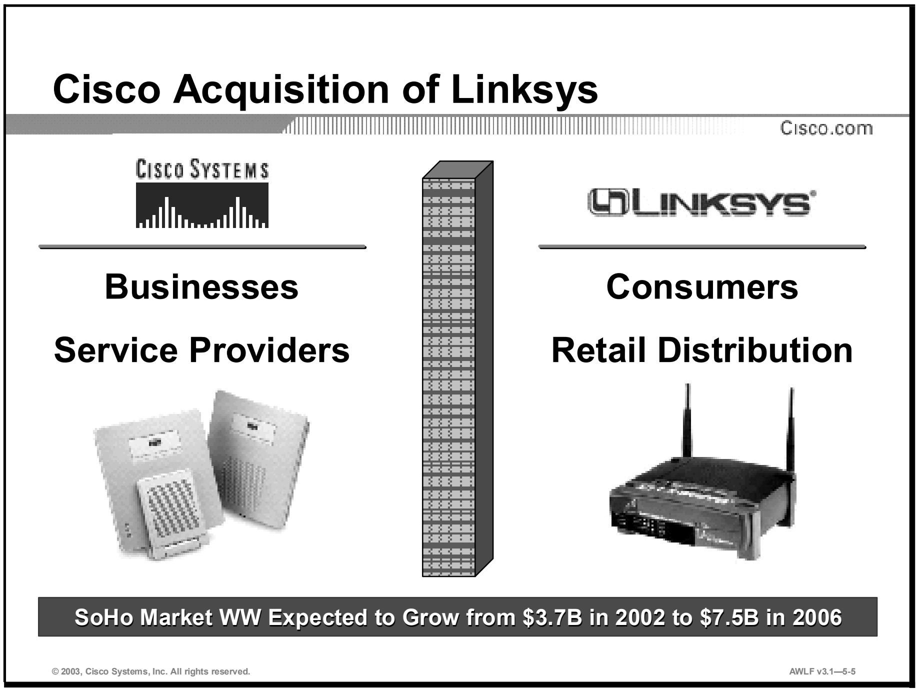
- Security
- Upgradability
- Network management
- Advanced features
- Choice of antennas
- High throughput
- Scalability

© 2003, Cisco Systems, Inc. All rights reserved. AWLF v3.1—5-4

Where WLAN market is today:

- Mature Standard
- Interoperability
- Deployed today
- Proven ROI
- Migration path to higher performance

More than just a line of wireless access points, bridges, adapters, and accessories, the Cisco Aironet family reflects Cisco's end-to-end approach to networking solutions, allowing organizations to leverage their wired infrastructure and extend intelligent services to wireless access points. Cisco's structured wireless LAN architecture delivers performance, scalability, manageability, and security to companies in an easy-to-deploy solution. The architecture, including the Cisco Aironet 1100 and 1200 Series Access Points, provides distributed intelligence and enterprise-class services such as VLANs, QoS, and proxy mobile IP. The result is a unique combination of enterprise-class features that allow organizations to segment wireless networks, prioritize wireless traffic, provide seamless connectivity across multiple wireless subnets, and bolster wireless LAN security to block intruders and safeguard transmitted data.



Cisco Acquisition of Linksys

Cisco.com

Cisco Systems

Linksys®

Cisco Systems	Linksys
Businesses	Consumers
Service Providers	Retail Distribution

SoHo Market WW Expected to Grow from $3.7B in 2002 to $7.5B in 2006

AWLF v3.1—5-5

Aironet Target Markets

- SMB, Enterprise, SP

Aironet Key Features

- Security options (LEAP, PEAP, EAP-TLS, VPN)
- Security policy management
- Managed infrastructure
- IOS-based advanced features (e.g. QoS, VLANs, fast roaming, etc.)
- Cisco Service & Support

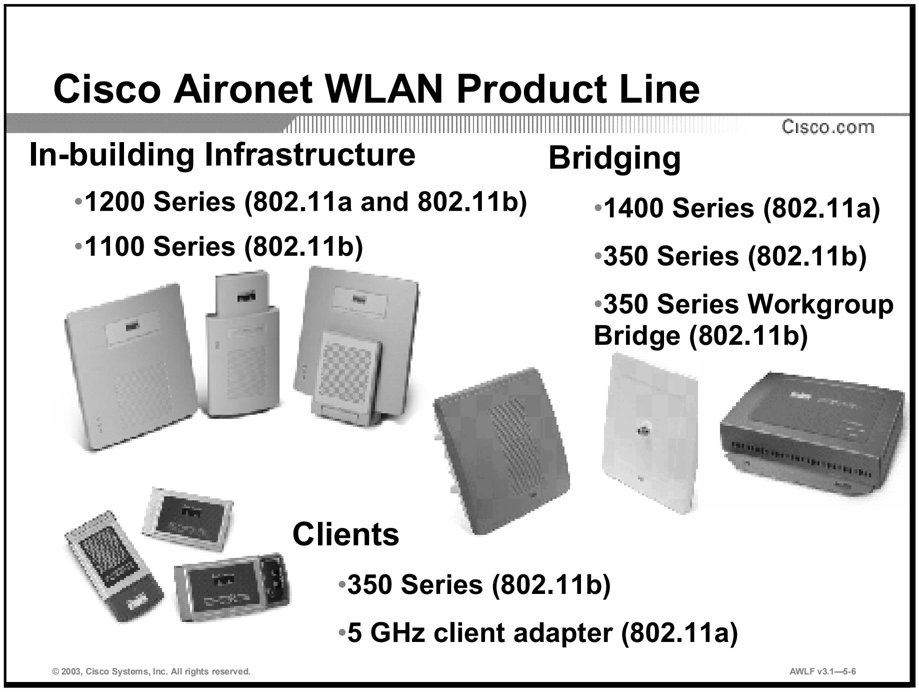
Linksys Target Markets

- SOHO (<20), Home consumer

Linksys Key Features

- Simple setup
- Low price where price is the ONLY consideration

Cisco Aironet WLAN Product Line



Cisco Aironet WLAN Product Line

Cisco.com

In-building Infrastructure

- 1200 Series (802.11a and 802.11b)
- 1100 Series (802.11b)

Bridging

- 1400 Series (802.11a)
- 350 Series (802.11b)
- 350 Series Workgroup Bridge (802.11b)

Clients

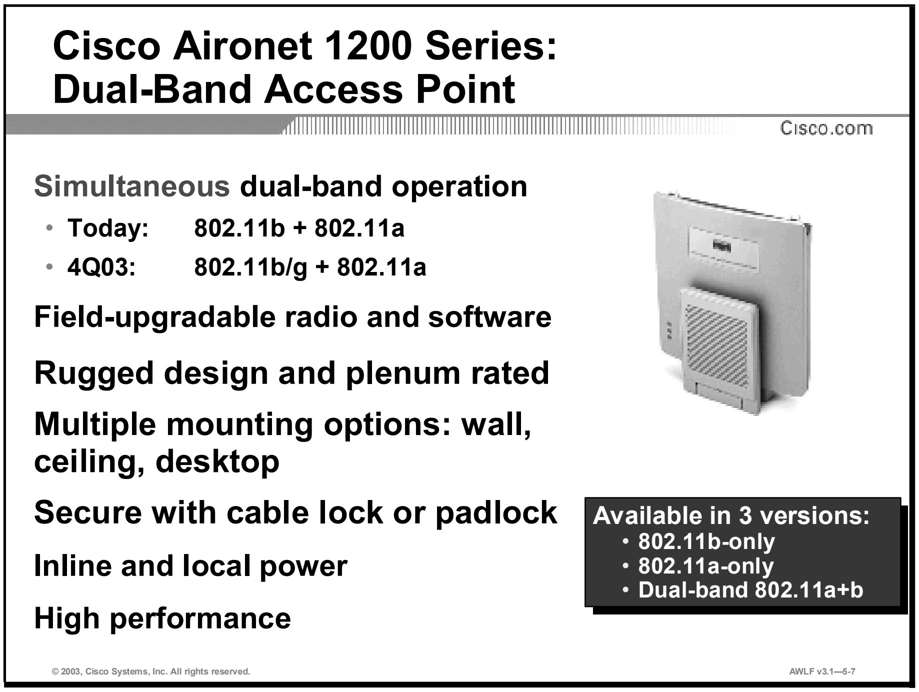
- 350 Series (802.11b)
- 5 GHz client adapter (802.11a)

AWLF v3.1—5-6

The Cisco Aironet product family is available in a variety of form factors to fit almost any application, and provides a complete solution to customers who require the mobility and flexibility of a wireless LAN to complement or replace a wired LAN.

The products seamlessly integrate into wired Ethernet networks and fully comply with the IEEE standards. They include the following:

- 802.11a and 802.11b Access Points
- 802.11a and 802.11b Client Adapters
- 802.11a and 802.11b Wireless Bridges
- 802.11b Workgroup Bridge



Cisco Aironet 1200 Series: Dual-Band Access Point

Cisco.com

Simultaneous dual-band operation

- **Today:** **802.11b + 802.11a**
- **4Q03:** **802.11b/g + 802.11a**

Field-upgradable radio and software

Rugged design and plenum rated

Multiple mounting options: wall, ceiling, desktop

Secure with cable lock or padlock

Inline and local power

High performance

Available in 3 versions:

- **802.11b-only**
- **802.11a-only**
- **Dual-band 802.11a+b**

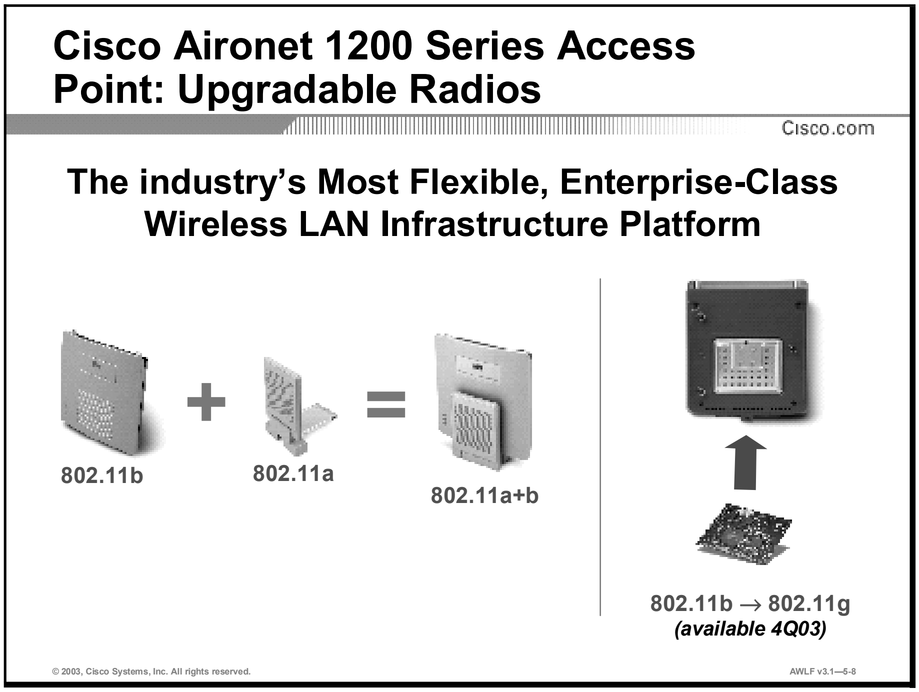
© 2003, Cisco Systems, Inc. All rights reserved. AWLF v3.1—5-7

Cisco Aironet 1200 Series Access Points set the standard for secure, manageable, and reliable wireless connectivity. With simultaneous support for both 2.4 GHz and 5 GHz radios, the Cisco Aironet 1200 Series preserves existing IEEE 802.11b investments, while providing a migration path to the faster IEEE 802.11a standard and future IEEE 802.11g products. Its modular design supports single- and dual-band configurations, plus the field upgradability to change these configurations as requirements change and technologies evolve. With its plenum rating, inline power support, and two separate locking mechanisms, this access point is suitable for installation in the most challenging locations, yet attractive enough for a company's lobby.

The 802.11a radio supports data rates of up to 54 Mbps and eight non-overlapping channels that offer high performance as well as maximum capacity and scalability. The 802.11b radio provides data rates up to 11 Mbps and three non-overlapping channels to support widely deployed 802.11b clients. The Mini-PCI form factor of the 802.11b radio allows for upgrade to higher-speed 2.4 GHz technologies such as the IEEE 802.11g standard.

The Cisco Aironet 1200 Series platform offers investment protection through field-upgradable CardBus and mini-PCI radios. The CardBus-based 802.11a modules can easily be fitted into installed Cisco Aironet 1200 Series Access Points.

Cisco Aironet 1200 Series Access Point is UL 2403 plenum rated. This means the access point does not give out toxic smoke when burned. Thus, the access point can be installed above dropped ceilings.



Cisco Aironet 1200 Series Access Point: Upgradable Radios

Cisco.com

The industry's Most Flexible, Enterprise-Class Wireless LAN Infrastructure Platform

AWLF v3.1—5-8

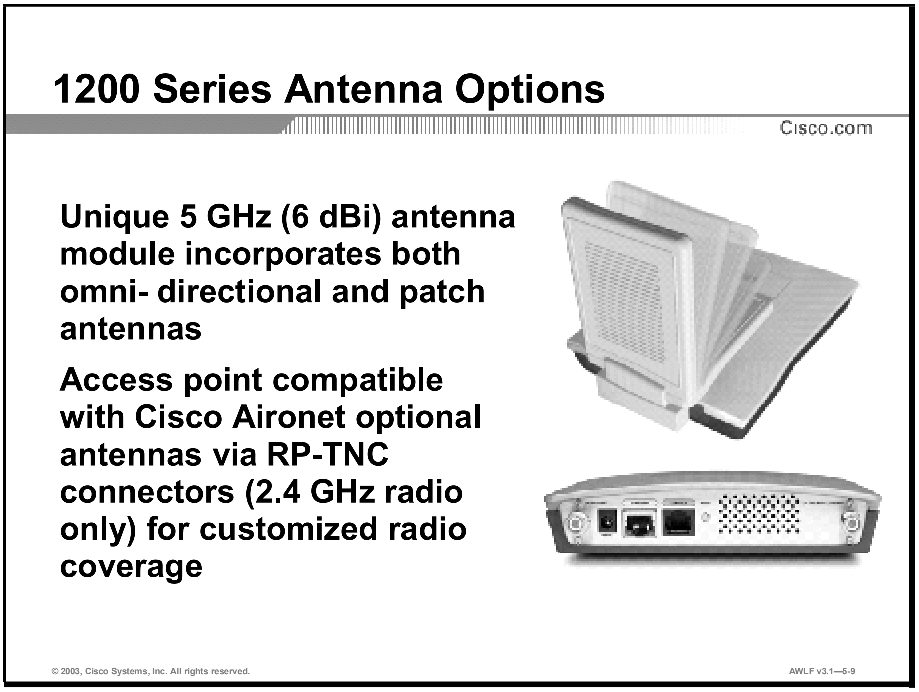
Modular platform for single or dual band operation

The access point can be configured for either 802.11b only, 802.11a only, or for simultaneous support of 802.11b and 802.11a to provide the maximum number of channels and maximum available data rates in a single device.

Field upgradeable radios

Flexibility and investment protection is provided through field-upgradeable card bus and mini-PCI radios. CardBus-based 802.11a modules can easily be fitted into installed Cisco Aironet 1200 Series access points.

- 5 GHz – UNII-1 and UNII-2 indoor compliant
- FCC requires the radio, antenna, and access point to be a single unit
- 40 mW radio
- Data rates 54 Mbps to 6 Mbps
- Two 5 GHz diversity antennas
- The 802.11a can be set to 8 different non-overlapping channels. Search for less-congested channel is supported.
  - UNII-1 channels USA are: 36 – 5180 MHz, 40 – 5200 MHz, 44 – 5200 MHz, and 48 – 5240 MHz
  - UNII-2 channels USA are: 52 – 5260 MHz, 56 – 5280 MHz, 60 – 5300 MHz, and 64 – 5320 MHz
- The 802.11a radio module connects to a CardBus slot on the Cisco Aironet 1200 Series Access Point. The 802.11a radio is held in place by two screws. The 802.11a module can be locked to the access point. Its power can be adjusted down to 5 mW for microcellular deployment. Power options are 40 mW, 20 mW, 10 mW, and 5 mW.
- The 11a radio can be configured to automatically shift its data rate among 54 Mbps to 6 Mbps. The available rates are 54, 48, 36, 24, 18, 12, 9, and 6, thus maintaining an optimized data rate and coverage. The rates can also be fixed.



1200 Series Antenna Options

Cisco.com

Unique 5 GHz (6 dBi) antenna module incorporates both omni- directional and patch antennas

Access point compatible with Cisco Aironet optional antennas via RP-TNC connectors (2.4 GHz radio only) for customized radio coverage

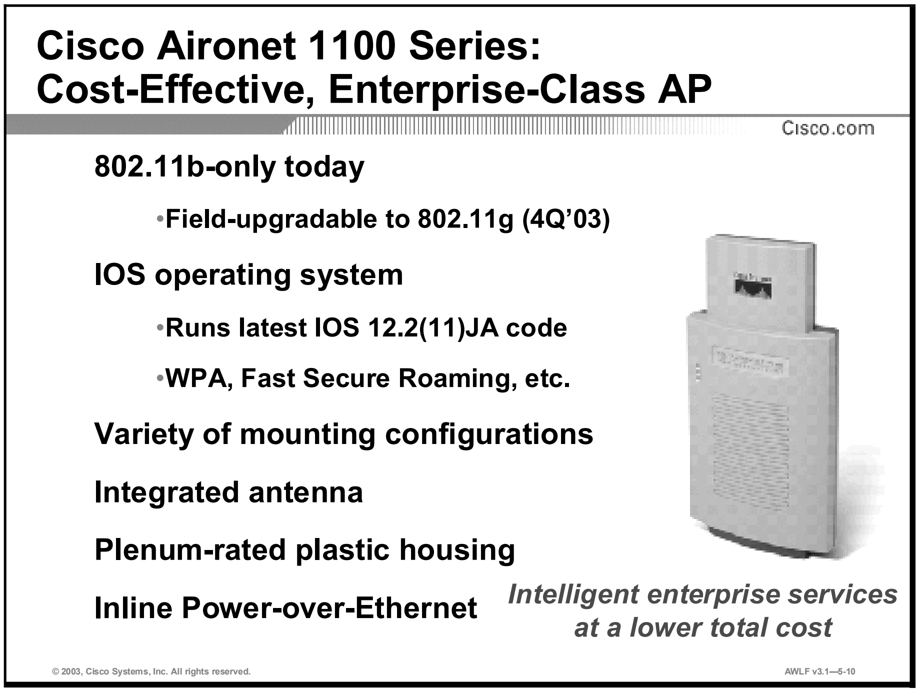
AWLF v3.1—5-9

5 GHz integrated antennas: Unique articulating antenna paddle incorporates high-gain omni directional and hemispherical patch antennas to deliver two distinct coverage patterns.

Cisco Aironet 1200 Series Access Points can be mounted horizontally or vertically. The 5 GHz module comes with an integrated antennas on a paddle. When vertically mounted set the paddle parallel to the access point. In this configuration the patch antennas with semi-spherical radiation pattern are used. When horizontally mounted, such as desktop and ceiling mount, set the paddle perpendicular to the access point. In this configuration the omni-directional antennas are used.

2.4 and 5 GHz Diversity Antennas: Diversity antennas for both the 2.4- and 5 GHz radios ensures optimum performance in high-multipath environments such as offices, warehouses, and other indoor installations.

Two reverse-polarity threaded naval connectors (RP-TNC) for external 2.4 GHz antenna connection: Diversity support for the 2.4 GHz radio to improve reliability in high-multipath environments. The RP-TNC connectors are compatible with the Cisco Aironet optional antennas, enabling WLAN architects to customize radio coverage for specific deployment scenarios.



Cisco Aironet 1100 Series: Cost-Effective, Enterprise-Class AP

Cisco.com

802.11b-only today

- Field-upgradable to 802.11g (4Q'03)

IOS operating system

- Runs latest IOS 12.2(11)JA code
- WPA, Fast Secure Roaming, etc.

Variety of mounting configurations

Integrated antenna

Plenum-rated plastic housing

Inline Power-over-Ethernet

Intelligent enterprise services at a lower total cost

AWLF v3.1—5-10

Cisco Aironet 1100 Series Access Points offer an affordable, intelligent, and upgradable 2.4 GHz wireless LAN solution that delivers enterprise-class security and manageability. Equipped for the IEEE 802.11b standard, a field-upgradable design ensures a smooth migration to the IEEE 802.11g standard. The compact size, integrated antenna, and innovative bracket design of this Cisco IOS-based access point allow for quick, easy installation in a variety of orientations.

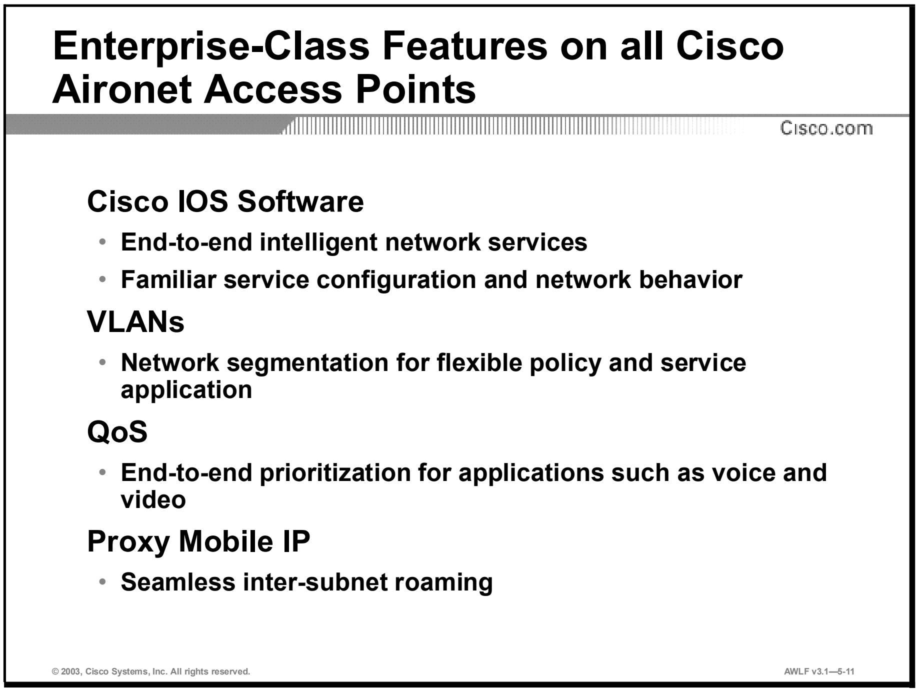
Enterprise features: The 1100 Series Cisco IOS operating system including features like VLAN, QoS and proxy mobile IP that extend end-to-end intelligent networking to the enterprise wireless LAN.

Secure as with all Cisco Aironet Access Points, the Cisco Aironet 1100 Series offers the Cisco Wireless Security Suite of security solutions.

Easy to use: The Cisco Aironet 1100 Series uses integrated antennas for installation in any orientation. The flexible mounting system allows the customer to install this in nearly any location. Cisco command-line interface (CLI) and the redesigned web GUI allow network managers to quickly set up access points.

Single 802.11b radio is a time tested technology. In addition, it supports an installed base of 802.11b clients while providing a migration path to 802.11g.

The Cisco Aironet 1100 Series is ideal for new deployments, or as an addition to existing deployments to support increasing capacity requirements. Engineered with extra system capacity, including memory, storage, and processing power, the Cisco Aironet 1100 Series is designed to support not only today's feature set, but future software releases for expanded functionality and capabilities. Companies can also upgrade the Cisco Aironet 1100 Series hardware to future radio technologies, such as those based on higher speed 802.11g specifications, unleashing increased performance and further investment value.



Enterprise-Class Features on all Cisco Aironet Access Points

Cisco.com

Cisco IOS Software

- End-to-end intelligent network services
- Familiar service configuration and network behavior

VLANs

- Network segmentation for flexible policy and service application

QoS

- End-to-end prioritization for applications such as voice and video

Proxy Mobile IP

- Seamless inter-subnet roaming

AWLF v3.1—5-11

Cisco IOS Software

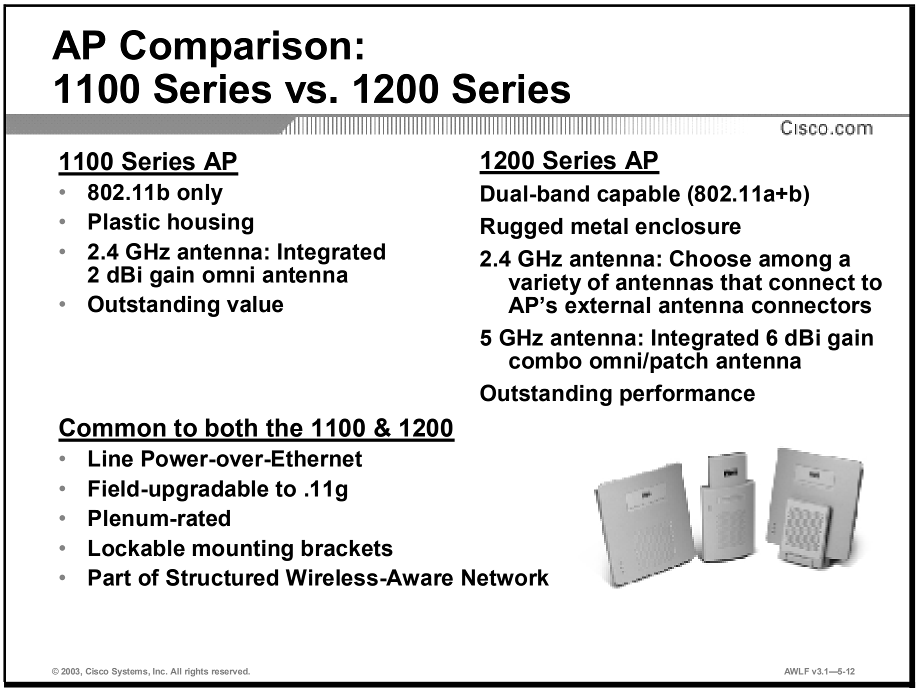
Cisco Aironet products leverage the same Cisco IOS Software that powers Cisco switches and routers, enabling customers to extend common services, management tools, and interfaces across their wired and wireless networks.

Intelligent Network Services: VLANs, QoS, and Proxy Mobile IP. Another key component of the Cisco Enterprise WLAN solution is the use of intelligent network services, including QoS, VLANs, and proxy mobile IP. Providing these features, allows your customers to truly look at the WLAN as an extension of their wired network because it offers much of the same functionality and management tools. These features can also enable new applications, such as video and voice, over wireless.

VLANs: Segregating Wireless Traffic Based on Policies and Services The Cisco Aironet family is capable of managing up to 16 VLANs per access point. This allows customers to vary WLAN policies and services, such as security and QoS, to accommodate different types of users and applications. For example, enterprise customers can use different wireless VLANs to separate employee traffic from guest traffic. VLANs are ideal for providing wireless access in public areas, such as lobbies and airports, without compromising network security. Similarly, educational institutions could take advantage of the Cisco LEAP security protocol on VLANs carrying faculty and administrator traffic, while using another authentication protocol on student VLANs to support a broader mix of client devices. VLANs can also be deployed in support of certain applications, such as time-sensitive voice traffic, to ensure peak performance.

QoS: End-to-End Traffic Prioritization Optimizes Network Performance With support for IEEE 802.1p QoS, the Cisco Enterprise WLAN solution provides true end-to-end traffic prioritization. This feature is an essential building block for real-time applications and integrates seamlessly with the existing QoS features found in Cisco routers and switches. 802.1p QoS allows time-sensitive traffic, such as voice and video, to be prioritized over less critical packets, such as e-mail data, for an improved user experience and optimal bandwidth utilization. The Cisco Aironet family already supports voice prioritization schemes for 802.11b wireless phones, and for maximum investment protection, field upgrades will offer the ability to migrate to emerging QoS standards such as 802.11e. Although this standard is not yet ratified, the Cisco Aironet APs software versions 12.0 and later contain major updates in the WLAN QoS tools, including portions of the 802.11e proposed draft.

Proxy Mobile IP: With proxy mobile IP, users can roam from one wireless access point to another while maintaining seamless network connectivity. This is achieved by transporting individual IP addresses as users move from one subnet to the next. As a result, IT managers can partition the WLAN into distinct, easily managed segments without affecting user mobility. This more closely mirrors the architecture of the wired network, yet the boundaries are transparent from the user's perspective.



AP Comparison: 1100 Series vs. 1200 Series

Cisco.com

1100 Series AP

- 802.11b only
- Plastic housing
- 2.4 GHz antenna: Integrated 2 dBi gain omni antenna
- Outstanding value

1200 Series AP

Dual-band capable (802.11a+b)

Rugged metal enclosure

2.4 GHz antenna: Choose among a variety of antennas that connect to AP's external antenna connectors

5 GHz antenna: Integrated 6 dBi gain combo omni/patch antenna

Outstanding performance

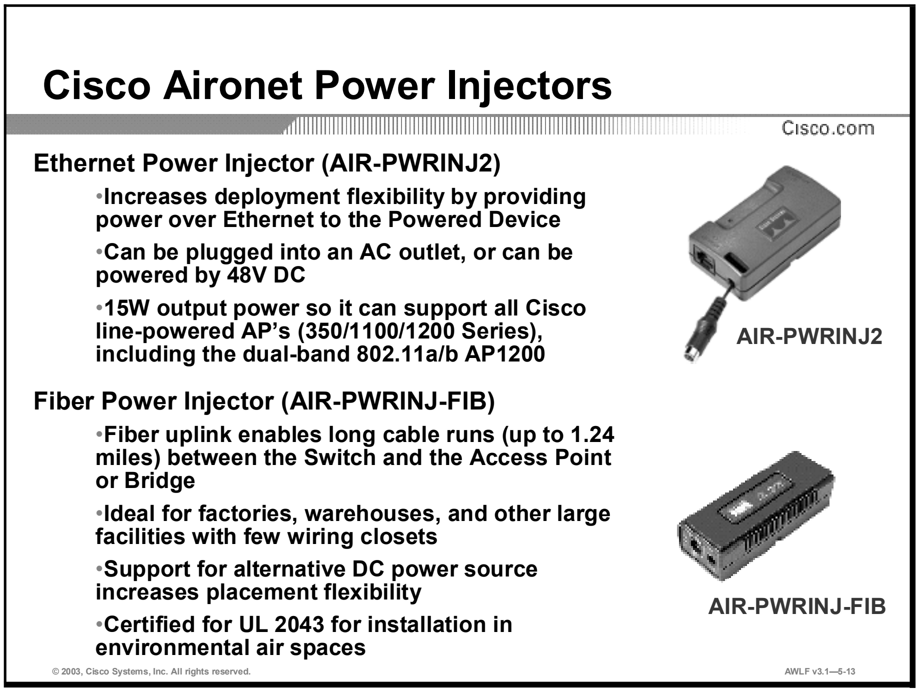
Common to both the 1100 & 1200

- Line Power-over-Ethernet
- Field-upgradable to .11g
- Plenum-rated
- Lockable mounting brackets
- Part of Structured Wireless-Aware Network

AWLF v3.1—5-12

With the Cisco Aironet 1100 and 1200 series access points, Cisco Systems enables wireless LAN customers to meet varying technical and business needs. Cisco Aironet 1200 Series access points deliver the flexibility of dual-band wireless connectivity, simultaneously supporting the popular 2.4 GHz, 802.11b standard and the newer, faster 5.2 GHz, 802.11a standard. Customers who require support for the higher data rates offered by 802.11a, or who need to meet the more rigorous environmental conditions of factories and other vertical markets, will find the Cisco Aironet 1200 Series an ideal choice. Cisco Aironet 1100 Series access points offer customers an affordable, easy-to install single-band alternative, supporting the large installed base of Wi-Fi–certified 802.11b wireless devices. The Cisco Aironet 1100 Series is ideal for price-sensitive enterprise customers, while still delivering enterprise-class management, security, and scalability. Both series are based on Cisco IOS Software*, and offer key features that extend intelligent networking features to the wireless LAN at the network edge, including:

- **VLAN Support:** With support for up to 16 virtual LANs (VLANs), the enterprise can segment traffic and offer differentiated services and policies to different user groups.
- **QoS Support:** Customers can provide QoS for high-priority traffic, such as voice and video.
- **Proxy Mobile IP Support:** Users can seamlessly roam between subnets, without losing connectivity.



Cisco Aironet Power Injectors

Cisco.com

Ethernet Power Injector (AIR-PWRINJ2)

- **Increases deployment flexibility by providing power over Ethernet to the Powered Device**
- **Can be plugged into an AC outlet, or can be powered by 48V DC**
- **15W output power so it can support all Cisco line-powered AP's (350/1100/1200 Series), including the dual-band 802.11a/b AP1200**

AIR-PWRINJ2

Fiber Power Injector (AIR-PWRINJ-FIB)

- **Fiber uplink enables long cable runs (up to 1.24 miles) between the Switch and the Access Point or Bridge**
- **Ideal for factories, warehouses, and other large facilities with few wiring closets**
- **Support for alternative DC power source increases placement flexibility**
- **Certified for UL 2043 for installation in environmental air spaces**

AIR-PWRINJ-FIB

AWLF v3.1—5-13

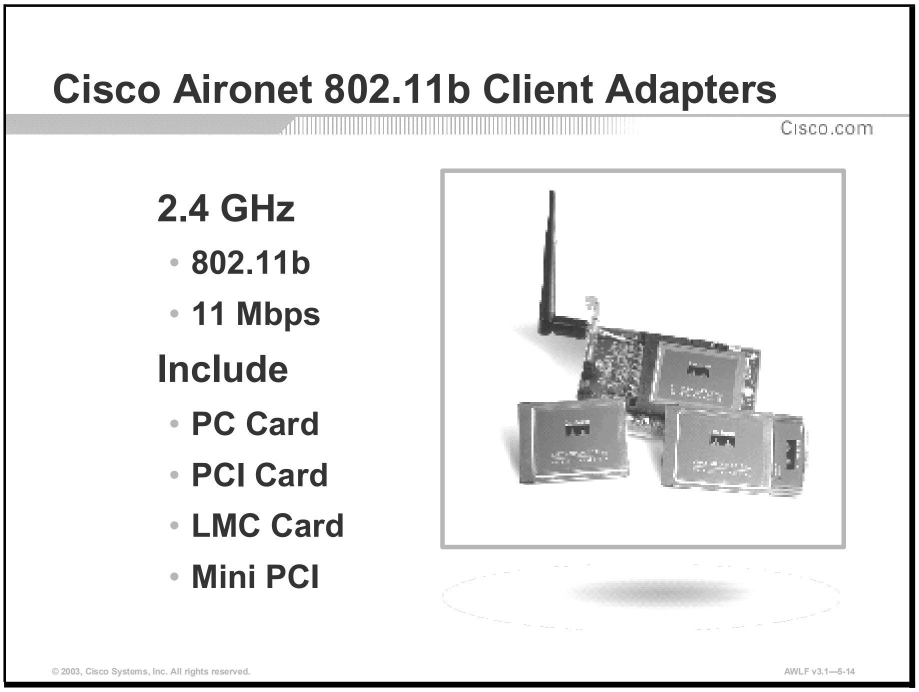
Cisco Aironet Power Injector products increase the deployment flexibility of Cisco Aironet wireless access points and bridges by providing an alternative powering option to local power, inline power-capable multiport switches, and multiport power patch panels.

The single-port Cisco Aironet power injectors combine 48-VDC power with the data signal, sending both to the Cisco Aironet access point or bridge. Cisco Aironet 350 Series access points and bridges include an integrated power supply and injector. The power injector for Cisco Aironet 1100 and 1200 series access points works with the power supply provided with the access point.

The Cisco Aironet Power Injector Media Converter converts fiber media to Category 5 media and combines the resulting data signal with power for delivery to the access point or bridge. The power injector media converter accepts 48 VDC power from either the barrel connector of the local power supply or an alternative 48 VDC power source. When powered by an alternate 48 VDC power source connected using the provided power supply pigtail, the Power Injector Media Converter is UL2043 certified and suitable for installation in environmental air spaces. The local power supply is provided with the Cisco Aironet 1100 and 1200 series access points, while applicable local power supplies for the Cisco Aironet 350 Series access points and bridges are available separately.

The Cisco Aironet Power Injector (part number AIR-PWRINJ=) is preassembled with the power supply. No additional power supply is required.

The 350 Series access points and bridges do not come with a standalone power supply. To use the power injector media converter (part number AIR-PWRINJ-FIB=) with these devices, you will need to procure the power supply with the part number AIR-PWR-A= or provide an external 48 VDC power supply. Cisco Aironet 1100 and 1200 series power injectors can be used with Cisco Aironet 350 Series devices, but because of the higher current demands of the Cisco Aironet 1100 and 1200 series access points, the Cisco Aironet 350 Series Power Injector cannot be used with the Cisco Aironet 1100 and 1200 series devices.



Cisco Aironet 802.11b Client Adapters

Cisco.com

2.4 GHz

- 802.11b
- 11 Mbps

Include

- PC Card
- PCI Card
- LMC Card
- Mini PCI

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—5-14

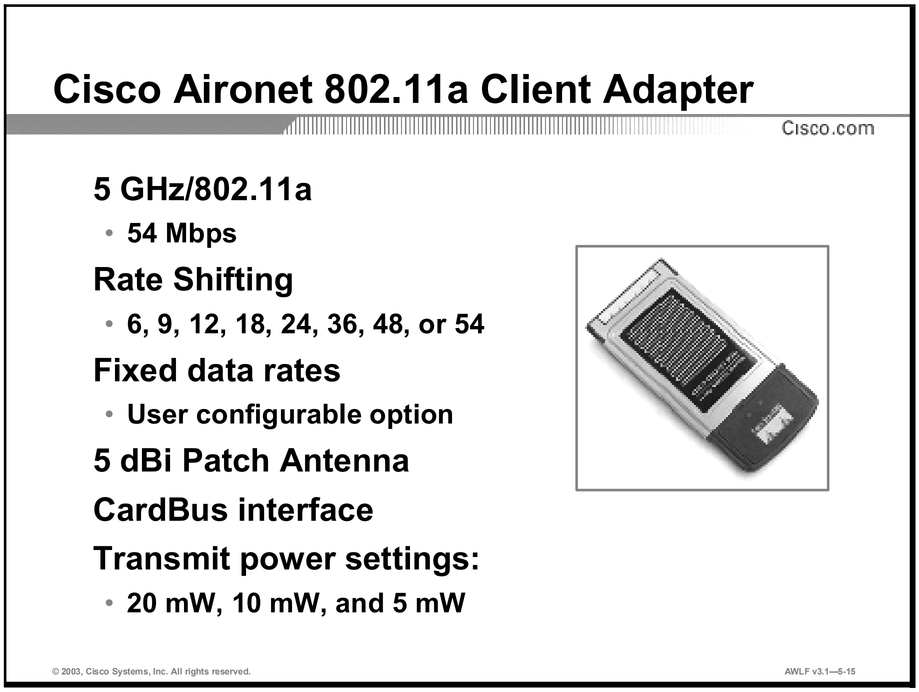
Cisco Aironet 350 Series Client Adapters complement Cisco Aironet 1200 Series and 1100 Series access points. Available in PCMCIA and PCI form factors, these 802.11b-compliant client adapters quickly connect desktop and mobile computing devices to the wireless LAN.

Cisco Aironet offers a variety of clients for the 802.11b WLAN. These include:

- PC Card: Standard PCMCIA product with attached end-cap antenna. Support both 40 and 128-bit encryption.
- LM Card: PCMCIA card with MMCX connectors. This card allows the attachment of any of the Cisco antennas utilizing the MMCX RP-TNC adapter cables. An end-cap antenna is offered for use with the LM card, giving it the same functionality as the PC card. The LM card is shipped without an antenna, and supported with both 40 and 128-bit encryption.
- PCI card: Standard PCI card typically used for desktop clients. The PCI card has the standard Cisco Aironet RP-TNC connector and can be used with all of the Cisco external antennas. The PCI card is shipped without an antenna, but is supported with both 40 and 128-bit encryption.

All Cisco Aironet client devices support IEEE 802.1X security including LEAP and EAP-TLS, for mutual authentication and dynamic per-user, per session WEP keys.

All Cisco Aironet client devices are capable of Load Balancing when used with Cisco Aironet Access Points.



Cisco Aironet 802.11a Client Adapter

Cisco.com

5 GHz/802.11a

- **54 Mbps**

Rate Shifting

- **6, 9, 12, 18, 24, 36, 48, or 54**

Fixed data rates

- **User configurable option**

5 dBi Patch Antenna

CardBus interface

Transmit power settings:

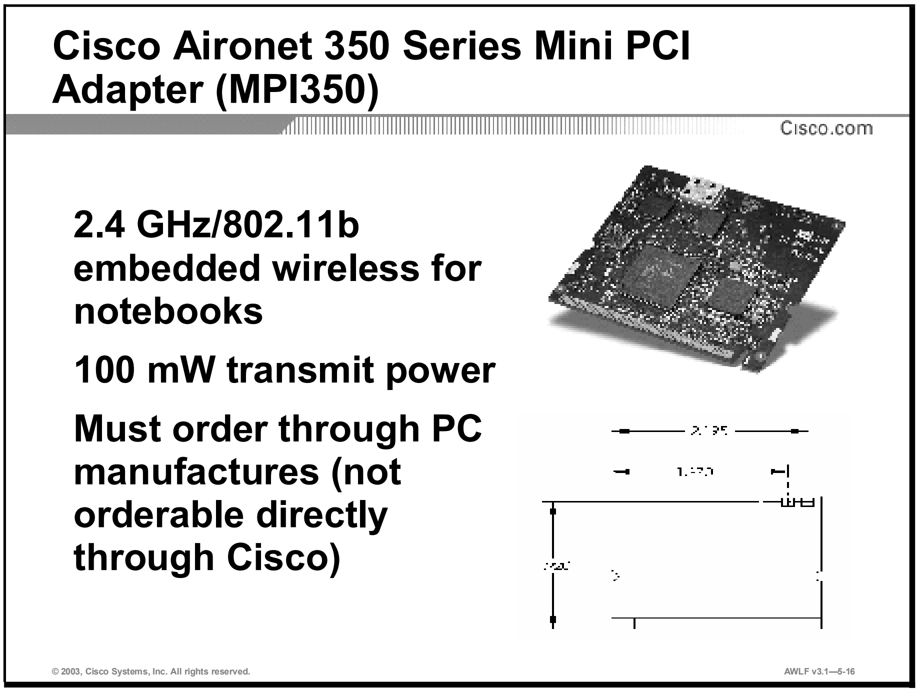
- **20 mW, 10 mW, and 5 mW**

AWLF v3.1—5-15

Cisco Aironet 5 GHz 54 Mbps Wireless LAN Client Adapters complement the Cisco Aironet 1200 Series Access Point, providing a solution that combines mobility with the security and manageability required by businesses. The 802.11a-compliant CardBus adapter operates in the UNII-1 and UNII-2 bands to allow 54 Mbps throughput.

Cisco's innovative radio and antenna design delivers industry-leading 802.11a enterprise performance. It provides for maximum capacity and scalability across the enterprise through eight non-overlapping channels in the UNII-1 and UNII-2 bands. The integrated 5 dBi gain patch antenna optimizes range. The -68 dBm receive sensitivity at 54 Mbps provides high-data-rate range performance. Advanced signal processing in the Cisco Aironet 5 GHz Wireless LAN Client Adapter helps manage the multipath propagation often found in office environments and intelligent filtering addresses ambient noise and interference that can decrease network performance. Various transmit power settings on the Cisco Aironet client adapter enable you to select range capabilities.

CardBus: (IEEE) 802.11a-compliant adapter that operates in the UNII-1 and UNII-2 bands. The CardBus 32-bit interface handles 400-6000 Mbps.



Cisco Aironet 350 Series Mini PCI Adapter (MPI350)

Cisco.com

- 2.4 GHz/802.11b embedded wireless for notebooks
- 100 mW transmit power
- Must order through PC manufactures (not orderable directly through Cisco)

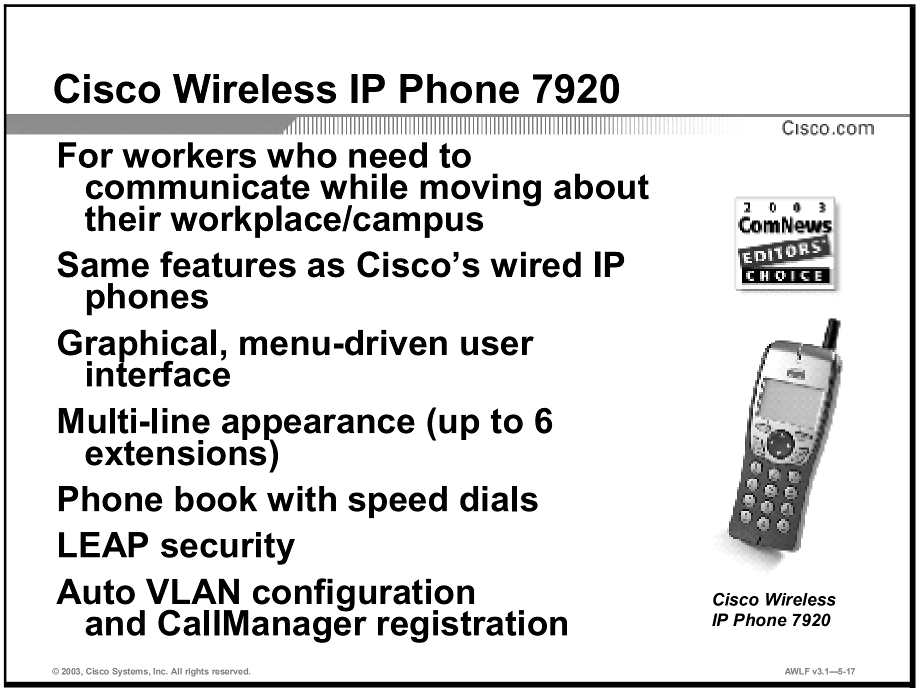
© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—5-16

The Cisco Aironet MPI350 is a mini-PCI card with IEEE 802.11b high-rate standard compliance. The type IIIa Mini-PCI form factor will allow for standard compatibility in a variety of mobile devices (IBM, Toshiba, Dell). Some of the features of the MPI350 include:

- Industry-leading range and throughput performance
- Supports hardware accelerated 128-bit Wired Equivalent Privacy (WEP) RC4 encryption for data security with negligible performance degradation
- 802.11X security support via LEAP for the most advanced wireless authentication scheme available
- World mode for international mobility across regulatory domains
- Dual antenna connectors supporting diversity
- True PCI bus interface
- Support for all popular operating systems

The MPI350 is embedded in laptops such as the Toshiba Tecra 9000 and Protégé 4000, as well as various models from IBM and Dell. The mini-PCI can not be ordered directly from Cisco. Because the product is embedded, it must be installed at the PC factory or by PC authorized dealers. Customers must request the Cisco option from PC manufacturers.



Cisco Wireless IP Phone 7920

Cisco.com

- For workers who need to communicate while moving about their workplace/campus
- Same features as Cisco's wired IP phones
- Graphical, menu-driven user interface
- Multi-line appearance (up to 6 extensions)
- Phone book with speed dials
- LEAP security
- Auto VLAN configuration and CallManager registration

2003
ComNews
EDITORS'
CHOICE

Cisco Wireless IP Phone 7920

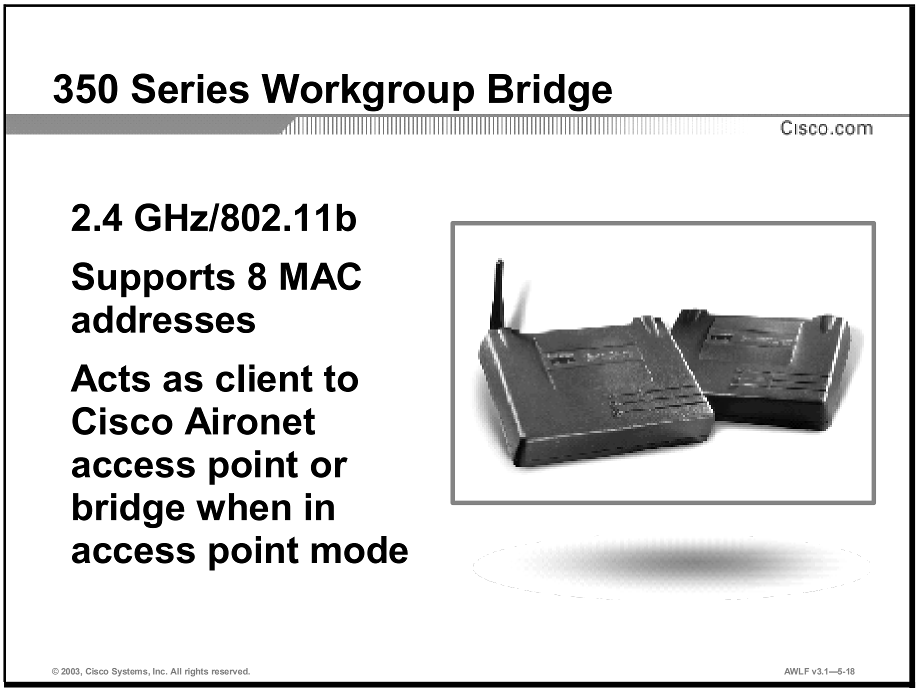
AWLF v3.1—5-17

The Cisco Wireless IP Phone 7920 solution enables enterprise users to globally answer business critical calls anywhere on a corporate campus and reduce telephone tag.

The Cisco Wireless IP Phone 7920 is equally adaptable for all mobile professionals, from managers on the move in an office environment to associates working in the warehouse, on the sales floor, or in the call center. Nurses, doctors, educators, and IT personnel can also increase their availability as an ever broadening range of industries adopt wireless LANs.

The solution allows Enterprises the flexibility to add coverage and capacity as needed to meet user needs. Additionally, the Cisco Wireless IP Communications solution operates seamlessly with existing Cisco Wired IP Communications solutions on a single intelligent network

When combined with the other Cisco IP phones, the result is a complete range of feature-rich, flexible, easy-to-use, and cost effective communication devices that is unmatched by other competitors.



350 Series Workgroup Bridge

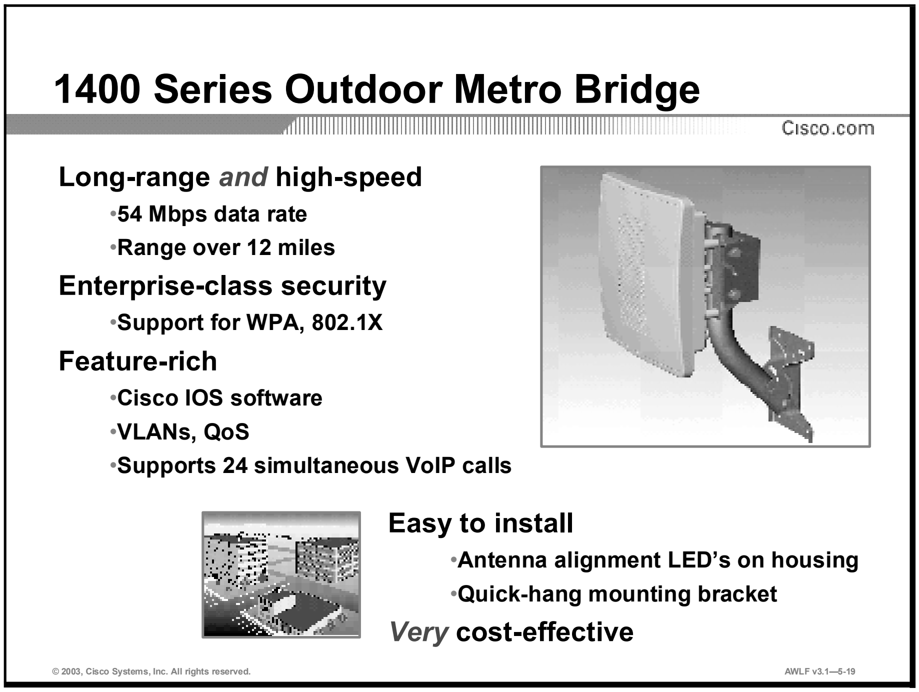
- 2.4 GHz/802.11b
- Supports 8 MAC addresses
- Acts as client to Cisco Aironet access point or bridge when in access point mode

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—5-18

Cisco Aironet 350 Wireless Workgroup Bridges meet the needs of remote workgroups, satellite offices, and mobile users by bringing the freedom and flexibility of wireless connectivity to any Ethernet-enabled device. The workgroup bridge quickly connects up to eight Ethernet-enabled devices, such as laptops, personal computers, and printers, to a wireless LAN, providing the link from these devices to any Cisco Aironet access point or wireless bridge.

The Cisco Aironet Workgroup Bridge product connects to the Ethernet port of a device that does not have a PCI or PCMCIA slot available or to a hub with up to 8 wired devices attached. It provides a wireless connection into an access point for up to 8 MAC address, and onto the LAN backbone. It cannot be used in a peer-to-peer mode connection, and must communicate to a Cisco Aironet Access Point or to a Cisco Aironet Bridge in access point mode.



1400 Series Outdoor Metro Bridge

Cisco.com

Long-range *and* high-speed

- **54 Mbps data rate**
- **Range over 12 miles**

Enterprise-class security

- **Support for WPA, 802.1X**

Feature-rich

- **Cisco IOS software**
- **VLANs, QoS**
- **Supports 24 simultaneous VoIP calls**

Easy to install

- **Antenna alignment LED's on housing**
- **Quick-hang mounting bracket**

***Very* cost-effective**

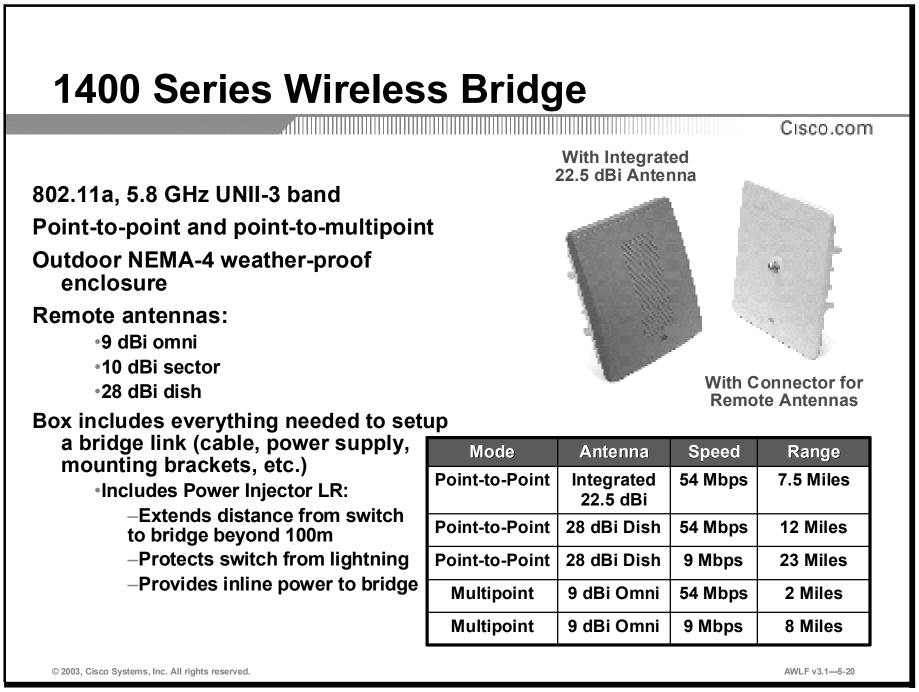
© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—5-19

The Cisco Aironet® 1400 Series Wireless Bridge creates a new benchmark for wireless bridging by providing a high-performance and feature-rich solution for connecting multiple LANs in a metro area. Designed to be a cost-effective alternative to leased lines, it is engineered specifically for harsh outdoor environments.

Key Features

- Support for both point-to-point or point-to-multipoint configurations
- Industry leading range and throughput, supporting data rates up to 54 Mbps
- Enhanced security mechanisms based on 802.11 standards
- Ruggedized enclosure optimized for harsh outdoor environments with extended operating temperature range
- Integrated or optional external antennas for flexibility in deployment
- Designed specifically for ease-of-installation and operation



1400 Series Wireless Bridge

802.11a, 5.8 GHz UNII-3 band

Point-to-point and point-to-multipoint

Outdoor NEMA-4 weather-proof enclosure

Remote antennas:

- 9 dBi omni
- 10 dBi sector
- 28 dBi dish

Box includes everything needed to setup a bridge link (cable, power supply, mounting brackets, etc.)

- Includes Power Injector LR:
  - Extends distance from switch to bridge beyond 100m
  - Protects switch from lightning
  - Provides inline power to bridge

With Integrated 22.5 dBi Antenna
With Connector for Remote Antennas

Mode	Antenna	Speed	Range
Point-to-Point	Integrated 22.5 dBi	54 Mbps	7.5 Miles
Point-to-Point	28 dBi Dish	54 Mbps	12 Miles
Point-to-Point	28 dBi Dish	9 Mbps	23 Miles
Multipoint	9 dBi Omni	54 Mbps	2 Miles
Multipoint	9 dBi Omni	9 Mbps	8 Miles

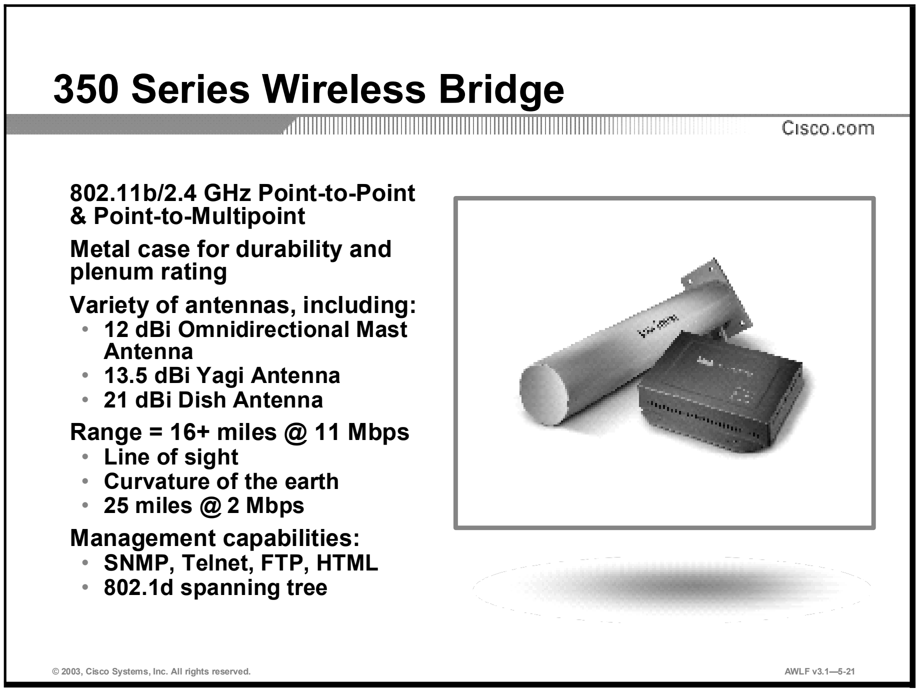
AWLF v3.1—5-20

Operating in the unlicensed 5.8 GHz band, the Cisco Aironet 1400 Series Wireless Bridge sets a new standard for performance, combining powerful 250 mW radios, industry-leading receive sensitivity, installation tools to assist in bridge placement, delay spread capabilities, and a choice of integrated or connectorized high gain antennas, Cisco provides a complete solution for a wide variety of fixed wireless applications.

Data rates of 54 Mbps can be enabled for point-to-point links up to 7.5 miles, and for point-to-multipoint links up to 2 miles. Aggregate throughput can be obtained in excess of 28 Mbps. Also, by using higher gain antennas or lower data rates, ranges in excess of 20 miles point-to-point can be covered.

Rapid deployment and redeployment can be achieved with no reliance upon telecommunications providers nor a lengthy license or trenching process. The Cisco Aironet 1400 Series Wireless Bridge allows placement in an outdoor environment without the use of an expensive additional National Electrical Manufacturers Association (NEMA) enclosure. Further flexibility is achieved by enabling point-to-point or point-to-multipoint networks with a single product line. The mounting bracket has been designed to allow installation on poles, walls, and roofs, while also providing a mechanism for choosing the desired polarization. The Cisco Aironet 1400 Series Wireless Bridge offers an outdoor wireless bridging solution in two product SKUs. The captured antenna version features an integrated radio and high-gain integrated antenna for user installations of point-to-point links and the non-root nodes of point-to-multipoint networks. The connectorized version provides professional installers with an N-Type connector that allows the deployment of the root nodes of point-to-multipoint networks with omni-directional or sector antennas, or of high gain dish antennas for longer links. The external antenna options are:

- 9.0 dBi vertically polarized omni antenna
- 9.5 dBi sector antenna with support for vertical or horizontal linear polarization
- 28.0 dBi dish antenna with support for vertical or horizontal linear polarization



350 Series Wireless Bridge

Cisco.com

802.11b/2.4 GHz Point-to-Point & Point-to-Multipoint

Metal case for durability and plenum rating

Variety of antennas, including:
- **12 dBi Omnidirectional Mast Antenna**
- **13.5 dBi Yagi Antenna**
- **21 dBi Dish Antenna**

Range = 16+ miles @ 11 Mbps
- **Line of sight**
- **Curvature of the earth**
- **25 miles @ 2 Mbps**

Management capabilities:
- **SNMP, Telnet, FTP, HTML**
- **802.1d spanning tree**

AWLF v3.1—5-21

Cisco Aironet 350 Series Wireless Bridges enable high-speed building-to-building links of up to 25 miles (40 km) in FCC regulated areas, or 6.5 miles (10.5 km) in Europe. Delivering throughput several times greater than T1/E1 lines at a fraction of the cost, wireless bridges are ideal for data-intensive, line-of-sight applications, such as connecting hard-to-wire sites, campus settings, satellite offices, and temporary networks. They can be configured for point-to-point or point-to-multi-point applications, allowing two or more sites to connect into a single LAN and/or share a single high-speed Internet connection.

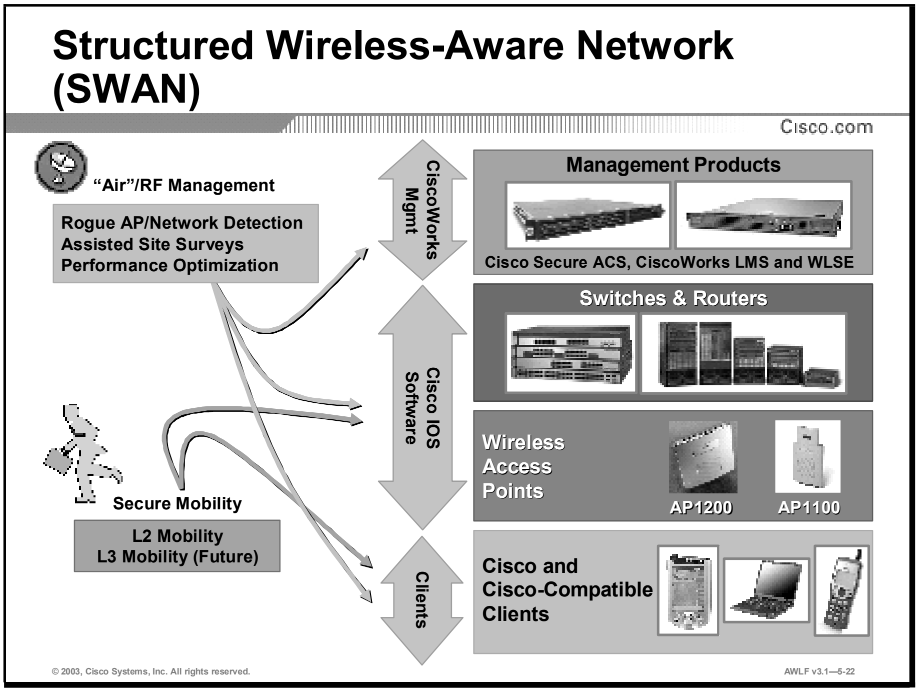
Some of the outstanding features include:

- 802.1D Spanning Tree capabilities
- Full SNMP capability
- FTP
- Bootstrap Protocol (BOOTP) and Telnet capabilities
- Flexibility of configuration with non-volatile Flash ROM
- Inline power
- Same security options available on the Cisco Aironet 350 Series Access Point

The Cisco Aironet 350 Series Bridge is also UL 2043 certified, and designed to achieve plenum rating as defined by various municipal fire codes.

Perhaps the most outstanding feature is the price. The Cisco bridge products are priced as one of the lowest in the industry, while still maintaining highest possible performance.

Structured Wireless-Aware Network



Structured Wireless-Aware Network (SWAN)

Cisco.com

"Air"/RF Management

Rogue AP/Network Detection
Assisted Site Surveys
Performance Optimization

Secure Mobility

L2 Mobility
L3 Mobility (Future)

CiscoWorks Mgmt

Cisco IOS Software

Clients

Management Products

Cisco Secure ACS, CiscoWorks LMS and WLSE

Switches & Routers

Wireless Access Points

AP1200

AP1100

Cisco and Cisco-Compatible Clients

© 2003, Cisco Systems, Inc. All rights reserved.

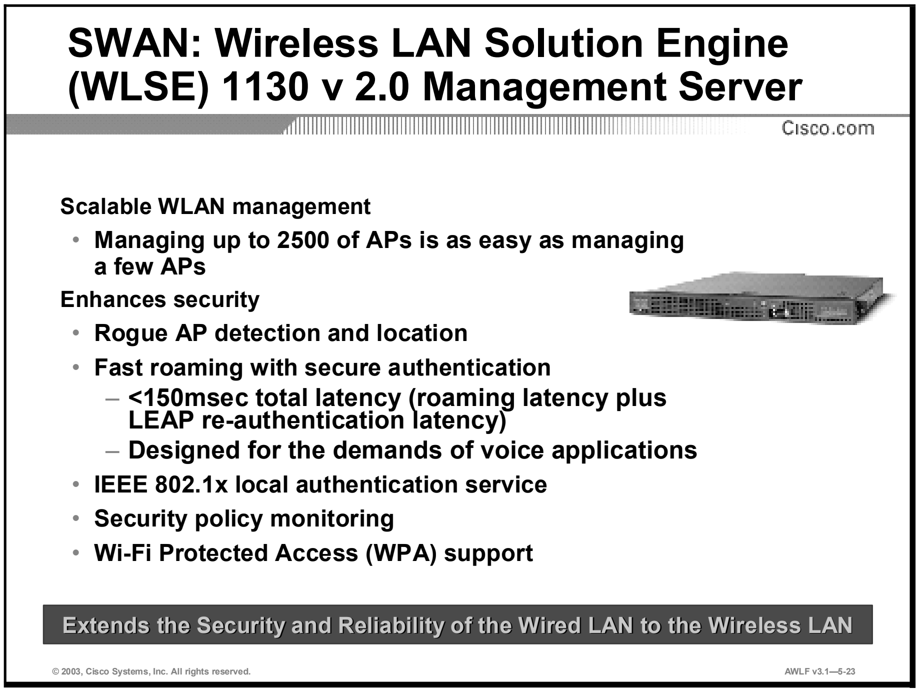
AWLF v3.1—5-22

The Cisco Structured Wireless-Aware Network combines the Cisco switch and router infrastructure with the Cisco wireless network, making one integrated "wireless-aware" network. This secure, integrated wired and wireless network extends Cisco's proven local area networking (LAN) infrastructure capabilities to the wireless LAN (WLAN), providing the security, management, ease-of-deployment, scalability, and reliability that our enterprise customers depend on for their core business applications.

Cisco Structured Wireless-Aware Network infrastructure enhancements will be integrated in Cisco Aironet 1100 and 1200 Series access points, Cisco Catalyst 3750, 4500 and 6500 Series switches and Cisco 2600XM and 3700 Series routers. Other components of the solution include CiscoWorks Wireless LAN Solution Engine (WLSE) for management and monitoring, Cisco IOS Software, Cisco Secure Access Control Server for centralized authentication and Cisco and Cisco Compatible client adapters for radio frequency (RF) monitoring and measurement.

Key Components

- Cisco Aironet Series wireless LAN access points
- Cisco Aironet Series wireless LAN client adapters
- Cisco Compatible client adapters
- Cisco Wireless Security Suite
- Cisco IOS Software
- Cisco Secure Access Control Server (ACS)
- CiscoWorks Wireless LAN Solution Engine version 2.0 and 2.5



SWAN: Wireless LAN Solution Engine (WLSE) 1130 v 2.0 Management Server

Scalable WLAN management

- Managing up to 2500 of APs is as easy as managing a few APs

Enhances security

- Rogue AP detection and location
- Fast roaming with secure authentication
  - <150msec total latency (roaming latency plus LEAP re-authentication latency)
  - Designed for the demands of voice applications
- IEEE 802.1x local authentication service
- Security policy monitoring
- Wi-Fi Protected Access (WPA) support

Extends the Security and Reliability of the Wired LAN to the Wireless LAN

The Cisco Structured Wireless-Aware Network provides intuitive and comprehensive reports for troubleshooting and capacity planning. It assists in pinpointing problems with utilizations and client associations to help maximize network uptime. It also allows client tracking, WLAN performance reports and fault monitoring to make network troubleshooting easier.

CiscoWorks Wireless LAN Solution Engine version 2.0

- Manage up to 2500 access points
- Simplified management of hundreds to thousands of central or remotely located access points
- Enhanced troubleshooting and diagnostic tools for proactive performance and fault monitoring
- Security policy monitoring
- Seamless delivery of enhanced network security solutions

The CiscoWorks Wireless LAN Solution Engine (WLSE) is a turnkey, centralized management solution for the entire Cisco Aironet® Wireless LAN infrastructure. The CiscoWorks WLSE is part of the Cisco Structured Wireless-Aware Network framework for deploying, maintaining and monitoring a secure, fully integrated, enterprise-class wireless LAN infrastructure. This unique Cisco framework introduces "wireless aware" capabilities into the Cisco infrastructure to extend to the WLAN the same level of security, scalability, and reliability that customers have come to expect in their wired LAN.

Target Customers

Enterprise customers implementing Cisco Aironet wireless LAN infrastructures, who want to simplify daily operation and management and enhance security. Typical devices managed: AP1100, AP1200, AP340, AP350, ACS

Benefits

- Simplifies operation and management of medium and large scale wireless LANs
- Saves time and resources by automating repetitive, time-consuming tasks and centralizing management activities
- Improves wireless LAN availability by proactive fault monitoring and by providing trouble shooting tools to quickly resolve problems
- Enhances security by monitoring polices and 802.1X performance and with release 2.5, will detect & mitigate against rogue access points
- Helps in wireless LAN capacity planning and by identifying the most utilized access points, and with release 2.5 enhances network performance by detecting and locating interference determining optimal settings for access points

Streamlined WLAN Management and Operations

The CiscoWorks WLSE 2.x of the Cisco Structured Wireless-Aware Network supports unattended mass access point firmware upgrades and configuration changes over both local and wide area networks. This allows deployment and management of hundreds to thousands of access points to be effortlessly managed. Firmware for all Cisco Aironet Series access points can be updated using CiscoWorks WLSE 2.x.

Other management and operations features include:

- Proactive fault and performance monitoring based on user-defined thresholds
- Centralized auto configuration of newly deployed access points
- Configuration archive of Cisco access points
- Security policy and fault/performance monitoring of the Cisco WLAN infrastructure
- Integration with existing network management infrastructure (SOAP/XML interface, Simple Network Management Protocol (SNMP) traps and Syslog messages)
- XML API for data export
- Integration with CiscoWorks LMS
- Centralized mass conversion of Cisco Aironet 1200 Series access point VxWorks operating system configuration files into Cisco IOS Software configuration files using an expanded version of the Cisco Aironet Conversion Tool for Cisco IOS Software

Rogue Access Point Detection and Location

(Available fourth quarter 2003)

The Cisco Structured Wireless-Aware Network detects, isolates, and mitigates rogue access points. Unauthorized access points installed by employees for their own or department use are a major concern to network managers. These employees typically install these access points because they are in coverage "dead" spots or because they are unsatisfied with the capacity supplied by their wired LANs. Unauthorized employee-installed access points create a parallel wireless LAN infrastructure that allows any user with a client adapter card to connect to the network. These rogue access points create an unsecured wireless LAN connection that puts the entire wired network at risk.

Employee-installed rogue access points are becoming more common as the demand for wireless networking increases, the cost of access points decreases, and access point installation becomes easier. Today, installing an access point is as easy as plugging the access point into an Ethernet port.

It is a distinct possibility that most enterprises, including those that have not rolled out a sanctioned wireless infrastructure, have some rogue access points installed. Technically savvy employees who see the benefit of wireless networking will often install wireless LANs for their convenience without IT or company approval. Not surprisingly, employee-installed access points are greatly reduced in companies that have corporate-sanctioned WLAN infrastructures.

The second type of rogue access point found today in enterprise organizations is the malicious rogue. This is an access point installed by an intruder attempting to gain unauthorized access to the enterprise facility. Malicious rogue access points may be placed outside a facility against an external wall or placed within the enterprise in a hidden location. Because access points broadcast their signals through walls, these hidden access points allow an intruder to gain undetected access to an enterprise network. While much less common than employee installed rogue access points, malicious rogues present a greater risk and challenge because they are intentionally hidden from physical and network view.

Until the Cisco Structured Wireless-Aware Network, network managers had difficulty finding and disabling rogue access points. Prior to this new Cisco framework, network managers needed to walk the entire length of the network with an air-sniffing device to locate rogue devices. This manual, time-consuming and costly task had to be repeated on a regular basis in order to detect newly installed rogue access points. With the Cisco Structured Wireless-Aware Network, this process is automated. IT managers can now easily and automatically detect, locate, and disable rogue access points.

Fast Secure Roaming

Fast secure roaming allows authenticated client devices to roam securely from one access point to another without any perceptible delay during reassociation (Figure 2). Fast secure roaming supports latency-sensitive applications such as wireless voice over IP (VoIP), enterprise resource planning (ERP), or Citrix-based solutions, without dropping connections during roaming. WDS provides fast, secure handoff services to access points for <150ms roaming within a subnet. Cisco fast secure roaming requires Cisco or Cisco Compatible client devices that support the Cisco Centralized Key Management (CCKM) protocol.

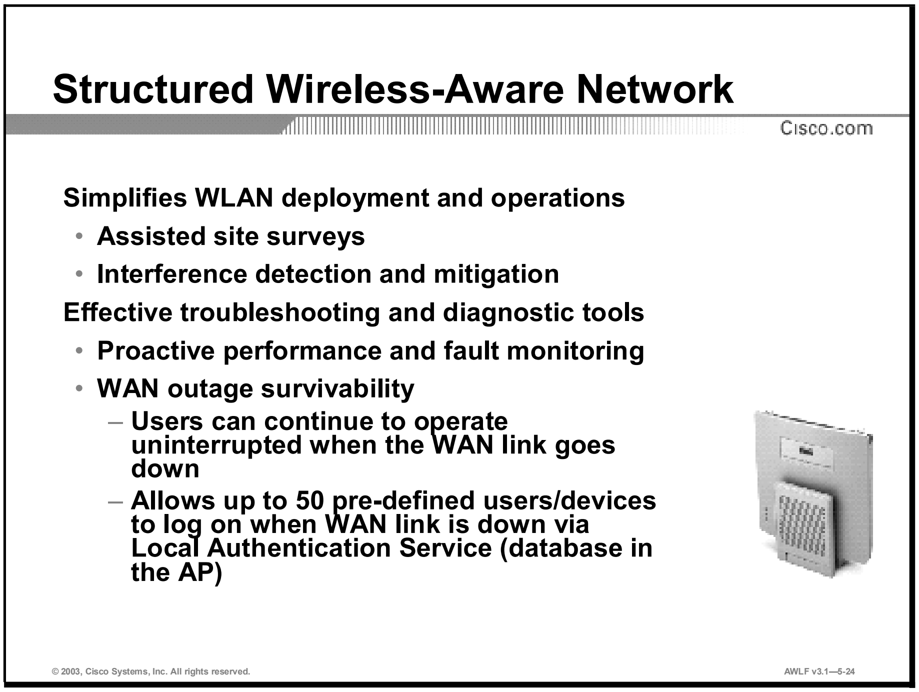
Fast Secure Roaming Across Subnets—Layer 3 Mobility

For deployments that require mobility across subnet boundaries, Cisco is developing an easy-to-configure, scalable solution that builds on the solid foundation of the Cisco Structured Wireless-Aware Network. This solution will be supported across Cisco devices, including Cisco Aironet access points, and specific Cisco Catalyst® LAN switches and Cisco routers.

IEEE 802.1X Local Authentication Service

With IEEE 802.1X local authentication service, Cisco Aironet access points are configured to act as a local Remote Authentication Dial-In User Service (RADIUS) server to authenticate wireless clients when the authentication, authorization, and accounting (AAA) server is not available. This provides authentication services for remote or branch office WLANs without a RADIUS server and backup authentication services during wide area network (WAN) link or server failure to provide access to local resources like file servers or printers.

IEEE 802.1X local authentication can support the authentication of up to 50 accounts for a given deployment in the local Cisco LEAP authentication database on the access point. One account is equal to one user name and password. The configuration of the IEEE 802.1X local authentication database can be centrally managed with the CiscoWorks WLSE 2.x management appliance. The access point with the IEEE 802.1X local authentication service does not need to be dedicated to the IEEE 802.1X local authentication service. This access point can function as a regular access point in addition to providing IEEE 802.1X local authentication.



Structured Wireless-Aware Network

Simplifies WLAN deployment and operations

- Assisted site surveys
- Interference detection and mitigation

Effective troubleshooting and diagnostic tools

- Proactive performance and fault monitoring
- WAN outage survivability
  - Users can continue to operate uninterrupted when the WAN link goes down
  - Allows up to 50 pre-defined users/devices to log on when WAN link is down via Local Authentication Service (database in the AP)

Simplified Wireless LAN Deployment with Assisted Site Survey Tool

(Available fourth quarter 2003)

Site surveys are a necessary part of the WLAN deployment process. It is only with a detailed onsite, site survey that complete and reliable WLAN coverage is achieved. Most organizations contract consultants to perform their site surveys. Unfortunately, hiring a consultant to perform site surveys for large-scale deployments and particularly those in geographically distributed locations is expensive and time-consuming.

Despite the high cost of site surveys, today's consultants use unsophisticated tools to perform them. They make initial access point placement decisions and channel selections based on radio frequency measurements, experience and intuition. They test the coverage area and signal quality of their provisionally placed access points by walking around the coverage area with a WLAN client adapter and monitoring software. They then make final adjustments to access point placement, orientation, and transmit settings based upon their testing results. Training a member of the IT staff to perform site surveys using this method is not cost-effective because site surveys are typically one-time events that need to occur at each distinct location—potentially hundreds of miles away for large scale branch office deployments.

With the Cisco Structured Wireless-Aware Network IT managers can perform cost-effective site surveys in-house without consultants—saving company time and money. With the wireless-aware network, site surveys are completed using site survey tools integrated into the CiscoWorks WLSE. With these tools, IT professionals who are not well versed in RF propagation and measurement can successfully complete a site survey.

The Cisco Structured Wireless-Aware Network assisted site survey tool in the CiscoWorks WLSE works in five simple steps:

1. A floor plan of the location to be surveyed is imported into the tool. The tool supports a variety of electronic file formats including .bmp, .jpg, and .gif. If an electronic file is unavailable, a rough building diagram can be drawn within the tool.

2. Initial access point locations are added to the diagram to provide a rough estimate of the number of access points required for the facility.

3. Cisco Aironet Series access points are installed in the facility at locations corresponding to their diagram placements.

4. Next, the installed Cisco Aironet Series access points are set to a site survey mode known as "AP Scan Mode" where they all assume the same channel and transmit at maximum power. In this mode, the access points detect the presence of one another and automatically select transmit power, frequency selection, and other settings to fully cover the facility area.

5. Finally, the access point RF settings are fine-tuned in the "Client Walkabout" mode. In this mode an individual walks the facility areas where coverage is needed, including the perimeter, with a client device that is sending continual RF measurements back to the Cisco Aironet Series access points.

Interference Detection

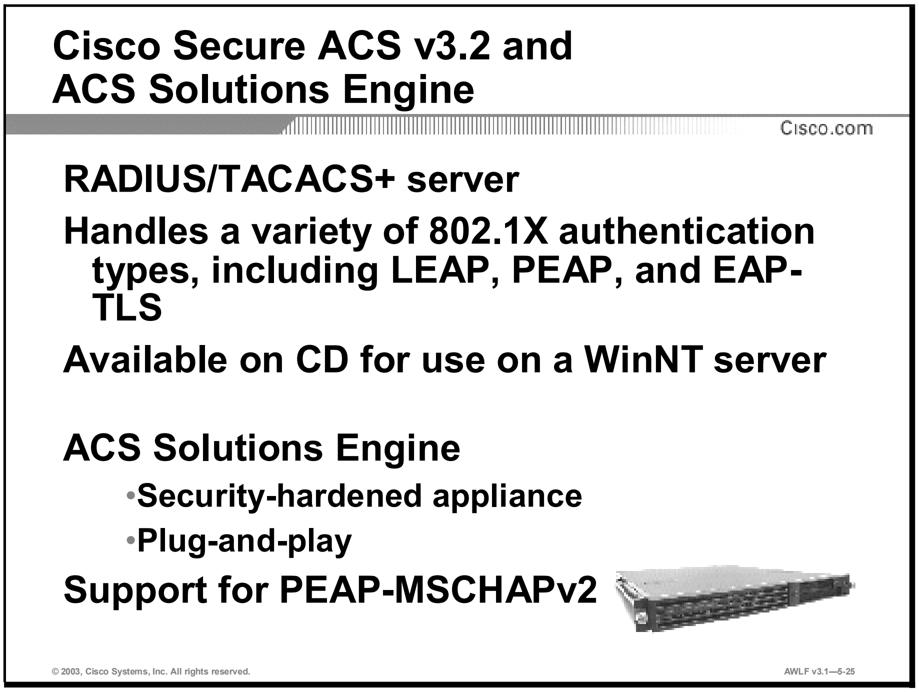
(Available fourth quarter 2003)

The Cisco Structured Wireless-Aware Network catalogues the physical location of all managed access points and creates a site map of the wireless LAN installation. This allows the wireless-aware network to detect points of interfering RF energy that are affecting network performance. The source of this unknown RF energy could be a rogue access point or a device that operates in the same frequency range such as a 2.4 GHz cordless telephone or leaky microwave oven.

Interference detection and location is key to maintaining a reliable WLAN. RF measurements sent to the CiscoWorks WLSE include measurements for both IEEE 802.11 and non- IEEE 802.11 interference. If the interference exceeds an administrator-defined threshold, a fault is generated so the administrator can quickly locate and suppress the source of the interference.

Enhanced Troubleshooting and Diagnostic Tools

Network downtime is a great expense for any enterprise. When WLAN network users lose connectivity, their productivity is compromised. Therefore, helping to ensure network uptime and reliability is a central requirement for wireless LANs. However, troubleshooting WLANs is more complicated and time consuming due to the nature of the RF infrastructure.



Cisco Secure ACS v3.2 and ACS Solutions Engine

RADIUS/TACACS+ server

Handles a variety of 802.1X authentication types, including LEAP, PEAP, and EAP-TLS

Available on CD for use on a WinNT server

ACS Solutions Engine

- Security-hardened appliance
- Plug-and-play

Support for PEAP-MSCHAPv2

AWLF v3.1—5-25

Wireless Security

A wide selection of Remote Access Dial-In User Service (RADIUS) servers that support these same authentication types can be used for scalable, centralized user management. When Cisco Aironet access points are used in conjunction with Cisco Catalyst intelligent switches, many of the security features of the wired LAN can be extended to the wireless LAN, further protecting organizations against internal and external threats.

Seamless Delivery of Enhanced Network Security

In addition to providing IEEE 802.1X local authentication service, the Cisco Structured Wireless-Aware Network provides extensive security management features that use the Cisco Wireless Security Suite including:

- Security policy monitoring—Monitoring of security policies for predefined Cisco Wireless Security Suite parameters across all access points is included. Alerts are generated for violations in areas such as Service Set Identifiers (SSID), broadcasts, 802.1X EAP settings, and wired equivalent privacy (WEP). Alerts can be delivered via e-mail, Syslog or SNMP trap notifications.
- Centralization of security settings—Parameters such as 802.1X EAP, WEP and W-Fi Protected Access (WPA) are ensured through centralized WLAN management of all local and remote access point settings.
- Monitoring of the 802.1X EAP RADIUS or AAA server—The RADIUS or AAA server providing support for Cisco LEAP and Protected-EAP (PEAP) is monitored and the availability of Cisco Secure ACS and Committed Access Rate (CAR) EAP servers is verified.
- Client device response time monitoring—The client device response time is monitored by simulating a client device via CiscoWorks WLSE.
- Notification of 802.1X EAP RADIUS or AAA server management thresholds—Notifications of user-defined security thresholds are managed via e-mail, Syslog, and SNMP trap notifications.

- IEEE 802.11i AES encryption support—Future support for IEEE 802.11i AES encryption is planned.

Summary

User authentication, authorization and accounting (AAA) access control framework that manages user and administrative access to the network. The Cisco Secure ACS is a highly scalable, high-performance access control server that operates as a centralized RADIUS server or TACACS+ server. The Cisco Secure ACS extends access security by combining authentication, user or administrator access, and policy control from a centralized identity networking solution, thereby allowing for greater flexibility and mobility, increased security, and user productivity gains. Cisco Secure ACS is a key component of Cisco's IBNS solution—an architecture built upon the 802.1X port based network access control IEEE standard. As a centralized authentication server, Cisco Secure ACS brings in RADIUS based AAA capabilities inside the LAN for both wired and wireless networks.

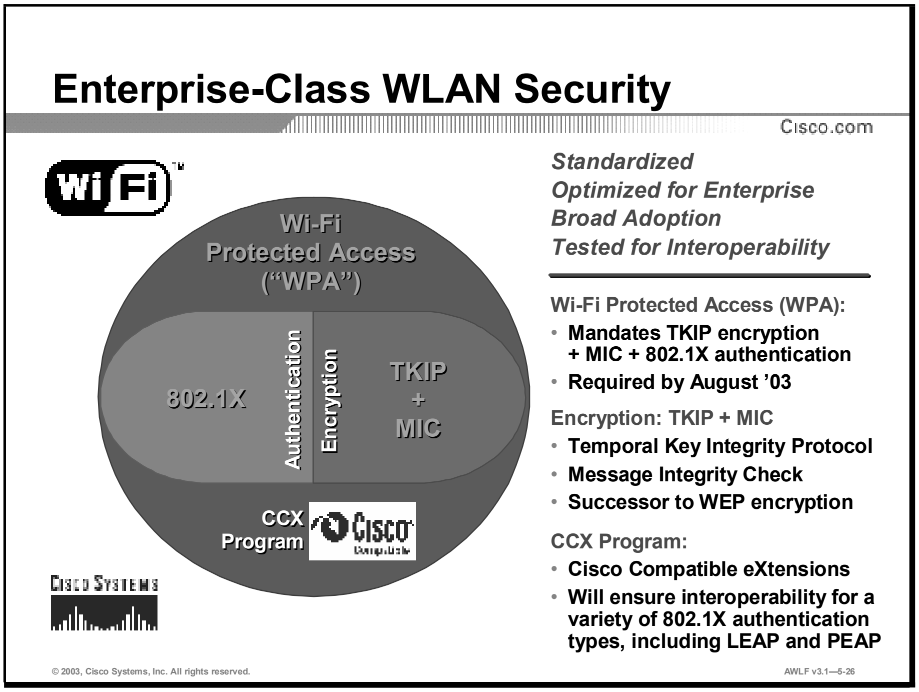
Target Customers

- Business type: Enterprises with remote access, VPN, firewall, content, storage, Voice-over IP, wireless and 802.1x switched LAN networks that need to control user access
- Networking Infrastructure: All customers using TACACS+ to control device administrative management for routers, switches, VPNs, PIX firewalls, and security managements applications (such as VMS)
- Typical devices managed: 2500, 3600, 1700, 7200, 7500 routers, Access Servers

Benefits

- Save time by managing all user access, authorization and accounting from central management tool
- Enhance network security by controlling user and administrative access to the network
- Reduce costs by deploying single, integrated user profile management system
- Track and audit user and administrative behavior via accounting service
- Interoperates with Cisco and all networking solutions that support either the RADIUS or TACACS+ protocols
- Cisco Secure ACS is now available on a “hardened” appliance for increased security, a plug and play solution, and faster, one-stop supportability

Enterprise-Class WLAN Security



Enterprise-Class WLAN Security

Cisco.com

Standardized
Optimized for Enterprise
Broad Adoption
Tested for Interoperability

Wi-Fi Protected Access (WPA):
- **Mandates TKIP encryption + MIC + 802.1X authentication**
- **Required by August '03**

Encryption: TKIP + MIC
- **Temporal Key Integrity Protocol**
- **Message Integrity Check**
- **Successor to WEP encryption**

CCX Program:
- **Cisco Compatible eXtensions**
- **Will ensure interoperability for a variety of 802.1X authentication types, including LEAP and PEAP**

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—5-26

The Cisco Wireless Security Suite provides strong, enterprise-class wireless LAN security based on IEEE 802.1X authentication and pre-standard Temporal Key Integrity Protocol (TKIP) enhancements to 40- and 128-bit wired equivalent privacy (WEP) encryption. As a Layer 2 authentication protocol, 802.1X supports mutual validity between the user and the authentication server, ensuring clients are not allowed onto the network until their credentials are individually validated. This is a major improvement upon first-generation wireless LANs, as the authentication specifications in the original 802.11 wireless LAN standard provided only a rudimentary level of shared or static client authentication, which was difficult to manage and easily compromise. With 802.1X, the credentials used for authentication, such as a log-on password, are never transmitted over wireless connections without encryption. In enterprise environments, mutual authentication can also confirm the validity of the access point through which the user is attempting to connect. This protects the organization from so-called "rogue access points" being used as gateways into the network or as diversion points away from the legitimate network. The Cisco Wireless Security Suite also addresses the weaknesses of WEP protection schemes: the ability of intruders to crack WEP encryption keys. Without the right safeguards, hackers can passively or actively monitor and analyze packets of wireless data, and use this information to break the WEP key that encrypts those packets. The Cisco Wireless Security Suite provides several enhancements to WEP keys, both static WEP keys and the dynamic per-user, per-session WEP keys that are derived as a result of successful 802.1X authentication. These WEP enhancements include pre-standard TKIP support for message integrity check (MIC), per-packet key hashing, and broadcast key rotation. MIC thwarts efforts to decipher WEP encryption keys using intercepted packets.

Using MIC, packets that have been modified in transit are dropped. Per-packet key hashing ensures that the base key of every packet is hashed with an initialization vector (IV) to create a new key for each packet. In this way, key hashing removes the predictability that an intruder relies on to determine the WEP key by exploiting weak IVs. Broadcast key rotation eliminates broadcast keys' susceptibility to the same attacks as unicast or static WEP keys. The Cisco Wireless Security Suite interoperates with a range of client devices, and supports

all 802.1X authentication types, including EAP Cisco Wireless (LEAP), Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), and types that operate over EAP-TLS, such as Protected Extensible Authentication Protocol (PEAP), EAP Tunneled TLS (EAP-TTLS), and EAP-Subscriber Identity Module (EAP-SIM).

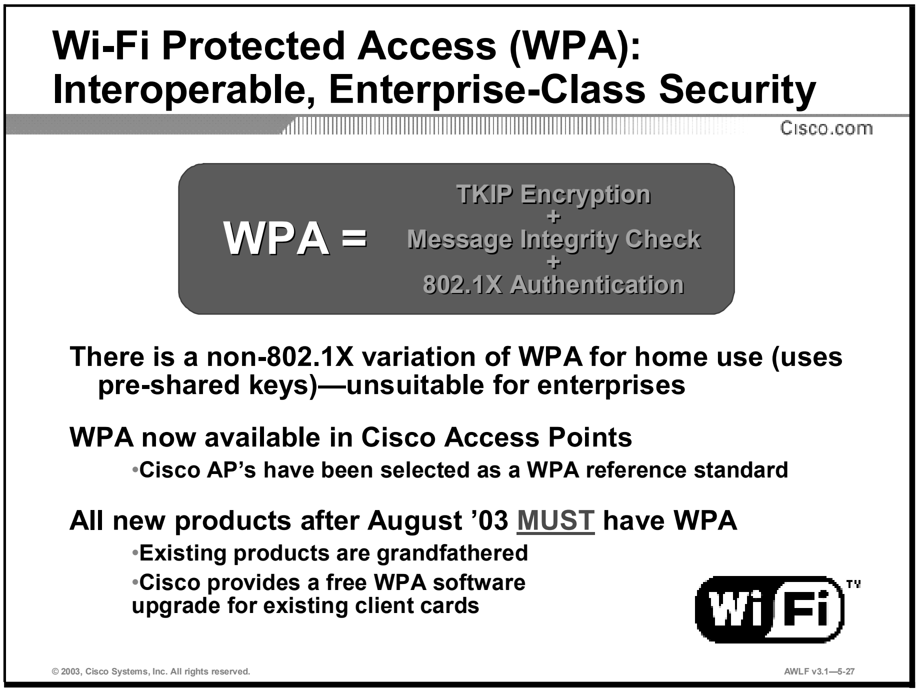
Wireless Security

A wide selection of Remote Access Dial-In User Service (RADIUS) servers that support these same authentication types can be used for scalable, centralized user management. When Cisco Aironet access points are used in conjunction with Cisco Catalyst intelligent switches, many of the security features of the wired LAN can be extended to the wireless LAN, further protecting organizations against internal and external threats. A wide selection of Remote Access Dial-In User Service (RADIUS) servers that support these same authentication types can be used for scalable, centralized user management. When Cisco Aironet access points are used in conjunction with Cisco Catalyst intelligent switches, many of the security features of the wired LAN can be extended to the wireless LAN, further protecting organizations against internal and external threats.

A variety of OEMs have committed to providing Cisco Compatible products in their laptops. This program enables suppliers of WLAN client devices the ability to design current and future Cisco wireless innovations, such as LEAP, into their products. Not only will these products be available in a variety of form factors and operating systems, but they will assure interoperability with Cisco wireless networks via independent third party testing.

For Cisco WLAN customers, the Cisco Compatible Extensions program:

- Delivers the confidence to IT personnel to deploy Cisco wireless networks with a greater selection of Cisco Compatible WLAN ready clients
- Provides tested compatibility with licensed Cisco infrastructure innovations
- Enables widespread availability of wireless client devices leveraging the Cisco wireless network
- Accelerates the availability of innovative features while maintaining interoperability
- Promotes investment protection of client devices with Cisco Compatible Extensions by maintaining compatibility with industry standards and Cisco infrastructure features



Wi-Fi Protected Access (WPA): Interoperable, Enterprise-Class Security

Cisco.com

WPA = TKIP Encryption + Message Integrity Check + 802.1X Authentication

There is a non-802.1X variation of WPA for home use (uses pre-shared keys)—unsuitable for enterprises

WPA now available in Cisco Access Points

- Cisco AP's have been selected as a WPA reference standard

All new products after August '03 MUST have WPA

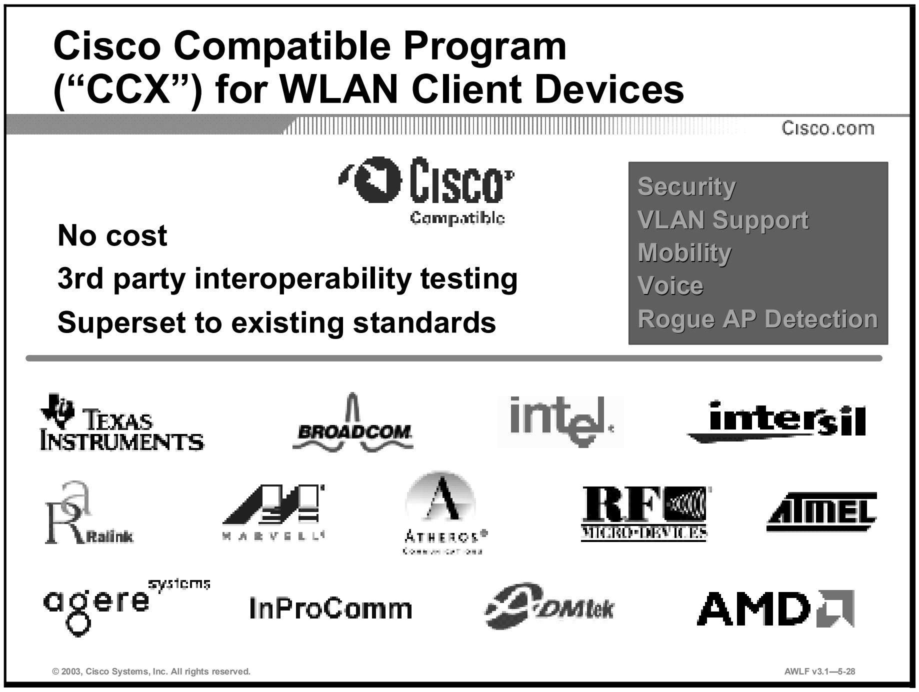
- Existing products are grandfathered
- Cisco provides a free WPA software upgrade for existing client cards

AWLF v3.1—5-27

Wireless LAN security is a primary concern. The Cisco Aironet 1200 Series secures the enterprise network with a scalable and manageable system featuring the award-winning Cisco Wireless Security Suite. Based on the 802.1X standard for port-based network access, the Cisco Wireless Security Suite takes advantage of the Extensible Authentication Protocol (EAP) framework for user-based authentication. This solution also supports Wi-Fi Protected Access (WPA) the new Wi-Fi Alliance specification for interoperable, standards-based wireless LAN security. It supports IEEE 802.1X authentication using extensible authentication protocol (EAP) authentication types and temporal key integrity protocol (TKIP) encryption.

The Cisco Wireless Security Suite interoperates with a range of client devices. It supports all 802.1X authentication types, including Cisco LEAP, Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) and types that operate over EAP-TLS, such as Protected Extensible Authentication Protocol (PEAP), EAP-Tunneled TLS (EAP-TTLS) and EAP-Subscriber Identity Module (EAP-SIM). A wide selection of RADIUS servers, such as the Cisco Secure Access Control Server (ACS), can be used for enterprise-class centralized user management that includes:

- Strong, mutual authentication to ensure that only legitimate clients associate with legitimate and authorized network RADIUS servers
- Dynamic per-user, per-session encryption keys that automatically change on a configurable basis to protect the privacy of transmitted data
- Stronger WEP keys provided by Temporal Key Integrity Protocol (TKIP) enhancements such as message integrity check (MIC), per-packet keys via initialization vector hashing, and broadcast key rotation
- RADIUS accounting records for all authentication attempts



Cisco Compatible Program ("CCX") for WLAN Client Devices

Cisco.com

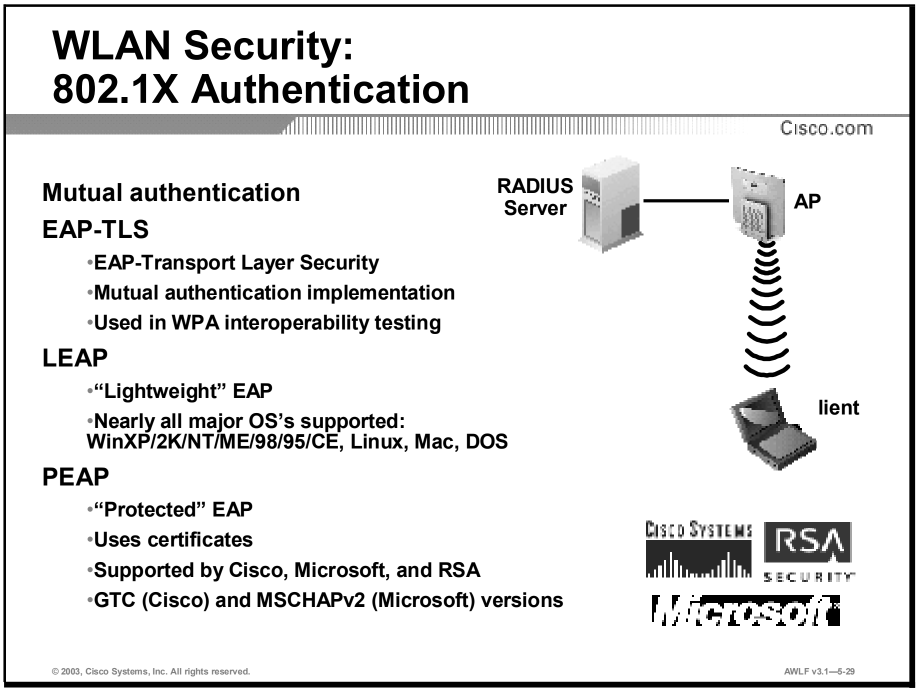
Cisco Compatible

- No cost
- 3rd party interoperability testing
- Superset to existing standards

- Security
- VLAN Support
- Mobility
- Voice
- Rogue AP Detection

Texas Instruments
Broadcom
intel
intersil
Ralink
Marvell
Atheros Communications
RF Micro-Devices
Atmel
agere systems
InProComm
ADMtek
AMD

AWLF v3.1—5-28



WLAN Security: 802.1X Authentication

Cisco.com

Mutual authentication

EAP-TLS

- EAP-Transport Layer Security
- Mutual authentication implementation
- Used in WPA interoperability testing

LEAP

- “Lightweight” EAP
- Nearly all major OS’s supported: WinXP/2K/NT/ME/98/95/CE, Linux, Mac, DOS

PEAP

- “Protected” EAP
- Uses certificates
- Supported by Cisco, Microsoft, and RSA
- GTC (Cisco) and MSCHAPv2 (Microsoft) versions

AWLF v3.1—5-29

The Cisco Wireless Security Suite provides strong, enterprise-class wireless LAN security based on IEEE 802.1X authentication and pre-standard Temporal Key Integrity Protocol (TKIP) enhancements to 40- and 128-bit wired equivalent privacy (WEP) encryption. As a Layer 2 authentication protocol, 802.1X supports mutual validity between the user and the authentication server, ensuring clients are not allowed onto the network until their credentials are individually validated. This is a major improvement upon first-generation wireless LANs, as the authentication specifications in the original 802.11 wireless LAN standard provided only a rudimentary level of shared or static client authentication, which was difficult to manage and easily compromised. With 802.1X, the credentials used for authentication, such as a log-on password, are never transmitted over wireless connections without encryption.

In enterprise environments, mutual authentication can also confirm the validity of the access point through which the user is attempting to connect. This protects the organization from so-called “rogue access points” being used as gateways into the network or as diversion points away from the legitimate network.

The Cisco Wireless Security Suite also addresses the weaknesses of WEP protection schemes: the ability of intruders to crack WEP encryption keys. Without the right safeguards, hackers can passively or actively monitor and analyze packets of wireless data, and use this information to break the WEP key that encrypts those packets.

The Cisco Wireless Security Suite provides several enhancements to WEP keys, both static WEP keys and the dynamic per-user, per-session WEP keys that are derived as a result of successful 802.1X authentication. These WEP enhancements include pre-standard TKIP support for message integrity check (MIC), per-packet key hashing, and broadcast key rotation.

MIC thwarts efforts to decipher WEP encryption keys using intercepted packets. Using MIC, packets that have been modified in transit are dropped. Per-packet key hashing ensures that the base key of every packet is hashed with an initialization vector (IV) to create a new key for each packet. In this way, key hashing removes the predictability that an intruder relies on to determine the WEP key by exploiting weak IVs. Broadcast key rotation eliminates broadcast keys’ susceptibility to the same attacks as unicast or static WEP keys.

The Cisco Wireless Security Suite interoperates with a range of client devices, and supports all 802.1X authentication types, including EAP Cisco Wireless (LEAP), Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), and types that operate over EAP-TLS, such as Protected Extensible Authentication Protocol (PEAP), EAP Tunneled TLS (EAP-TTLS), and EAP-Subscriber Identity Module (EAP-SIM).

A wide selection of Remote Access Dial-In User Service (RADIUS) servers that support these same authentication types can be used for scalable, centralized user management. When Cisco Aironet access points are used in conjunction with Cisco Catalyst intelligent switches, many of the security features of the wired LAN can be extended to the wireless LAN, further protecting organizations against internal and external threats.

EAP-TLS

EAP-TLS is an Internet Engineering Task Force (IETF) standard (RFC 2716) that is based on the TLS protocol (RFC 2246). EAP-TLS uses digital certificates for both user and server authentication and supports the three key elements of 802.1X/EAP mentioned previously. As shown in Figure 3, the RADIUS server sends its certificate to the client in phase 1 of the authentication sequence (server-side TLS). The client validates the RADIUS server certificate by verifying the issuer of the certificate—a certificate authority server entity—and the contents of the digital certificate.

When this is complete, the client sends its certificate to the RADIUS server in phase 2 of the authentication sequence (client-side TLS). The RADIUS server validates the client’s certificate by verifying the issuer of the certificate (certificate authority server entity) and the contents of the digital certificate. When this is complete, an EAP-Success message is sent to the client and both the client and the RADIUS server derive the dynamic WEP key.

Cisco LEAP

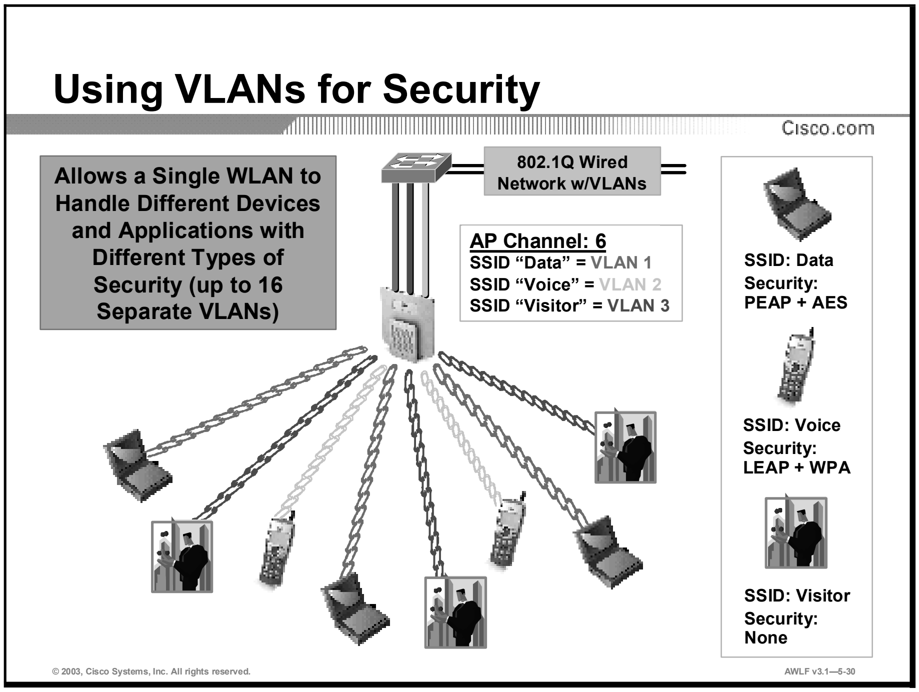
Cisco LEAP is the widely deployed EAP type in use today in WLANs. LEAP supports all three of the 802.1X and EAP elements mentioned previously. With LEAP, mutual authentication relies on a shared secret, the user’s logon password, which is known by the client and the network. As shown in Figure 2, the RADIUS server sends an authentication challenge to the client. The client uses a one-way hash of the user-supplied password to fashion a response to the challenge and sends that response to the RADIUS server. Using information from its user database, the RADIUS server creates its own response and compares that to the response from the client. When the RADIUS server authenticates the client, the process repeats in reverse, enabling the client to authenticate the RADIUS server.

When this is complete, an EAP-Success message is sent to the client and both the client and the RADIUS server derive the dynamic WEP key.

PEAP

PEAP is an IETF draft RFC authored by Cisco Systems, Microsoft, and RSA Security. PEAP uses a digital certificate for server authentication. For user authentication, PEAP supports various EAP-encapsulated methods within a protected TLS tunnel. PEAP supports the three main elements of 802.1X/EAP, as mentioned previously. As shown in Figure 4, phase 1 of the authentication sequence is the same as that for EAP-TLS (server-side TLS). At the end of phase 1, an encrypted TLS tunnel is created between the user and the RADIUS server for transporting EAP authentication messages. In phase 2, the RADIUS server authenticates the client through the encrypted TLS tunnel via another EAP type. As an example, a user can be authenticated using an OTP using the EAP-GTC subtype (as defined by the PEAP DRAFT). In this case, the RADIUS server will relay the OTP credentials (user ID and OTP) to an OTP server to validate the user login.

When this is complete, an EAP-Success message is sent to the client and both the client and the RADIUS server derive the dynamic WEP key. For more information on PEAP, refer to the IETF Web site for the latest draft.



Using VLANs for Security

Allows a Single WLAN to Handle Different Devices and Applications with Different Types of Security (up to 16 Separate VLANs)

802.1Q Wired Network w/VLANs

AP Channel: 6
SSID "Data" = VLAN 1
SSID "Voice" = VLAN 2
SSID "Visitor" = VLAN 3

SSID: Data
Security:
PEAP + AES

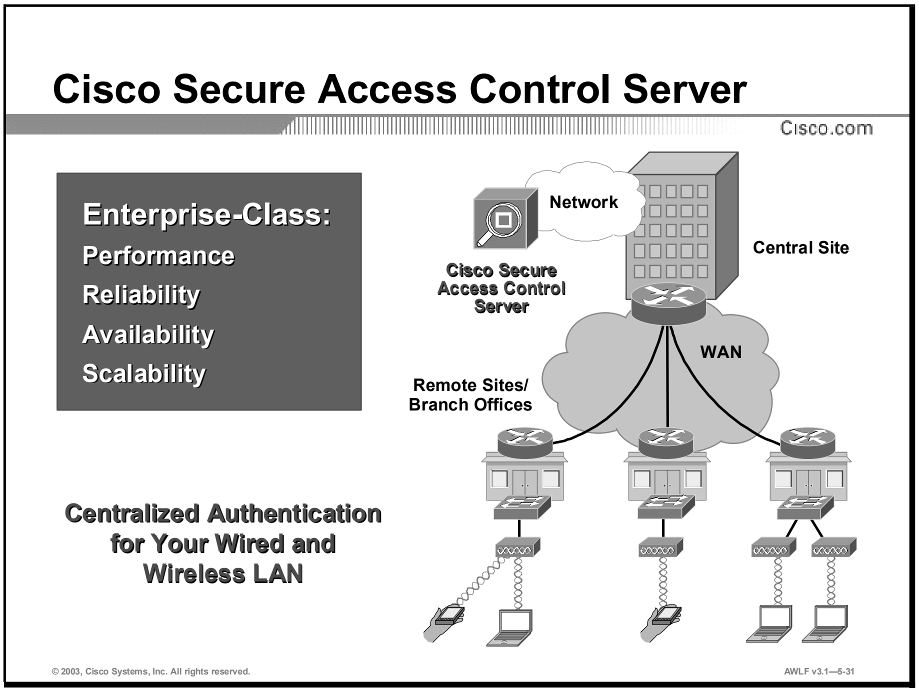
SSID: Voice
Security:
LEAP + WPA

SSID: Visitor
Security:
None

AWLF v3.1—5-30

Segregating Wireless Traffic Based on Policies and Services

The Cisco Aironet family is capable of managing up to 16 VLANs per access point. This allows customers to vary wireless LAN policies and services, such as security and QoS, to accommodate different types of users and applications. For example, enterprise customers can use different wireless VLANs to separate employee traffic from guest traffic. VLANs are ideal for providing wireless access in public areas, such as lobbies and airport lounges, without compromising network security. VLANs can also be deployed for certain applications, such as time-sensitive voice traffic, to ensure peak performance. Organizations may wish to implement VLANs to meet varying policy requirements. For example, educational institutions could take advantage of the Cisco LEAP security protocol on VLANs carrying faculty and administrator traffic, while using another authentication protocol on student VLANs to support a broader mix of client devices.



Cisco Secure Access Control Server

Cisco.com

Enterprise-Class:

Performance

Reliability

Availability

Scalability

Centralized Authentication for Your Wired and Wireless LAN

Network
Cisco Secure Access Control Server
Central Site
WAN
Remote Sites/ Branch Offices

AWLF v3.1—5-31

New in version 3.2: support for Microsoft PEAP added to existing Cisco PEAP

As security becomes increasingly important, customers are concerned about the "securability" of their systems.

The most important system to secure are the security systems themselves!

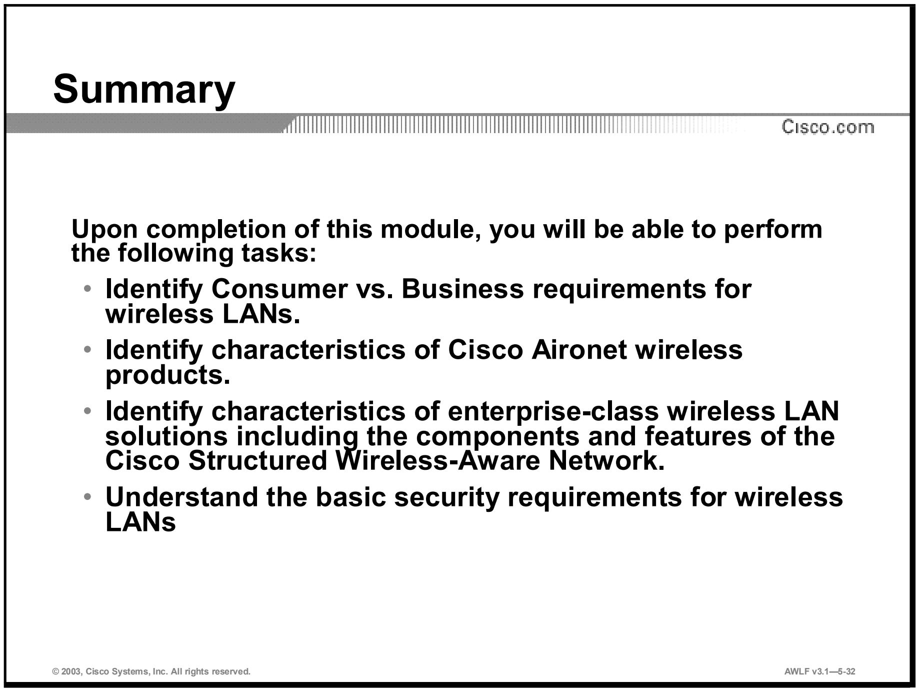
ACS is now highly secure, on a dedicated, locked-down appliance.

Network access relevant to wireless, all managed together in ACS, include (but not limited to):

- Wired/wireless LAN
- VPN
- Broadband
- Telecommuters
- Branch office
- Dialup

Summary

This section summarizes the concepts you learned in this module.



Summary

Cisco.com

Upon completion of this module, you will be able to perform the following tasks:

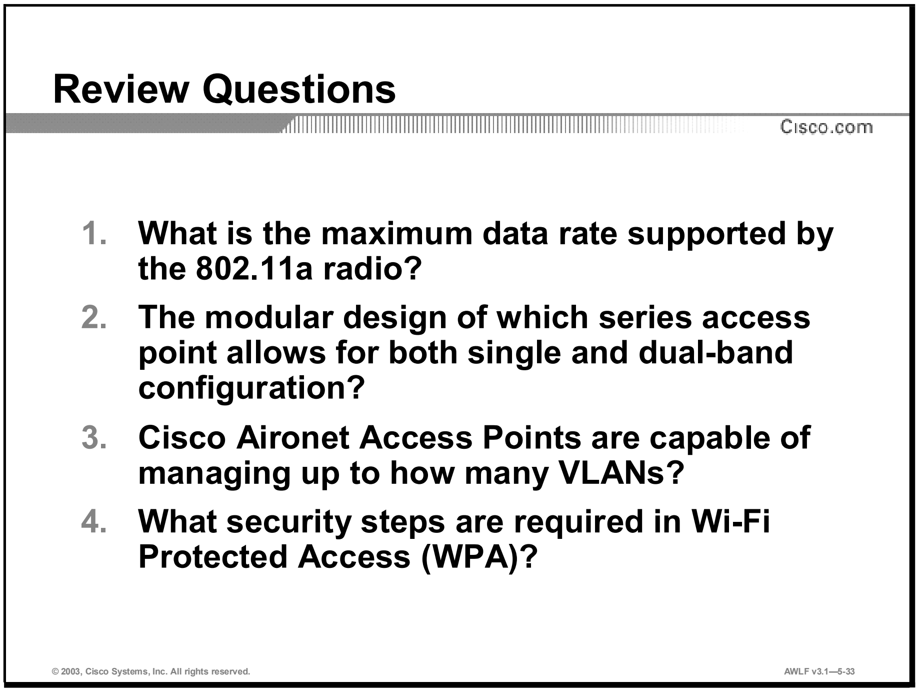
- **Identify Consumer vs. Business requirements for wireless LANs.**
- **Identify characteristics of Cisco Aironet wireless products.**
- **Identify characteristics of enterprise-class wireless LAN solutions including the components and features of the Cisco Structured Wireless-Aware Network.**
- **Understand the basic security requirements for wireless LANs**

AWLF v3.1—5-32

Upon completion of this module, you will be able to perform the following tasks:

- Identify Consumer vs. Business requirements for wireless LANs.
- Identify characteristics of Cisco Aironet products including Access Points, Clients, Bridges, Workgroup Bridges, Antennas, and Power Injectors.
- Identify characteristics of an Enterprise-Class WLAN Solutions including the components and features of the Cisco Structured Wireless-Aware Network.
- Understand the basic security requirements for wireless LANs.

Review Questions

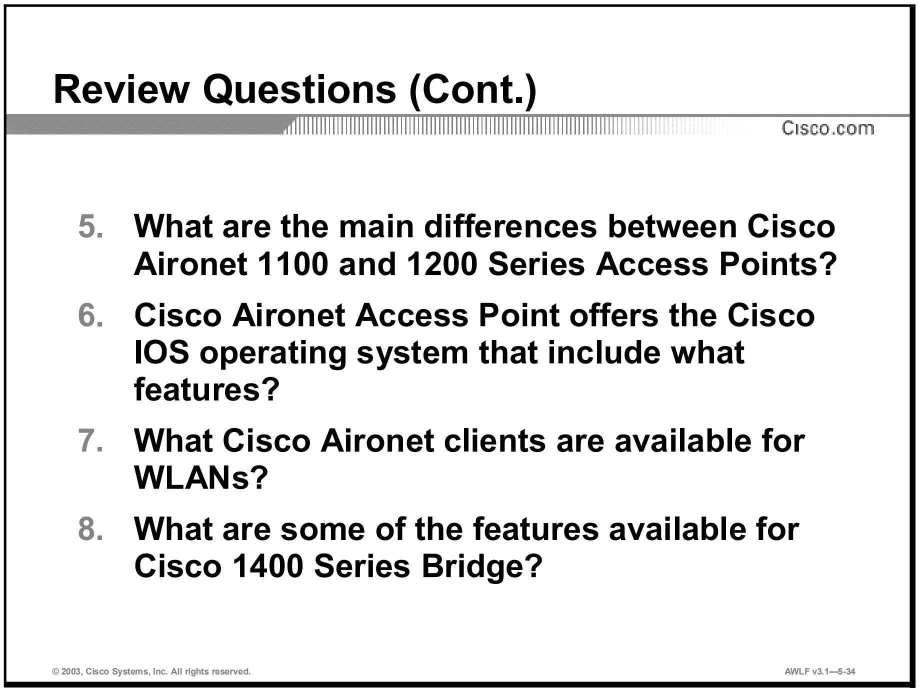


Review Questions

1. What is the maximum data rate supported by the 802.11a radio?
2. The modular design of which series access point allows for both single and dual-band configuration?
3. Cisco Aironet Access Points are capable of managing up to how many VLANs?
4. What security steps are required in Wi-Fi Protected Access (WPA)?

AWLF v3.1—5-33

Answer these review questions.



Review Questions (Cont.)

5. What are the main differences between Cisco Aironet 1100 and 1200 Series Access Points?
6. Cisco Aironet Access Point offers the Cisco IOS operating system that include what features?
7. What Cisco Aironet clients are available for WLANs?
8. What are some of the features available for Cisco 1400 Series Bridge?

AWLF v3.1—5-34

Answer these review questions.

Module 6

Antenna Concepts

Overview

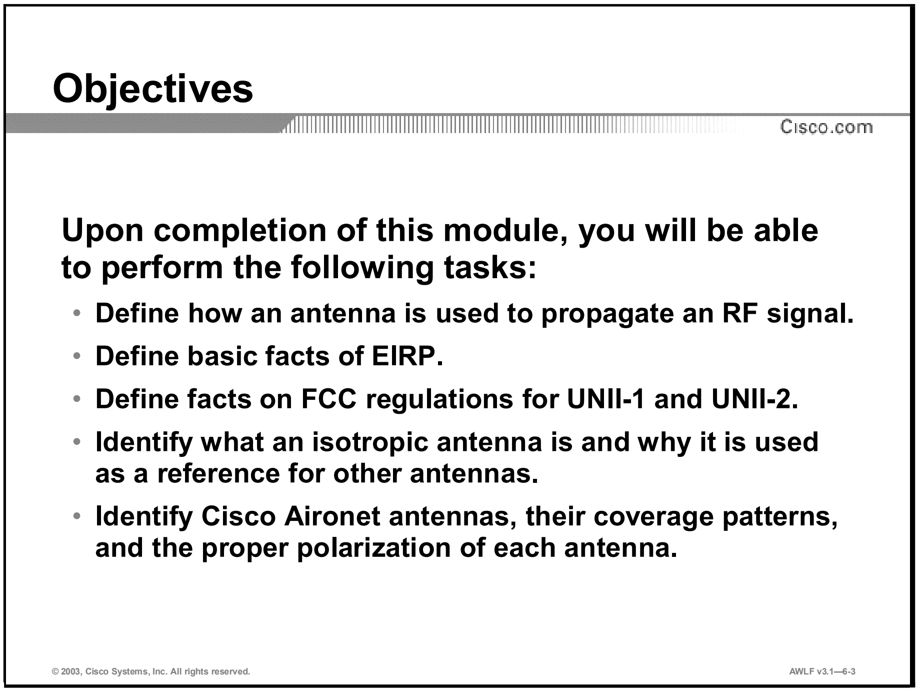
This module is an overview of how antennas are designed and how they can affect the propagation of an RF signal. It also covers the Cisco Aironet Wireless antenna offerings.

It includes the following topics:

- Objectives
- FCC Standards
- General Antenna Concepts
- Antenna Gain
- Antenna Design
- Cisco Aironet Antennas
- Cisco Aironet 1100 Series Access Point
- Summary
- Review Questions

Objectives

This section lists the module's objectives.



Objectives

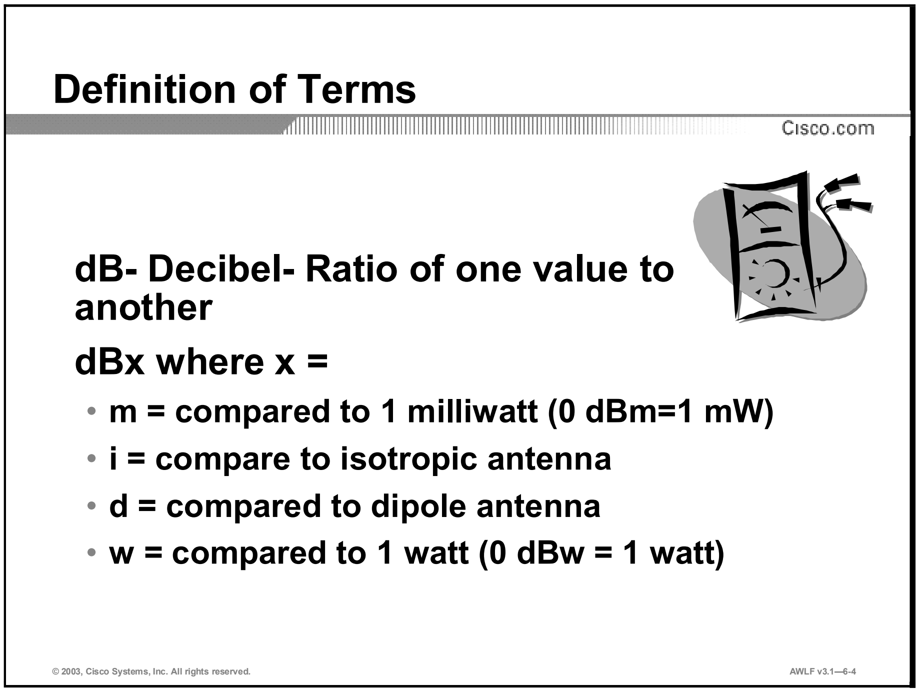
Upon completion of this module, you will be able to perform the following tasks:

- **Define how an antenna is used to propagate an RF signal.**
- **Define basic facts of EIRP.**
- **Define facts on FCC regulations for UNII-1 and UNII-2.**
- **Identify what an isotropic antenna is and why it is used as a reference for other antennas.**
- **Identify Cisco Aironet antennas, their coverage patterns, and the proper polarization of each antenna.**

AWLF v3.1—6-3

Upon completion of this module, you will be able to perform the following tasks:

- Define how an antenna is used to propagate an RF signal.
- Define basic facts of EIRP.
- Define facts on FCC regulations for UNII-1 and UNII-2.
- Identify what an isotropic antenna is and why it is used as a reference for other antennas.
- Identify Cisco Aironet antennas, their coverage patterns, and the proper polarization of each antenna.



Definition of Terms

Cisco.com

dB- Decibel- Ratio of one value to another

dBx where x =

- **m = compared to 1 milliwatt (0 dBm=1 mW)**
- **i = compare to isotropic antenna**
- **d = compared to dipole antenna**
- **w = compared to 1 watt (0 dBw = 1 watt)**

AWLF v3.1—6-4

dB (Decibel)

The difference or ratio between two signal levels. Named after Alexander Graham Bell and used to describe the effect of system devices on signal strength.

dBm (dB milliWatt)

A signal strength or power level. 0 dBm is defined as 1 mW (milliWatt) of power into a terminating load such as an antenna or power meter. Small signals are negative numbers (e.g.-83 dBm).

dBd (dB dipole)

The gain an antenna has over a dipole antenna at the same frequency. A dipole antenna is the smallest, least gain practical antenna that can be made.

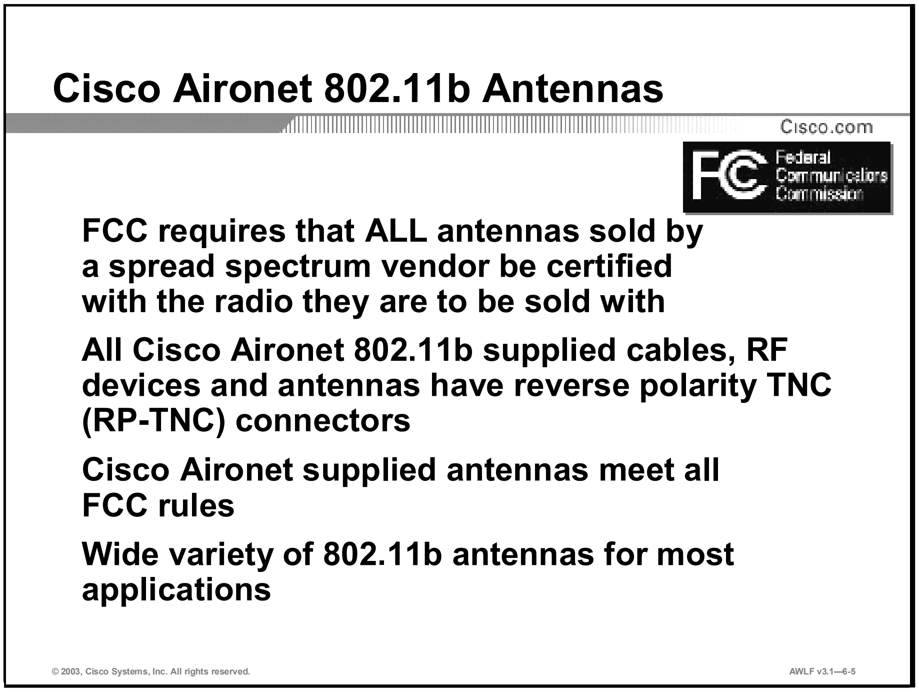
dBi (dB isotropic)

The gain a given antenna has over a theoretical isotropic (point source) antenna. Unfortunately, an isotropic antenna cannot be made in the real world, but it is useful for calculating theoretical fade and System Operating Margins.

EIRP (Effect Radiated Power)

Effect Radiated Power is defined as the effective power found in the main lobe of transmitter antenna. It is equal to sum of the antenna gain (in dBi) plus the power (in dBm) into that antenna.

FCC Standards



Cisco Aironet 802.11b Antennas

Cisco.com
FC Federal Communications Commission

FCC requires that ALL antennas sold by a spread spectrum vendor be certified with the radio they are to be sold with

All Cisco Aironet 802.11b supplied cables, RF devices and antennas have reverse polarity TNC (RP-TNC) connectors

Cisco Aironet supplied antennas meet all FCC rules

Wide variety of 802.11b antennas for most applications

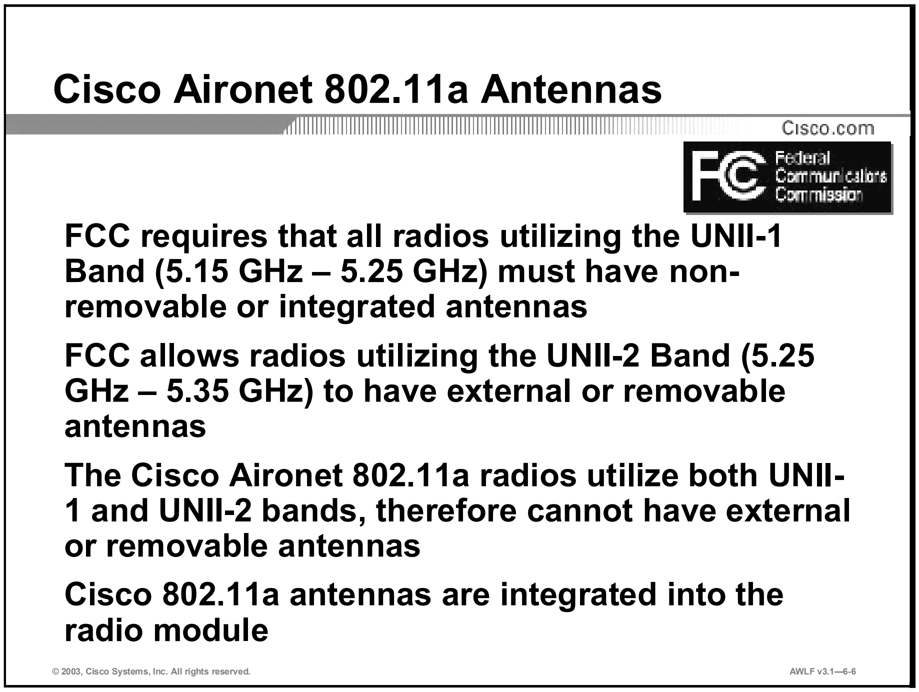
AWLF v3.1—6-5

In 1994, the FCC (and Canada's ISTC) added new rules covering spread spectrum products. These rules require than an antenna that is sold with a product MUST be tested and approved with that product.

In order to keep the "average user" from installing whatever antenna they want, the FCC also implemented a rule stating that any removable antenna had to use a unique, "non-standard" connector that is not available in general distribution channels.

Cisco Aironet 802.11b antennas and all Cisco Aironet cables use a reverse polarity TNC (RP-TNC). This connector looks like a TNC, but the center contacts have been reversed. This prohibits a standard off-the-shelf antenna from being attached to a Cisco Aironet RF product.

The FCC does permit a professional installer to use different antennas or connectors. A professional installer is defined as someone who has been trained in the applicable rules and regulations, is receiving compensation for their work, has knowledge of radio emissions, and can verify that a site which deviates from the standard product set requirements meets the limitations of the FCC rules.



Cisco Aironet 802.11a Antennas

Cisco.com

FCC requires that all radios utilizing the UNII-1 Band (5.15 GHz – 5.25 GHz) must have non-removable or integrated antennas

FCC allows radios utilizing the UNII-2 Band (5.25 GHz – 5.35 GHz) to have external or removable antennas

The Cisco Aironet 802.11a radios utilize both UNII-1 and UNII-2 bands, therefore cannot have external or removable antennas

Cisco 802.11a antennas are integrated into the radio module

AWLF v3.1—6-6

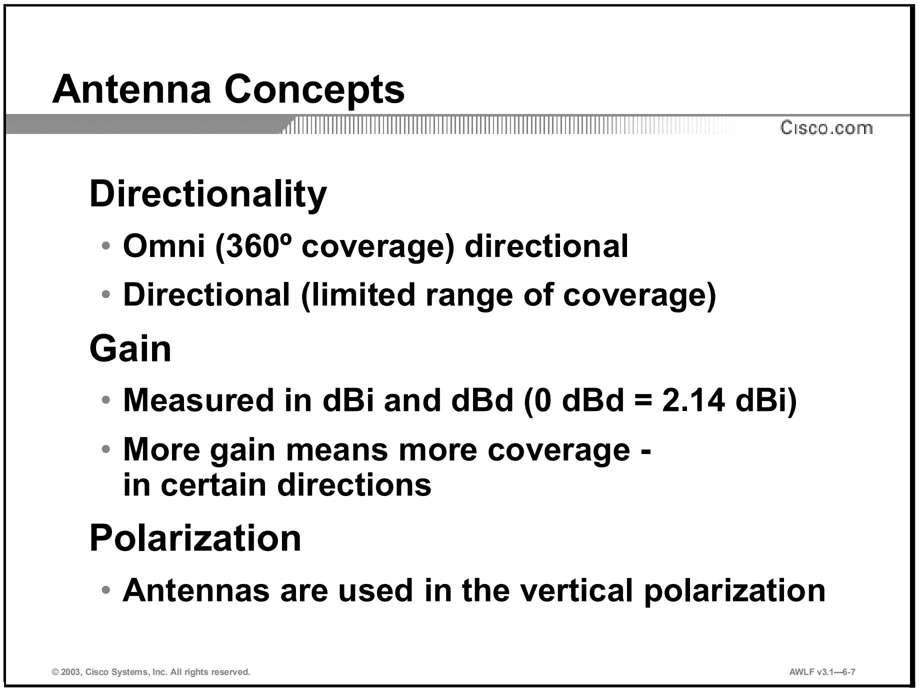
The slide discusses the FCC standards that Cisco Aironet products adhere to. The following is an excerpt from that document:

From Title 47 Section 15.407:

- (d) Any UNII device that operates in the 5.15-5.25 GHz band shall use a transmitting antenna that is an integral part of the device.

- (e) Within the 5.15-5.25 GHz band, UNII devices will be restricted to indoor operations to reduce any potential for harmful interference to co-channel MSS operations.

General Antenna Concepts



Antenna Concepts

Cisco.com

Directionality

- Omni (360º coverage) directional
- Directional (limited range of coverage)

Gain

- Measured in dBi and dBd (0 dBd = 2.14 dBi)
- More gain means more coverage - in certain directions

Polarization

- Antennas are used in the vertical polarization

AWLF v3.1—6-7

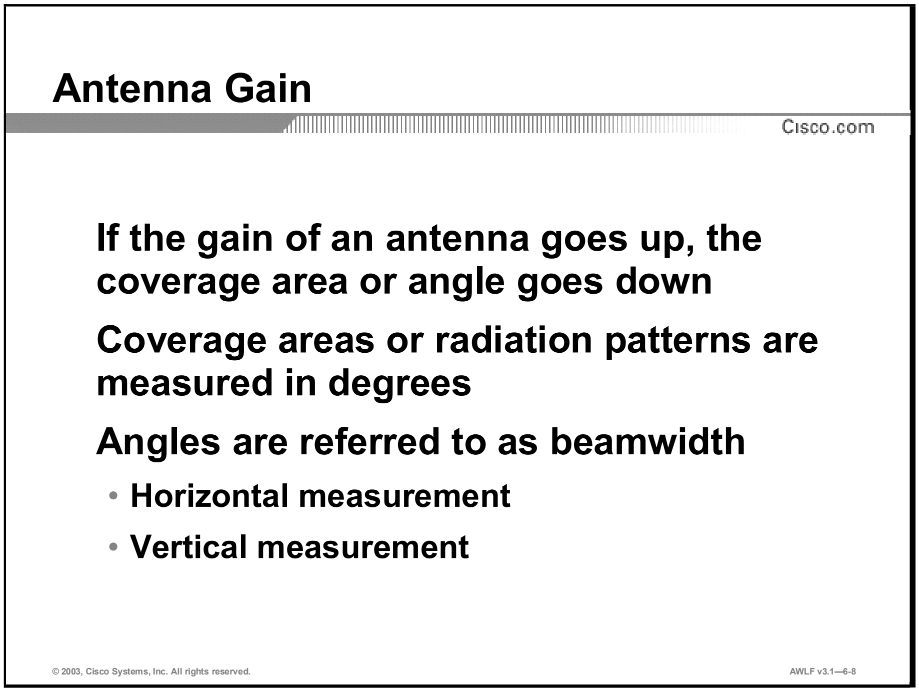
In order to understand wireless networks, as well as how to set them up and optimize them for best performance, some knowledge of antennas is essential.

In this module we will cover some of the basics of antennas and how they work, in order to give you an understanding of when to use which antenna.

There are several key terms that you need to understand:

- Gain: The amount of increase in energy that an antenna APPEARS to add to an RF signal. There are different methods for measuring this, depending on the reference point chosen. To ensure a common understanding, Cisco Aironet wireless is standardizing on dBi (which is gain using a theoretical isotropic antenna as a reference point), to specify gain measurements. Some antennas are rated in dBd, which uses a dipole type antenna, instead of an isotropic antenna, as the reference point. To convert any number from dBd to dBi, simply add 2.14 to the dBd number.
- Polarization: The physical orientation of the element on the antenna that actually emits the RF energy. An omni-directional antenna, for example, is usually a vertical polarized antenna. All Cisco Aironet antennas are set for vertical polarization.

Antenna Gain



Antenna Gain

If the gain of an antenna goes up, the coverage area or angle goes down

Coverage areas or radiation patterns are measured in degrees

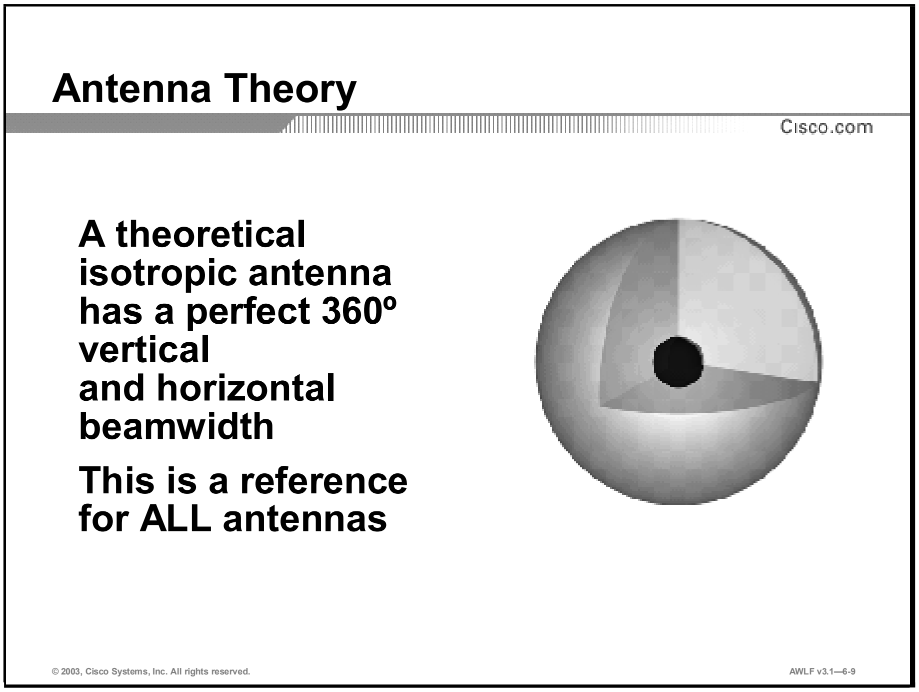
Angles are referred to as beamwidth

- Horizontal measurement
- Vertical measurement

AWLF v3.1—6-8

In RF, as with anything in life, you have to give up something to gain something else. In antenna gain, this comes in the form of coverage angle (beamwidth). As the gain of an antenna goes up, the beamwidth goes down.

Antenna Design



Antenna Theory

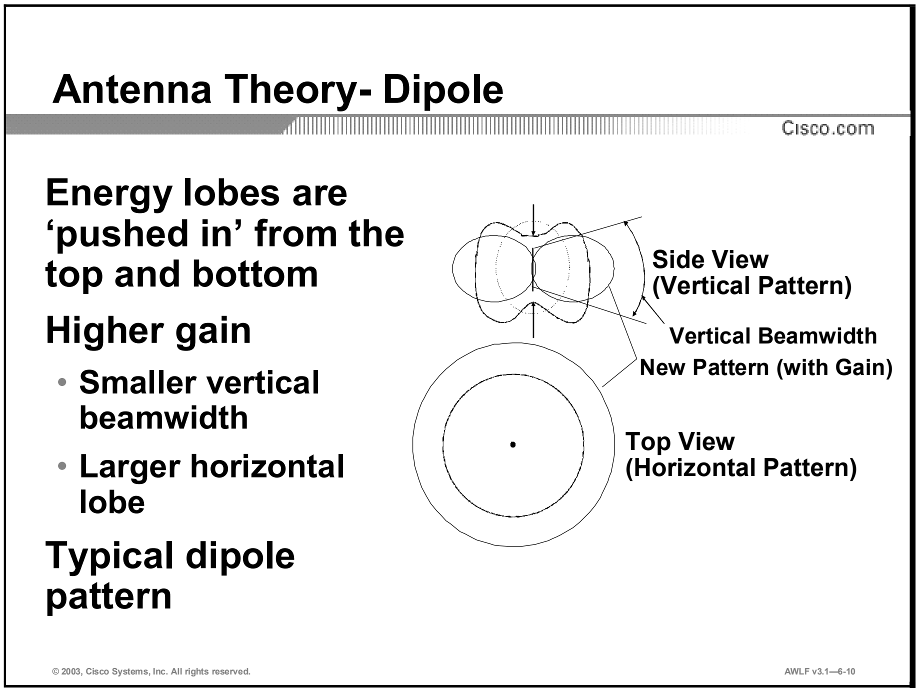
Cisco.com

A theoretical isotropic antenna has a perfect 360º vertical and horizontal beamwidth

This is a reference for ALL antennas

AWLF v3.1—6-9

All FCC rules and all antennas are measured against what is known as an isotropic antenna, which is a theoretical antenna. This is the basis for ALL other antennas. An isotropic antenna's coverage can be thought of as a balloon. It extends in all directions equally.



Antenna Theory- Dipole

Cisco.com

Energy lobes are 'pushed in' from the top and bottom

Higher gain

- Smaller vertical beamwidth
- Larger horizontal lobe

Typical dipole pattern

Side View (Vertical Pattern)

Vertical Beamwidth

New Pattern (with Gain)

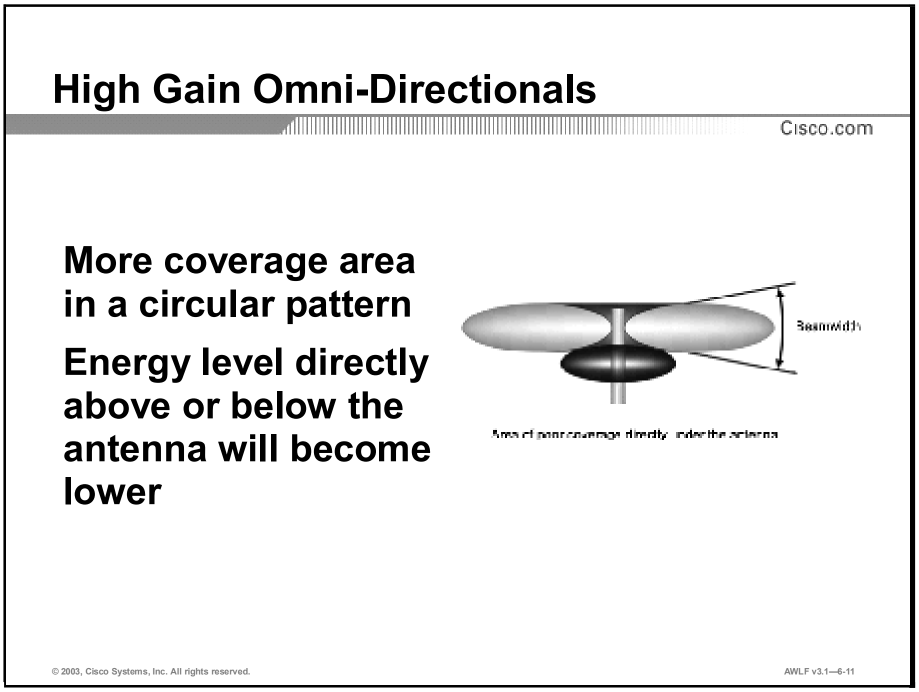
Top View (Horizontal Pattern)

AWLF v3.1—6-10

When an omni-directional antenna is designed to have gain, it results in loss of coverage in certain areas.

Imagine the radiation pattern of an isotropic antenna as a balloon, which extends from the antenna equally in all directions. Now imagine pressing in on the top and bottom of the balloon. This causes the balloon to expand in an outward direction, covering more area in the horizontal pattern, but reducing the coverage area above and below the antenna. This yield a higher gain, as the antenna "appears" to extend to a larger coverage area.

The higher the gain on an antenna means the smaller the vertical beamwidth.



High Gain Omni-Directionals

Cisco.com

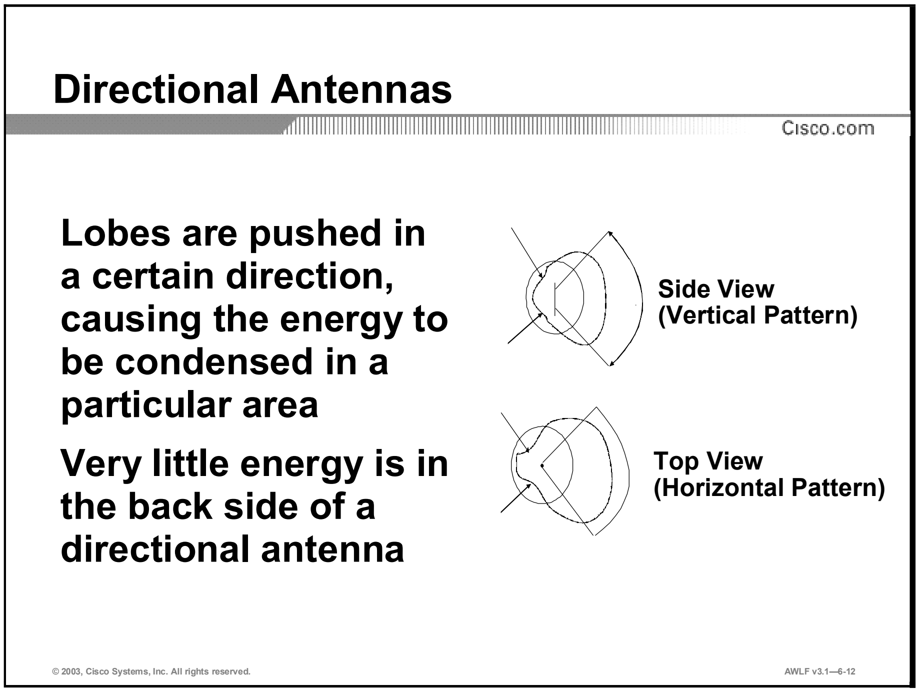
- More coverage area in a circular pattern
- Energy level directly above or below the antenna will become lower

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—6-11

If we continue to push in on the ends of the balloon, it results a pancake effect with very narrow vertical beamwidth, but very large horizontal coverage. This type of antenna design can deliver very long communications distances, but has one drawback - poor coverage below the antenna.

With high gain omni-directional antennas, this problem can be partially solved by designing in something called downtilt. An antenna that uses downtilt is designed to radiate at a slight angle rather that at 90 degree from the vertical element. This does help for local coverage, but reduces effectiveness of the long-range ability. Cellular antennas use downtilt. The Cisco Aironet 12 dBi omni antenna has a downtilt of 0 degrees.



Directional Antennas

Cisco.com

- Lobes are pushed in a certain direction, causing the energy to be condensed in a particular area
- Very little energy is in the back side of a directional antenna

Side View
(Vertical Pattern)

Top View
(Horizontal Pattern)

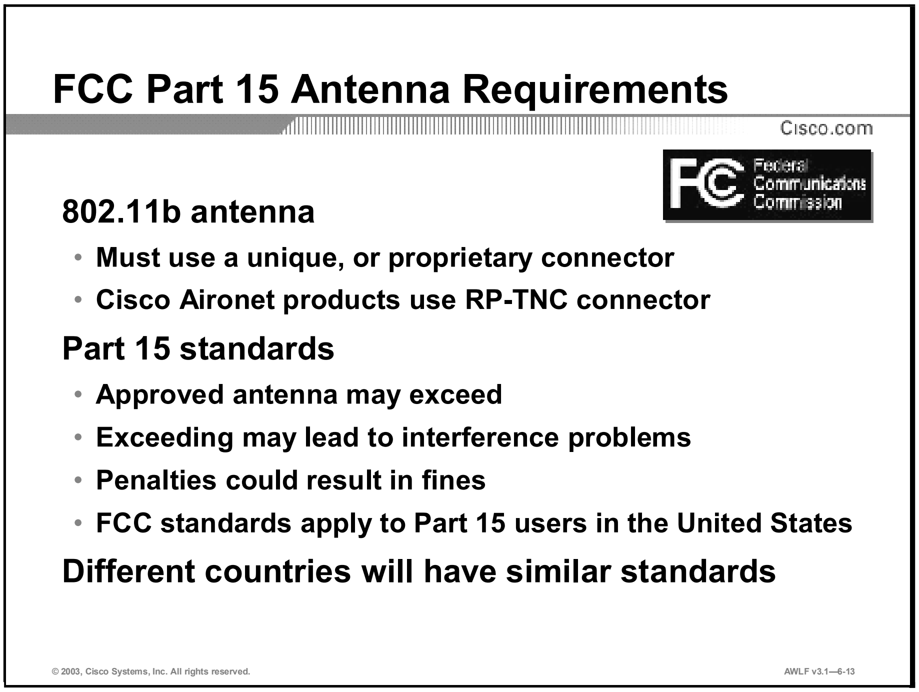
© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—6-12

For a directional antenna, the design has the same idea, but simply redirects the energy in a single direction.

Consider one of the adjustable beam focus flashlights. There are only two batteries, and the same bulb, but the intensity and width of the light beam can be changed. Moving the back reflector and directing the light in tighter or wider angles accomplish this. As the beam gets wider, the intensity in the center decreases, and it travels a shorter distance.

The same is true of a directional antenna. The same power is reaching the antenna, but by building it in certain ways, the RF energy can be directed in tighter and stronger waves, or wider and less intense waves, just as with the flashlight.



Cisco.com
Federal Communications Commission

FCC Part 15 Antenna Requirements

802.11b antenna

- Must use a unique, or proprietary connector
- Cisco Aironet products use RP-TNC connector

Part 15 standards

- Approved antenna may exceed
- Exceeding may lead to interference problems
- Penalties could result in fines
- FCC standards apply to Part 15 users in the United States

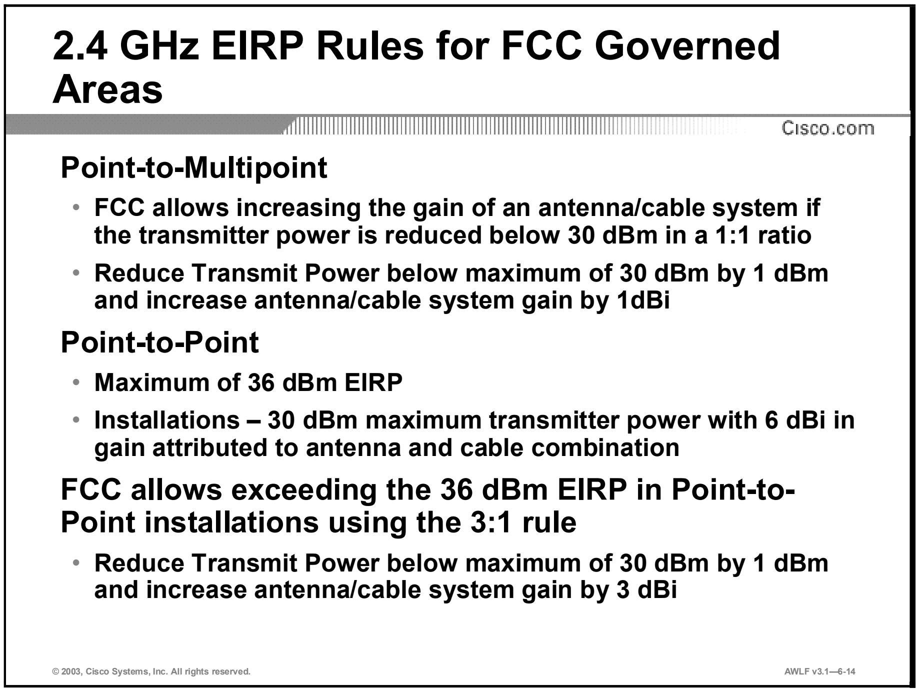
Different countries will have similar standards

© 2003, Cisco Systems, Inc. All rights reserved. AWLF v3.1—6-13

The slide discusses the FCC standards that Cisco Aironet products adhere to. The following is an excerpt from Title 47 Section 15.203

§ 15.203 Antenna Requirements

An intentional radiator shall be designed to ensure that no antenna other than that furnished by the responsible party shall be used with the device. The use of a permanently attached antenna or of an antenna that uses a unique coupling to the intentional radiator shall be considered sufficient to comply with the provisions of this section. The manufacturer may design the unit so that a broken antenna can be replaced by the user, but the use of a standard antenna jack or electrical connector is prohibited. This requirement does not apply to carrier current devices or to devices operated under the provisions of §15.211, § 15.213, § 15.217, § 15.219, or § 15.221. Further, this requirement does not apply to intentional radiators that must be professionally installed, such as perimeter protection systems and some field disturbance sensors, or to other intentional radiators, which, in accordance with § 15.31(d), must be measured at the installation site. However, the installer shall be responsible for ensuring that the proper antenna is employed so that the limits in this part are not exceeded.



2.4 GHz EIRP Rules for FCC Governed Areas

Point-to-Multipoint

- **FCC allows increasing the gain of an antenna/cable system if the transmitter power is reduced below 30 dBm in a 1:1 ratio**
- **Reduce Transmit Power below maximum of 30 dBm by 1 dBm and increase antenna/cable system gain by 1dBi**

Point-to-Point

- **Maximum of 36 dBm EIRP**
- **Installations – 30 dBm maximum transmitter power with 6 dBi in gain attributed to antenna and cable combination**

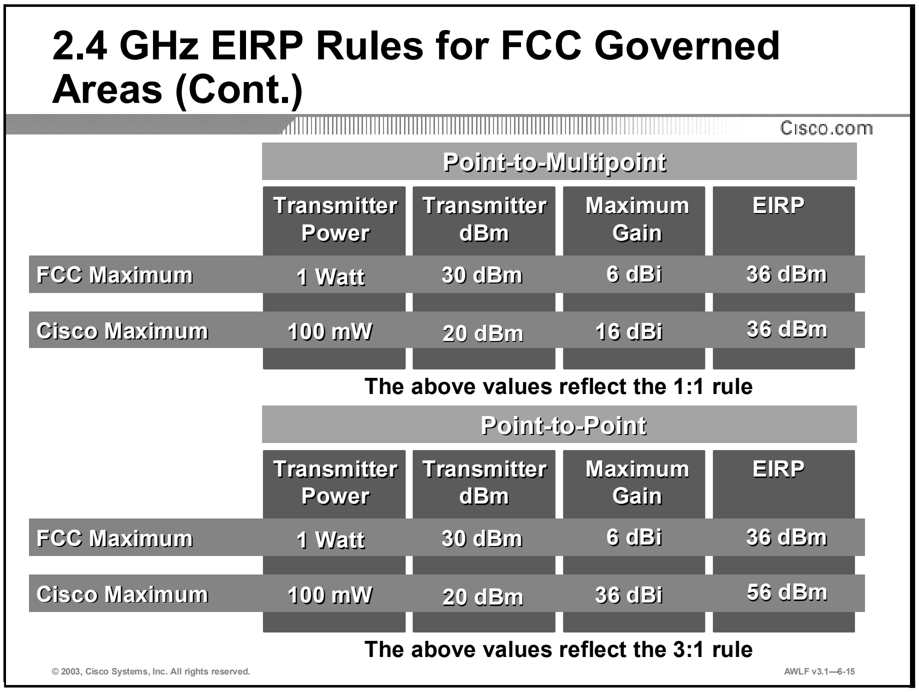
FCC allows exceeding the 36 dBm EIRP in Point-to-Point installations using the 3:1 rule

- **Reduce Transmit Power below maximum of 30 dBm by 1 dBm and increase antenna/cable system gain by 3 dBi**

AWLF v3.1—6-14

This slide discusses the FCC standards that Cisco Aironet products adhere to. The following is an excerpt from FCC Title 47 Section 15.247:

- (b) The maximum peak output power of the intentional radiator shall not exceed the following:
  - (1) For frequency hopping systems in the 2400-2483.5 MHz band employing at least 75 hopping channels, all frequency hopping systems in the 5725-5850 MHz band, and all direct sequence systems: 1 watt. For all other frequency hopping systems in the 2400-2483.5 MHz band: 0.125 watts.
  - (3) “if transmitting antennas of directional gain greater than 6 dBi are used the peak output power from the intentional radiator shall be reduced below the stated values in paragraphs (b)(1) or (b)(2) of this section, as appropriate, by the amount in dB that the directional gain of the antenna exceeds 6 dBi. Systems operating in the 2400-2483.5 MHz band that are used exclusively for fixed, point-to-point operations may employ transmitting antennas with directional gain greater than 6 dBi provided the maximum peak output power of the intentional radiator is reduced by 1 dB for every 3 dB that the directional gain of the antenna exceeds 6 dBi.”



2.4 GHz EIRP Rules for FCC Governed Areas (Cont.)

Cisco.com

Point-to-Multipoint

	Transmitter Power	Transmitter dBm	Maximum Gain	EIRP
FCC Maximum	1 Watt	30 dBm	6 dBi	36 dBm
Cisco Maximum	100 mW	20 dBm	16 dBi	36 dBm

The above values reflect the 1:1 rule

Point-to-Point

	Transmitter Power	Transmitter dBm	Maximum Gain	EIRP
FCC Maximum	1 Watt	30 dBm	6 dBi	36 dBm
Cisco Maximum	100 mW	20 dBm	36 dBi	56 dBm

The above values reflect the 3:1 rule

AWLF v3.1—6-15

The Effective Isotropic Radiated Power (EIRP) of a transmitter is the power that the transmitter appears to have if the transmitter were an isotropic radiator (if the antenna radiated equally in all directions). By virtue of the gain of a radio antenna (or dish), a beam is formed that preferentially transmits the energy in one direction. The EIRP is estimated by adding the gain (of the antenna) and the transmitter power (of the radio).

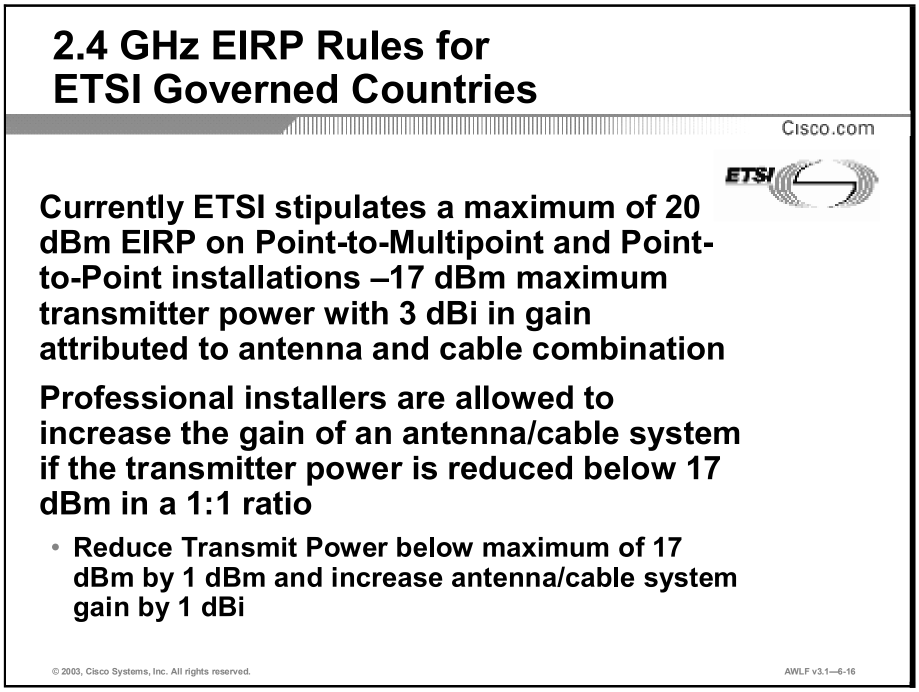
- EIRP = transmitter power + antenna gain – cable loss

When using radio equipment, there are limits on the output of the system. These limits are given as EIRP, and must not be exceeded. Different countries will have different standards. Check with authorities in the country of installation to determine maximum EIRP.

The output of the radio will be measured in dBm (decibels per milliwatt). The slide shows a table that lists the dBm ratings for the various output levels available with the Cisco Aironet Wireless equipment and the resulting EIRP when used with a 6 dBi patch antenna.

The maximum EIRP allowed by the FCC for a Part 15 802.11b device in the United States is 36 dBm. The standards are different for specific point-to-point systems. However, this class is focused on WLANs that would be considered point-to-multipoint solutions, so the maximum EIRP allowed must not exceed 36 dBm and the maximum gain on an antenna must not exceed 16 dBi (for the United States) unless installed by a professional installer.

Note The highest gain antenna approved by Cisco is the 21 dBi Parabolic Dish Antenna.



2.4 GHz EIRP Rules for ETSI Governed Countries

Cisco.com
ETSI

Currently ETSI stipulates a maximum of 20 dBm EIRP on Point-to-Multipoint and Point-to-Point installations –17 dBm maximum transmitter power with 3 dBi in gain attributed to antenna and cable combination

Professional installers are allowed to increase the gain of an antenna/cable system if the transmitter power is reduced below 17 dBm in a 1:1 ratio

- **Reduce Transmit Power below maximum of 17 dBm by 1 dBm and increase antenna/cable system gain by 1 dBi**

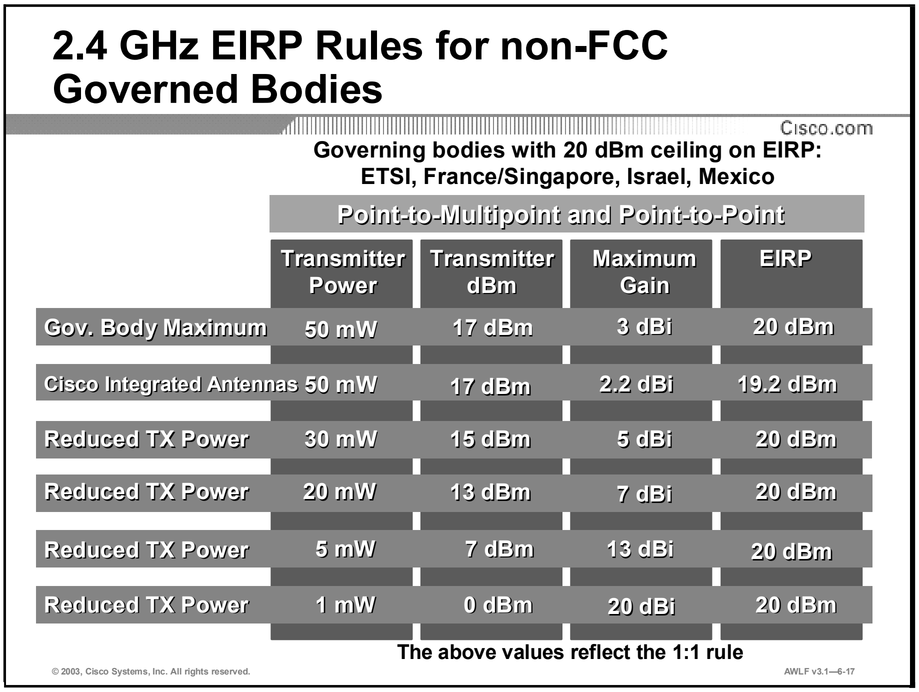
AWLF v3.1—6-16

This slide discusses the ETSI standards that Cisco Aironet products adhere to. The following is an excerpt from that document.

ETSI EN 300 328-1 V1.2.2 (2000-07)

5.2 Transmitter parameter limits:

- 5.2.1 Effective radiated power
  - The effective radiated power is defined as the total power of the transmitter and is calculated according to the procedure given in sub clause 7.2.1. The effective radiated power shall be equal to or less than -10 dBW (100 mW) EIRP. This limit shall apply for any combination of power level and intended antenna assembly.
- 5.2.2 Peak power density
  - The peak power density is defined as the highest instantaneous level of power in Watts per Hertz generated by the transmitter within the power envelope. For equipment using FHSS modulation, the power density shall be limited to -10 dBW (100 mW) per 100 kHz EIRP. For equipment using other types of modulation, the peak power shall be limited to -20 dBW (10 mW) per MHz EIRP.



2.4 GHz EIRP Rules for non-FCC Governed Bodies

Governing bodies with 20 dBm ceiling on EIRP:
ETSI, France/Singapore, Israel, Mexico

	Point-to-Multipoint and Point-to-Point			
	Transmitter Power	Transmitter dBm	Maximum Gain	EIRP
Gov. Body Maximum	50 mW	17 dBm	3 dBi	20 dBm
Cisco Integrated Antennas	50 mW	17 dBm	2.2 dBi	19.2 dBm
Reduced TX Power	30 mW	15 dBm	5 dBi	20 dBm
Reduced TX Power	20 mW	13 dBm	7 dBi	20 dBm
Reduced TX Power	5 mW	7 dBm	13 dBi	20 dBm
Reduced TX Power	1 mW	0 dBm	20 dBi	20 dBm

The above values reflect the 1:1 rule

AWLF v3.1—6-17

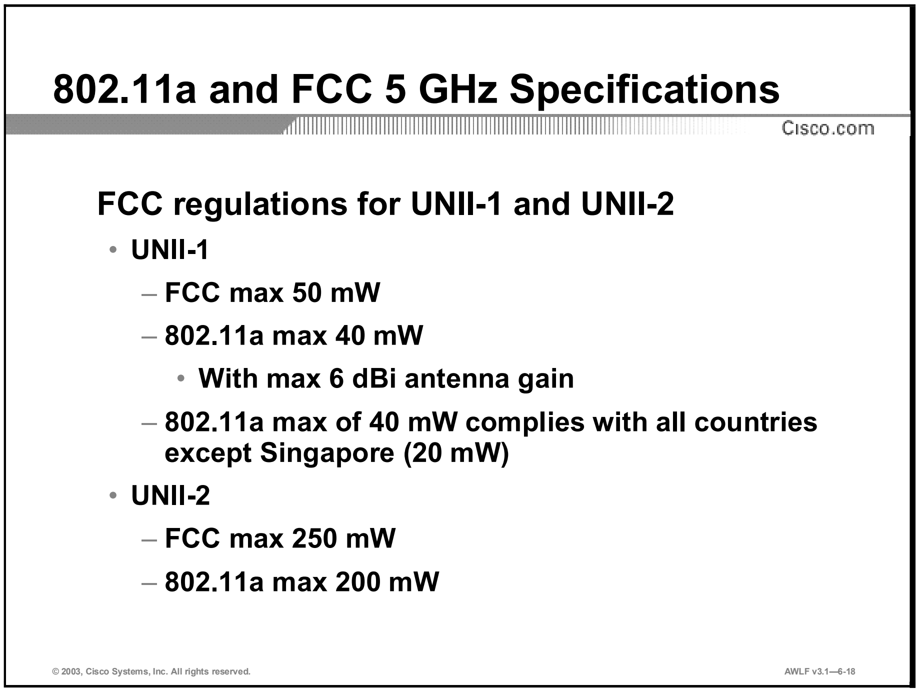
The Effective Isotropic Radiated Power (EIRP) of a transmitter is the power that the transmitter appears to have if the transmitter were an isotropic radiator (if the antenna radiated equally in all directions). By virtue of the gain of a radio antenna (or dish), a beam is formed that preferentially transmits the energy in one direction. The EIRP is estimated by adding the gain (of the antenna) and the transmitter power (of the radio).

- EIRP = transmitter power + antenna gain – cable loss

When using radio equipment, there are limits on the output of the system. These limits are given as EIRP, and must not be exceeded. Different countries will have different standards. Check with authorities in the country of installation to determine maximum EIRP.

The output of the radio will be measured in dBm (decibels per milliwatt). The slide shows a table that lists the dBm ratings for the various output levels available with the Cisco Aironet Wireless equipment and the resulting EIRP when used with a different antenna.

The maximum EIRP allowed for a 2.4 GHz device in France, Singapore, Israel, Mexico and ETSI is 20 dBm. The standards are different for specific point-to-point systems. However, this class is focused on WLANs that would be considered point-to-multipoint solutions, so the maximum EIRP allowed must not exceed 20 dBm and the maximum gain on an antenna must not exceed 20 dBi.



802.11a and FCC 5 GHz Specifications

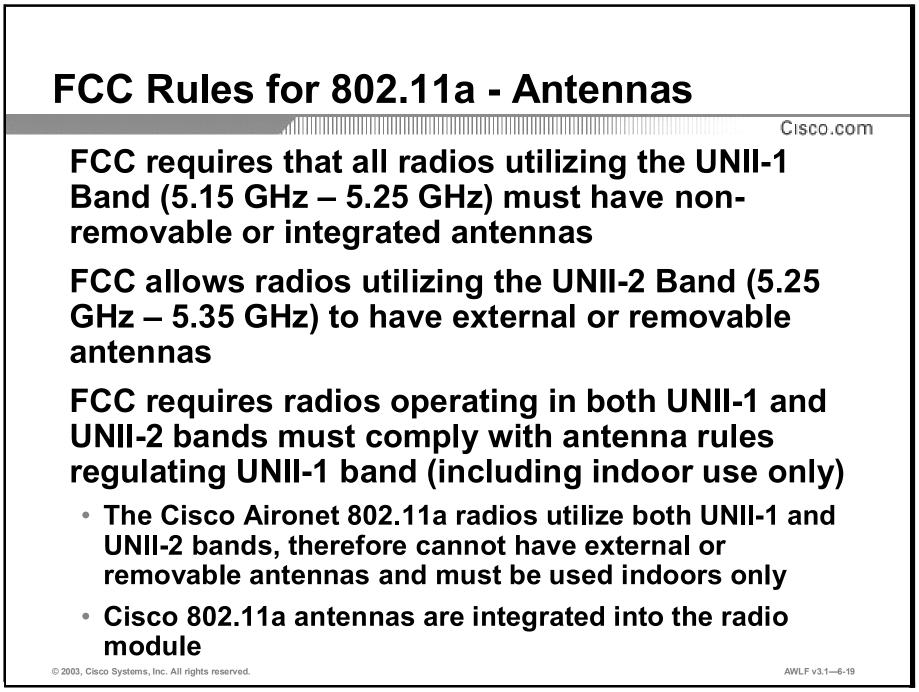
FCC regulations for UNII-1 and UNII-2

- UNII-1
  - FCC max 50 mW
  - 802.11a max 40 mW
    - With max 6 dBi antenna gain
  - 802.11a max of 40 mW complies with all countries except Singapore (20 mW)
- UNII-2
  - FCC max 250 mW
  - 802.11a max 200 mW

AWLF v3.1—6-18

The following is an excerpt from FCC Title 47 Section 15.407:

- (a) Power limits:
  - (1) For the band 5.15-5.25 GHz, the peak transmit power over the frequency band of operation shall not exceed the lesser of 50 mW or 4 dBm + 10logB, where B is the 26-dB emission bandwidth in MHz. In addition, the peak power spectral density shall not exceed 4 dBm in any 1-MHz band. If transmitting antennas of directional gain greater than 6 dBi are used, both the peak transmit power and the peak power spectral density shall be reduced by the amount in dB that the directional gain of the antenna exceeds 6 dBi.
  - (2) For the band 5.25-5.35 GHz, the peak transmit power over the frequency band of operation shall not exceed the lesser of 250 mW or 11 dBm + 10logB, where B is the 26-dB emission bandwidth in MHz. In addition, the peak power spectral density shall not exceed 11 dBm in any 1-MHz band. If transmitting antennas of directional gain greater than 6 dBi are used, both the peak transmit power and the peak power spectral density shall be reduced by the amount in dB that the directional gain of the antenna exceeds 6 dBi.



FCC Rules for 802.11a - Antennas

Cisco.com

FCC requires that all radios utilizing the UNII-1 Band (5.15 GHz – 5.25 GHz) must have non-removable or integrated antennas

FCC allows radios utilizing the UNII-2 Band (5.25 GHz – 5.35 GHz) to have external or removable antennas

FCC requires radios operating in both UNII-1 and UNII-2 bands must comply with antenna rules regulating UNII-1 band (including indoor use only)

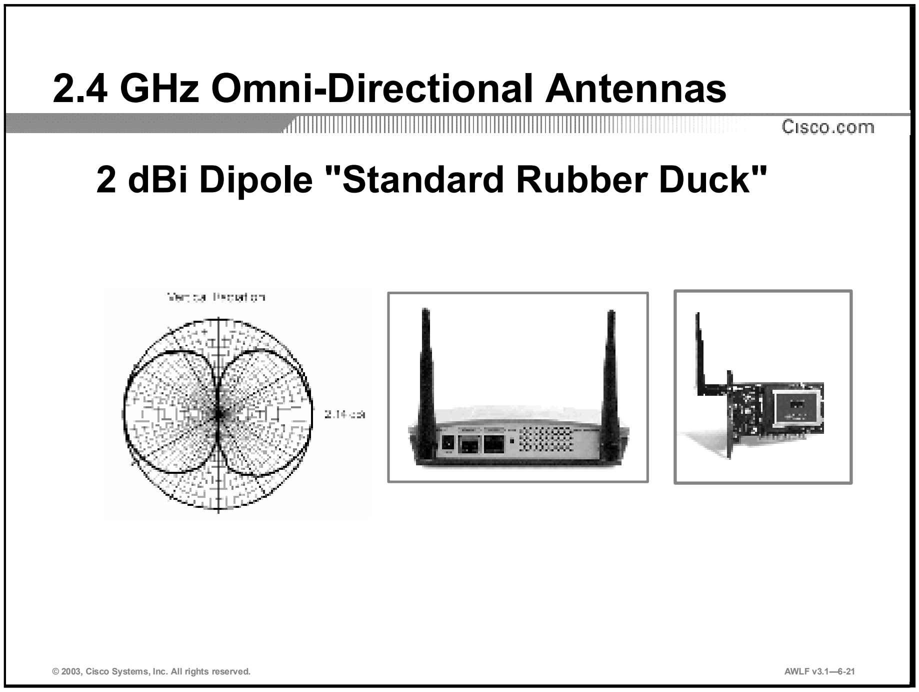
- The Cisco Aironet 802.11a radios utilize both UNII-1 and UNII-2 bands, therefore cannot have external or removable antennas and must be used indoors only
- Cisco 802.11a antennas are integrated into the radio module

AWLF v3.1—6-19

The following is an excerpt from FCC Title 47 Section 15.407:

- (d) Any UNII device that operates in the 5.15-5.25 GHz band shall use a transmitting antenna that is an integral part of the device.
- (e) Within the 5.15-5.25 GHz band, UNII devices will be restricted to indoor operations to reduce any potential for harmful interference to co-channel MSS operations

Cisco Aironet Antennas



2.4 GHz Omni-Directional Antennas

Cisco.com

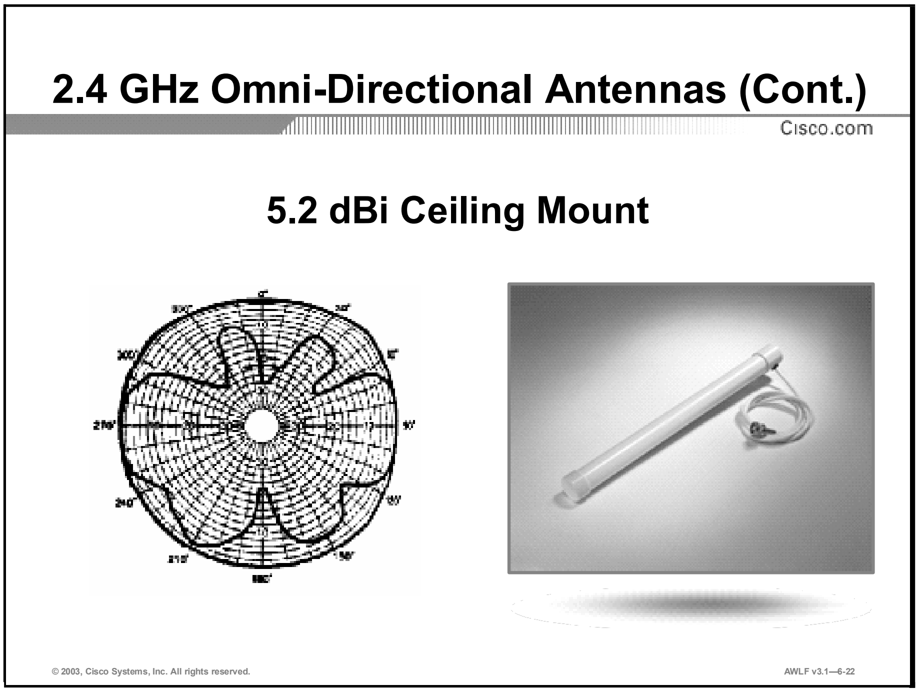
2 dBi Dipole "Standard Rubber Duck"

Vertical Radiation
2.14 dBi

AWLF v3.1—6-21

2.4 GHz Antennas

The “Rubber Duck” Dipole antenna is a standard dipole supplied with some Cisco Aironet Access Points and client devices.



2.4 GHz Omni-Directional Antennas (Cont.)

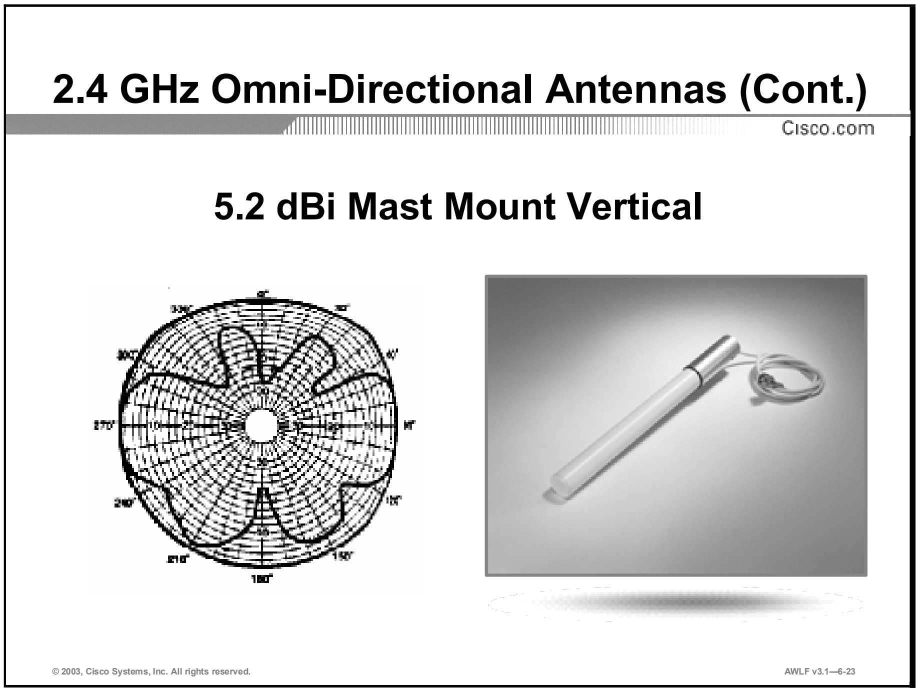
Cisco.com

5.2 dBi Ceiling Mount

AWLF v3.1—6-22

The 5.2 dBi ceiling mount omni is designed to mount to the metal grid of a suspended ceiling. It has a ¼" x 20 thread bolthole on its base and a clamp that screws into this hole. When utilized, this clamp expands enough to allow you to install the antenna on the metal ceiling grid and then slide the clamp snugly back together. Other options are to drill a hole into a ceiling beam and use a ¼" x 20 thread bolt to bolt it in a vertical position.

- This antenna is more aesthetically pleasing than the mast mount version.
- This antenna is only for indoor applications and should be mounted with the bolt hole end pointing to the ceiling.
- This antenna is not a good choice for schools or hospitals as it may be damaged.
- This antenna is vertically polarized but does have a slightly downward tilted beam, allowing its coverage pattern to cover the areas below the ceiling.



2.4 GHz Omni-Directional Antennas (Cont.)

Cisco.com

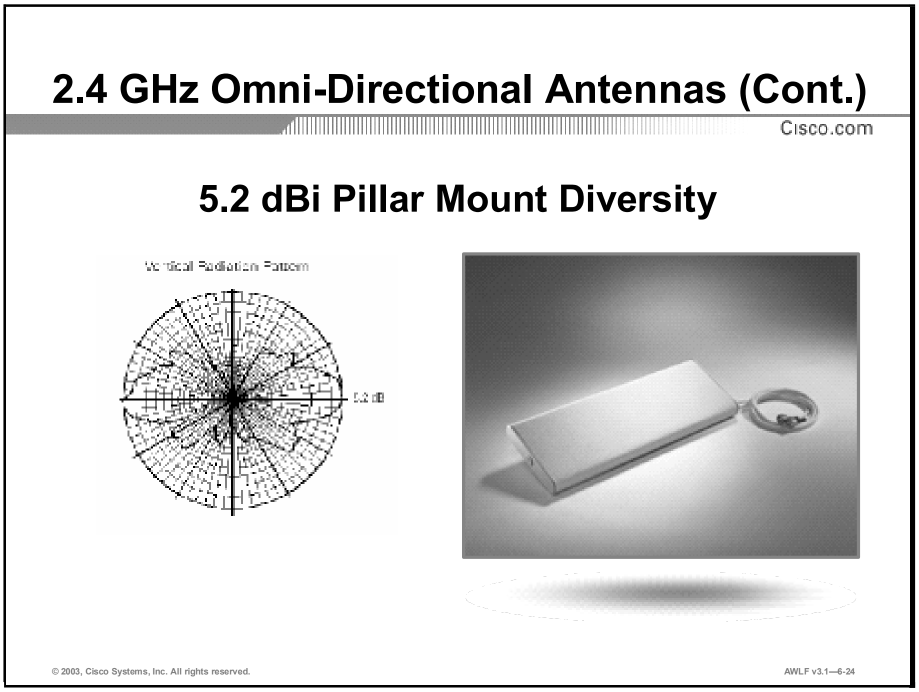
5.2 dBi Mast Mount Vertical

AWLF v3.1—6-23

The 5.2 dBi mast mount omni is designed to clamp to a mast or pole. The base of the antenna has an aluminum section that gives it enough strength to withstand being clamped.

This antenna is delivered with a hose clamp and aluminum friction bracket for mounting. You must supply the mast to which the antenna will be clamped.

- Designed for more industrial applications.
- In outdoor applications, the antenna cable end must be facing down to prevent moisture from entering the antenna.
- In indoor applications, the cable end should be facing the ceiling.
- Whether indoor or outdoor, this antenna is vertically polarized and should be mounted perpendicular to the floor or ground.



2.4 GHz Omni-Directional Antennas (Cont.)

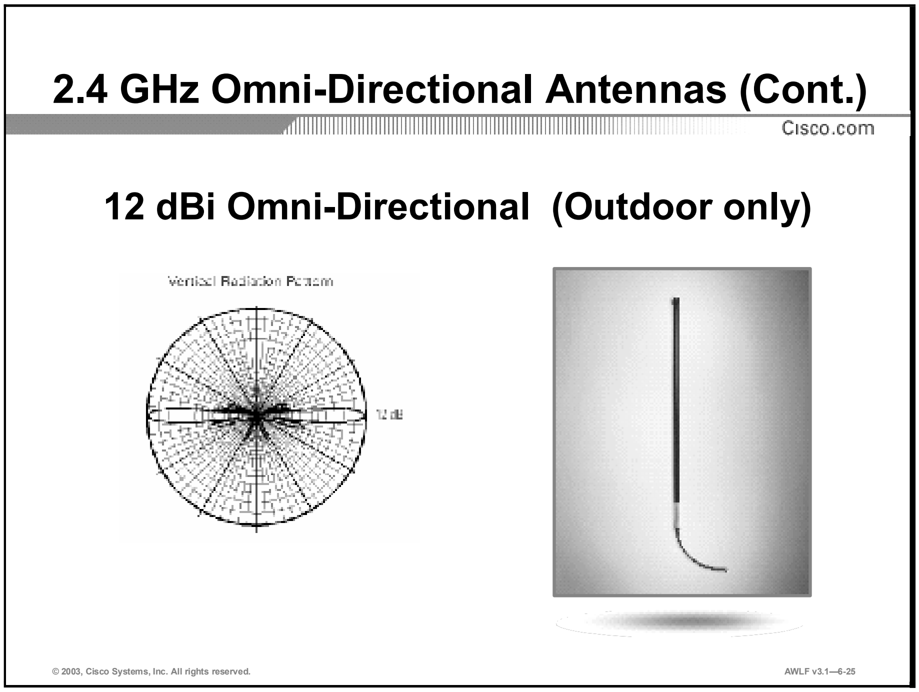
Cisco.com

5.2 dBi Pillar Mount Diversity

AWLF v3.1—6-24

The 5.2 dBi pillar mount diversity omni is designed to mount to the side of a pillar. It is two antennas in one package, wrapped by cloth to make it look like something other than an antenna, such as a stereo speaker. Sears deploys these antennas.

- This antenna has two pigtails with two RP-TNC connectors. In order to utilize diversity antennas only one of these types of antenna is needed per access point.
- This antenna is only for indoor applications.
- This antenna comes with two brackets that make it easy to mount it to a pillar.



2.4 GHz Omni-Directional Antennas (Cont.)

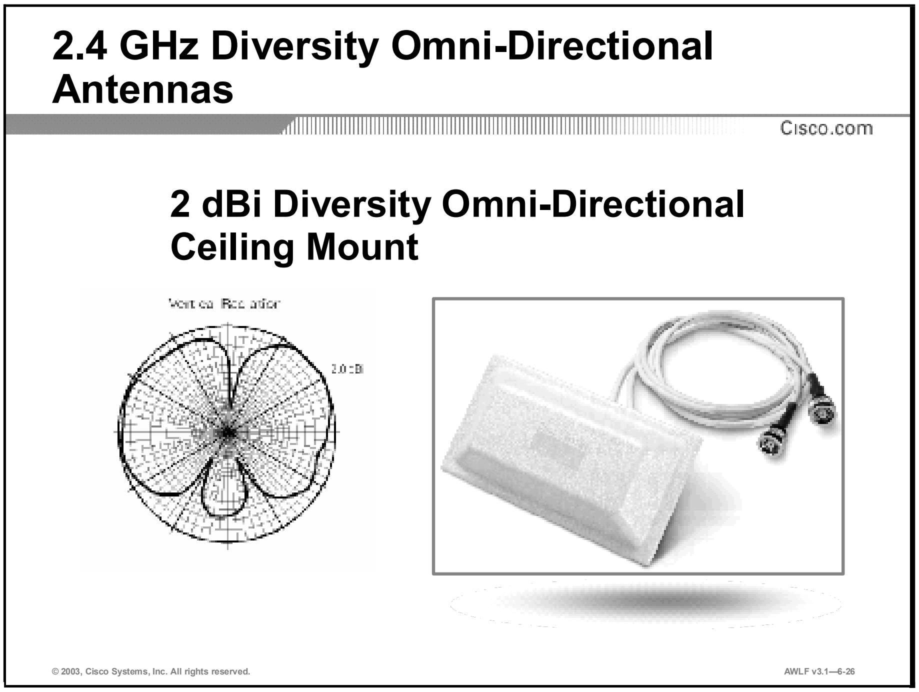
12 dBi Omni-Directional (Outdoor only)

Vertical Radiation Pattern
12 dB

AWLF v3.1—6-25

The 12 dBi antenna is ONLY for outdoor long-range applications. The antenna has a short 12" coax pigtail making it necessary to utilize antenna extension cables.

- This antenna is designed to clamp to a mast or pole. The base of the antenna has a metal section giving it enough strength to withstand being clamped.
- This antenna is delivered with a set of U-bolts and friction brackets. You must supply the mast to which the antenna will be clamped.
- This antenna is vertically polarized and must be mounted perpendicular to the ground with the pigtail on the bottom.
- This antenna has a +3.5 and –3.5 degree beam spread from perpendicular.



2.4 GHz Diversity Omni-Directional Antennas

Cisco.com

2 dBi Diversity Omni-Directional Ceiling Mount

Vertical Radiation
2.0 dBi

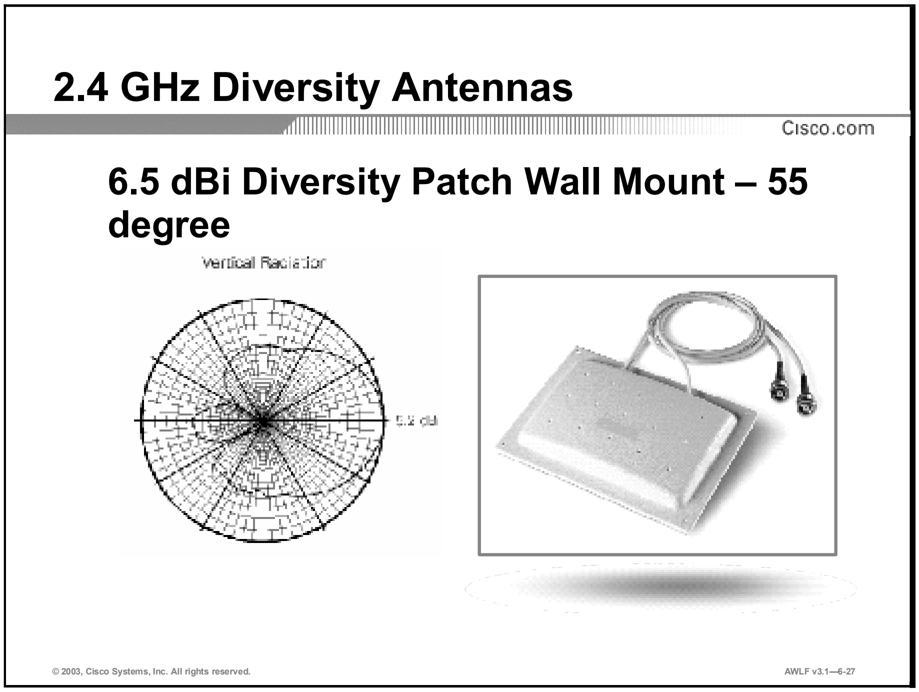
AWLF v3.1—6-26

The diversity omni-directional ceiling mount antenna is an excellent companion to an access point supporting diversity. It was designed to interface with remotely located access points thereby maximizing installation flexibility. This antenna takes full advantage of the diversity functionality built into Aironet Access Points, improving performance and range particularly in high multipath indoor environments. The 2-dBi antenna provides a circular coverage pattern and is ideal for mounting on ceilings.

This antenna features two separate 2 dBi omni-directional radiating elements sharing a common backplane and enclosure.

The antenna is vertically polarized but does have a slightly downward tilted beam, allowing its coverage pattern to cover areas below the ceiling.

- Ideal for installation where multipath is an issue.
- More aesthetically pleasing than the rubber duck.
- Durable clips ensure easy installation.



2.4 GHz Diversity Antennas

Cisco.com

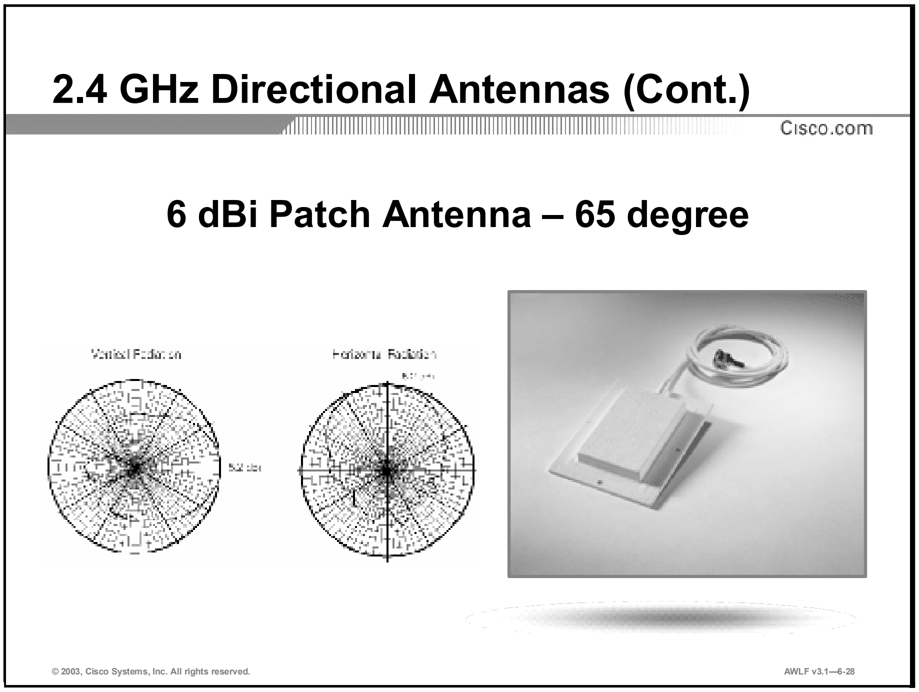
6.5 dBi Diversity Patch Wall Mount – 55 degree

Vertical Radiation
5.2 dBi

AWLF v3.1—6-27

The diversity patch mount antenna is an excellent companion to an access point supporting diversity. It was designed to interface with remotely located access points thereby maximizing installation flexibility. This antenna take full advantage of the diversity functionality built into Aironet Access Points, improving performance and range particularly in high multipath indoor environments. It provides a hemispherical coverage pattern and is ideal for mounting on walls. Features include to following:

- Offers 2 antennas in one package for spatial diversity
- Outdoor/indoor applications
- Ideal for installations where multipath is an issue.
- More aesthetically pleasing than the rubber duck.
- Durable ceiling clips ensure easy installation.


Vertical Radiation
Horizontal Radiation

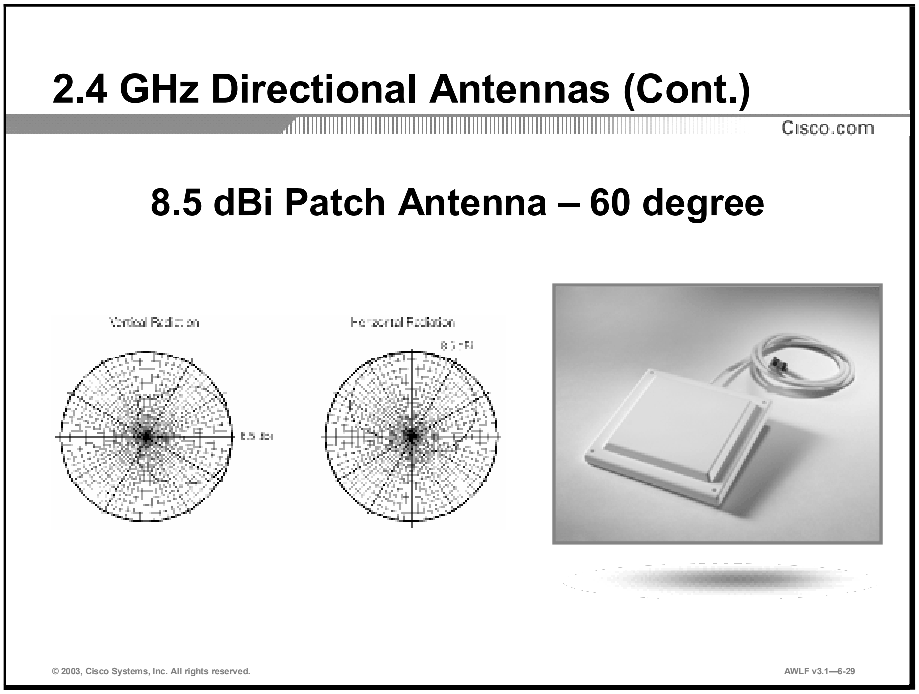
2.4 GHz Directional Antennas (Cont.)

Cisco.com

6 dBi Patch Antenna – 65 degree

The 6-dBi patch provides excellent coverage with a wide radiation pattern.

- This antenna looks identical to the 3-dBi patch only but comes with 3 feet of RG-58 coax antenna cable instead of 20 feet.
- This antenna is a choice for indoor and outdoor applications when properly mounted.
- This antenna has three holes around the perimeter of antenna, allowing the antenna to be mounted to a wide variety of surfaces.



2.4 GHz Directional Antennas (Cont.)

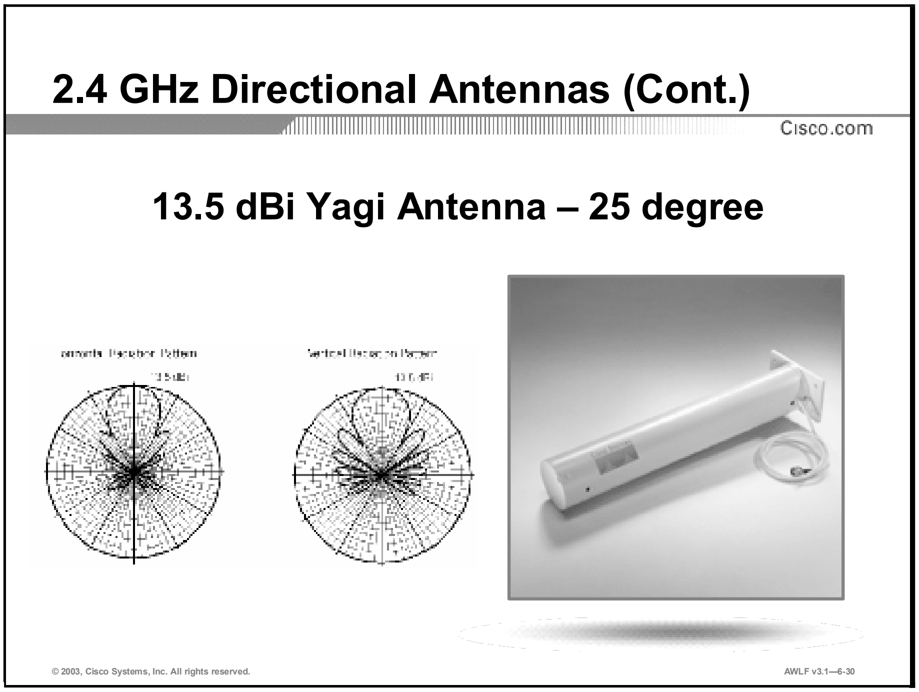
Cisco.com

8.5 dBi Patch Antenna – 60 degree

AWLF v3.1—6-29

The 8.5 dBi provides more gain than the 6 dBi, but less beam width.

- This antenna comes with a 3-foot coax pigtail.
- This antenna is a choice for indoor and outdoor applications when properly mounted.
- This antenna has a hole at each corner of the antenna, allowing the antenna to be mounted to a wide variety of surfaces.



2.4 GHz Directional Antennas (Cont.)

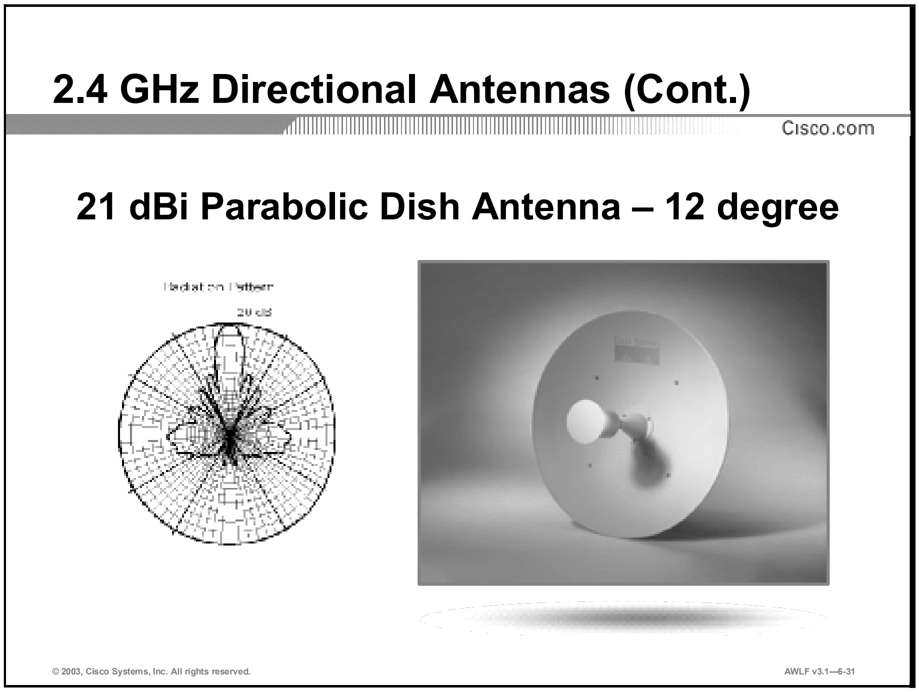
Cisco.com

13.5 dBi Yagi Antenna – 25 degree

AWLF v3.1—6-30

The 13.5 dBi Yagi is used for long distance communication, and provides excellent results in a small package.

- This antenna comes with a 3-foot coax pigtail.
- This is a good antenna for outdoor and some indoor applications.
- This antenna has four holes in the corners of antenna base and comes with two u-bolts for mounting to a mast.
- Optional articulating mount is available.



2.4 GHz Directional Antennas (Cont.)

Cisco.com

21 dBi Parabolic Dish Antenna – 12 degree

© 2003, Cisco Systems, Inc. All rights reserved.

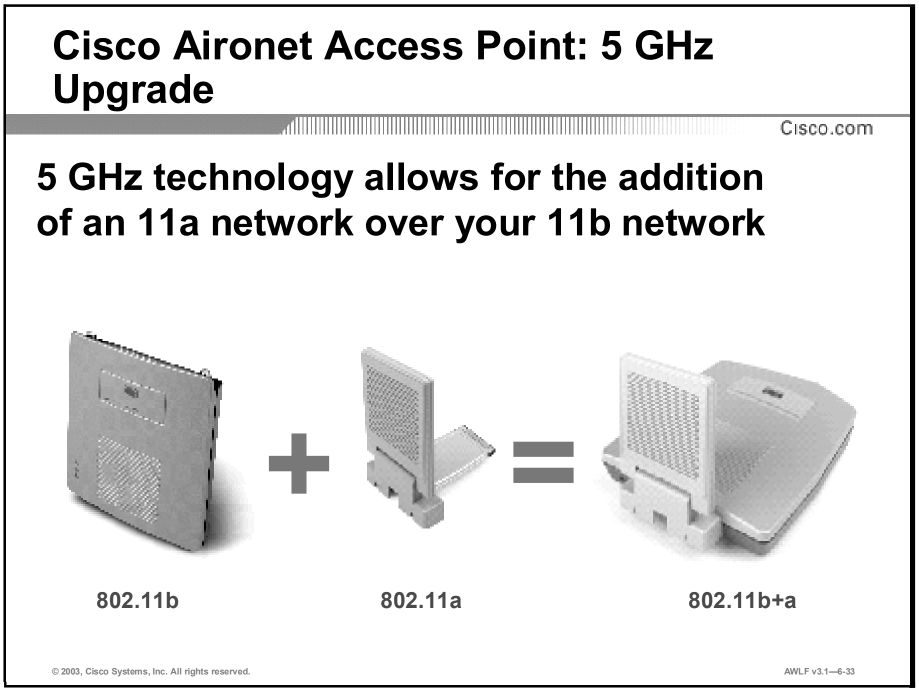
AWLF v3.1—6-31

For very long distances Cisco offers the 21 dBi parabolic dish.

Note The use of this dish antenna with the standard Cisco product may exceed the FCC limitation on radiated power for point to multi point systems if a short antenna extension cable is used.

This antenna, as with all outdoor only antennas, has a short 12-inch coax pigtail making it necessary to utilize antenna extension cables. This is a very effective antenna for outdoor long distance bridging applications.

The antenna has very sturdy mounting hardware on backside with adjusting turnbuckles allowing for altitude and latitude adjustments. The antenna is also delivered with u-bolts for mounting to a mast. Keep in mind that the mast must be very sturdy; the 21 dBi parabolic dish is rated to 120 mph with one-half inch of ice.



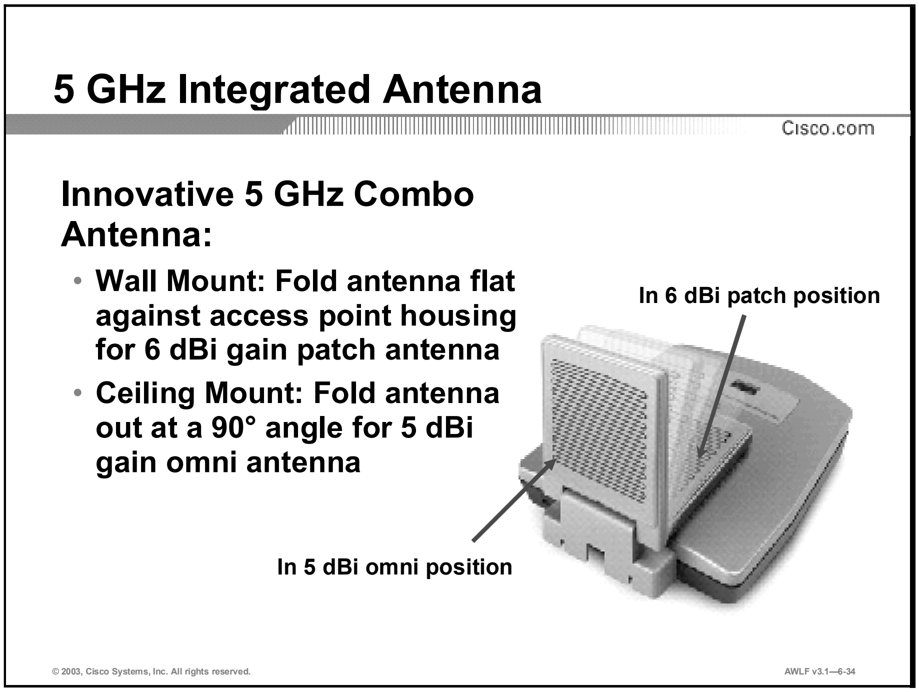
Cisco Aironet Access Point: 5 GHz Upgrade

5 GHz technology allows for the addition of an 11a network over your 11b network

AWLF v3.1—6-33

802.11a Antennas

With simultaneous support for both 2.4 GHz and 5 GHz radios, the Cisco Aironet 1200 Series preserves existing IEEE 802.11b investments and provides a migration path to future IEEE 802.11a and IEEE 802.11g technologies. Its modular design supports single- and dual-band configuration, plus the field upgradability to change these configurations as requirements change and technologies evolve. Investment protection is further provided by large storage capacity and support for Cisco management tools, delivering the capacity and means to upgrade firmware and deliver new features as they become available.



5 GHz Integrated Antenna

Innovative 5 GHz Combo Antenna:

- **Wall Mount: Fold antenna flat against access point housing for 6 dBi gain patch antenna**
- **Ceiling Mount: Fold antenna out at a 90° angle for 5 dBi gain omni antenna**

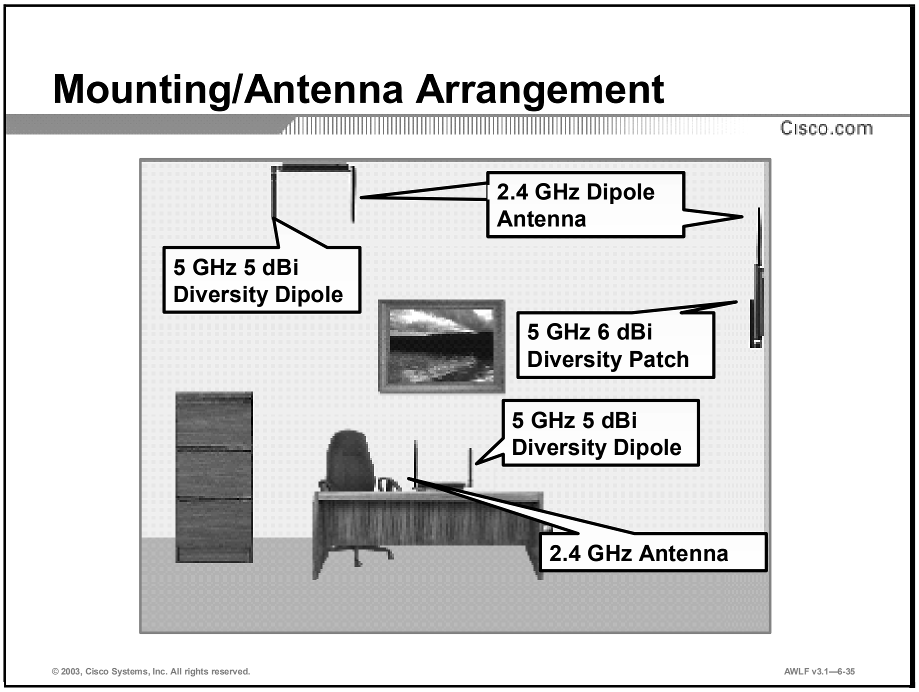
In 6 dBi patch position

In 5 dBi omni position

AWLF v3.1—6-34

Items to note:

- The module has 2 paired diversity antennas.
- 1 Pair for diversity patch use.
- 1 Pair for diversity omni use.
- When the module is flat against the 1200 Series Access Point shell the patch antennas are on.
- When the module is vertical from the 1200 Series Access Point shell the omni antennas are on.
- The omni has a gain of 5 dBi and a 360-degree pattern.
- The patch has a gain of 6 dBi and a 180-degree pattern.
- There is ***no connection*** from the 5 GHz radio to the 2.4 GHz RP-TNC antenna ports.
- FCC requirements to UNII-1 are 50 mW max TX radio power, antenna gain 6-dBi antenna must be fixed to the radio and access point, indoor use only.
- FCC requirements to UNII-2 are 250 mW max TX radio power, antenna gain 23 dBi removals allowed. If the radio does both UNII-2 and UNII-2 then the UNII-1 antenna rules apply.



Mounting/Antenna Arrangement

2.4 GHz Dipole Antenna

5 GHz 5 dBi Diversity Dipole

5 GHz 6 dBi Diversity Patch

5 GHz 5 dBi Diversity Dipole

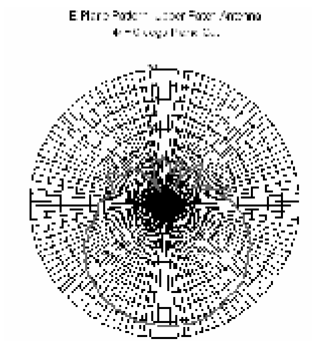
2.4 GHz Antenna

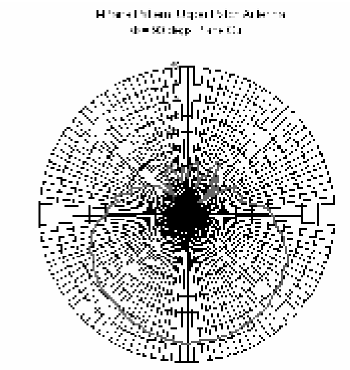
AWLF v3.1—6-35

The above diagram shows proper antenna orientation for both the 2.4 GHz and 5 GHz antennas in various mounting positions.

5 GHz Radiation Pattern

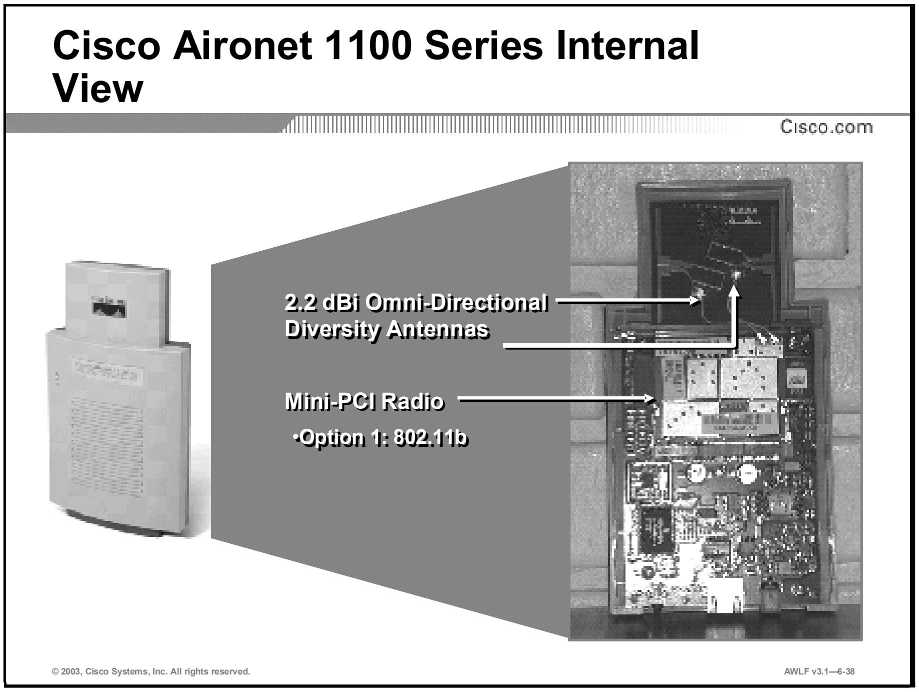
Cisco.com





AWLF v3.1—6-36

Cisco Aironet 1100 Series Access Point



Cisco Aironet 1100 Series Internal View

Cisco.com

2.2 dBi Omni-Directional Diversity Antennas

Mini-PCI Radio

•Option 1: 802.11b

AWLF v3.1—6-38

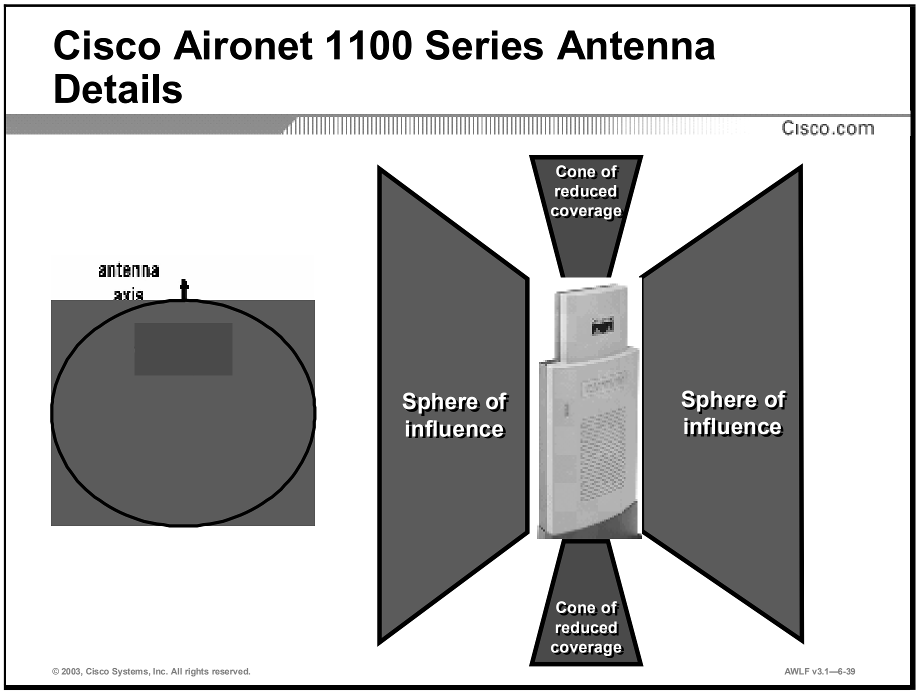
Antenna and Mounting Considerations

The chassis design of Cisco Aironet 1100 Series Access Point allows the end user to upgrade the Mini-PCI radio from 802.11b to 802.11g in the future. Simply remove one screw from the back of Cisco Aironet 1100 Series to access the Mini-PCI Radio. Then remove the 802.11b radio and replace it with an 802.11g radio. The procedure likens the same process as removing and installing computer memory modules.

End users *will not* be able to upgrade Cisco Aironet 1100 Series antennas because it uses a captured antenna. A captured antenna is an antenna that is integrated into the access point to provide ease of installation and WLAN design. The 2.2 dBi omni-directional antenna is engineered to provide antenna diversity to help combat Multipath distortion. Cisco Aironet 1100 Series Access Points antennas provide comparable coverage performance as a pair of 2.2 dBi rubber duckie antennas.

Note Cisco Aironet 1100 Series Access Points only supports the 802.11b. In the near future it will support 802.11g.

Note Cisco Aironet 1100 Series Access Points will not support external antennas.



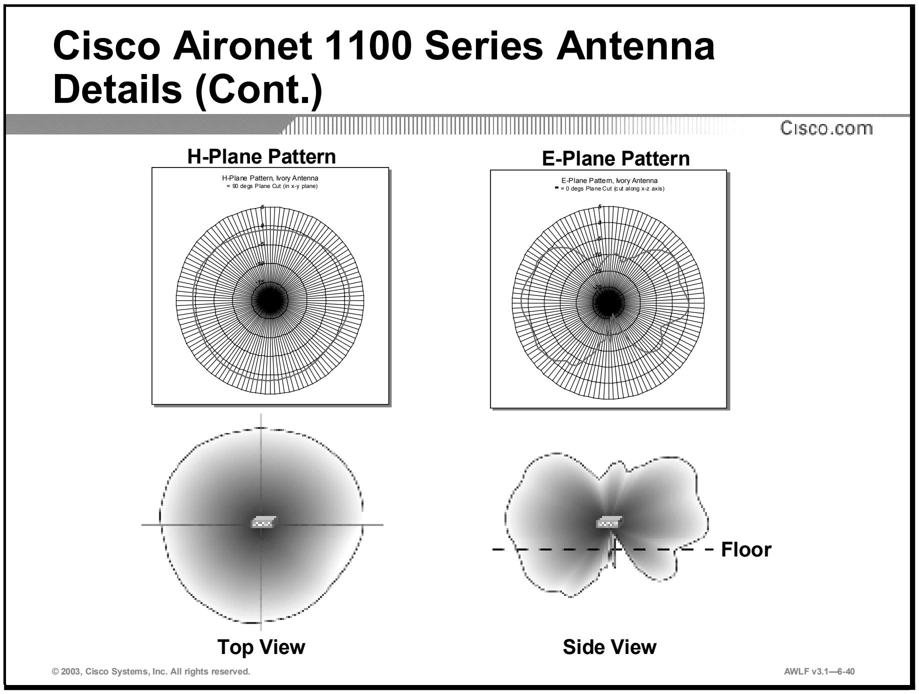
Cisco Aironet 1100 Series Antenna Details

Cisco.com

AWLF v3.1—6-39

The RF propagation of the antenna must be considered when selecting an antenna system for any WLAN device. Since Cisco Aironet 1100 Series Access Point uses a captured 2.2 dBi omni-directional antenna, the installer needs to be aware that the ***cone of reduced coverage*** is directly above and below the Access Point (red zone). An end user located in the cone of reduced coverage will experience poorer connectivity to the access point. End users located in the ***sphere of influence*** (green zone) will experience better connectivity to the access point.

Cisco Aironet 1100 Series Access Point has been designed for different deployment mounting options, e.g., desk, wall, cubical, and ceiling. In order for Cisco Aironet 1100 Series antenna to function reliably in all mounting orientations, the antenna was designed to produce a stronger sphere of influence than a pair of 2.2 dBi rubber duck antennas.

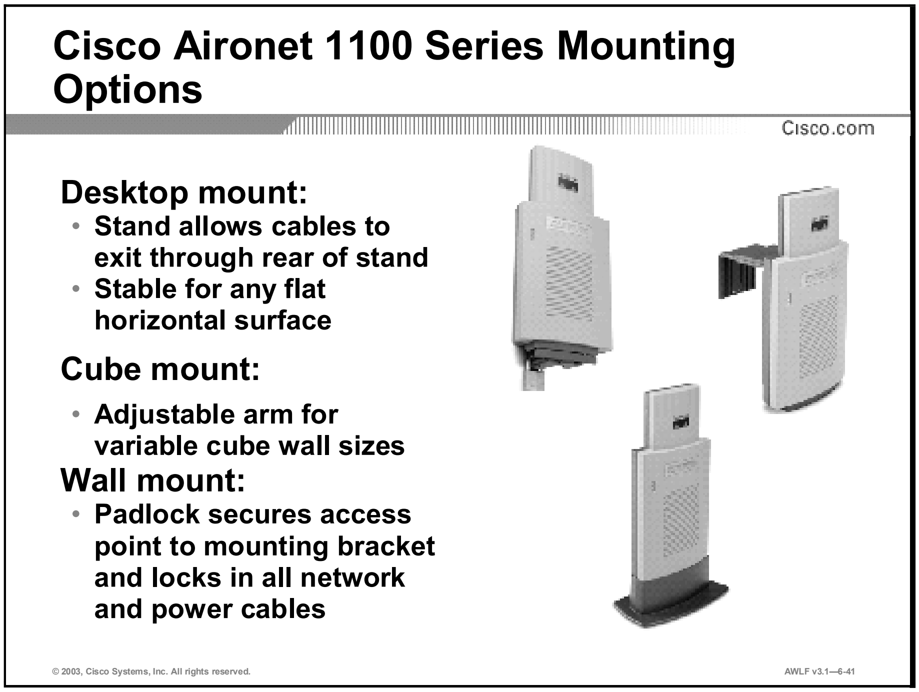


Cisco Aironet 1100 Series Antenna Details (Cont.)

AWLF v3.1—6-40

RF propagation patterns are useful to help WLAN designers "see" how the RF energy propagates from the antenna. Cisco Aironet 1100 Series patterns shown above shows the Horizontal Plane (H-Plane) and the Elevation Plane (E-Plane) of the antenna. The H-Plane shows how the RF energy propagates looking down on the top of the antenna. This H-Plane example shows the antenna has a 360° horizontal coverage pattern.

The E-Plane shows how the RF energy propagates looking at the side of the antenna. This E-Plane example shows the antenna's sphere of influence and the cone of reduced coverage. The E-Plane can be best though of as a doughnut cut in half to show the doughnuts shape, the E-Plane shows the shape of the RF propagation produced by the antenna.



Cisco Aironet 1100 Series Mounting Options

Cisco.com

Desktop mount:

- **Stand allows cables to exit through rear of stand**
- **Stable for any flat horizontal surface**

Cube mount:

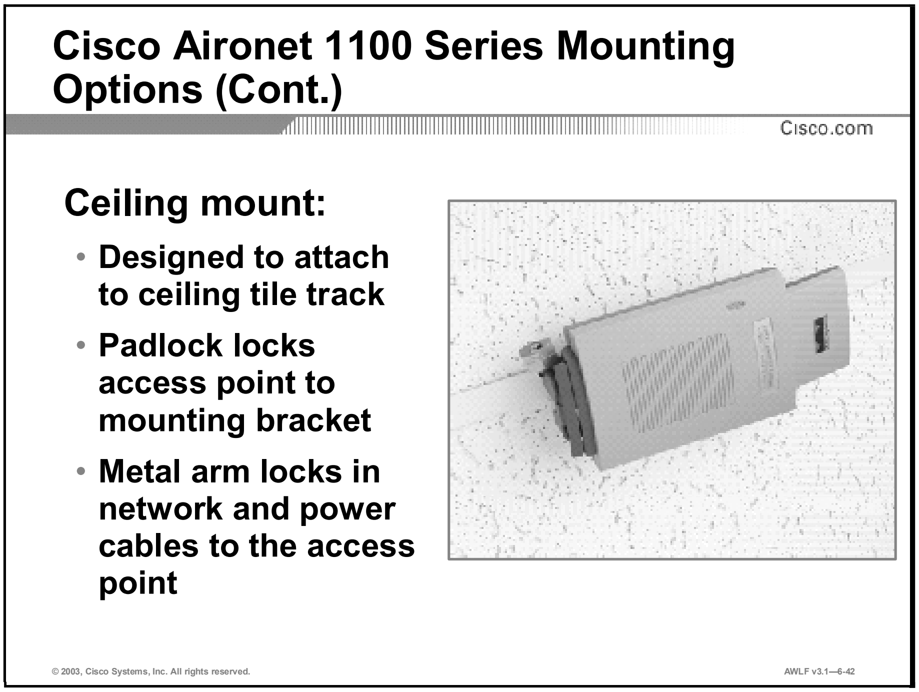
- **Adjustable arm for variable cube wall sizes**

Wall mount:

- **Padlock secures access point to mounting bracket and locks in all network and power cables**

AWLF v3.1—6-41

The Cisco Aironet 1100 Series defines enterprise office deployment capability. Designed in an attractive, durable plastic enclosure, with integrated diversity dipole antennas, the Cisco Aironet 1100 Series provides for quick deployment with a reliable, omni-directional coverage pattern. Supported in various mounting orientations and locations, it can be easily moved throughout the work area as needs change. A standard surface-mounting bracket supports installation on office walls and ceilings for elevated placement. The broad operating temperature range and UL 2043 certification for plenum rating requirements set by local fire codes supports installation in environmental air spaces such as areas above suspended ceilings. The design protects against tampering and theft using single- or master-keyed padlocks. The Cisco Aironet 1100 Series can also be brought into the cubicle space with a cubicle wall-mounting bracket or device stand. The device stand positions the access point on any horizontal surface, such as a desktop or shelf. Theft is deterred in these installations using the security slot with standard security cables. Support for either local or inline power over Ethernet further simplifies installation. The Cisco Aironet 1100 Series is Wi-Fi™ certified to ensure interoperability with other IEEE 802.11b devices.



Cisco Aironet 1100 Series Mounting Options (Cont.)

Ceiling mount:

- **Designed to attach to ceiling tile track**
- **Padlock locks access point to mounting bracket**
- **Metal arm locks in network and power cables to the access point**

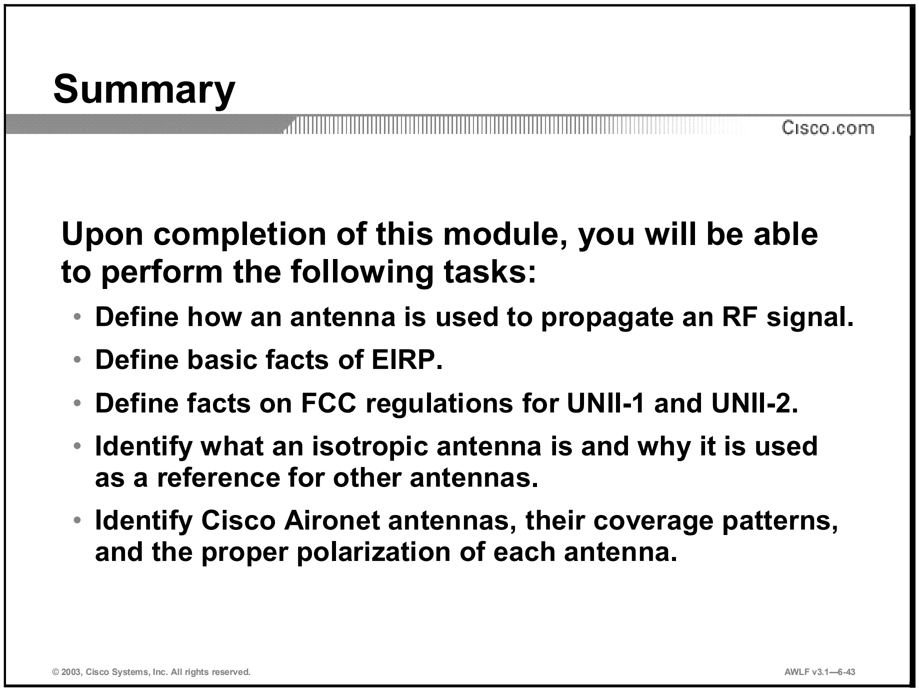
AWLF v3.1—6-42

A *standard ceiling mounting bracket* supports installation on the office ceiling. The broad operating temperature range of 32° to 104° F (0° to 40° C) and UL 2043 certification for plenum rating requirements set by local fire codes supports installation in environmental air spaces such as areas above suspended ceilings.

Note The Cisco Aironet 1100 Series captured antenna is in a stationary position and can not be adjusted for ceiling installations. This means that the RF propagation pattern remains the same even if it is mounted on the ceiling. Please verify the coverage area to ensure that mounting the Cisco Aironet 1100 Series on the ceiling does not affect end users connectivity performance.

Summary

This section summarized the concepts you learned in this module.



Summary

Cisco.com

Upon completion of this module, you will be able to perform the following tasks:

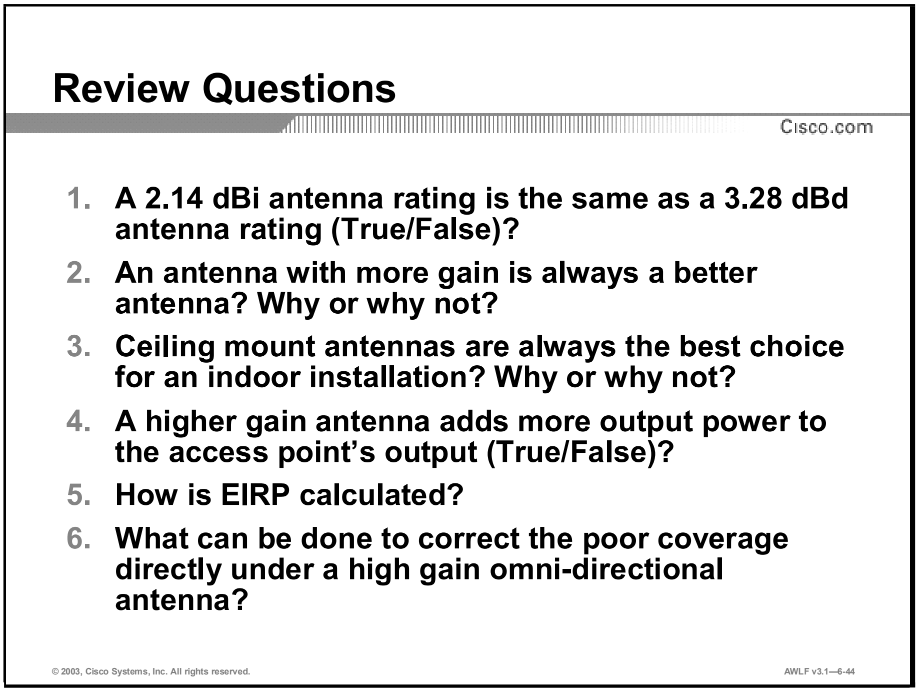
- **Define how an antenna is used to propagate an RF signal.**
- **Define basic facts of EIRP.**
- **Define facts on FCC regulations for UNII-1 and UNII-2.**
- **Identify what an isotropic antenna is and why it is used as a reference for other antennas.**
- **Identify Cisco Aironet antennas, their coverage patterns, and the proper polarization of each antenna.**

AWLF v3.1—6-43

Upon completion of this module, you will be able to perform the following tasks:

- Define how an antenna is used to propagate an RF signal.
- Define basic facts of EIRP.
- Define facts on FCC regulations for UNII-1 and UNII-2.
- Identify what an isotropic antenna is and why it is used as a reference for other antennas.
- Identify Cisco Aironet antennas, their coverage patterns, and the proper polarization of each antenna.

Review Questions



Review Questions

Cisco.com

1. A 2.14 dBi antenna rating is the same as a 3.28 dBd antenna rating (True/False)?
2. An antenna with more gain is always a better antenna? Why or why not?
3. Ceiling mount antennas are always the best choice for an indoor installation? Why or why not?
4. A higher gain antenna adds more output power to the access point’s output (True/False)?
5. How is EIRP calculated?
6. What can be done to correct the poor coverage directly under a high gain omni-directional antenna?

AWLF v3.1—6-44

Answer these review questions.

Module 7

Aironet Client Utility and Drivers

Overview

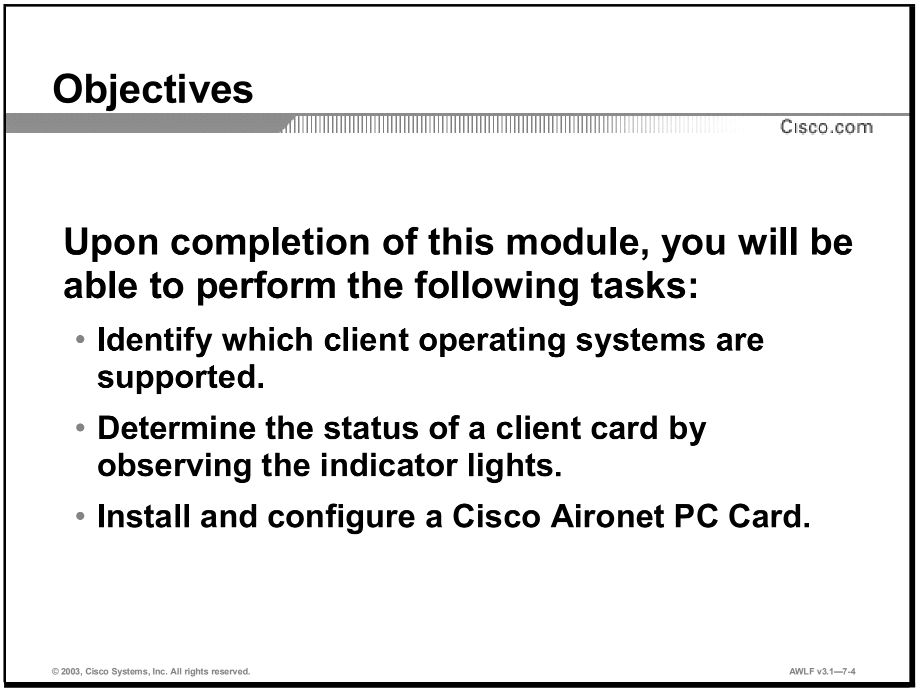
This module explores the Aironet Client Utility and the drivers available for the Cisco Aironet products.

It includes the following topics:

- Objectives
- Supported Operating Systems
- PC Card LEDs
- Aironet Client Utility
- Laboratory Exercise
- Summary
- Review Question

Objectives

This section lists the module's objectives.



Objectives

Cisco.com

Upon completion of this module, you will be able to perform the following tasks:

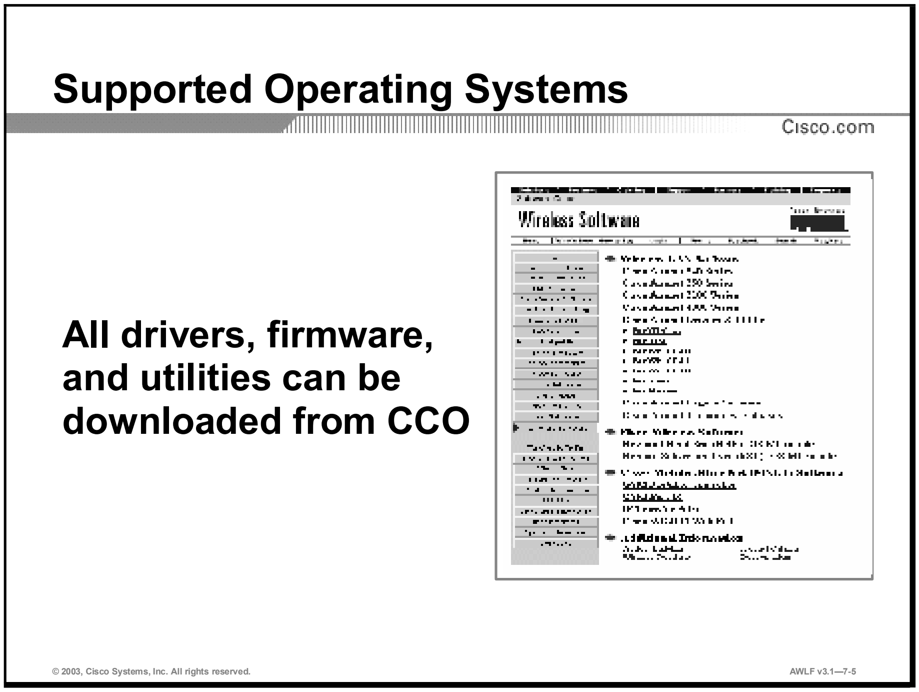
- **Identify which client operating systems are supported.**
- **Determine the status of a client card by observing the indicator lights.**
- **Install and configure a Cisco Aironet PC Card.**

AWLF v3.1—7-4

Upon completion of this module, you will be able to perform the following tasks:

- Identify which client operating systems are supported.
- Determine the status of a client card by observing the indicator lights.
- Install and configure a Cisco Aironet PC Card.

Supported Operating Systems



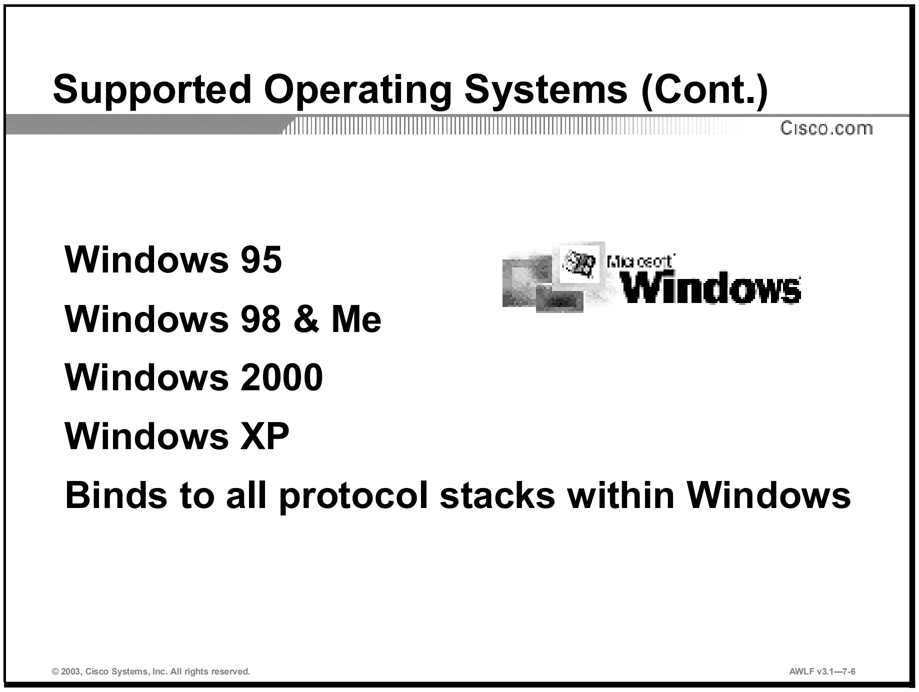
Supported Operating Systems

Cisco.com

All drivers, firmware, and utilities can be downloaded from CCO

AWLF v3.1—7-5

All of the available drivers, utilities, and firmware can be downloaded via the web from the Cisco Connection On-line. From the main Cisco page (www.cisco.com), go to Solutions for Your Network drop-down box, select **wireless**, and go to the Products drop-down box. The latest updates to all Cisco Aironet firmware and software are available via this link.



Supported Operating Systems (Cont.)

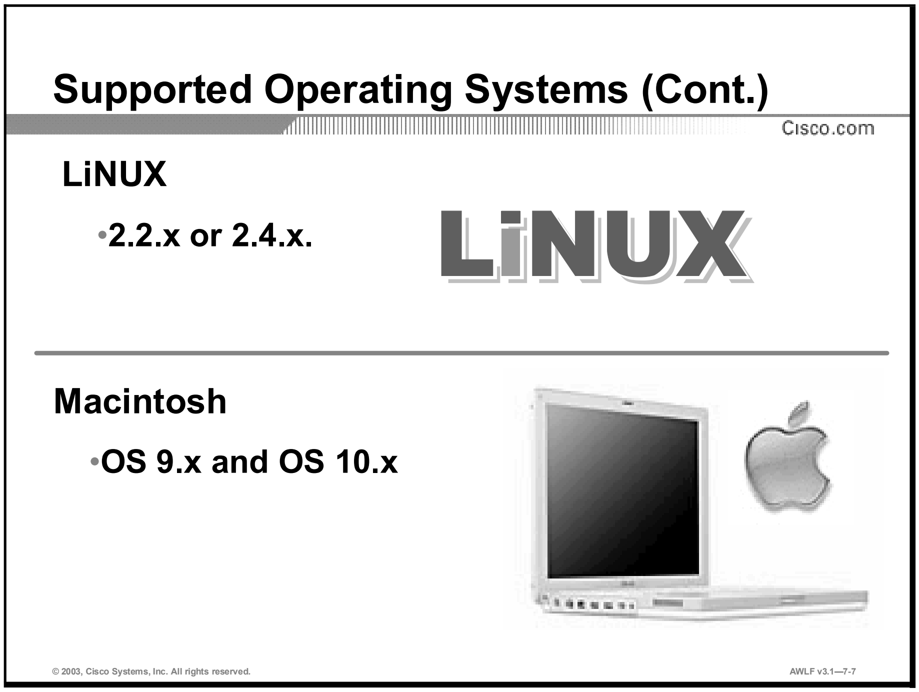
Cisco.com

- Windows 95
- Windows 98 & Me
- Windows 2000
- Windows XP
- Binds to all protocol stacks within Windows

AWLF v3.1—7-6

Driver disk includes drivers for all Windows 9x, XP, and Me, 2000.

Driver is included on the Windows Me, 2000, and XP CDs.



Supported Operating Systems (Cont.)

Cisco.com

LiNUX

- 2.2.x or 2.4.x.

Macintosh

- OS 9.x and OS 10.x

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—7-7

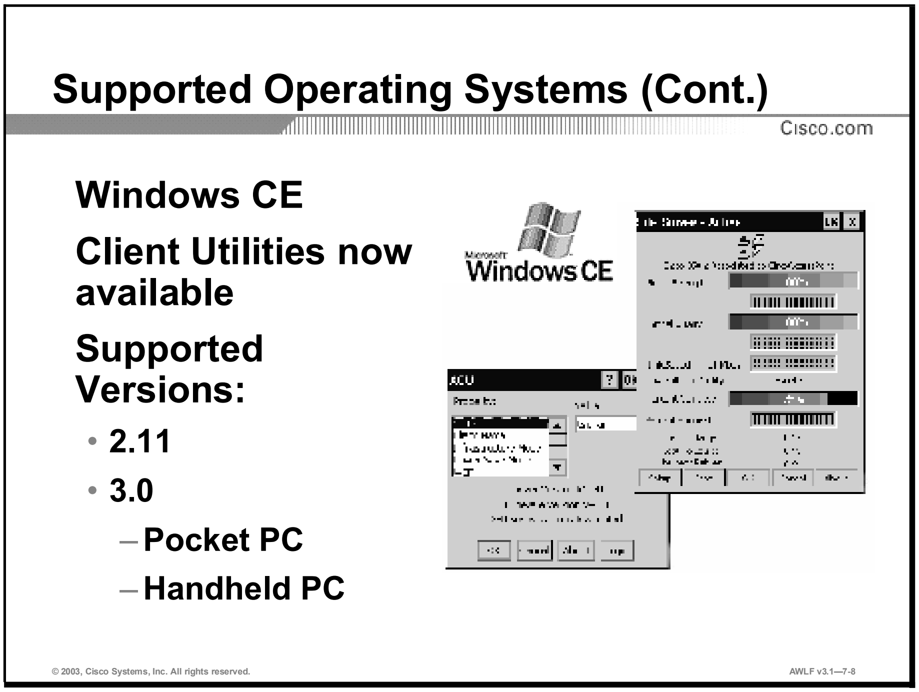
Cisco Aironet offers support for Linux and Macintosh, and are available for specific versions of these operating systems.

The Cisco Aironet Linux driver is for use with any version of Linux using kernel 2.2.x or 2.4.x.

The Cisco Aironet Macintosh driver is for use with the Macintosh PowerBook and PowerMac using Mac OS 9.x or Mac OS X 10.1. The driver is not for use with Macintosh notebooks that have a built-in wireless card.

Cisco recommends using the following third-party card and socket services for LINUX:

- pcmcia-cs-3.1.21.tar.gz which can be found at: http://sourceforge.net/project/showfiles.php?group_id=2405
- Customer support for this can be found at: http://sourceforge.net/forum/?group_id=2405



Supported Operating Systems (Cont.)

Cisco.com

Windows CE

Client Utilities now available

Supported Versions:

- **2.11**
- **3.0**
  - **Pocket PC**
  - **Handheld PC**

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—7-8

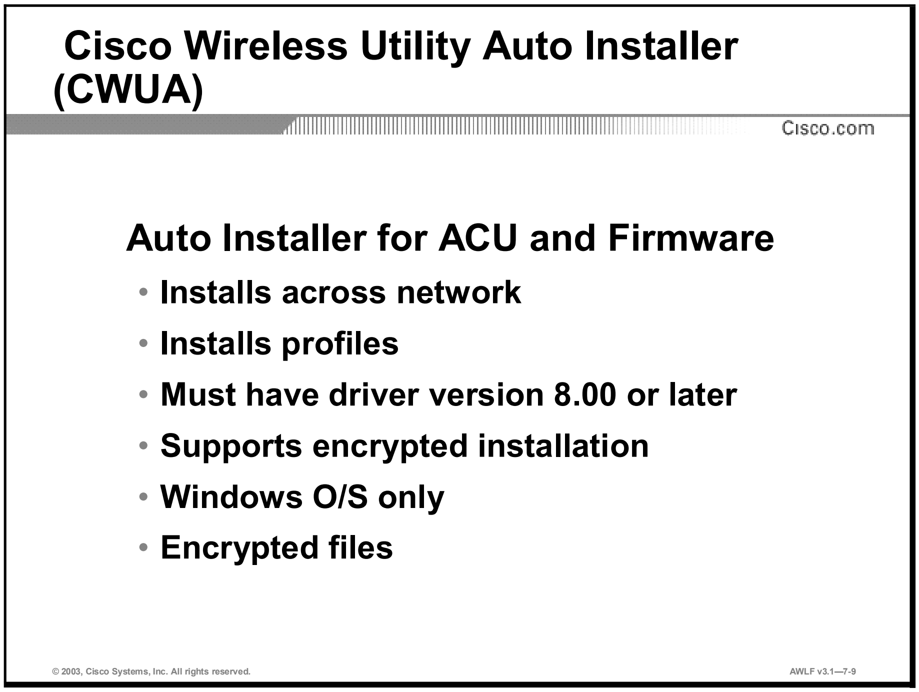
It is necessary to develop a separate compiled version of the driver on a per-processor basis. All reduced instruction set computing (RISC) processors are not alike.

Also, due to the nature of Windows CE, it is necessary to develop a separate driver for each version. This means that whenever a new version of Windows CE is released, a new driver needs to be developed on a per-processor basis.

Not all CE devices adhere to the Personal Computer Memory Card International Association (PCMCIA) standards, due to their limited size and cost-cutting construction. This means that even though a driver is available for the processor and CE release that is in the machine, the PC card still may not work.

Engineering is trying to bring in as many CE devices for compatibility testing as possible, and a matrix of working devices is being developed.

A machine will not work if after receiving card, it displays the message “Unknown card inserted”. It should say, “Network card inserted”. The “unknown card” message is typically due to the vendor not following the PCMCIA specification fully, causing incompatibility issues.



Cisco Wireless Utility Auto Installer (CWUA)

Auto Installer for ACU and Firmware

- Installs across network
- Installs profiles
- Must have driver version 8.00 or later
- Supports encrypted installation
- Windows O/S only
- Encrypted files

AWLF v3.1—7-9

The Cisco Wireless Utility Auto Installer (CWUA) enables an administrator to install the Aironet Client Utility (ACU) across a network, eliminating the need to install and configure the ACU on each wireless client. The auto installer runs in a silent batch mode and will install and configure the ACU (thereby configuring the Cisco Aironet client adapter) on a computer running the Windows operating system.

The auto installer allows the administrator to selectively install and configure parameters for:

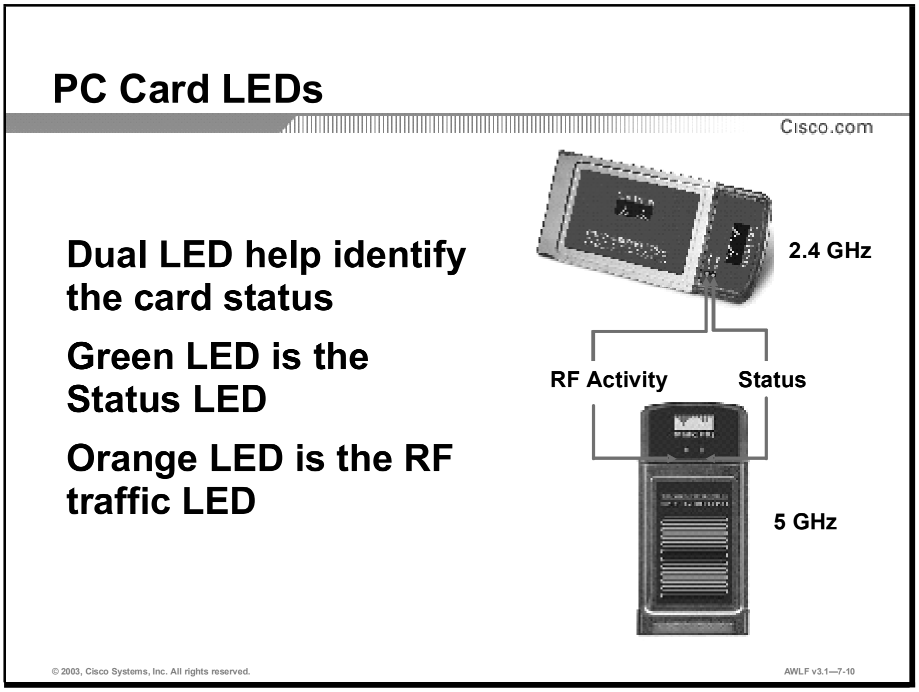
- The drive and directory where the ACU will be stored on the computer.
- The folder where the ACU will be installed on the computer.
- The drive and directory where client card firmware and drivers will be stored on the computer.
- Profiles will be loaded on the computer.

Each profile allows the administrator to selectively configure the following parameters on the ACU for:

- Radio settings
- Wireless network settings
- Network security settings (service set identifier [SSID], wired equivalent privacy [WEP] keys, Network Security)

The auto installer can also be used with its own encryption utility to encrypt the files before they are sent across the network to insure that network security is not compromised while performing auto-installs.

PC Card LEDs



PC Card LEDs

Cisco.com

- Dual LED help identify the card status
- Green LED is the Status LED
- Orange LED is the RF traffic LED

2.4 GHz
RF Activity
Status
5 GHz

AWLF v3.1—7-10

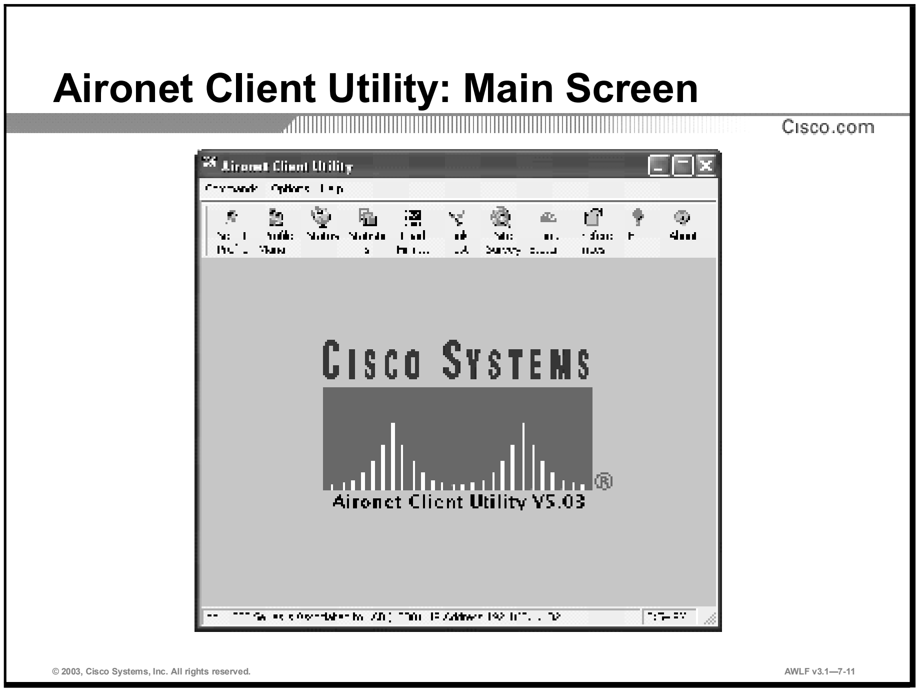
The status light emitting diode (LED) on the PC card is the green LED. It has three modes of operation:

- Blinking once every half-second: Operating in infrastructure mode, scanning for an access point to associate with.
- Blinking once every 2 seconds: Operating in infrastructure mode, associated to an access point.
- Solid Green: Operating in “ad hoc” mode (will not communicate to an access point).

The orange LED is the radio frequency (RF) traffic LED. It has two modes of operation:

- Blinking: Indicates RF traffic.
- Solid ORANGE: Indicates the card is in reset mode, not in operational mode. Typically this means the driver has not been installed properly, or has not loaded properly.

Aironet Client Utility



Aironet Client Utility: Main Screen

Cisco.com

AWLF v3.1—7-11

Aironet Client Utility is a Windows graphical user interface (GUI) diagnostic and configuration utility. It will allow you to upgrade firmware, edit configuration and perform RF link testing.

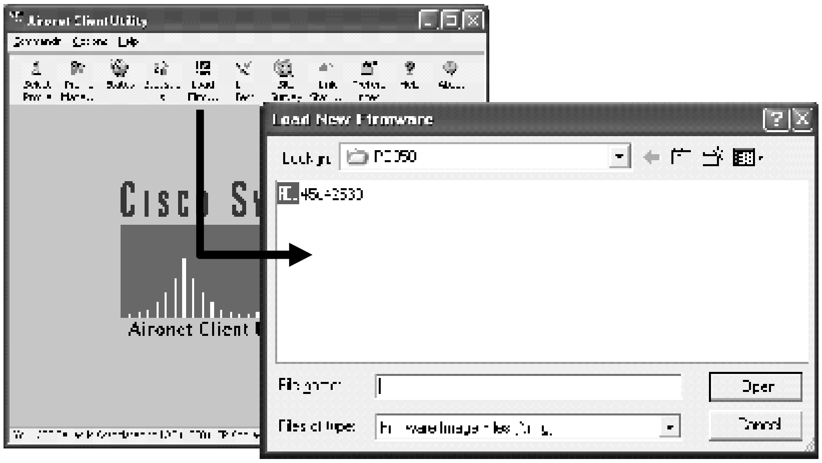
Caution When using Aironet Client Utility under the Windows NT or Mac OS operating systems, a user must log in as administrator (or have administrative privileges for the Mac OS). The Aironet utilities and drivers follow Microsoft's programming requirements for proper operation. For Aironet Client Utility to function properly and retrieve the radio information needed, it is necessary to make calls directly to the driver operating the radio card. Windows NT does not allow any non-administrator user the ability to make those calls (part of the security imposed by Microsoft). This is a function of NT and its user security, not the Aironet utility or driver, and there is no available work around. So, while the programs of Aironet Client Utility operate as designed by Microsoft, they will not operate under NT except when the installer is logged in as Administrator.

The user under Windows NT, using the Aironet Client Utility must log in as Administrator, or use one of the other Windows operating systems.

The new programs for diagnostics will also follow this rule. It is not a deficiency of the Cisco product, but a restriction imposed by Microsoft.

Aironet Client Utility: Loading Firmware

Cisco.com

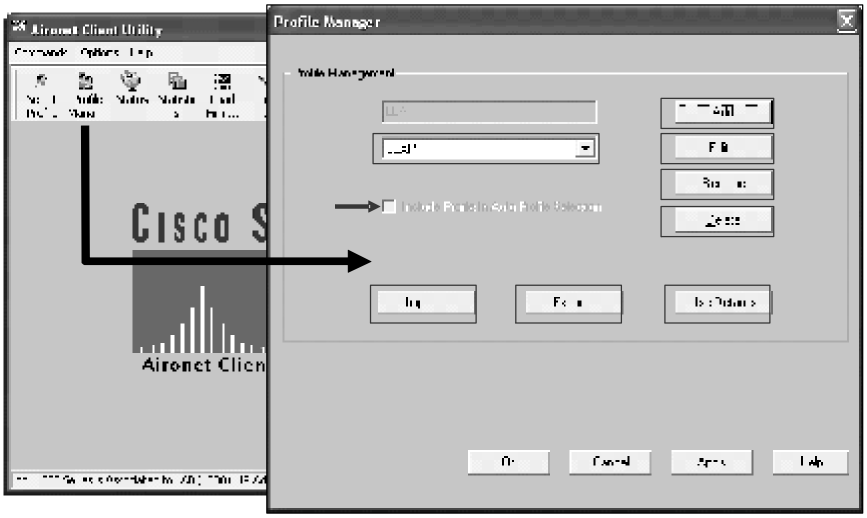


AWLF v3.1—7-12

Loading new firmware is as easy as copying a file under Windows. From the Aironet Client Utility (ACU) main window, click the **Firmware** button. Then simply select the path to the location of the new firmware image file, highlight the file, and click **Open**.

Aironet Client Utility: Profile Manager

Cisco.com



AWLF v3.1—7-13

The ACU allows the wireless client to use different “profiles” to connect to different wireless local-area networks (WLANs). Each profile will allow the user to selectively configure all parameters on the client card. The profile manager can then be used to change profiles. When the user selects a different profile, the settings for the client card are changed without requiring a reboot. ACU can accommodate a maximum of 16 profiles.

- **Use Profile Management:** This allows you to switch to a different profile that will be used by your wireless LAN adapter. The wireless LAN adapter will be configured with the new profile as soon as you click the Apply or OK buttons at the bottom of the Profile Manager window. If you select a profile that is using Lightweight and Extensible Application Protocol (LEAP) (without a saved user name and password), then Auto Profile Selection will be disabled. Under Windows XP, manually selecting a profile will block Windows XP Wireless Network Settings from overriding your profile selection.
- **Use Auto Profile Selection:** This radio button is available under the **Profile Manager** icon. This feature is available if two or more profiles have “Include Profile In Auto Profile Selection” selected. If Auto Profile Selection is enabled, whenever the wireless LAN adapter loses association for a predetermined amount of time, it will automatically be configured with the next profile that has “Include Profile In Auto Selection” checked. Under Windows XP, selecting Auto Profile Selection will block Windows XP Wireless Network Settings from overriding the current profile.**Use Another Application To Configure My Wireless Settings:** You will find this setting by clicking on the **Select Profile** icon. This option is only available for Windows XP. Selecting this radio button will allow Windows XP Wireless Network Settings to configure your Cisco wireless LAN adapter. It precludes the use of Use Selected Profile and Use Auto Profile Selection.

Note You cannot Auto Switch to or from a profile that is using LEAP, unless that profile is using a Saved User Name and Password. If you manually change to a profile that is using LEAP (without a Saved User Name and Password), then Auto Profile Selection will be disabled.

The Profile Management functions include:

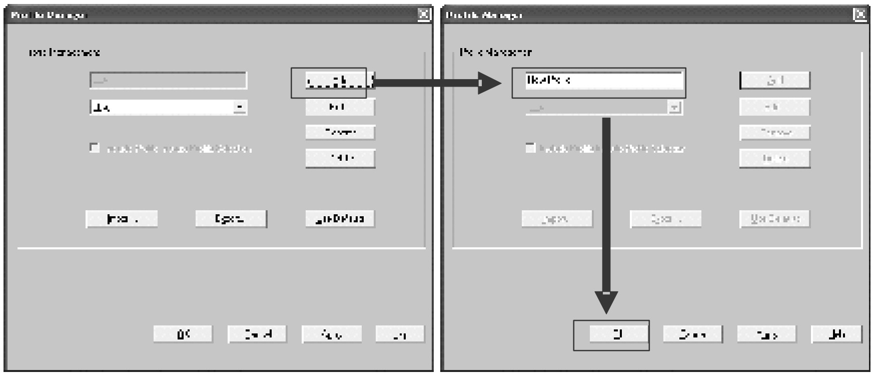
- **Add:** Adds profiles, up to the limit of 16. Once you have 16 profiles, the Add and Import buttons will be disabled.
- **Edit:** Edit the selected profile. The property sheets for the wireless LAN adapter will be displayed.
- **Rename:** Change the name of an existing profile to one that does not already exist.
- **Delete:** Delete a profile from the list.
- **Import:** Import a profile from a disk file.
- **Export:** Export a profile to a disk file.
- **Use Defaults:** Set the entire selected profile to default values.

Additionally, it is possible to specify that the selected profile is to be included in “Use Auto Profile Selection” by checking the “**Include Profile In Auto Profile Selection**” box. Profiles that use LEAP security are excluded from “Use Auto Profile Selection” (unless they are using a saved user name and password), and “Include Profile In Auto Profile Selection” is disabled.

Note A system administrator can selectively enable or disable certain features of the Profile Manager, such as Export Profile, and can enable or disable the same features on a per-profile basis. For example, an administrator can mark a profile that has been set up to access the corporate network as non-exportable, so that it cannot be made into a copy that could be lost or stolen.

Aironet Client Utility: Adding a Profile

Cisco.com



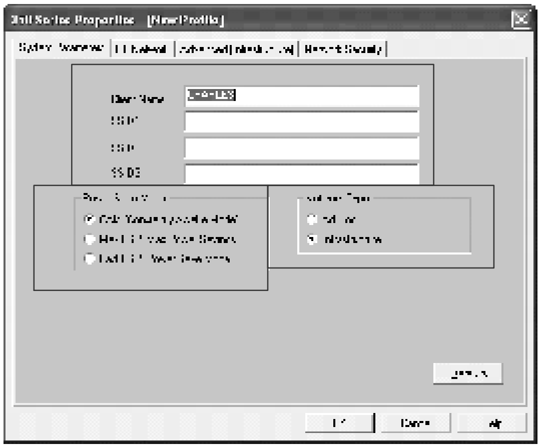
AWLF v3.1—7-15

In order to add a new profile:

1. Click on the **Add** button.
2. Type the name of your new profile in the white box area.
3. Press **Enter** (or click **OK** or **Apply**). The property sheets for that profile will then be displayed and may be edited.

Profile: System Parameters

Cisco.com

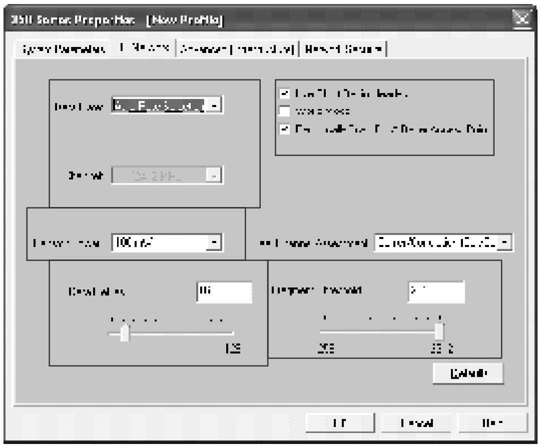


AWLF v3.1—7-16

- **Client Name:** Allows you to change the name of the client card for ease of manageability.
- **SSID:** Configurable parameter that must match the access point the client is attempting to associate with. Change the SSID on the card or add multiple SSIDs in a multiple-RF network.
- **If the Note:** SSID is left blank, it is considered a “null” value and will request the SSID of the access point the client is associating with to be sent to the client. The ability to broadcast its SSID is a configurable parameter on the Cisco Aironet application processors (Aps). Only the first SSID slot can be configured as a null. If any of the other slots are left blank, they will not be considered nulls. The ACU will not allow you to configure the first SSID with a blank and have SSID 2 and SSID 3 configured with known SSIDs. The ACU will automatically move SSID 2 to the SSID 1 position and SSID 3 to the SSID 2 position. This can be observed after answering OK to these settings.
- **Power Save Mode: Select** the power save mode for this client.
- **Network Type: Select** a network type to communicate to an access point (infrastructure) or in “ad hoc” mode to other client cards.

Profile: RF Network

Cisco.com

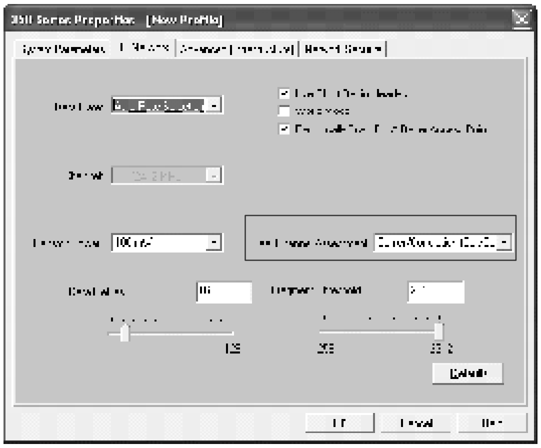


AWLF v3.1—7-17

- **Data Rate:** Selects the data rate of the client card. Selecting Auto will auto-scan to find an access point to associate with. Specific data rate may also be specified. If specifying a specific data rate, note that the client card will then communicate with access points at that data rate only.
- **Use Short Radio Headers**: Allows for the use of short radio headers with access point configured to them. Improves performance.
- **World Mode**: Allows the client to "learn" the channel set of the associated access point.
- **Periodically Scan For A Better Access**: Selecting this checkbox causes the client to look for a better Access Point if its signal strength becomes low and to switch associations if it finds one.
- **Channel:** Indicates which channel the card is currently using.
- **Transmit Power:** Allow for lowering the transmit power of the card.
- **Data Retries:** Allows selection of the number of retries that the radio will attempt on a per-packet basis.
- **Fragment Threshold:** Sets the maximum packet size that the radio will transmit. If the packet is beyond the threshold, it will be fragmented.

Profile: RF Network

Cisco.com



AWLF v3.1—7-18

- **Clear Channel Assessment:** This parameter specifies the method that determines whether the channel on which your client adapter will operate is clear prior to the transmission of data. Options include:
  - Firmware Default (xxx) – The Clear Channel Assessment (CCA) mechanism will report that the channel is busy based on the default value of the client adapter's firmware. The firmware's CCA default value is shown in parentheses.

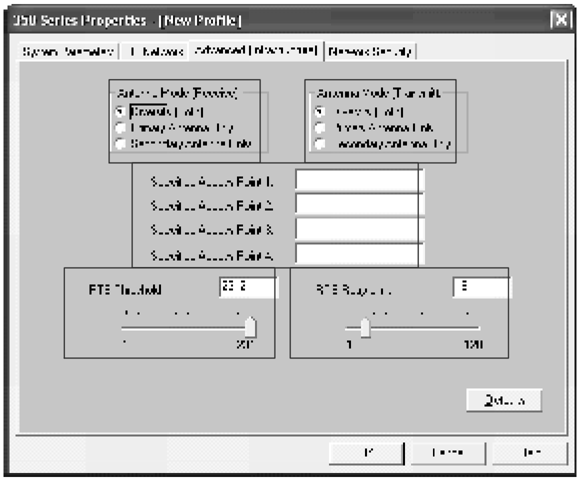
Note The default value for PC, LM, and PCI card firmware is Carrier/Correlation (Car/Cor). The default value for MiniPCI card firmware is Energy Detect (ED).

  - Carrier/Correlation (Car/Cor) – The CCA mechanism will report that the channel is busy upon detection of a direct-sequence spread spectrum (DSSS) signal. This signal may be above or below the Energy Detect (ED) threshold.
  - Energy Detect (ED) – The CCA mechanism will report that the channel is busy upon detection of any RF energy above the Energy Detect threshold.
  - ED or Car/Cor – The CCA mechanism will report that the channel is busy upon detection of a DSSS signal or any RF energy above the Energy Detect threshold.

Note Some laptop models emit low power 2.4 GHz noise out of the mother board CCA helps to negate this problem.

Profile: Advanced (Infrastructure)

Cisco.com



AWLF v3.1—7-19

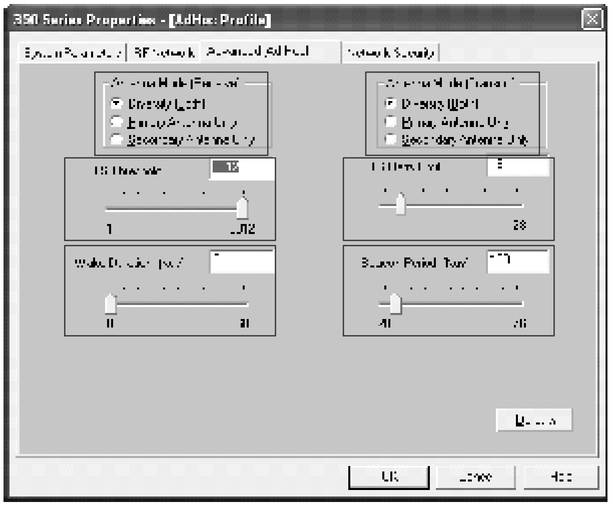
- **Antenna Mode (Receive):** Allows the user to disable receive diversity and specify the antenna port to transmit the packet from.
- **Antenna Mode (Transmit):** Allows the user to disable transmit diversity and specify the antenna port to transmit the packet from.
- **Specified access point:** Specifies the access point by Media Access Control (MAC) address that the client attempts to associate with.
- **RTS Threshold:** Specifies the size of the packet that the client will send as a request to the access point prior to transmit. It will not transmit the packet until it receives an ACK back from the access point.
- **RTS Retry Limit:** Sets the number of times that the Request To Send (RTS) packet is retried.

Items to note:

- **Primary Antenna Only:** If you are *not* using the standard snap on antenna, choose this option if the antenna you are using is connected to the **Primary (right-hand) antenna port** (denoted J1). This tells the Cisco Wireless LAN Adapter not to attempt to communicate using the Secondary (left-hand) antenna port (J2), since no antenna is connected to it.
- **Secondary Antenna Only:** If you are *not* using the standard snap on antenna, choose this option if the antenna you are using is connected to the **Secondary (left-hand) antenna port** (denoted J2). This tells the Cisco Wireless LAN Adapter not to attempt to communicate using the Primary (right-hand) antenna port (J1), since no antenna is connected to it.

Profile: Advanced (Ad Hoc)

Cisco.com

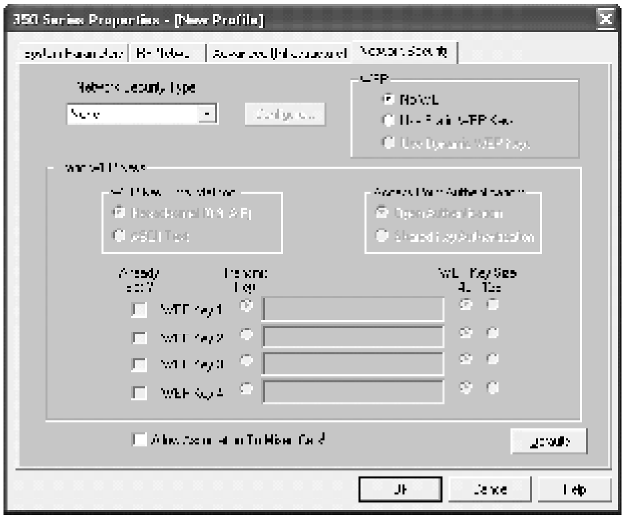


AWLF v3.1—7-20

- **Antenna Mode (Receive):** Allows the user to disable receive diversity and specify the antenna port to transmit the packet from.
- **Antenna Mode (Transmit):** Allows the user to disable transmit diversity and specify the antenna port to transmit the packet from.
- **RTS Threshold:** Specifies the size of the packet that the client will send as a request to the access point prior to transmit. It will not transmit the packet until it receives an ACK back from the access point.
- **RTS Retry Limit:** Sets the number of times that the Request To Send (RTS) packet is retried.
- **Wake Duration:** This parameter specifies the amount of time per Hop Dwell Period that the adapter stays awake, listening for data packets. This is only used in Power Save Mode. This parameter is represented in Kilo Microseconds.
- **Beacon Period:** This parameter specifies the duration between beacon packets, which are used by IEEE 802.11 systems for synchronization. The beacon packet contains timing and other information that is broadcast over the airwaves. Any station that can hear the beacon packet can then synchronize with that cell. The default beacon period is 100 milliseconds.

Profile: Network Security

Cisco.com



AWLF v3.1—7-21

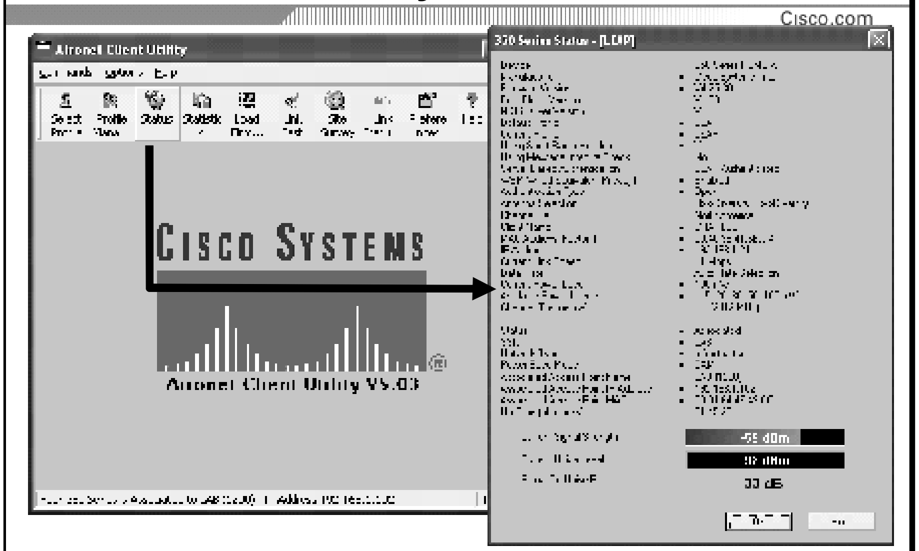
- **Network Security Type:** Choose None, LEAP, or Host-Based EAP (if using Windows XP). Choosing None as the Network Security type allows the use of static WEP keys or no WEP (no encryption).
- **Use Static WEP Keys:** Allows the use of statically entered WEP keys for encryption (but not using an Extensible Authentication Protocol [EAP], such as LEAP). Selecting this option will make the WEP keys slots available. Enter the WEP keys; choose the Access Point Authentication method, and Enable WEP.
- **Access Point Authentication:** Configured to match the Authentication type of the access point. Access point authentication types are discussed further in Module 9, Security.
- **LEAP:** Allows Cisco software and firmware to cause the network logon to trigger server-based authentication using user name and password. Requires a LEAP-enabled Remote Authentication Dial-In User Service (RADIUS) server running on the network. The Configure button may then be used to launch the LEAP configuration page. LEAP configuration settings for client cards and access points are discussed in Module 9, Security.

Note **Host**-Based EAP (EAP-TLS or EAP-MD5) can be configured on the Windows XP operating system (ACU is not required).

- **Allow Association to Mixed Cells**: Enables the client card to associate to access points that permit association of clients with or without a WEP key.

Aironet Client Utility: Status

Cisco.com



AWLF v3.1—7-22

The status window gives a snapshot of how the card is configured--the driver version, firmware version, data rate, and so on. This information is needed during a diagnostic processing of the system.

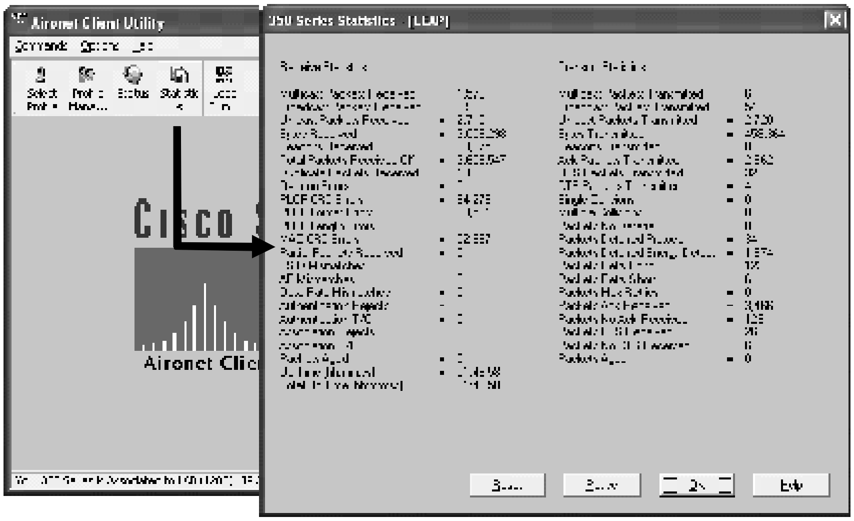
If a customer is having some problems, go to this window to verify that all the settings for the card match what the overall RF network is set for.

This window shows the configuration of every parameter for the card, as well as firmware and driver versions, and reports information on the link between the card and the access point.

For an explanation of each parameter, click the **Help** button and an explanation of each parameter will be displayed.

Aironet Client Utility: Statistics

Cisco.com



AWLF v3.1—7-23

To view the Statistics screen, click on the **Statistics** button on the main page.

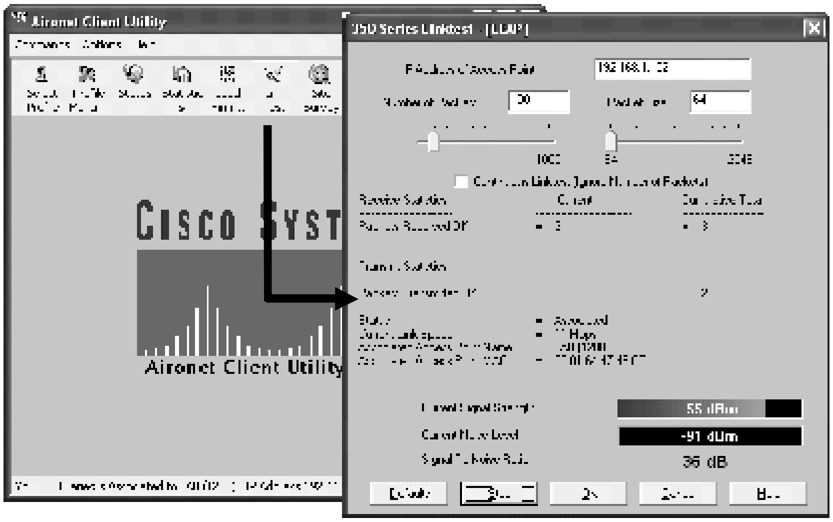
The statistics screen is a valuable resource for diagnostic purposes on a per-client basis.

The screen helps determine the amount of packets that the client card has received both on a multicast and unicast basis. It also gives a count of errors that have occurred from the last time a reset was done. These are invaluable tools to determine if the card is experiencing any difficulties or if the network is bogging the card down with multicast traffic.

For an explanation of the different statistics, click the **Help** button and the definitions will be displayed.

Aironet Client Utility: Link Test

Cisco.com



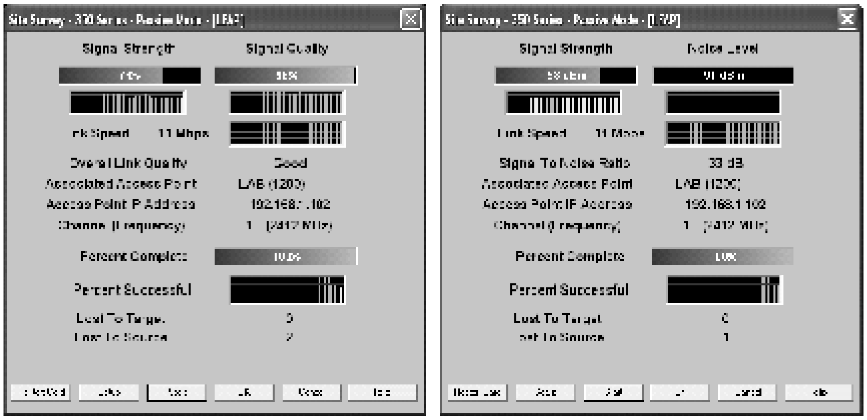
© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—7-24

The Link Test Utility screen permits test of specific packet size and quantity to verify wireless connection characteristics with a specific data payload.

Aironet Client Utility: Site Survey

Cisco.com



Site Survey - 350 Series - Passive Mode - [LEAP]

Signal Strength: [illegible]
Signal Quality: [illegible]
Link Speed: 11 Mbps
Overall Link Quality: Good
Associated Access Point: LAB (1200)
Access Point IP Address: 192.168.1.102
Channel (Frequency): 1 (2412 MHz)
Percent Complete: 100%
Percent Successful
Lost To Target: 0
Lost To Source: 2

Site Survey - 350 Series - Passive Mode - [LEAP]

Signal Strength: -58 dBm
Noise Level: -91 dBm
Link Speed: 11 Mbps
Signal To Noise Ratio: 33 dB
Associated Access Point: LAB (1200)
Access Point IP Address: 192.168.1.102
Channel (Frequency): 1 (2412 MHz)
Percent Complete: 100%
Percent Successful
Lost To Target: 0
Lost To Source: 1

AWLF v3.1—7-25

The Site Survey utility allows a user to perform a site survey to determine the best placement of the access points in order to provide the desired coverage.

The Site Survey can run in either Passive or Active mode. The Active mode is used to perform site surveys.

The Site Survey utility can be set to display results as percentages, or as actual values (for example, as dBm, or decibels per milliwatt). Complete the following steps to switch from percentage to dBm.

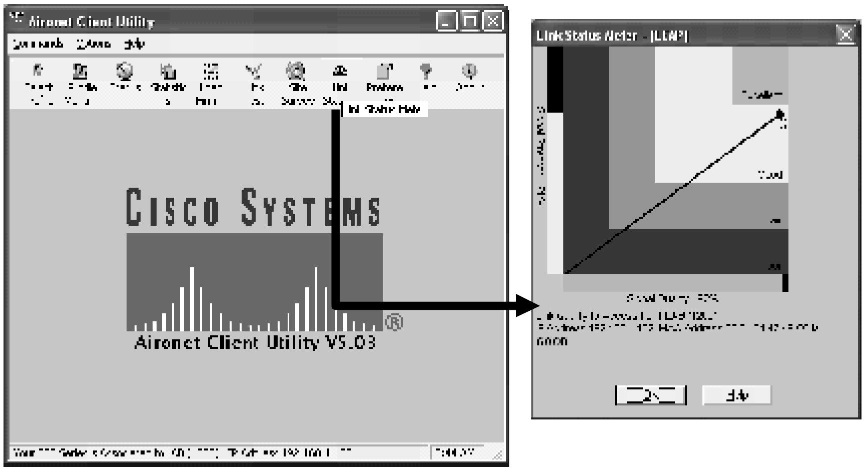
Step 1 Click on the Preferences icon on the main page.

Step 2 Select the dBm radio button under **Signal Strength Display Units.**

Now your ACU Site Survey will show signal to noise ratio.

Link Status Meter

Cisco.com



AWLF v3.1—7-26

Link Status Meter for Windows provides a graphical display of the RF connection between the client card and the access point.

The left side of the display is a bar graph that shows signal strength.

On the bottom of the display is a bar graph showing the signal quality.

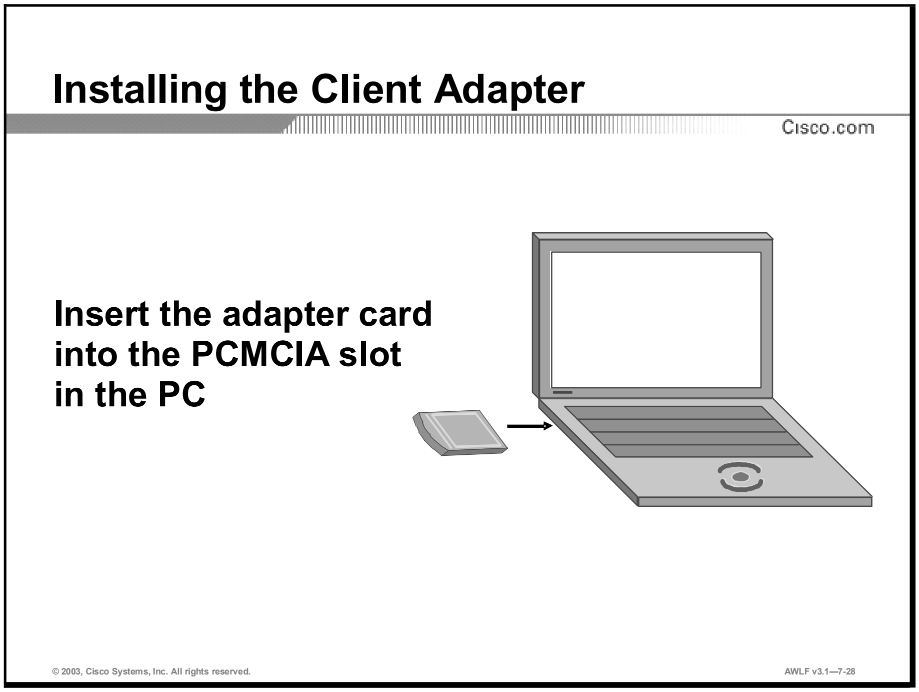
As a combination of the two, the line extending form the apex, is an overall signal performance indicator.

Just below the display is the access point being associated with (the MAC address) and the performance of the link (i.e., GOOD).

As a client moves around the site, the display will indicate the performance of the link, based upon signal strength and signal quality.

Under the file menu, there is a preference selection to allow changes to the display to your preference.

Laboratory Exercise: Client Card Adapter Installation



Installing the Client Adapter

Cisco.com

Insert the adapter card into the PCMCIA slot in the PC

AWLF v3.1—7-28

Setup

Obtain a Cisco Aironet Wireless PCMCIA adapter card from the instructor.

Scenario

You are installing a Cisco Aironet Wireless PCMCIA adapter card on a client machine.

Task 1: Installing the PCMCIA Adapter Card

When you install the client card adapter, make sure the Cisco label is facing up. As the card slides into the PCMCIA slot, it may be necessary to apply slight pressure to ensure that the card seats properly. The card should slide easily into the PCMCIA slot and you should not force it. If it seems the card will not seat properly, remove the card and attempt to reinsert it. If the card will still not seat properly ask the instructor for assistance.

Windows 95, NT, and MacOS users: Do not insert the card into your PC at this point. Proceed to the installation section for your operating system, listed below.

Task 2: Loading Drivers for the PCMCIA adapter

Identify the operating system on your PC below and proceed to that section of the lab to continue the installation process.

■ Windows 95	pg. 26–27
■ Windows 98	pg. 28
■ Windows Me	pg. 29
■ Windows 2000	pg. 30
■ Windows NT	pg. 31
■ Windows XP	pg. 32–33
■ Mac OS X and Mac OS 9.x	pg. 34–38

Windows 95 Version A

For Windows 95 Version A, follow these steps to install your client adapter card.

Step 1 Insert the driver CD into your laptop.

Step 2 Open the Windows 95 directory.

Step 3 Copy the **Win95Driver.exe** file to a directory (other than the root directory) on your PC.

Step 4 Remove the driver CD from your laptop.

Step 5 Locate the **Win95Driver.exe** on your PC and double-click the file. This will start the extraction process.

Step 6 You will be prompted for a location for the files. By default this is the A: drive (most likely your floppy disk drive). Instead, enter the location C:\Cisco\drivers for the files. Click **Unzip.** When finished, click **Close.**

Step 7 Now insert the client adapter card into your PC. Windows should detect the device and open a New Hardware Found window.

Step 8 Select Driver from disk provided by hardware manufacturer and click OK.

Step 9 In the Install From Disk screen, enter the path C:\Cisco\drivers and click **OK**.

Step 10 If you are prompted to insert the Windows 95 operating system disk, click **OK** and enter one of the following paths in the dialog box:

- The Windows CD (if you have a copy of your installation CD).
- The C:\Windows\Options\Cabs directory (if your PC has the installation Cab files loaded).
- The C:\Windows directory.
- The C:\Windows\System directory.

Step 11 When prompted to restart your computer, click **Yes**.

Windows 95 Version B

For Windows 95 Version B, follow these steps to install you client adapter card.

Step 1 Insert the driver CD into your laptop.

Step 2 Open the Windows 95 directory.

Step 3 Copy the **Win95Driver.exe** file to a directory (other than the root directory) on your PC.

Step 4 Remove the driver CD from your laptop.

Step 5 Locate the **Win95Driver.exe** on your PC and double-click the file. This will start the extraction process.

Step 6 You will be prompter for a location for the files. By default this is the A:\ drive (most likely your floppy disk drive). Enter the location C:\Cisco\drivers for the files instead. Click **Unzip.** When finished, click **Close.**

Step 7 Now insert the client adapter card into your PC. Windows should detect the device and open a New Hardware Found screen.

Step 8 The Update Device Driver Wizard launches and will eventually indicate that it was unable to locate a driver for the device. Click **Next**.

Step 9 Click Other Locations.

Step 10 In the Select Other Location screen, enter the path C:\Cisco\drivers and click **OK**.

Step 11 The Update Device Driver Wizard should indicate it has found the driver.

Step 12 Click **Finish**.

Step 13 An Insert Disk screen will appear prompting you to insert the Aironet wireless LAN adapter Installation Disk. Insert the disk and click **OK**.

Step 14 If a screen appears indicating that the pcx500.sys file could not be found, enter the path C:\Cisco\drivers and click **OK**.

Step 15 If you are prompted to insert the Windows 95 operating system disk, click **OK** and enter one of the following paths in the dialog box:

- The Windows CD (if you have a copy of your installation CD).
- C:\Windows\Options\Cabs directory (if your PC has the installation Cab files loaded).
- C:\Windows directory.
- C:\Windows\System directory.

Step 16 When prompted to restart your computer click **Yes**.

Windows 98

For Windows 98, follow these steps to install your client adapter card:

Step 1 After you insert the client adapter card into your PC, Windows will automatically detect the device.

Step 2 Windows will briefly open the New Hardware Found screen, and start collecting information for a driver information database.

Step 3 The Add New Hardware Wizard dialog box opens and indicates that Windows is searching for new drivers. Click **Next**.

Step 4 Another dialog box opens and asks what you want Windows to do. Select Search for the best driver for your device (Recommended) and click **Next.**

Step 5 Select your CD-ROM drive, deselect all other options, insert the driver CD into your computer's CD-ROM drive, and click **Next**.

Step 6 The hardware wizard finds the installation files on the CD and indicates that it is ready to install the drivers. Click **Next**.

Step 7 If you are prompted to insert the Windows 98 operating system disk, click **OK** and enter one of the following paths in the dialog box:

- The Windows CD (if you have a copy of your installation CD).
- C:\Windows\Options\Cabs directory (if your PC has the installation Cab files loaded).
- C:\Windows directory.
- C:\Windows\System directory.

Step 8 The Add New Hardware Wizard screen opens and indicates that the installation is complete. Click **Finish**.

Step 9 When prompted to restart your computer, remove the CD and click **Yes**.

Windows ME

A driver for the client adapter card is included with Windows ME. When installed, the Add New Hardware Wizard will launch, detect the device, and begin updating the driver database to accommodate the new device.

Note The device driver included with Windows ME will need to be updated, as driver version 8.00 (not included with Windows ME) will be needed to complete this lab exercise.

To update the driver, follow these steps

Step 1 From the Windows Task bar, click **Start> Settings>Control Panel>System**. This will launch the System Properties Screen.

Step 2 Click the **Device Manager** tab. This will bring up the Device manager screen.

Step 3 Click the + symbol next to the Network Adapters icon.

Step 4 Click on the **Cisco Systems 350 Series Wireless LAN Adapter** icon. Click the **Properties** button.

Step 5 This will launch the Cisco Systems 350 Series wireless LAN adapter **Properties** page.

Step 6 Click on the **Driver** tab. Click the **Update Driver** button. This will launch the Update Device Driver Wizard.

Step 7 Click the Specify location of the driver (Advanced) radio button. Click Next.

Step 8 Select Search for a better driver than the one your device is using now (Recommended) radio button. Make sure the Removable Media checkbox is deselected.

Step 9 Insert the CD-ROM that was provided to you by the instructor into your CD-ROM drive. Select the **Specify a location** checkbox and click the **Browse** button. Browse to your computer's CD-ROM drive. Click **Next**.

Step 10 When asked what you would like to install, select **The updated driver (recommended)** and click **Next**.

Step 11 A screen will appear indicating the driver that will be installed and listing the driver location. Click **Next**.

Step 12 If Windows cannot find the pcx500.sys file and requests that you insert the CD (even though the CD is already in your computer's CD-ROM drive), enter the letter of your CD-ROM drive (such as **D:**) in the Copy Files From Dialog box and click **OK**.

Note A screen may appear during the process indicating that Windows cannot find the file netX500.cat. Click the **Skip** button. The file is not needed when installing later version of the driver. Windows may launch this screen several times while trying to locate the file. Each time the screen appears, click the **Skip** button.

Step 13 When you are notified that the installation is complete, click the **Finish** button.

Step 14 When you are prompted to restart your computer, remove the CD and click **Yes**.

Windows 2000

Step 1 After you insert the client adapter card into your PC, Windows 2000 automatically detects it and briefly opens the Found New Hardware screen.

Note The device driver included with Windows 2000 will need to be updated, as driver version 8.00 (not included with Windows 2000) will be needed to complete this lab exercise. To insure that you have the correct driver version installed, follow Steps 2-7.

Step 2 The Found New Hardware Wizard screen opens and indicates that the wizard will assist you in the installation of the driver. Click **Next**.

Step 3 Another screen opens and asks what you want the wizard to do. Select the **Search for a suitable driver for my device (recommended)** radio button and click **Next**.

Step 4 Select CD-ROM drives, deselect all other options, insert the driver CD into your computer's CD-ROM drive, and click **Next**.

Step 5 A screen will appear indicating the driver that will be installed and listing the driver location. Click **Next** to start copying the files.

Note A screen may appear during the process indicating that Windows cannot find the file netX500.cat. Click the **Skip** button. The file is not needed when installing later version of the driver. Windows may launch this screen several times while trying to locate the file. Each time the screen appears, click the **Skip** button.

Step 6 A screen will appear indicating that the installation is complete. Click **Finish**.

Step 7 When prompted to restart the computer, remove the CD from your computer's CD-ROM drive, and click **Yes**.

Windows NT

Step 8 If an error message appears indicating that at least one service or driver failed during system setup, click **OK**.

Step 9 Follow the steps below to obtain an available interrupt request (IRQ):

- Select Start > Programs > Administrative Tools > Windows NT Diagnostics.
- Click the Resources tab.
- The used IRQs are listed in numerical order along the left side of the Resources screen. Write down the number of an IRQ that is not being used. You will need this IRQ for the installation.

Step 10 On the computer desktop, click **Start>Control Panel**>**Devices**.

Step 11 Scroll down and select **PCMCIA**. Click **Startup**, select **Automatic**, and click **OK**.

Note For PC cards also ensure that the CardBus service is deselected.

Step 12 Insert the driver CD into your computer's CD-ROM drive.

Step 13 Click **Start>Control Panel>Network.**

Step 14 Click the **Adapters** tab and select **Add**.

Step 15 In the Select Network Adapter screen, click **Have Disk**.

Step 16 In the Insert Disk screen, enter the letter of your CD-ROM drive (such as **D:**\) and click **OK**.

Step 17 In the Select OEM Option box, select the Cisco Systems wireless LAN adapter and click **OK**.

Step 18 In the Adapter Setup screen, enter an available IRQ number, which you obtained earlier.

Step 19 Click **OK**. Click **Close**.

Step 20 The Microsoft TCP/IP Properties screen should open. (If it does not open, Click **Start>Control Panel**>**Network**.

Step 21 Select **Protocols>TCP/IP>Properties**.

Step 22 Click the **Specify an IP address** radio button and enter your IP address and subnet mask. Click **OK**. To obtain your IP Address, see page 39, Step 4.

Step 23 When prompted to restart your computer, remove the CD and click **Yes**.

Windows XP

Step 1 A driver for the client adapter card is included with Windows XP. When the card is inserted, the New Hardware icon appears in the taskbar indicating that a new device has been found and Windows XP is attempting to locate drivers for the device.

Step 2 Windows XP will install drivers for the new device, and the New Device icon will appear in the taskbar indicating, "Windows has detected the installation of a new networking device. If you want to set up a network, click here to run the Network Setup Wizard".

Step 3 **Right-click the icon** and the Windows message will disappear.

Note The device driver included with Windows XP will need to be updated, as driver version 8.00 (not included with Windows XP) will be needed to complete this lab exercise.

To update the driver, follow these steps:

Step 4 From the Windows Task Bar click **Start>Settings>Control Panel>System**. This will launch the System Properties screen. Click the **Hardware** tab. Click the **Device Manager** button.

Step 5 Click the + symbol next to the **Network Adapters** icon. Double click the **Cisco Systems 350 Series Wireless LAN Adapter** icon.

Step 7 This will launch the Cisco Systems 350 Series wireless LAN adapter **Properties** screen.

Step 8 Click the **Update Driver** tab. This will launch the **Hardware Update Wizard**.

Step 9 Click the **Install from a list or specific location (Advanced)** radio button. Click **Next**.

Step 10 Insure that the **Search for the best driver in these locations** radio button is checked, and the **Search removable media (floppy, CD-ROM…)** box is checked. Insure that the CD provided by your instructor is in your CR-ROM drive and click **Next**.

Step 11 The Hardware Wizard will then begin copying files and will display the message "Please wait while Windows installs the new software", while it sets a system restore point and backs up old files in case of a problem.

Note A screen may appear during the process indicating that Windows cannot find the file netX500.cat. Click the **Skip** button. The file is not needed when installing a later version of the driver. Windows may launch this screen several times while trying to locate the file. Each time the screen appears, click the **Skip** button.

Step 12 Once the Hardware Wizard is finished copying files, it will tell you that "The Wizard has finished installing software for: Cisco Systems 350 Series wireless LAN adapter". Click **Finish**.

Step 13 Close the Device Manager and System Properties screens.

Step 14 A message will appear over the network icon in the system tray indicating “One or more wireless networks are available. To see a list of available networks, click here”. **Click on the message** or the icon. This will launch the **Connect to Wireless Network** screen.

Step 15 Click the **Advanced** button. This will launch the Wireless Network Connection Properties screen. Insure that the Use **Windows to manage my wireless network settings box** is not checked. Click **OK**.

Note While Windows XP is capable of managing the configuration of the Cisco Aironet client card, this class is focused on the Cisco Aironet products and how to configure and use the client adapter using the Cisco Aironet software. For more information on how to use Windows XP to manage your wireless connections, see your Windows documentation.

PowerBook and PowerMac: Mac OS X and Mac OS 9.x

Note For Mac OS 9.x, you must install the driver and client utility before installing the client adapter into your PowerBook or PowerMac.

Note For Mac OS X, you should install the client adapter into your PowerBook or PowerMac before installing the driver and client utility.

Step 1 Insert the Cisco Aironet Series wireless LAN adapters CD into your computer's CD-ROM drive. Choose the MAC OS directory.

Step 2 Double-click the **MACOSInstallv2x.sit** file to expand the file.

Step 3 Double-click **Cisco WLAN Install** to activate the installer.

Note You should keep the Cisco WLAN Install file. The file may be needed in the future to possibly uninstall your client utility and driver for a clean install.

Step 4 If you are using Mac OS X, when the Authenticate screen appears, enter your password in the Password field. Your Macintosh user name will appear in the Name field. Click **OK**.

Note To install the client utility on Mac OS X, you must have administrator privileges for the Macintosh.

Step 5 When the Cisco Aironet wireless LAN adapter Software screen appears, click **Continue**.

Step 6 Read the terms and conditions of the Software License Agreement and click **Accept** or **Decline**. If you decline the license agreement, the client utility installation ends.

Step 7 Read the Read Me screen information and click **Continue**.

Step 8 The Cisco WLAN Installer detects your computer operating system and displays the appropriate installation screen. When the Cisco WLAN Install screen appears, perform the following operations:

Expand the Mac OS software component list by clicking the right triangle on the left of the Mac OS name.

Note The installer normally installs both the PCI and PC Card drivers. You can deselect one of the drivers by clicking the selection box to remove the X; for example: you can deselect the PCI driver when using a PowerBook or you can deselect the PC Card driver when using a PowerMac.

Step 9 Click **Install** to begin the installation process.

Step 10 Click **Continue** when a screen appears indicating your computer must restart after installing the software.

Step 11 A message appears indicating "One moment please..." then a screen appears that shows the installation progress. After the files are copied to the Macintosh hard disk, a screen appears indicating that the installation was successful. Click **Restart** to restart your computer and finish the client utility installation. The installer has installed the client utility, the help files, and the drivers.

Step 12 When your Macintosh completes the power-up process following a successful install, the Client Adapter Setup Assistant activates. The setup assistant guides you through the initial configuration options of your client adapter or it allows you to manually select the screens by clicking the configuration tabs. Each screen contains descriptive information to assist you in configuring your client adapter.

Follow the steps below to complete the initial configuration settings for your wireless system:

Step 13 If the Introduction screen is not visible, click the **Introduction** tab. Read the screen information and click **Start** to continue to the Client Name screen.

Step 14 Click the **Done** button (on any screen) to exit the setup assistant.

Note For MAC OS X, follow steps 15-22 to assign your IP address and complete this task.

Note For Mac OS 9.x users, proceed to step 23 to assign your IP address and complete this task.

Step 15 Click **Network Settings** to configure your Macintosh network parameters.

Step 16 When the Network screen appears, verify that the Location dialog box contains **Automatic** or click the Location up or down arrows and select **Automatic**.

Step 17 Click the Show up or down arrows and select **Ethernet Adaptor (enx)** or **PCI Ethernet Slot x** (where x is a number that indicates a specific adapter or slot).

Step 18 Click the **TCP/IP** tab. The TCP/IP screen appears.

Step 19 Select **manually** in the Configure drop-down box and enter the client adapter IP address as 10.0.0.xxx with xxx being the number of the PC Card that was given to you by the instructor, and the subnet mask (255.255.255.0).

Step 20 Click **Apply Now** to apply your TCP/IP configuration options.

Step 21 Click **System Prefs** on the main menu bar and click **Quit System Prefs**.

Step 22 You may now proceed to **Task 4** to configure the wireless client. Because the ACU has already been installed on your computer, launch the ACU and proceed to Step 11 (page 46).

PowerBook and PowerMac: Mac OS 9.x

Step 1 After your computer reboots, insert the client adapter into your PowerBook's PC card slot. The Cisco wireless LAN adapter icon appears on the desktop.

Step 2 Click the apple-shaped icon in the top left corner of the desktop.

Step 3 Select **Control Panels** > **AppleTalk**. The AppleTalk screen appears.

Step 4 Make sure the name of the correct wireless LAN adapter appears in the Connect via dialog box. If it does not, click the up or down arrow on the right side of the Connect via dialog box and select the correct adapter.

Step 5 Close the AppleTalk screen.

Step 6 Click the apple-shaped icon in the top left corner of the desktop.

Step 7 Select **Control Panels** > **TCP/IP**. The TCP/IP screen appears.

Step 8 Select **Cisco wireless LAN adapter** in the Connect via drop-down box.

Step 9 Select **manually** in the Configure drop-down box and enter the IP address, subnet mask. To obtain your IP address see page 39, Step 4.

Step 10 Close the TCP/IP screen.

Step 11 When a screen appears asking if you want to save changes to the current configuration, click the **Save** button.

Step 12 Double-click the **Macintosh HD** icon on the desktop. The Macintosh HD screen appears.

Step 13 Double-click the **Cisco pcm3x0 Folder** icon. The Cisco pcm3x0 Folder screen appears.

Step 14 Double-click the **pcm3x0PPC** icon. The Cisco pcm3x0 screen appears, and the computer searches for the client adapter. After the adapter is found, the Cisco pcm3x0 : Basic Properties screen appears.

Step 15 Under Radio, make sure that radio status is on. If it is off, click the **Turn radio on** button.

Step 16 Perform one of the following:

Step 17 Select **Computer to base station** in the Network subwindow.

Step 18 Type your RF network's (case-sensitive) SSID in the SSID dialog box.

Step 19 Click **OK**.

Step 20 Eject the CD by clicking the CD icon on the desktop and dragging it to the trashcan.

Step 21 You may now proceed to **Task 4** to configure the wireless client. Because the ACU has already been installed on your computer, launch the ACU and proceed to Step 11 (page 46).

Setup

When the wireless adapter has been installed, it will need to have TCP/IP configured to connect to the access point.

Scenario

Your customer needs TCP/IP configured so that the computer can access the network.

Task 3: Assigning Your IP Address

Complete the following tasks to assign an IP address that will allow you to connect to the access point.

You will now need to change the IP address of your computer to allow you to browse to the access point. Your client card is currently connected to the access point, but you would be unable to configure the access point via the web browser because your client card and the access point are not part of the same subnet.

Note Windows NT and MacOS users: Proceed directly to Step 4 to obtain your IP address.

Step 1 From the Windows task bar click the **Start**>**Settings>Control Panel>Network**. This will launch the Network Properties page. Insure that the **Cisco Systems 350 Series wireless LAN adapter** is listed as a network device.

Step 2 Scroll down and highlight **TCP/IP -> Cisco Systems 350 Series Wireless LAN Adapter**, then click **Properties**. This will launch the Properties Page for the TCP/IP configuration of your adapter.

Step 3 Click the **Specify an IP Address** radio button. Notice that the **IP Address** and **Subnet Mask** boxes are no longer grayed out.

Step 4 For the IP Address, enter 10.0.0.xxx, with xxx being the number printed on the label of the card you have been assigned. For the Subnet Mask, enter 255.255.255.0.

Note Windows NT and MAC OS 9.x users: return to your Task 2 page to finish assigning your IP address

Step 5 Windows NT and Mac OS 9.x users return to your installation page

Step 6 Click **OK**. This will return you to the Network Properties screen. Click **OK**.

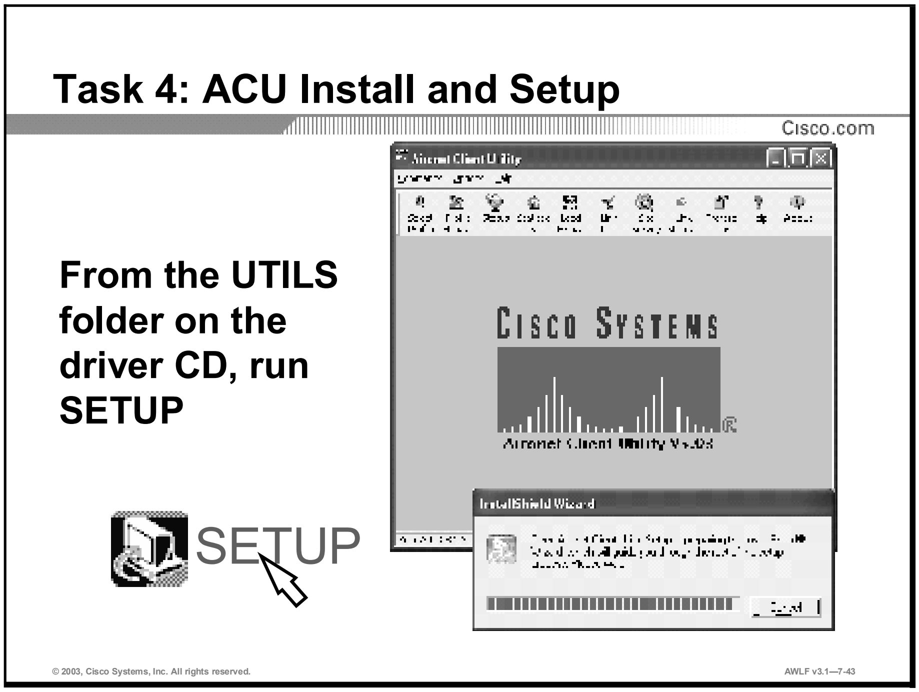
Windows will begin copying files and may ask for the Windows CD. All of the files you require should already be loaded on your PC.

Step 7 As Windows prompts you for various drivers you can usually direct it to one four places for the drivers:

- The Windows CD (if you have a copy of your installation CD).
- The C:\Windows\Options\Cabs directory (if your PC has the installation Cab files loaded).
- The C:\Windows directory.
- The C:\Windows\System directory.

Note If your computer is already part of a network, you probably already have all of the files loaded on your computer. These files will be stored in either the C:\Windows or C:\Windows\System directory. Each time the computer asks for a non-Cisco file, direct it to these directories and your computer should be able to locate the files.

Step 8 Once the installation is complete, Windows will prompt you to reboot. Click **Yes** to reboot the computer.



Task 4: ACU Install and Setup

Cisco.com

From the UTILS folder on the driver CD, run SETUP

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—7-43

Setup

Use the driver CD to load the Aironet Client Utility on your laptop.

Scenario

You have just installed a Cisco Aironet Wireless PCMCIA adapter for your client and must now install the Aironet Client Utility.

Task 4: Installing and configuring the ACU.

Complete the following steps to install the ACU.

Step 1 Install the driver CD in your laptop. From the Start menu, choose **Run**. Type in [appropriate drive letter]/utilities/setup. This will run the utilities setup program.

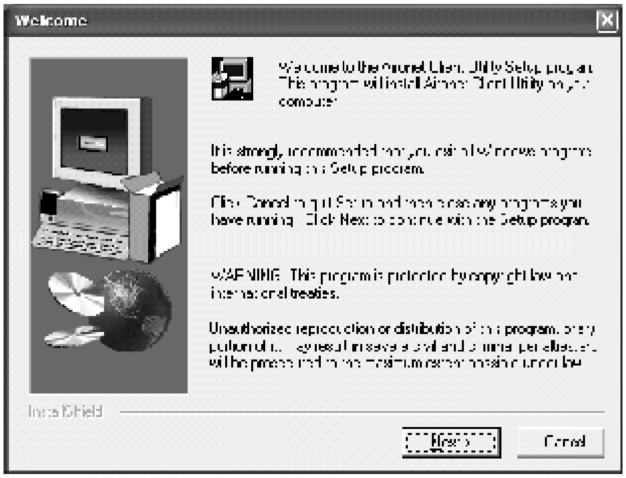
Or

Step 1 Browse to (or explore) the driver CD, open the **UTILS** folder, and click the **SETUP** icon. This will start the SETUP utility.

Visual Objective

This figure shows the Aironet Client Utility Setup screen.

Task 4: ACU Install and Setup (Cont.)



Welcome to the Aironet Client Utility Setup program. This program will install Aironet Client Utility on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup program.

Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

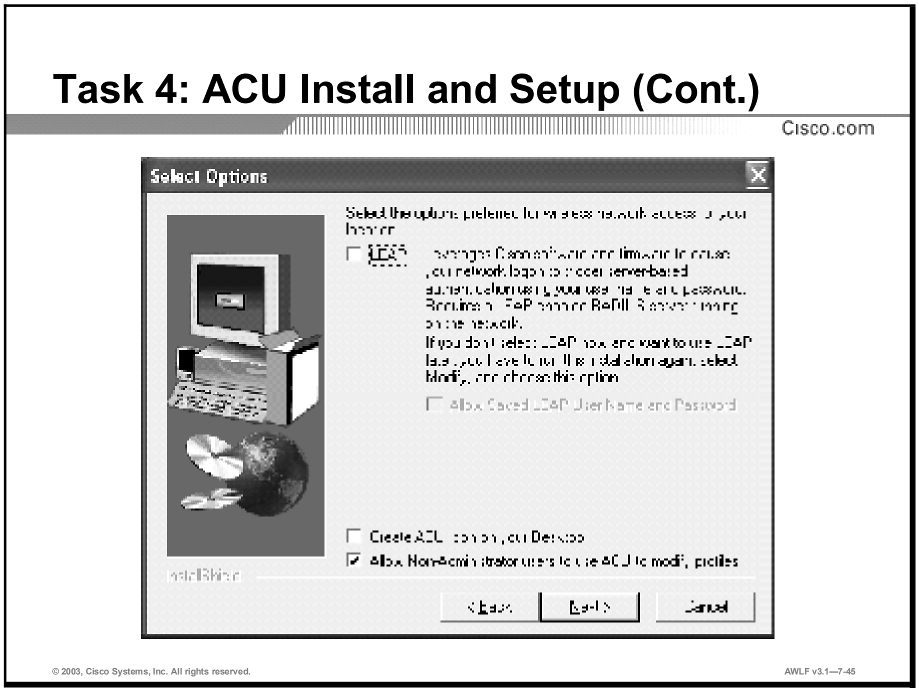
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

AWLF v3.1—7-44

The initial installation screen will appear. Click **Next** to begin the installation process.

Visual Objective

This figure shows the Aironet Welcome screen.



Task 4: ACU Install and Setup (Cont.)

Cisco.com

Select Options

Select the options preferred for wireless network access to your location.

☐ LEAP Leverages Cisco network and firmware to ensure your network logon to a user server-based authentication using your user name and password. Requires an EAP-enabled RADIUS server running on the network.
If you don't select LEAP now and want to use LEAP later, you have to run this installation again, select Modify, and choose this option.

☐ Allow Saved LEAP User Name and Password

☐ Create ACU Icon on your Desktop

☑ Allow Non-Administrator users to use ACU to modify profiles

AWLF v3.1—7-45

You will be prompted to select the options preferred for your wireless network.

Insure the box marked **LEAP** is not checked.

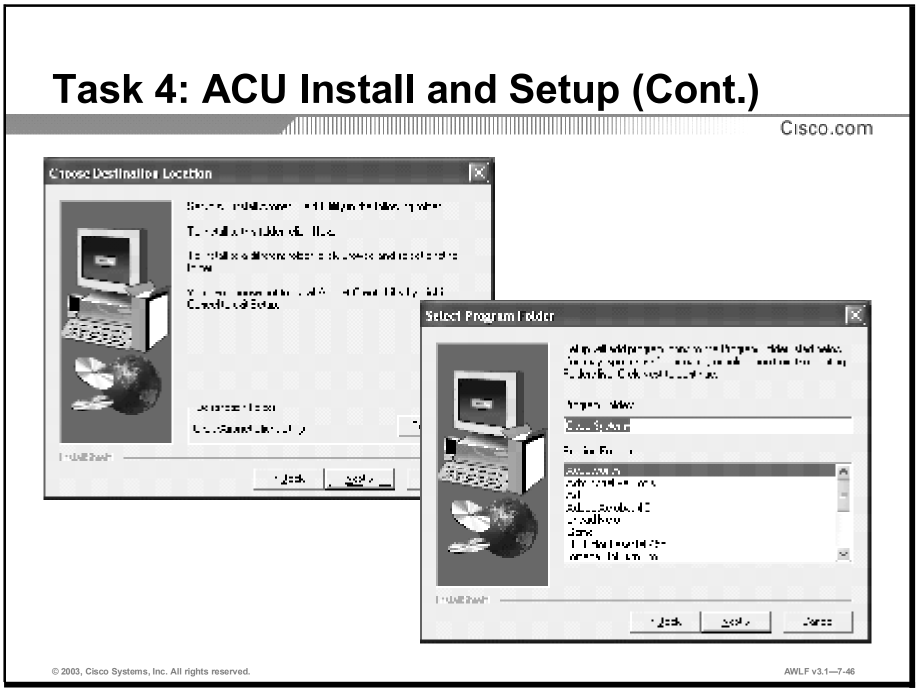
Insure that the box marked **Create ACU Icon on your Desktop** is checked.

Insure the box marked **Allow Non-Administrator users to use ACU to modify profiles** is checked. Click **Next**.

Note	If LEAP or EAP authentication is needed later, the SETUP utility can be run again and modifications can be made without having to uninstall and reinstall the utility.

Visual Objective

This figure shows the Select Options screen.



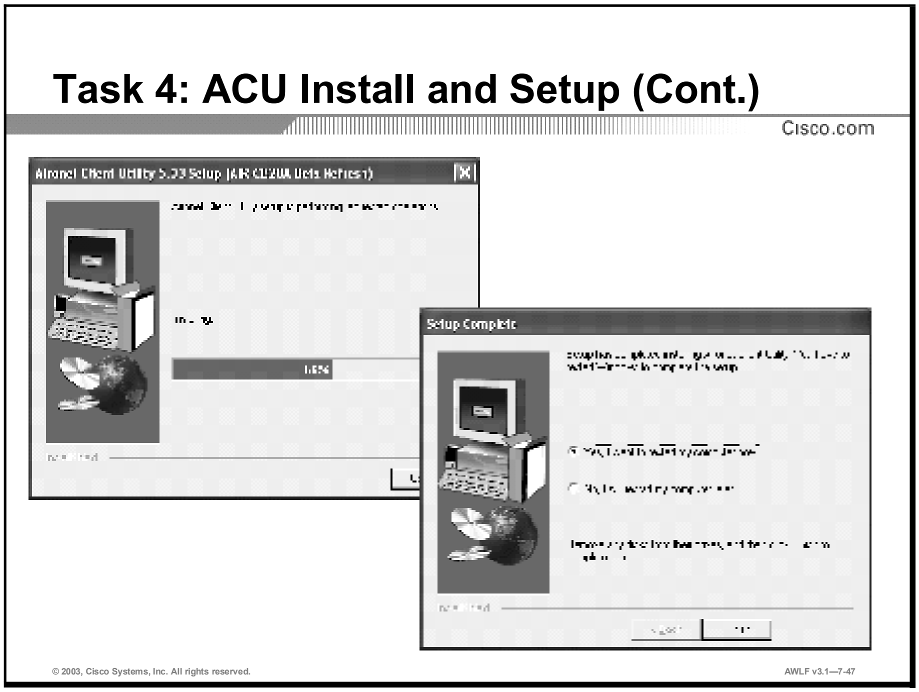
Task 4: ACU Install and Setup (Cont.)

AWLF v3.1—7-46

Choose the local directory where the ACU files will be installed on your laptop. By default this is C:\Program Files\Cisco Aironet\ Aironet Client Utility. **Click Next.**The Setup utility will then prompt you for the location where you want the program icons installed. By default this is the Accessories folder. Click **Next**.

Visual Objective

This figure shows the Aironet Client Choose Destination Location and Select Program Folder window screens.



Task 4: ACU Install and Setup (Cont.)

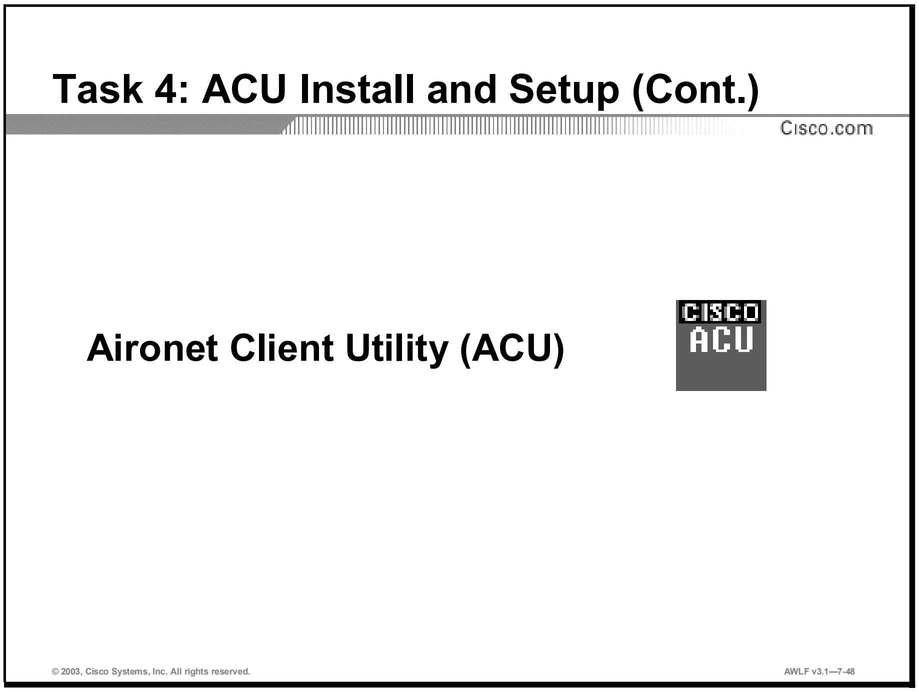
AWLF v3.1—7-47

The SETUP utility will then begin copying files to your hard drive.

Once all files have been installed, the **Setup Complete** screen will be displayed. Click **Finish**.

Visual Objective

This figure shows the Aironet Client Utility Setup screen.



Task 4: ACU Install and Setup (Cont.)

Cisco.com

Aironet Client Utility (ACU)

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—7-48

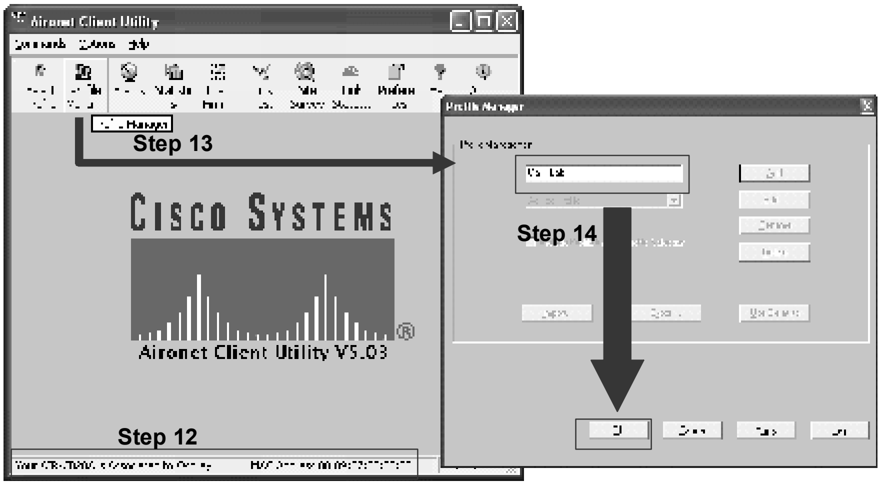
The Utilities are now installed on your PC and you should see the new ACU icon on your desktop.

Visual Objective

This figure shows the ACU icon.

Task 4: ACU Install and Setup (Cont.)

Cisco.com



AWLF v3.1—7-49

Double click on the ACU icon. This should launch the ACU. In the status bar along the bottom of the ACU screen you should see “Your Cisco WLAN Client Card is Associated to XXXX access point”, where XXXX is the name of the access point that your instructor has assigned to the access point. Your instructor will provide you with this information.

You will now need to create a new profile. From the main screen, click the **Profile Manager** button. The Profile Manger screen will appear.

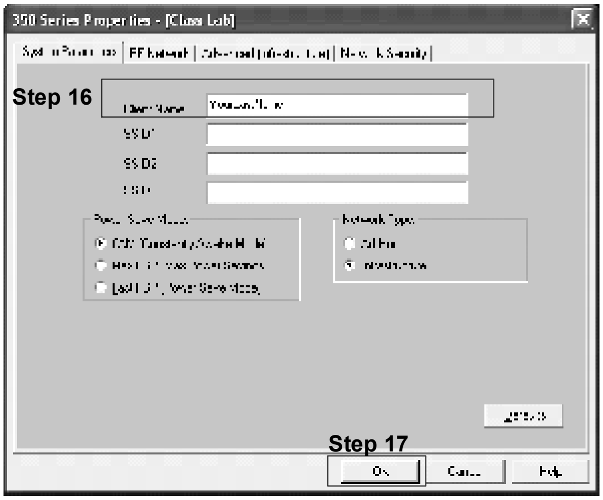
Highlight the word Enterprise in the field. Type in **profile 1** and click **OK**.

Visual Objective

This figure shows the Aironet Client main screen (Step 12), and the Profile Manager screen (Steps 13 and 14).

Task 4: ACU Install and Setup (Cont.)

Cisco.com



350 Series Properties - [Class Lab]

System Parameters | RF Network | Advanced (Infrastructure) | Network Security

Step 16

Client Name: YourLastName

SSID1:

SSID2:

SSID3:

Power Save Mode

● CAM (Constantly Awake Mode)

○ Max PSP (Max Power Savings)

○ Fast PSP (Power Save Mode)

Network Type

○ Ad Hoc

● Infrastructure

Step 17

AWLF v3.1—7-50

The properties for **profile 1** will be displayed.

This screen gives you the ability to change the settings on the card and apply the settings without having to restart the computer (if you went through Network Neighborhood to change the properties, Windows would prompt you for a reboot).

Client Name: Notice that there is no client name. If no client name is entered the device will be identified by IP address on the access point.

If the network you are connecting to uses a Domain Name Service (DNS) server, the client name will be used to identify the device. Simple Network Management Protocol (SNMP) managers may also use this parameter to identify the device.

Enter *your last name* for the **Client Name**.

When you are finished, click **OK** to return to the Profile Manager screen.

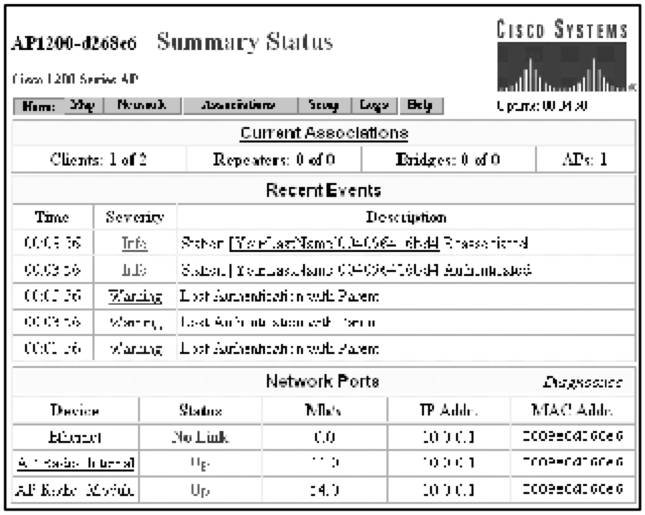
From the Profile Manager screen, click **OK**.

Visual Objective

This figure shows the System Properties for **profile 1**.

Task 4: ACU Install and Setup (Cont.)

Cisco.com



AP1200-d268e6 Summary Status

Cisco 1200 Series AP

Current Associations			
Clients: 1 of 2	Repeaters: 0 of 0	Bridges: 0 of 0	APs: 1

Recent Events

Time	Severity	Description
00:03:56	Info	Station [illegible] Reassociated
00:03:56	Info	Station [illegible] Authenticated
00:02:56	Warning	Lost Authentication with Parent
00:03:56	Warning	Lost Authentication with Parent
00:02:56	Warning	Lost Authentication with Parent

Network Ports — Diagnostics

Device	Status	Mb/s	IP Addr.	MAC Addr.
Ethernet	No Link	0.0	10.0.0.1	[illegible]
AP Radio: Internal	Up	11.0	10.0.0.1	[illegible]
AP Radio: Module	Up	54.0	10.0.0.1	[illegible]

AWLF v3.1—7-51

Launch your web browser and type the address 10.0.0.1 (IP address of the access point) and press **Enter**. This should bring up the home page of the access point.

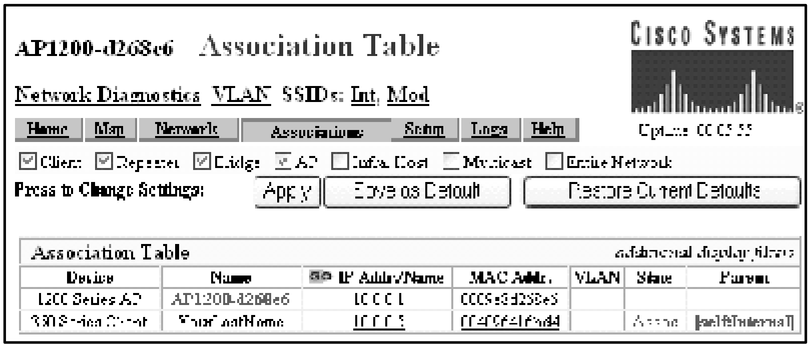
Note If your browser is having trouble connecting to the access point you may be set up to use a proxy server. Disable the proxy server settings and then try connecting to the access point.

Visual Objective

This figure shows the access point Main page.

Task 4: ACU Install and Setup (Cont.)

Cisco.com



AP1200-d268e6 Association Table

Network Diagnostics VLAN SSIDs: Int, Mod

Uptime: 00:05:55

Home
Map
Network
Associations
Setup
Logs
Help
☑ Client ☑ Repeater ☑ Bridge ☑ AP ☐ Infra. Host ☐ Multicast ☐ Entire Network
Press to Change Settings:
Apply
Save as Default
Restore Current Defaults
additional display filters

Association Table

Device	Name	IP Addr/Name	MAC Addr.	VLAN	State	Parent
1200 Series AP	AP1200-d268e6	10.0.0.1	0005e3d268e5			
350 Series Client	YourLastName	10.0.0.5	004096416d44		Assoc	[self]Internal]

AWLF v3.1—7-52

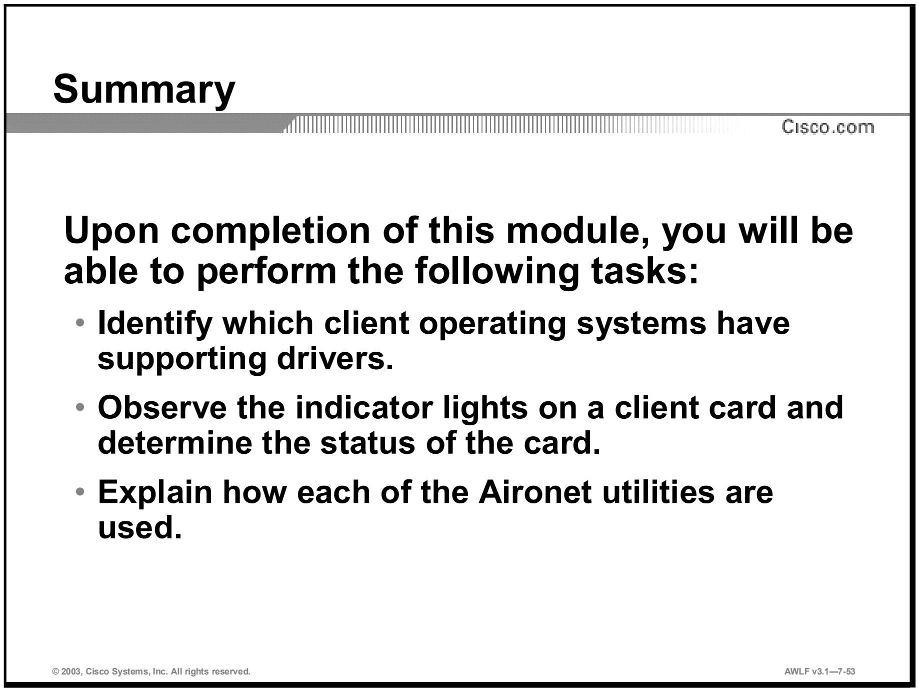
From the main page of the access point, click on the Current Associations link. This will take you to the Associations page. Look through the table and insure that you can identify yourself in the table. You should see yourself listed by the Name that you assigned, as well as by IP address. If you are not in the table, press the F5 key to refresh the page. If you are not listed, read through the exercise again to insure you did not miss a task. If you are still not listed, ask your instructor for assistance.

Visual Objective

This figure shows the access point Association Table page.

Summary

This section summarizes the concepts you learned in this module.



Summary

Upon completion of this module, you will be able to perform the following tasks:

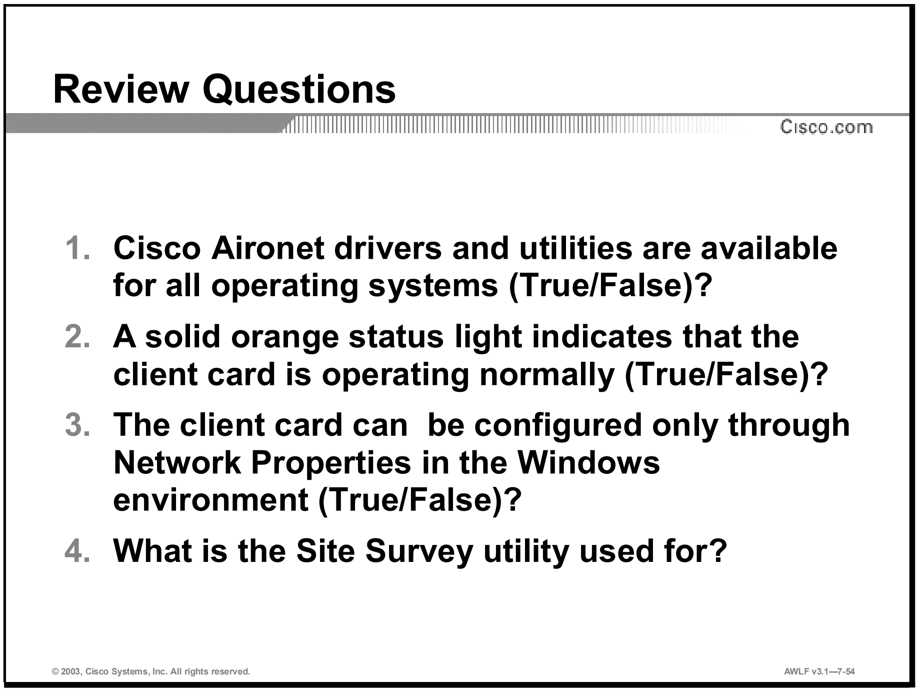
- Identify which client operating systems have supporting drivers.
- Observe the indicator lights on a client card and determine the status of the card.
- Explain how each of the Aironet utilities are used.

AWLF v3.1—7-53

Upon completion of this module, you will be able to perform the following tasks:

- Identify what client operating systems have supporting drivers.
- Observe the indicator lights on a client card and determine the status of the card.
- Explain how each of the Aironet utilities are used.

Review Questions



Review Questions

Cisco.com

1. Cisco Aironet drivers and utilities are available for all operating systems (True/False)?
2. A solid orange status light indicates that the client card is operating normally (True/False)?
3. The client card can be configured only through Network Properties in the Windows environment (True/False)?
4. What is the Site Survey utility used for?

AWLF v3.1—7-54

Answer these review questions.

AWLF

Aironet Wireless LAN Fundamentals

Volume 2

Version 3.1

Student Guide

Text Part Number: 67-1689-01

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia •
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary
India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands
New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia
Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine •
United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Table of Contents

Volume 1

Volume 2

Module 8

Access Point and Bridge Basic Configuration

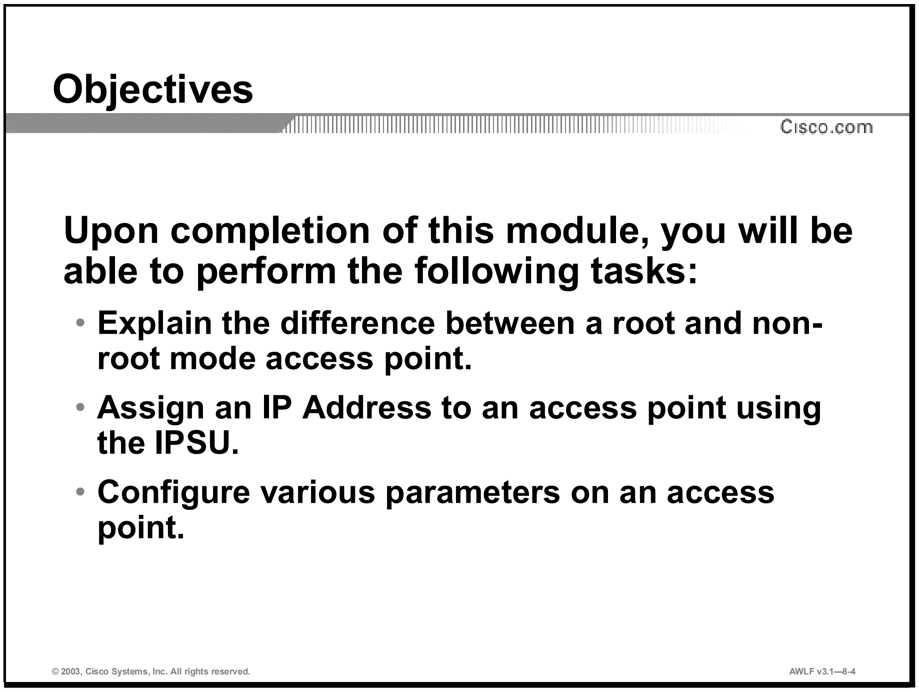
Overview

This module discusses the basic configuration features that may need to be performed on an installed access point. It includes the following topics:

- Objectives
- Access Point LEDs
- Connecting to the Access Point
- Setup of Network Ports
- Statistics
- Setup of Association Parameters and Features
- Cisco Services
- Firmware Upgrade and Distribution
- System Management
- SNMP Setup
- Filtering
- VLAN Configuration
- QoS Configuration
- Cisco Aironet Local Radius Authentication
- Cisco Aironet Proxy Mobile IP
- Cisco Aironet Access Point IOS CLI Interface
- Summary
- Review Questions

Objectives

This section lists the module's objectives.



Objectives

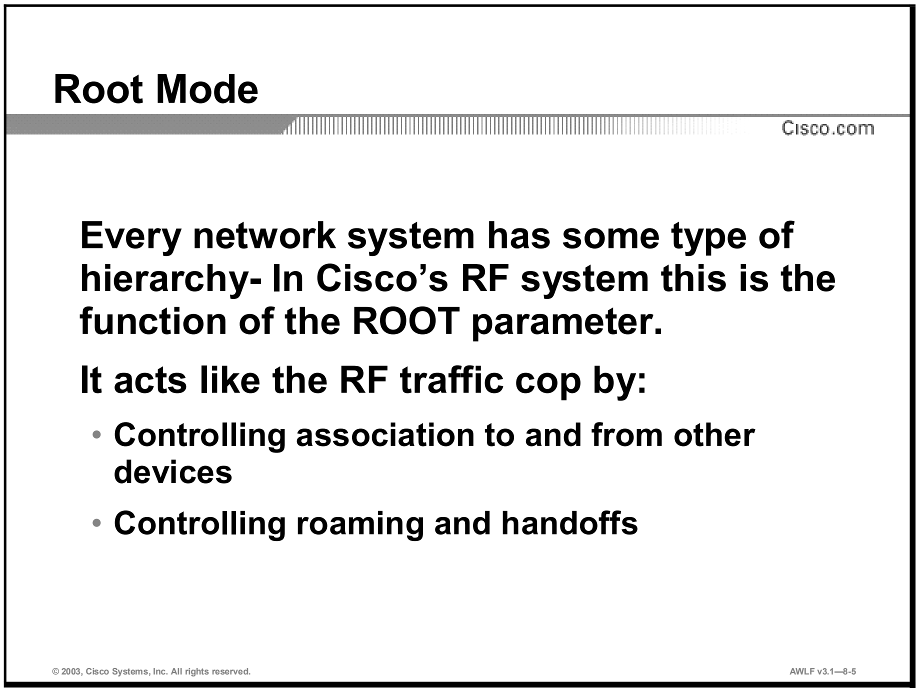
Upon completion of this module, you will be able to perform the following tasks:

- **Explain the difference between a root and non-root mode access point.**
- **Assign an IP Address to an access point using the IPSU.**
- **Configure various parameters on an access point.**

AWLF v3.1—8-4

Upon completion of this module, you will be able to perform the following tasks:

- Explain the difference between a root and non-root mode access point.
- Assign an IP Address to an access point using the IPSU.
- Configure various parameters on an access point.



Root Mode

Every network system has some type of hierarchy- In Cisco's RF system this is the function of the ROOT parameter.

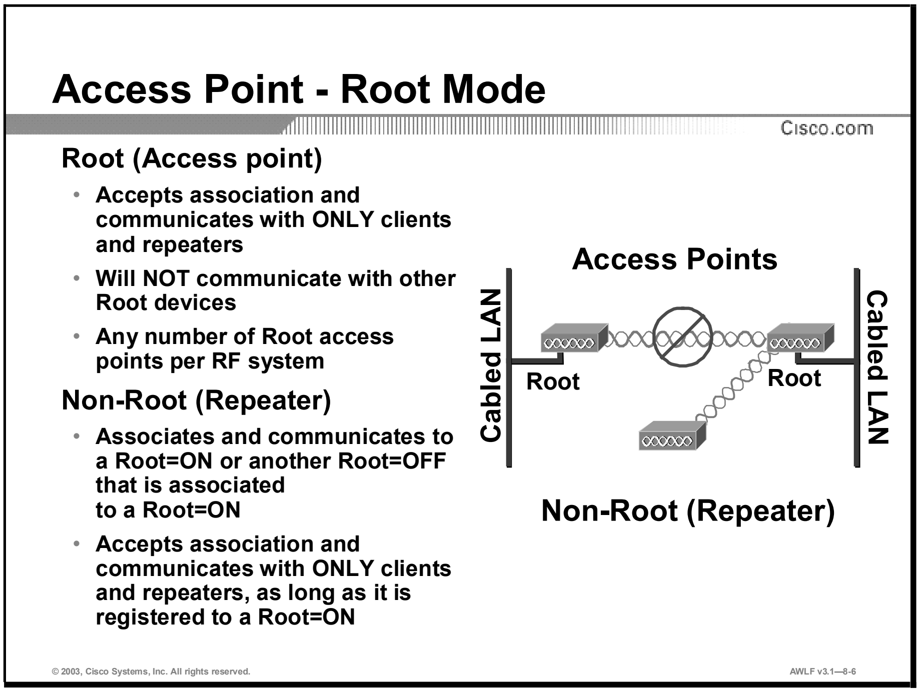
It acts like the RF traffic cop by:

- Controlling association to and from other devices
- Controlling roaming and handoffs

AWLF v3.1—8-5

In the Cisco Aironet Wireless system, the RF network has a hierarchy that starts at the Root unit.

For an access point, the Root unit is attached to the cabled LAN. This is called the Root device. Clients and repeaters associate with the Root. A client may move out of range with the root unit and into range of another root unit. This will cause the old Root unit to drop the client from the association table, and the new access point to the client to its table. The Root is the top of the structure for data flow.



Access Point - Root Mode

Cisco.com

Root (Access point)

- Accepts association and communicates with ONLY clients and repeaters
- Will NOT communicate with other Root devices
- Any number of Root access points per RF system

Non-Root (Repeater)

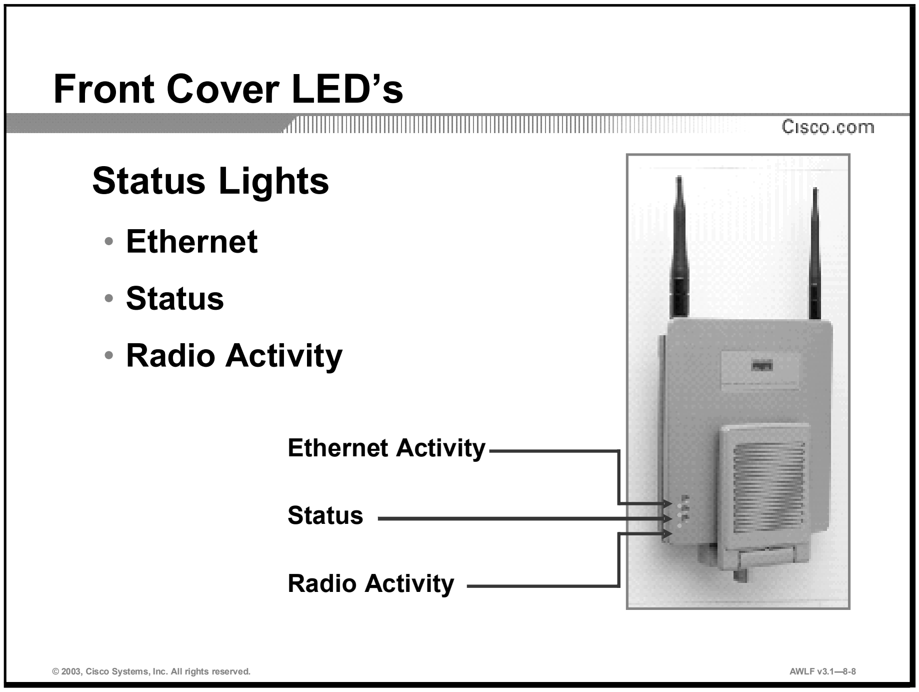
- Associates and communicates to a Root=ON or another Root=OFF that is associated to a Root=ON
- Accepts association and communicates with ONLY clients and repeaters, as long as it is registered to a Root=ON

AWLF v3.1—8-6

All Cisco Aironet® Access Points can be configured as either a root unit (access point mode), or as a Non root unit (repeater mode). Root units cannot communicate with other root units via the RF. They can only communicate over the backbone. Non-root units can communicate with a root unit (known as the parent unit) via the RF, but do not send or receive data via the Ethernet port. Non root units may also communicate with another non root unit via the RF. Non root units will "lock on" to another non root or root unit, and will not stray from this connection unless the connection is lost.

Both root and non-root units can accept associations and communicate with wireless clients via the RF.

Access Point LEDs



Front Cover LED's

Cisco.com

Status Lights

- Ethernet
- Status
- Radio Activity

Ethernet Activity

Status

Radio Activity

AWLF v3.1—8-8

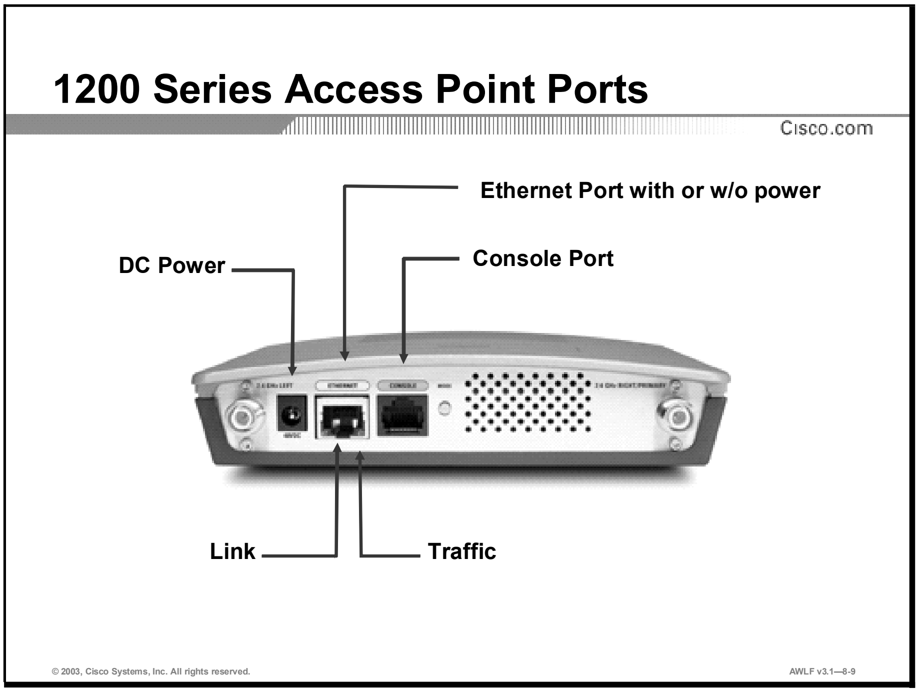
The status light provides updates on the operation of the unit itself. The most important feature of the light is the ability to determine if there are any remote devices communicating with it.

- **Blinking:** No associations
- **Solid:** At least one association

The status light will also flash amber any time the system notes that an error has occurred. This light would prompt you to look into the history logs to form a review of errors that have been reported.

The radio and Ethernet LED indicate activity (TX or RX) over these mediums. Typically the Ethernet will blink much faster than the RF since there will be more traffic on the Ethernet side than the RF side. If the RF LED is blinking much more that the Ethernet, this is an indication there is a lot of radio traffic going on without corresponding Ethernet traffic. This could be from an RF test routine, or from poor communication causing RF retries.

Any RED LED during normal operation indicates a problem, and typically indicates a firmware or hardware failure.



1200 Series Access Point Ports

Ethernet Port with or w/o power

DC Power

Console Port

Link

Traffic

AWLF v3.1—8-9

The 1200 Access Point has the following ports on the top port panel:

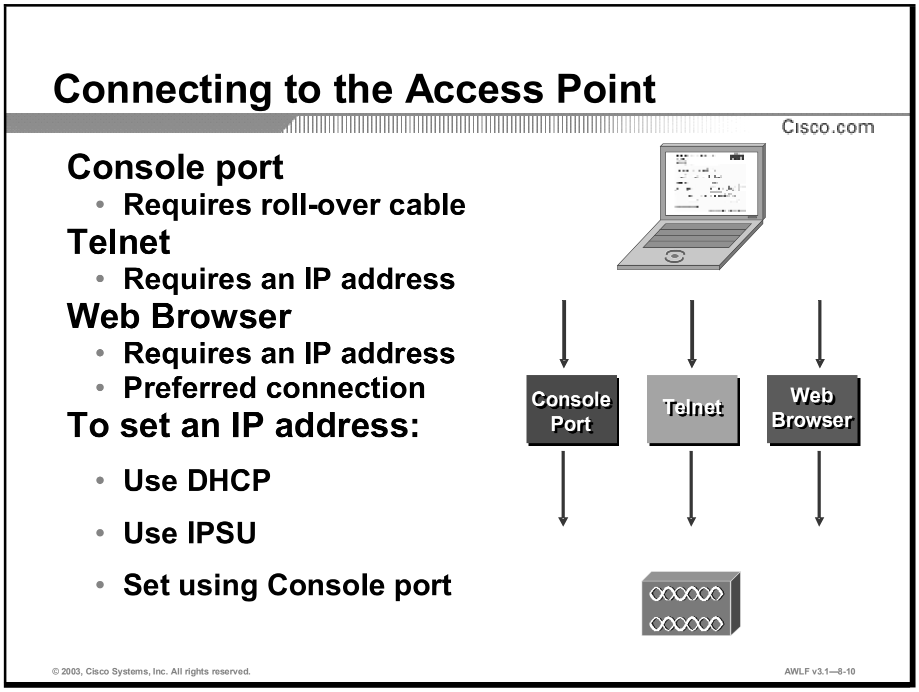
- **Link Light**: Lights solid green to indicate that 10BaseT/100BaseT has been configured as the active port.
- **Traffic**: Flashes green when an Ethernet packet has been received.
- **Console Port**: RJ-45 Console port (rollover cable).

The 1200 Access Point can be powered by its DC power port or by power over Ethernet using an optional power injection module, or using another powered Cisco device (patch panel, switch).

To communicate with the access point via the console port, use a terminal emulation program (such as HyperTerminal) with the following settings:

- 9600 Baud
- 8 Data Bits
- No Parity
- 1 Stop Bit
- Flow Control Xon/Xoff

Connecting to the Access Point



Connecting to the Access Point

Cisco.com

Console port

- **Requires roll-over cable**

Telnet

- **Requires an IP address**

Web Browser

- **Requires an IP address**
- **Preferred connection**

To set an IP address:

- **Use DHCP**
- **Use IPSU**
- **Set using Console port**

Console Port
Telnet
Web Browser

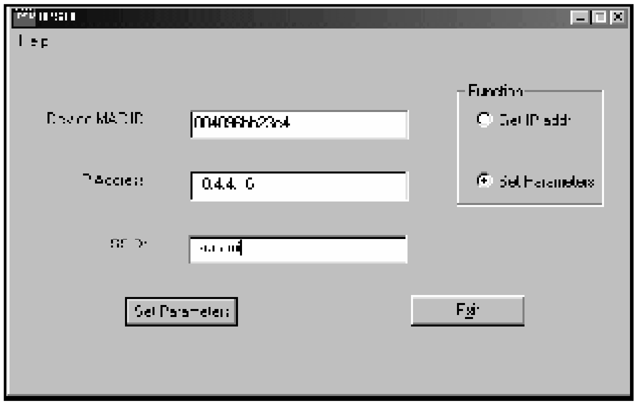
AWLF v3.1—8-10

As designed, manage Cisco Aironet Access Point using a Web browser. Telnet and Serial port menus are much more difficult to utilize.

To set an IP address you can either use DHCP or the Cisco Aironet IP Setup utility (IPSU).

IPSU

Cisco.com



Device MAC ID: 004096bb23c4

IP Address: 0.4.4. 0

SSID: [illegible]

Function

○ Set IP addr

● Set Parameters

Set Parameters

AWLF v3.1—8-11

Make sure that the IPSU is installed on your laptop. You must also have a wireless adapter and an RF connection with the access point on which you want to change the IP address. The IPSU is available as a download from the Cisco website.

Step 1 Double-click the **IPSU** icon on your computer desktop to start IPSU.

Step 2 Make sure **Set Parameters** is selected in the Function box.

Step 3 In the Device MAC ID field, enter the MAC address as it appears on the label on the bottom of the access point. It should contain six pairs of hexadecimal digits separated by periods or dashes.

Step 4 In the IP Address field, enter the IP address you want to assign to the access point. The IP address should be on the same subnet as the device to which you will connect the access point.

Step 5 In the SSID field, enter the SSID you want to assign to the access point.

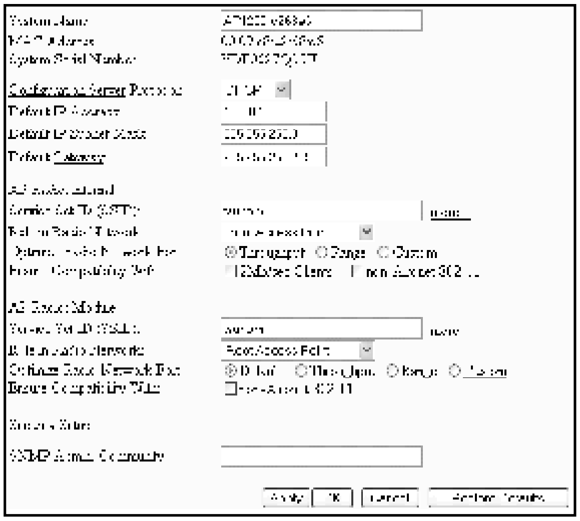
You cannot set the SSID without also setting the IP address. However, you can set the IP address without setting the SSID.

Step 6 Click **Set Parameters**.

IP address is set on the access point. This is best done through a wired Ethernet connection.

Express Setup Menu

Cisco.com



System Name

MAC Address

System Serial Number

Configuration Server Protocol: DHCP

Default IP Address

Default IP Subnet Mask: 255.255.255.0

Default Gateway

AP Radio Internal

Service Set ID (SSID)

Role in Radio Network

Optimize Radio Network For: ● Throughput ○ Range ○ Custom

Ensure Compatibility With: □ 2Mb/sec Clients □ non-Aironet 802.11

AP Radio Module

Service Set ID (SSID)

Role in Radio Network: Root Access Point

Optimize Radio Network For: ● Default ○ Throughput ○ Range ○ Custom

Ensure Compatibility With: □ non-Aironet 802.11

Security Setup

SNMP Admin. Community

AWLF v3.1—8-12

The first time the access point is turned on, this is the default web page for the access point. It will remain the default page until a configuration is successfully applied or click OK.

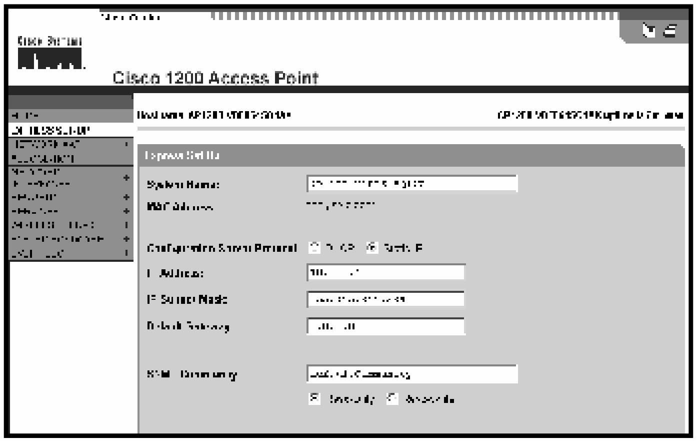
- **System Name:** This is the name of the system that appears in the titles of browser pages.
- **MAC Address:** The Media Access Control address is a unique serial number permanently assigned by the manufacturer.
- **Configuration Server Protocol:** This setting must match the network's method of IP address assignment.
- **IP Address/ IP Subnet Mask/ Gateway Default or IP Address/ Default IP Subnet Mask/ Default Gateway:** These fields allow the assignment or change of the associated addresses of a station, specifically, the "bvi 1" interface for the IOS AP.

AP Radio Internal: (2.4 GHz)

- **Service Set ID (SSID):** A unique identifier that stations must use to be able to communicate with an access point. The SSID can be any alphanumeric entry up to a maximum of 32 characters.
- **Role in Radio Network:** Specifies what role the device will play in the WLAN. Settings available will be dependent upon whether the device is an access point or bridge.
- **Optimize Radio Network For:** This field offers three choices for optimizing the performance of the network. Selecting either throughput or range will maximize either data volume or operating range with a possible trade off of the opposing parameter. Clicking on the Custom link will take you to the access point Radio Hardware page that offers a range of specific parameter settings.
- **Ensure Compatibility:** IEEE 802.11 is the industry wireless networking standard. If your network contains Cisco Aironet 2 Mbps stations, choose **2Mb/sec Clients** to ensure operating compatibility. Choose non-Cisco 802.11 if there are non-Cisco devices (which are be 802.11 compliant) in the network.

Express Setup Menu (Cont.)

Cisco.com



Cisco 1200 Access Point

Express Set-Up

System Name:

MAC Address

Configuration Server Protocol ○ DHCP ● Static IP

IP Address:

IP Subnet Mask

Default Gateway

SNMP Community

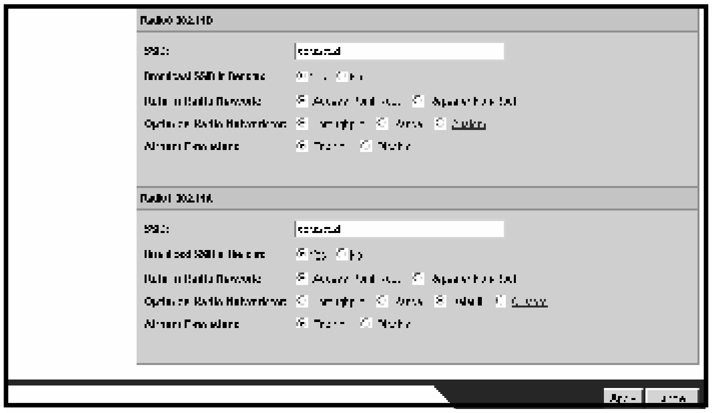
☒ Read-Only ☐ Read-Write

AWLF v3.1—8-13

AP Radio Module: (5 GHz)

- **Service Set ID (SSID):** A unique identifier that stations must use to be able to communicate with an access point. The SSID can be any alphanumeric entry up to a maximum of 32 characters.
- **Role in Radio Network:** Specifies what role the device will play in the WLAN. Settings available will be dependant upon whether the device is an access point or bridge.
- **Optimize Radio Network For:** This field offers three choices for optimizing the performance of the network. Selecting either throughput or range will maximize either data volume or operating range with a possible trade off of the opposing parameter. Clicking on the Custom link will take you to the access point Radio Hardware page that offers a range of specific parameter settings.
- **Aironet Extensions**: This field permits the user the option of disabling Aironet Extensions, which may permit association by some non-Aironet client devices. Also, Aironet Extensions must be enabled in order to enable Cisco Load Balancing and Cisco-specific security options.
- **Security Setup:** Clicking on Security Setup will automatically launch the Access Point’s security configuration page (VxWorks AP only).
- **SNMP Admin Community:** The SNMP community name required by the trap destination before it records traps sent by the device. Clicking on SNMP will automatically launch the Access Point’s SNMP configuration page.

Express Setup



Radio0-802.11B

SSID: [illegible]

Broadcast SSID in Beacon ○ Yes ○ No

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

Optimize Radio Network for ● Throughput ○ Range ○ Custom

Aironet Extensions ● Enable ○ Disable

Radio1-802.11A

SSID: [illegible]

Broadcast SSID in Beacon ● Yes ○ No

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

Optimize Radio Network for ○ Throughput ○ Range ● Default ○ Custom

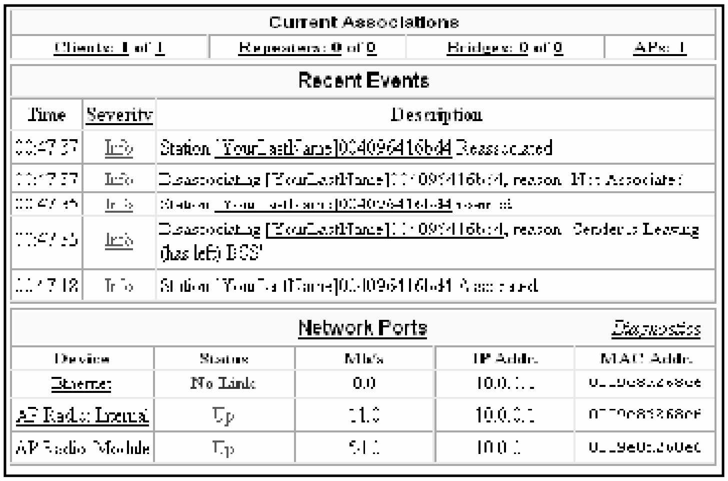
Aironet Extensions ● Enable ○ Disable

The Express Setup page allows the configuration of the AP's basic parameters. These parameters may be set for either of the AP's radio interfaces:

- **SSID**: Configure the primary SSID for use on the specified radio interface
- **Broadcast SSID in Beacon**: Set Yes to send SSID in AP's beacon information, which permits association by "guest" users
- **Role in Radio Network**: Set AP for either Root or Repeater
- **Optimize Radio Network for**: AP's data rates may be set to send broadcast packets at more data rates for "Range" or less data rates for "Throughput". Data rates permitted may also be explicitly configured via "Custom" link.
- **Aironet Extensions**: Enabled or Disabled. Aironet extensions permit function of Cisco client-specific features such as roaming/ load-balancing and security features such as Cisco TKIP and MIC.

Main Menu (Home)

Cisco.com



Current Associations			
Clients: 1 of 1	Repeaters: 0 of 0	Bridges: 0 of 0	APs: 1

Recent Events

Time	Severity	Description
00:47:37	Info	Station [YourLastName]0040964l6bd4 Reassociated
00:47:37	Info	Disassociating [YourLastName]0040964l6bd4, reason "Not Associated"
00:47:45	Info	Station [YourLastName]0040964l6bd4 [illegible]
00:47:45	Info	Disassociating [YourLastName]0040964l6bd4, reason "Sender is Leaving (has left) BSS"
00:47:18	Info	Station [YourLastName]0040964l6bd4 Associated

Network Ports *Diagnostics*

Device	Status	Mb/s	IP Addr.	MAC Addr.
Ethernet	No Link	0.0	10.0.[illegible]	[illegible]
AP Radio: Internal	Up	11.0	10.0.0.1	[illegible]
AP Radio Module	Up	54.0	10.0.[illegible]	[illegible]

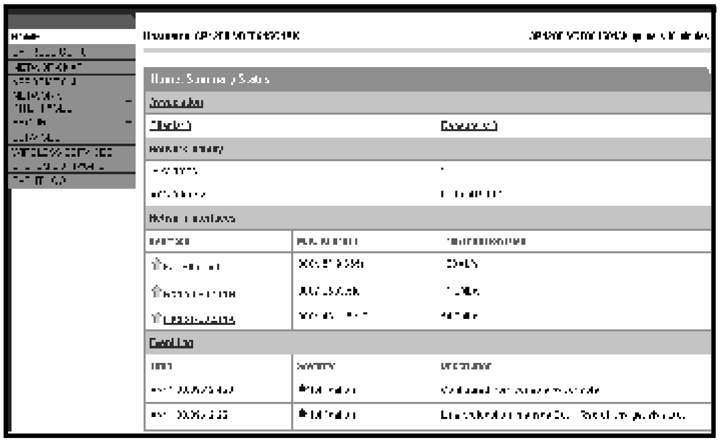
AWLF v3.1—8-15

After the access point has been initially configured the Current Associations table is displayed. This Home page provides a summary of associated stations, system events, as well as port status. Additionally, this page provides many links to pages with detailed information.

- **Ports:** The bottom section of the page shows basic information on access point's network ports. The title line is a link to the Network Ports page that provides more information on data traffic through the ports. Access Point Radio: Internal = 2.4 GHz and Module = 5 GHz.
- **Device:** This column lists the wired and wireless port connections. Each listed device is also a link to the individual port page that provides complete information on port configuration and data statistics.
- **Status:** Displays one of three possible operating states for the port: Up, Down, or Error.
- **Mb/s:** Maximum rate of data transmission in megabits per second. Use the individual Port Hardware page to set data rates [Summary Status > Device/port > Set Properties].
- **IP Address:** Internet protocol address of the device. Use the Express Setup page to assign or change IP address [Summary Status > Setup > Express Setup].
- After the access point has been running, the events area will display the recent events that have taken place.
- **Time:** The first column shows the time of the event expressed in system uptime or wall-clock time. The upper right corner of every page shows either wall-clock time (as configured in Time Server Setup) or the current system uptime expressed in the cumulative number of days, hours, minutes and seconds of operation since startup or reset.
- **Severity:** This column notes the significance of the event. You can link to the Event Log Summary screen to see a tally of events at each security level.
- **Description:** This column is a brief explanation of the event.

Main Menu (Home) (Cont.)

Cisco.com

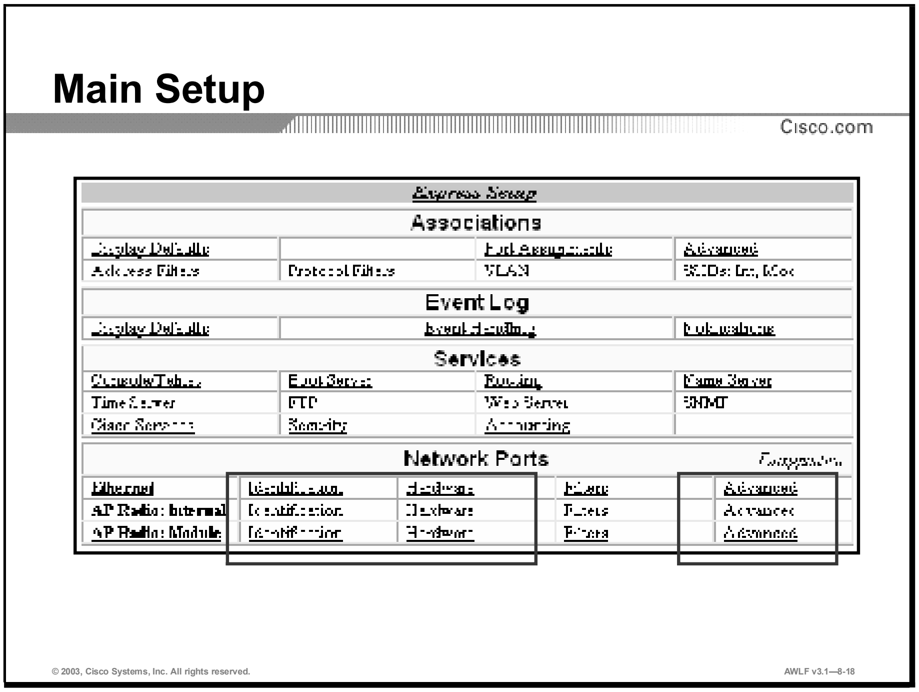


AWLF v3.1—8-16

This Home page on the IOS AP may be returned to at any time via the “HOME” menu tab on the left menu bar. The Home page provides a quick summary of the AP/bridge status.

- **Network Identity:** The section summarizes the configuration of the access point’s “bvi” interface and Ethernet MAC address
- **Network Interfaces:** This section of the page shows basic information on access point’s network interfaces. The title line is a link to the Network Interfaces page that provides more information on data traffic through the ports. Access Point Radio: Radio0-802.11b = 2.4 GHz and Radio1-802.11a = 5 GHz
- **Interface:** Displays current interface status
- **MAC Address:** Displays MAC address of each interface
- **Transmission Rate:** Current interface operational data rate
- **Event Log:** After the access point has been running, the events area will display the recent events that have taken place.
- **Time:** The first column shows the time of the event expressed in system uptime or wall-clock time.
- **Severity:** Indicates the level of each event/alarm that is processed by the AP
- **Description:** Brief description of error/alarm event

Setup of Network Ports



Main Setup

Cisco.com

Express Setup			
Associations			
Display Defaults		Port Assignments	Advanced
Address Filters	Protocol Filters	VLAN	SSIDs: Int, Mod
Event Log			
Display Defaults	Event Handling		Notifications
Services			
Console/Telnet	Boot Server	Routing	Name Server
Time Server	FTP	Web Server	SNMP
Cisco Services	Security	Accounting	

Network Ports					Diagnostics
Ethernet	Identification	Hardware	Filters		Advanced
AP Radio: Internal	Identification	Hardware	Filters		Advanced
AP Radio: Module	Identification	Hardware	Filters		Advanced

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—8-18

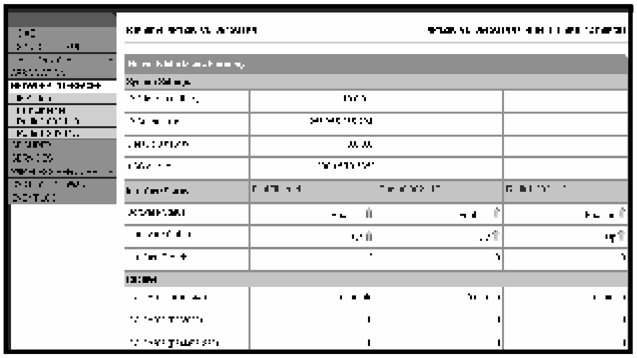
To change the Ethernet and access point radio parameters from the Main Menu, you can access the menus by clicking on the links, as shown above.

Note	**Ethernet = Access** Point’s internal 10/100 Mbps Ethernet card.

Note	**AP Radio: Internal** = Access Point’s internal 2.4 GHz radio.

Note	**AP Radio: Module** = Access Point’s external 5 GHz CardBus radio module.

Network Interfaces



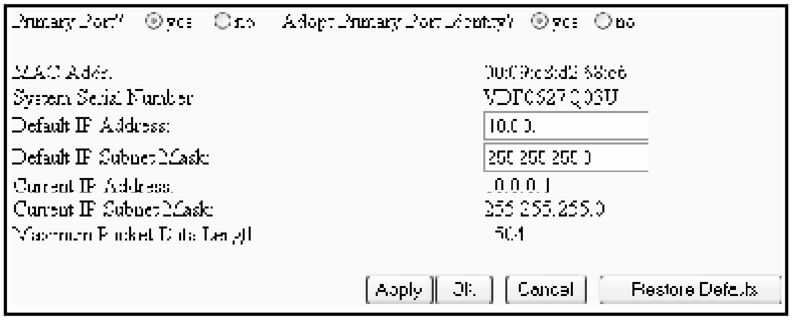
AWLF v3.1—8-19

The IOS AP’s interfaces may be accessed from the “NETWORK INTERFACES” tab on the left menu bar. Statistics and configuration options are available for each of the displayed interfaces. Each interface may be reached either via the left menu bar or the link in the Network Interface summary page.

- **FastEthernet:** Access Point’s integrated 10/100 Mbps Ethernet port
- **Radio0-802.11b:** Access Point’s internal 2.4 GHz PCI radio module.
- **Radio1-802.11a:** Access Point’s external 5 GHz CardBus radio module.

Ethernet Identification

Cisco.com



Primary Port? ● yes ○ no Adopt Primary Port Identity? ● yes ○ no

MAC Addr. 00:09:7c:d2:68:e6
System Serial Number VDF0627Q03U
Default IP Address: 10.0.0.
Default IP Subnet Mask: 255.255.255.0
Current IP Address: 10.0.0.1
Current IP Subnet Mask: 255.255.255.0
Maximum Packet Data Length 1504

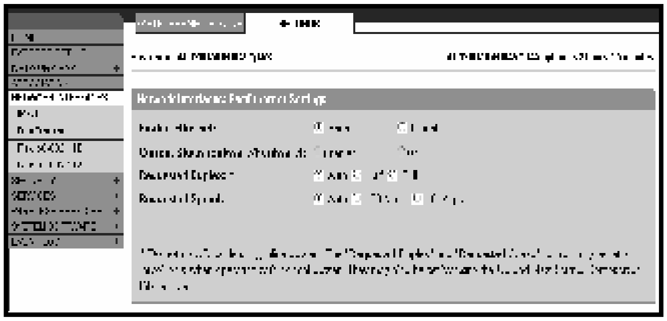
AWLF v3.1—8-20

The Identification page contains the basic location and identification information for the access point radio port. The access point Radio Identification page differs slightly from the Ethernet port in that it manages the connection with the wireless network.

- **Primary Port Selection:** Two sets of yes/no options allow you to designate this port as the primary port of the access point and select whether this port adopts or assumes the identity of the primary port.
- **Primary Port:** Ordinarily, the primary port is the access points Ethernet port which is connected to the wired LAN. The primary port determines the access point's MAC and IP addresses. For this page, which identifies the access point radio port and not the Ethernet port, the normal setting for this question is "No".
- **Adopt Primary Port Identity:** Indicates whether this port adopts the settings of the primary port (MAC and IP addresses). For this page, which identifies the access point radio port, the normal setting is "Yes." Advanced bridge configurations sometimes require a setting of 'NO'.
- **Port Identification:** This section is common to all Identification pages. It displays both default and current identification for MAC Address, IP Address and IP Subnet Mask. Changing a default address on the access point can have very serious consequences including the chance of losing network connectivity or forcing a re-boot of the system. *Note:* Since the access point radio port normally adopts the Ethernet port settings, "Default" values here are generally ignored and "current" settings come from the Ethernet port.

FastEthernet Network Interface

Cisco.com

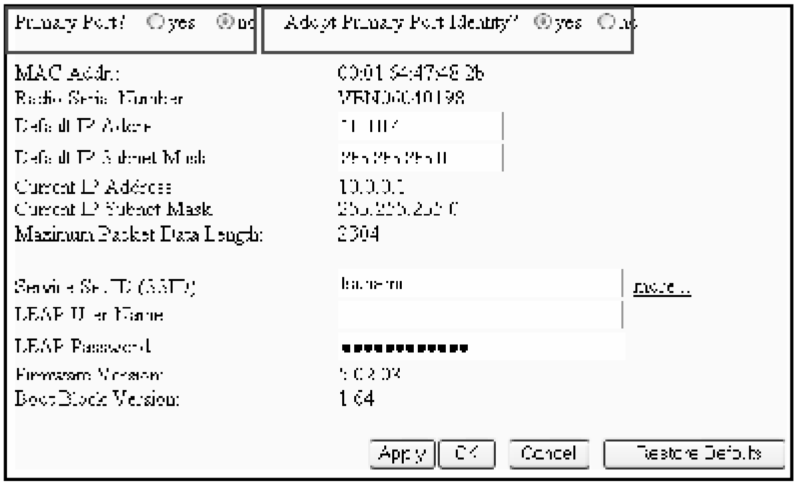


The FastEthernet Network Interface page permits the simple configuration of the access point Ethernet port.

- **Enable Ethernet:** Enable or disable Ethernet port
- **Current Status (Hardware/Software):** Enabled/disabled hardware status and Up/down software status
- **Requested Duplex:** Either "Auto" configured for negotiation with terminating hub/switch or "Half duplex"/ "Full duplex"
- **Requested Speed:** Either "Auto" configured for negotiation with terminating hub/switch or "10 Mbps"/ "100 Mbps"

Access Point Radio: Internal Identification

Cisco.com



Primary Port? ○ yes ● no | Adopt Primary Port Identity? ● yes ○ no

MAC Addr.:	00:01:64:47:48:26
Radio Serial Number	VBN0640198
Default IP Address	[illegible]
Default IP Subnet Mask	255.255.255.0
Current IP Address	10.0.0.1
Current IP Subnet Mask	255.255.255.0
Maximum Packet Data Length:	2304
Service Set ID (SSID)	tsunami
LEAP User Name	
LEAP Password	●●●●●●●●●●●●●
Firmware Version	5.02.03
BootBlock Version:	1.64

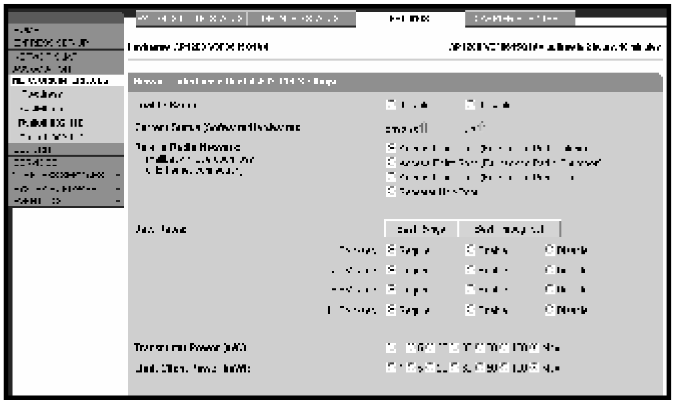
AWLF v3.1—8-22

The Identification page contains the basic location and identification information for the access point 2.4 GHz internal radio port. The access point Radio Identification page differs slightly from the Ethernet port in that it manages the connection with the wireless network.

- **Primary Port Selection:** Two sets of yes/no options allow you to designate this port as the primary port of the access point and select whether this port adopts or assumes the identity of the primary port.
- **Primary Port:** Ordinarily, the primary port is the access point's Ethernet port which is connected to the wired LAN. The primary port determines the access point's MAC and IP addresses. For this page, which identifies the access point radio port and not the Ethernet port, the normal setting for this question is "No".
- **Adopt Primary Port Identity:** Indicates whether this port adopts the settings of the primary port (MAC and IP addresses). For this page which identifies the access point radio port, the normal setting is "Yes." Advanced bridge configurations sometimes require a setting of "NO".
- **Port Identification:** This section is common to all Identification pages. It displays both default and current identification for MAC Address, IP Address and IP Subnet Mask. Changing a default address on the access point can have very serious consequences including the chance of losing network connectivity or forcing a re-boot of the system.

Note Since the access point radio port normally adopts the Ethernet port settings, "Default" values here are generally ignored and "current" settings come from the Ethernet port.

Radio0-802.11B Network Interface

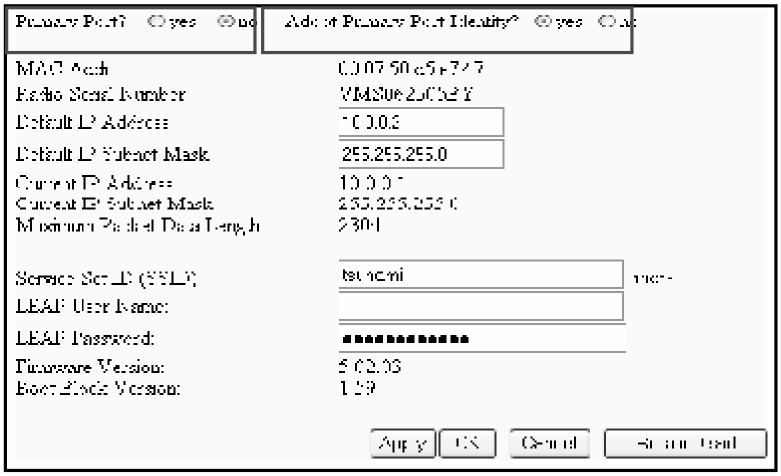


The Network Interface menu for the Radio0-802.11B permits the configuration of specific parameters for the 2.4 GHz radio interface.

- **Enable Radio:** Radio interface may be Enabled or Disabled from the radio buttons.
- **Current Status**: Indicates Software/Hardware status- software status either enabled or disabled, hardware status up or down.
- **Role in Radio Network**: AP may be set as a Root AP or Repeater AP. The “fallback” mechanism for Lost Ethernet may also be modified here.
- **Data Rates**: The data rates supported for this interface may be controlled via this menu. The setting for “Require” configures the data rate at which broadcast 802.11 packets are sent at. “Enable” configures the supported unicast 802.11 packet rates supported. “Disable” turns off the packets transmit at this data rate.
- **Transmitter Power**: The transmit power setting of the AP may be controlled via this parameter.
- **Limit Client Power**: Information may be sent in beacons to control the maximum transmit power for client devices.

Access Point Radio: Module Identification

Cisco.com



Primary Port? ○ yes ● no | Adopt Primary Port Identity? ● yes ○ no

MAC Addr 00:07:50:c5:e7:47
Radio Serial Number VMS0625C52Y
Default IP Address 10.0.0.2
Default IP Subnet Mask 255.255.255.0
Current IP Address 10.0.0.1
Current IP Subnet Mask 255.255.255.0
Maximum Packet Data Length 2304

Service Set ID (SSID) tsunami more...
LEAF User Name:
LEAF Password: ●●●●●●●●●●●●●
Firmware Version: 5.02.03
Boot Block Version: 1.59

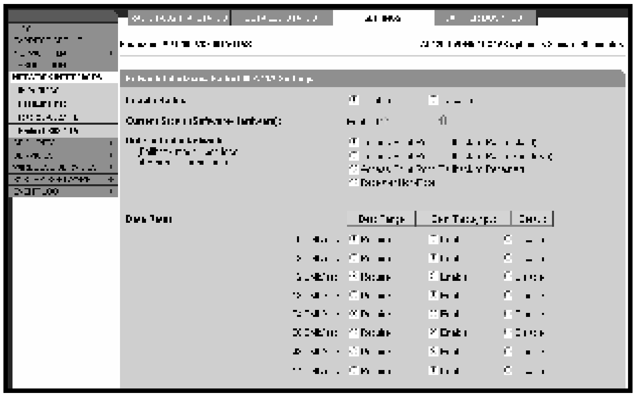
AWLF v3.1—8-24

The Identification page contains the basic location and identification information for the access point 5 GHz module radio port. The access point Radio Identification page differs slightly from the Ethernet port in that it manages the connection with the wireless network.

- **Primary Port Selection:** Two sets of yes/no options allow you to designate this port as the primary port of the access point and select whether this port adopts or assumes the identity of the primary port.
- **Primary Port:** Ordinarily, the primary port is the access point's Ethernet port which is connected to the wired LAN. The primary port determines the access point's MAC and IP addresses. For this page, which identifies the access point radio port and not the Ethernet port, the normal setting for this question is "No".
- **Adopt Primary Port Identity:** Indicates whether this port adopts the settings of the primary port (MAC and IP addresses). For this page which identifies the access point radio port, the normal setting is "Yes." Advanced bridge configurations sometimes require a setting of "NO".
- **Port Identification:** This section is common to all Identification pages. It displays both default and current identification for MAC Address, IP Address and IP Subnet Mask. Changing a default address on the access point can have very serious consequences including the chance of losing network connectivity or forcing a re-boot of the system.

Note Since the access point radio port normally adopts the Ethernet port settings, "Default" values here are generally ignored and "current" settings come from the Ethernet port.

Radio1-802.11A Network Interface

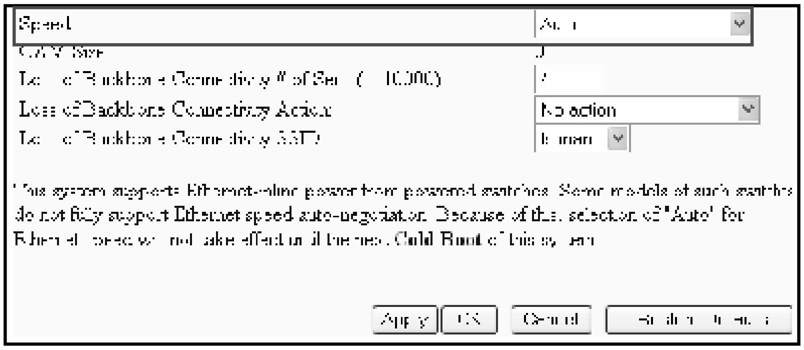


The Network Interface menu for the Radio0-802.11A permits the configuration of specific parameters for the 5 GHz radio interface.

- **Enable Radio:** Radio interface may be Enabled or Disabled from the radio buttons.
- **Current Status**: Indicates Software/Hardware status- software status either enabled or disabled, hardware status up or down.
- **Role in Radio Network**: AP may be set as a Root AP or Repeater AP. The “fallback” mechanism for Lost Ethernet may also be modified here.
- **Data Rates**: The data rates supported for this interface may be controlled via this menu. The setting for “Require” configures the data rate at which broadcast 802.11 packets are sent at. “Enable” configures the supported unicast 802.11 packet rates supported. “Disable” turns off the packets transmit at this data rate.
- **Transmitter Power**: The transmit power setting of the AP may be controlled via this parameter.
- **Limit Client Power**: Information may be sent in beacons to control the maximum transmit power for client devices.

Ethernet Hardware

Cisco.com



Speed: Auto

CWM Size: 0

Loss of Backbone Connectivity # of Sec (- 10,000): [illegible]

Loss of Backbone Connectivity Action: No action

Loss of Backbone Connectivity SSID: [illegible]

This system supports Ethernet-inline power from powered switches. Some models of such switches do not fully support Ethernet speed auto-negotiation. Because of this, selection of "Auto" for Ethernet speed will not take effect until the next Cold Boot of this system.

AWLF v3.1—8-26

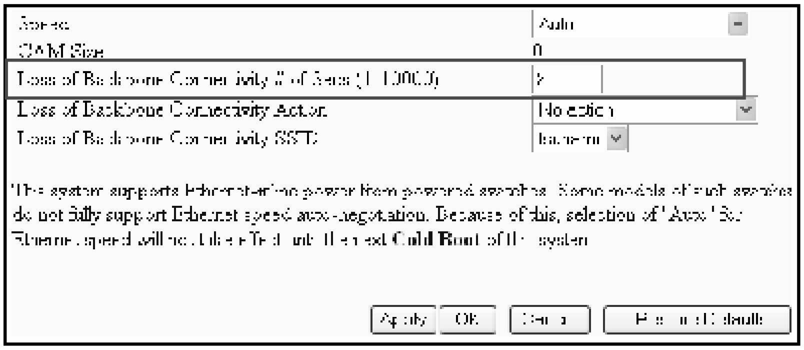
- **Speed:** The Speed drop-down menu lists five options for the type of connector, connection speed, and duplex setting used by the port. The option you select must match the actual connector type, speed, and duplex settings used to link the port with the wired network.
- **Auto:** This is the default and the recommended setting. The connection speed and duplex setting are automatically negotiated between the access point and the hub, switch, or router to which the access point is connected.

Note Some switches with inline power do not fully support Ethernet speed auto-negotiation. If your access point is powered by a switch with inline power, the Auto speed setting is applied only after you reboot the access point.

- 10-Base-T / Half Duplex—Ethernet network connector for 10-Mbps transmission speed over twisted-pair wire and operating in half-duplex mode.
- 10-Base-T / Full Duplex—Ethernet network connector for 10-Mbps transmission speed over twisted-pair wire and operating in full-duplex mode.
- 100-Base-T / Half Duplex—Ethernet network connector for 100-Mbps transmission speed over twisted-pair wire and operating in half-duplex mode.
- 100-Base-T / Full Duplex—Ethernet network connector for 100-Mbps transmission speed over twisted-pair wire and operating in full-duplex mode.

Ethernet Hardware (Cont.)

Cisco.com



Speed	Auto
CAM Size	0
Loss of Backbone Connectivity # of Secs (1-10000)	2
Loss of Backbone Connectivity Action	No action
Loss of Backbone Connectivity SSID	tsunami

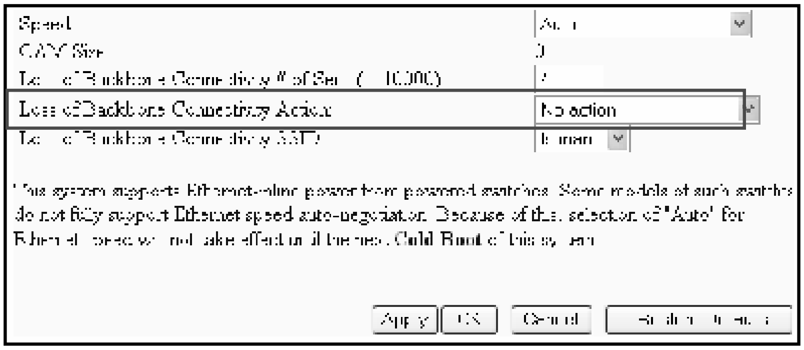
This system supports Ethernet-inline power from powered switches. Some models of such switches do not fully support Ethernet speed auto-negotiation. Because of this, selection of 'Auto' for Ethernet speed will not take effect until the next Cold Boot of the system.

AWLF v3.1—8-27

- **Loss of Backbone Connectivity # of Secs (1-10000):** This setting specifies the amount of time the access point has before taking action when it detects a loss of backbone connectivity (such as a loss of Ethernet link and no active trunks available on its radio). The action the access point takes is specified in the Loss of Backbone Connectivity Action setting, described in the next section.

Ethernet Hardware (Cont.)

Cisco.com



Speed	Auto
CAM Size	0
Loss of Backbone Connectivity # of Sec (1-10000)	[illegible]
Loss of Backbone Connectivity Action	No action
Loss of Backbone Connectivity SSID	[illegible]

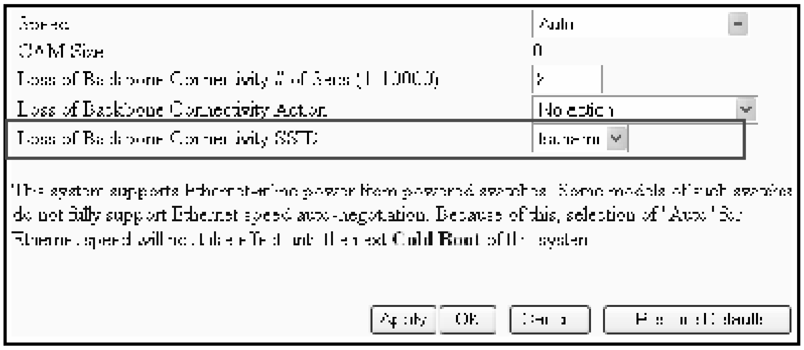
This system supports Ethernet-inline power from powered switches. Some models of such switches do not fully support Ethernet speed auto-negotiation. Because of this, selection of "Auto" for Ethernet speed will not take effect until the next Cold Boot of this system.

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—8-28

- **Loss of Backbone Connectivity Action:** This setting determines what action the access point takes when a loss of backbone connectivity occurs after the time specified in the previous setting. The following actions can be taken:
  - No action—nothing is done.
  - Switch to repeater mode—the access point disassociates all its current clients and becomes a repeater during the period when its backbone connectivity is lost. The access point attempts to communicate with another root access point using the same SSIDs. If it establishes a connection, clients can associate with the root access point through this repeater to maintain connectivity to the backbone LAN. If an appropriate root access point is found, no clients can associate to this access point.
  - Shut the radio off—the access point effectively removes itself from the infrastructure by disassociating its current clients and not allowing further associations until backbone connectivity is restored.
  - Restrict to SSID—the access point disassociates all its current clients and switches to use the SSID configured in the Loss of Backbone Connectivity: SSID setting. After this action is taken, only a client using the specified SSID can associate with the access point, allowing an administrator to perform failure recovery or diagnostic procedures.

Ethernet Hardware (Cont.)



Speed	Auto
CAM Size	0
Loss of Backbone Connectivity # of Secs (1-10000)	2
Loss of Backbone Connectivity Action	No action
Loss of Backbone Connectivity SSID	tsunami

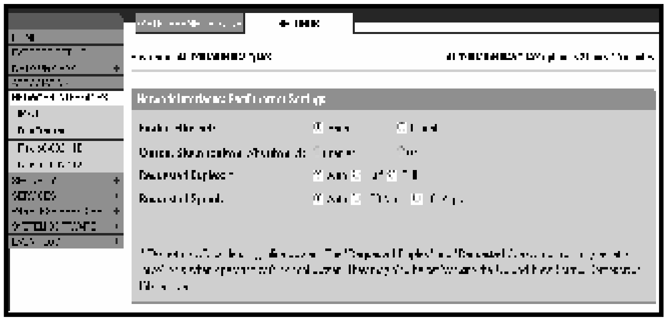
This system supports Ethernet-inline power from powered switches. Some models of such switches do not fully support Ethernet speed auto-negotiation. Because of this, selection of 'Auto' for Ethernet speed will not take effect until the next Cold Boot of the system

AWLF v3.1—8-29

- **Loss of** Backbone **Connectivity SSID:** This setting specifies the SSID used by the access point if the Loss of Backbone Connectivity Action setting is set as Restrict to SSID and backbone connectivity is lost for longer than the time specified in the Loss of Backbone Connectivity: Number of Seconds setting. The setting also defines an administrator-only SSID an administrator uses to communicate with the access point for diagnostic and failure-recovery purposes. If VLANs are active on the access point, the VLAN names are displayed in the Loss of Backbone Connectivity SSID field.

FastEthernet Network Interface

Cisco.com



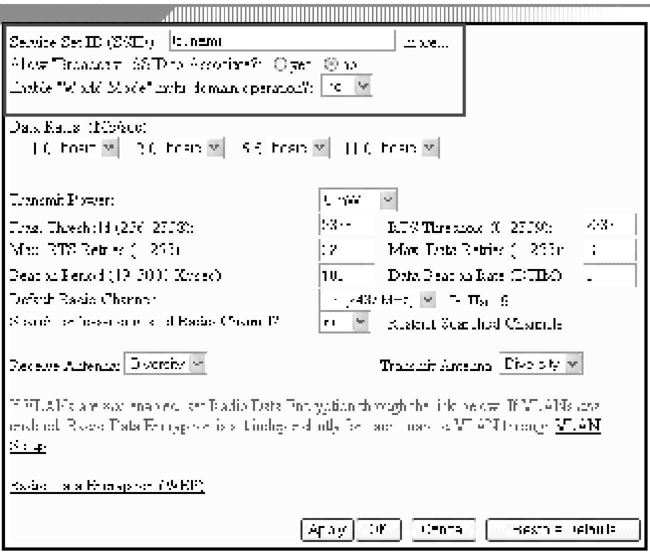
AWLF v3.1—8-30

The FastEthernet Network Interface page permits the simple configuration of the access point Ethernet port.

- **Enable Ethernet:** Enable or disable Ethernet port
- **Current Status (Hardware/Software):** Enabled/disabled hardware status and Up/down software status
- **Requested Duplex:** Either “Auto” configured for negotiation with terminating hub/switch or “Half duplex”/ “Full duplex”
- **Requested Speed:** Either “Auto” configured for negotiation with terminating hub/switch or “10 Mbps”/ “100 Mbps”

Access Point Radio: Internal Hardware

Cisco.com



Service Set ID (SSID): [illegible] more...

Allow "Broadcast" SSID to Associate?: ○ yes ● no

Enable "World Mode" multi-domain operation?: [illegible]

Data Rates (Mb/sec): 1.0 basic 2.0 basic 5.5 basic 11.0 basic

Transmit Power: [illegible]

Frag. Threshold (256-2338): [illegible] RTS Threshold (0-2339): [illegible]

Max. RTS Retries (1-255): [illegible] Max. Data Retries (1-255): [illegible]

Beacon Period (19-5000 Kusec): 100 Data Beacon Rate (DTIM): [illegible]

Default Radio Channel: [illegible] MHz

Search for less-congested Radio Channel?: [illegible] Restrict Searched Channels

Receive Antenna: Diversity Transmit Antenna: Diversity

[illegible] VLAN Setup

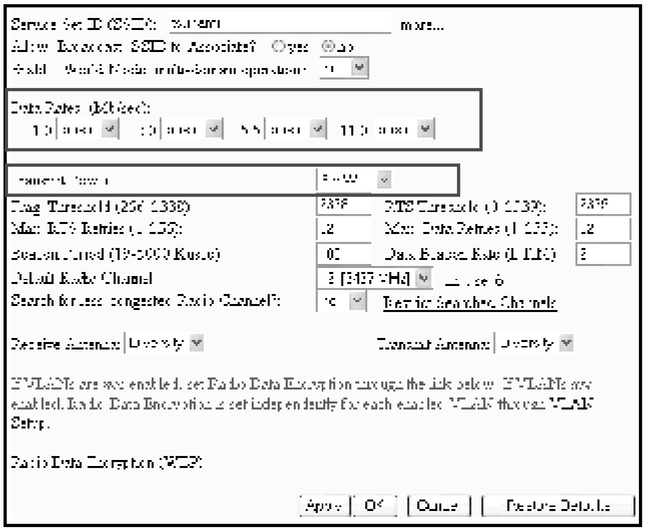
[illegible] Data Encryption (WEP)

AWLF v3.1—8-31

- **Service Set ID (SSID):** An identifier that stations must use to be able to communicate with an access point. Cisco recommends assigning or changing the SSID on the Express Setup page [Summary Status > Setup > Express Setup]. You can enter non-ASCII characters in the SSID by typing a backslash (\ ), a lower-case x, and the characters to represent the non-ASCII character. For example, \xbd inserts the symbol ½. Click more to go to the AP Internal Radio Service Sets page where you can create additional SSIDs. From this page you can also edit an existing SSID or remove one from the system.
- **Allow "Broadcast" SSID to Associate?:** Allows you to choose whether devices that do not specify an SSID (devices that are "broadcasting" in search of an access point to associate with) are allowed to associate with the access point.
  - **Yes:** The default setting allows devices that do not specify an SSID (devices that are "broadcasting" in search of an access point to associate with) to associate with the access point.
  - **No:** Devices that do not specify an SSID (devices that are "broadcasting" in search of an access point to associate with) are *not* allowed to associate with the access point. The SSID used by the client device must match that of the access point.
- **Enable World Mode:** When you select yes from the world-mode pull-down menu, the access point adds channel carrier set information to its beacon. Client devices with world-mode enabled receive the carrier set information and adjust their settings automatically.

Access Point Radio: Internal Hardware (Cont.)

Cisco.com



Service Set ID (SSID): tsunami more...

Allow "Broadcast" SSID to Associate? ○ yes ● no

Enable "World Mode" multi-domain operation: no

Data Rates (Mb/sec): 1.0 basic 2.0 basic 5.5 basic 11.0 basic

Transmit Power: 100 mW

Frag. Threshold (256-2338): 2338 RTS Threshold (0-2339): 2339

Max. RTS Retries (1-128): 32 Max. Data Retries (1-128): 32

Beacon Period (19-5000 Kusec): 100 Data Beacon Rate (1-100): 2

Default Radio Channel: 6 [2437 MHz] In Use: 6

Search for less congested Radio Channel?: no Restrict Searched Channels

Receive Antenna: Diversity Transmit Antenna: Diversity

If VLANs are not enabled, set Radio Data Encryption through the link below. If VLANs are enabled, Radio Data Encryption is set independently for each enabled VLAN through VLAN Setup.

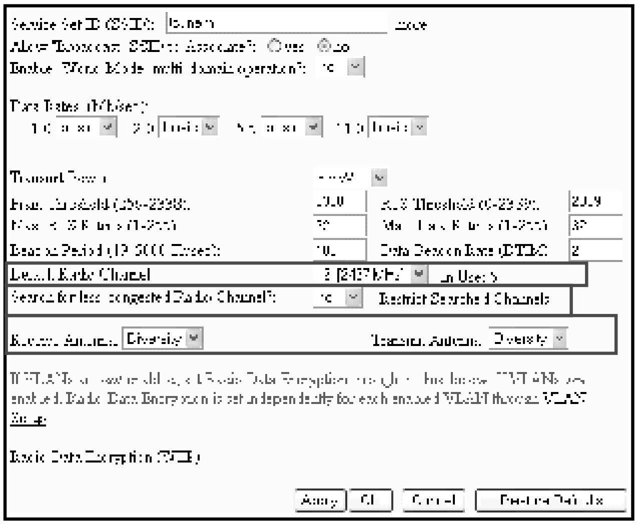
Radio Data Encryption (WEP)

AWLF v3.1—8-32

- **Data Rates:** You use the data rate settings to choose the data rates the access point uses for data transmission. The rates are expressed in megabits per second. The access point always attempts to transmit at the highest rate selected. If there are obstacles or interference, the access point steps down to the highest rate that allows data transmission. For each of four rates (1, 2, 5.5, and 11 megabits per second), a drop-down menu lists three options:
  - Basic (default)—Allows transmission at this rate for all packets, both unicast and multicast. At least one data rate must be set to Basic.
  - Yes—Allows transmission at this rate for unicast packets only.
  - No—Does not allow transmission at this rate.
- The **Optimize Radio Network For** setting on the Express Setup page selects the data rate settings automatically. When you select Optimize Radio Network For Throughput on the Express Setup page, all four data rates are set to basic. When you select Optimize Radio Network For Range on the Express Setup page, the 1.0 data rate is set to basic, and the other data rates are set to Yes.
- **Transmit Power:** This setting determines the power level of radio transmission. To reduce interference or to conserve power, select a lower power setting. The settings in the drop-down menu on 2.4 GHz radios include 1, 5, 20, 50, and 100 milliwatts (mW). Some countries limit the maximum power setting to 50 mW.

Access Point Radio: Internal Hardware (Cont.)

Cisco.com



Service Set ID (SSID): tsunami more

Allow "Broadcast" SSID to Associate? ○ yes ● no

Enable "World Mode" multi-domain operation? no

Data Rates (Mb/sec):

1.0 basic 2.0 basic 5.5 basic 11.0 basic

Transmit Power 100mW

Frag. Threshold (256-2338): 2338 RTS Threshold (0-2339): 2339

Max. RTS Retries (1-255): 32 Max. Data Retries (1-255): 32

Beacon Period (19-5000 Kusec): 100 Data Beacon Rate (DTIM): 2

Default Radio Channel 2 [2417 MHz] In Use: 5

Search for less-congested Radio Channel? no Restrict Searched Channels

Receive Antenna: Diversity Transmit Antenna: Diversity

If VLANs are not enabled, set Radio Data Encryption through the link below. If VLANs are enabled, Radio Data Encryption is set independently for each enabled VLAN through VLAN Setup.

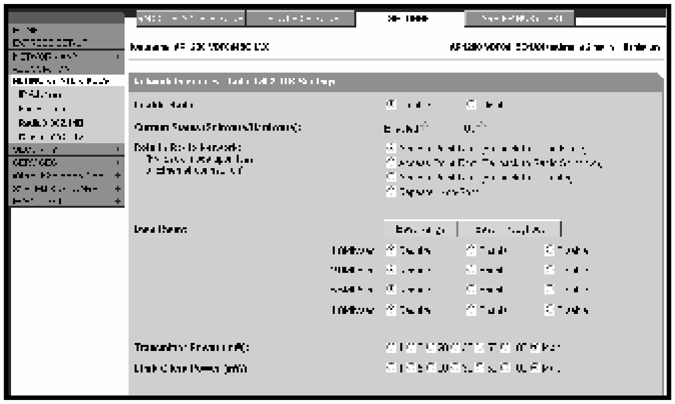
Radio Data Encryption (WEP)

AWLF v3.1—8-33

- **Default Radio Channel:** specifies which channel the access point will use for operation.
- **Search for less-congested Radio Channel?:** Upon applying this setting, or when the access point is restarted, the access point will listen for beacons from other access points and automatically choose the best channel (the channel that will cause least interference with other access points).
- **Restrict Searched Channels:** This screen allows you to limit the channels the Access Point scans when Search for less-congested radio channel is enabled. All the channels in the Access Point's regulatory domain are listed. Click the **Search** check boxes beside the channels to include or exclude channels in the scan for less-congested channels. All the channels are included in the search by default.
- **Receive Antenna / Transmit Antenna:**
  - Diversity-This default setting tells the device to use the antenna that receives the best signal. If your device has two fixed (non-removable) antennas, you should use this setting for both receive and transmit.
  - Right / Primary-If your device has removable antennas and you install a high-gain antenna on the primary connector, you should use this setting for both receive and transmit. When you look at the top panel, the primary antenna is on the right.
  - Left / Secondary-If your device has removable antennas and you install a high-gain antenna on the secondary connector, you should use this setting for both receive and transmit. When you look at the top panel, the secondary antenna is on the left.

Radio0-802.11B Network Interface

Cisco.com



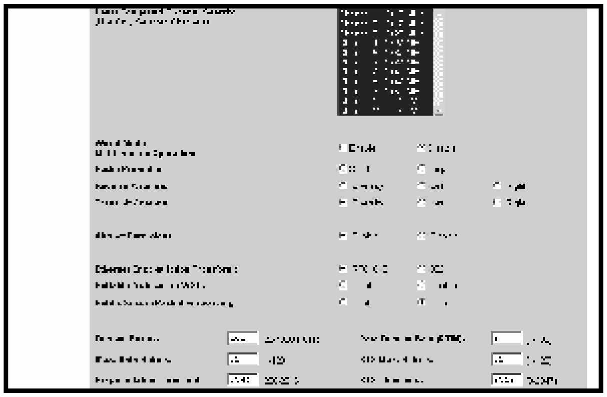
The Network Interface menu for the Radio0-802.11B permits the configuration of specific parameters for the 2.4 GHz radio interface.

- **Role in Radio Network**: AP may be set as a Root AP or Repeater AP. The "fallback" mechanism for Lost Ethernet may also be modified here. AP may be configured for one of the following fallback modes:
- **Fallback to Radio Island-** radio is still activated, clients maintain association, but have not wired network connection
- **Fallback to Radio Shutdown-** radio disabled upon loss of Ethernet
- **Fallback to Repeater-** radio switches to repeater mode upon loss of Ethernet
- **Repeater Non-root-** radio operates in repeater mode- Ethernet disabled
- **Data Rates**: The setting for "Require" configures the data rate at which broadcast 802.11 packets are sent at. "Enable" configures the supported unicast 802.11 packet rates supported. "Disable" turns off the packets transmit at this data rate. The setting for "Best Range" configures broadcast ONLY for 1 Mbps. The setting for "Best Throughput" configures broadcast for all data rates. This permits clients to transmit all packets at their highest possible rate.

Radio0-802.11B Network Interface

Cisco.com

Middle Portion of screen

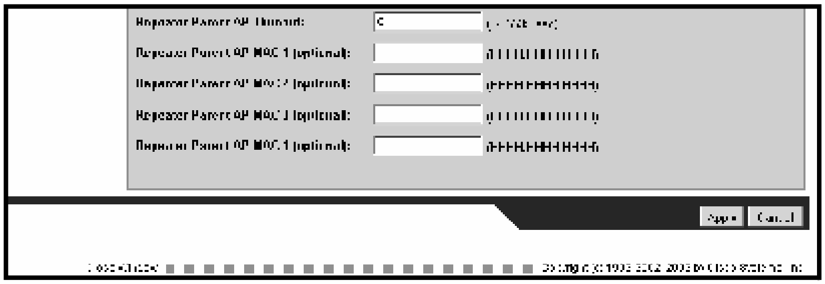


Also on Network Interface screen:

- **Default Radio Channel**: Permits the configuration of an explicit frequency for the AP to utilize or permits the AP to select the “Least Congested Channel” based upon 802.11 activity.
- **Least Congested Channel Search**: Permits the configuration of explicit frequencies for the AP to search when determining frequency to use.
- **World Mode Multi-Domain Operation**: When this feature is enabled, the AP will transmit information in the 802.11 beacons which informs the client devices which frequencies and power are allowable for the AP’s configured regulatory domain.
- **Radio Preamble**: Configure either Long or Short, depending on network device capabilities.
- **Receive Antenna**: Configure either Right/Left/Diversity antennas, depending on requirements and per any special installation
- **Transmit Antenna**: Configure either Right/Left/Diversity antennas, depending on requirements and per any special installation
- **Aironet Extensions**: Enabled or Disabled- enable to allow roaming and Cisco-specific security options
- **Ethernet Encapsulation Transform**: Specify either RFC1042 or 802.1H- 802.1H permits optimal performance with Cisco equipment/ RFC1042 permits optimal interoperability

Radio0-802.11B Network Interface

Lower Portion of Screen



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)

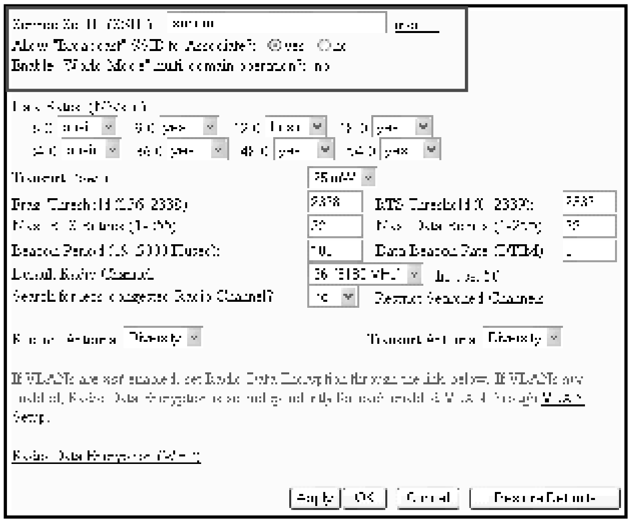
Repeater Parent AP MAC 4 (optional): (HHHH.HHHH.HHHH)

AWLF v3.1—8-36

- **Reliable Multicast to WGB**: If enabled, this parameter requires the acknowledgement of all packets transmit to WGB. Depending on network, this may result in lower aggregate throughput
- **Publicly Secure Packet Forwarding**: If enabled, this parameter prevents communication between clients on a single AP
- **Beacon Period**: This parameter controls the rate at which beacons are transmitted from the AP to the client devices (in milliseconds).
- **Data Beacon Rate (DTIM):** Rate at which Traffic Indicator Map information is sent to clients- indicating buffered data for client
- **Max. Data Retries**: Maximum allowable retries for 802.11 packets
- **RTS Max. Retries**: Maximum allowable retries for messages which are rejected due to packets beyond RTS threshold
- **Fragmentation Threshold**: Maximum allowable size packet prior to fragmenting packet
- **RTS Threshold**: Packet size (and larger) for which RTS messaging is used
- **Repeater Parent AP Timeout:** The parameter allows the configuration of a timeout parameter for which the repeater AP will pause before seeking the “next” AP in it’s list of valid parent AP’s.
- **Repeater Parent AP MAC X:** This parameter allows the assignment and prioritization of “Parent” AP’s for the configured AP to associate to.

Access Point Radio: Module Hardware

Cisco.com



Service Set ID (SSID): [illegible] more

Allow "Broadcast" SSID to Associate?: ● yes ○ no

Enable "World Mode" multi-domain operation?: no

Data Rates (Mb/sec):

6.0 basic 9.0 yes 12.0 basic 18.0 yes

24.0 basic 36.0 yes 48.0 yes 54.0 yes

Transmit Power: 25 mW

Frag. Threshold (256-2338): 2338 RTS Threshold (0-2339): 2339

Max. RTS Retries (1-128): 32 Max. Data Retries (1-128): 32

Beacon Period (19-5000 Kusec): 100 Data Beacon Rate (DTIM): [illegible]

Default Radio Channel: 36 [5180 MHz] In Use: 36

Search for less-congested Radio Channel? no Restrict Searched Channels

Receive Antenna: Diversity Transmit Antenna: Diversity

If VLANs are not enabled, set Radio Data Encryption through the link below. If VLANs are enabled, Radio Data Encryption is set independently for each enabled VLAN through VLAN Setup.

Radio Data Encryption (WEP)

AWLF v3.1—8-37

- **Service Set ID (SSID):** An identifier that stations must use to be able to communicate with an access point. Cisco recommends assigning or changing the SSID on the Express Setup page [Summary **Status > Setup > Express Setup**]. You can enter non-ASCII characters in the SSID by typing a backslash (\ ), a lower-case x, and the characters to represent the non-ASCII character. For example, \xbd inserts the symbol ½. Click **more** to go to the AP Internal Radio Service Sets page where you can create additional SSIDs. From this page you can also edit an existing SSID or remove one from the system.

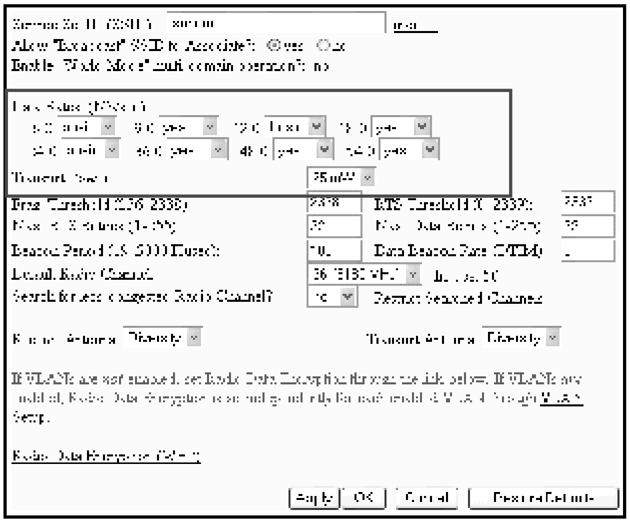
- **Allow "Broadcast" SSID to Associate?:** Allows you to choose whether devices that do not specify an SSID (devices that are "broadcasting" in search of an access point to associate with) are allowed to associate with the access point.

  - **Yes:** The default setting allows devices that do not specify an SSID (devices that are "broadcasting" in search of an access point to associate with) to associate with the access point.

  - **No:** Devices that do not specify an SSID (devices that are "broadcasting" in search of an access point to associate with) are *not* allowed to associate with the access point. The SSID used by the client device must match that of the access point.

- **Enable World Mode:** When you select yes from the world-mode pull-down menu, the access point adds channel carrier set information to its beacon. Client devices with world-mode enabled receive the carrier set information and adjust their settings automatically. Currently world-mode is not supported on 5 GHz.

Access Point Radio: Module Hardware (Cont.)



Service Set ID (SSID): [illegible]

Allow "Broadcast" SSID to Associate?: ● yes ○ no

Enable "World Mode" multi-domain operation?: no

Data Rates (Mbps):
6.0 basic | 9.0 yes | 12.0 basic | 18.0 yes
24.0 basic | 36.0 yes | 48.0 yes | 54.0 yes

Transmit Power: 25 mW

Frag. Threshold (256-2338): 2338 | RTS Threshold (0-2339): 2339

Max. RTS Retries (1-128): 32 | Max. Data Retries (1-128): 32

Beacon Period (19-5000 Kusec): 100 | Data Beacon Rate (DTIM): 2

Default Radio Channel: 36 5180 MHz | In Use: [illegible]

Search for less congested Radio Channel?: no | Restrict Searched Channels

Receive Antenna: Diversity | Transmit Antenna: Diversity

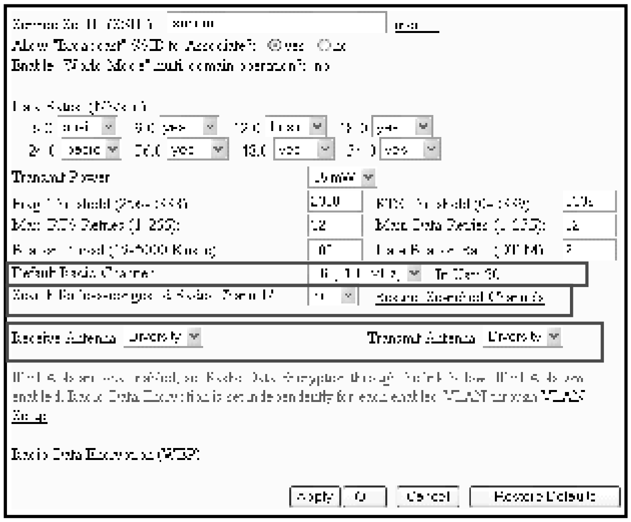
If VLANs are not enabled, set Radio Data Encryption through the link below. If VLANs are enabled, Radio Data Encryption is set independently for each enabled VLAN through VLAN Setup.

Radio Data Encryption (WEP)

- **Data Rates:** You use the data rate settings to choose the data rates the access point uses for data transmission. The rates are expressed in megabits per second. The access point always attempts to transmit at the highest rate selected. If there are obstacles or interference, the access point steps down to the highest rate that allows data transmission. For each of eight rates (6,9,12,18,24,36,48, and 54 megabits per second), a drop-down menu lists three options:
  - Basic (default)—Allows transmission at this rate for all packets, both unicast and multicast. At least one data rate must be set to Basic.
  - Yes—Allows transmission at this rate for unicast packets only.
  - No—Does not allow transmission at this rate.
- The **Optimize Radio Network For** setting on the Express Setup page selects the data rate settings automatically. When you select Optimize Radio Network For Throughput on the Express Setup page, all four data rates are set to basic. When you select Optimize Radio Network For Range on the Express Setup page, the 1.0 data rate is set to basic, and the other data rates are set to Yes.
- **Transmit Power:** This setting determines the power level of radio transmission. To reduce interference or to conserve power, select a lower power setting. The settings in the drop-down menu on 5 GHz Module 5,10,20, and 40 milliwatts.

Access Point Radio: Module Hardware (Cont.)

Cisco.com



Service Set ID (SSID): [illegible]

Allow "Broadcast" SSID to Associate?: ◉ yes ○ no

Enable "World Mode" multi-domain operation?: no

Data Rates (Mb/sec):

6.0 [illegible] 9.0 yes 12.0 [illegible] 18.0 yes

24.0 basic 36.0 yes 48.0 yes 54.0 yes

Transmit Power [illegible] mW

Frag. Threshold (256-2338) 2338 RTS Threshold (0-2339) [illegible]

Max. RTS Retries (1-128): 32 Max. Data Retries (1-128): 32

Beacon Period (19-5000 Kusec) [illegible] Data Beacon Rate (DTIM) 2

Default Radio Channel [illegible] In Use: [illegible]

Search for less-congested Radio Channel? [illegible] Restrict Searched Channels

Receive Antenna Diversity Transmit Antenna Diversity

If VLANs are not enabled, set Radio Data Encryption through the link below. If VLANs are enabled, Radio Data Encryption is set independently for each enabled VLAN through VLAN Setup.

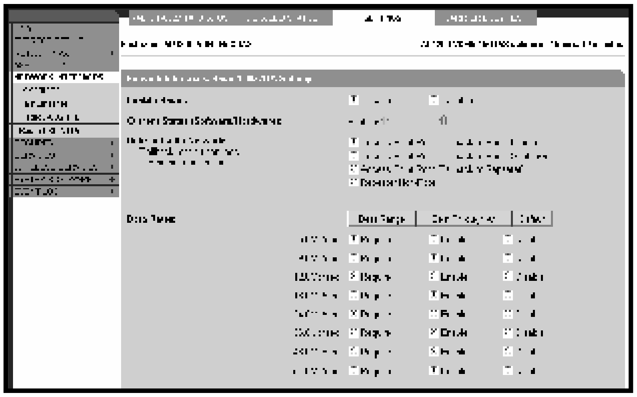
Radio Data Encryption (WEP)

AWLF v3.1—8-39

- **Default Radio Channel:** specifies which channel the access point will use for operation.
- **Search for less-congested Radio Channel?:** Upon applying this setting, or when the access point is restarted, the access point will listen for beacons from other access points and automatically choose the best channel (the channel that will cause least interference with other access points).
- **Restrict Searched Channels:** This screen allows you to limit the channels the Access Point scans when Search for less-congested radio channel is enabled. All the channels in the Access Point's regulatory domain are listed. Click the **Search** check boxes beside the channels to include or exclude channels in the scan for less-congested channels. All the channels are included in the search by default.
- **Receive Antenna / Transmit Antenna:** The FCC requires 5 GHz access point using UNI-1 and UNII-2 bands to use a fixed antenna. Since external antennas can not be attached to the 5 GHz radio module, both ***Receive Antenna and Transmit Antenna need to be set to Diversity***. The 1200 Series Access Points 5 GHz radio module contains two diversity antennas. 1). 6 dBi diversity patch antenna in the wall mount position. 2). 5 dBi omni-directional antenna in the ceiling mount position.

Radio1-802.11A Network Interface

Cisco.com



AWLF v3.1—8-40

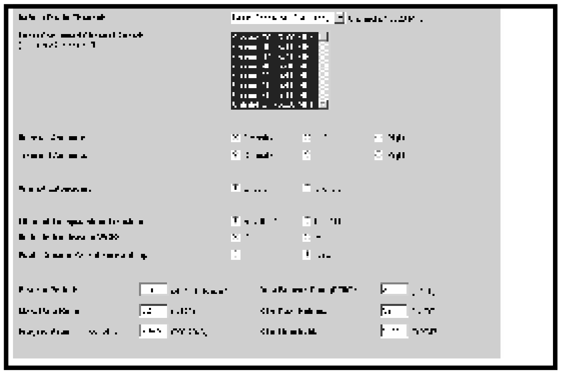
The Network Interface menu for the Radio0-802.11A permits the configuration of specific parameters for the 5 GHz radio interface.

- **Role in Radio Network**: AP may be set as a Root AP or Repeater AP. The “fallback” mechanism for Lost Ethernet may also be modified here. AP may be configured for one of the following fallback modes:
  - **Fallback to Radio Island-** radio is still activated, clients maintain association, but have not wired network connection
  - **Fallback to Radio Shutdown-** radio disabled upon loss of ethernet
  - **Fallback to Repeater-** radio switches to repeater mode upon loss of ethernet
  - **Repeater Non-root-** radio operates in repeater mode- ethernet disabled
- **Data Rates**: The setting for “Require” configures the data rate at which broadcast 802.11 packets are sent at. “Enable” configures the supported unicast 802.11 packet rates supported. “Disable” turns off the packets transmit at this data rate. The setting for “Best Range” configures broadcast ONLY for 6 Mbps. The setting for “Best Throughput” configures broadcast for all data rates. This permits clients to transmit all packets at their highest possible rate. Note that “Default” setting is to broadcast at 6, 12, and 24 Mbps.

Radio1-802.11A Network Interface

Cisco.com

Middle Portion of screen



AWLF v3.1—8-41

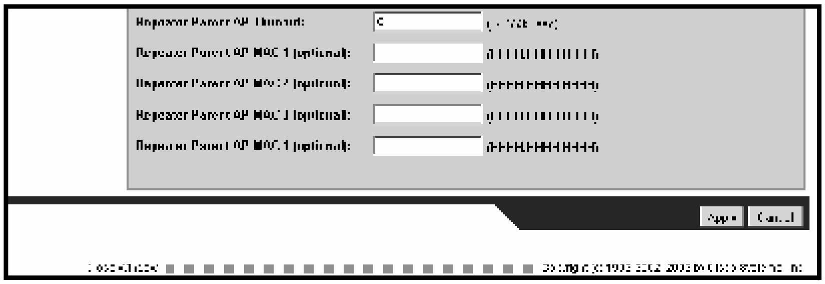
Also on Network Interface screen:

- **Default Radio Channel**: Permits the configuration of an explicit frequency for the AP to utilize or permits the AP to select the “Least Congested Channel” based upon 802.11 activity.
- **Least Congested Channel Search**: Permits the configuration of explicit frequencies for the AP to search when determining frequency to use.
- **Radio Preamble**: Configure either Long or Short, depending on network device capabilities.
- **Receive Antenna**: Configure either Right/Left/Diversity antennas, depending on requirements and per any special installation
- **Transmit Antenna**: Configure either Right/Left/Diversity antennas, depending on requirements and per any special installation
- **Aironet Extensions**: Enabled or Disabled- enable to allow roaming and Cisco-specific security options
- **Ethernet Encapsulation Transform**: Specify either RFC1042 or 802.1H- 802.1H permits optimal performance with Cisco equipment/ RFC1042 permits optimal interoperability

Radio1-802.11A Network Interface

Cisco.com

Lower Portion of Screen



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)

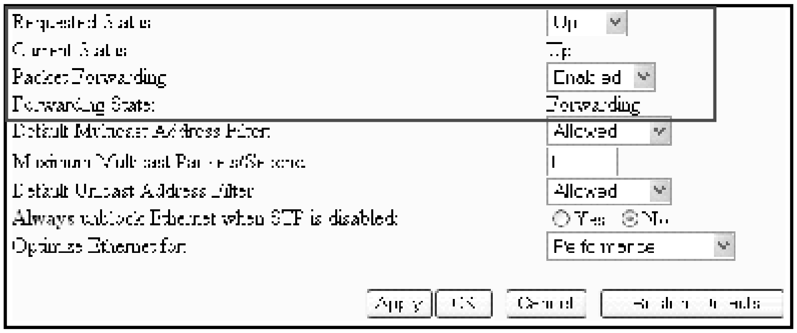
Repeater Parent AP MAC 3 (optional): (HHHH.HHHH.HHHH)

Repeater Parent AP MAC 4 (optional): (HHHH.HHHH.HHHH)

- **Reliable Multicast to WGB**: If enabled, this parameter requires the acknowledgement of all packets transmit to WGB. Depending on network, this may result in lower aggregate throughput
- **Publicly Secure Packet Forwarding**: If enabled, this parameter prevents communication between clients on a single AP
- **Beacon Period**: This parameter controls the rate at which beacons are transmitted from the AP to the client devices. (in milliseconds)
- **Data Beacon Rate (DTIM):** Rate at which Traffic Indicator Map information is sent to clients- indicating buffered data for client
- **Max. Data Retries**: Maximum allowable retries for 802.11 packets
- **RTS Max. Retries**: Maximum allowable retries for messages which are rejected due to packets beyond RTS threshold
- **Fragmentation Threshold**: Maximum allowable size packet prior to fragmenting packet
- **RTS Threshold**: Packet size (and larger) for which RTS messaging is used
- **Repeater Parent AP Timeout:** The parameter allows the configuration of a timeout parameter for which the repeater AP will pause before seeking the “next” AP in it’s list of valid parent AP’s.
- **Repeater Parent AP MAC X:** This parameter allows the assignment and prioritization of “Parent” AP’s for the configured AP to associate to.

Ethernet Advanced

Cisco.com



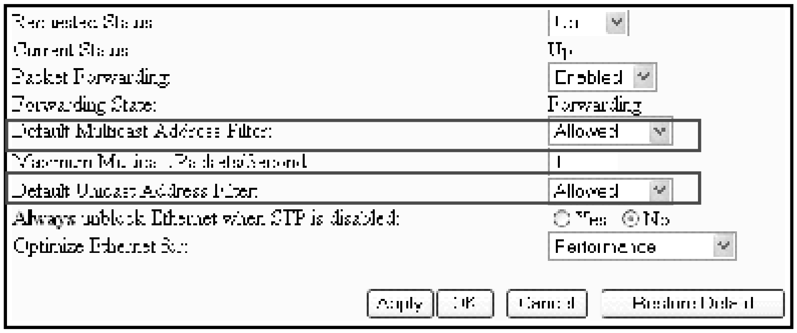
Requested Status:	Up
Current Status:	Up
Packet Forwarding:	Enabled
Forwarding State:	Forwarding
Default Multicast Address Filter:	Allowed
Maximum Multicast Packets/Second:	1
Default Unicast Address Filter:	Allowed
Always unblock Ethernet when STP is disabled:	○ Yes ● No
Optimize Ethernet for:	Performance

AWLF v3.1—8-43

- **Requested Status:** This setting is useful for troubleshooting problems on your network. Up, the default setting, enables the Ethernet port for normal operation. Down disables the access point's Ethernet port. The Current Status line under the setting displays the current status of the Ethernet port. This field can also display Error, meaning the port is in an error condition.
- **Packet Forwarding:** This setting is always set to Enabled for normal operation. For troubleshooting, you might want to set packet forwarding to Disabled, which prevents data from moving between the Ethernet and the radio. The Forwarding State line under the setting displays the current forwarding state. The state for normal operation is Forwarding. Four other settings are possible:
  - **Unknown**—The state cannot be determined.
  - **Disabled**—Forwarding capabilities are disabled.
  - **Blocking**—The port is blocking transmission.
  - **Broken**—This state reports an Ethernet port failure.

Ethernet Advanced (Cont.)

Cisco.com



Requested Status: Up

Current Status: Up

Packet Forwarding: Enabled

Forwarding State: Forwarding

Default Multicast Address Filter: Allowed

Maximum Multicast Packets/Second: 0

Default Unicast Address Filter: Allowed

Always unblock Ethernet when STP is disabled: ○ Yes ● No

Optimize Ethernet for: Performance

AWLF v3.1—8-44

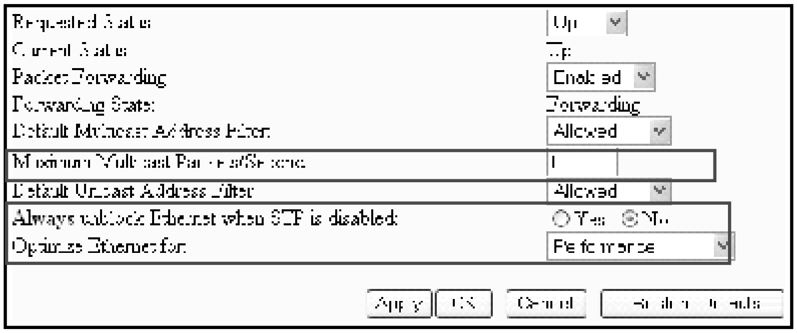
- **Default Unicast and Multicast Address Filter:** MAC address filters allow or disallow the forwarding of unicast and multicast packets sent to specific MAC addresses. You can create a filter that passes traffic to all MAC addresses except those you specify, or you can create a filter that blocks traffic to all MAC addresses except those you specify. Read the "MAC Address Filtering" section for complete instructions on setting up MAC address filters. Unicast packets are addressed to just one device on the network. Multicast packets are addressed to multiple devices on the network. The drop-down menus for unicast and multicast address filters contain two options:
  - **Allowed**—The access point forwards all traffic except packets sent to the MAC addresses listed as disallowed on the Address Filters page.
  - **Disallowed**—The access point discards all traffic except packets sent to the MAC addresses listed as allowed on the Address Filters page.

Note For most configurations, you should leave Default Multicast Address Filter set to Allowed. If you intend to set it to Disallowed, add the broadcast MAC address (ffffffffffff) to the list of allowed addresses on the Address Filters page before changing the setting.

Note If you plan to discard traffic to all MAC addresses except those you specify (the Disallowed setting), be sure to enter your own MAC address as allowed on the Address Filters page.

Ethernet Advanced (Cont.)

Cisco.com



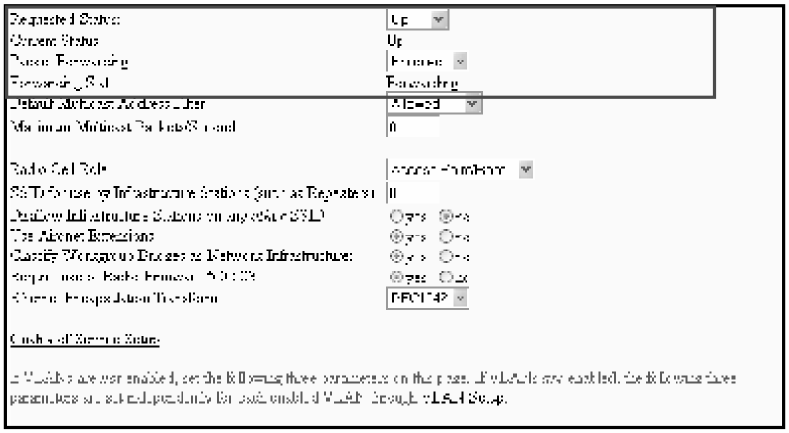
Requested Status	Up
Current Status	Up
Packet Forwarding	Enabled
Forwarding State	Forwarding
Default Multicast Address Filter	Allowed
Maximum Multicast Packets/Second	0
Default Unicast Address Filter	Allowed
Always unblock Ethernet when STP is disabled	○ Yes ● No
Optimize Ethernet for	Performance

AWLF v3.1—8-45

- **Maximum Multicast Packets/Second:** Use this setting to control the number of multicast packets that can pass through the Ethernet port each second. If you enter 0, the access point passes an unlimited number of multicast packets. If you enter a number other than 0, the device passes only that number of multicast packets per second.
- **Always Unblock Ethernet When STP is Disabled:** Use this setting to maintain a bridge link when Spanning Tree Protocol (STP) is disabled. If STP is enabled, select no.
- **Optimize Ethernet for:** Use this setting to specify how you want the Ethernet link to perform. You have two choices: performance and statistics collection. Selecting either results in a compromise. However, on a well-designed network, this compromise is virtually unnoticed.

Access Point Radio: Internal Advanced

Cisco.com



Requested Status:	Up
Current Status	Up
Packet Forwarding	Enabled
Forwarding State	Forwarding
Default Multicast Address Filter	Allowed
Maximum Multicast Packets/Second	0
Radio Cell Role	Access Point/Root
SSID for use by Infrastructure Stations (such as Repeaters)	0
Disallow Infrastructure Stations on any other SSID	○ yes ● no
Use Aironet Extensions	● yes ○ no
Classify Workgroup Bridges as Network Infrastructure:	● yes ○ no
Require use of Radio Firmware 5.00.03	● yes ○ no
Ethernet Encapsulation Transform	RFC1042

Class of Service Setup

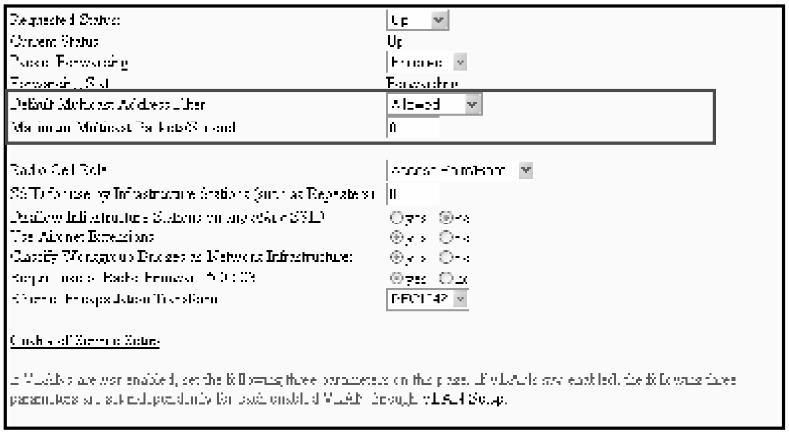
If VLANs are not enabled, set the following three parameters on this page. If VLANs are enabled, the following three parameters are set independently for each enabled VLAN through VLAN Setup.

AWLF v3.1—8-46

- **Requested Status:** This setting is useful for troubleshooting problems on your network. Up, the default setting, turns the radio on for normal operation. Down turns the access point's radio off.
- **Current Status:** The Current Status line under the setting displays the current status of the radio port. This field can also display Error, meaning the port is operating but is in an error condition.
- **Packet Forwarding:** This setting is always set to Enabled for normal operation. For troubleshooting, you might want to set packet forwarding to Disabled, which prevents data from moving between the Ethernet and the radio.
- **Forwarding State:** The Forwarding State line under the setting displays the current forwarding state. For normal access point operation, the forwarding state is Forwarding. Four other states are possible:
  - **Unknown**—The state cannot be determined.
  - **Disabled**—Forwarding capabilities are disabled.
  - **Blocking**—The port is blocking transmission. This is the state when no stations are associated.
  - **Broken**—This state reports radio failure.

Access Point Radio: Internal Advanced (Cont.)

Cisco.com



Requested Status:	Up
Current Status:	Up
Packet Forwarding:	Enabled
Forwarding State:	Forwarding
Default Multicast Address Filter:	Allowed
Maximum Multicast Packets/Second:	0
Radio Cell Role:	Access Point/Root
SSID for use by Infrastructure Stations (such as Repeaters):	
Disallow Infrastructure Stations on any other SSID:	○ yes ● no
Use Aironet Extensions:	● yes ○ no
Classify Workgroup Bridges as Network Infrastructure:	● yes ○ no
Require use of Radio Firmware [illegible]:	● yes ○ no
Ethernet Encapsulation Transform:	RFC1042

[illegible]

If VLANs are not enabled, set the following three parameters on this page. If VLANs are enabled, the following three parameters are set independently for each enabled VLAN through VLAN Setup.

AWLF v3.1—8-47

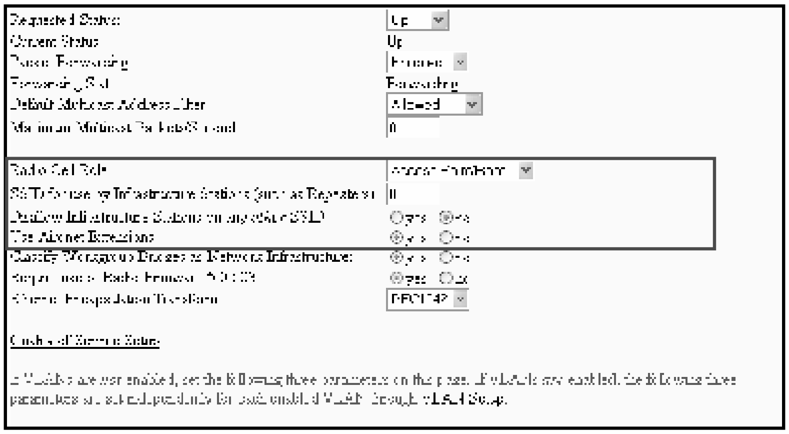
- **Default Multicast Address Filters:** MAC address filters allow or disallow the forwarding of multicast packets sent to specific MAC addresses. You can create a filter that passes traffic to all MAC addresses except those you specify, or you can create a filter that blocks traffic to all MAC addresses except those you specify. The drop-down menus for multicast address filters contain two options:
  - Allowed—The access point forwards all traffic except packets sent to the MAC addresses listed as disallowed on the Address Filters page.
  - Disallowed—The access point discards all traffic except packets sent to the MAC addresses listed as allowed on the Address Filters page.

Note If you plan to discard traffic to all MAC addresses except those you specify (the Disallowed setting), be sure to enter your own MAC address as allowed on the Address Filters page.

- **Maximum Multicast Packets/Second:** Use this setting to control the number of multicast packets that can pass through the radio port each second. If you enter 0, the access point passes an unlimited number of multicast packets. If you enter a number other than 0, the device passes only that number of multicast packets per second.

Access Point Radio: Internal Advanced (Cont.)

Cisco.com



Requested Status:	Up
Current Status:	Up
Packet Forwarding:	Enabled
Forwarding State:	Forwarding
Default Multicast Address Filter:	Allowed
Maximum Multicast Packets/Second:	0
Radio Cell Role:	Access Point/Root
SSID for use by Infrastructure Stations (such as Repeaters):	0
Disallow Infrastructure Stations on any other SSID:	○ yes ● no
Use Aironet Extensions:	● yes ○ no
Classify Workgroup Bridges as Network Infrastructure:	● yes ○ no
Require use of Radio Firmware 5.0.1.x:	● yes ○ no
Ethernet Encapsulation Transform:	RFC1042

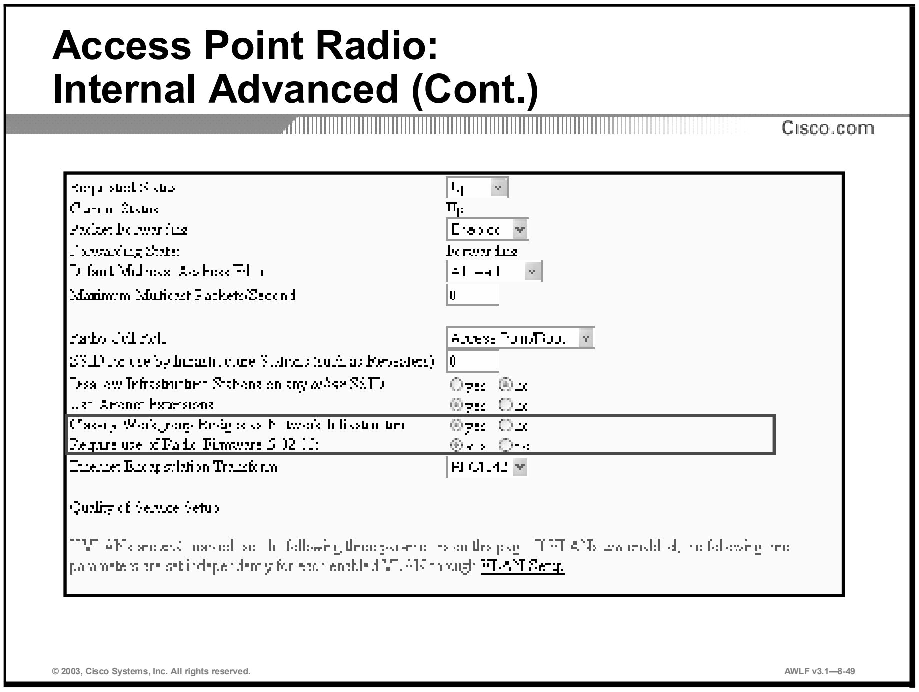
[illegible]

If VLANs are not enabled, set the following three parameters on this page. If VLANs are enabled, the following three parameters are set independently for each enabled VLAN through VLAN Setup.

AWLF v3.1—8-48

- **Radio Cell Role:** This parameter is also located on the Express Setup Menu. Refer to the Express Setup Menu for the definition of this parameter.
- **SSID for use by Infrastructure Stations (such as Repeaters**): This parameter is also located on the Express Setup Menu. Refer to the Express Setup Menu for the definition of this parameter.
- **Disallow Infrastructure Stations on any other SSID:** Prevents repeaters or workgroup bridges from associating to SSIDs other than the infrastructure SSID. The default setting is No, so to invoke this condition, you must change the setting to Yes.
- **Use Aironet Extensions:** Select yes or no to use Cisco Aironet 802.11 extensions. This setting must be set to yes (the default setting) to enable these features:
  - Load balancing
  - Message Integrity Check (MIC)
  - Temporal Key Integrity Protocol (TKIP)

The extensions also improve the access point's ability to understand the capabilities of Cisco Aironet client devices associated with the access point.



Access Point Radio: Internal Advanced (Cont.)

Requested Status	Up
Current Status	Up
Packet Forwarding	Enabled
Forwarding State	Forwarding
Default Multicast Address Filter	Allowed
Maximum Multicast Packets/Second	0
Radio Cell Role	Access Point/Root
SSID for use by Infrastructure Stations (such as Repeaters)	0
Disallow Infrastructure Stations on any other SSID	○ yes ● no
Use Aironet Extensions	● yes ○ no
Classify Workgroup Bridges as Network Infrastructure	● yes ○ no
Require use of Radio Firmware 5.02.10	● yes ○ no
Ethernet Encapsulation Transform	RFC1042

Quality of Service Setup

If VLANs are not enabled, set the following three parameters on this page. If VLANs are enabled, the following three parameters are set independently for each enabled VLAN through VLAN Setup.

AWLF v3.1—8-49

- **Classify Workgroup Bridges as Network Infrastructure:** Select no to allow more than 20 Cisco Aironet Workgroup Bridges to associate to the access point. The default setting, yes, limits the number of workgroup bridges that can associate to the access point to 20 or less.

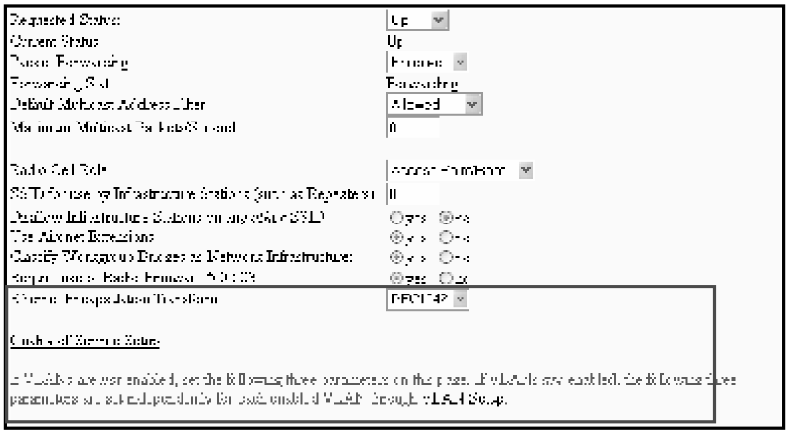
Access points and bridges normally treat workgroup bridges not as client devices but as infrastructure devices, like access points or bridges. Treating a workgroup bridge as an infrastructure device means that the access point reliably delivers multicast packets, including Address Resolution Protocol (ARP) packets, to the workgroup bridge.

Note This feature is best suited for use with stationary workgroup bridges. Mobile workgroup bridges might encounter spots in the access point's coverage area where they do not receive multicast packets and lose communication with the access point even though they are still associated to it.

- **Require Use of Radio Firmware x.xx:** This setting affects the firmware upgrade process when you load new firmware for the access point. Select yes to force the radio firmware to be upgraded to a firmware version compatible with the current version of the management system. Select no to exempt the current radio firmware from firmware upgrades.

Access Point Radio: Internal Advanced (Cont.)

Cisco.com



Requested Status:	Up
Current Status:	Up
Packet Forwarding:	Enabled
Forwarding State:	Forwarding
Default Multicast Address Filter:	Allowed
Maximum Multicast Packets/Second:	0
Radio Cell Role:	Access Point/Root
SSID for use by Infrastructure Stations (such as Repeaters):	0
Disallow Infrastructure Stations on any other SSID:	○ yes ● no
Use Aironet Extensions:	● yes ○ no
Classify Workgroup Bridges as Network Infrastructure:	● yes ○ no
Reject Clients with Radio Firmware < 5.02.09:	● yes ○ no
Ethernet Encapsulation Transform:	RFC1042

Quality of Service Setup

If VLANs are not enabled, set the following three parameters on this page. If VLANs are enabled, the following three parameters are set independently for each enabled VLAN through VLAN Setup.

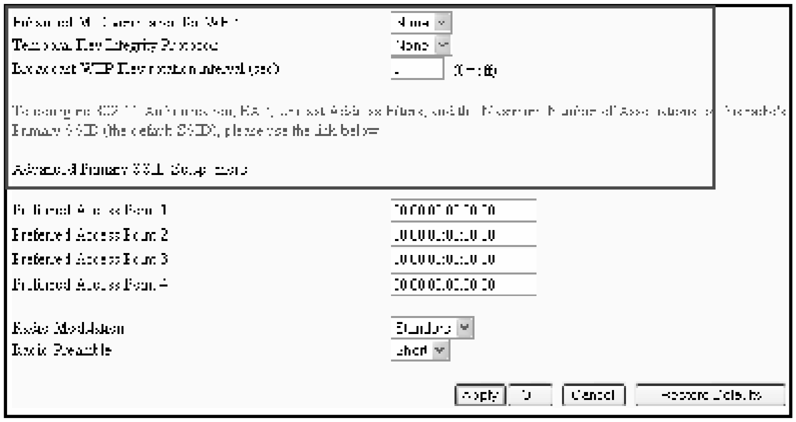
AWLF v3.1—8-50

- **Ethernet Encapsulation Transform:** Choose 802.1H or RFC1042 to set the Ethernet encapsulation type. Data packets that are not 802.2 packets must be formatted to 802.2 using 802.1H or RFC1042. Cisco Aironet equipment uses 802.1H because it provides optimum interoperability.
  - **802.1H**—This default setting provides optimum performance for Cisco Aironet wireless products.
  - **RFC1042**—Use this setting to ensure interoperability with non-Cisco Aironet wireless equipment. RFC1042 does not provide the interoperability advantages of 802.1H but is used by other manufacturers of wireless equipment.
- **Quality of Service Setup Link:** Clicking on the Quality of Service (QoS) Setup link accesses the AP Radio Quality of Service page. Use this page to configure the radio's QoS setup and priorities.
- **VLAN Setup Link:** Clicking the VLAN Setup link accesses the VLAN Setup page. Use this page to configure, add, edit, and remove VLANs associated with your access point.

Access Point Radio: Internal Advanced (Cont.)

Cisco.com

Lower Portion of Screen



Enhanced MIC verification for WEP: None

Temporal Key Integrity Protocol: None

Broadcast WEP Key rotation interval (sec): 0 (0 = off)

To configure 802.11 Authentication, EAP, Unicast Address Filters, and the Maximum Number of Associations of the radio's Primary SSID (the default SSID), please use the link below

Advanced Primary SSID Setup menu

Preferred Access Point 1: 00:00:00:00:00:00

Preferred Access Point 2: 00:00:00:00:00:00

Preferred Access Point 3: 00:00:00:00:00:00

Preferred Access Point 4: 00:00:00:00:00:00

Basic Modulation: Standard

Basic Preamble: Short

AWLF v3.1—8-51

- **Enhanced MIC verification for WEP:** This setting enables Message Integrity Check (MIC), a security feature that protects your WEP keys by preventing attacks on encrypted packets called bit-flip attacks. Select MMH from the drop-down menu and click Apply to enable MIC.
- **Temporal Key Integrity Protocol:** This setting enables the temporal key integrity protocol (TKIP, or WEP key hashing). To enable WEP key hashing, chose CISCO from the drop down menu.
- **Broadcast WEP Key rotation interval (sec):** This option enables broadcast key rotation by setting a key rotation interval. To enable broadcast key rotation, enter the rotation interval in seconds in the Broadcast WEP Key rotation interval entry field. If you enter 900, for example, the access point sends a new broadcast WEP key to all associated client devices every 15 minutes. To disable broadcast WEP key rotation, enter 0.

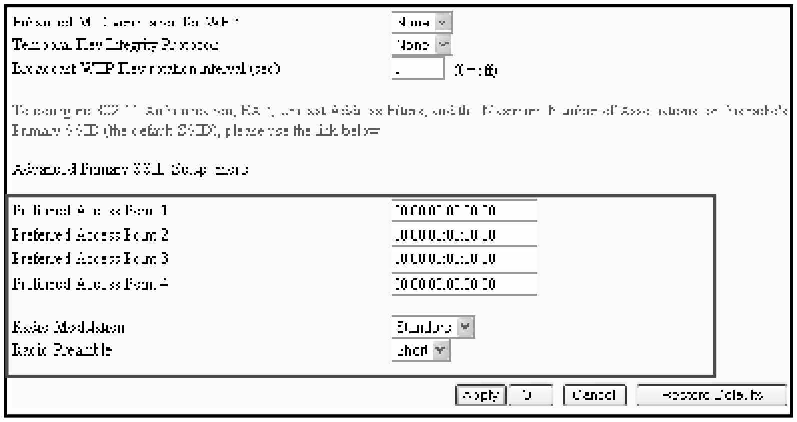
Note When you enable broadcast key rotation, only wireless client devices using LEAP or EAP-TLS authentication can use the access point. Client devices using static WEP (with open, shared key, or EAP-MD5 authentication) cannot use the access point when you enable broadcast key rotation.

- **Advanced Primary SSID Setup:** Go to this link to configure 802.11 authentication, EAP, Unicast address filters, and the maximum number of associations for the radio's primary SSID.

Access Point Radio: Internal Advanced (cont.)

Cisco.com

Lower Portion of Screen



Enhanced MIC verification for WEP: None

Temporal Key Integrity Protocol: None

Broadcast WEP Key rotation interval (sec): 0 (0 = off)

To configure 802.11 Authentication, EAP, Port Address Filters, and the Maximum Number of Associations for this radio's Primary SSID (the default SSID), please use the link below:

Advanced Primary SSID Setup menu

Preferred Access Point 1: 00:00:00:00:00:00

Preferred Access Point 2: 00:00:00:00:00:00

Preferred Access Point 3: 00:00:00:00:00:00

Preferred Access Point 4: 00:00:00:00:00:00

Radio Modulation: Standard

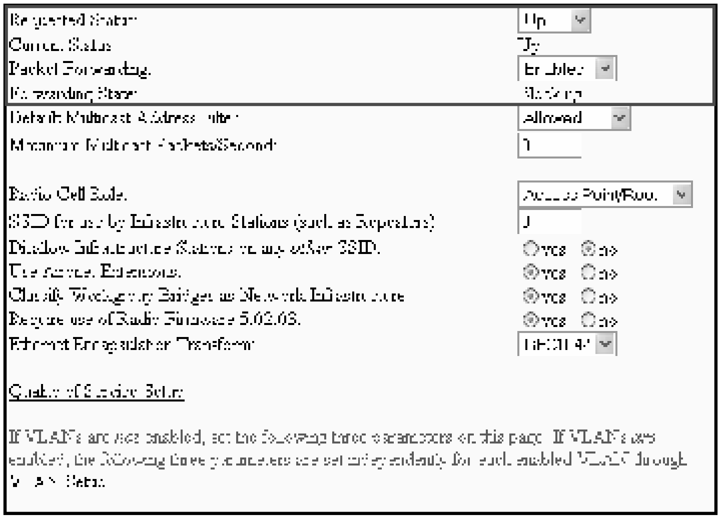
Radio Preamble: Short

AWLF v3.1—8-52

- **Specified Access Points:** You use these fields to set up a chain of repeater access points. Repeater access points function best when they associate with specific access points connected to the wired LAN. If this access point is a repeater, type the MAC address of one or more root-unit access points with which you want this access point to associate. With MAC addresses in these fields, the repeater access point always tries to associate with the specified access points instead of with other less-efficient access points.
- **Radio Modulation:** Select Standard or MOK for the radio modulation the access point uses. Chose from the following values:
  - **Standard**—This default setting is the modulation type specified in IEEE 802.11, the wireless standard published by the Institute of Electrical and Electronics Engineers (IEEE) Standards Association.
  - **MOK**—This modulation was used before the IEEE finished the high-speed 802.11 standard and may still be in use in older wireless networks.
- **Radio Preamble:** The radio preamble is a section of data at the head of a packet that contains information the access point and client devices need when sending and receiving packets. The drop-down menu allows you to select a long or short radio preamble:
  - Long—A long preamble ensures compatibility between the access point and all early models of Cisco Aironet Wireless LAN Adapters (PC4800 and PC4800A).
  - Short—A short preamble improves throughput performance. Cisco Aironet's Wireless LAN Adapter supports short preambles. Early models of Cisco Aironet's Wireless LAN Adapter (PC4800 and PC4800A) require long preambles.

Access Point Radio: Module Advanced

Cisco.com



Requested Status:	Up
Current Status:	Up
Packet Forwarding:	Enabled
Forwarding State:	Blocking
Default Multicast Address Filter:	Allowed
Maximum Multicast Packets/Second:	0
Radio Cell Role:	Access Point/Root
SSID for use by Infrastructure Stations (such as Repeaters):	[illegible]
Disallow Infrastructure Stations on any other SSID:	○ yes ● no
Use Aironet Extensions:	● yes ○ no
Classify Workgroup Bridges as Network Infrastructure:	● yes ○ no
Require use of Radio Firmware 5.02.03:	● yes ○ no
Ethernet Encapsulation Transform:	RFC1042

Quality of Service Setup

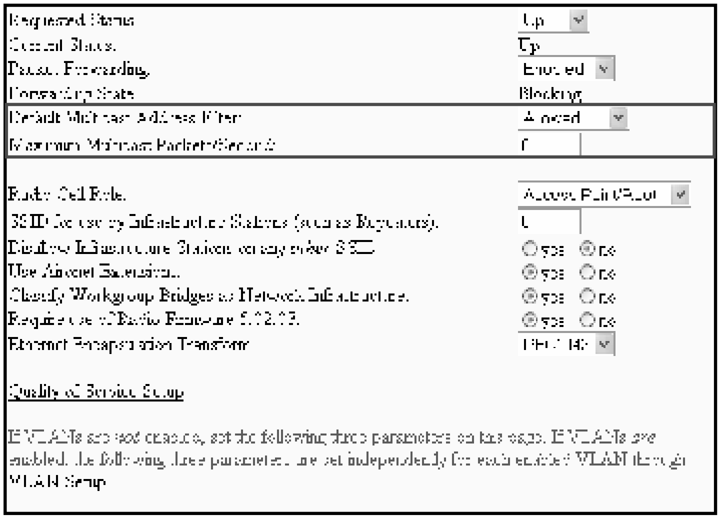
If VLANs are not enabled, set the following three parameters on this page. If VLANs are enabled, the following three parameters are set independently for each enabled VLAN through VLAN Setup.

AWLF v3.1—8-53

- **Requested Status:** This setting is useful for troubleshooting problems on your network. Up, the default setting, turns the radio on for normal operation. Down turns the access point's radio off.
- **Current Status:** The Current Status line under the setting displays the current status of the radio port. This field can also display Error, meaning the port is operating but is in an error condition.
- **Packet Forwarding:** This setting is always set to Enabled for normal operation. For troubleshooting, you might want to set packet forwarding to Disabled, which prevents data from moving between the Ethernet and the radio.
- **Forwarding State:** The Forwarding State line under the setting displays the current forwarding state. For normal access point operation, the forwarding state is Forwarding. Four other states are possible:
  - **Unknown**—The state cannot be determined.
  - **Disabled**—Forwarding capabilities are disabled.
  - **Blocking**—The port is blocking transmission. This is the state when no stations are associated.
  - **Broken**—This state reports radio failure.

Access Point Radio: Module Advanced (Cont.)

Cisco.com



Requested Status: Up
Current Status: Up
Packet Forwarding: Enabled
Forwarding State: Blocking
Default Multicast Address Filter: Allowed
Maximum Multicast Packets/Second: 0

Radio Cell Role: Access Point/Root
SSID for use by Infrastructure Stations (such as Repeaters):
Disallow Infrastructure Stations on any other SSID: ○ yes ● no
Use Aironet Extensions: ● yes ○ no
Classify Workgroup Bridges as Network Infrastructure: ● yes ○ no
Require use of Radio Firmware 5.02.03: ● yes ○ no
Ethernet Encapsulation Transform: RFC1042

Quality of Service Setup

If VLANs are not enabled, set the following three parameters on this page. If VLANs are enabled, the following three parameters are set independently for each enabled VLAN through VLAN Setup

AWLF v3.1—8-54

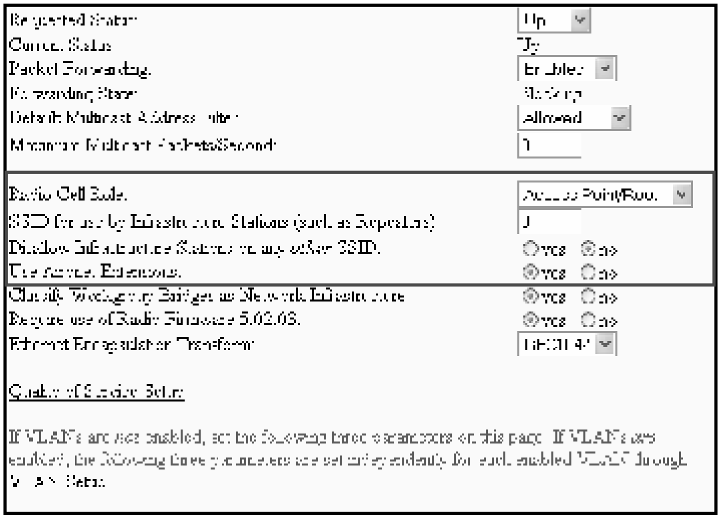
- **Default Multicast Address Filters:** MAC address filters allow or disallow the forwarding of multicast packets sent to specific MAC addresses. You can create a filter that passes traffic to all MAC addresses except those you specify, or you can create a filter that blocks traffic to all MAC addresses except those you specify. The drop-down menus for multicast address filters contain two options:
  - Allowed—The access point forwards all traffic except packets sent to the MAC addresses listed as disallowed on the Address Filters page.
  - Disallowed—The access point discards all traffic except packets sent to the MAC addresses listed as allowed on the Address Filters page.

Note If you plan to discard traffic to all MAC addresses except those you specify (the Disallowed setting), be sure to enter your own MAC address as allowed on the Address Filters page.

- **Maximum Multicast Packets/Second:** Use this setting to control the number of multicast packets that can pass through the radio port each second. If you enter 0, the access point passes an unlimited number of multicast packets. If you enter a number other than 0, the device passes only that number of multicast packets per second.

Access Point Radio: Module Advanced (Cont.)

Cisco.com



Requested Status: Up
Current Status: Up
Packet Forwarding: Enabled
Forwarding State: Blocking
Default Multicast Address Filter: Allowed
Maximum Multicast Packets/Second: 0

Radio Cell Role: Access Point/Root
SSID for use by Infrastructure Stations (such as Repeaters): J
Disallow Infrastructure Stations on any other SSID: ○yes ●no
Use Aironet Extensions: ●yes ○no
Classify Workgroup Bridges as Network Infrastructure: ●yes ○no
Require use of Radio Firmware 5.02.08: ●yes ○no
Ethernet Encapsulation Transform: RFC1042

Quality of Service Setup

If VLANs are not enabled, set the following three parameters on this page. If VLANs are enabled, the following three parameters are set independently for each enabled VLAN through VLAN Setup.

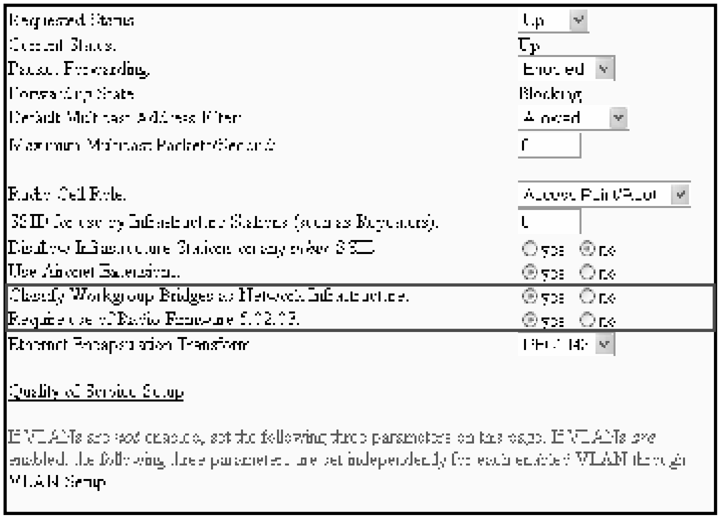
AWLF v3.1—8-55

- **Radio Cell Role:** This parameter is also located on the Express Setup Menu. Refer to the Express Setup Menu for the definition of this parameter.
- **SSID for use by Infrastructure Stations (such as Repeaters):** This parameter is also located on the Express Setup Menu. Refer to the Express Setup Menu for the definition of this parameter.
- **Disallow Infrastructure Stations on any *other*** SSID**:** Prevents repeaters or workgroup bridges from associating to SSIDs other than the infrastructure SSID. The default setting is No, so to invoke this condition, you must change the setting to Yes.
- **Use Aironet Extensions:** Select yes or no to use Cisco Aironet 802.11 extensions. This setting must be set to yes (the default setting) to enable these features:
  - Load balancing
  - Message Integrity Check (MIC)
  - Temporal Key Integrity Protocol (TKIP)

The extensions also improve the access point's ability to understand the capabilities of Cisco Aironet client devices associated with the access point.

Access Point Radio: Module Advanced (Cont.)

Cisco.com



Requested Status:	Up
Current Status:	Up
Packet Forwarding:	Enabled
Forwarding State:	Blocking
Default Multicast Address Filter:	Allowed
Maximum Multicast Packets/Second:	0
Radio Cell Role:	Access Point/Root
SSID for use by Infrastructure Stations (such as Repeaters):	
Disallow Infrastructure Stations on any other SSID:	○ yes ● no
Use Aironet Extensions:	● yes ○ no
Classify Workgroup Bridges as Network Infrastructure:	● yes ○ no
Require use of Radio Firmware 5.02.03:	● yes ○ no
Ethernet Encapsulation Transform:	RFC1042

Quality of Service Setup

If VLANs are not enabled, set the following three parameters on this page. If VLANs are enabled, the following three parameters are set independently for each enabled VLAN through VLAN Setup

AWLF v3.1—8-56

- **Classify Workgroup Bridges as Network Infrastructure:** Select no to allow more than 20 Cisco Aironet Workgroup Bridges to associate to the access point. The default setting, yes, limits the number of workgroup bridges that can associate to the access point to 20 or less.

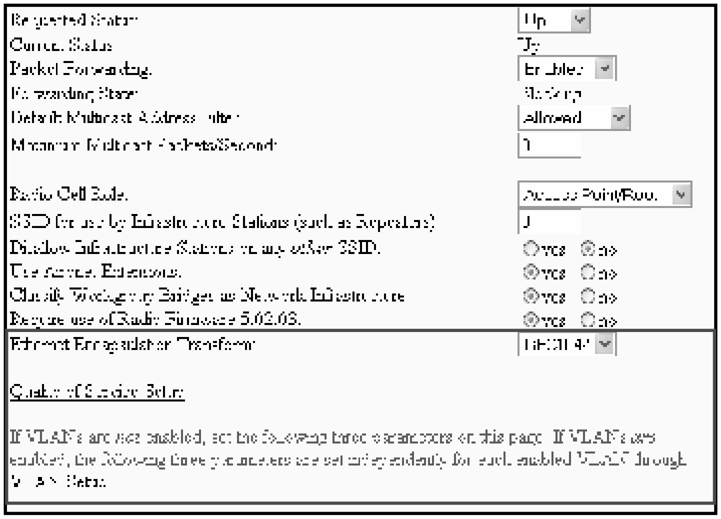
  Access points and bridges normally treat workgroup bridges not as client devices but as infrastructure devices, like access points or bridges. Treating a workgroup bridge as an infrastructure device means that the access point reliably delivers multicast packets, including Address Resolution Protocol (ARP) packets, to the workgroup bridge.

Note This feature is best suited for use with stationary workgroup bridges. Mobile workgroup bridges might encounter spots in the access point's coverage area where they do not receive multicast packets and lose communication with the access point even though they are still associated to it.

- **Require Use of Radio Firmware x.xx:** This setting affects the firmware upgrade process when you load new firmware for the access point. Select yes to force the radio firmware to be upgraded to a firmware version compatible with the current version of the management system. Select no to exempt the current radio firmware from firmware upgrades.

Access Point Radio: Module Advanced (Cont.)

Cisco.com



Requested Status:	Up
Current Status:	Up
Packet Forwarding:	Enabled
Forwarding State:	Blocking
Default Multicast Address Filter:	Allowed
Maximum Multicast Packets/Second:	0
Radio Cell Role:	Access Point/Root
SSID (for use by Infrastructure Stations (such as Repeaters):	
Disallow Infrastructure Stations on any other SSID:	○ yes ● no
Use Aironet Extensions:	● yes ○ no
Classify Workgroup Bridges as Network Infrastructure:	● yes ○ no
Require use of Radio Firmware 5.02.03:	● yes ○ no
Ethernet Encapsulation Transform:	RFC1042

Quality of Service Setup

If VLANs are not enabled, set the following three parameters on this page. If VLANs are enabled, the following three parameters are set independently for each enabled VLAN through VLAN Setup.

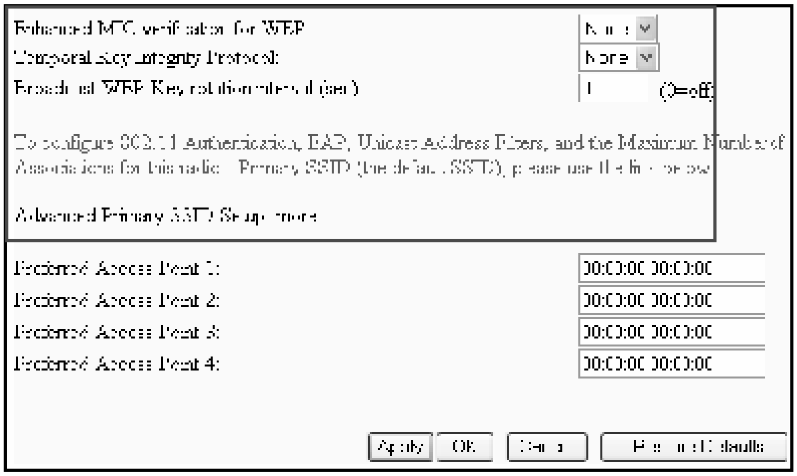
AWLF v3.1—8-57

- **Ethernet Encapsulation Transform:** Choose 802.1H or RFC1042 to set the Ethernet encapsulation type. Data packets that are not 802.2 packets must be formatted to 802.2 using 802.1H or RFC1042. Cisco Aironet equipment uses 802.1H because it provides optimum interoperability.
  - **802.1H**—This default setting provides optimum performance for Cisco Aironet wireless products.
  - **RFC1042**—Use this setting to ensure interoperability with non-Cisco Aironet wireless equipment. RFC1042 does not provide the interoperability advantages of 802.1H but is used by other manufacturers of wireless equipment.
- **Quality of Service Setup Link:** Clicking on the Quality of Service (QoS) Setup link accesses the AP Radio Quality of Service page. Use this page to configure the radio's QoS setup and priorities.
- **VLAN Setup Link:** Clicking the VLAN Setup link accesses the VLAN Setup page. Use this page to configure, add, edit, and remove VLANs associated with your access point.

Access Point Radio: Module Advanced (Cont.)

Cisco.com

Lower Portion of Screen



Enhanced MIC verification for WEP: None

Temporal Key Integrity Protocol: None

Broadcast WEP Key rotation interval (sec): (0=off)

To configure 802.11 Authentication, EAP, Unicast Address Filters, and the Maximum Number of Associations for this radio's Primary SSID (the default SSID), please use the link below:

Advanced Primary SSID Setup more

Preferred Access Point 1: 00:00:00 00:00:00

Preferred Access Point 2: 00:00:00 00:00:00

Preferred Access Point 3: 00:00:00 00:00:00

Preferred Access Point 4: 00:00:00 00:00:00

AWLF v3.1—8-58

- **Enhanced MIC verification for WEP:** This setting enables Message Integrity Check (MIC), a security feature that protects your WEP keys by preventing attacks on encrypted packets called *bit-flip* attacks. Select MMH from the drop-down menu and click Apply to enable MIC.
- **Temporal Key Integrity Protocol:** This setting enables the temporal key integrity protocol (TKIP, or WEP key hashing). To enable WEP key hashing, chose CISCO from the drop down menu.
- **Broadcast WEP Key rotation interval (sec):** This option enables broadcast key rotation by setting a key rotation interval. To enable broadcast key rotation, enter the rotation interval in seconds in the Broadcast WEP Key rotation interval entry field. If you enter 900, for example, the access point sends a new broadcast WEP key to all associated client devices every 15 minutes. To disable broadcast WEP key rotation, enter 0.

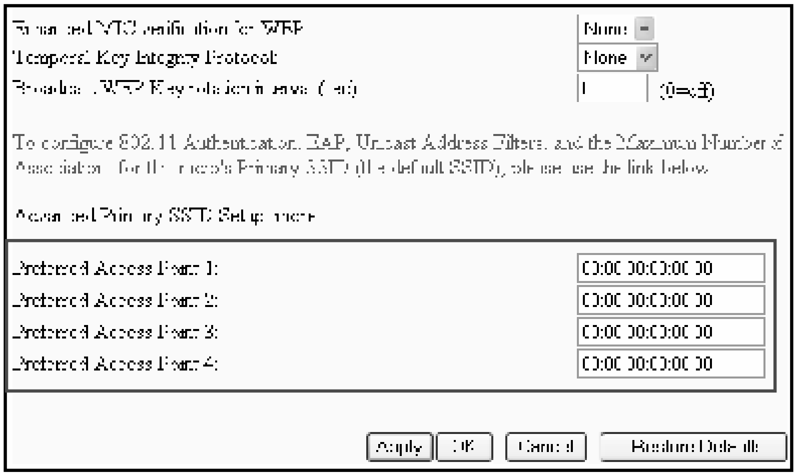
Note When you enable broadcast key rotation, only wireless client devices using LEAP or EAP-TLS authentication can use the access point. Client devices using static WEP (with open, shared key, or EAP-MD5 authentication) cannot use the access point when you enable broadcast key rotation.

- **Advanced Primary SSID Setup:** Go to this link to configure 802.11 authentication, EAP, Unicast address filters, and the maximum number of associations for the radio's primary SSID.

Access Point Radio: Module Advanced (Cont.)

Cisco.com

Lower Portion of Screen



Enhanced MIC verification for WEP: None

Temporal Key Integrity Protocol: None

Broadcast WEP Key rotation interval (sec): 0 (0=off)

To configure 802.11 Authentication, EAP, Unicast Address Filters, and the Maximum Number of Associations for the radio's Primary SSID (the default SSID), please use the link below.

Advanced Primary SSID Setup: more

Preferred Access Point 1: 00:00:00:00:00:00

Preferred Access Point 2: 00:00:00:00:00:00

Preferred Access Point 3: 00:00:00:00:00:00

Preferred Access Point 4: 00:00:00:00:00:00

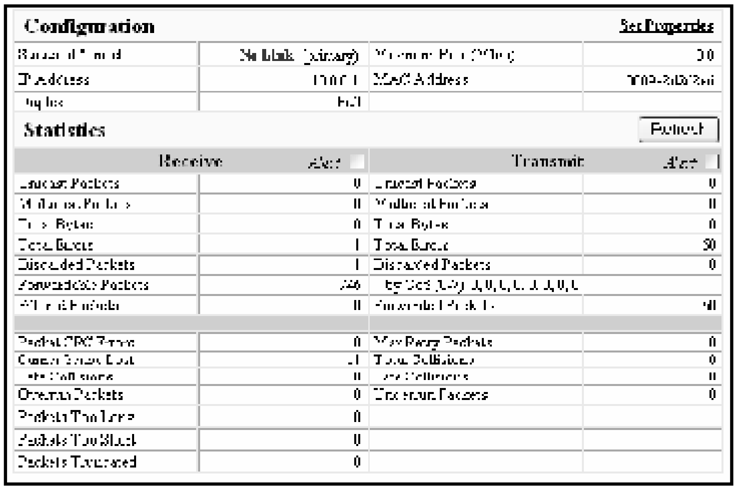
AWLF v3.1—8-59

- **Specified Access Points:** You use these fields to set up a chain of repeater access points. Repeater access points function best when they associate with specific access points connected to the wired LAN. If this access point is a repeater, type the MAC address of one or more root-unit access points with which you want this access point to associate. With MAC addresses in these fields, the repeater access point always tries to associate with the specified access points instead of with other less-efficient access points.

Statistics

Statistics - Ethernet Port

Cisco.com



Configuration — Set Properties

Status of "fec0"	Up Link (primary)	Maximum Rate (Mb/s)	10.0
IP Address	[illegible]	MAC Address	[illegible]
Duplex	Full		

Statistics — Refresh

Receive	Alert □	Transmit	Alert □
Unicast Packets	0	Unicast Packets	0
Multicast Packets	0	Multicast Packets	0
Total Bytes	0	Total Bytes	0
Total Errors	1	Total Errors	50
Discarded Packets	1	Discarded Packets	0
Forwardable Packets	226	[illegible] 0, 0, 0, 0, 0, 0, 0, 0	
Filtered Packets	0	Forwardable Packets	40
Packet CRC Errors	0	Max Retry Packets	0
Carrier Sense Lost	1	Total Collisions	0
Late Collisions	0	Late Collisions	0
Overrun Packets	0	Underrun Packets	0
Packets Too Long	0		
Packets Too Short	0		
Packets Truncated	0		

© 2003, Cisco Systems, Inc. All rights reserved.

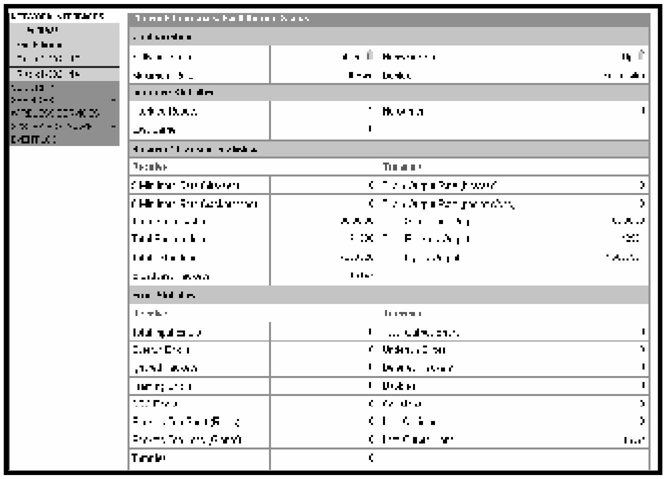
AWLF v3.1—8-61

This page presents key information on the access point's Ethernet port. The Ethernet port is the wired connection to the Ethernet network. The top four cells report the operational status, maximum data rate and the identifying addresses of the Ethernet port. See the Express Setup page for information on device and port identification.

- **Set Properties:** This is a link to the Ethernet Hardware page.
- **Status of "fec0":** "Fast Ethernet Controller" is part of Motorola's naming convention for the Ethernet device used by the access point. This field displays one of the three possible operating states for the port. The added term "primary" identifies the port as the primary port for the access point.
- **Up:** The port is operating properly.
- **Down:** The port is not operating.
- **Error:** The port is in an error condition.
- **Maximum Rate (Mb/s):** Maximum rate of data transmission in megabits per second.
- **IP Address:** Internet protocol address of the device. Use the Express Setup page to assign or change IP address.
- **MAC (Media Access Control) Address:** The MAC address is a unique identifier assigned by the manufacturer.

Statistics - Ethernet Port

Cisco.com

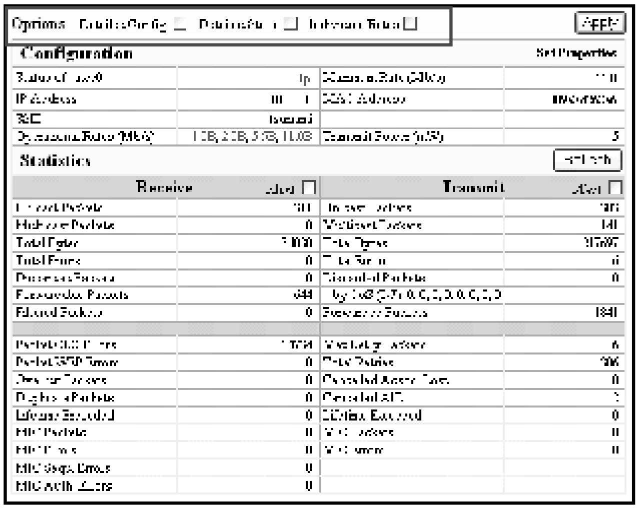


Network Interface Screen for Fast Ethernet Status/ Statistics. Configuration, Interface Summary Statistics, Transmit/ Receive Statistics, and Error Statistics are available from this page.

- **Configuration** section details hardware and software status of port, link state and speed.
- **Interface Statistics** section gives interface state change statistics, i.e., resets, lost carrier, no carrier.
- **Receive/Transmit Statistics** section gives detailed data on traffic on Ethernet interface, including transmit/receive rates, and total packets.
- **Error Statistics** section gives details on Ethernet errors reported on interface, including receive CRC errors, transmit collisions, etc.

Statistics – Access Point Radio: Internal Port

Cisco.com



Options Detailed Config □ Detailed Stats □ Individual Rates □ Apply

Configuration Set Properties

Status of Awc0	Up	Current Rate (Mb/s)	11.0
IP Address	[illegible]	MAC Address	[illegible]
SSID	tsunami		
Operational Rates (Mb/s)	1.0B, 2.0B, 5.5B, 11.0B	Transmit Power (mW)	5

Statistics Refresh

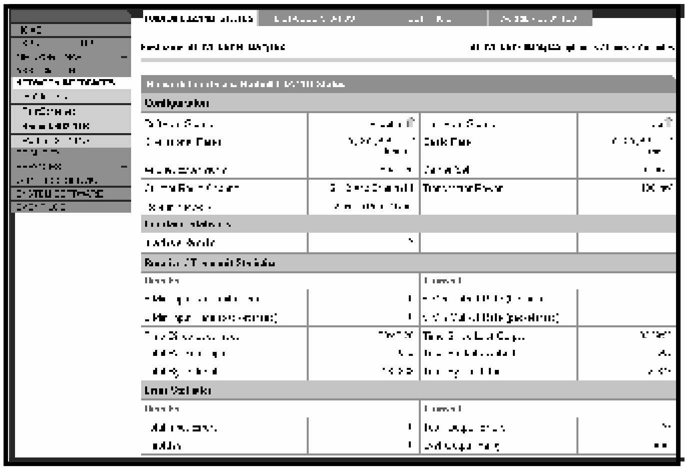
Receive	Alert □	Transmit	Alert □
Unicast Packets	[illegible]	Unicast Packets	[illegible]
Multicast Packets	0	Multicast Packets	141
Total Bytes	[illegible]	Total Bytes	[illegible]
Total Errors	0	Total Errors	0
Discarded Packets	0	Discarded Packets	0
Forwardable Packets	644	By Rate (Mb/s) 0.0, 0, 0, 0.0, 0, 0	
Filtered Packets	0	Forwarded Packets	1841
Packet CRC Errors	[illegible]	Max Retry Packets	6
Packet WEP Errors	0	Total Retries	[illegible]
Overrun Packets	0	Canceled Assoc Lost	0
Duplicate Packets	0	Canceled AID	[illegible]
Lifetime Exceeded	0	Lifetime Exceeded	0
MIC Packets	0	MIC Packets	0
MIC Errors	0	MIC Errors	0
MIC Seqn. Errors	0		
MIC Auth. Errors	0		

AWLF v3.1—8-63

This sample page is the basic access point radio port page. The options section provides three check boxes that deliver more details on the port configuration and operating statistics. The basic page without any of the options will ordinarily provide all information needed to monitor and administer the port in normal operation. The options would most likely be needed in comprehensive site surveys or advanced system troubleshooting.

- **Detailed Configuration:** Added configuration details include request to send (RTS) and data retry settings; firmware and boot block version levels; and regulatory domain code.
- **Detailed Statistics:** The detailed statistics checkbox provides 20 more statistical fields covering packet fragments, collisions, and other errors.
- **Individual Rates:** This checkbox reports the data transmission statistics at each of the individual rates.

Statistics- Access Point Radio Interface: Radio0-802.11B

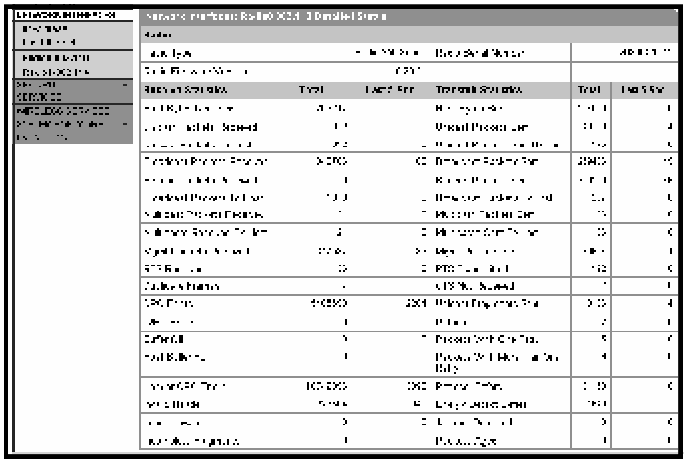


Network Interface Screen for Radio0-802.11B Status/ Statistics. Configuration, Interface Summary Statistics, Transmit/ Receive Statistics, and Error Statistics are available from this page.

- **Configuration** section details hardware and software status of interface, link status and data rates supported.
- **Interface Statistics** section gives interface state change statistics, i.e., resets.
- **Receive/Transmit Statistics** section gives detailed data on traffic on Radio interface, including transmit/receive rates, total packets.
- **Error Statistics** section gives details on Radio interface errors reported on interface.

Statistics- Access Point Radio Interface: Radio0-802.11B (Detailed Statistics)

Cisco.com



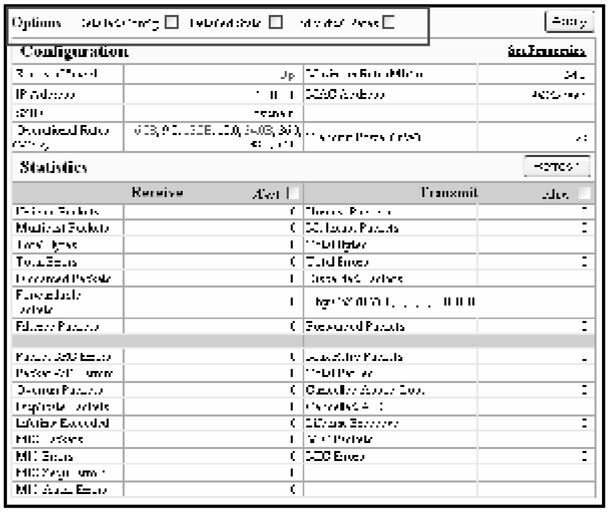
AWLF v3.1—8-65

The Detailed Statistics page provides information on the specific 802.11 traffic. Specific transmit and receive protocol statistics are collected for the radio interface. Included in the statistics are:

- Receive Unicast/ Broadcast packets
- Beacon packets received
- CRC errors (receive)
- WEP packet errors (receive)
- Transmit Unicast/ Broadcast packets
- Beacon packets transmit
- Transmit retries/ Packets with multiple retry

Statistics – Access Point Radio: Module Port

Cisco.com



Options [illegible] □ [illegible] □ [illegible] □ [illegible]

Configuration [illegible]

[illegible]	Up	[illegible]	[illegible]
IP Address	[illegible]	[illegible] Address	[illegible]
SSID	[illegible]		
[illegible] Rates [illegible]	[illegible]	[illegible] Power [illegible]	[illegible]

Statistics [illegible]

Receive	[illegible]	Transmit	[illegible]
[illegible] Packets	0	[illegible] Packets	[illegible]
Multicast Packets	0	[illegible] Packets	[illegible]
Total Bytes	0	Total Bytes	[illegible]
Total Errors	0	Total Errors	[illegible]
Discarded Packets	0	[illegible]	[illegible]
[illegible] Packets	0	[illegible]	[illegible]
Filtered Packets	0	Forwarded Packets	[illegible]
[illegible] Errors	0	[illegible] Packets	[illegible]
[illegible]	0	Total [illegible]	[illegible]
[illegible] Packets	0	[illegible]	[illegible]
[illegible] Packets	0	[illegible]	[illegible]
Lifetime Exceeded	0	[illegible]	[illegible]
MIC [illegible]	0	[illegible] Packets	[illegible]
MIC Errors	0	[illegible] Errors	[illegible]
MIC [illegible]	0		
MIC [illegible] Errors	0		

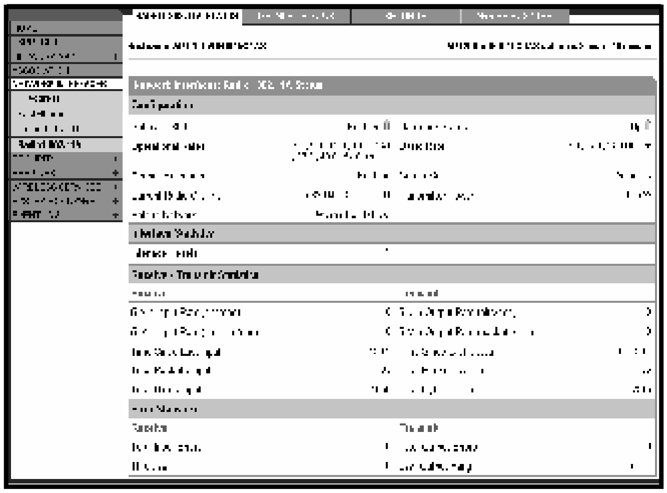
© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—8-66

This sample page is the basic access point radio port page. The options section provides three check boxes that deliver more details on the port configuration and operating statistics. The basic page without any of the options will ordinarily provide all information needed to monitor and administer the port in normal operation. The options would most likely be needed in comprehensive site surveys or advanced system troubleshooting.

- **Detailed Configuration:** Added configuration details include request to send (RTS) and data retry settings; firmware and boot block version levels; and regulatory domain code.
- **Detailed Statistics:** The detailed statistics checkbox provides 20 more statistical fields covering packet fragments, collisions, and other errors.
- **Individual Rates:** This checkbox reports the data transmission statistics at each of the individual rates.

Statistics – Access Point Radio: Radio1-802.11A

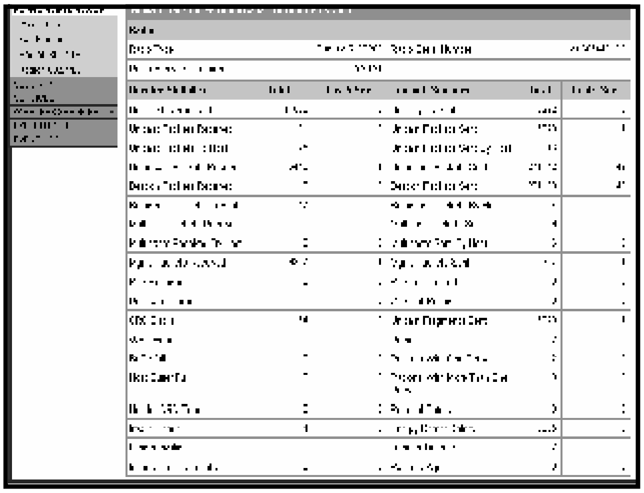


Network Interface Screen for Radio0-802.11A Status/ Statistics. Configuration, Interface Summary Statistics, Transmit/ Receive Statistics, and Error Statistics are available from this page.

- **Configuration** section details hardware and software status of interface, link status and data rates supported.
- **Interface Statistics** section gives interface state change statistics, i.e., resets.
- **Receive/Transmit Statistics** section gives detailed data on traffic on Radio interface, including transmit/receive rates, total packets
- **Error Statistics** section gives details on Radio interface errors reported on interface.

Statistics – Access Point Radio: Radio1-802.11A (Detailed Statistics)

Cisco.com

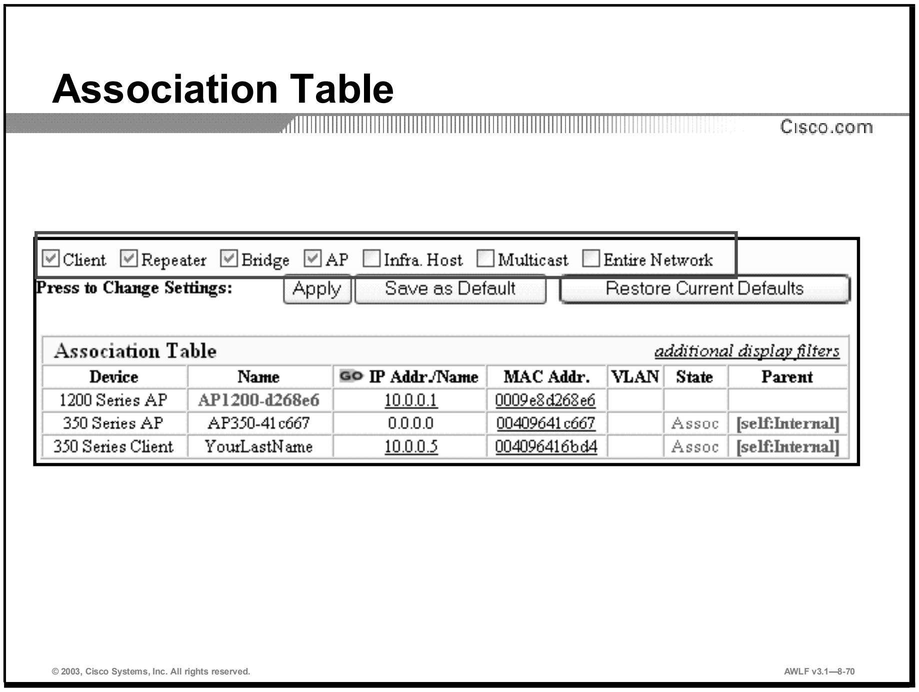


AWLF v3.1—8-68

The Detailed Statistics page provides information on the specific 802.11 traffic. Specific transmit and receive protocol statistics are collected for the radio interface. Included in the statistics are:

- Receive Unicast/ Broadcast packets
- Beacon packets received
- CRC errors (receive)
- WEP packet errors (receive)
- Transmit Unicast/ Broadcast packets
- Beacon packets transmit
- Transmit retries/ Packets with multiple retry

Setup of Association Parameters and Features



Association Table

☑ Client ☑ Repeater ☑ Bridge ☑ AP □ Infra. Host □ Multicast □ Entire Network

Press to Change Settings:

Association Table *additional display filters*

Device	Name	GO IP Addr./Name	MAC Addr.	VLAN	State	Parent
1200 Series AP	AP1200-d268e6	10.0.0.1	0009e8d268e6			
350 Series AP	AP350-41c667	0.0.0.0	00409641c667		Assoc	[self:Internal]
350 Series Client	YourLastName	10.0.0.5	004096416bd4		Assoc	[self:Internal]

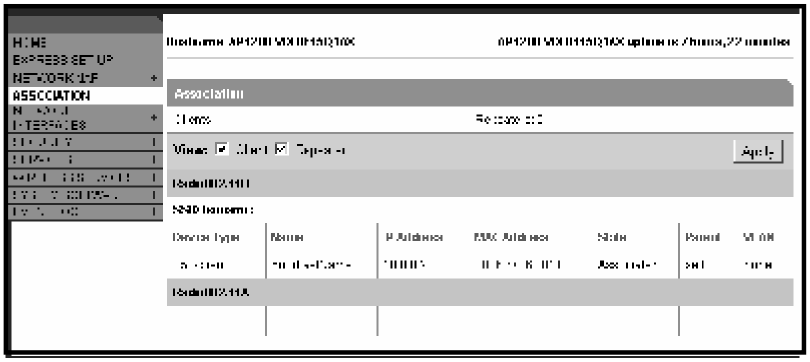
Display Filter Options

Seven check boxes allow selection of the type of stations to be displayed. The link *additional display filters* provides more display options on the association table filters page. The check box settings can be used in various combinations to focus on selected groups or combinations of stations.

- **Client:** A station that is wirelessly connected to an access point or bridge.
- **Repeater:** A station (typically another access point) that forwards data from a client station to another access point.
- **Bridge:** A station that connects two wired networks together via a wireless network.
- **AP (Access point):** A station that connects a wired network with wireless client stations.
- **Infra. (Infrastructure) Host:** A node that has a wired connection to the network.
- **Multicast:** An address that specifies a set of nodes within the overall network. Examples of multicast destinations could include “broadcast,” bridges, and Novell stations.
- **Entire Network:** All nodes, both wired and wireless, of which the access point is aware.

Association Table (Cont.)

Cisco.com



Hostname [illegible] [illegible] uptime is 7 hours, 22 minutes

Association

Clients: Repeaters: 0

View: ☑ Client ☑ Repeater

Radio802.11G

SSID [illegible] :

Device Type	Name	IP Address	MAC Address	State	Parent	VLAN
[illegible]	[illegible]	[illegible]	[illegible]	Associated	self	none

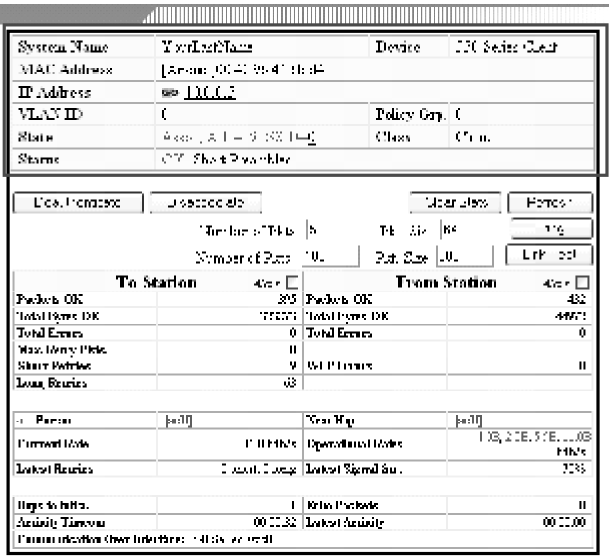
Radio802.11A

AWLF v3.1—8-71

Association Table shows currently associated client devices, their configured 802.11 client **Name**, **IP Address**, **MAC Address**, **State** (Associated, EAP authenticating, Unauthenticated, etc.), **Parent** (Either “self” for associated to root or repeater/WGB for remote clients), and **VLAN** (ID, if AP is configured with multiple VLAN).

Note that the MAC Address is a link which will guide the administrative user to a page containing Link Test utilities, as well as detailed statistics on this client association.

Station Information



System Name	YourLastName	Device	350 Series Client
MAC Address	[illegible]		
IP Address	[illegible]		
VLAN ID	0	Policy Grp.	0
State	Assoc [illegible]	Class	Client
Status	OK, Short Preambles		

To Station	☐	From Station	☐
Packets OK	305	Packets OK	482
Total Bytes OK	[illegible]	Total Bytes OK	[illegible]
Total Errors	0	Total Errors	0
Max. Retry Pkts.	0		
Short Retries	9	WEP Errors	0
Long Retries	63		

Parent	[self]	Next Hop	[self]
Current Rate	11.0 Mb/s	Operational Rates	1.0, 2.0, 5.5, 11.0 Mb/s
Latest Retries	[illegible]	Latest Signal Str.	[illegible]

Hops to Infra.	1	Echo Packets	0
Activity Timeout	00:00:32	Latest Activity	00:00:00
Communication Over Interface: [illegible]			

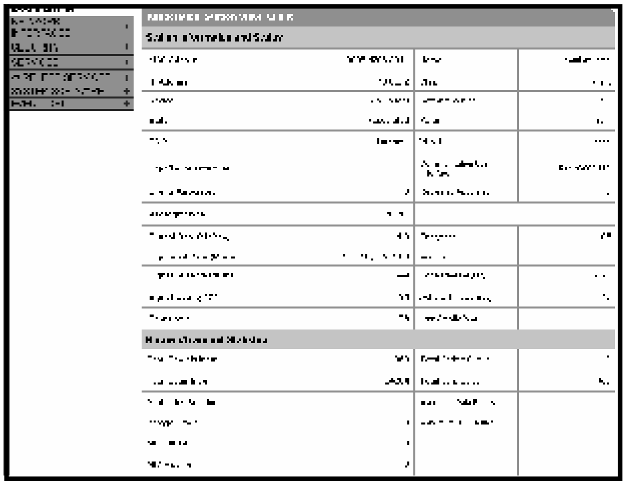
AWLF v3.1—8-72

To access station information click on **MAC Address** (in the association table- see previous page).

- **System Name:** The Cisco name assigned to the station.
- **Device:** The device type and model number of the station.
- **MAC Address:** The Media Access Control address is a unique identifier assigned by the manufacturer.
- **IP Address:** Internet protocol address of the device. When you click the IP address link, the browser attempts to browse to any web server operating on the station.
- **State:** Displays the operational state of the wireless station:
- **[self]-, Assoc-, Unauth-**,**Auth-**, **Local Auth-**
- **Class:** This field displays the type of station. Class types include:
- **Access Point, Client, PS Client-**, **Bridge, Bridge R-**, **Rptr-**, **Mcast**, **Infra-**
- **Status: "**OK" indicates proper operating status. Other possible status options include: IP Forwarding Agent, BOOTP/DHCP Client, ARP Proxy Server, IP Virtual Router, and WEP if WEP is enabled. Status also tells you if short radio preambles are in use with this station.

Station Information (Cont.)

Cisco.com



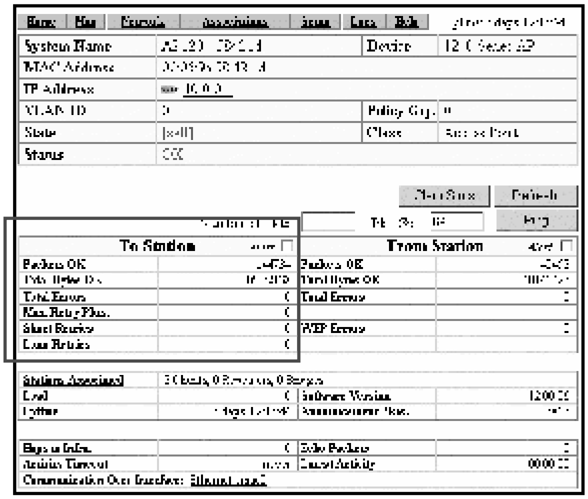
AWLF v3.1—8-73

Station Information (802.11 statistics on associated client) are available from the hyperlink under the associated client MAC address on the association table screen.

Specific details on this client’s association status, including device type, SSID, supported data rates, signal strength, and association time are visible from this interface. In addition, 802.11 protocol statistics are available for packets sent and received for this client.

Link Test

Cisco.com



System Name	[illegible]	Device	[illegible] AP
MAC Address	[illegible]		
IP Address	[illegible]		
VLAN ID	0	Policy Grp.	0
State	[illegible]	Class	Access Point
Status	OK		

To Station	Alert □	From Station	Alert □
Packets OK	[illegible]	Packets OK	[illegible]
Total Bytes OK	[illegible]	Total Bytes OK	[illegible]
Total Errors	0	Total Errors	0
Max. Retry Pkts.	0		
Short Retries	0	WEP Errors	0
Long Retries	0		

Stations Associated	[illegible]		
Load	0	Software Version	[illegible]
Uptime	[illegible]		[illegible]

Hops to Infra.	0	Echo Packets	0
Activity Timeout	[illegible]	Latest Activity	00:00:[illegible]
Communication Over Interface: [illegible]			

AWLF v3.1—8-74

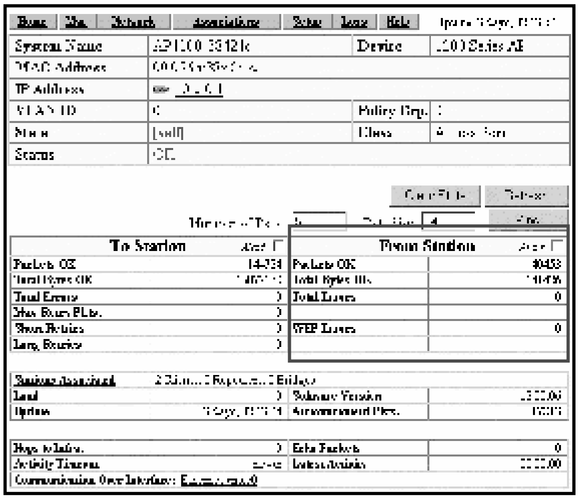
Link test is one method that allows the user to test the RF link between two radio devices. Selecting link test from the station information (see previous page) results in this sample screen.

In this screen we are observing the “To the Station” information column located on the left side.

- **Alert:** Click this box if you want detailed packet trace information captured for the Association Table page. This option is only available to users with administrator capability.
- **Packets OK:** Reports the number of good packets coming to the station.
- **Total Bytes OK:** Reports the number of good bytes coming to the station.
- **Total Errors:** Reports the total number of packet errors coming to the station.
- **Max. Retry Pkts.:** Reports the number of times requests to send (RTSs) have reached the maximum retry number. The maximum retry value is set on Hardware page.
- **RTS (Short) Retries:** Reports the number of times the RTS packet had to be retried.
- **Data (Long) Retries:** Reports the number of times the data packet had to be retried.

Link Test (Cont.)

Cisco.com



System Name	[illegible]	Device	1200 Series AP
MAC Address	[illegible]		
IP Address	[illegible]		
VLAN ID	0	Policy Grp.	0
State	[self]	Class	[illegible]
Status	OK		

To Station	Alert □	From Station	Alert □
Packets OK	[illegible]	Packets OK	40453
Total Bytes OK	[illegible]	Total Bytes OK	[illegible]
Total Errors	0	Total Errors	0
Max. Retry Pkts.	0		
Short Retries	0	WEP Errors	0
Long Retries	0		

Stations Associated	[illegible]		
Load	0	Software Version	[illegible]
Uptime	[illegible]	Announcement Pkts.	[illegible]
Hops to Infra.	0	Echo Packets	0
Activity Timeout	[illegible]	Latest Activity	00:00:00
Communicating Over Interface: [illegible]			

AWLF v3.1—8-75

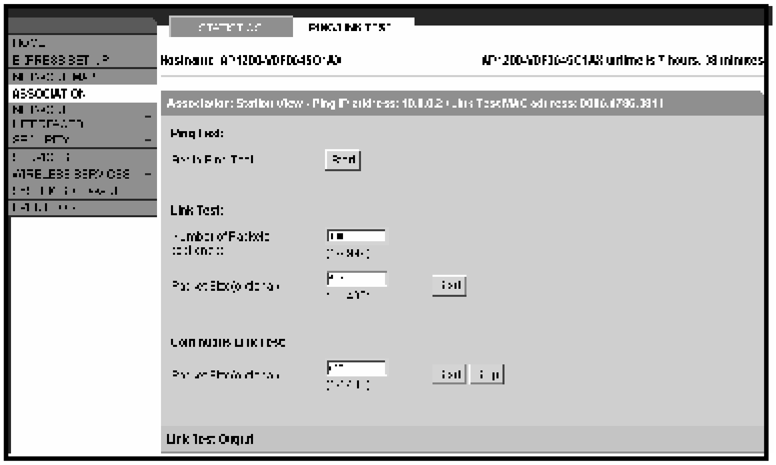
In this screen we are observing the "From the Station" information.

- **Alert:** Click this box if you want detailed packet trace information captured for the Association Table page.

  This option is only available to users with administrator capability.
- **Packets OK:** Reports the number of good packets sent from the station.
- **Total Bytes OK:** Reports the number of good bytes sent from the station.
- **Total Errors:** Reports the total number of packet errors sent from the station.
- **WEP Errors:** Reports the number of encryption errors sent from the station.

Link Test (Cont.)

Cisco.com



Hostname AP1200-[illegible]

[illegible] uptime is 7 hours, 38 minutes

ASSOCIATION

Association: Station View - Ping IP address: 10.0.0.2 - Link Test MAC address: [illegible]

Ping Test:

[illegible] Send

Link Test:

Number of Packets [illegible]

Packet Size [illegible] Send

Continuous Link Test

Packet Size [illegible] Send Stop

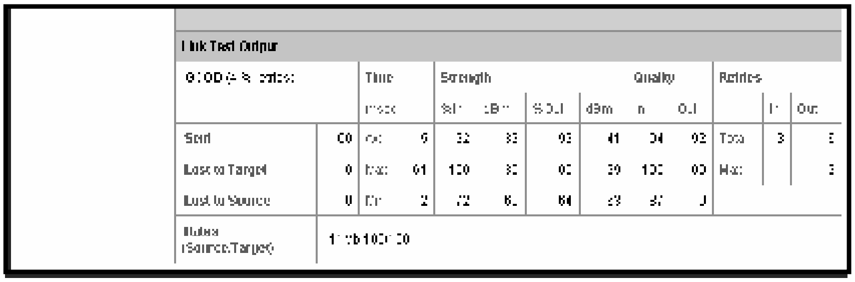
Link Test Output

Under the specific client’s association table entry, there is a Ping/Link test link by each client MAC address.

Either a **Ping Test, Link Test or Continuous Link Test** may be initiated from this link page. Note the specific packet size and number of packets for Link Test may be configured from this page.

Link Test (Cont.)

Cisco.com



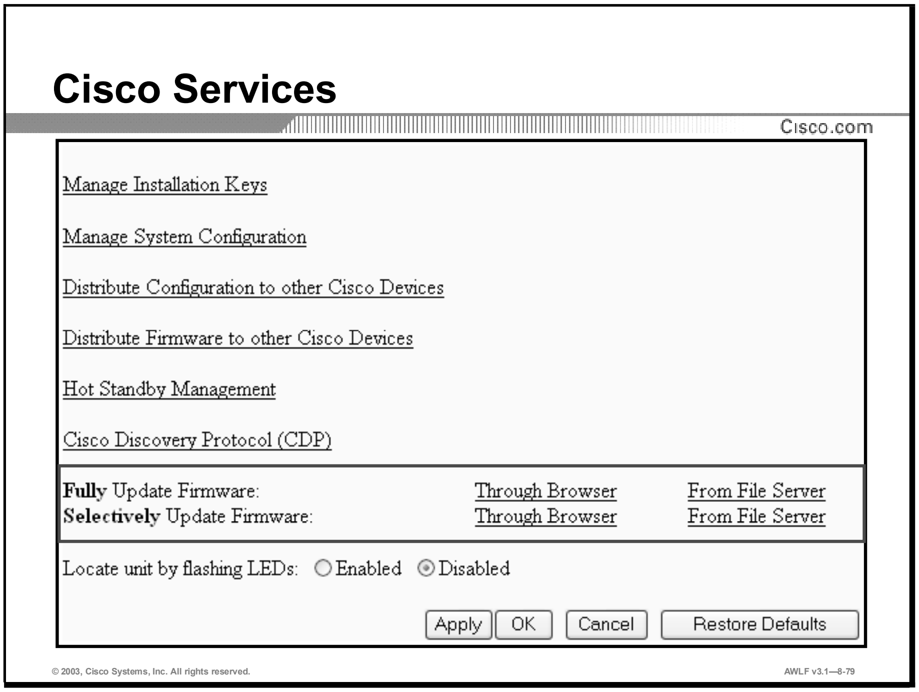
Link Test Output												
[illegible]		Time		Strength				Quality		Retries		
		msec		%In	dBm	%Out	dBm	In	Out		In	Out
Sent	50	Avg	5	32	83	93	41	34	92	Total	3	5
Lost to Target	0	Max	61	100	85	95	39	100	90	Max		3
Lost to Source	0	Min	2	72	61	84	23	37	[illegible]			
Rates (Source:Target)	11Mb 100% [illegible]											

At the bottom of the **Link Test** page, the Link Test results are visible after completion of the link test.

Note that overall test success, delay, signal strength, signal quality, and retries are displayed for both “upstream” and “downstream” packets.

Packets “Lost to Target” reflect packets lost downstream to host and “Lost to Source” reflects packets lost upstream to AP.

Cisco Service



Cisco Services

Cisco.com
Manage Installation Keys
Manage System Configuration
Distribute Configuration to other Cisco Devices
Distribute Firmware to other Cisco Devices
Hot Standby Management
Cisco Discovery Protocol (CDP)

Fully Update Firmware:	Through Browser	From File Server
Selectively Update Firmware:	Through Browser	From File Server

Locate unit by flashing LEDs: ○ Enabled ● Disabled

Apply
OK
Cancel
Restore Defaults

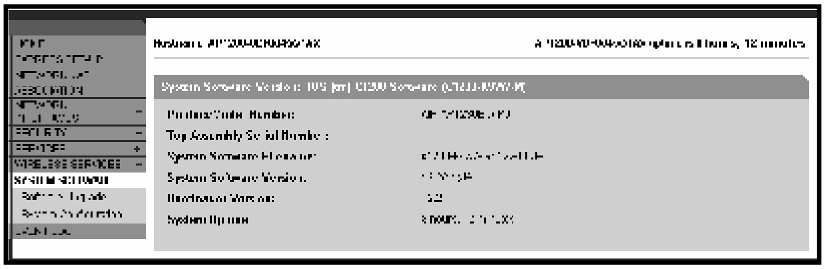
AWLF v3.1—8-79

From the setup page, click the Cisco Services link to take you to the Cisco Services page. From this page the access point's firmware can be upgraded through a web browser or from a file server.

- **Fully Update Firmware:** These are links to alternative ways for reading and updating system firmware, radio firmware, and web pages, all in one step.
- **Through Browser:** This method allows you to browse your hard drive or mapped network drives to find the desired firmware and web page files and updates all the firmware components at the same time.
- **From File Server:** With this method, you enter named file information to update all the firmware components at the same time.
- **Selectively Update Firmware:** These are links to alternative ways for reading and updating system firmware, radio firmware, and web pages. You can select which firmware to update (system firmware, radio firmware, or web pages) rather than updating them all at once.
- **Through Browser:** This method allows you to browse your hard drive or mapped network drives to find the desired firmware and web page files and updates firmware components individually.
- **From File Server:** With this method, you enter named file information to update firmware components individually.

Cisco Services (Cont.)

Cisco.com



Hostname [illegible] uptime is [illegible] hours, 12 minutes

System Software Version: IOS (tm) C1200 Software (C1200-K9W7-M)

Product/Model Number: [illegible]

Top Assembly Serial Number :

System Software Filename: [illegible]

System Software Version: [illegible]

Bootloader Version: [illegible]

System Uptime [illegible]

AWLF v3.1—8-80

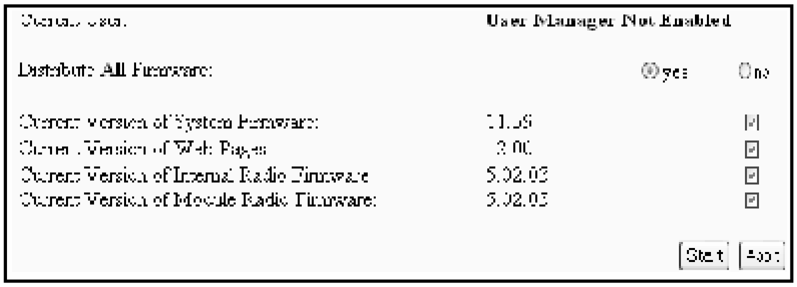
Under System Software page, the system software and hardware details for the AP are visible.

Model Number, Serial Number, System Software, Software Version, Bootloader version, and system uptime may be examined from this status screen.

Firmware Upgrade and Distribution

Firmware Distribution

Cisco.com



Current User: User Manager Not Enabled

Distribute All Firmware: ● yes ○ no

Current Version of System Firmware:	11.08	☑
Current Version of Web Pages	2.00	☑
Current Version of Internal Radio Firmware	5.02.03	☑
Current Version of Module Radio Firmware:	5.02.03	☑

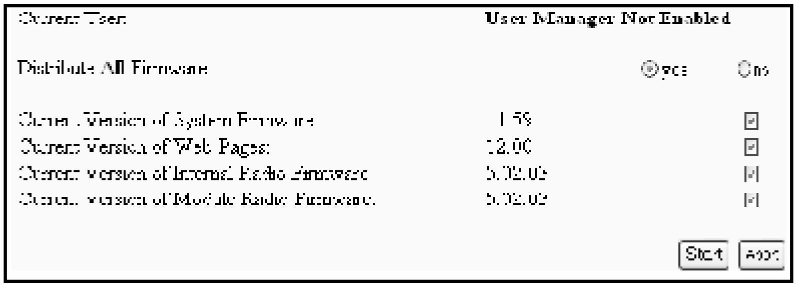
AWLF v3.1—8-82

From the Cisco services menu, click the **Distribute firmware to other Devices** link. This page allows you to distribute the Cisco firmware on an access point to other Cisco devices. The distributing access point sends the firmware to all the access points on your network that:

- Are running firmware that supports the Distribute Firmware feature;
- Can hear the IP multicast “query” issued by the distributing access point (network devices such as routers can block multicast messages);
- Have their web servers enabled for external browsing;
- And, if they have User Manager enabled, contain in their User Lists a user with the same user name, password, and capabilities as the user performing the distribution (the person logged in on the distributing access point.

Firmware Distribution (Cont.)

Cisco.com



Current User: User Manager Not Enabled

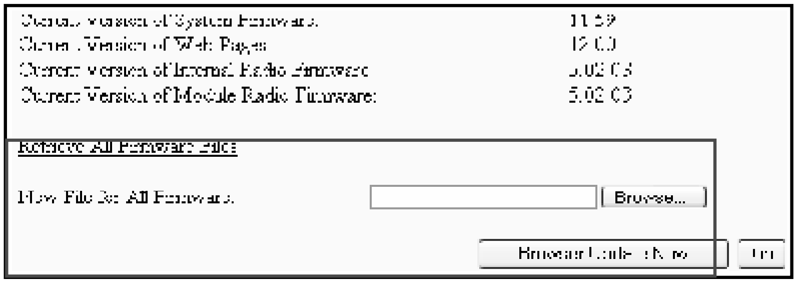
Distribute All Firmware ● yes ○ no

Current Version of System Firmware	11.59	☑
Current Version of Web Pages:	12.00	☑
Current version of Internal Radio Firmware	5.02.02	☑
Current version of Module Radio Firmware:	5.02.02	☑

AWLF v3.1—8-83

- **Current User**: This is the user who has logged in to distribute the firmware. If user manager is enabled on the access points on your network, the User Lists in those access points must contain a user with the same user name, password, and capabilities as the user performing the distribution (the person logged in on the distributing access point).
- **Distribute All Firmware**: This feature works as a “Select all” button for distributing firmware. Select Yes to distribute the current version of the system firmware, the web pages, and, if applicable, the radio firmware.
- **Current Version of System Firmware**: This is the version of system firmware on the distributing access point. Click the checkbox to mark this version for distribution. (The checkbox is already selected if you select Yes under distribute All Firmware.)
- **Current Version of Web Pages**: This is the version of the management system web pages on the distributing access point. Click the checkbox to mark this version for distribution.
- **Current Version of Radio Firmware**: This is the version of the radio firmware for each of the radios (internal 2.4 GHz and external 5 GHz module) on the distributing access point. Click the checkbox to mark this version for distribution.
- **Action Buttons:** The two action buttons control the firmware distribution.
  - **Start**: After you select the firmware you want to distribute, click Start to begin the distribution.
  - **Abort**: Click Abort to cancel the distribution.

Update Firmware (Through Browser)



Current Version of System Firmware: 11.59

Current Version of Web Pages: 12.03

Current Version of Internal Radio Firmware: 5.02.03

Current Version of Module Radio Firmware: 5.02.03

Retrieve All Firmware Files

New File for All Firmware:

AWLF v3.1—8-84

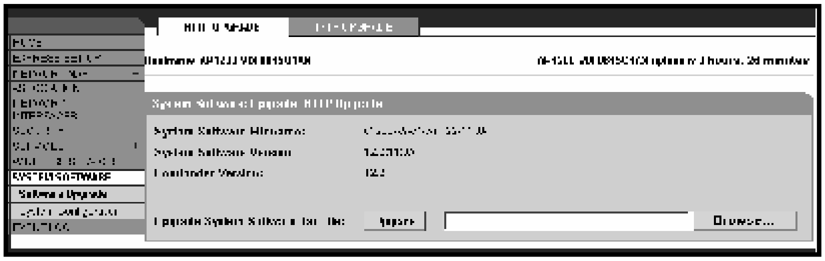
From the Setup page, click **Cisco Services**, then click **Fully** Update Firmware: **Through Browser** link.

This section shows three current firmware version levels:

- System Firmware, Web Pages, and Radio Firmware
- **Retrieve All Firmware Files:** Click the underlined Retrieve All Firmware link to save the current System Firmware and Web Pages to a local hard drive or disk.
- **New File for All Firmware:** Use this section to browse your hard drive or mapped network drives to find the new firmware file. Clicking the **Browser Update Now** button will start the firmware update process on the access point.

Update Firmware (Through Browser) (Cont.)

Cisco.com



Hostname [illegible] uptime is [illegible] hours, 28 minutes

System Software Upgrade: HTTP Upgrade

System Software Filename: [illegible]

System Software Version: [illegible]

Bootloader Version: [illegible]

Upgrade System Software Tar File:

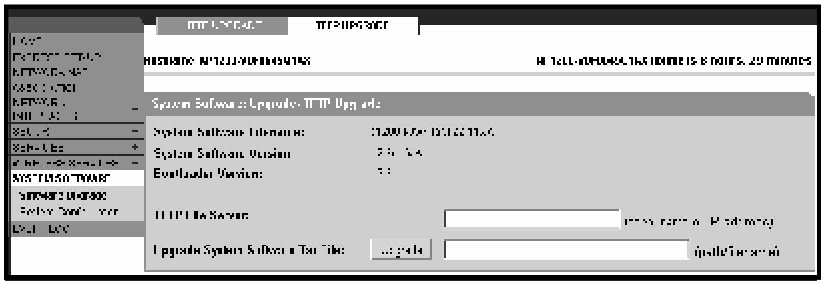
Under the System Software> Software Upgrade page, the currently loaded System Software Filename and Version (and Bootloader version) are displayed.

In addition, the an HTTP Upgrade of the System Software may be initiated from this screen.

Upgrade System Software Tar File: allows the user to enter a locally stored archive file (locatable via the “**Browse**” radio button) for upload to AP via HTTP. The “**Upgrade**” radio button initiates the upload of the “.tar” file to the AP.

Update Firmware (TFTP Server)

Cisco.com



System Software Upgrade - TFTP Upgrade

System Software Filename:

System Software Version:

Bootloader Version:

TFTP File Server: (DNS name or IP address)

Upgrade System Software Tar File: (path/filename)

AWLF v3.1—8-86

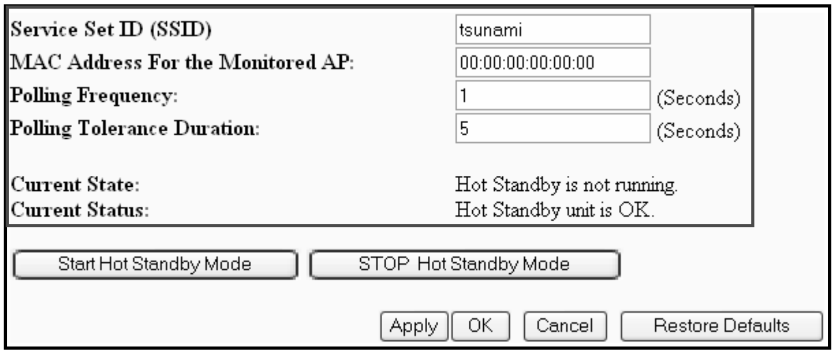
Under the System Software> Software Upgrade page, the currently loaded System Software Filename and Version (and Bootloader version) are displayed.

The **TFTP Upgrade** menu permits the specification of the **TFTP File Server**: to be used for upgrade of AP software via TFTP protocol. Either IP or DNS address of the TFTP server to be used is entered from this interface.

To initiate the software upgrade, the filename (and directory, if necessary) is specified under the “**Upgrade System Software Tar File**:” menu and the “**Upgrade**” radio button is selected.

Hot Standby Management

Cisco.com



Service Set ID (SSID)	tsunami	
MAC Address For the Monitored AP:	00:00:00:00:00:00	
Polling Frequency:	1	(Seconds)
Polling Tolerance Duration:	5	(Seconds)
Current State:	Hot Standby is not running.	
Current Status:	Hot Standby unit is OK.	

AWLF v3.1—8-87

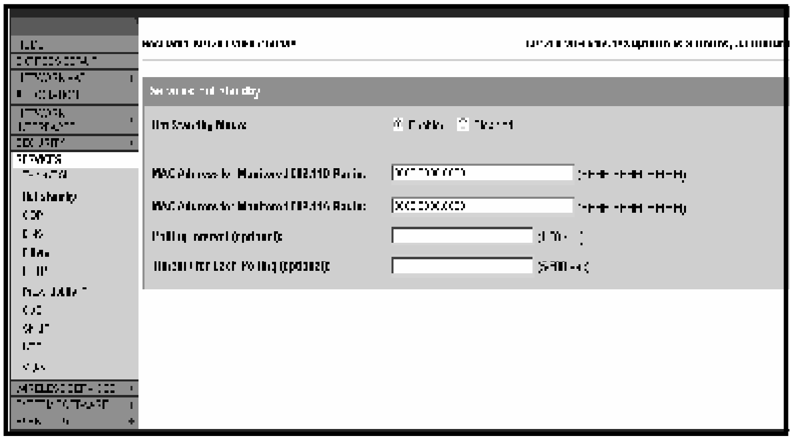
Except for the IP address, the standby access point's settings should be identical to the settings on the monitored access point. You use the Hot Standby page to set up the standby access point.

To utilize hot standby, configure the following parameters:

- **Service Set ID (SSID):** The SSID is a unique identifier that client devices use to associate with the access point. The SSID allows client devices to distinguish between multiple wireless networks in the same vicinity. The SSID can be any alphanumeric entry from 2 up to 32 characters long.
- **MAC Address for the Monitored Access Point:** Enter the monitored access point’s MAC address.
- **Polling Frequency:** Enter the number of seconds between each query the standby access point sends to the monitored access point.
- **Timeout for Each Polling:** Enter the number of seconds the standby access point should wait for a response from the monitored access point before it assumes the monitored access point has malfunctioned.
- **Current Status:** Reports the access point’s standby status.

Hot Standby Management (Cont.)

Cisco.com



Services: Hot Standby

Hot Standby Mode: ● Enable ○ Disable

MAC Address for Monitored 802.11b Radio: [illegible] (HHHH.HHHH.HHHH)

MAC Address for Monitored 802.11a Radio: [illegible] (HHHH.HHHH.HHHH)

Polling Interval (optional): [illegible]

Timeout for Each Polling (optional): [illegible]

AWLF v3.1—8-88

Hot Standby Management may be enabled or disabled from the Services> Hot Standby menu.

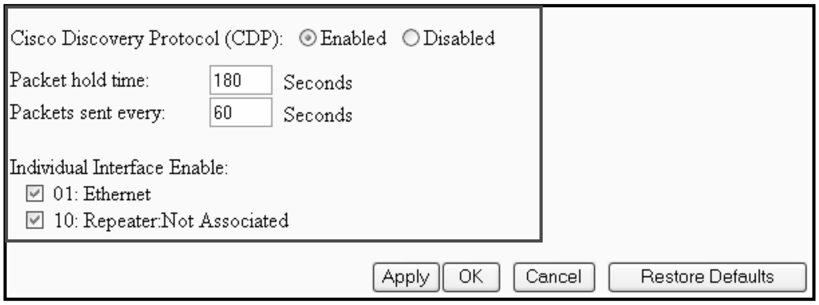
For each standby AP, the MAC addresses of the appropriate Radio interface of the monitored (or main) AP is entered under the “**MAC Address for Monitored 802.1X Radio:**”.

Additionally, the **Polling Interval** and **Timeout for Each Polling Interval** may be specified for the Standby AP. Note the shorted polling interval results in some additional overhead on the 802.11 network.

Note that it is recommended to set the monitored hot standby access point for “Fallback to Radio Shutdown” in the event of Ethernet loss. This will prevent client devices from remaining associated to the AP in the event of Ethernet loss and thus not switch to standby AP.

Cisco Discovery Protocol

Cisco.com



Cisco Discovery Protocol (CDP): ● Enabled ○ Disabled

Packet hold time: 180 Seconds

Packets sent every: 60 Seconds

Individual Interface Enable:

☑ 01: Ethernet

☑ 10: Repeater:Not Associated

AWLF v3.1—8-89

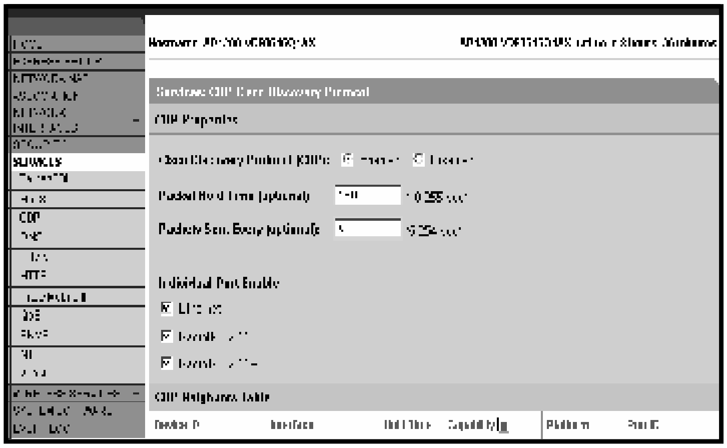
Cisco Discovery Protocol (CDP) is a device-discovery protocol that runs on all Cisco network equipment. Information in CDP packets is used in network management software such as CiscoWorks2000.

Use the CDP Setup page to adjust the access point's CDP settings. CDP is enabled by default.

- **Cisco Discovery Protocol (CDP):** Select Disabled to disable CDP on the access point; select Enabled to enable CDP on the access point. CDP is enabled by default.
- **Packet Hold Time:** The number of seconds other CDP-enabled devices should consider the access point's CDP information valid. If other devices do not receive another CDP packet from the access point before this time elapses, they should assume that the access point has gone offline. The default value is 180. The packet hold time should always be greater than the value in the “Packets sent every” field.
- **Packets Sent Every:** The number of seconds between each CDP packet the access point sends. The default value is 60. This value should always be less than the packet hold time.
- **Individual Port Enable**: Ethernet—When selected, the access point sends CDP packets through its Ethernet port and monitors the Ethernet for CDP packets from other devices.
- **Individual Port Enable: AP Radio**—This checkbox appears when the access point radio is linked to another radio infrastructure device, such as an access point, bridge or repeater. When selected, the access point sends CDP packets through the radio port and monitors the radio for CDP packets from other devices.

Cisco Discovery Protocol (Cont.)

Cisco.com



Services: CDP - Cisco Discovery Protocol

CDP Properties

Cisco Discovery Protocol (CDP): [illegible]

Packet Hold Time (optional): [illegible] (10-255 sec)

Packets Sent Every (optional): [illegible] (5-254 sec)

Individual Port Enable

☒ [illegible]

☒ [illegible]

☒ [illegible]

CDP Neighbors Table

Device ID	Interface	Hold Time	Capability	Platform	Port ID

AWLF v3.1—8-90

Cisco Discovery Protocol may be enabled or disabled from the **CDP** menu accessible via the Services> CDP menu selection.

The “validity period” or **Packet Hold Time** and the CDP packet frequency or “**Packets Sent Every**” period may be specified from the CDP menu.

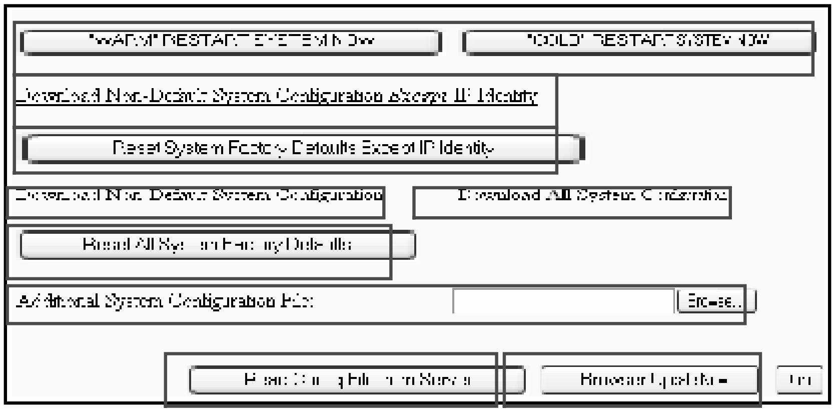
The specific interfaces used for sending CDP data may also be specified from the **Individual Port Enable** selection boxes.

The **CDP Neighbors Table** at the bottom of the screen permits adjacent devices discovered via CDP to be viewed.

System Management

Manage System Configuration

Cisco.com


"WARM" RESTART SYSTEM NOW
"COLD" RESTART SYSTEM NOW
Download Non-Default System Configuration Except IP Identity
Reset System Factory Defaults Except IP Identity
Download Non-Default System Configuration
Download All System Configuration
Reset All System Factory Defaults
Additional System Configuration File:
Browse...
Read Config File from Server
Browser Update Now
Help

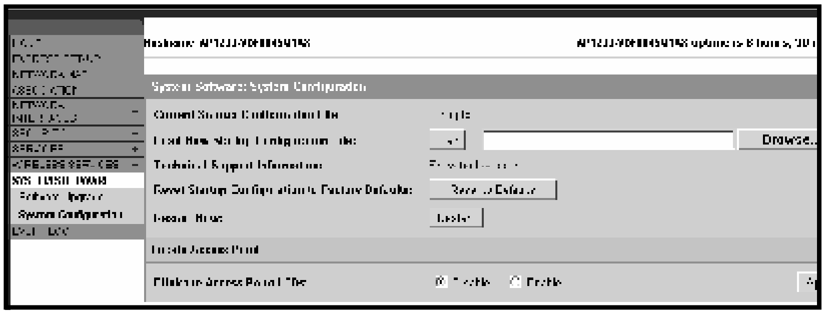
AWLF v3.1—8-92

From the Cisco services page click the **Manage System Configuration** link. This page allows you to perform the following tasks:

- **"WARM" RESTART SYSTEM NOW:** Click this button to perform a warm restart of the access point. A warm restart reboots the access point.
- **"COLD" RESTART SYSTEM NOW:** Click this button to perform a cold restart of the access point. A cold restart is the equivalent of removing and then reapplying power for the access point.
- **Download Non-Default System Configuration Except IP Identity:** Click this button to save the access point's non-default system configuration file, minus the access point's IP (Internet Protocol) Identity information, to your computer, or to any accessible drive.
- **Reset System Factory Defaults Except IP Identity:** Click this button to reset all of the access point's settings, except the access point's IP identity information, to their factory defaults. By not resetting the access point's IP identity information to the factory defaults, you ensure that you will maintain Ethernet connectivity to the access point.
- **Download Non-Default System Configurations:** Click this button to save the access point's non-default configuration file to your computer, or to any accessible drive.
- **Download All System Configurations:** Click this button to save the access point's configuration file to your computer, or to any accessible drive.
- **Reset All System Factory Defaults:** Click this button to reset all of the access point's settings, including the access point's IP identity information, to their factory defaults.
- **Read Config File from Server:** Click this button to retrieve a configuration file from the server for the access point.
- **Browser Update Now:** Click this button to send the configuration file you named in the additional system configuration file entry field to the access point.

Configuration File Management

Cisco.com



System Software: System Configuration

Current Startup Configuration File

Load New Startup Configuration File:

Technical Support Information:

Reset Startup Configuration to Factory Defaults: Reset to Defaults

Restart Now: Restart

Blink the Access Point

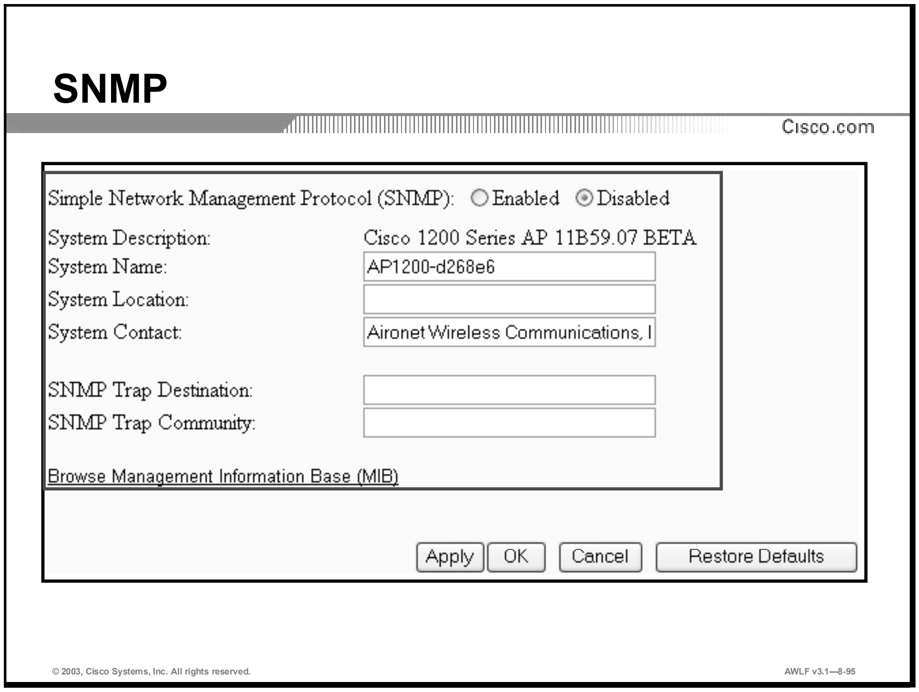
Blink the Access Point LEDs: ☒ Disable ○ Enable

© 2003, Cisco Systems, Inc. All rights reserved. AWLF v3.1—8-93

From the System Software> **System Configuration** screen, the Configuration (a.k.a. config.txt) file used for the IOS AP may be either archived to a local store or may be restored from a locally stored file. In addition, the “show tech” output (**Technical Support Information**)may be obtained from the AP, and the AP may be returned to default configuration parameters.

There are also diagnostic aid utilities available from this screen such as “**Restart Now**” and “**Blink the Access Point LED’s**”.

SNMP Setup



SNMP

Simple Network Management Protocol (SNMP): ○ Enabled ● Disabled

System Description: Cisco 1200 Series AP 11B59.07 BETA

System Name: AP1200-d268e6

System Location:

System Contact: Aironet Wireless Communications, I

SNMP Trap Destination:

SNMP Trap Community:

Browse Management Information Base (MIB)

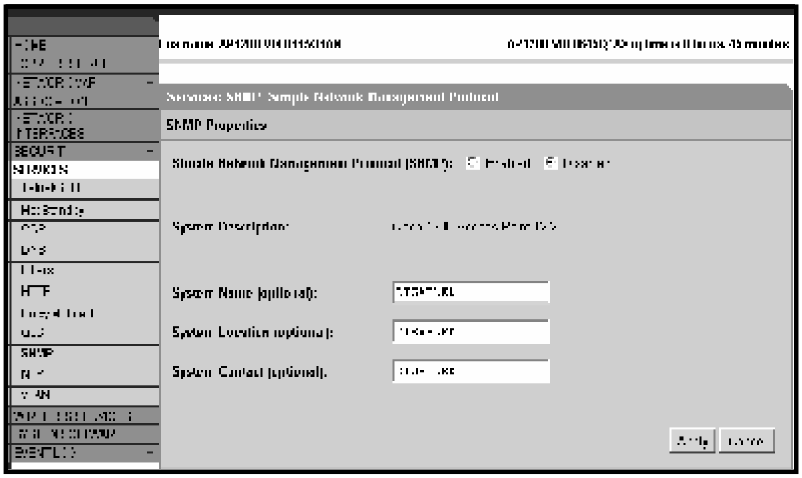
© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—8-95

This page configures this access point to work with your network administrator’s Simple Network Management Protocol (SNMP) station. In addition to enabling SNMP, you must create a user with the SNMP capability to serve as an SNMP community.

- **Simple Network Management Protocol**: This setting must be enabled to use SNMP.
- **System Description**: The system’s device type as listed at the bottom of the page.
- **System Name:** The name of this access point. This will be reported to your SNMP management station as the name of the device when you are using SNMP to communicate.
- **System Location**: Enter the location of this access point, such as a building name or other identifier.
- **System Contact**: Enter the name of the System Administrator responsible for this access point.
- **SNMP Trap Destination**: The IP address of the SNMP management station. If using DNS, enter a host name that would resolve into an IP address.
- **SNMP Trap Community**: The SNMP community name required by the Trap Destination before it will record traps sent by the access point.
- **Browse Management Information Base (MIB)**: This link allows direct browsing of named objects in the access point’s MIB.

SNMP (Cont.)



Services: SNMP - Simple Network Management Protocol

SNMP Properties

Simple Network Management Protocol (SNMP): ○ Enabled ● Disabled

System Description:

System Name (optional):

System Location (optional):

System Contact (optional):

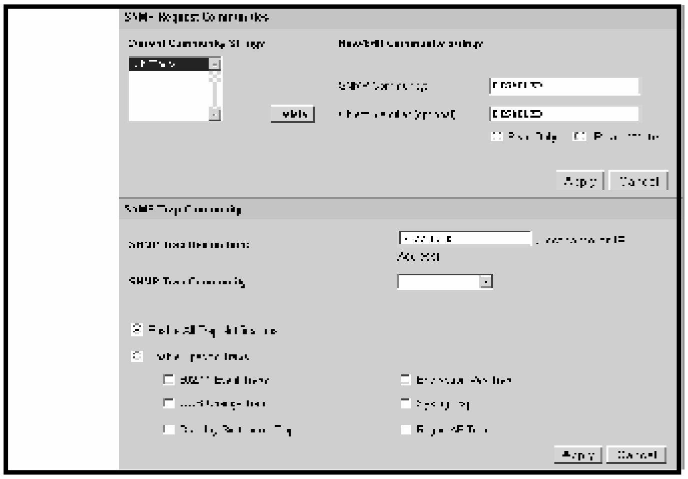
Simple Network Management Protocol (SNMP) is enabled from the Services> SNMP menu selection.

The system information (**System Name, System Location, and System Contact**) for the AP which the AP sends to the SNMP management station for SNMPqueries is configured or queried from this interface.

SNMP (Cont.)

Cisco.com

Lower portion of screen



AWLF v3.1—8-97

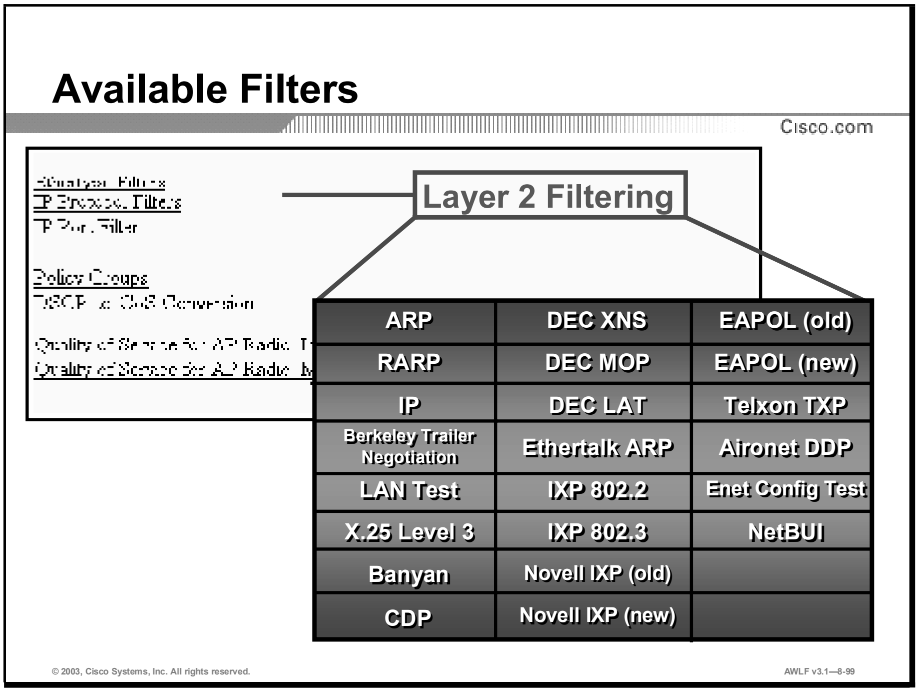
From the lower section of the SNMP service screen, the specific parameters used by the AP for SNMP messaging are configured.

The **SNMP Community** string(s) used to communicate with SNMP management entities is configured from this screen.

The **SNMP Trap Destination**, which is the Network Management station used to collect SNMP “traps” or defined system performance or exception thresholds is configured here. An **SNMP Trap Community** string is also used to make sure that the Trap destination has the correct string to accept SNMP traps from the AP.

In addition, the specific events which trigger an SNMP trap are specified from this interface.

Filtering



Available Filters

Cisco.com

Ethertype Filters
IP Protocol Filters
IP Port Filter

Policy Groups
DSCP to CoS Conversion

Quality of Service for AP Radio T
Quality of Service for AP Radio M

Layer 2 Filtering

ARP	DEC XNS	EAPOL (old)
RARP	DEC MOP	EAPOL (new)
IP	DEC LAT	Telxon TXP
Berkeley Trailer Negotiation	Ethertalk ARP	Aironet DDP
LAN Test	IXP 802.2	Enet Config Test
X.25 Level 3	IXP 802.3	NetBUI
Banyan	Novell IXP (old)	
CDP	Novell IXP (new)	

© 2003, Cisco Systems, Inc. All rights reserved.

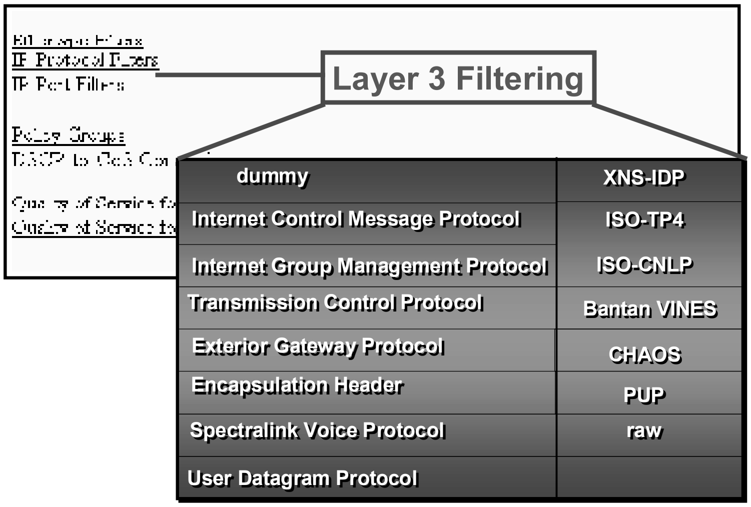
AWLF v3.1—8-99

Access points with v11.0 or higher VxWorks and all versions of IOS firmware have the ability to use filtering options. This might be done to preserve wireless bandwidth and improve WLAN performance. There is no latency associated with filtering due to faster processing and more RAM on the access points.

To access the Protocol Filter Lists, go to the following URL:

- VxWorks:
  http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/accsspts/ap350scg/ap350axa.htm#wp997996
- IOS:
  http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo1100/accsspts/i12211ja/i12211sc/s11prof.htm#58801

Available Filters (Cont.)

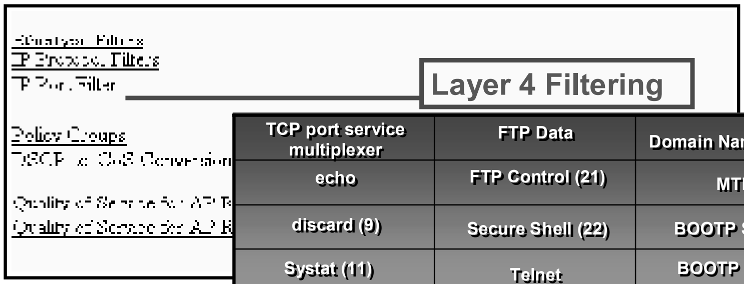


dummy	XNS-IDP
Internet Control Message Protocol	ISO-TP4
Internet Group Management Protocol	ISO-CNLP
Transmission Control Protocol	Bantan VINES
Exterior Gateway Protocol	CHAOS
Encapsulation Header	PUP
Spectralink Voice Protocol	raw
User Datagram Protocol	

AWLF v3.1—8-100

Available Filters (Cont.)

Cisco.com



Ethertype Filters
IP Protocol Filters
IP Port Filter

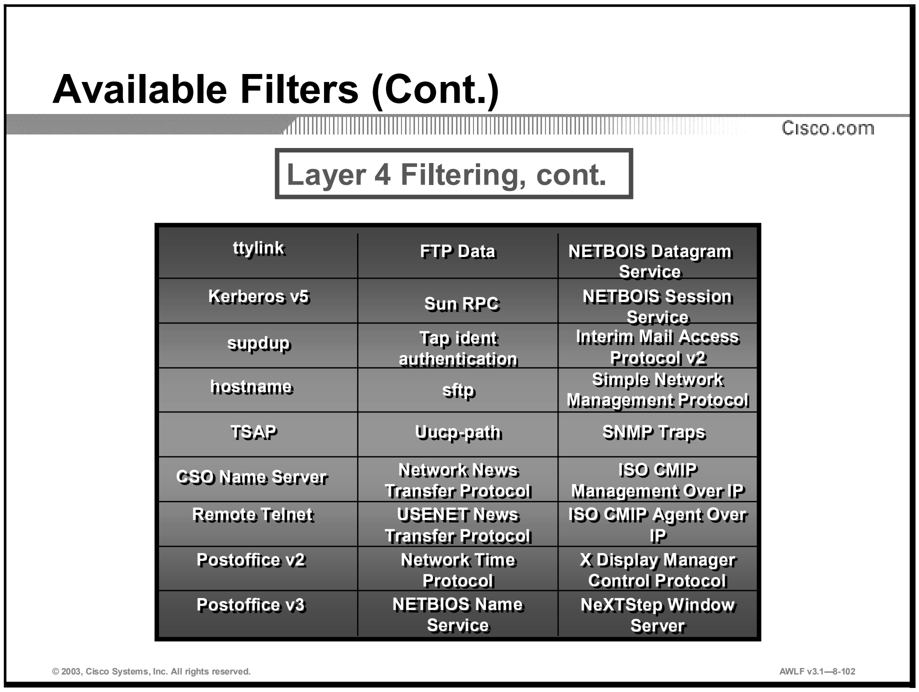
Policy Groups
DSCP to CoS Conversion

Quality of Service for AP T
Quality of Service for AP R

Layer 4 Filtering

TCP port service multiplexer	FTP Data	Domain Name Server
echo	FTP Control (21)	MTP
discard (9)	Secure Shell (22)	BOOTP Server
Systat (11)	Telnet	BOOTP Client
daytime (13)	Simplet Mail Transport Protocol	FTP
netstat (15)	time	gopher
Quote of the Day	Resource Location Protocol	rje
Message Send Protocol	IEN 116 Name Server	finger
Ttytst source	whois	Hypertext Transport Protocol

AWLF v3.1—8-101



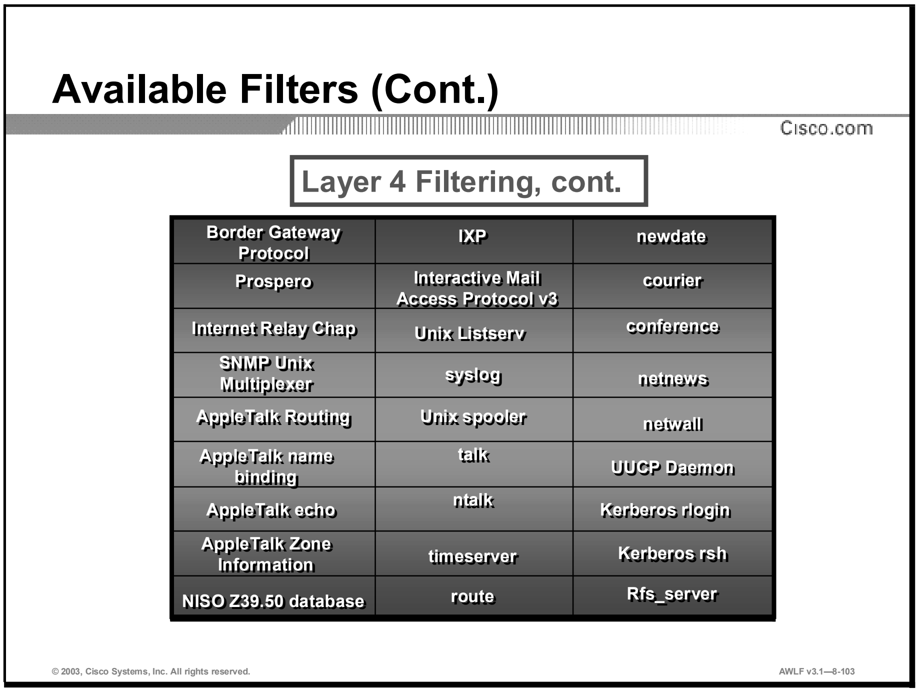
Available Filters (Cont.)

Cisco.com

Layer 4 Filtering, cont.

ttylink	FTP Data	NETBOIS Datagram Service
Kerberos v5	Sun RPC	NETBOIS Session Service
supdup	Tap ident authentication	Interim Mail Access Protocol v2
hostname	sftp	Simple Network Management Protocol
TSAP	Uucp-path	SNMP Traps
CSO Name Server	Network News Transfer Protocol	ISO CMIP Management Over IP
Remote Telnet	USENET News Transfer Protocol	ISO CMIP Agent Over IP
Postoffice v2	Network Time Protocol	X Display Manager Control Protocol
Postoffice v3	NETBIOS Name Service	NeXTStep Window Server

AWLF v3.1—8-102



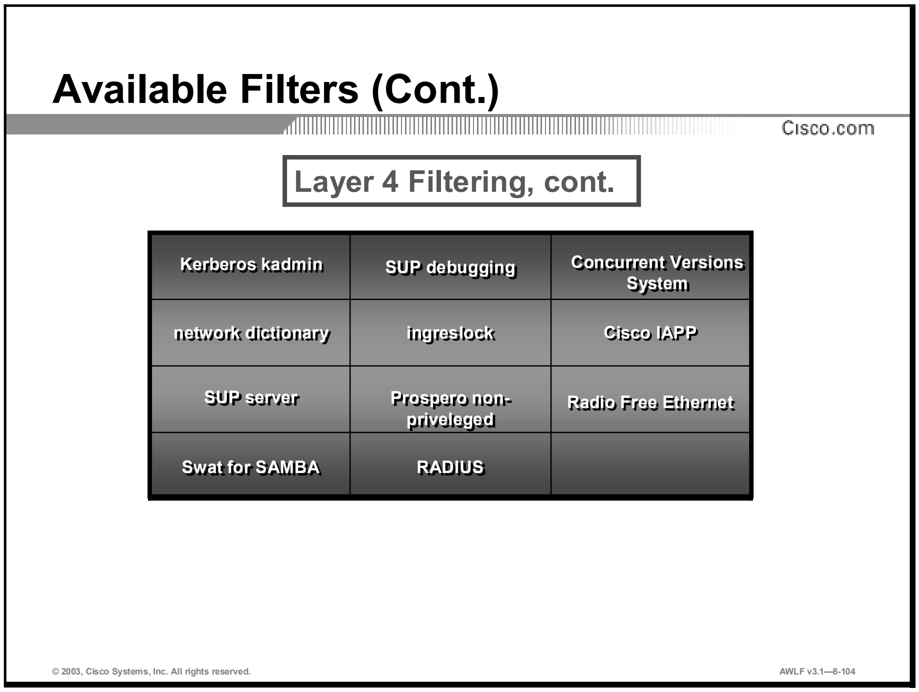
Available Filters (Cont.)

Cisco.com

Layer 4 Filtering, cont.

Border Gateway Protocol	IXP	newdate
Prospero	Interactive Mail Access Protocol v3	courier
Internet Relay Chap	Unix Listserv	conference
SNMP Unix Multiplexer	syslog	netnews
AppleTalk Routing	Unix spooler	netwall
AppleTalk name binding	talk	UUCP Daemon
AppleTalk echo	ntalk	Kerberos rlogin
AppleTalk Zone Information	timeserver	Kerberos rsh
NISO Z39.50 database	route	Rfs_server

AWLF v3.1—8-103



Available Filters (Cont.)

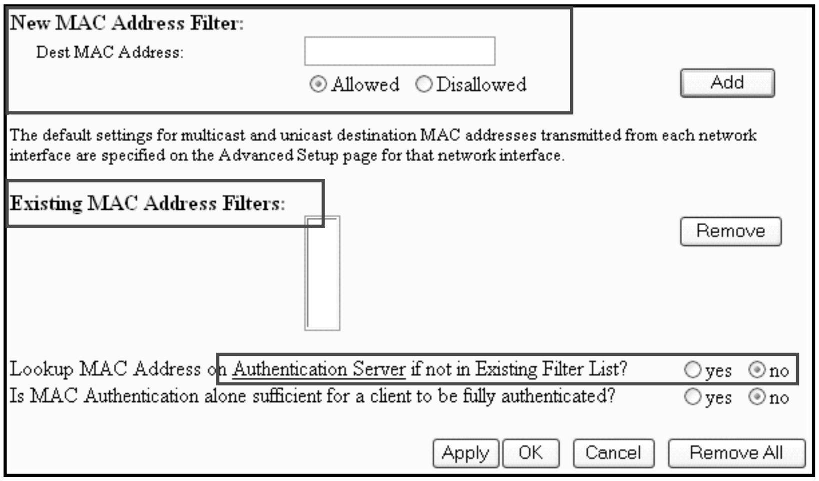
Cisco.com

Layer 4 Filtering, cont.

Kerberos kadmin	SUP debugging	Concurrent Versions System
network dictionary	ingreslock	Cisco IAPP
SUP server	Prospero non-priveleged	Radio Free Ethernet
Swat for SAMBA	RADIUS	

AWLF v3.1—8-104

MAC Address Filters



New MAC Address Filter:

Dest MAC Address:

● Allowed ○ Disallowed

The default settings for multicast and unicast destination MAC addresses transmitted from each network interface are specified on the Advanced Setup page for that network interface.

Existing MAC Address Filters:

Lookup MAC Address on Authentication Server if not in Existing Filter List? ○ yes ● no

Is MAC Authentication alone sufficient for a client to be fully authenticated? ○ yes ● no

AWLF v3.1—8-105

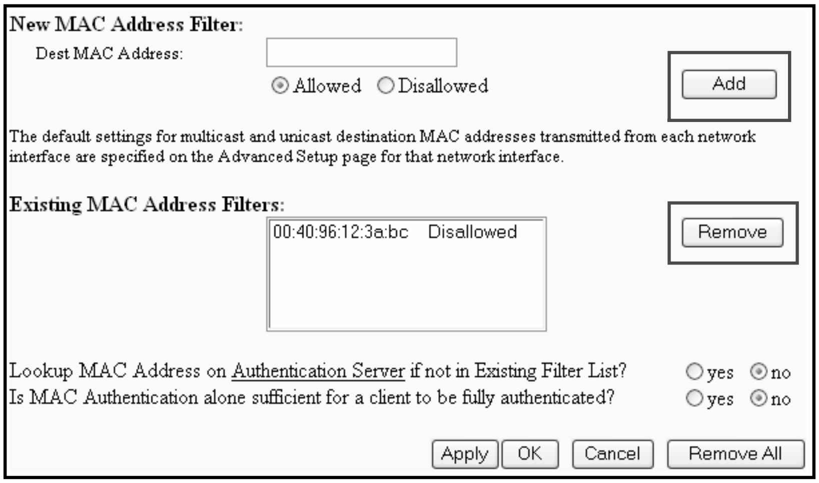
Use this page to allow or disallow the forwarding of packets containing specific MAC addresses.

Entering a new MAC address filter

- **Dest MAC Address:** Enter the destination of the new MAC address you want to establish as allowed or disallowed.
- **Allowed:** Enable Allowed if you want to forward all packets containing the destination MAC address.
- **Disallowed:** Enable Disallowed if you want to filter all packets containing the destination MAC address.
- **Existing MAC Address Filters:** Displays the added MAC address filter and labels it as allowed or disallowed.
- **Lookup MAC Address on Authentication Server if not in Existing Filter List?:** Check yes to allow the access point to use MAC address authentication with Cisco LEAP authentication. The access point will forward 802.1x packets to the configured authentication server for authentication.

Applied MAC Address Filter

Cisco.com


New MAC Address Filter:

Dest MAC Address:

● Allowed ○ Disallowed

The default settings for multicast and unicast destination MAC addresses transmitted from each network interface are specified on the Advanced Setup page for that network interface.

Existing MAC Address Filters:

00:40:96:12:3a:bc Disallowed

Lookup MAC Address on Authentication Server if not in Existing Filter List? ○ yes ● no

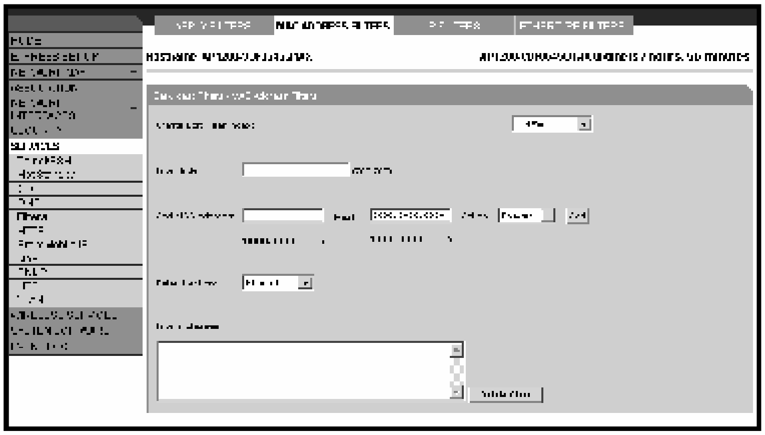
Is MAC Authentication alone sufficient for a client to be fully authenticated? ○ yes ● no

AWLF v3.1—8-106

- **Add/Remove*:*** Click **Add** to place the destination address into the Existing MAC Address Filters field. Click **Remove** to delete a highlighted MAC address filter from the Existing MAC Address Filters field.

MAC Address Filters

Cisco.com



AWLF v3.1—8-107

Use this page to allow or disallow the forwarding of packets containing specific MAC addresses.

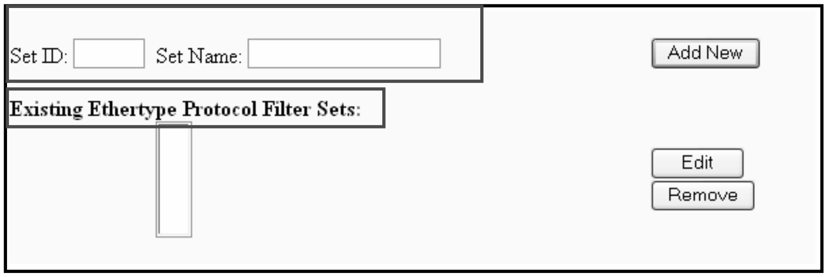
Entering a new MAC address filter

- **Create/Edit Filter Index**: Select <NEW> or select appropriate index to edit
- **Filter Index**: Enter a designator for the filter
- **Add MAC Address**: Specify MAC Address, Ethernet mask, and Action (Forward or block) for the entered MAC
- **Default Action**: Specify either Forward all or Block all
- **Filters Classes:** Displays configured filters after configuration

Note	Multiple MAC address filters may be aggregated to make up a MAC address filter Class.

Ethertype Protocol Filters

Cisco.com



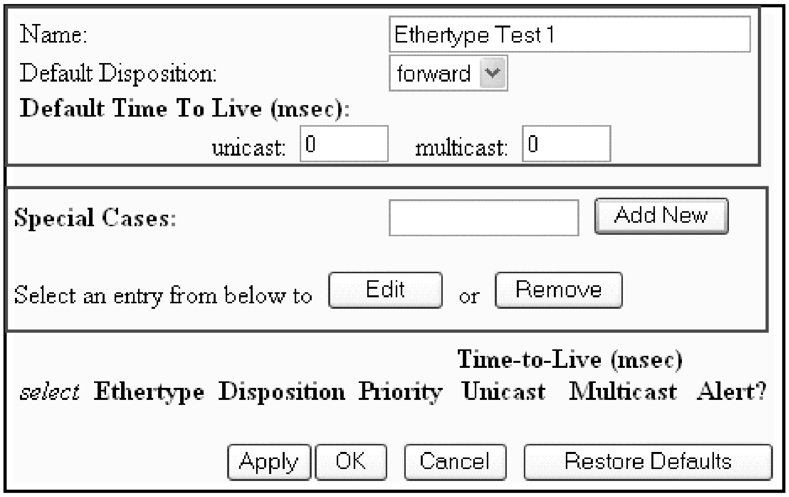
AWLF v3.1—8-108

Use this page to assign protocols to an Ethertype filter set.

- **Set ID:** Enter an identification number if you want to assign a specific SNMP identifier to the filter set. If you don't enter an ID, an SNMP identifier will be assigned to the set automatically, starting with 1 for the first filter set and incrementing by one for each additional set.
- **Set Name:** Enter a descriptive filter set name. The
- **Existing Ethertype Filter Set:** This portion of the screen shows the Ethertype filters that are currently set.

Adding Ethertype Protocol Filters

Cisco.com



Name: Ethertype Test 1

Default Disposition: forward

Default Time To Live (msec):

unicast: 0 multicast: 0

Special Cases:

Select an entry from below to Edit or Remove

				Time-to-Live (msec)		
select	**Ethertype**	**Disposition**	**Priority**	**Unicast**	**Multicast**	**Alert?**

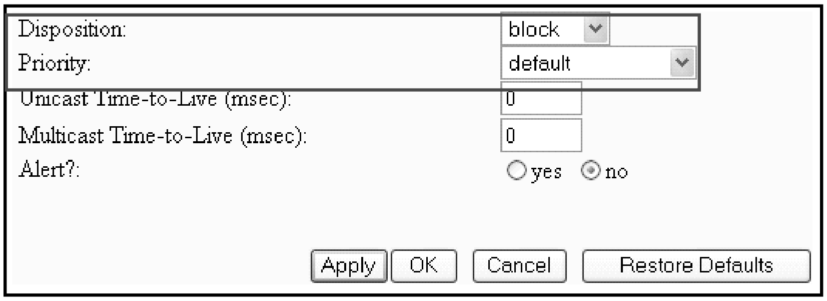
AWLF v3.1—8-109

This screen appears when you select Add New on the Ethertype Filters page.

- **Name:** Displays the name you entered in the Set Name field of the Ethertype Protocol Filters screens.
- **Default Disposition:** Select forward or block. This setting is the default action for the protocols you include in the filter set. You can override this setting for specific protocols.
- **Default Time to Live (msec): Unicast and Multicast;** Enter the number of milliseconds unicast and multicast packets should stay in the access point's buffer before they are discarded. These settings will be the default time-to-live values for the protocols you include in the filter set, but you can override the settings for specific protocols. If you leave these settings at 0, the time-to-live settings default to 3 seconds for multicast packets and 5 seconds for directed packets.
- **Special Cases:** Type the name or the ISO numeric designator for the protocol you want to add. Once you enter the name and click Add New, the Protocol Filter Set page appears.
- **Select an Entry from Below to Edit or Remove:** If you want to edit or remove a filter, click the appropriate Edit or Remove button.

Adding Ethertype Protocol Filters (Cont.)

Cisco.com



Disposition: block

Priority: default

Unicast Time-to-Live (msec): 0

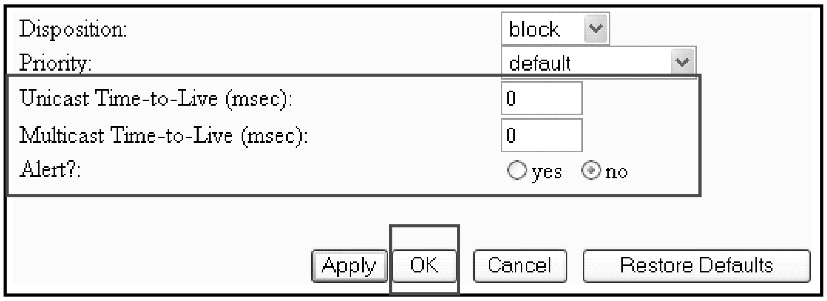
Multicast Time-to-Live (msec): 0

Alert?: ○ yes ● no

This screen appears when you select Add New on the Ethertype Filter Set page.

- **Disposition:** Select forward or block to determine how the protocol traffic is handled.
- **Priority:** Select a priority for the protocol. The menu includes the following options:
  - Background: Use this setting for bulk transfers and other activities that are allowed on the network but should not impact network use by other users and applications.
  - Default: This setting is the same as best effort, which applies to normal LAN traffic.
  - Excellent Effort: Use this setting for a network's most important users.
  - Controlled Load: Use this setting for important business applications that are subject to form of admission control.
  - Interactive Video: Use this setting for traffic with less than 100 ms delay
  - Interactive Voice: Use this setting for traffic with less than 10 ms delay
  - Network Control: Use this setting for traffic that must get through to maintain and support the network infrastructure

Adding Ethertype Protocol Filters (Cont.)



Disposition: block

Priority: default

Unicast Time-to-Live (msec): 0

Multicast Time-to-Live (msec): 0

Alert?: ○ yes ● no

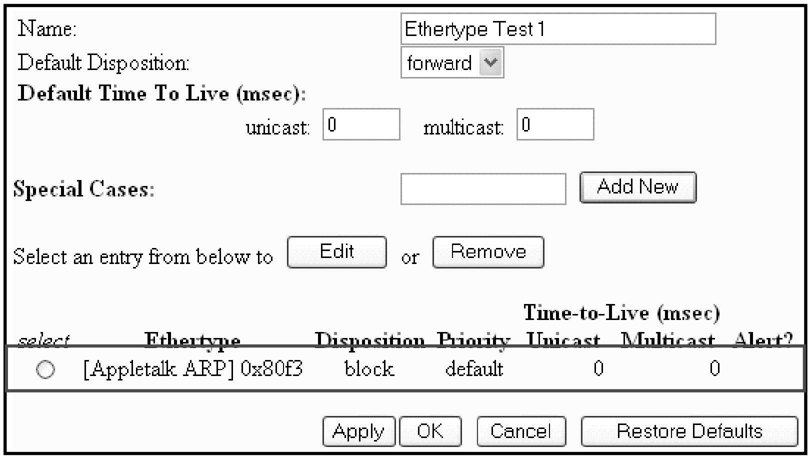
AWLF v3.1—8-111

- **Unicast Time to Live (msec):** Enter the number of milliseconds unicast packets should stay in the access point's buffer before they are discarded. These settings will be the default time-to-live values for the protocols you include in the filter set, but you can override the settings for specific protocols. If you leave these settings at 0, the protocol adopts the default time-to-live values.
- **Multicast Time to Live (msec):** Enter the number of milliseconds unicast packets should stay in the access point's buffer before they are discarded. These settings will be the default time-to-live values for the protocols you include in the filter set, but you can override the settings for specific protocols. If you leave these settings at 0, the protocol adopts the default time-to-live values.

  The time-to-live values you enter should be compatible with the priority you select for the protocol. For example, if you select interactive Voice as the priority and enter high time-to-live values, voice packets will stay in the access point buffer longer than necessary, causing delivery of stale, useless packets.
- **Alert?:** Select yes to send an alert to the event log when a user transmits or receives the protocol through the access point.
- Click **OK**.

Adding Ethertype Protocol Filters (Cont.)

Cisco.com



Name: Ethertype Test 1

Default Disposition: forward

Default Time To Live (msec):

unicast: 0 multicast: 0

Special Cases:

Select an entry from below to Edit or Remove

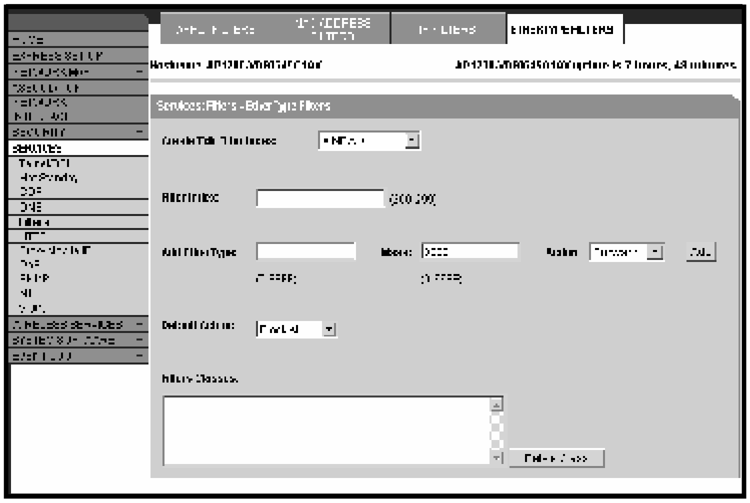
				Time-to-Live (msec)		
select	**Ethertype**	**Disposition**	**Priority**	**Unicast**	**Multicast**	**Alert?**
○	[Appletalk ARP] 0x80f3	block	default	0	0	

AWLF v3.1—8-112

The Filter Set page appears with the protocol listed at the bottom of the page.

Ethertype Filters

Cisco.com



Filter Index: (200-299)

Add Filter Type: (0-FFFF)   Mask: 0000 (0-FFFF)   Action   Add

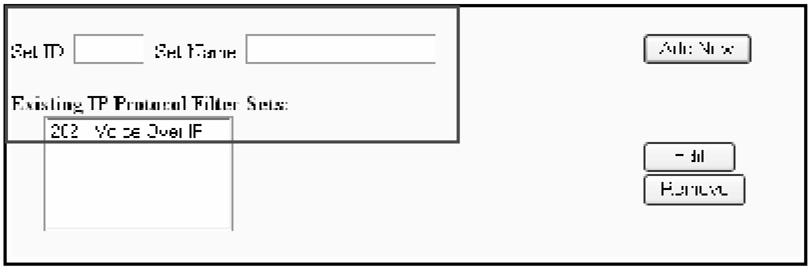
Default Action:

Filters Classes:

AWLF v3.1—8-113

IP Protocol Filter Sets

Cisco.com



Set ID   Set Name

Existing IP Protocol Filter Sets:

202   Voice Over IP

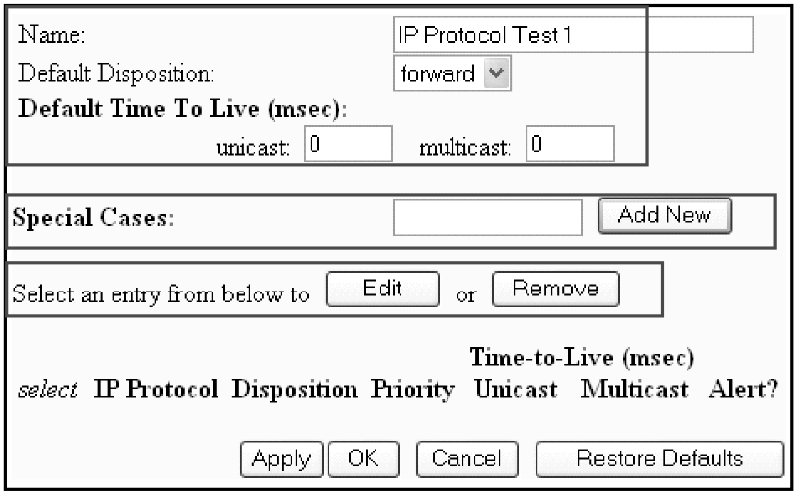
AWLF v3.1—8-114

Use this page to assign protocols to an IP Protocol filter set.

- **Set ID:** Enter an identification number if you want to assign a specific SNMP identifier to the filter set. If you don’t enter an ID, an SNMP identifier will be assigned to the set automatically, starting with 1 for the first filter set and incrementing by one for each additional set.
- **Set Name:** Enter a descriptive filter set name.
- **Existing IP Protocol Filter Set:** This portion of the screen shows the Ethertype filters that are currently set.

Adding IP Protocol Filters

Cisco.com



Name: IP Protocol Test 1

Default Disposition: forward

Default Time To Live (msec):

unicast: 0 multicast: 0

Special Cases:

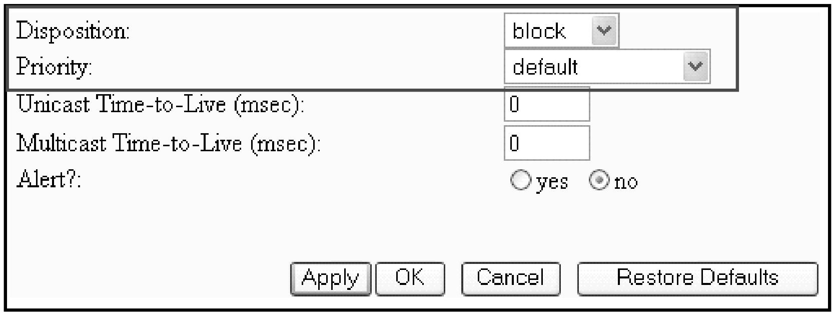
Add New
Select an entry from below to Edit or Remove
select IP Protocol Disposition Priority Time-to-Live (msec) Unicast Multicast Alert?
Apply
OK
Cancel
Restore Defaults

AWLF v3.1—8-115

This screen appears when you select Add New on the IP Protocols Filters page.

- **Name:** Displays the name you entered in the Set Name field of the Ethertype Protocol Filters screens.
- **Default Disposition:** Select forward or block. This setting is the default action for the protocols you include in the filter set. You can override this setting for specific protocols.
- **Default Time to Live (msec): Unicast and Multicast;** Enter the number of milliseconds unicast and multicast packets should stay in the access point's buffer before they are discarded. These settings will be the default time-to-live values for the protocols you include in the filter set, but you can override the settings for specific protocols. If you leave these settings at 0, the time-to-live settings default to 3 seconds for multicast packets and 5 seconds for directed packets.
- **Special Cases:** Type the name or the ISO numeric designator for the protocol you want to add. Once you enter the name and click Add New, the Protocol Filter Set page appears.
- **Select an Entry from Below to Edit or Remove:** If you want to edit or remove a filter, click the appropriate Edit or Remove button.

Adding IP Protocol Filters (Cont.)



Disposition: block

Priority: default

Unicast Time-to-Live (msec): 0

Multicast Time-to-Live (msec): 0

Alert?: ○ yes ● no

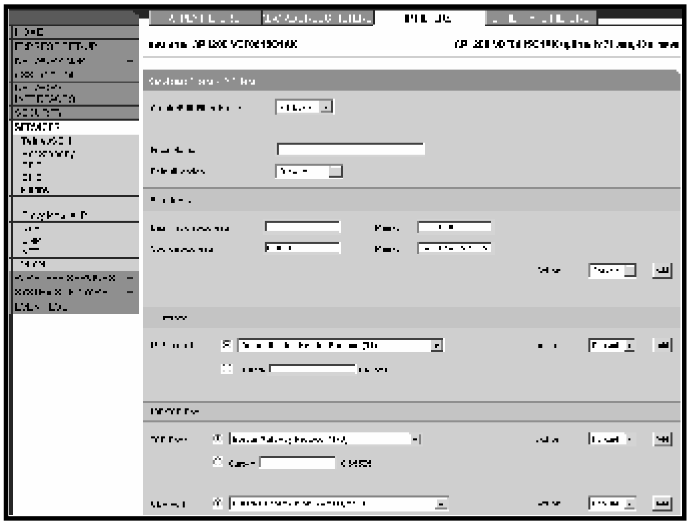
AWLF v3.1—8-116

This screen appears when you select Add New on the IP Protocol Filter Set page.

- **Disposition:** Select forward or block to determine how the protocol traffic is handled.
- **Priority;** Select a priority for the protocol. The menu includes the following options:
  - Background: Use this setting for bulk transfers and other activities that are allowed on the network but should not impact network use by other users and applications
  - Default: This setting is the same as best effort, which applies to normal LAN traffic.
  - ExcellentEffort: Use this setting for a network's most important users.
  - ControlledLoad: Use this setting for important business applications that are subject to form of admission control.
  - InteractiveVideo: Use this setting for traffic with less than 100 ms delay
  - InteractiveVoice: Use this setting for traffic with less than 10 ms delay
  - NetworkControl: Use this setting for traffic that must get through to maintain and support the network infrastructure

IP Protocol and Port Filters

Cisco.com



© 2003, Cisco Systems, Inc. All rights reserved.

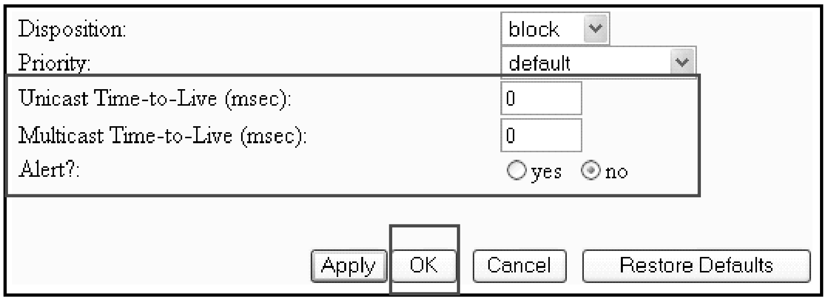
AWLF v3.1—8-117

IP Protocol and Port Filters may be defined for the following categories:

- **IP Address-** Configure Destination/ source address and disposition of filter to either block or forward traffic to specified IP address(es).
- **IP Protocol-** Configure IP Protocol and disposition of filter to either block or forward traffic to/from specified IP port.
- **UDP/ TCP Port-** Configure UDP/TCP port number and disposition of filter to either block or forward traffic to/from specified UDP/TCP port.

Note	IP Address, IP Protocol, or TCP/UDP Port numbers may be either independently or grouped to configure filter classes. Via this mechanism, either specific IP address ranges or specific protocols or a combination of address & protocol may be used to either restrict or grant access to the AP.

Adding Ethertype Protocol Filters (Cont.)



Disposition: block

Priority: default

Unicast Time-to-Live (msec): 0

Multicast Time-to-Live (msec): 0

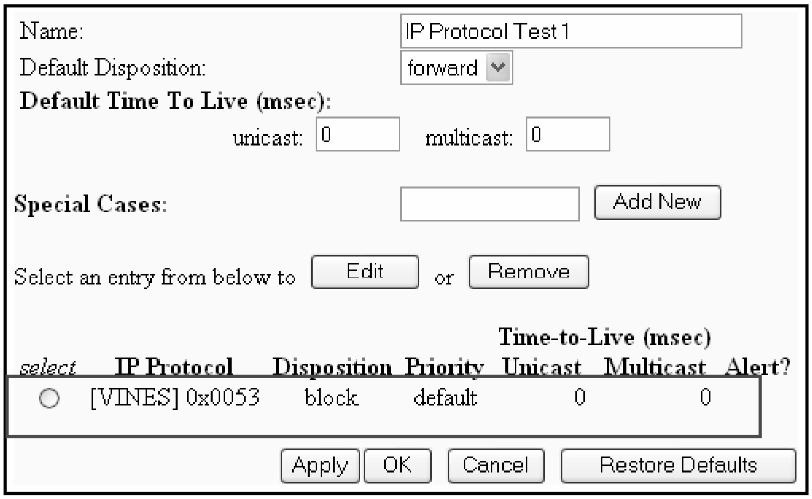
Alert?: ○ yes ● no

- **Unicast Time to Live (msec):** Enter the number of milliseconds unicast packets should stay in the access point's buffer before they are discarded. These settings will be the default time-to-live values for the protocols you include in the filter set, but you can override the settings for specific protocols. If you leave these settings at 0, the protocol adopts the default time-to-live values.
- **Multicast Time to Live (msec):** Enter the number of milliseconds unicast packets should stay in the access point's buffer before they are discarded. These settings will be the default time-to-live values for the protocols you include in the filter set, but you can override the settings for specific protocols. If you leave these settings at 0, the protocol adopts the default time-to-live values.

  The time-to-live values you enter should be compatible with the priority you select for the protocol. For example, if you select interactive Voice as the priority and enter high time-to-live values, voice packets will stay in the access point buffer longer than necessary, causing delivery of stale, useless packets.
- **Alert?:** Select yes to send an alert to the event log when a user transmits or receives the protocol through the access point.
- Click **OK**.

Adding IP Protocol Filters (Cont.)

Cisco.com



Name: IP Protocol Test 1

Default Disposition: forward

Default Time To Live (msec):

unicast: 0 multicast: 0

Special Cases:

Select an entry from below to

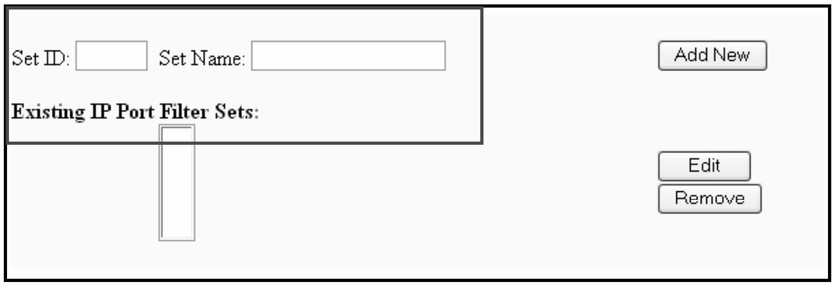
or

				Time-to-Live (msec)		
select	**IP Protocol**	**Disposition**	**Priority**	**Unicast**	**Multicast**	**Alert?**
○	[VINES] 0x0053	block	default	0	0	

The Filter Set page appears with the protocol listed at the bottom of the page.

IP Port Filter Sets

Cisco.com



Set ID: Set Name:

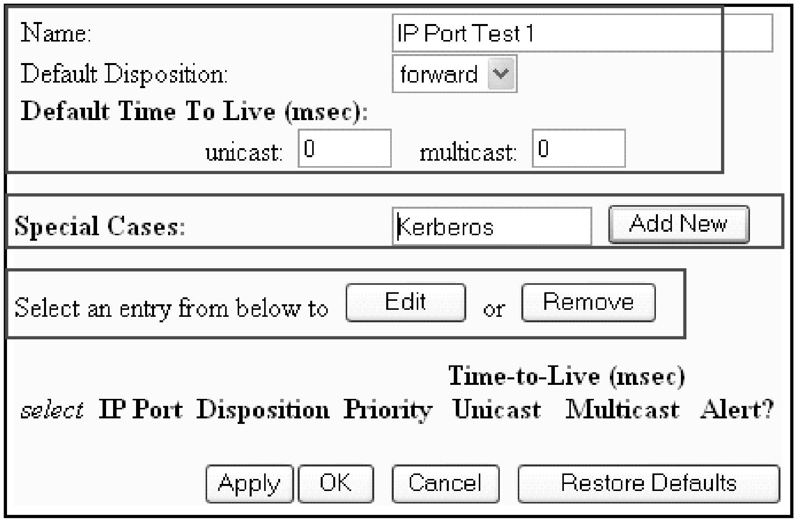
Existing IP Port Filter Sets:

AWLF v3.1—8-120

Use this page to assign protocols to an Ethertype filter set.

- **Set ID:** Enter an identification number if you want to assign a specific SNMP identifier to the filter set. If you don't enter an ID, an SNMP identifier will be assigned to the set automatically, starting with 1 for the first filter set and incrementing by one for each additional set.
- **Set Name:** Enter a descriptive filter set name.
- **Existing IP Port Filter Set:** This portion of the screen shows the Ethertype filters that are currently set.

Adding IP Port Filters (Cont.)



Name: IP Port Test 1

Default Disposition: forward

Default Time To Live (msec):

unicast: 0 multicast: 0

Special Cases: Kerberos

Select an entry from below to Edit or Remove

				Time-to-Live (msec)		
select	IP Port	Disposition	Priority	Unicast	Multicast	Alert?

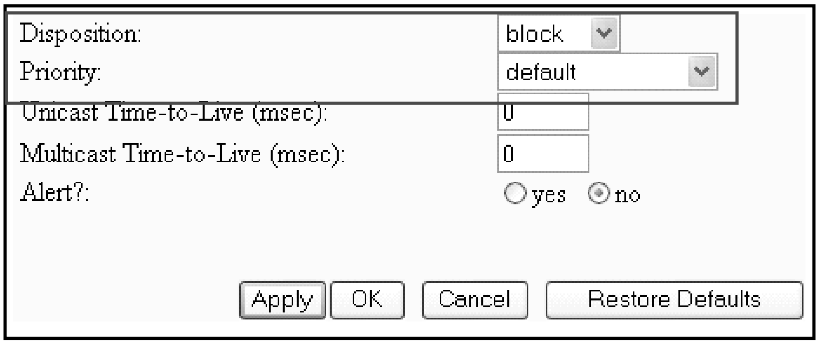
© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—8-121

This screen appears when you select Add New on the IP Port Filters page.

- **Name:** Displays the name you entered in the Set Name field of the Ethertype Protocol Filters screens.
- **Default Disposition:** Select forward or block. This setting is the default action for the protocols you include in the filter set. You can override this setting for specific protocols.
- **Default Time to Live (msec): Unicast and Multicast;** Enter the number of milliseconds unicast and multicast packets should stay in the access point's buffer before they are discarded. These settings will be the default time-to-live values for the protocols you include in the filter set, but you can override the settings for specific protocols. If you leave these settings at 0, the time-to-live settings default to 3 seconds for multicast packets and 5 seconds for directed packets.
- **Special Cases:** Type the name or the ISO numeric designator for the protocol you want to add. Once you enter the name and click Add New, the Protocol Filter Set page appears.
- **Select an Entry from Below to Edit or Remove:** If you want to edit or remove a filter, click the appropriate Edit or Remove button.

Adding IP Port Filters (Cont.)



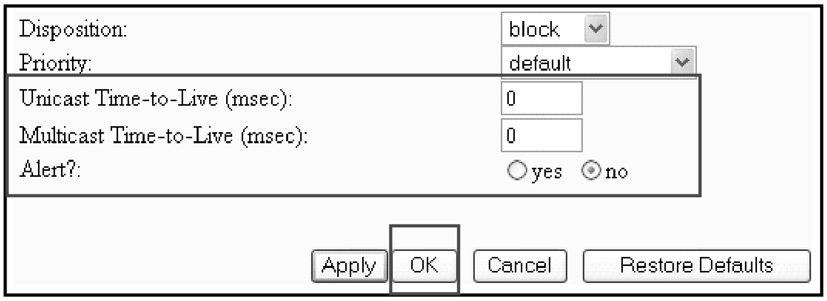
Disposition:	block
Priority:	default
Unicast Time-to-Live (msec):	0
Multicast Time-to-Live (msec):	0
Alert?:	○ yes ● no

AWLF v3.1—8-122

This screen appears when you select Add New on the IP Port Filter Set page.

- **Disposition**: Select forward or block to determine how the protocol traffic is handled.
- **Priority**: Select a priority for the protocol. The menu includes the following options:
  - Background**:** Use this setting for bulk transfers and other activities that are allowed on the network but should not impact network use by other users and applications
  - Default: This setting is the same as best effort, which applies to normal LAN traffic.
  - Excellent Effort: Use this setting for a network’s most important users.
  - Controlled Load: Use this setting for important business applications that are subject to form of admission control.
  - Interactive Video: Use this setting for traffic with less than 100 ms delay
  - Interactive Voice: Use this setting for traffic with less than 10 ms delay
  - Network Control: Use this setting for traffic that must get through to maintain and support the network infrastructure

Adding Ethertype Protocol Filters (Cont.)



Disposition: block

Priority: default

Unicast Time-to-Live (msec): 0

Multicast Time-to-Live (msec): 0

Alert?: ○ yes ● no

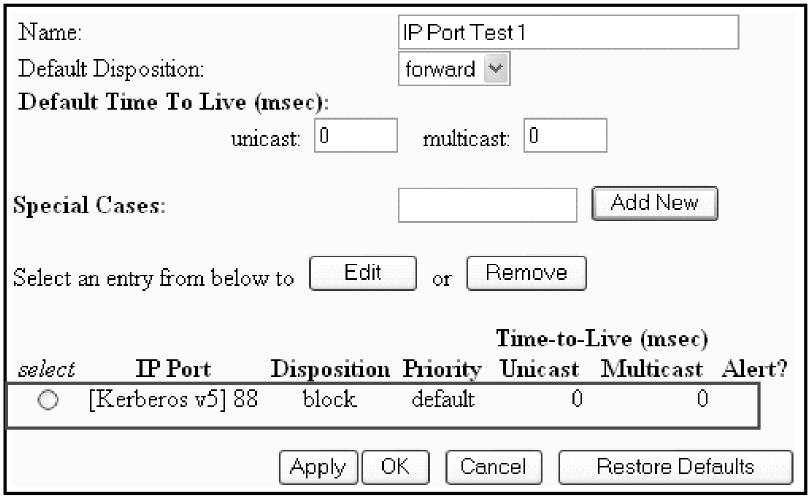
AWLF v3.1—8-123

- **Unicast Time to Live (msec):** Enter the number of milliseconds unicast packets should stay in the access point's buffer before they are discarded. These settings will be the default time-to-live values for the protocols you include in the filter set, but you can override the settings for specific protocols. If you leave these settings at 0, the protocol adopts the default time-to-live values.
- **Multicast Time to Live (msec):** Enter the number of milliseconds unicast packets should stay in the access point's buffer before they are discarded. These settings will be the default time-to-live values for the protocols you include in the filter set, but you can override the settings for specific protocols. If you leave these settings at 0, the protocol adopts the default time-to-live values.

  The time-to-live values you enter should be compatible with the priority you select for the protocol. For example, if you select interactiveVoice as the priority and enter high time-to-live values, voice packets will stay in the access point buffer longer than necessary, causing delivery of stale, useless packets.
- **Alert?:** Select yes to send an alert to the event log when a user transmits or receives the protocol through the access point.
- Click **OK**.

Adding IP Port Filters (Cont.)

Cisco.com



Name: IP Port Test 1

Default Disposition: forward

Default Time To Live (msec):

unicast: 0 multicast: 0

Special Cases:

Select an entry from below to Edit or Remove

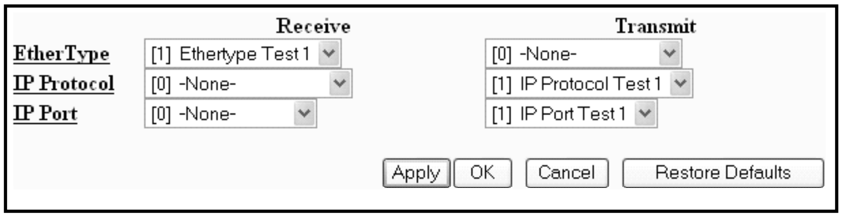
				Time-to-Live (msec)		
select	**IP Port**	**Disposition**	**Priority**	**Unicast**	**Multicast**	**Alert?**
○	[Kerberos v5] 88	block	default	0	0	

AWLF v3.1—8-124

The Filter Set page appears with the protocol listed at the bottom of the page.

Applying Filters

Cisco.com



	Receive	Transmit
EtherType	[1] Ethertype Test 1	[0] -None-
IP Protocol	[0] -None-	[1] IP Protocol Test 1
IP Port	[0] -None-	[1] IP Port Test 1

AWLF v3.1—8-125

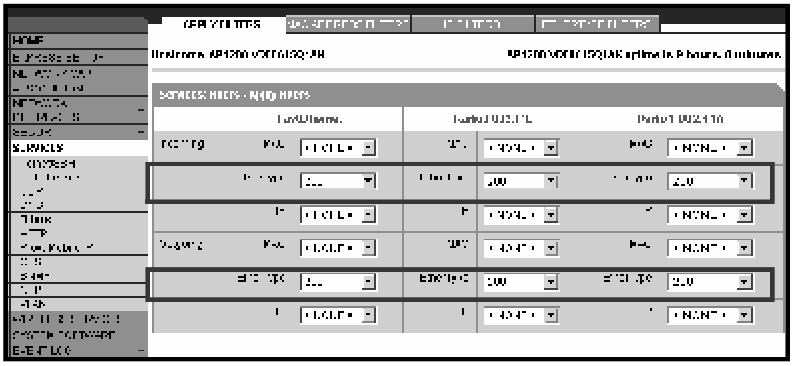
Once filter sets have been created, they will have to be enabled.

If VLANs are being implemented on the access point, they must be enabled in policy groups which are assigned to each VLAN. See VLAN configuration for details on this. If VLANs are not being implemented on the access point, filter sets can be enabled on the Ethernet port, the Radio port, or both. From the Setup menu, under Network Ports, click either the Ethernet or the access point Radio Filters link (the example shown in the slide is the access point Radio Filters menu). This will take you to the Filters page for that port. From the drop-down menus, choose the filter set(s) that you want to enable, and then click Apply or OK. You may choose to apply the filter sets to the receive port, the transmit port, or both.

Once the filters are applied, an edit link appears next to each filter. Clicking this link will take you to the menu for that filter set and allow you to edit the filter set.

Applying Filter

Cisco.com



AWLF v3.1—8-126

After creation of Filter on applicable Filters page.

Apply filter Index to appropriate incoming/ outgoing interfaces.

Note that this has the same effect as applying access lists to bridge group and interfaces associated with that bridge group, e.g.,

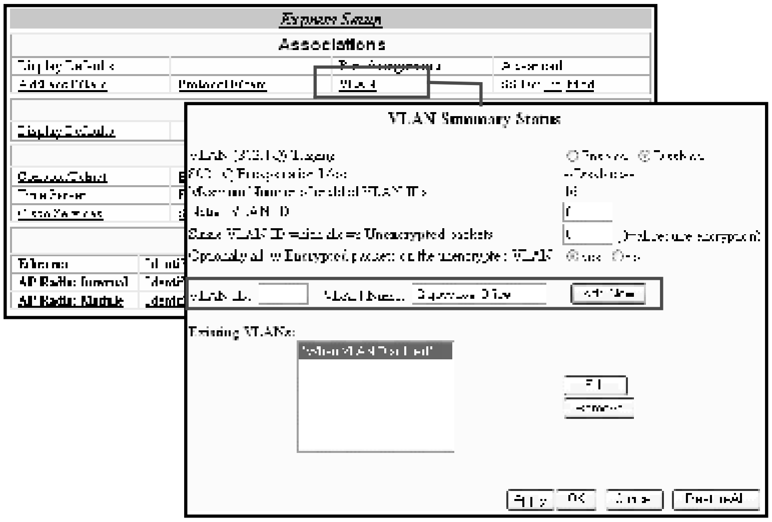
Example IOS configuration:

- global:
  - access-list 200 deny 0x80F3 0x0000
  - access-list 200 permit 0x0000 0xFFFF
- per interface:
  - bridge-group 1 input-type-list 200
  - bridge-group 1 output-type-list 200

VLAN Configuration

VLAN Setup

Cisco.com



Express Setup

Associations

VLAN Summary Status

VLAN (802.1Q) Tagging ○ Enabled ● Disabled

802.1Q Encapsulation Mode <Disabled>

Maximum Number of Enabled VLAN IDs 16

Native VLAN ID

Same VLAN ID ... Unencrypted packets

Optionally allow Encrypted packets on the unencrypted VLAN ● Yes ○ No

VLAN ID: VLAN Name: Add New

Existing VLANs:

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—8-128

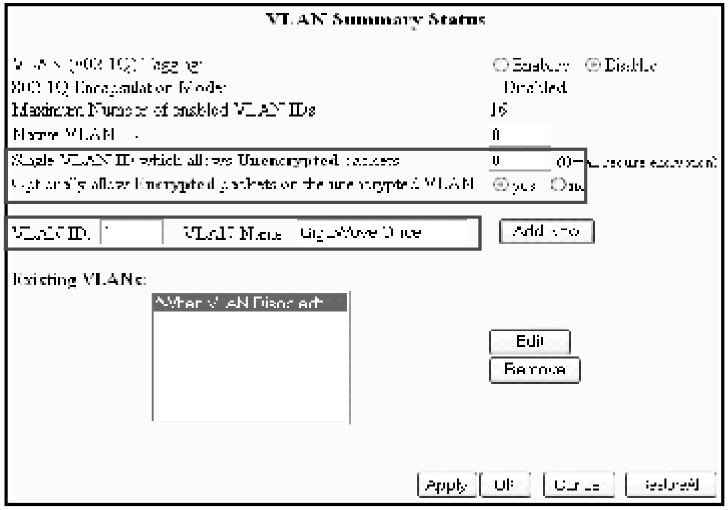
VLAN Summary Status

Click the link to access the VLAN Summary Status page, which lists the VLANs created on this access point.

- **VLAN (802.1Q) Tagging:** This setting determines whether the IEEE 802.1Q protocol is used to tag VLAN packets. IEEE 802.1Q protocol is used to connect multiple switches and routers and for defining VLAN topologies.
- **802.1Q Encapsulation Mode:** This setting indicates the presence of VLANs on the access point. When you create and enable a VLAN, this setting changes from Disabled to Hybrid Trunk.
- **Maximum Number of Enabled VLAN IDs:** Indicates the maximum allowable number of VLANs for the access point. The current maximum is 16.
- **Native VLAN ID:** Indicates the identification number of the VLAN you designate as the Native VLAN.

VLAN Setup (Cont.)

Cisco.com



VLAN Summary Status

VLANs (802.1Q) Tagging ○ Enable ● Disable

802.1Q Encapsulation Mode Disabled

Maximum Number of enabled VLAN IDs 16

Native VLAN 0

Single VLAN ID which allows Unencrypted packets 0 (0=[illegible])

Optionally allow Encrypted packets on the unencrypted VLAN ● yes ○ no

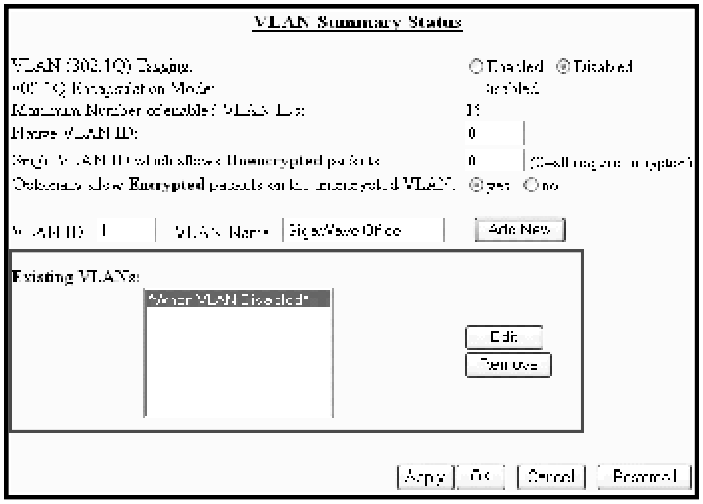
VLAN ID: 1 VLAN Name: GigaWave Office

AWLF v3.1—8-129

- **Single VLAN ID which allows Unencrypted packets:** Identifies the number of the VLAN on which unencrypted packets can pass between the access point and the switch. This setting is configurable.
- **Optionally allow Encrypted packets on the unencrypted VLAN:** Determines whether the access point passes encrypted packets on an unencrypted VLAN. This setting permits a client device to associate to the access point allowing both WEP and non-WEP associations.
- **VLAN ID:** A unique number that identifies a VLAN. This number must match VLANs set on the switch. The user configures the setting.
- **VLAN Name:** A unique name for a VLAN configured on the access point. The user configures this setting. The VLAN name is for information only and is not used by the switch or access point as a parameter for determining the destination of data.

VLAN Setup (Cont.)

Cisco.com



VLAN Summary Status

VLAN (802.1Q) Tagging: ○ Enabled ● Disabled

802.1Q Encapsulation Mode: Enabled

Maximum Number of enabled VLANs: 16

Native VLAN ID: 0

Single VLAN ID which allows Unencrypted packets: 0 (0=all traffic encrypted)

Clients allow Encrypted packets on the unencrypted VLAN: ● yes ○ no

VLAN ID: 1 VLAN Name: GigaWave Office

Existing VLANs: *Native VLAN Disabled*

AWLF v3.1—8-130

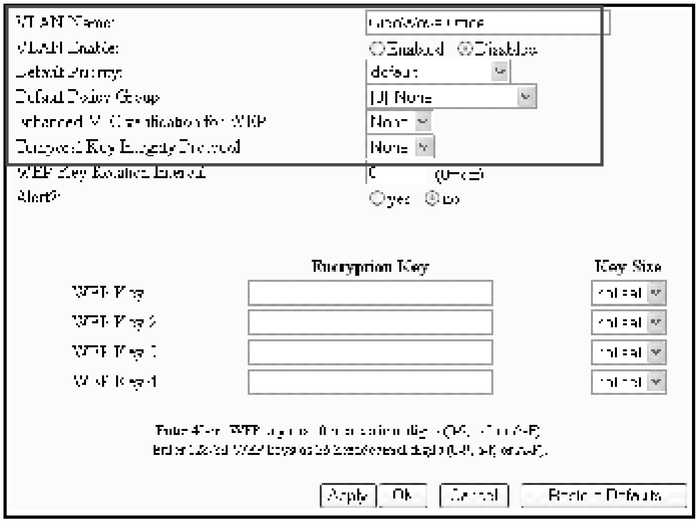
Existing VLANs

The window contains a list of VLANs created on this access point. Use the window as a starting point to edit or remove the VLAN you select.

- Click **Edit** to access the VLAN ID page for the highlighted VLAN.
- Click **Remov**e to remove a highlighted VLAN.

VLAN Setup (Cont.)

Cisco.com



VLAN Name: [illegible]

VLAN Enable: ○ Enabled ● Disabled

Default Priority: default

Default Policy Group: [0] None

Enhanced MIC Verification for WEP: None

Temporal Key Integrity Protocol: None

WEP Key Rotation Interval: 0 (0=off)

Alert? ○ yes ● no

	Encryption Key	Key Size
WEP Key 1		not set
WEP Key 2		not set
WEP Key 3		not set
WEP Key 4		not set

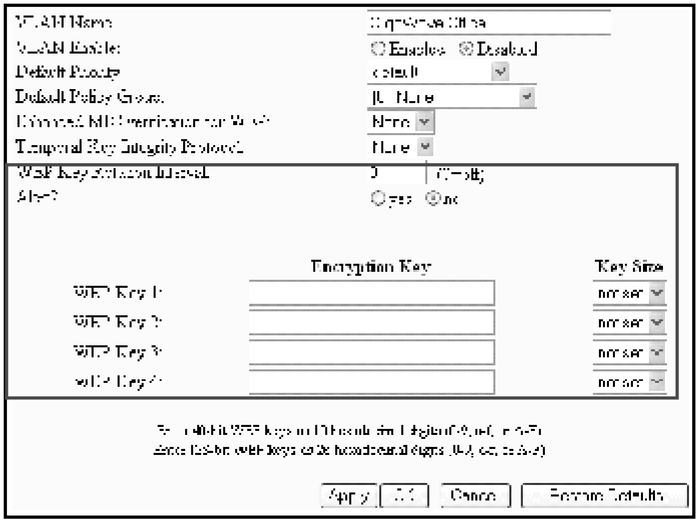
Enter 40-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F).
Enter 128-bit WEP keys as 26 hexadecimal digits (0-9, a-f, or A-F).

AWLF v3.1—8-131

- **VLAN Name:** The VLAN name.
- **VLAN Enable:** Enables or disables the VLAN.
- **Default Priority:** Use the drop-down menu to select the default priority you want the VLAN to use.
- **Default Policy Group:** Use the drop-down menu to assign a policy group (set of Layer 2, 3, and 4 filters) for each VLAN. Each filter within a policy group can be configured to allow or deny a certain type of traffic.
- **Enhanced MIC Verification for WEP:** This setting enables Message Integrity Check (MIC), a security feature that protects your WEP keys by preventing attacks on encrypted packets called *bit-flip* attacks. During a bit-flip attack, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receive accepts the retransmitted message as legitimate. The MIC, implemented on both the access point and all associated client devices, adds a few bytes to each packet to make the packets tamperproof. Select **MMH** from the drop-down menu to enable MIC or select **None**.
- **Temporal Key Integrity Protocol:** TKIP, also known as WEP key hashing, is an additional WEP security feature that defends against an attack on WEP in which the intruder uses an encrypted segment called the initialization vector (IV) in encrypted packets to calculate the WEP key. Use the drop-down menu to choose either **None** or **Cisco**.

VLAN Setup (Cont.)

Cisco.com



VLAN Name:	[illegible]
VLAN Enable:	○ Enabled ● Disabled
Default Priority:	default
Default Policy Group:	(0) None
Enhanced MIC Verification for WEP:	None
Temporal Key Integrity Protocol:	None
WEP Key Rotation Interval:	0 (0=off)
Alert?:	○ yes ● no

	Encryption Key	Key Size
WEP Key 1:		not set
WEP Key 2:		not set
WEP Key 3:		not set
WEP Key 4:		not set

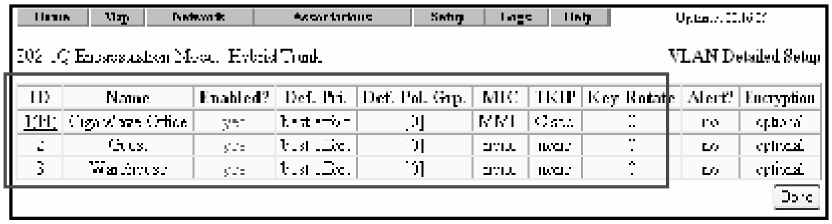
Enter 40-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F)
Enter 128-bit WEP keys as 26 hexadecimal digits (0-9, a-f, or A-F)

AWLF v3.1—8-132

- **WEP Key Rotation Interval:** This option enables broadcast key rotation by setting a key rotation interval. With broadcast, or multicast, WEP key rotation enabled, the access point provides a dynamic broadcast WEP key and changes it at the interval you select. To enable key rotation, enter the rotation interval in seconds. Enter a **0** to turn key rotation off.
- **Alert?:** Determine if you want to print the packet data to the console log for troubleshooting.
- **Encryption Key:** For 40-bit encryption, enter 10 hexadecimal digits; for 128-bit encryption, enter 26 hexadecimal digits. Hexadecimal digits include the numbers 0 through 9 and the letters A through F. The WEP key you use to transmit data must be set up exactly the same on your access point and any wireless devices with which it associates. For example, if you set WEP Key 3 on your wireless LAN adapter to 0987654321 and select it as the transmit key, you must also set WEP Key 3 on the access point to exactly the same value.
- **Key Size:** Use the drop-down menu to select **40-bit** or **128-bit** encryption for each key. The **not set** option clears the key. You can disable WEP altogether by selecting **not set** for each key.

VLAN Summary Status

Cisco.com



802.1Q Encapsulation Mode: Hybrid Trunk

VLAN Detailed Setup

ID	Name	Enabled?	Def. Pri.	Def. Pol. Grp.	MIC	TKIP	Key Rotate	Alert?	Encryption
1(N)	[illegible] Office	yes	Best Effort	[0]	MMH	Cisco	0	no	optional
2	Guest	yes	Best Effort	[0]	none	none	0	no	optional
3	Warehouse	yes	Best Effort	[0]	none	none	0	no	optional

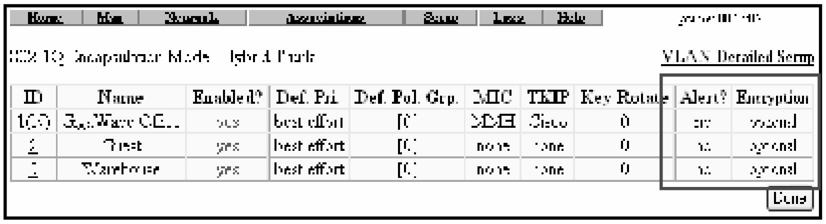
AWLF v3.1—8-133

This page displays a list of VLANs created on the access point. The list contains pertinent data about each VLAN.

- **ID:** The identification number of the VLAN.
- **Name:** The VLAN's name.
- **Enabled?:** The status of the VLAN.
- **Def. Pri.:** The QoS setting for the VLAN.
- **Def. Pol. Grp.:** The default policy group for the VLAN. 0 = no policy group
- **MIC:** Determines whether MIC is being used on this VLAN.
- **TKIP:** Determines whether TKIP is being used on this VLAN.
- **Key Rotate:** Determines the interval that the WEP key will be rotated. The ability to enable WEP key rotation for each VLAN is supported only for wireless VLANs with IEEE 802.1X protocols enabled.

VLAN Summary Status (Cont.)

Cisco.com



[illegible]

802.1Q Encapsulation Mode: Hybrid Trunk

VLAN Detailed Setup

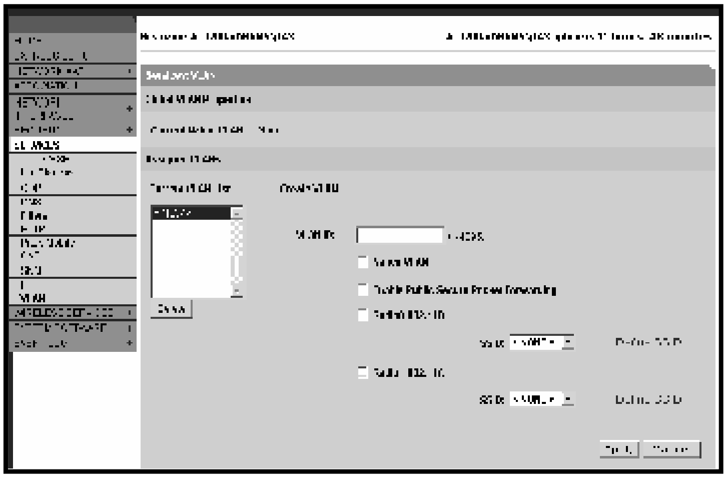
ID	Name	Enabled?	Def. Pri.	Def. Pol. Grp.	MIC	TKIP	Key Rotate	Alert?	Encryption
1(*)	GigaWare Ctl...	yes	best effort	[0]	MMH	Cisco	0	no	optional
2	Guest	yes	best effort	[0]	none	none	0	no	optional
3	Warehouse	yes	best effort	[0]	none	none	0	no	optional

AWLF v3.1—8-134

- **Alert?:** Determines if you want to print the packet data to the console log for troubleshooting.
- **Encryption:** Determines if the VLAN is using no encryption, optional, or full encryption.
  - **No encryption:** The device communicates only with client devices that are not using WEP.
  - **Optional**: Client devices can communicate with this access point or bridge either with or without WEP.
  - **Full encryption**: Client devices must use WEP when communicating with the access point or bridge. Devices not using WEP are not allowed to communicate.

VLAN Setup

Cisco.com



AWLF v3.1—8-135

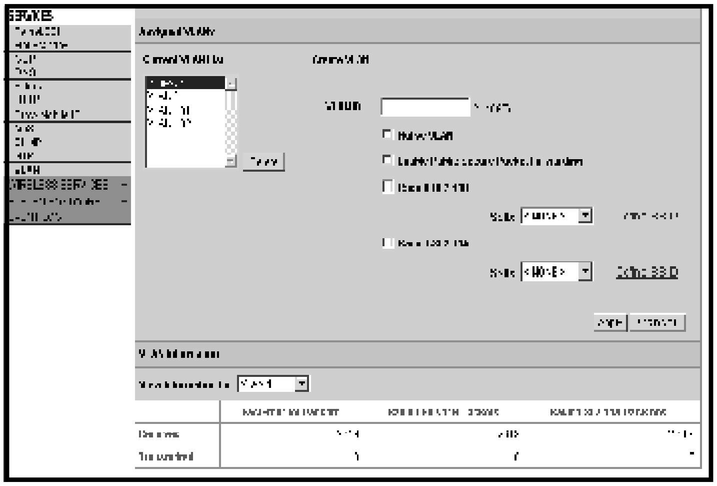
From Services> VLAN Menu tab, you are able to configure VLAN's on access point, which may then be assigned encryption policies and may have SSID's assigned.

Note that from "VLAN ID" textbox, the VLAN's are defined and are assigned as either:

- **Native VLAN**: This checkbox denotes the Native VLAN for the access point. Only one VLAN ID may be defined as the Native VLAN.
- **Enable Publicly Secure Packet Forwarding**: This checkbox permits the application of PSPF on each VLAN, as requirements dictate. PSPF prevents client devices from linking to other WLAN-associated client
- **Radio0-802.11B**: Assign VLAN to 802.11B interface
- **Radio1-802.11A**: Assign VLAN to 802.11A interface

VLAN Setup (Cont.)

Cisco.com

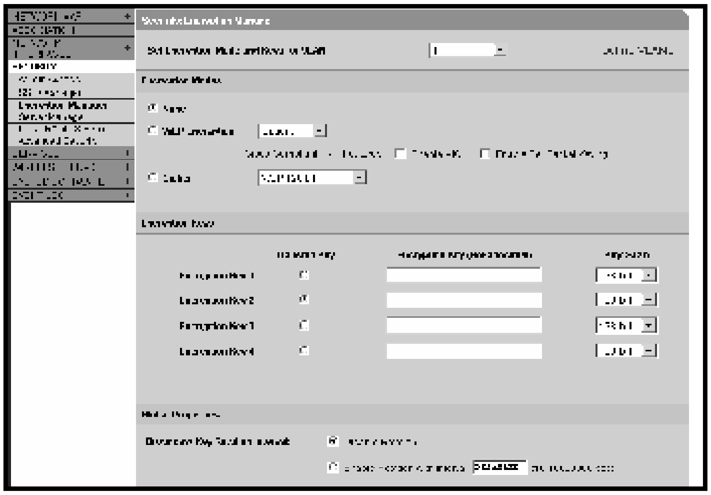


AWLF v3.1—8-136

After VLAN’s are defined from the “Assign VLAN” interface and they are assigned to Radio interfaces, the throughput statistics for the specified VLAN are visible form the “VLAN Information” menu at the bottom of the **VLAN Setup** screen. The transmit and receive statistics are obtainable for each interface and for each configured VLAN.

Encryption Manager

Cisco.com

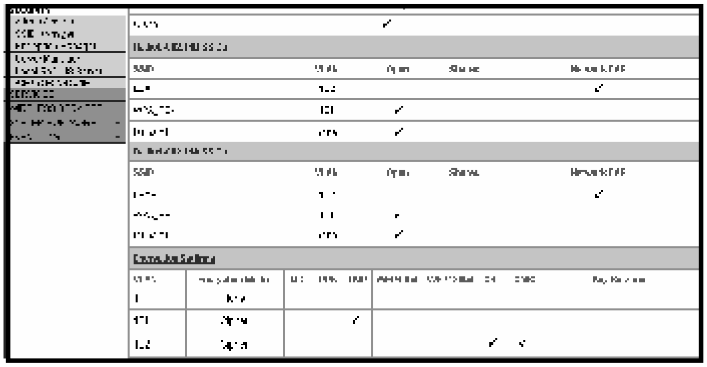


AWLF v3.1—8-137

Encryption Manager screen permits the assignment of Encryption parameters either globally, or per VLAN, dependent on whether VLAN function is enabled on AP.

- **Set Encryption Mode and Keys for VLAN** dropdown box is used to select VLAN for which encryption parameters are to be set
- **Encryption Modes** permits the assignment of:
- **None**: no encryption applied
- **WEP Encryption**: WEP encryption, either Mandatory or optional
- **Cipher**: WEP 128/40, TKIP, or CKIP/CMIP
- **Encryption Keys** permits the assignment of static WEP keys in each of the 4 encryption key fields
- **Global Properties** permits the configuration of the AP broadcast key operation:
- **Broadcast Key Rotation Interval** permits the definition of the interval at which the key used to encrypt broadcast traffic will be refreshed
- **WPA Group Key Update** permits the configuration of Group (broadcast) key negotiation, either 1) upon client association termination and/or 2) upon client capability change.

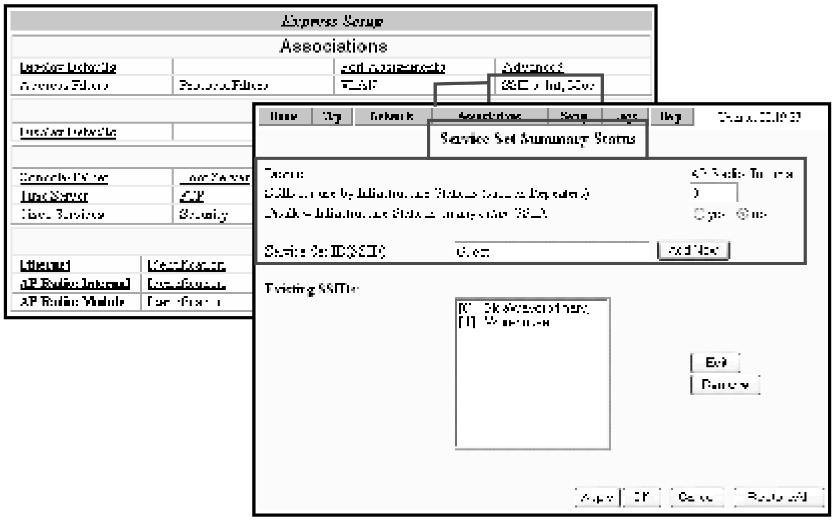
VLAN Summary Status



After configuration of VLAN, assignment of encryption parameters, and assignment of those encryption and VLAN parameters to an SSID, the details on the configured parameters are available in a tabular summary page from the “**Security**” menu tab.

Specific configured parameters, including **VLAN** and authentication methods configured for each SSID on each Radio interface, as well as **Encryption Settings** for each VLAN are visible from this screen.

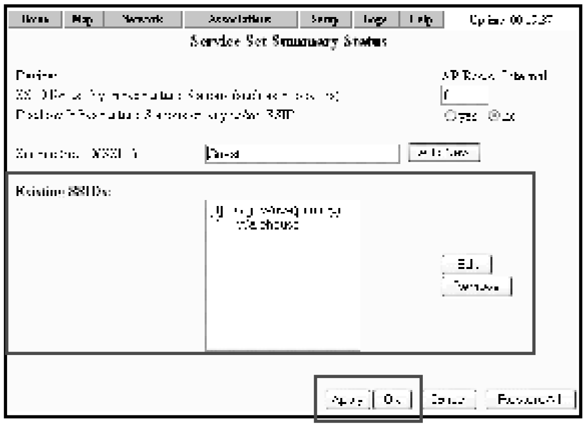
Assigning SSIDs to VLANs



Use this page to create multiple SSIDs. Click the **Service Set Summary Status** link to display a list of SSIDs created on the access point. The list also displays configuration information for each SSID.

- **Device:** This field is an information field that shows the device for which the settings on the page apply.
- **SSID for use by Infrastructure Stations (such as Repeaters):** This setting identifies the SSID to be used by repeaters and workgroup bridges to associate with the access point. It is also the SSID used by a non-root bridge to associate to a root bridge. The SSID should be mapped to the native VLAN ID in order to facilitate communications between infrastructure devices and a non-root access point or bridge.
- **Disallow Infrastructure Stations on any *other* SSID:** Prevents repeaters or workgroup bridges from associating to SSIDs other than the infrastructure SSID. The default setting is **No**, so to invoke this condition, you must change the setting to **Yes**.
- **Service Set ID(SSID):** Use this field to name and create a new SSID. When you click **Add New**, the **AP Radio SSID** setup screen appears. You configure the new SSID on that page.

Assigning SSIDs to VLANs (Cont.)



AWLF v3.1—8-140

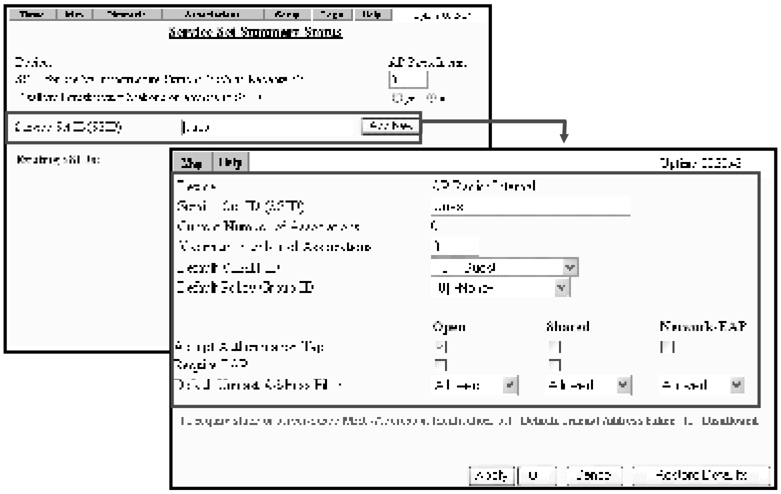
- **Existing SSIDs:** This field contains a list of SSIDs that have been created on this access point. The numbers in brackets to the left of each SSID indicates the VLAN to which the SSID is mapped.

  To edit an existing SSID, highlight the SSID and click **Edit**. The AP Radio SSID setup screen for that SSID appears. Make any changes and click **Apply** or **OK** to save them.

  To remove an existing SSID, highlight the SSID you wish to remove and click **Remove**. The SSID and its configuration is removed.

Assigning SSIDs to VLANs (Cont.)

Cisco.com

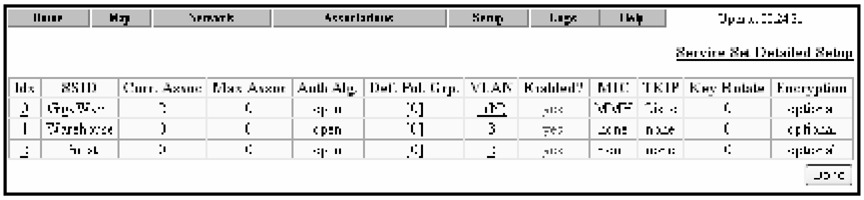


This screen appears when you click **Add New** from the AP Radio Service Set screen.

- **Device:** The name of the device you are configuring.
- **Service Set ID (SSID):** Identifies the SSID to be used by repeaters and workgroup bridges to associate with the access point.
- **Current Number of Associations**
- **Maximum Number of Associations**
- **Default VLAN ID:** Use the drop-down menu to determine which VLAN will be the default.
- **Default Policy Group ID:** Use the drop-down menu to determine which policy group will be the default.
- **Accept Authentication Type:** Select which authentication type the access point recognizes.
- **Require EAP:** If you want to force all client devices to perform EAP authentication before joining the network, select either the Open or Shared check box.
- **Default Unicast Address Filter:** Use the drop-down to determine whether you want to allow a default unicast address filter for each authentication type.

Service Set Summary Status

Cisco.com



Idx	SSID	Curr. Assoc	Max Assoc	Auth Alg.	Def. Pol. Grp.	VLAN	Enabled?	MIC	TKIP	Key Rotate	Encryption
0	[illegible]	0	0	open	[0]	[illegible]	yes	[illegible]	[illegible]	0	optional
1	Warehouse	0	0	open	[0]	3	yes	none	none	0	optional
2	[illegible]	0	0	open	[0]	2	yes	none	none	0	optional

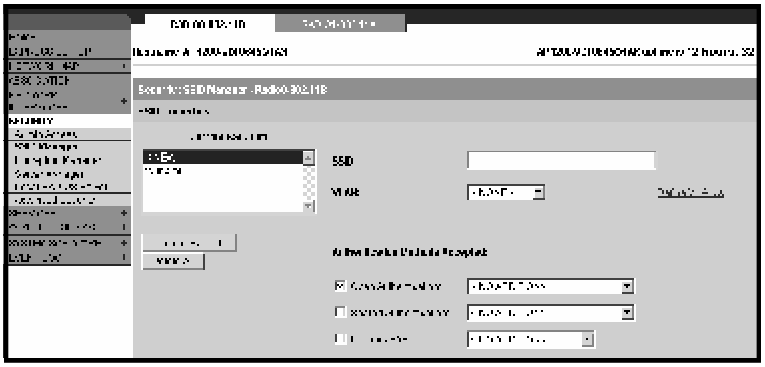
AWLF v3.1—8-142

This screen displays the status of service sets.

Settings

- **Idx:** The index number of the service set. You can click this number to move to the Repeater Radio Primary SSID page.
- **SSID:** The SSID assigned.
- **Curr. Assoc:** Current Associations.
- **Max Assoc:** Maximum Associations.
- **Auth Alg.:** Displays whether Open, Shared Key, or Network EAP is the authentication the access point recognizes.
- **Def. Pol. Grp.:** Displays which policy group is applied for each VLAN. **VLAN:** Displays which VLAN configuration is being used.
- **Enabled?:** Displays whether VLANs are enabled or not.
- **MIC:** Determines whether MIC is being used on this VLAN.
- **TKIP:** Determines whether TKIP is being used on this VLAN.
- **Key Rotate:** Determines the interval that the WEP key will be rotated. The ability to enable WEP key rotation for each VLAN is supported only for wireless VLANs with IEEE 802.1x protocols enabled.
- **Encryption:** Determines if the VLAN is using no, optional, or full encryption.

SSID Manager



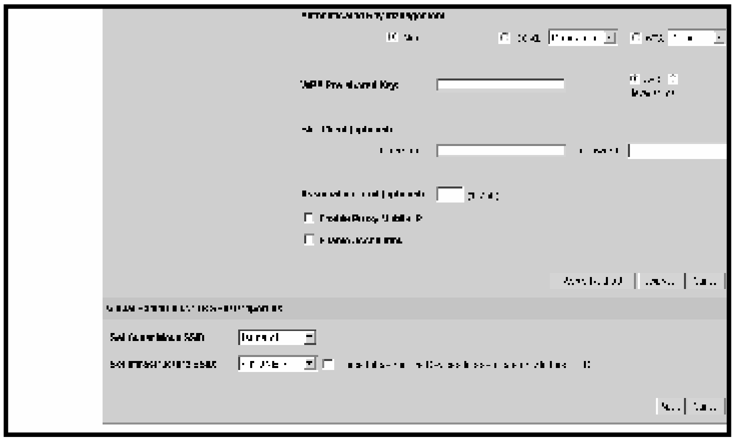
AWLF v3.1—8-143

The **SSID Manager** screen permits the configuration of **SSID** (System Service ID) after **VLAN** and Encryption parameters have been setup on the Access Point.

The **Authentication Methods Accepted** selections for "**Open Authentication**", "**Shared Authentication**", and "**Network EAP**" authentication permit the types of authentication available on the SSID to be specified. Either MAC or EAP authentication may be added to Open or Shared authentication. MAC authentication may be added to Network EAP authentication to permit adding a MAC authentication step to the LEAP authentication process.

SSID Manager (Cont.)

Cisco.com



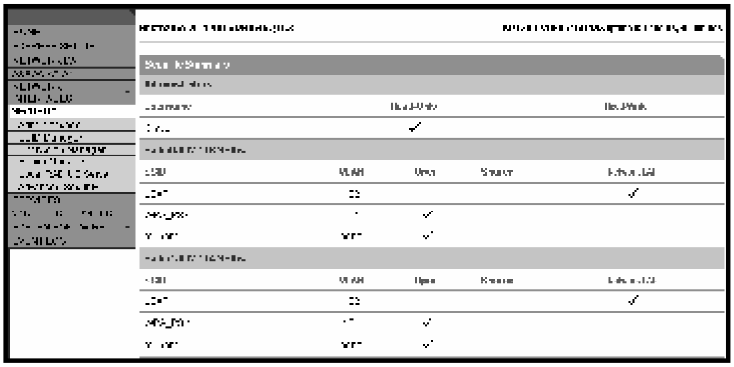
AWLF v3.1—8-144

On the bottom of the SSID Manager screen, additional authentication parameters may be configured for the selected SSID.

- **Authenticated Key Management**, either for Cisco Centralized Key Management (**CCKM**) or for WiFi Protected Access (**WPA**) may be configured as "Optional" or "Mandatory", depending on the desired system operation and client capabilities. If using WPA, the **WPA Pre-shared Key** (used as to authenticate the encryption parameters between client and AP in non-802.1X environment) may be entered from this interface.
- **EAP Client Username** and **Password**, which are used to authenticate the AP to a LEAP server, for operation of the AP/Bridge in repeater or non-root mode is entered from this interface.
- **Association Limit** determines the maximum number of client associations that the AP will permit to the specified SSID.
- **Enable Proxy Mobile IP** allows the Proxy Mobile IP protocol to be enabled for the specified SSID. Note that Proxy Mobile IP is not used with VLAN's enabled.
- **Enable Accounting** allows client accounting to be recorded and transmit to a AAA accounting server for the specified SSID.
- Under **Global Radio SSID Properties**, the properties used for ALL 802.11 interfaces may be configured. **Set Guest Mode SSID** configures the single SSID that the AP transmits in its beacon information. **Set Infrastructure SSID** configures the SSID for use by repeaters and WGB, and permits restriction of these infrastructure devices to this SSID only via the "**Force Infrastructure Devices to associate only to this SSID**" selection box.

SSID Summary

Cisco.com



AWLF v3.1—8-146

The SSID Summary and **Administrators** user information is available from the Security menu selection and is shown under “**Security Summary**”.

The administrative users configured from the “**Admin Access**” menu and their capabilities (**Read-Only** or **Read-Write**)

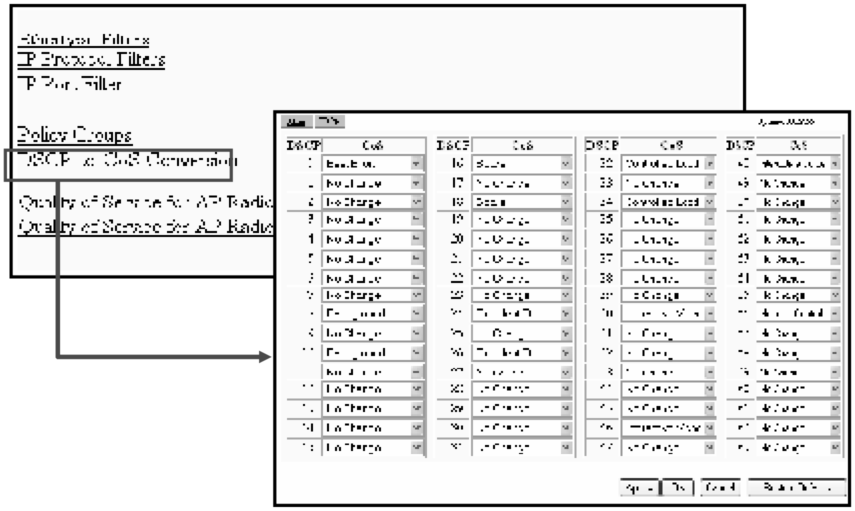
Note that VLAN’s and SSID’s associated to each Radio interface and their configured authentication mechanisms are indicated on this screen.

SSID’s may also be configured from this Summary screen. The configuration menu for each Radio Interface is accessible from either “**Radio0-802.11B-SSIDs**” or “**Radio1-802.11A-SSIDs**” link.

QoS Configuration

DSCP to CoS Conversion

Cisco.com



Ethertype Filters
IP Protocol Filters
IP Port Filter

Policy Groups
DSCP to CoS Conversion

Quality of Service for AP Radio
Quality of Service for AP Radio

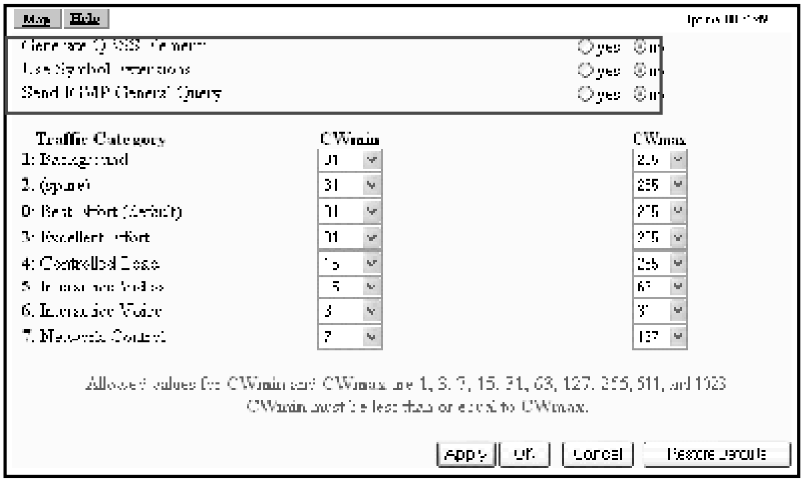
AWLF v3.1—8-148

Traffic that comes to the access point over an Ethernet trunk is already classified by its Class of Service (CoS) settings. This page allows you to classify the traffic by mapping the differentiated services code point (DSCP) values to COs in the IP packets.

Use the drop-down menus to choose the traffic category. The category choices are no change, background, spare, best effort, excellent effort, controlled load, or interactive video.

Quality of Service

Cisco.com



Generate QBSS Element ○ yes ● no
Use Symbol Extensions ○ yes ● no
Send IGMP General Query ○ yes ● no

Traffic Category	CWmin	CWmax
1: Background	31	255
2: (spare)	31	255
0: Best Effort (Default)	31	255
3: Excellent Effort	31	255
4: Controlled Load	15	255
5: Interactive Video	7	63
6: Interactive Voice	3	31
7: Network Control	7	127

Allowed values for CWmin and CWmax are 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1023
CWmin must be less than or equal to CWmax.

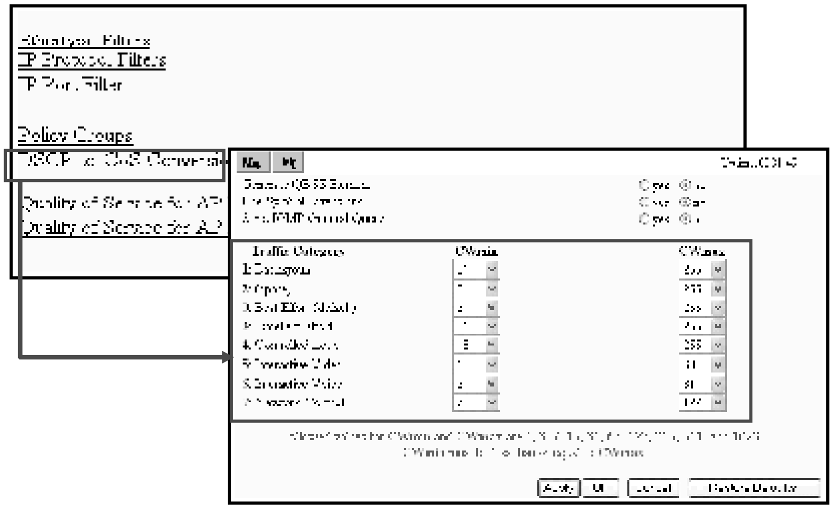
AWLF v3.1—8-149

Qualities of Service (QoS) settings are accomplished on this page. You can also fine tune traffic category contention window settings.

- **Generate QBSS Element:** Use this setting to determine whether a QoS basic service set (QBSS) element is generated. The QBSS element determines the best access point with which to associate.
- **Use Symbol Extensions:** This setting configures the access point to use Symbol Voice over IP (VoIP) phones. When this setting is enabled, the access point uses the Symbol Phone Support protocol. This protocol identifies Symbol handsets and classifies traffic for them as interactive voice.
- **Send IGMP General Query:** This setting configures the access point to perform IP multicast filtering. Automatic IP multicast filtering is not directly supported on the access point. This setting is the mechanism that injects IP multicast filtering onto Ethernet switches.

Quality of Service (Cont.)

Cisco.com



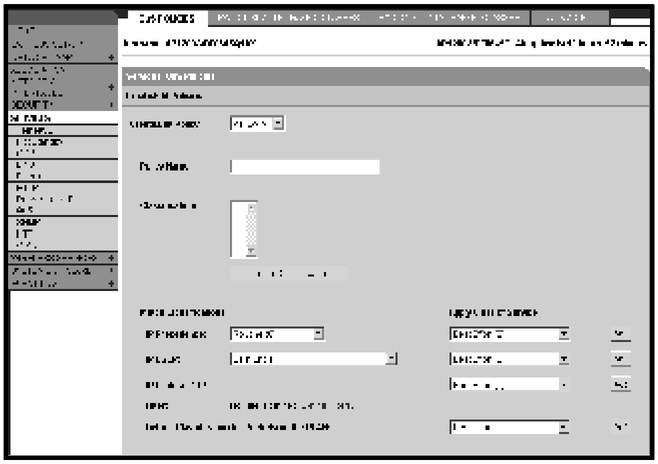
AWLF v3.1—8-150

- **Traffic Category:** Traffic category identifies a type of traffic in which data processed by the access point is categorized. Following are the traffic categories:
  - Background Spare
  - Best effort (default setting)
  - Excellent effort
  - Controlled load
  - Interactive video
  - Interactive voice
  - Network control
- **CWmin and CWmax:** Each traffic category is assigned a minimum contention window (CWmin) value and a maximum contention window (CWmax) value. Allowed values for **CWmin** and **CWmax** are 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1023.

Note Cisco recommends that you do not alter these settings without significant testing. If you do alter the values, **CWmin** must be less than or equal to **CWmax**.

Quality of Service

Cisco.com



AWLF v3.1—8-151

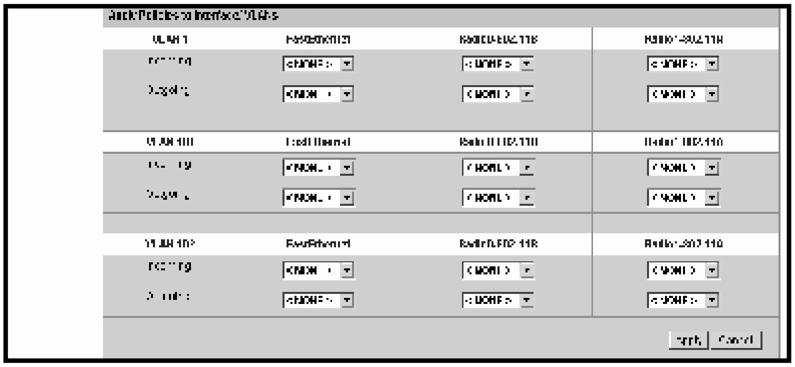
QoS (Quality of Service) Policies may be created from the Services> QoS menu. QoS policies permit the prioritization of packets based on the device type, IP tags, VLAN, or predefined filter (ACL).

The **Policy Name** is used as an descriptor to uniquely identify each QoS policy defined in the AP. After the association of parameters to a QoS Policy, these associated parameters will appear in the “**Classifications**” selection box.

Under the **Match Classifications** menu, the specific mechanism used to prioritize packets (either **IP Precedence**, **IP DSCP**, **IP Protocol 119**, **Filter**, **Default Classification for Packets on the VLAN**) and the **Apply Class of Service** menu pulldown menu is used to apply CoS for each defined Classification.

Quality of Service (Cont.)

Cisco.com



Apply Policies to Interface/VLANs

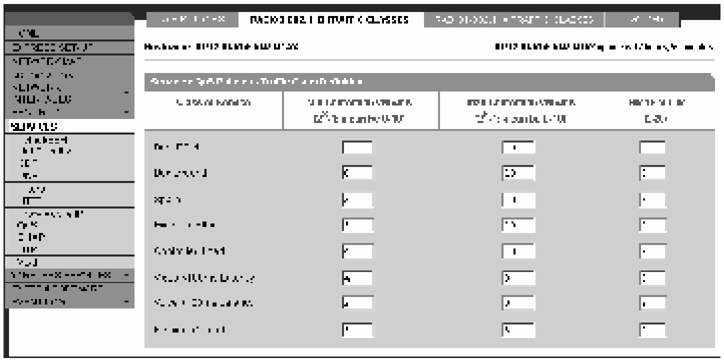
VLAN 1	FastEthernet0	Radio0-802.11B	Radio1-802.11A
Incoming	< NONE >	< NONE >	< NONE >
Outgoing	< NONE >	< NONE >	< NONE >
VLAN 100	FastEthernet0	Radio0-802.11B	Radio1-802.11A
Incoming	< NONE >	< NONE >	< NONE >
Outgoing	< NONE >	< NONE >	< NONE >
VLAN 102	FastEthernet0	Radio0-802.11B	Radio1-802.11A
Incoming	< NONE >	< NONE >	< NONE >
Outgoing	< NONE >	< NONE >	< NONE >

AWLF v3.1—8-152

After configuration of QoS policies, the configured policies may be applied to the desired interface, either for inbound (**Incoming**) or outbound (**Outgoing**) traffic. Additionally, policies may be uniquely defined for each configured VLAN on the AP in order to permit unique packet prioritization for different VLAN and user classes.

Quality of Service (Traffic Classes)

Cisco.com



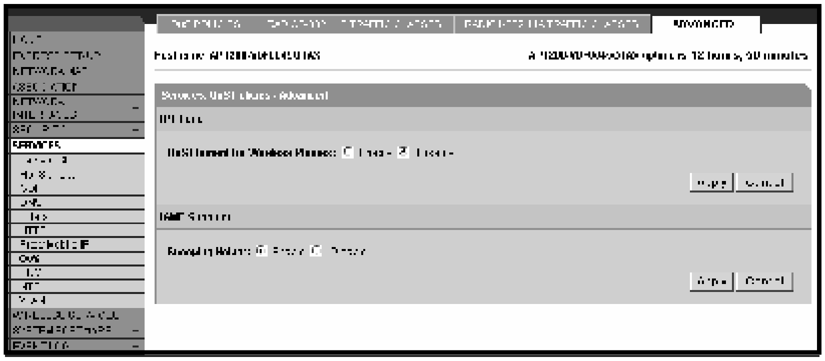
AWLF v3.1—8-153

Under the “**Traffic Classes**” menu, the **Traffic Class Definitions** (as relate to 802.11 contention window) for each Class of Service defined in the AP may be reviewed and edited.

The screen indicated on this slide shows the default contention window settings defined for each Class of Service which is assigned via the QoS policy menu.

Quality of Service (Cont.)

Cisco.com

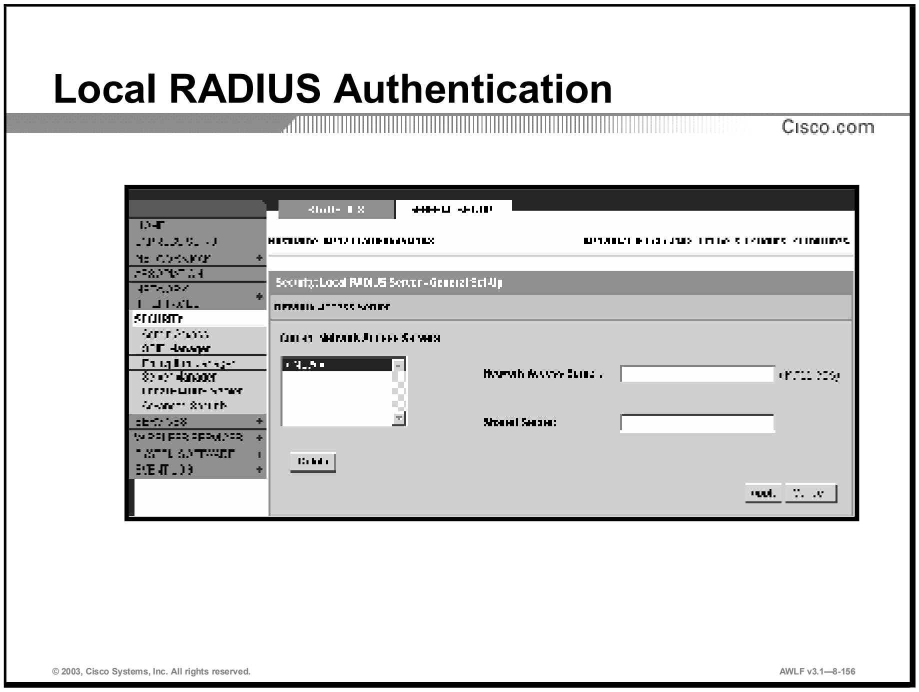


AWLF v3.1—8-154

The **Advanced** menu permits the configuration of specific Quality of Service parameters for unique applications:

- **IP Phone** permits the **QoS Element for Wireless Phones** to be **Enabled** or **Disabled**. This parameter configures the AP to broadcast "quality beacon" information in the beacons for association by 802.11 telephony devices.
- **IGMP Snooping** permits the AP to "proxy" an IGMP query to the (IGMP snooping enabled) network on behalf of an IGMP client in order to preserve the integrity of the multicast stream to IGMP members. Note the "**Snooping Helper**" is enabled by default.

Cisco Aironet Local Radius Authentication



Local RADIUS Authentication

Cisco.com

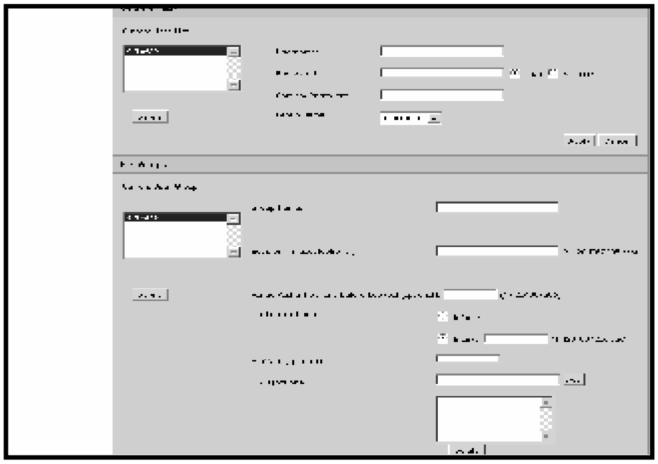
AWLF v3.1—8-156

Local RADIUS Authentication is enabled from the Security> Local RADIUS Server menu selection under the **General Set-Up** tab. By entering a **Network Access Server** at this screen's textbox, Local RADIUS Authentication is enabled on the AP. As with any AAA server, the NAS and its associated RADIUS **Shared Secret** string are required to communicate between the RADIUS server and RADIUS client (or NAS).

All currently configured NAS's are displayed in the **Current Network Access Servers** menu.

Local Radius Authentication (Cont.)

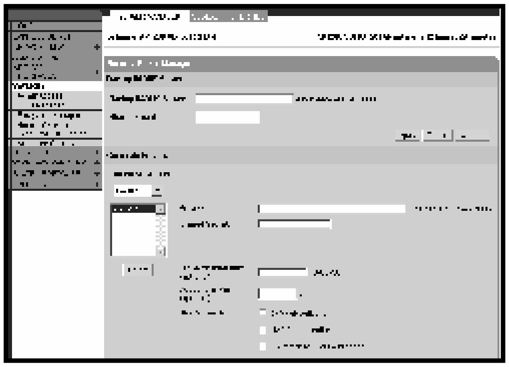
Cisco.com



At the bottom of the General Set-Up screen for Local RADIUS Server configuration, **Current User List** and **User Group** parameters are configured. Note that up to 50 users may be configured in the Local RADIUS Server database. Users may be assigned to Default Group, thus it is not required to setup User Groups. However, **Session timeout**, **VLAN** parameters, number of **Failed Authentications before Lockout,** and **SSID** restriction are only configurable per Group, not definable per user.

Server Manager and Local RADIUS

Cisco.com



AWLF v3.1—8-158

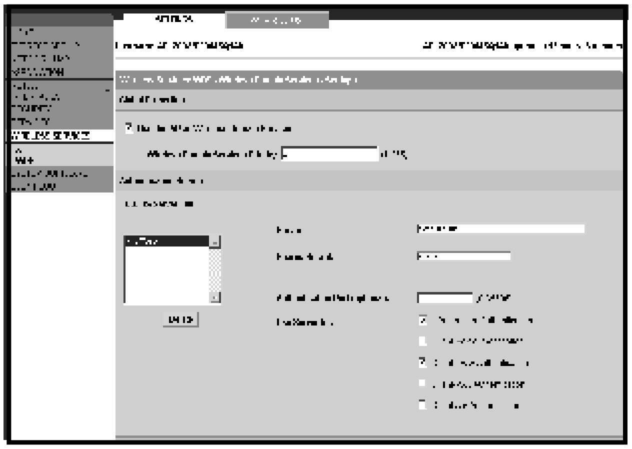
The **Backup** (a.k.a. Local) **RADIUS Server** is configured on the AP configured for Local RADIUS operation as well as other AP's which will use this AP for backup RADIUS service from the "**Server Manager**" menu selection. Note that the Backup RADIUS Server is valid only for LEAP authentication.

The Backup RADIUS Server is only used for LEAP authentication upon a non-responsive RADIUS request. Invalid username or password will not initiate use of Backup RADIUS.

Note that UDP port 1812 is used for authentication to the Local RADIUS server, whereas port 1645 is the default port for RADIUS authentication.

Wireless Domain Services

Cisco.com



AWLF v3.1—8-159

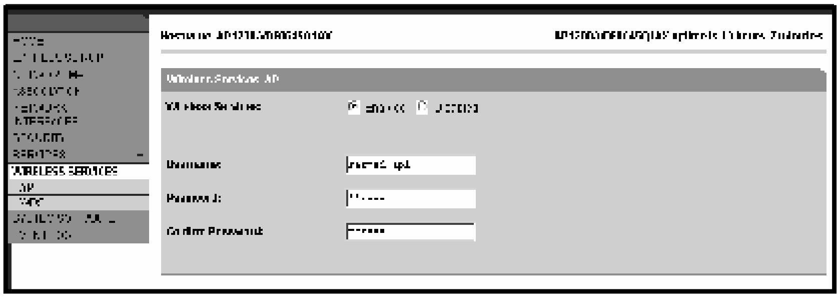
Wireless Domain Services (WDS) is a mechanism in the AP for caching user authentication credentials which may be used for subsequent client authentication requests. This caching mechanism permits the operation of Cisco Centralized Key Management or Fast Secure Roaming. Only a single AP per subnet is active as the “master” Wireless Domain Server. However, other AP’s may take over the master role upon failure of the main AP.

The **Wireless Domain Services Priority** setting controls the master priority of the configured AP, with a smaller number indicating higher priority.

The **Authentication Servers** section permits the configuration of RADIUS servers for use by the WDS for authentication of both AP’s and clients. Note that each AP that uses the WDS for CCKM must be capable of authenticating as an EAP client to the configured RADIUS server under “Authentication Servers”. Thus both AP and clients must be capable of Authentication against the RADIUS server.

Wireless Domain Services (Cont.)

Cisco.com



Wireless Services ● Enable ○ Disable

Username: [illegible]

Password: [illegible]

Confirm Password: [illegible]

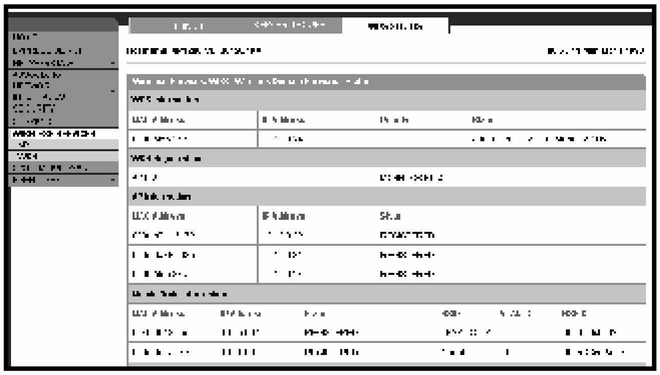
AWLF v3.1—8-160

For each AP served by a Wireless Domain Server (including the AP serving as the WDS), **Wireless Services** must be Enabled to permit client devices to authenticate to the AP using the CCKM protocol and to permit Fast Secure Roaming to/from the AP.

The **Username** and **Password** that the AP uses to authenticate with the WDS (and in turn, the RADIUS server) are entered from this screen. Note that this username/ password combination must be entered from the server configured in the WDS under "Infrastructure Authentication".

Wireless Domain Services (Cont.)

Cisco.com



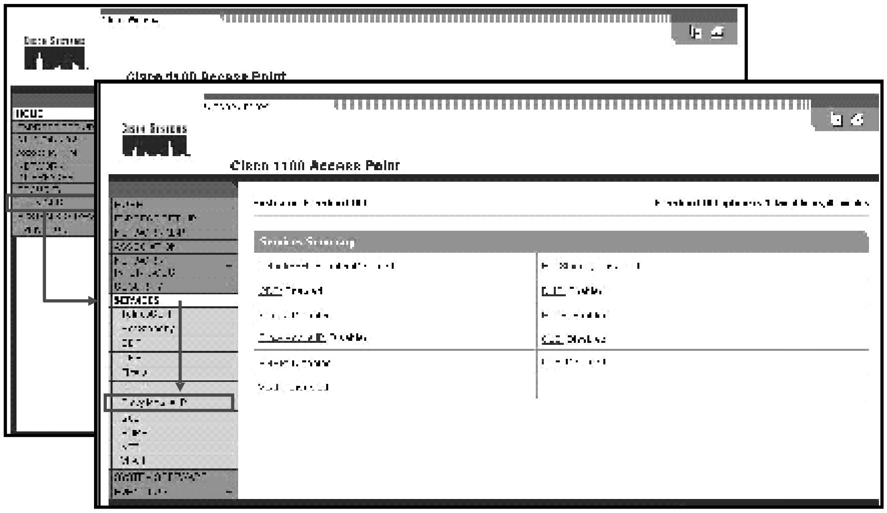
AWLF v3.1—8-161

After configuration of Wireless Domain Services, the status of the AP's associated (either registered or not registered) to the WDS and any clients associated to the AP's which are registered to the WDS are indicated at the Wireless Services> WDS screen. Summary data is available for **WDS Information-** indicating active WDS "master" and **WDS Registration-** indicating number of associated AP's and clients- from this screen.

Cisco Aironet Proxy Mobile IP

Proxy Mobile IP

Cisco.com

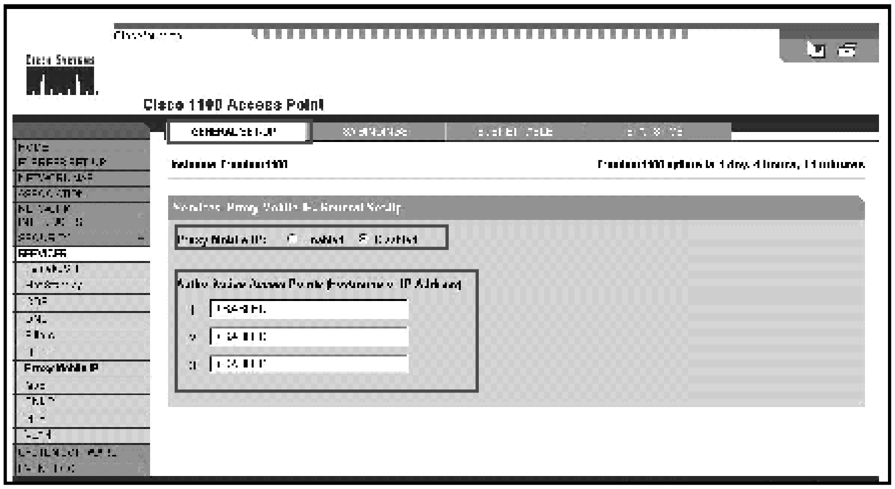


AWLF v3.1—8-163

Proxy Mobile IP implementation on Cisco Aironet products is intended to provide Mobile IP functionality on behalf of the roaming mobile devices. It supports mobility in the IP infrastructure, allowing users to keep the same IP address and maintain ongoing applications while roaming between IP networks. The roaming individual could continue communication without sessions or connections being dropped. This Proxy Mobile IP functionality is provided without the need for any Mobile IP-capable software running on the devices.

Proxy Mobile IP General-Setup

Cisco.com



AWLF v3.1—8-164

Services: Proxy Mobile IP—General Setup

Proxy Mobile IP has four main phases:

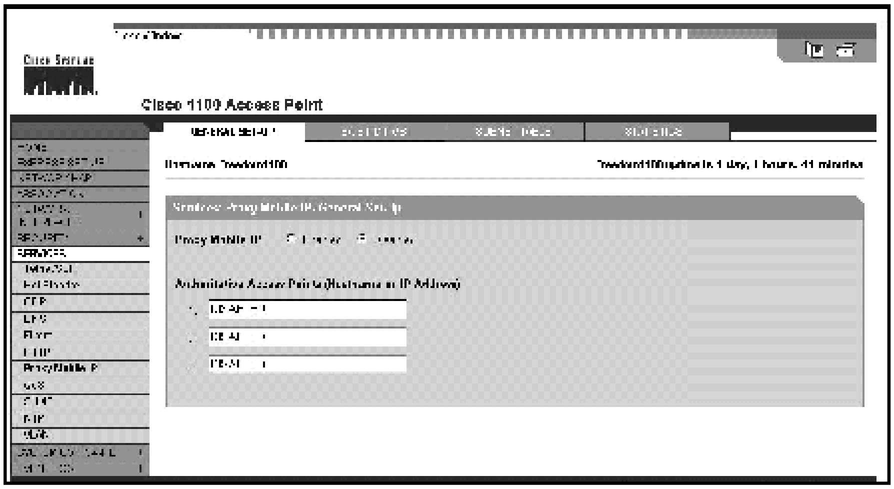
- **Agent discovery** - The access point discovers the foreign and home agents.
- **Subnet map exchange** - The access point obtains information regarding other mobile device's home agents during the subnet map exchange.
- **Registration** - The access point registers the mobile devices with the foreign agent and home agent during registration.
- **Tunneling** - A reciprocal tunnel is set up by the home agent to the current location of the mobile device on the foreign network. Packets are routed to the mobile device as it roams.

Proxy Mobile IP

This feature can be enabled only if your device is not in repeater mode. Enable Proxy Mobile IP on all interfaces and enable at least one SSID. If you disable Proxy Mobile IP, your entire Proxy Mobile IP configuration is cleared, including your security parameter index (SPI) and key entries.

Proxy Mobile IP General-Setup (Cont.)

Cisco.com



Cisco 1100 Access Point

GENERAL SET-UP

Proxy Mobile IP

Authoritative Access Points (Hostname or IP Address)

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—8-165

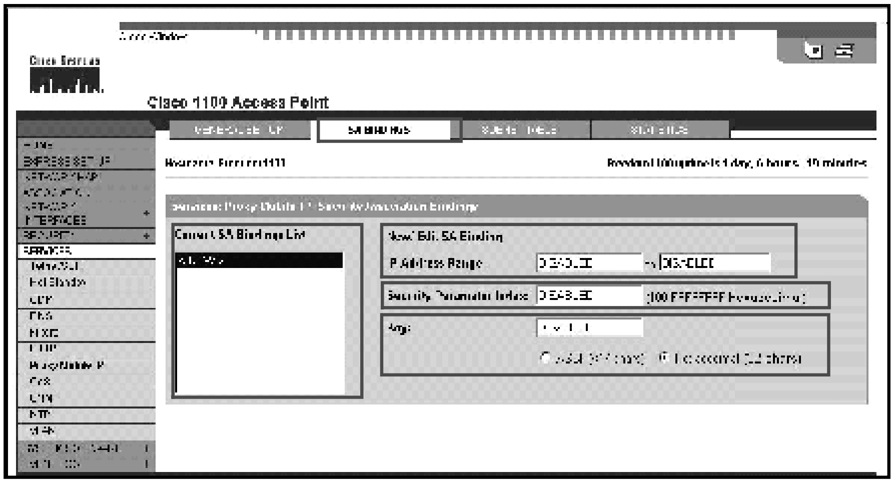
Authoritative Access Points (host name or IP Address)

An authoritative access point (AAP) must be specified in order to use the Proxy Mobile IP feature. These AAPs keep track of the home agent information on all of the mobile devices. They keep the latest subnet map table, which maps client IP addresses to home agent addresses. This information is needed to activate the Proxy Mobile IP functionality.

An access point sends packets with the subnet and home agent information to the AAP. The AAP distributes this information (in the form of a table) to all the access points participating in the PMIP network. By having this information local, the access point can do a faster lookup for the home agent information when a foreign mobile device roams into the network. If an access point is unreachable during this update process, the AAP retries. If the retry fails, the next configured AAP is tried. You should have more than one AAP in the system so that you do not lose subnet map table information if an AAP goes down. To rebuild the subnet table, you must either reboot all your access points or clear the subnet map table from each one.

Proxy Mobile IP Security Association Bindings

Cisco.com



Current SA Bindings List

New/Edit SA Binding

IP Address Range: DISABLED to DISABLED

Security Parameter Index: DISABLED

AWLF v3.1—8-166

Services: Proxy Mobile IP—Security Association (SA) Bindings

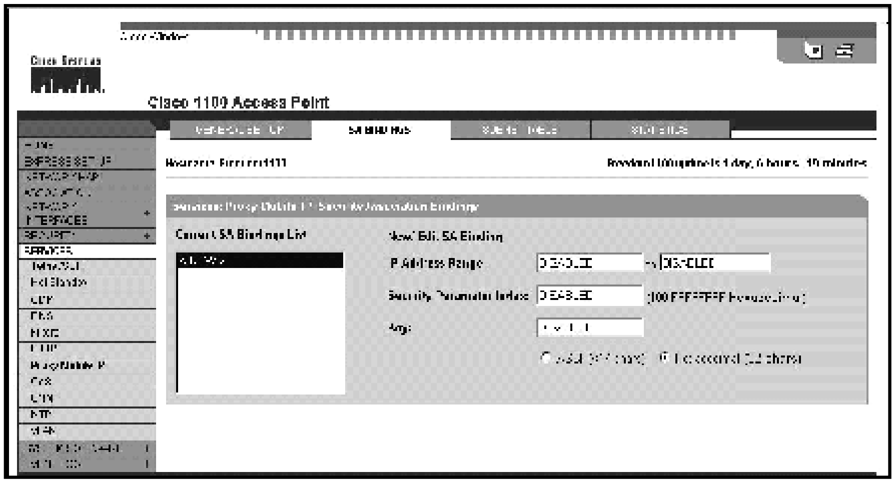
You must specify a security association for the mobile device in order to use Proxy Mobile IP. The security association can be specified locally on the access point with this screen or can be specified externally on the RADIUS server.

All potential mobile devices and their corresponding home agents must have security associations. The security association can be configured locally via this page or through an authentication, authorization, and accounting (AAA) server (configured on the Security/Server Manager screen). Security associations are used to authenticate the mobile client in Proxy Mobile IP messages to the home agent. If the AAA server is configured with the SA bindings, nothing must be configured on this page. If the SA bindings are configured locally, enter security association information for either one IP or a range of IP addresses on this page.

- **Current SA Bindings List:** Displays the range of IP addresses in the security association bindings that are currently set.

Proxy Mobile IP Security Association Bindings (Cont.)

Cisco.com

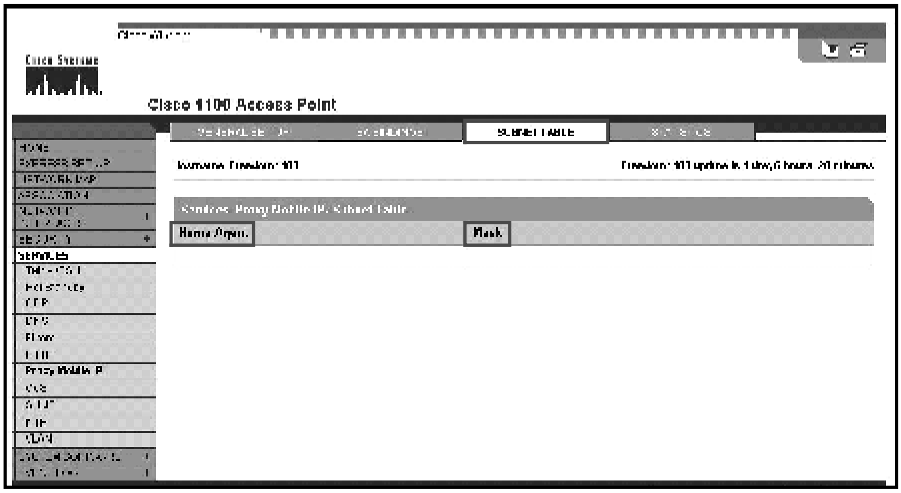


AWLF v3.1—8-167

- **New/Edit SA Binding:** This section enables you to enter security association information for either one IP or a range of IP addresses.
- **IP Address Range:** Enter the starting and ending IP address in the range. The first IP address must be less than the ending address.
- **Security Parameter Index:** Supply an index that identifies a security context between a pair of nodes.
- **Key:** Include the shared encryption key. Choose if it is represented in ASCII or Hexadecimal.

Proxy Mobile IP Subnet Table

Cisco.com



AWLF v3.1—8-168

Services: Proxy Mobile IP—Subnet Table

Each access point keeps a subnet table that consists of a list of home agent IP addresses and their subnet masks. When a mobile device associates to an access point and has roamed into a foreign network, the access point performs a lookup on the subnet map table. The access point proceeds with the registration process.

You can click Refresh if the subnet table displayed appears out of date.

Home Agent

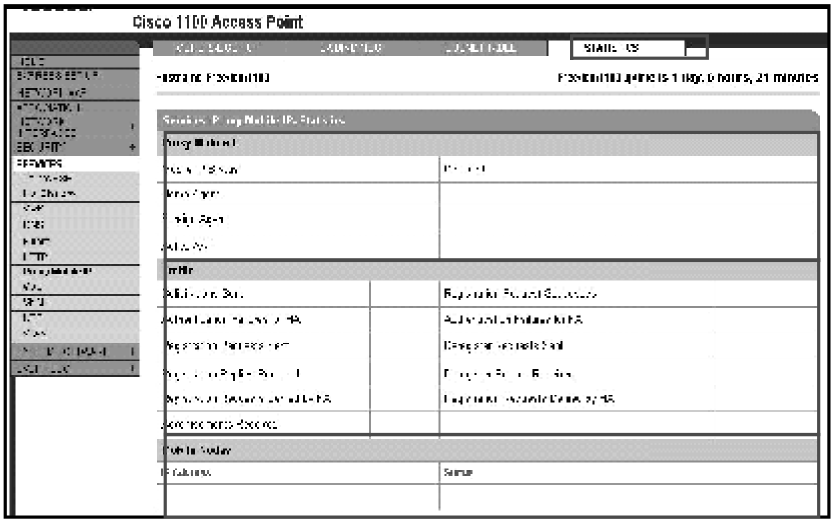
A router on the home network serving as the anchor point for communication with the access point. It transports packets from a device on the Internet to the roaming mobile device. The mobility binding and visitor entry of the home agent is updated during reregistration. If registration is denied, the access point makes the necessary adjustments and attempts to register again. For example, if the registration is denied because of time mismatch, and the home agent sent back its time stamp for synchronization, the access point adjusts the time stamp in future registration requests.

Mask

The subnet mask to identify the subnetwork so the IP address be recognized by the LAN.

Proxy Mobile IP Statistics

Cisco.com



AWLF v3.1—8-169

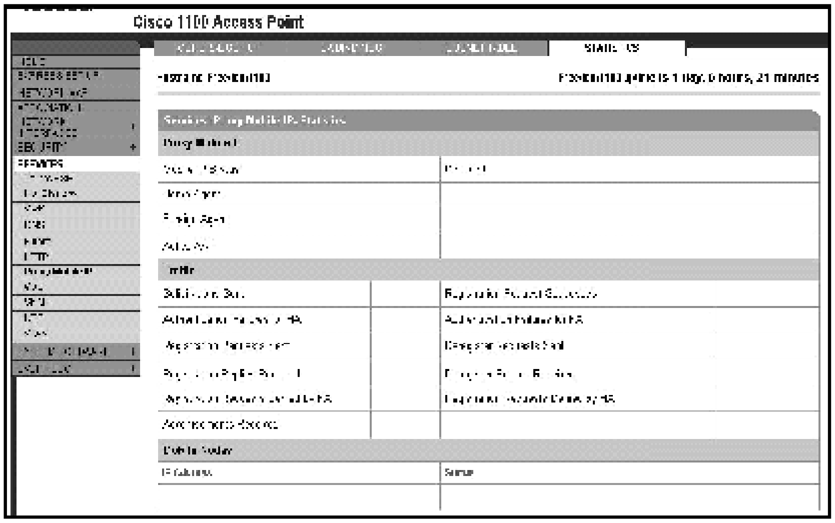
Services: Proxy Mobile IP—Statistics

Proxy Mobile IP

- **Mobile IP Status:** An Enabled status indicates that you want to support clients that do not have Mobile IP capability.
- **Home Agent**: Displays the home agent or router on this network.
- **Foreign Agent**: Displays the foreign agent on your network. The foreign agent is a router that might function as the point of attachment for the mobile device when it roams to a foreign network, delivering packets from the home agent to the mobile device.
- **Active AAP**: Displays the active AAPs on your network. An AAP is an authoritative access point that must be specified in order to use the Proxy Mobile IP feature. These AAPs keep track of the home agent information on all of the mobile devices.

Proxy Mobile IP Statistics (Cont.)

Cisco.com



Cisco 1100 Access Point

STATISTICS

Hostname ProxyMobile

uptime is 1 day, 0 hours, 21 minutes

Services: Proxy Mobile IP Statistics

Proxy Mobile IP

Status	
Home Agent	
Foreign Agent	
Care-of-Address	

Traffic

Solicitations Sent		Registration Request Successes	
Authentication Failures for HA		Authentication Failures for FA	
Registration Requests Sent		Deregister Requests Sent	
Registration Replies Received		Deregister Replies Received	
Registration Requests Denied by FA		Registration Requests Denied by HA	
Advertisements Received			

Mobile Node

IP Address	State

© 2003, Cisco Systems, Inc. All rights reserved.

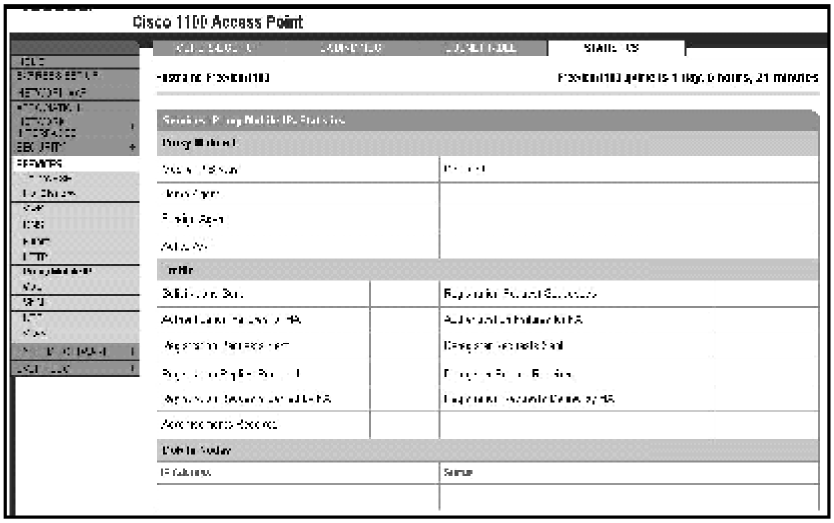
AWLF v3.1—8-170

Traffic

- **Solicitations Sent**: The number of agent solicitation packets sent out to detect home or foreign agents.
- **Registration Request Successes**: The number of successful registration requests that are sent by the access point for the visiting mobile device.
- **Authentication Failures for HA**: The number of authentication failures received by the access point from the home agent.
- **Authentication Failures for FA**: The number of authentication failures received by the access point from the foreign agent.
- **Registration Requests Sen**t: The number of registration requests that were sent by the access point for the visiting mobile device.
- **Deregister Requests Sent**: The number of deregistration requests sent by the access point for the mobile device that returned home.
- **Registration Replies Received**: The number of registration replies received by the access point in response to the registration request.
- **Deregister Replies Received**: The number of deregistration replies received by the access point in response to its deregistration request.

Proxy Mobile IP Statistics (Cont.)

Cisco.com



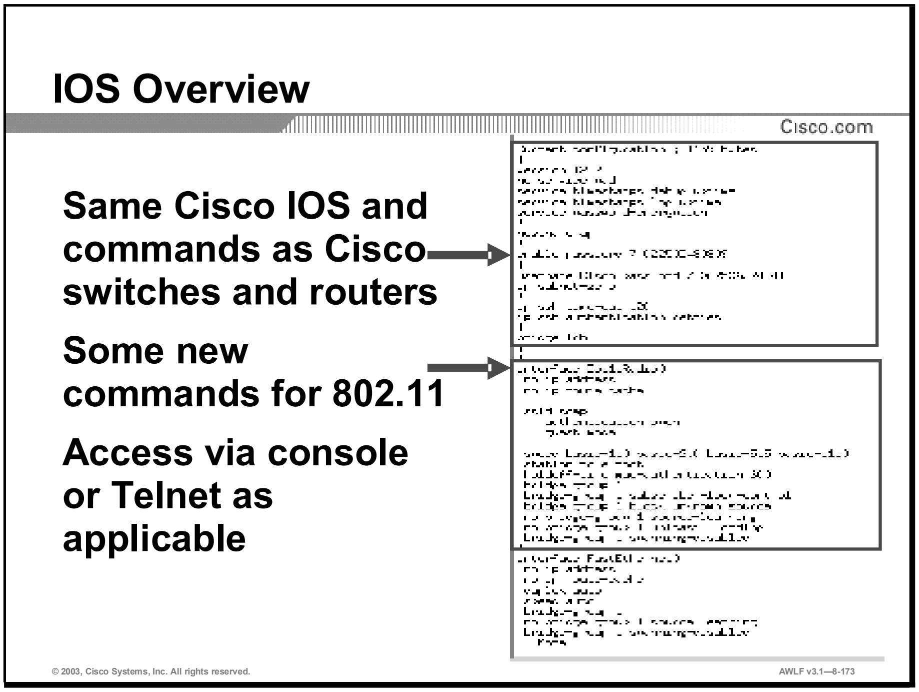
AWLF v3.1—8-171

- **Registration Requests Denied by FA:** The number of registration requests sent by the access point for the visiting mobile device that resulted in a failure because the foreign agent denied the request.
- **Registration Requests Denied by HA:** The number of registration requests sent by the access point for the visiting mobile device that resulted in a failure because the home agent denied the request.
- **Advertisements Received:** How often the home or foreign agent advertised their presence and capabilities.

Mobile Nodes

- **IP Address:** The IP address of the mobile device.
- **Status:** The current status of the mobile device.

Cisco Aironet Access Point IOS CLI Interface



IOS Overview

Cisco.com

- Same Cisco IOS and commands as Cisco switches and routers
- Some new commands for 802.11
- Access via console or Telnet as applicable

AWLF v3.1—8-173

ISO Overview

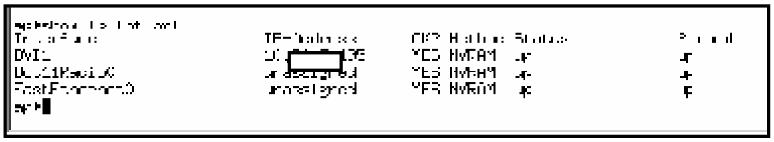
The Cisco Aironet 1100 and 1200 Series GUI introduces the next level of intuitive, browser-based management for an improved user experience. A menu-based organization simplifies navigation and configuration for easy setup and ongoing management with out compromised security. The Cisco Aironet 1100/1200 Series can also be managed using Cisco IOS Software CLI, which is familiar to IT professionals and makes use of their existing skills. There are new 802.11 commands added to IOS (e.g.) commands for applying an SSIDs, entering WEP keys, changing IP Address, changing channels and many more. As with other Cisco IOS products, this interface may be accessed either via telnet or local console interface.

IOS Overview (Cont.)

802.11 is simply another interface on AP

- **Falls within wired architecture**

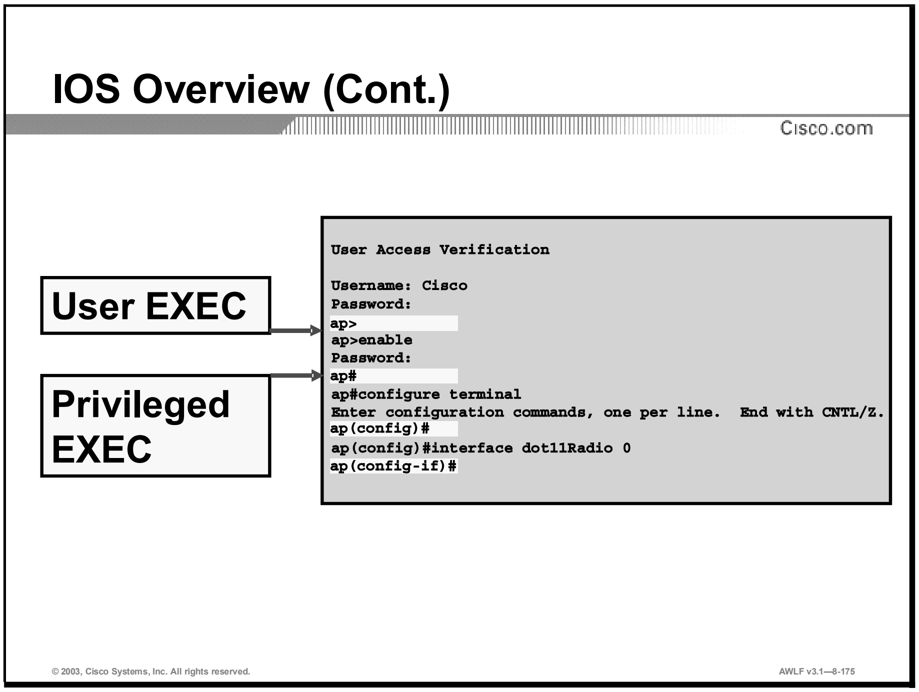
Extends wired features to the wireless



```
ap#show ip int brief
Interface              IP-Address      OK? Method Status          Protocol
BVI1                   10.[illegible]135   YES NVRAM  up              up
Dot11Radio0            unassigned      YES NVRAM  up              up
FastEthernet0          unassigned      YES NVRAM  up              up
ap#
```

AWLF v3.1—8-174

The 802.11 commands fit into the IOS architecture as just another interface. Taking features used in a wired environment and extending them to a wireless interface. In the example above you see the FastEthernet0 is the first interface and the Dot11Radio0 is the second interface.



IOS Overview (Cont.)

```
User Access Verification

Username: Cisco
Password:
ap>
ap>enable
Password:
ap#
ap#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)#
ap(config)#interface dot11Radio 0
ap(config-if)#
```

User EXEC Mode

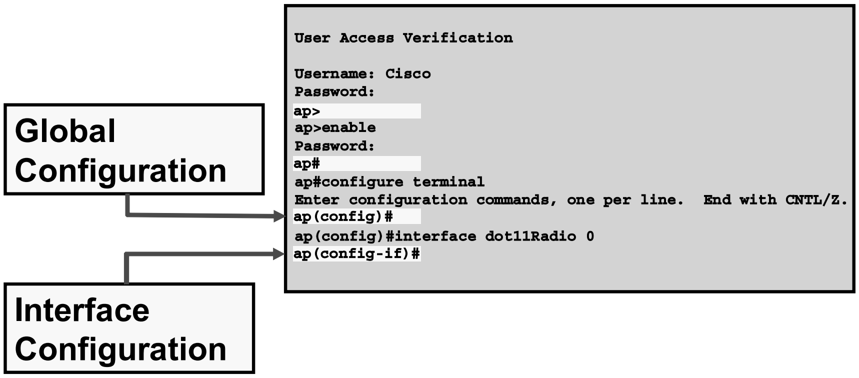
After you access the device, you are automatically in user EXEC command mode. The EXEC commands available at the user level are a subset of those available at the privileged level. In general, use the EXEC commands to temporarily change the terminal settings, perform basic test and list system information. The supported commands can vary depending on the version of IOS software in use.

Privileged EXEC Mode

Because many of the privileged commands configure operating parameters, privileged access should be password-protected to prevent unauthorized use. The privileged command set includes those commands contained in the EXEC mode, as well as the **configure** privileged EXEC command through which you access the remaining command modes.

If your system administrator has set a password, you are prompted to enter it before being granted access to privileged EXEC mode. The password does not appear on the screen and is case sensitive.

IOS Overview (Cont.)



Global Configuration

Interface Configuration

```
User Access Verification

Username: Cisco
Password:
ap>
ap>enable
Password:
ap#
ap#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)#
ap(config)#interface dot11Radio 0
ap(config-if)#
```

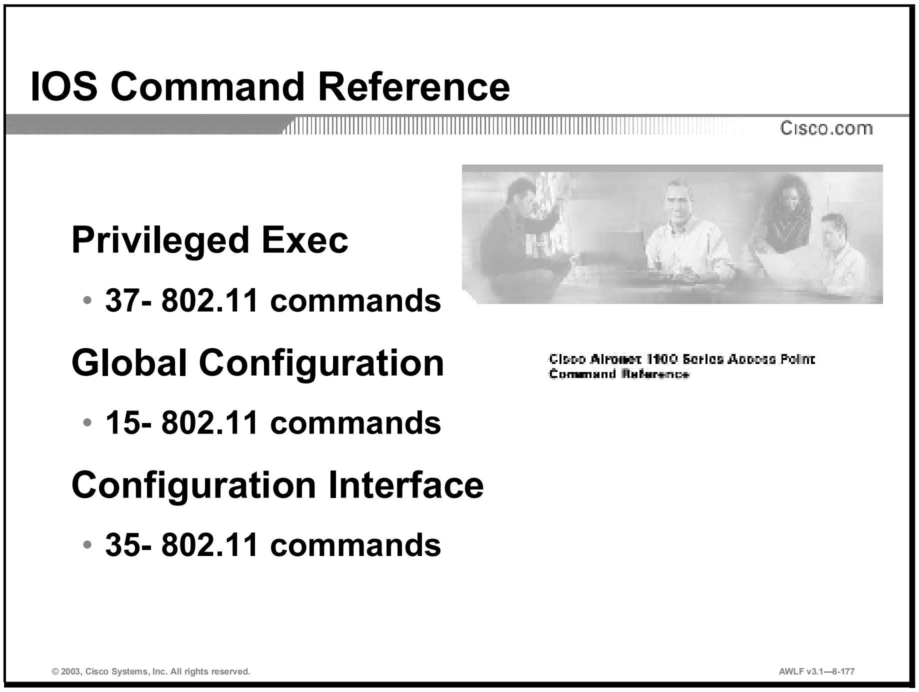
AWLF v3.1—8-176

Global Configuration Mode

Global configuration commands apply to features that affect the device as a whole. Use the **configure** privileged EXEC command to enter global configuration mode. The default is to enter commands from the management console. When you enter the **configure** command, a message prompts you for the source of the configuration commands.

Interface Configuration Mode

Interface configuration commands modify the operation of the interface. Interface configuration commands always follow a global configuration command, which defines the interface type. Use the **interface** *interface-id* command to access interface configuration mode.



IOS Command Reference

Cisco.com

Privileged Exec

- 37- 802.11 commands

Global Configuration

- 15- 802.11 commands

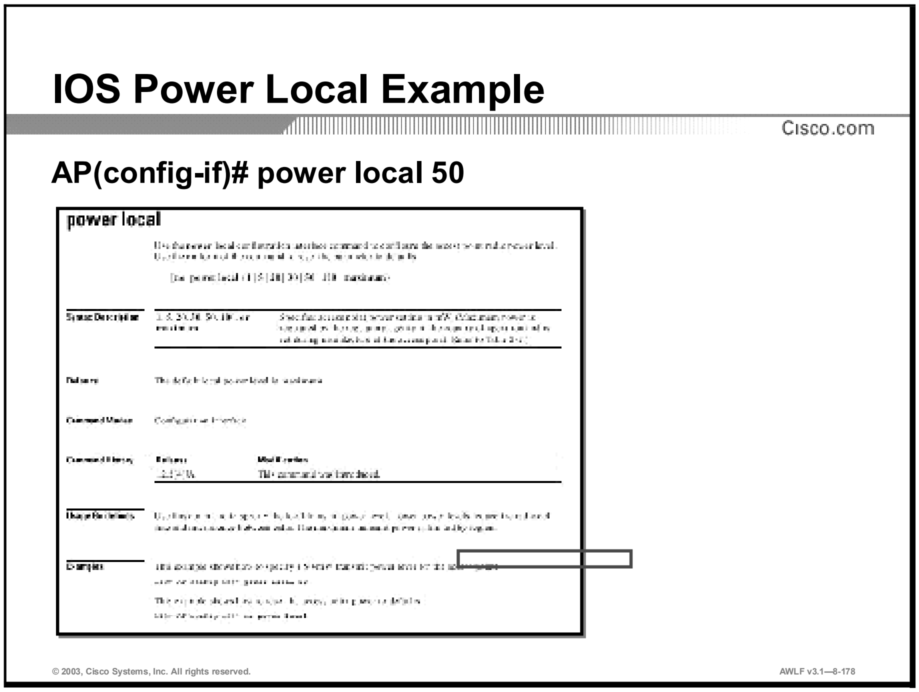
Configuration Interface

- 35- 802.11 commands

Cisco Aironet 1100 Series Access Point Command Reference

AWLF v3.1—8-177

This guide is for the networking professional using the Cisco IOS command-line-interface to manage the Cisco Aironet 1100 Access Point. This documentation also provides information about the standard IOS Release 12.2 commands.



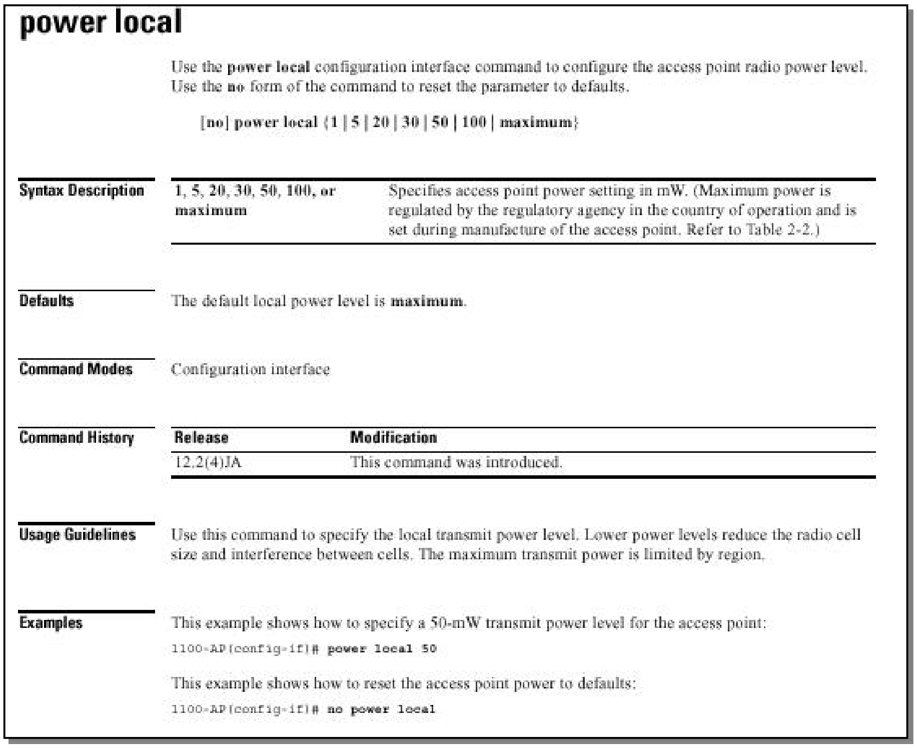
IOS Power Local Example

Cisco.com

AP(config-if)# power local 50

AWLF v3.1—8-178

Use this command to specify the local transmit level. Lower power levels reduce the radio cell size and interferences between cells. The maximum transmit power is limited by region. The example above shows how to specify a 50 mW transmit power level for the access point.



power local

Use the **power local** configuration interface command to configure the access point radio power level. Use the **no** form of the command to reset the parameter to defaults.

[no] power local {1 | 5 | 20 | 30 | 50 | 100 | maximum}

Syntax Description

1, 5, 20, 30, 50, 100, or maximum	Specifies access point power setting in mW. (Maximum power is regulated by the regulatory agency in the country of operation and is set during manufacture of the access point. Refer to Table 2-2.)

Defaults

The default local power level is **maximum**.

Command Modes

Configuration interface

Command History

Release	Modification
12.2(4)JA	This command was introduced.

Usage Guidelines

Use this command to specify the local transmit power level. Lower power levels reduce the radio cell size and interference between cells. The maximum transmit power is limited by region.

Examples

This example shows how to specify a 50-mW transmit power level for the access point:

```
1100-AP(config-if)# power local 50
```

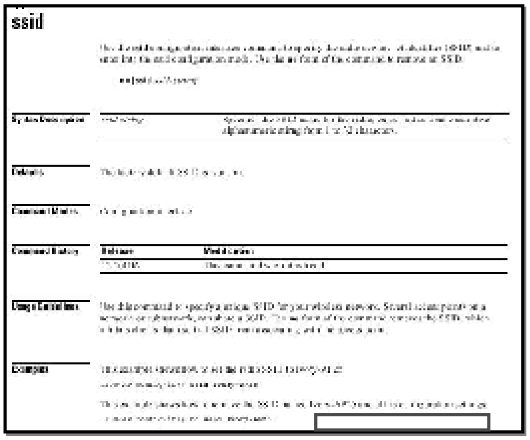
This example shows how to reset the access point power to defaults:

```
1100-AP(config-if)# no power local
```

IOS SSID Example

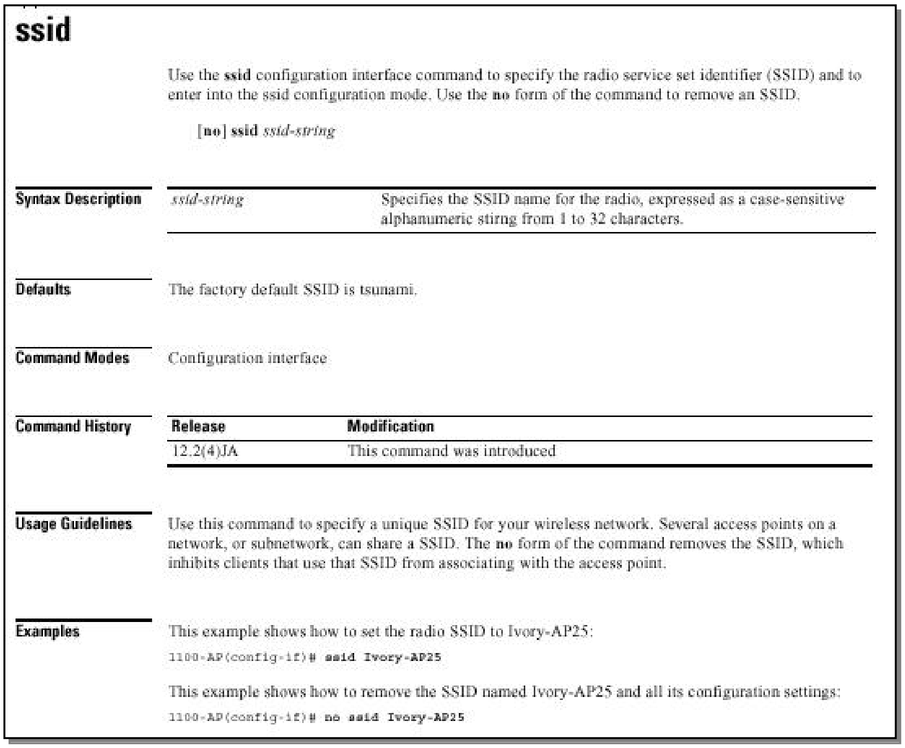
Cisco.com

AP(config-if)# ssid Ivory-AP25



AWLF v3.1—8-179

Use the SSID configuration interface command to specify the radio service set identifier (SSID) and to enter into the SSID configuration mode. The example above will create a SSID Ivory-AP25.



ssid

Use the **ssid** configuration interface command to specify the radio service set identifier (SSID) and to enter into the ssid configuration mode. Use the **no** form of the command to remove an SSID.

[**no**] **ssid** *ssid-string*

Syntax Description

ssid-string	Specifies the SSID name for the radio, expressed as a case-sensitive alphanumeric stirng from 1 to 32 characters.

Defaults

The factory default SSID is tsunami.

Command Modes

Configuration interface

Command History

Release	Modification
12.2(4)JA	This command was introduced

Usage Guidelines

Use this command to specify a unique SSID for your wireless network. Several access points on a network, or subnetwork, can share a SSID. The **no** form of the command removes the SSID, which inhibits clients that use that SSID from associating with the access point.

Examples

This example shows how to set the radio SSID to Ivory-AP25:

```
1100-AP(config-if)# ssid Ivory-AP25
```

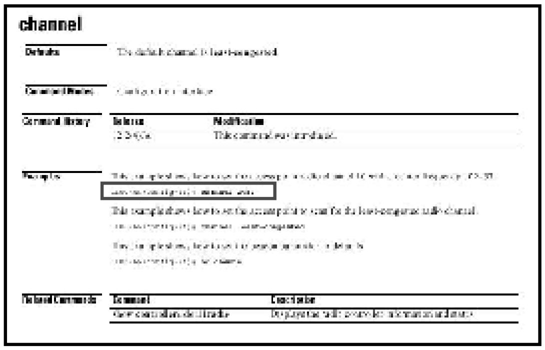
This example shows how to remove the SSID named Ivory-AP25 and all its configuration settings:

```
1100-AP(config-if)# no ssid Ivory-AP25
```

IOS Channel Example

Cisco.com

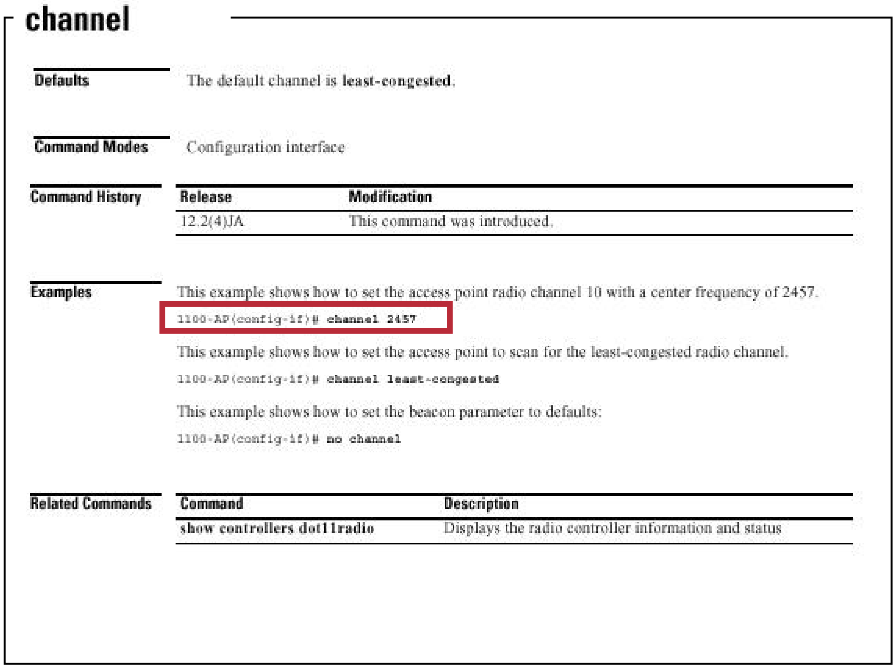
AP(config-if)# channel 2457



© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—8-180

Use the channel configuration interface command to set the radio channel frequency. The example above will change the access point to channel 10.



channel

Defaults The default channel is **least-congested**.

Command Modes Configuration interface

Command History

Release	Modification
12.2(4)JA	This command was introduced.

Examples This example shows how to set the access point radio channel 10 with a center frequency of 2457.

```
1100-AP(config-if)# channel 2457
```

This example shows how to set the access point to scan for the least-congested radio channel.

```
1100-AP(config-if)# channel least-congested
```

This example shows how to set the beacon parameter to defaults:

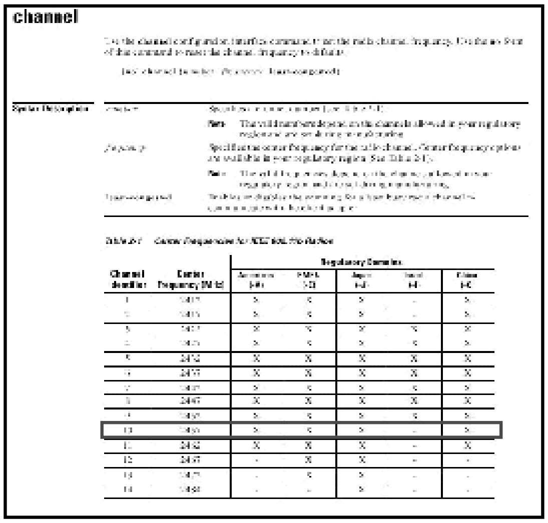
```
1100-AP(config-if)# no channel
```

Related Commands

Command	Description
show controllers dot11radio	Displays the radio controller information and status

IOS Channel Example (Cont.)

Cisco.com



channel

Use the channel configuration interface command to set the radio channel frequency. Use the no form of this command to reset the channel frequency to defaults.

[no] channel {number | frequency | least-congested}

Syntax Description

number	Specifies a channel number (see Table 2-1). **Note** The valid channel numbers depend on the channels allowed in your regulatory region and are set during manufacturing.
frequency	Specifies the center frequency for the radio channel. Center frequency options are available in your regulatory region. (See Table 2-1.) **Note** The valid frequencies depend on the channels allowed in your regulatory region and are set during manufacturing.
least-congested	Enables or disables the scanning for a least busy radio channel to communicate with the client adapter.

Table 2-1 Center Frequencies for IEEE 802.11b Radios

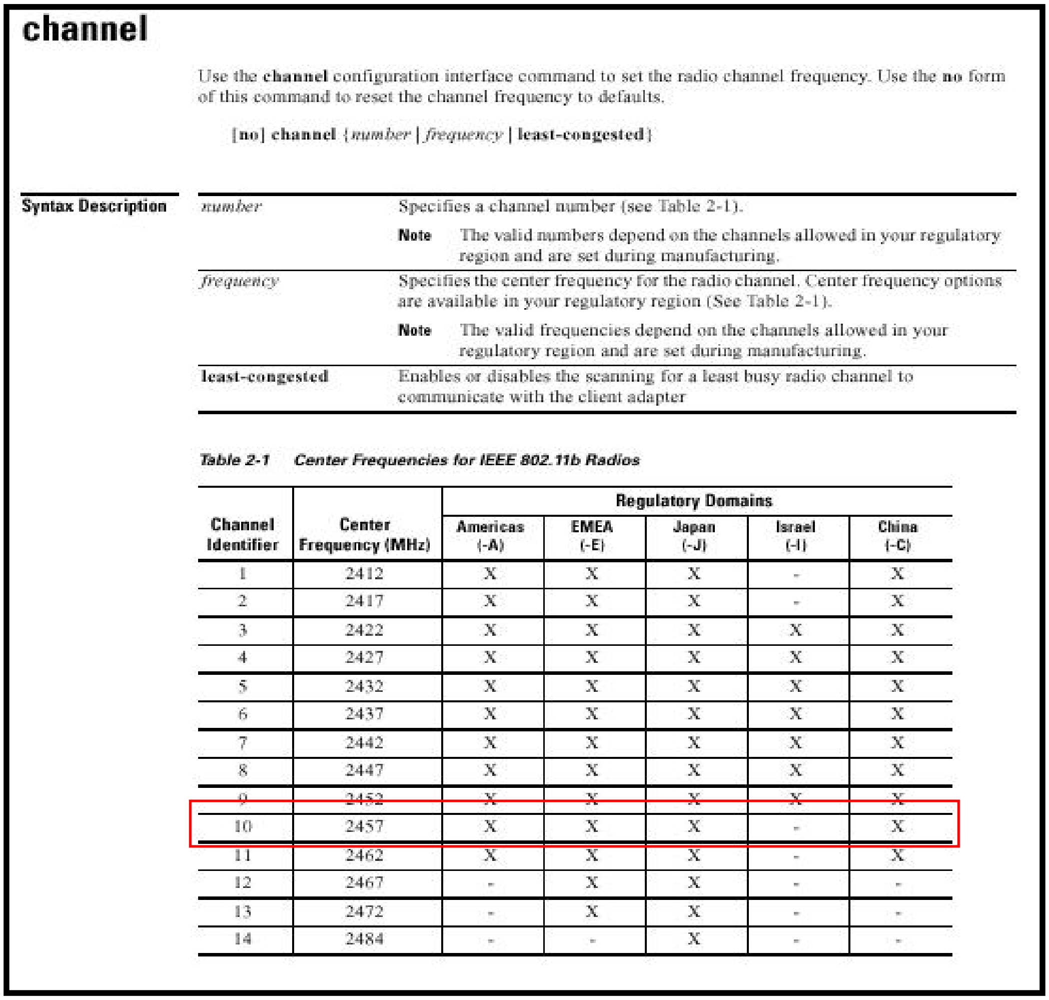
Channel Identifier	Center Frequency (MHz)	Regulatory Domains				
		Americas (-A)	EMEA (-E)	Japan (-J)	Israel (-I)	China (-C)
1	2412	X	X	X	–	X
2	2417	X	X	X	–	X
3	2422	X	X	X	X	X
4	2427	X	X	X	X	X
5	2432	X	X	X	X	X
6	2437	X	X	X	X	X
7	2442	X	X	X	X	X
8	2447	X	X	X	X	X
9	2452	X	X	X	X	X
10	2457	X	X	X	–	X
11	2462	X	X	X	–	X
12	2467	–	X	X	–	–
13	2472	–	X	X	–	–
14	2484	–	–	X	–	–

AWLF v3.1—8-181

The channel configuration interface command allows the option of entering the channel three different ways.

- By the assigned channel number.
  - (e.g.) AP(config-if)# channel 10
- By the frequency.
  - (e.g.) AP(config-if)# channel 2457
- Scan for the least-congested radio channel.
  - (e.g.) AP(config-if)# channel least-congested

See the following page for a larger copy of this picture.



channel

Use the **channel** configuration interface command to set the radio channel frequency. Use the **no** form of this command to reset the channel frequency to defaults.

[no] channel {*number* | *frequency* | **least-congested**}

Syntax Description

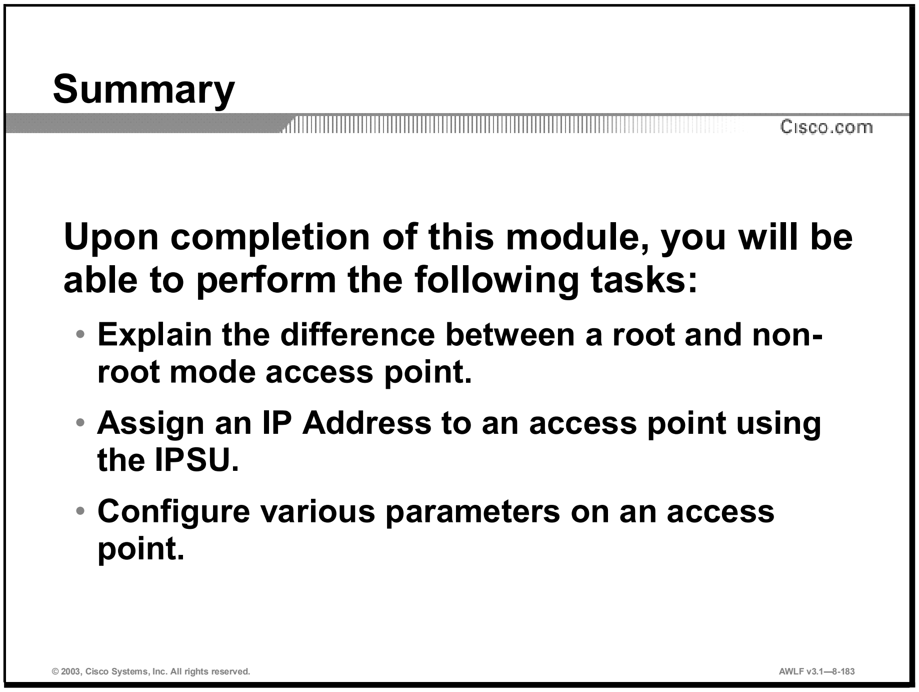
number	Specifies a channel number (see Table 2-1). **Note** The valid numbers depend on the channels allowed in your regulatory region and are set during manufacturing.
frequency	Specifies the center frequency for the radio channel. Center frequency options are available in your regulatory region (See Table 2-1). **Note** The valid frequencies depend on the channels allowed in your regulatory region and are set during manufacturing.
least-congested	Enables or disables the scanning for a least busy radio channel to communicate with the client adapter

Table 2-1 Center Frequencies for IEEE 802.11b Radios

Channel Identifier	Center Frequency (MHz)	Regulatory Domains				
		Americas (-A)	EMEA (-E)	Japan (-J)	Israel (-I)	China (-C)
1	2412	X	X	X	-	X
2	2417	X	X	X	-	X
3	2422	X	X	X	X	X
4	2427	X	X	X	X	X
5	2432	X	X	X	X	X
6	2437	X	X	X	X	X
7	2442	X	X	X	X	X
8	2447	X	X	X	X	X
9	2452	X	X	X	X	X
10	2457	X	X	X	-	X
11	2462	X	X	X	-	X
12	2467	-	X	X	-	-
13	2472	-	X	X	-	-
14	2484	-	-	X	-	-

Summary

This section summarizes the concepts you learned in this module.



Summary

Upon completion of this module, you will be able to perform the following tasks:

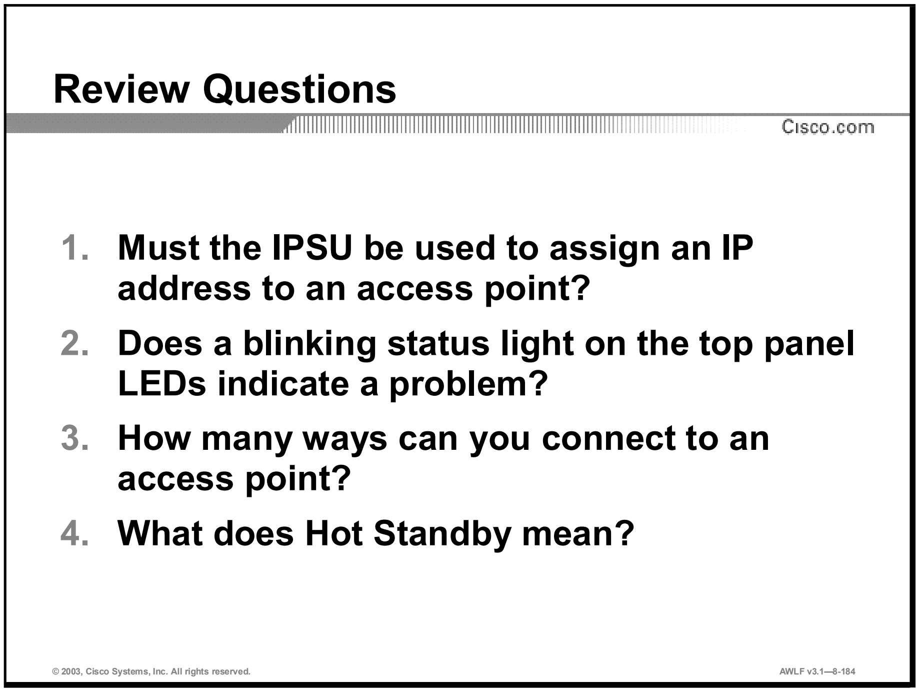
- **Explain the difference between a root and non-root mode access point.**
- **Assign an IP Address to an access point using the IPSU.**
- **Configure various parameters on an access point.**

AWLF v3.1—8-183

Upon completion of this module, you will be able to perform the following tasks:

- Explain the difference between a root and non-root mode access point
- Assign an IP Address to an access point using the IPSU
- Configure various parameters on an access point

Review Questions



Review Questions

1. **Must the IPSU be used to assign an IP address to an access point?**
2. **Does a blinking status light on the top panel LEDs indicate a problem?**
3. **How many ways can you connect to an access point?**
4. **What does Hot Standby mean?**

AWLF v3.1—8-184

Answer these review questions.

Module 9

Security

Overview

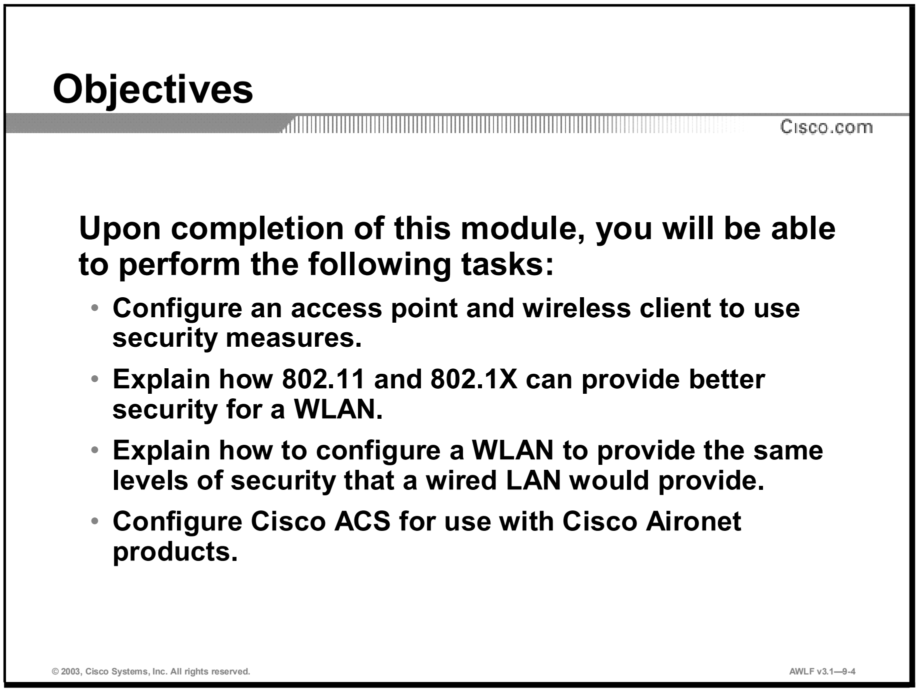
This module explores security features on the Cisco Aironet product set.

It includes the following topics:

- Objectives
- Basic Security Features
- 802.11 Security
- Configuring the Access Point for WEP
- Configuring the Client for WEP
- Problems with 802.11 WEP Security
- Security Suite
- WLAN Attacks
- Configuring WLAN Devices for Configuration
- Configuring the Client for Authentication
- Configuring Non-Root Devices for Authentication
- Configuring Cisco ACS
- User Setup
- Summary
- Review Questions

Objectives

This section lists the module's objectives.



Objectives

Cisco.com

Upon completion of this module, you will be able to perform the following tasks:

- **Configure an access point and wireless client to use security measures.**
- **Explain how 802.11 and 802.1X can provide better security for a WLAN.**
- **Explain how to configure a WLAN to provide the same levels of security that a wired LAN would provide.**
- **Configure Cisco ACS for use with Cisco Aironet products.**

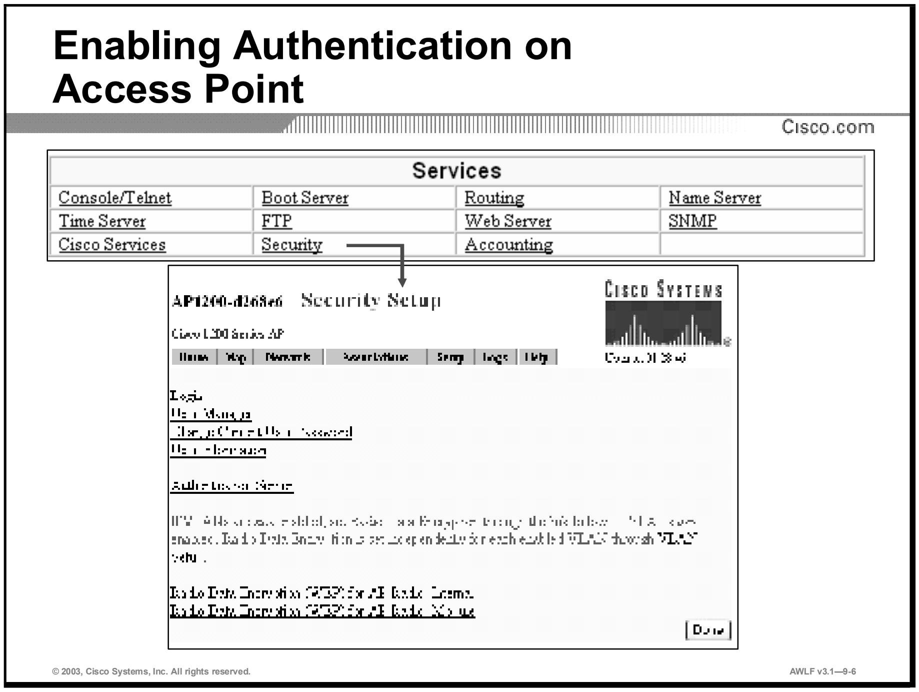
© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—9-4

Upon completion of this module, you will be able to perform the following tasks:

- Configure an access point and wireless client to use security measures
- Explain how 802.11 and 802.1X can provide better security for a WLAN
- Explain how to configure a WLAN to provide the same levels of security that a wired LAN would provide
- Configure Cisco ACS for use with Cisco Aironet products

Basic Security Features



Enabling Authentication on Access Point

Services			
Console/Telnet	Boot Server	Routing	Name Server
Time Server	FTP	Web Server	SNMP
Cisco Services	Security	Accounting	

AP1200-d268e6 Security Setup

Cisco 1200 Series AP

Login
User Manager
Change Current User Password
User Information

Authentication Server

[illegible]

Radio Data Encryption (WEP) for AP Radio Internal
Radio Data Encryption (WEP) for AP Radio Module

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—9-6

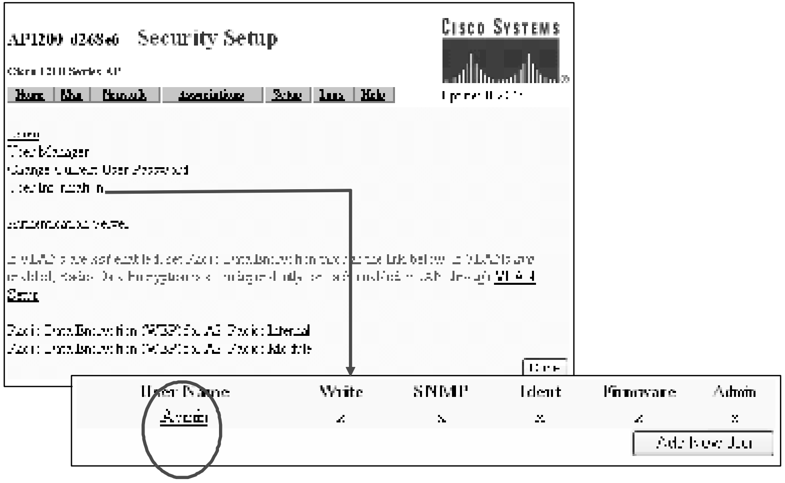
In order to maximize security on the wireless LAN (WLAN), a number of features need to be enabled and configured. These include the login manager, which requires users to log in to the access point. User can have various abilities on the access point to include the following:

- Ability to view the access point settings, but not makes changes to them.
- To write, or make changes to the access point.
- Configuration
- Perform SNMP operations.
- Change the IP address and SSID
- Or update firmware

It is also possible to prevent users from seeing any of the access point settings or making any changes to the access point.

User Information

Cisco.com



AP1200 d268e6 Security Setup

Cisco 1200 Series AP

[illegible]

User Manager

Change Current User Password

User Information

[illegible]

[illegible] VLAN [illegible]

Radio Data Encryption (WEP) for AP Radio Internal

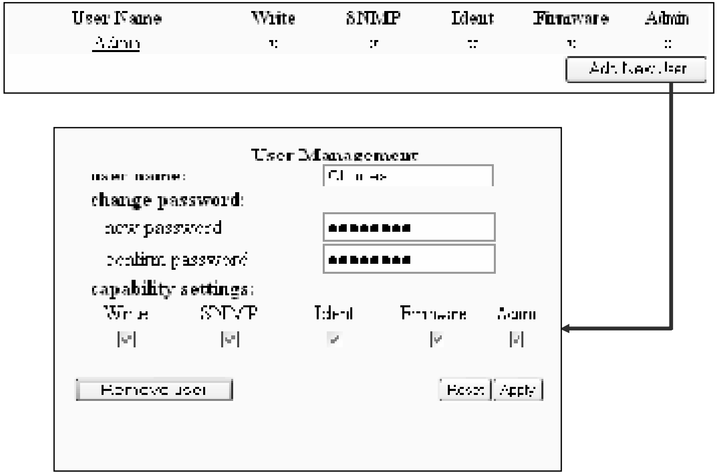
Radio Data Encryption (WEP) for AP Radio Module

User Name	Write	SNMP	Ident	Firmware	Admin
Admin	✓	x	x	✓	x

AWLF v3.1—9-7

The user information screen will display all users and their capabilities. Clicking on a user's name will take you to the properties screen for that user.

User Manager



User Name	Write	SNMP	Ident	Firmware	Admin
Admin	x	x	x	x	x

User Management

user name: Charles

change password:

new password ••••••••

confirm password ••••••••

capability settings:

Write	SNMP	Ident	Firmware	Admin
☑	☑	☑	☑	☑

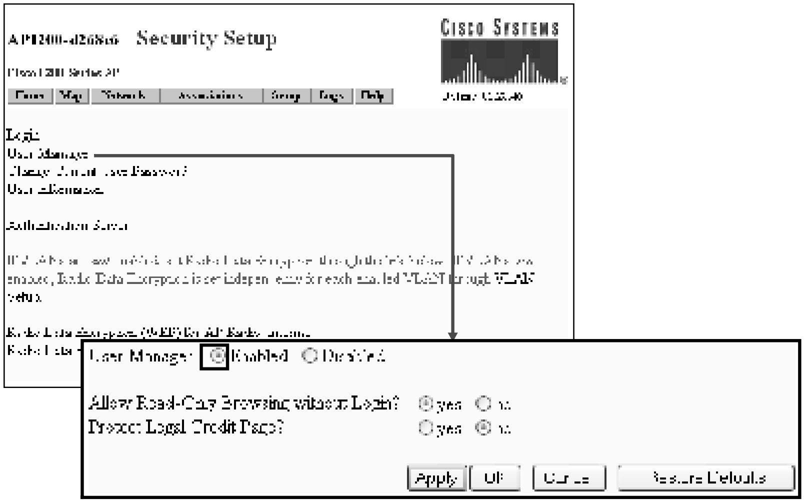
From the User Information screen, click the **Add New User** button to add a new user. This will launch the **User Management** screen. Enter the user name, password, and confirmation of the password. Then check any of the following capabilities boxes:

- **Write:** Allows the specified user to change system settings. When you assign **Write** capability to a user, the user also automatically receives **Admin** capability.
- **SNMP:** Designates the specified user name as a Simple Network Management Protocol (SNMP) community name. The user will use this SNMP community name to perform SNMP operations. SNMP operations performed by the user will be restricted according to the user's assigned capabilities. The User Manager does not have to be enabled for SNMP communities to operate correctly.
- **Ident:** Allows the specified user to change the access point's identity settings (MAC address, IP address, and SSID). When you assign **Ident** capability to a user, the user also automatically receives **Write** and **Admin** capabilities.
- **Firmware:** Allows the specified user to update the access point's firmware. When you assign **Firmware** capability to a user, the user also automatically receives **Write** and **Admin** capabilities.
- **Admin:** Allows the specified user to view all sensitive system screens and, with **Write** capability, to make changes to the system.

To remove users click the **Remove User** button. If logged in as a user, it is not possible to delete that user. At least one user must remain while **User Management** is enabled. To remove all users, disable **User Management** and remove the users.

Enabling Access Point Console Security

Cisco.com



AP1200-d268e6 Security Setup

Cisco 1200 Series AP

Home | Map | Network | Associations | Setup | Logs | Help

Login
User Manager
Change Current User Password
User Information

Authentication Server

[illegible] enabled, Radio Data Encryption is set independently for each enabled VLAN through VLAN Setup.

Radio Data Encryption (WEP) for All Radio [illegible]

User Manager: ● Enabled ○ Disabled

Allow Read-Only Browsing without Login? ● yes ○ no
Protect Legal Credit Page? ○ yes ● no

AWLF v3.1—9-9

From the **User Manager** screen, you can enable or disable the user manager. If the user manager is enabled, there must be at least one user defined. If no users are defined, the user manager cannot be enabled. This user must have administrative rights and be able to write to the access point and change the identity of the access point.

- **User** Manager: Click Enabled to enable user manager. Click Disable to disable the user manager. User manager provides the access point with a level of security that is common to wired networking components. An administrator would not want just anyone to telnet into their company's switch and make changes to the configuration. The same precautions should be taken with all access points.
- **Allow read-Only Browsing without Login?**: Click **yes** to allow any user to view the access point's basic screens. Click **no** to restrict access to all of the access point's screens to only the users in the user list. This can be very useful for preventing individuals from gaining access to your access point and information about your network, both wired and wireless.

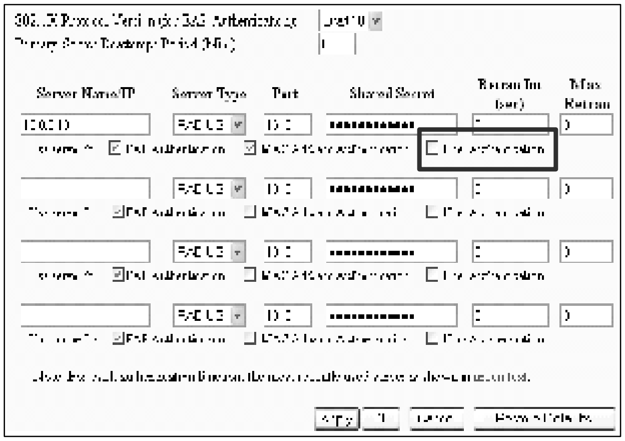
Additional Method for Enabling Access Point Console Security

Cisco.com

Centralized

Administrator

Authentication



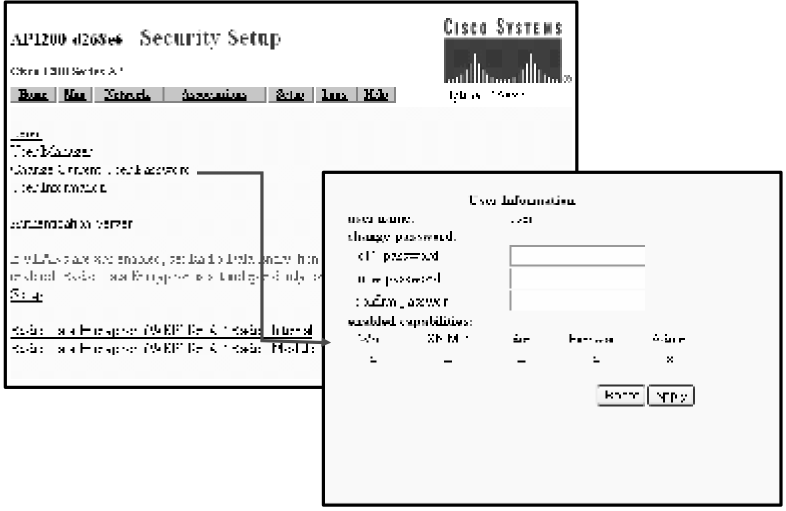
AWLF v3.1—9-10

Centralized Administrator Authentication

This feature allows the use of an AAA server to authenticate clients if the user manager functionality is enabled on the access point. At the end of a successful login, the AAA server verifies the user login and passes back the appropriate privileges for the user or an administrator.

User Password

Cisco.com



Security Setup

User Information

change password:

enabled capabilities:

Apply

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—9-11

To change a user’s password you must first access the **Security Setup** screen. From the **Security Setup** screen click **Change Current User Password**. The **User Information** screen will be displayed. To change a user’s password, enter the old password, the new password, and confirm the new password by entering the information on the spaces provided.

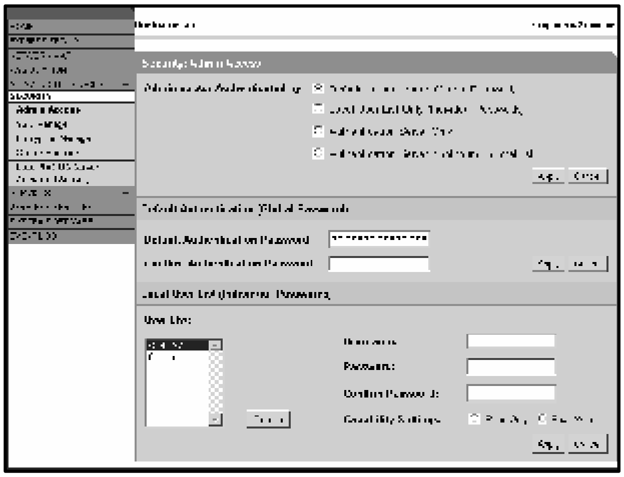
All enabled capabilities for the user will be displayed as an X under the listed **enabled capabilities**.

Click **Apply**.

Keep in mind that when logged in as a user, changing the user password will force the access point to then prompt the user to log in again with the new password before refreshing the screen.

Enabling Admin Access on IOS AP

Cisco.com



AWLF v3.1—9-12

There are a number of Administrator Authentication options in the Access Point for authentication and authorization of administrative users.

Under Administrator Authenticated by:

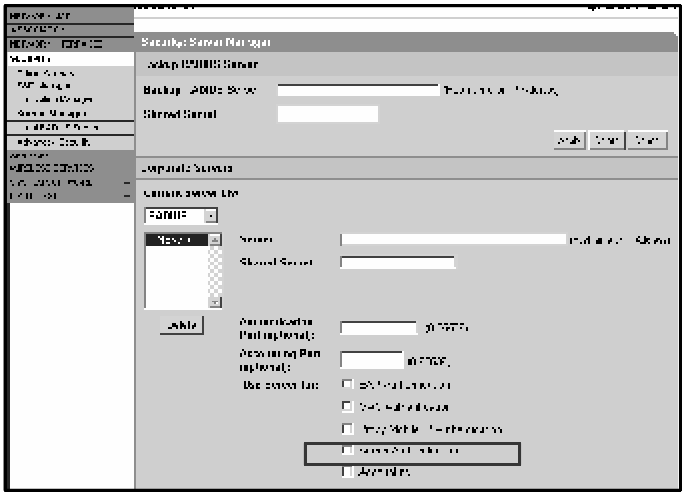
- **Default Authentication** (Global Password)- single password used for all administrators
- **Local User List Only** (Individual Passwords)- username/ passwords stored locally on AP & can be read only or read-write privilege.
- **Authentication Server Only-** users are authenticated/ authorized by a centralized authentication server- either TACACS+ or RADIUS.
- **Authentication Server is not found in Local List-** users are authenticated by Local list first, server if not found locally.

Note that the default setting is Default Authentication/ Global Password. If enabling either Local User List or Authentication Server, make sure that you have first enabled an Administrative User for yourself to avoid being locked out of the AP.

- **Local User List** permits the configuration of usernames/ passwords locally on the AP, along with their **Capability Settings**: (Read Only or Read/Write)

Authentication Server Configuration

Cisco.com



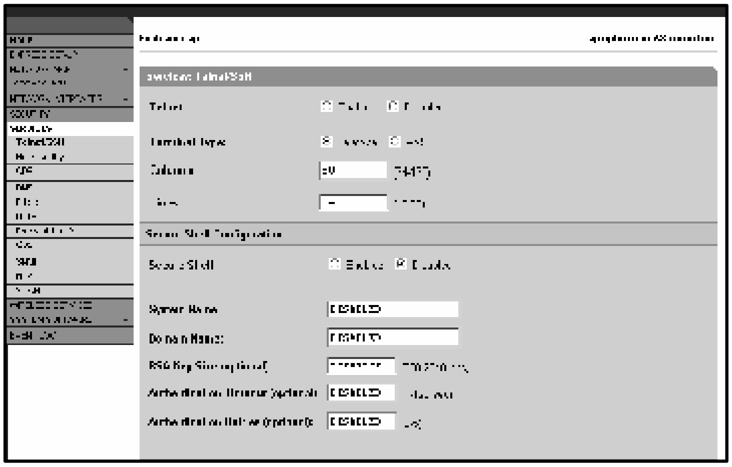
AWLF v3.1—9-13

If Access Point is enabled for Authentication Server Only or Authentication Server if not found in Local List, either a TACACS+ or RADIUS server may be used to provide authentication and authorization for Administrative users.

Via **Security**> **Server Manager**, the server used for Administrative user authentication is configured with its IP address or hostname entered in “**Server**:” field and **Shared Secret** string entered in textbox.

Use Server for: selection box should be set to **Admin Authentication** for TACACS+ or RADIUS administrative server.

Telnet/ SSH Configuration



Telnet

Columns: 80

Secure Shell Configuration

Secure Shell ○ Enable ● Disable

System Name: DISABLED

Domain Name: DISABLED

RSA Key Size (optional):

Authentication Timeout (optional): DISABLED

Authentication Retries (optional): DISABLED

For further restriction/ security on the access point’s administrative interface, Telnet access to the AP may be configured/ disabled from the Services> **Telnet/SSH** menu selection.

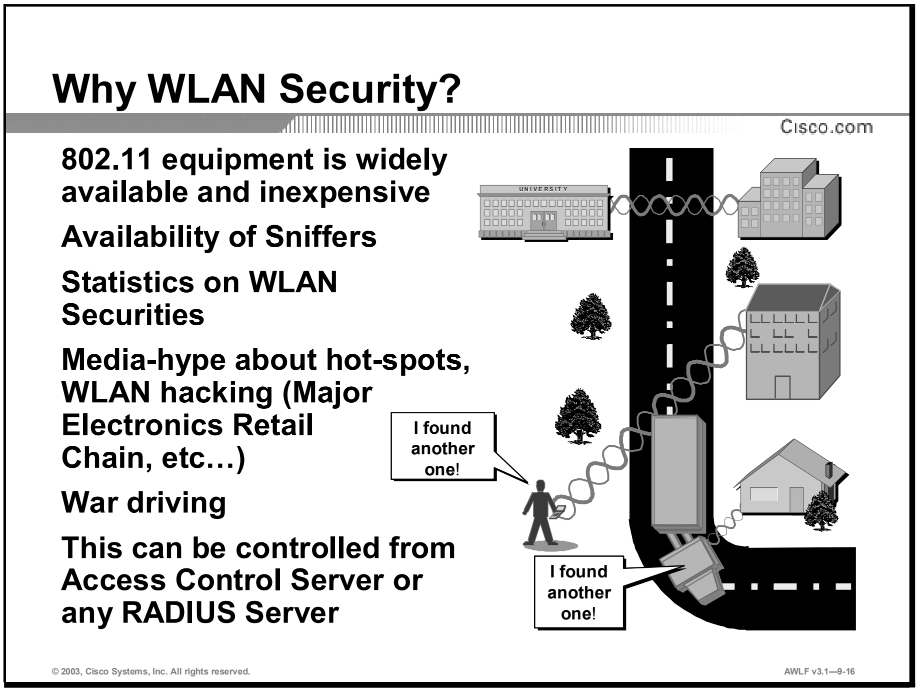
Secure Shell (SSH) is an application and a protocol that provides secure replacement for the suite of Berkeley r-tools such as rsh, rlogin and rcp. (Cisco IOS supports rlogin.) The protocol secures the sessions using standard cryptographic mechanisms, and the application can be used similarly to the Berkeley rexec and rsh tools.

The AP may be configured for SSH server functionality to secure and encrypt administrative sessions to the AP. This requires configuration of:

- **System Name**: system name used in generation of crypto key
- **Domain Name**: domain name used in generation of crypto key

After configuration of these parameters, a crypto key can be generated for a session initiated by an SSH client to the AP.

802.11 Security



Why WLAN Security?

Cisco.com

- 802.11 equipment is widely available and inexpensive
- Availability of Sniffers
- Statistics on WLAN Securities
- Media-hype about hot-spots, WLAN hacking (Major Electronics Retail Chain, etc…)
- War driving
- This can be controlled from Access Control Server or any RADIUS Server

UNIVERSITY
I found another one!
I found another one!

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—9-16

With the cost of 802.11b systems' coming down it is inevitable that hackers will have a lot more unsecured WLANs to choose from.

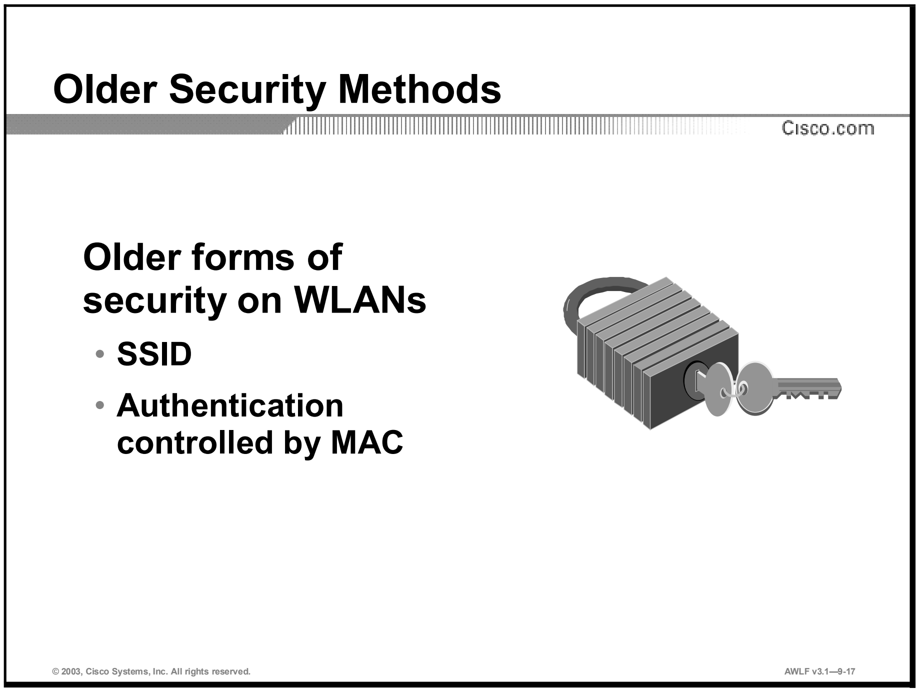
802.11b "Sniffers" enable network engineers (and hackers) to passively capture data packets so they can be examined to correct system problems.

War driving is a phrase that describes someone who is using a cellular scanning device looking for cell phone numbers to exploit. Now days, war driving refers to someone driving around with their laptop and an 802.11b client card looking for an 802.11b system to exploit.

A major electronics retail chain vulnerability became public in a May 1 posting to a mailing list on Security Focus Online, the Web site for a company that provides security threat management systems. The anonymous writer reported that he had been able to detect the network at a Major Electronics Retail Chain store from his car after installing a wireless card he purchased there in his laptop.

Running "kismet," a Linux network monitoring utility, he was able to record and examine packets of network data—and he claimed to have found what looked like credit card numbers in clear text within that data, along with other data about customer transactions and commands to the store's database. He also found that other major electronics retail chain stores in his area had wireless networks enabled.

This can be controlled by deploying an Access Control Server or any RADIUS Server that supports 802.1X over 802.11.



Older Security Methods

Cisco.com

Older forms of security on WLANs

- SSID
- Authentication controlled by MAC

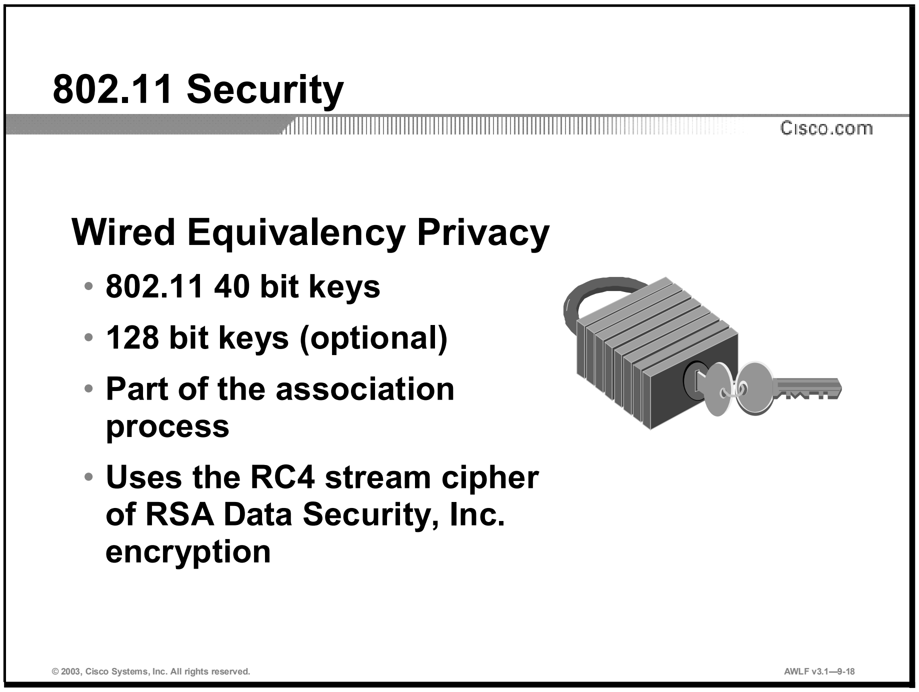
AWLF v3.1—9-17

In the past, security on WLANs was not a major concern. This was, in large part, due to the fact that WLANs were restrictive. Some of these restrictions were bandwidth, proprietary systems, and the inability to manage the WLAN as part of the LAN. The most common methods of securing the WLAN were the System Set Identifier (SSID) and the Authentication process.

The SSID a network-naming scheme that both the client and the access point must share. If the client did not have the proper SSID, it was unable to associate to the access point, and would have no access to the network.

As previous modules have shown, when connecting to an access point, a client must go through the process of authenticating and associating. Some WLANs support filtering by MAC address. Tables are manually constructed on the access point to allow or disallow clients based upon their physical hardware address.

With the new high speed 802.11 compliant products; users are now implementing WLANs to support more typical users. As company networks have progressed, and more valuable information is sent and kept electronically, security has become an issue. WLANs are no exception.



802.11 Security

Wired Equivalency Privacy

- 802.11 40 bit keys
- 128 bit keys (optional)
- Part of the association process
- Uses the RC4 stream cipher of RSA Data Security, Inc. encryption

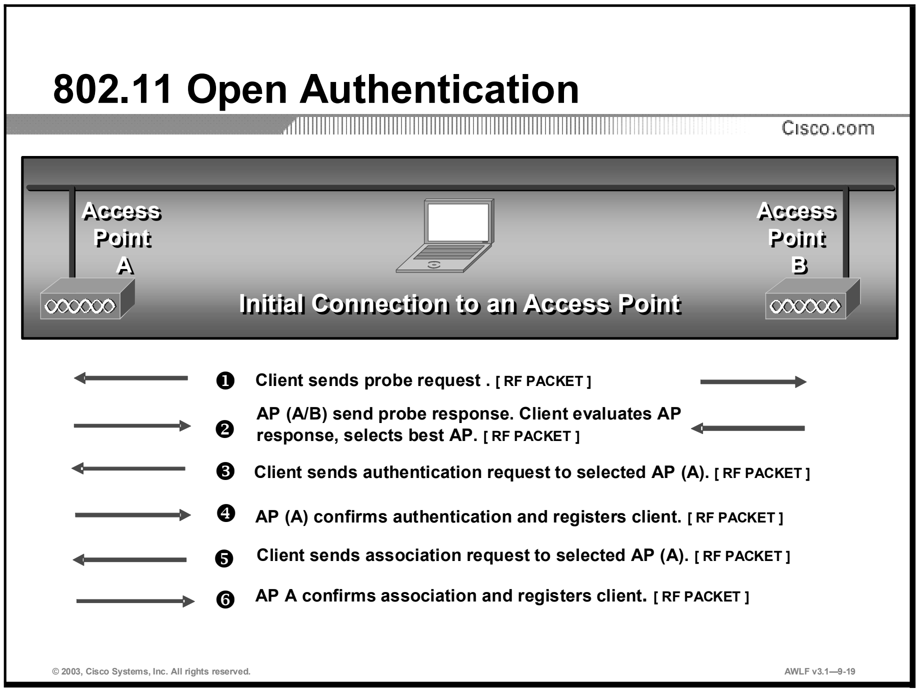
© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—9-18

The 802.11 standard define a type of security. This security is WEP (Wired Equivalency Privacy) using 40 bit keys. This method a wireless client and access point shared static WEP keys. This key is checked during the authentication process. If the client's WEP key does not match that of the access point, the client is not allowed to associate, and is unable to connect to the network.

WEP is based upon an existing and familiar encryption type, RC4. This allows encryption up to 128-bit. IEEE 802.11 has chosen to use 40-bit keys. Several vendors such as Proxim and Cisco Systems support 128-bit WEP encryption with their WLAN solutions for improved security. Cisco Aironet 128-bit devices will support both 40-bit and 128-bit encryption. Both the encrypting and decrypting endpoints must share the key. Key distribution or key negotiation is not mentioned in the standard.

The IEEE 802.11 standard provides two schemes for defining the WEP keys to be used on a wireless LAN. With the first scheme, a set of as many as four default keys are shared by all stations—clients and access points—in a wireless subsystem. When a client obtains the default keys, that client can communicate securely with all other stations in the subsystem. The problem with default keys is that when they become widely distributed they are more likely to be compromised. Cisco Systems uses this method. In the second scheme, each client establishes a "key mapping" relationship with another station. This is a more secure form of operation because fewer stations have the keys, but distributing such unicast keys becomes more difficult as the number of stations increases.



802.11 Open Authentication

Cisco.com

❶ Client sends probe request . [RF PACKET]

❷ AP (A/B) send probe response. Client evaluates AP response, selects best AP. [RF PACKET]

❸ Client sends authentication request to selected AP (A). [RF PACKET]

❹ AP (A) confirms authentication and registers client. [RF PACKET]

❺ Client sends association request to selected AP (A). [RF PACKET]

❻ AP A confirms association and registers client. [RF PACKET]

AWLF v3.1—9-19

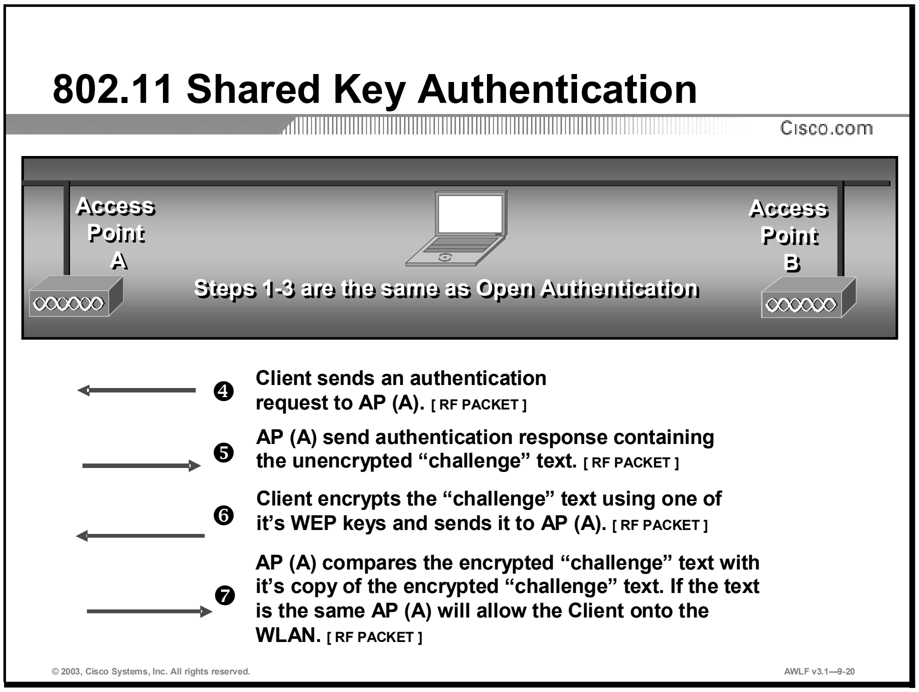
Two types of WEP encryption are defined: Open and Shared Key. This section will look at both of these and the process the client undergoes during the authentication process.

Open Authentication

The Open Authentication method allows authorization and associations with or without a WEP key. If the client does not use a WEP key, the client undergoes the normal association process with the access point. The user is then granted access to the network.

If a WEP key is used, both the client and the access point must have matching WEP keys. If the client uses a WEP key(s) that is different than the WEP key(s) of the access point, data traffic cannot be passed because the *data* is encrypted. Keep in mind that the header is not encrypted; only the payload (or data) is encrypted.

Using Open Authentication, the client goes through the normal association process, whether or not the client is using a WEP key. Once the client is associated, and data transmission begins, a client using a WEP key will encrypt the data. If the WEP key on the access point does not match, then the access point is unable to decrypt the data so it is impossible to send data via the WLAN.



802.11 Shared Key Authentication

Cisco.com

Access Point A

Access Point B

Steps 1-3 are the same as Open Authentication

❹ Client sends an authentication request to AP (A). [RF PACKET]

❺ AP (A) send authentication response containing the unencrypted “challenge” text. [RF PACKET]

❻ Client encrypts the “challenge” text using one of it’s WEP keys and sends it to AP (A). [RF PACKET]

❼ AP (A) compares the encrypted “challenge” text with it’s copy of the encrypted “challenge” text. If the text is the same AP (A) will allow the Client onto the WLAN. [RF PACKET]

AWLF v3.1—9-20

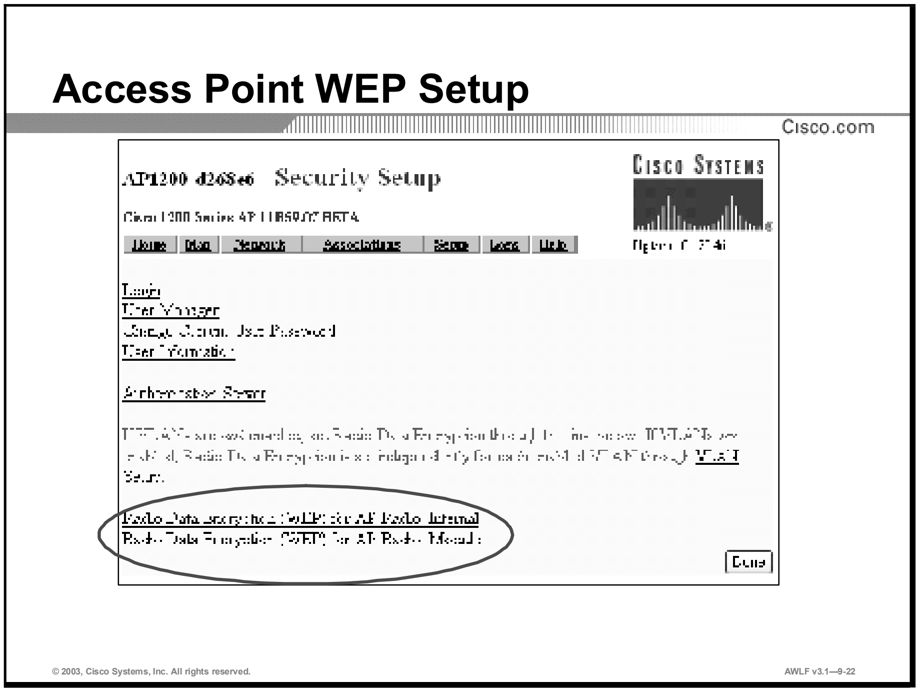
Shared Key Authentication

Note Steps 1-3 are the same as Open Authentication, but this time Shared Key Authentication will be used. Using Shared Key Authentication the wireless client will attempt to associate with an access point.

1. The client sends an Authentication Request to Access Point (A).
2. Access Point (A) sends an authentication response. The authentication response from the access point to the client is sent containing “challenge” text. This packet is unencrypted.
3. The client then uses the text from the authentication response to form another authentication packet, which will be encrypted using one of the client’s WEP keys, and sends this as a response to the access point.
4. Access Point (A) will then compare the encrypted “challenge” text against the access point’s own copy of the encrypted “challenge” text. If the encrypted text is the same, then the access point allows the client on the WLAN.

Shared Key Authentication is considered less secure than OPEN Authentication because of the challenge text packet. Because this packet is sent unencrypted and then returned as an encrypted packet, it may be possible to capture both packets and determine the stream cipher.

Configuring the Access Point for WEP



Access Point WEP Setup

AP1200 d268e6 Security Setup

Cisco 1200 Series AP 11.85 [illegible] BETA

Login
User Manager
Change Current User Password
User Information

Authentication Server

If VLANs are not enabled, set Radio Data Encryption through the links below. If VLANs are enabled, Radio Data Encryption is set independently for each enabled VLAN through VLAN Setup.

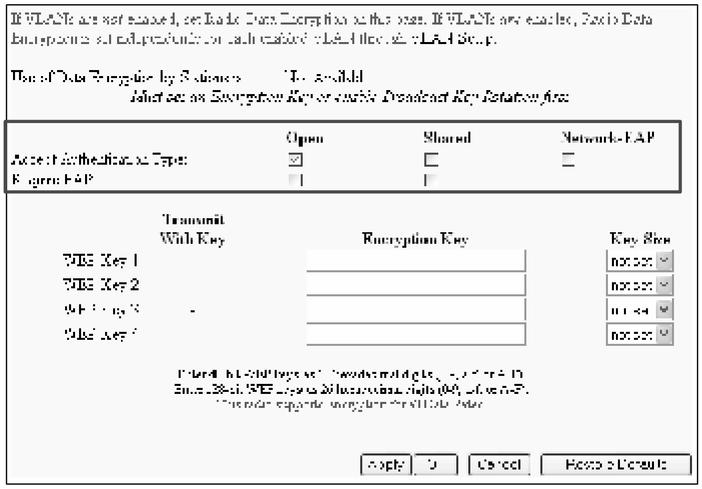
Radio Data Encryption (WEP) for AP Radio Internal
Radio Data Encryption (WEP) for AP Radio Module

AWLF v3.1—9-22

From the **Security Setup** screen, click on **Radio Data Encryption (WEP)** to launch the WEP configuration screen.

Access Point WEP Setup (Cont.)

Cisco.com



If VLANs are not enabled, set Radio Data Encryption on this page. If VLANs are enabled, Radio Data Encryption is set independently for each enabled VLAN through VLAN Setup.

Use of Data Encryption by Stations: Not Available

Must set an Encryption Key or enable Broadcast Key Rotation first.

	Open	Shared	Network-EAP
Accept Authentication Type:	☑	□	□
Require EAP:	□	□	

	Transmit With Key	Encryption Key	Key Size
WEP Key 1			not set
WEP Key 2			not set
WEP Key 3	-		not set
WEP Key 4			not set

Enter 40-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F).
Enter 128-bit WEP keys as 26 hexadecimal digits (0-9, a-f, or A-F).
This radio supports encryption for all Data Rates.

AWLF v3.1—9-23

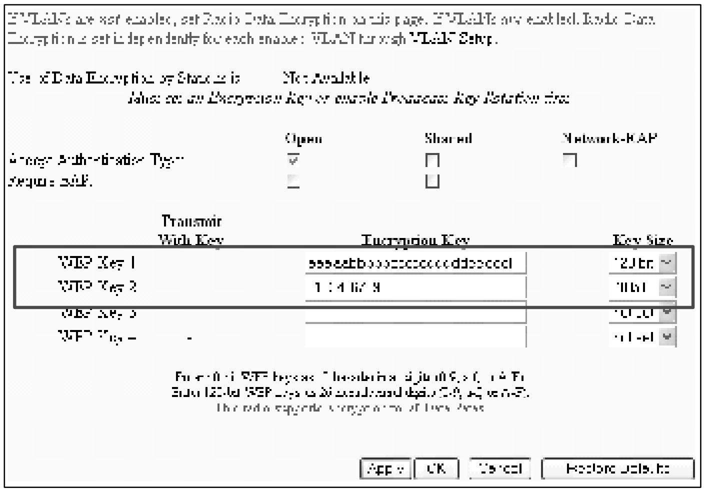
To configure WEP, an encryption type must be chosen by checking the appropriate box.

- **Open (default)**: Allows any device, regardless of its WEP settings, to authenticate and then attempt to communicate with the access point.
- **Shared Key**: The access point sends a plain text, shared-key query to any device attempting to communicate with the access point. This query can leave the device open to a known-text attack from intruders, however, and is therefore not as secure as the Open setting.
- **Network-EAP**: The access point uses the Extensible Authentication Protocol (EAP) to interact with an EAP-compatible RADIUS server on your network to provide authentication for wireless client devices.

The standard 802.11 WEP can be used without using EAP or an authentication server, allowing for data encryption between the clients and the access point. Using 802.11 WEP does not encrypt all data on the network. Only the data sent between the client and the access point will be encrypted.

Access Point WEP Setup (Cont.)

Cisco.com



If VLANs are not enabled, set Radio Data Encryption on this page. If VLANs are enabled, Radio Data Encryption is set independently for each enabled VLAN through VLAN Setup.

Use of Data Encryption by Stations is: Not Available

Must set an Encryption Key or enable Broadcast Key Rotation first

	Open	Shared	Network-EAP
Accept Authentication Type:	☑	□	□
Require EAP:	□	□	

	Transmit With Key	Encryption Key	Key Size
WEP Key 1		[illegible]	128 bit
WEP Key 2		[illegible]	40 bit
WEP Key 3			not set
WEP Key 4			not set

Enter 40-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F).
Enter 128-bit WEP keys as 26 hexadecimal digits (0-9, a-f, or A-F).
This radio supports Encryption for all Data Rates.

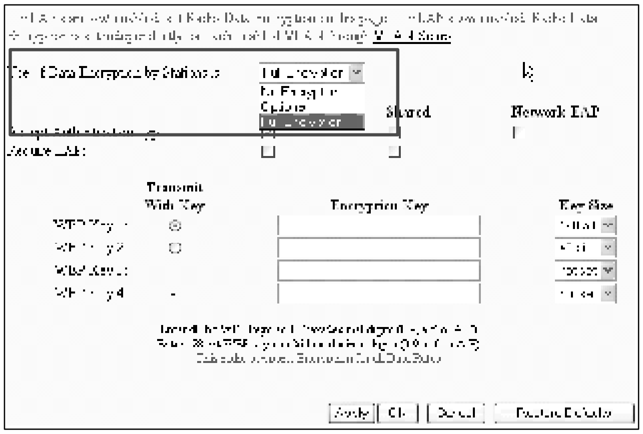
AWLF v3.1—9-24

- **Transmit With Key:** These buttons allow you to select the key this access point will use when transmitting data. Only one key can be selected at a time. All set keys can be used to receive data. The selected key must already be set before it can be specified as the Transmit key.
- **Encryption Key:** These fields allow you to enter the WEP keys. Type ten hexadecimal digits (any combination of 0-9, a-f, or A-F) for 40-bit WEP keys. Type 26 hexadecimal digits (any combination of 0-9, a-f, or A-F) for 128-bit WEP keys. To protect WEP key security, existing WEP keys do not appear in the entry fields. You can write over existing keys, but you cannot edit or delete them.
- **Key Size:** Use this setting to set the keys to either 40 or 128-bit WEP. If "not set" appears for this selection, the key has not been set.

Note	You cannot delete a key by selecting "not set." You may use the Restore Defaults button to remove all WEP Keys.

Access Point WEP Setup (Cont.)

Cisco.com



AWLF v3.1—9-25

Uses of data Encryption by Stations are:

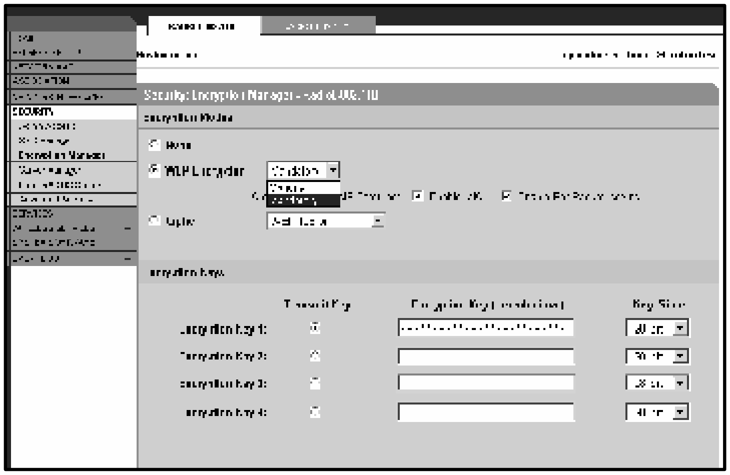
- No Encryption (default): The access point communicates only with client devices that are not using WEP.
- Optional: Client devices can communicate with the access point either with or without WEP.
- Full Encryption: Client devices must use WEP when communicating with the access point. Clients not using WEP are not allowed to communicate.

If using Network-EAP as the authentication method then a key must be set in the WEP Key 1 slot. This is the key that is used for multicast packets and is sent during the authentication process.

The access point is not restricted to use of only 40-bit or 128-bit keys and any combination of 40-bit and 128-bit keys may be used.

IOS Access Point WEP Setup

Cisco.com



AWLF v3.1—9-26

Static WEP key encryption may be enabled on the Cisco IOS AP from the Security> **Encryption Manager** screen.

Under **Encryption Modes**, select WEP Encryption and either **Optional** or **Mandatory** WEP Encryption

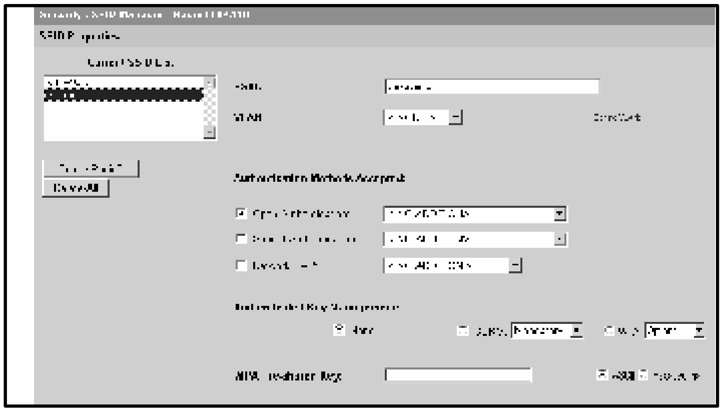
For additional encryption protection when using Cisco client cards, you may also enable Message Integrity Check (MIC) and Per Packet Keying (TKIP). These features minimize the vulnerability of the WEP protocol to either Man-in-the-middle (inductive) key attacks or passive key attacks.

Under **Encryption Keys**, enter the **Encryption Key** in hexadecimal format and select the appropriate **Key Size** and select the **Transmit Key** index.

Note that, if using a dynamic key derivation (802.1X) mechanism, it is necessary to enter a key under Encryption Key for broadcast only, the unicast key will be derived for each client using the 802.1X mechanism.

Authentication Mechanisms and WEP

Cisco.com



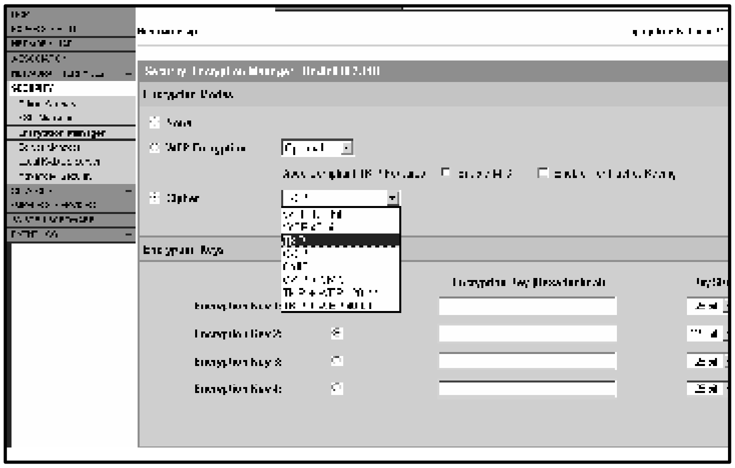
To fully configure WEP, an authentication method should be specified by checking the appropriate box.

- **Open (default):** Allows any device, regardless of its WEP settings, to authenticate and then attempt to communicate with the access point.
- **Shared Key:** The access point sends a plain text, shared-key query to any device attempting to communicate with the access point. This query can leave the device open to a known-text attack from intruders, however, and is therefore not as secure as the Open setting.
- **Network-EAP:** The access point uses the Extensible Authentication Protocol (EAP) to interact with an EAP-compatible RADIUS server on your network to provide authentication for wireless client devices.

By default, Open authentication is enabled, which, if WEP key is enabled, will permit authentication only be devices which have the correct WEP key configured.

WPA (Authenticated Key Mgmt)

Cisco.com



WiFi Protected Access (**WPA**) is the WiFi Alliance standards-based mechanism to create secure and interoperable WLAN networks. WPA provides a mechanism to authenticate keys for use in 802.11 environments as well as providing enhancements to WEP encryption to increase the robustness of the security protocol.

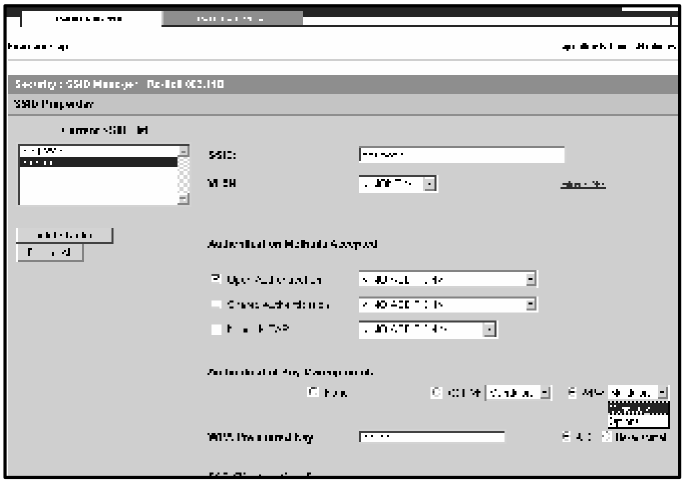
To enable WPA on an access point, an appropriate **Cipher** (or combination of ciphers) must be chosen. TKIP is the cipher used for WPA compliant devices. The following are valid WPA ciphers:

- TKIP
- TKIP + WEP 128 bit
- TKIP + WEP 40 bit

Also note that when using WPA encryption on an access point, Encryption Key 1 must not be used- as the WPA key negotiation mechanism uses this key position in the AP to transfer authentication data to the client.

WPA (Cont.)

Cisco.com



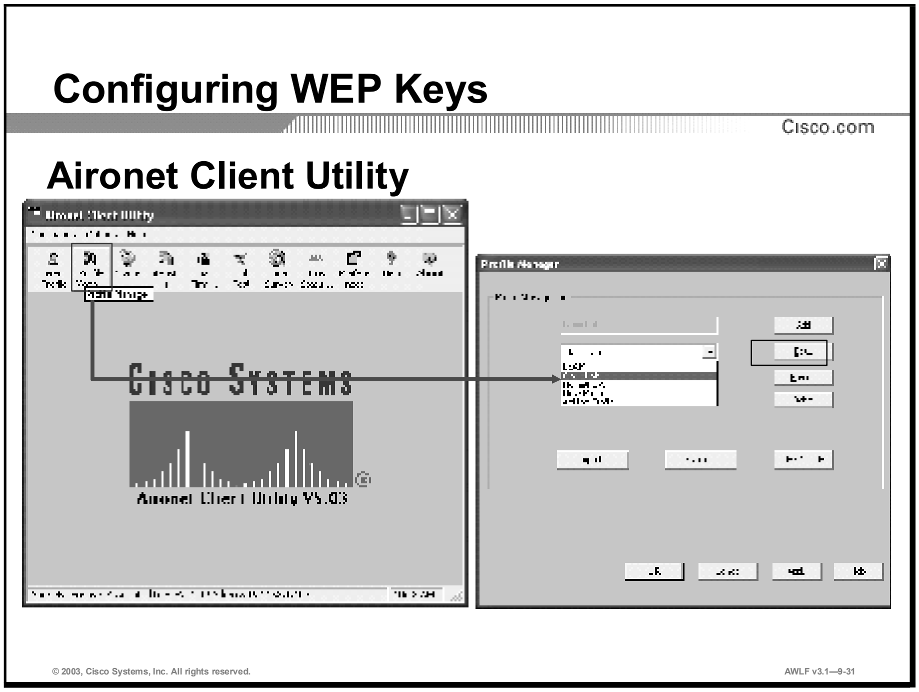
AWLF v3.1—9-29

In order to enable WPA Authentication on the AP, after enabling the Encryption mechanism which supports WPA, the SSID must be configured to use a form of **Authenticated Key Management**.

For the selected SSID, under the **Authenticated Key Management** section, select **WPA** and select the appropriate dropdown menu selection, either **Mandatory** for WPA-only clients, or **Optional** for coexistence between WPA and legacy WEP clients.

If using a **WPA Pre-shared Key** (as opposed to using 802.1X authentication), enter the Pre-shared key in either ASCII text (minimum 8 characters) or via a hexadecimal string (64 hex characters). Note that this same pre-shared key must be configured on the WPA client.

Configuring the Client for WEP



Configuring WEP Keys

Cisco.com

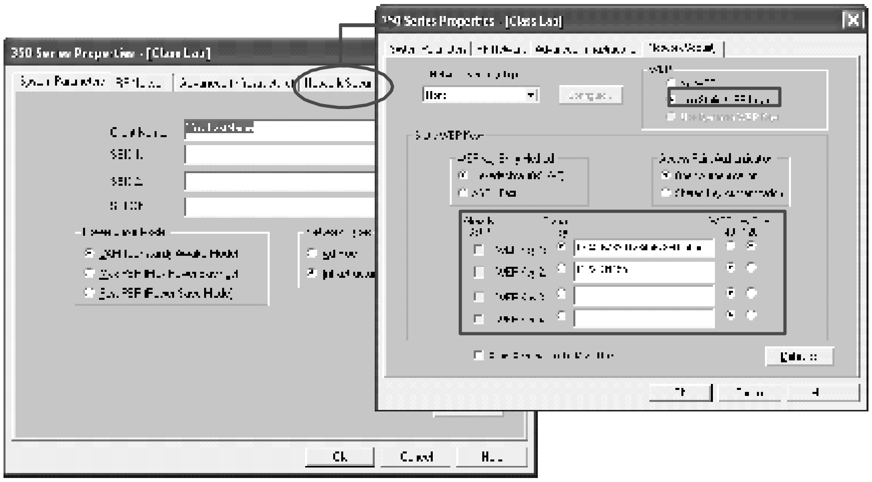
Aironet Client Utility

AWLF v3.1—9-31

Static WEP keys are set on the client using the **Aironet Client Utility (ACU)**. From the ACU, click **Profile Manager**. This will launch the **Profile Manager** screen. From the **Profile Manager**, choose the desired profile from the drop down box and click the **Edit** button.

Configuring WEP Keys (Cont.)

Cisco.com


350 Series Properties - [Class Lab]
350 Series Properties - [Class Lab]

AWLF v3.1—9-32

Once the desired profile is brought up, click the **Network Security** tab. This will allow you to view and edit the Security settings for this profile.

To set up static WEP keys, click the **Use Static WEP Keys** radio button under WEP. Once this button has been checked, the WEP keys can be entered.

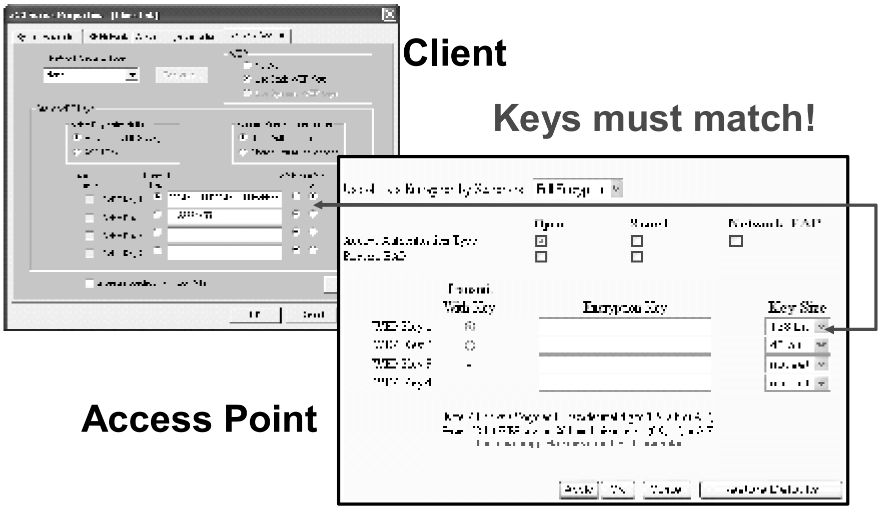
The WEP keys are entered here just as they are on the access point. 26 hexadecimal characters (13 bytes) for 128-bit, 10 hexadecimal characters (5 bytes) for 40-bit. Choose the key size by checking the appropriate radio button next to the WEP key entry box. Once a WEP key is entered, it can be overwritten, but it cannot be edited or deleted. Up to four keys may be configured.

- **Access Point Authentication:** Choose which type of authentication will be used, **Open Authentication** (default, more secure) or **Shared Key** Authentication (less secure).
- **WEP Key Entry Method:** You can choose to enter the WEP key as hexadecimal characters, or as ASCII text. The default is hexadecimal characters.
- **Allow Association to Mixed Cells**: If a client is to associate with an access point using Optional WEP (Open Authentication supporting both encrypted and non-encrypted clients) this box must be checked.

Note If this box is not checked, the client will be able to communicate with clients configured for Full Encryption only.

Configuring WEP Keys (Cont.)

Cisco.com



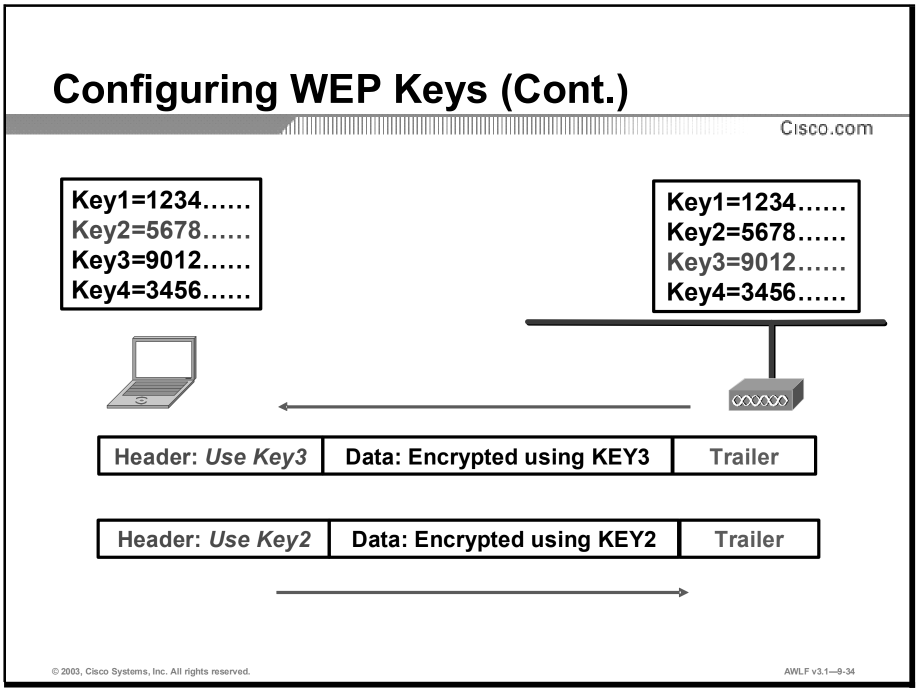
Client

Keys must match!

Access Point

AWLF v3.1—9-33

No matter which type of authentication is used, the WEP keys entered on the client and the access point must match. The key(s) themselves must match, and the order of the key(s) must match (i.e., 40 bit key entered as Key 1 on the client must match the 40 bit key entered as Key 1 on the access point).



Configuring WEP Keys (Cont.)

Key1=1234……
Key2=5678……
Key3=9012……
Key4=3456……

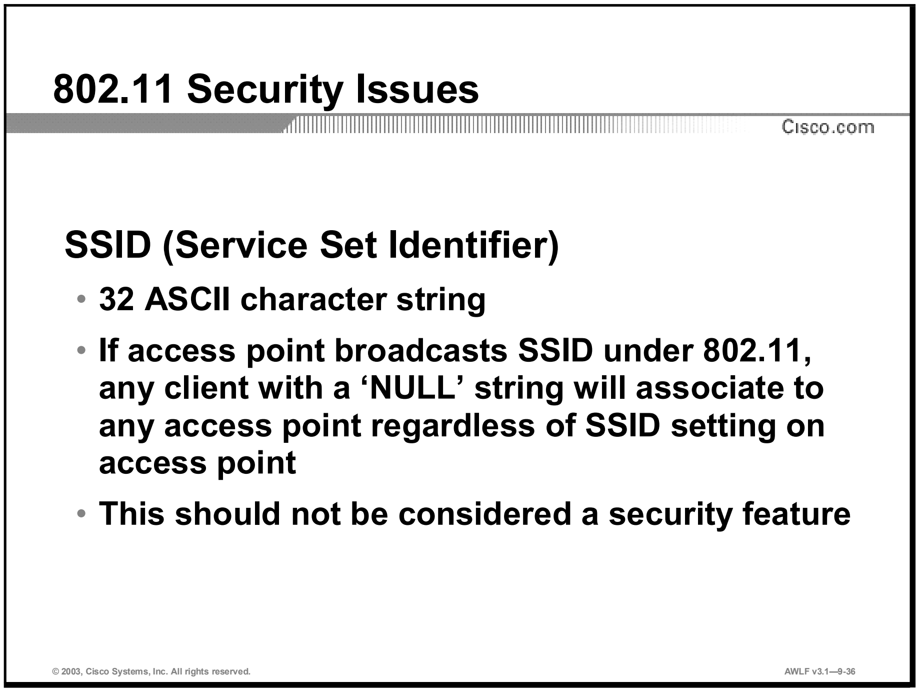
Key1=1234……
Key2=5678……
Key3=9012……
Key4=3456……

Header: *Use Key3*	Data: Encrypted using KEY3	Trailer

Header: *Use Key2*	Data: Encrypted using KEY2	Trailer

The reason the order of the keys must match is because a transmit key will have to be chosen. When sending encrypted data, the client (or access point) will use the transmit key to encrypt the packet. The Transmit Key information is included in the packet’s header. This lets the access point (or client) know which key to use to decrypt the packet.

Problems with 802.11 WEP Security



802.11 Security Issues

Cisco.com

SSID (Service Set Identifier)

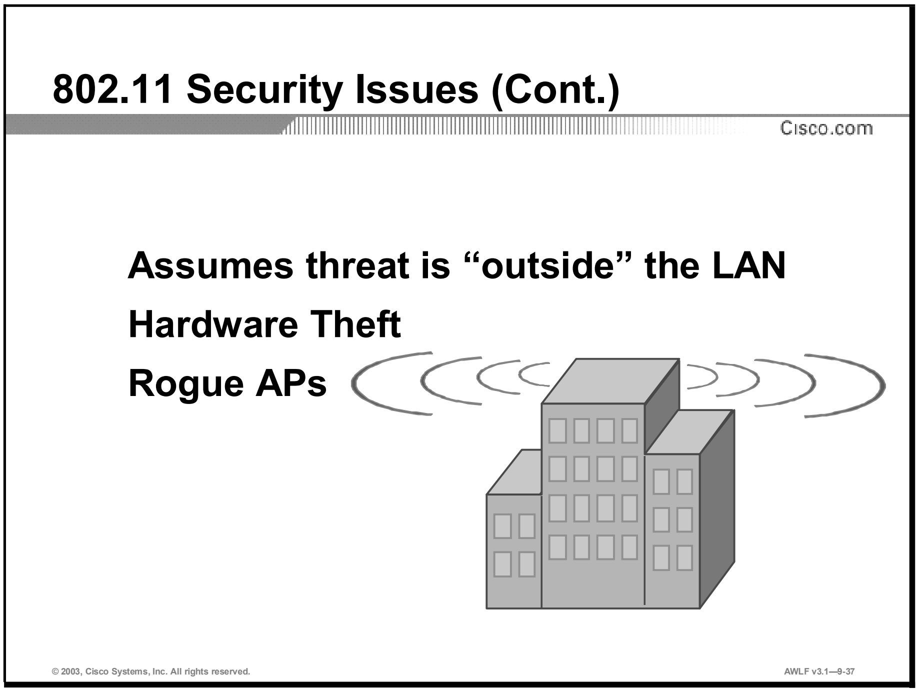
- 32 ASCII character string
- If access point broadcasts SSID under 802.11, any client with a 'NULL' string will associate to any access point regardless of SSID setting on access point
- This should not be considered a security feature

AWLF v3.1—9-36

The SSID is a configurable parameter that must match on both the wireless client and the access point. This value is checked as part of the association process. If a wireless client does not possess the proper SSID it may not be able to associate. In the past this was used WLANs to provides some measure of security. But as WLANs have changed, this feature now offers at best a rudimentary level of security.

The SSID feature serves to logically segment the users and access points that form part of a wireless subsystem. Under 802.11 specifications, an access point may "advertise" or broadcast its SSID. During the association process, any 802.11 wireless clients with a "null" (no value entered into the SSID field) will request that the access point broadcast its SSID. If the access point is so configured, it will send the SSID to the client. The client will then use this SSID to associate to the access point.

For these reasons, the SSID should not be considered a security feature on the Cisco Aironet Wireless LAN products.



802.11 Security Issues (Cont.)

Cisco.com

Assumes threat is “outside” the LAN

Hardware Theft

Rogue APs

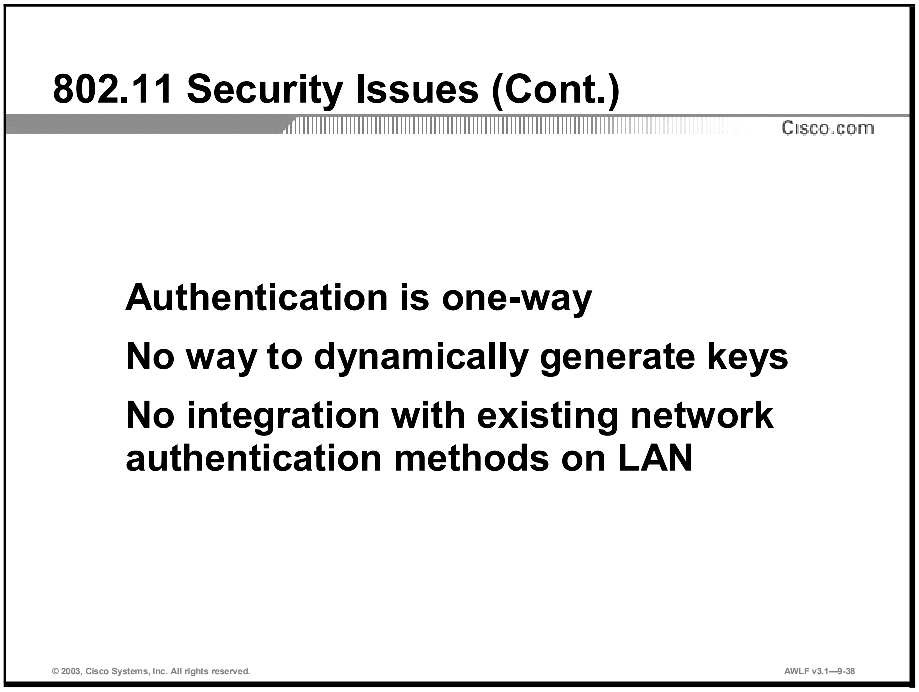
© 2003, Cisco Systems, Inc. All rights reserved. AWLF v3.1—9-37

802.11 WEP security makes the assumption that the threat to network security is located “outside” the LAN, meaning that the concern is that someone could “hack” into the network. There is no real protection from users who have been granted access to the network.

If persistent WEP Keys are assigned to a client adapter, and the adapter is stolen, then the adapter still contains those keys. A stolen card could then be used to access the WLAN. The measure of protection against such intrusions is if the card is reported stolen, and the MAC address then disallowed. Then all of the WEP Keys must be changed. As there is no way to remotely administer WEP Keys, this could be a very burdensome task (depending on the number of wireless devices).

Someone trying to hack into the network may wirelessly attach an access point to the LAN (repeater) without anyone’s knowledge. A “rogue access point” is an access point that has been placed on a WLAN and might be used to interfere with normal network operations (denial of service attacks, for example). This access point may also provide unwanted users with information about the network such as MAC addresses of clients (both wireless and wired), the ability to capture and spoof data packets, and at worst, access to servers and files.

Another problem is that an allowed user may unknowingly attach an access point to a LAN, not realizing that they may be granting access to unwanted users.



802.11 Security Issues (Cont.)

Authentication is one-way

No way to dynamically generate keys

No integration with existing network authentication methods on LAN

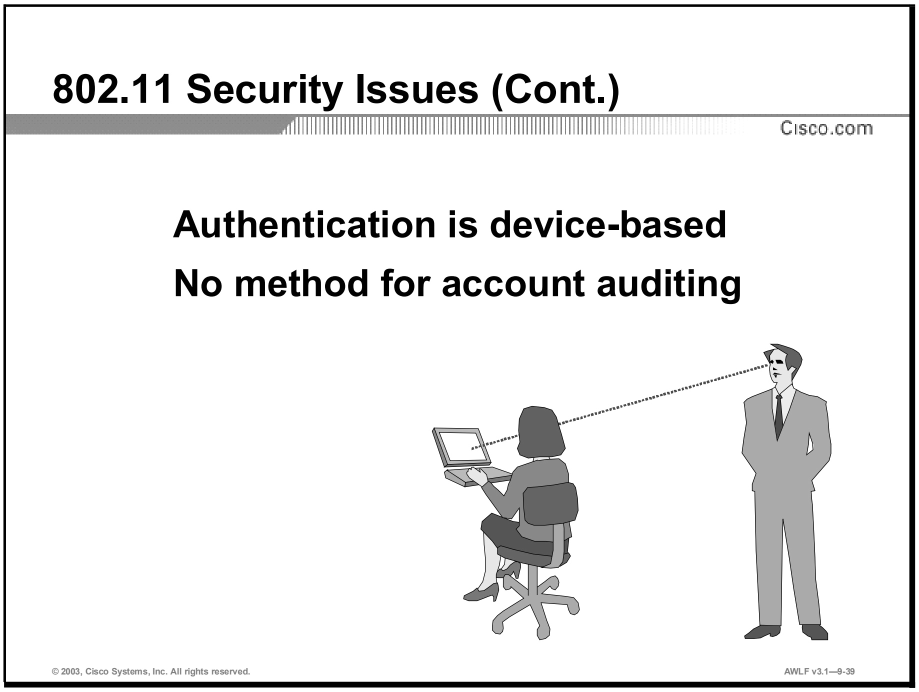
AWLF v3.1—9-38

There are other issues with the 802.11 security methods having less to do with hardware, and more to do with administration. One of these issues is the WEP encryption is a one-way authentication.

The client is authenticated with the access point, but not vice-versa. The client has no way of knowing if the access point is actually an allowed access point or potentially a rogue access point.

No matter which method of authentication is used, the keys are entered statically. There is no way to generate or administer keys remotely. The best method of security is to frequently change WEP Keys. But without the ability to remotely administer these keys, this can be a daunting task. Changing keys on a global basis could be a tremendous task.

There is also no way to integrate with existing network authentication methods, such as the Lightweight Directory Access Protocol (LDAP) or Remote Access Dial Up Service (RADIUS).



802.11 Security Issues (Cont.)

Cisco.com

Authentication is device-based

No method for account auditing

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—9-39

The authentication is also device-based. With this method identification is based upon MAC address, not username. And keys are typically stored in the flash memory of the card. As we have already seen, a stolen card could circumvent this authentication method. A more effective method is for authentication to be dependent on usernames and passwords, which are client independent, and which users may already possess.

But even if authentication were based upon username and password, we would still want to be able to audit and/or account for usage to warn against unusual activities, such as:

- Unusual activity
- Users who don't log in for long periods of time
- Users who transfer too much data, stay on too long
- Multiple simultaneous logins. Logins from "wrong" account

In other words, what is needed is the ability to administer and monitor wireless clients just as you would wired clients.

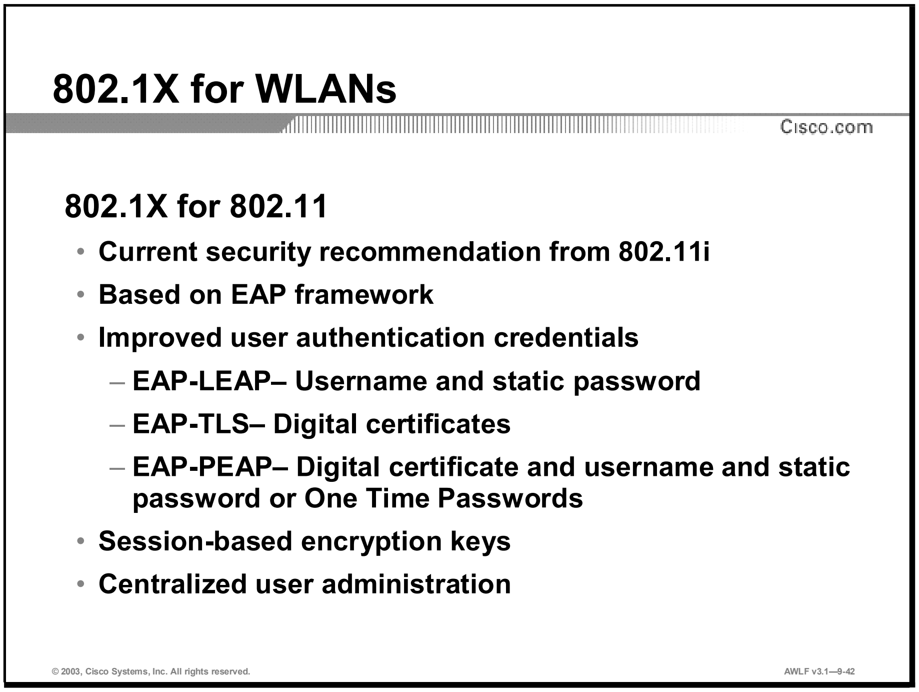
To increase the security of the 802.11 standards-based WEP, Cisco supports an implementation of IEEE 802.11 Task Group i recommendations which is part of Cisco's Temporal Key Integrity Protocol:

- **IV Key Hashing:** An initialization vector (IV) is used to alter the key stream. The IV is a numeric value that is concatenated to the base key before the key stream is generated. Every time the IV changes, so does the key stream. The 802.11 standard recommends that the IV change on a per-frame basis. This way, if the same packet is transmitted twice, the resulting cipher-text will be different for each transmission.
- **Message Integrity Check** (MIC) prevents bit-flip attacks on encrypted packets. During a bit-flip attack, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. The client adapter's driver and firmware must support MIC functionality, and MIC must be enabled on the access point.

- **Broadcast Key Rotation** is a security feature for use with dynamic WEP keys. If your client adapter uses LEAP or EAP-TLS authentication and you enable this feature, the access point changes the dynamic broadcast WEP key that it provides at the interval you select.

Cisco also supports the pre-802.11i Wi-Fi Protected Access industry standard.

Security Suite



802.1X for WLANs

Cisco.com

802.1X for 802.11

- **Current security recommendation from 802.11i**
- **Based on EAP framework**
- **Improved user authentication credentials**
  - **EAP-LEAP– Username and static password**
  - **EAP-TLS– Digital certificates**
  - **EAP-PEAP– Digital certificate and username and static password or One Time Passwords**
- **Session-based encryption keys**
- **Centralized user administration**

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—9-42

The IEEE is working on a supplement to the 802.1d standard which will define the changes necessary to the operation of a MAC layer bridge in order to provide Port based network access control capability. This is the 802.1X standard.

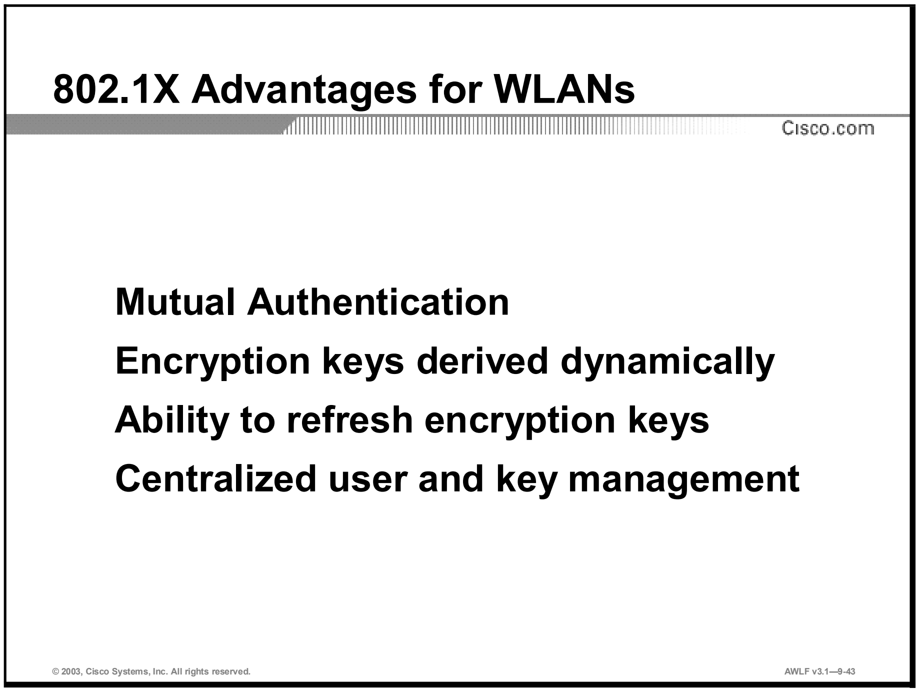
802.1X will offer:

- RADIUS/EAP for encapsulation of EAP packets within RADIUS.
- Identification based on Network access identifier.
- Support for roaming access in public spaces.
- RADIUS support for centralized authentication, authorization, and accounting.
- WEP keys that will be dynamic instead of static and will no require user intervention based management.
- Compatibility with existing roaming technologies, enabling use in hotels and public places.

Note EAP-LEAP: Cisco (EAP) **E**xtensible **A**uthentication **P**rotocol

Note EAP-TLS: **T**ransport **L**ayer **S**ecurity

Note EAP-PEAP: **P**rotected **E**xtensible **A**uthentication **P**rotocol



802.1X Advantages for WLANs

Mutual Authentication

Encryption keys derived dynamically

Ability to refresh encryption keys

Centralized user and key management

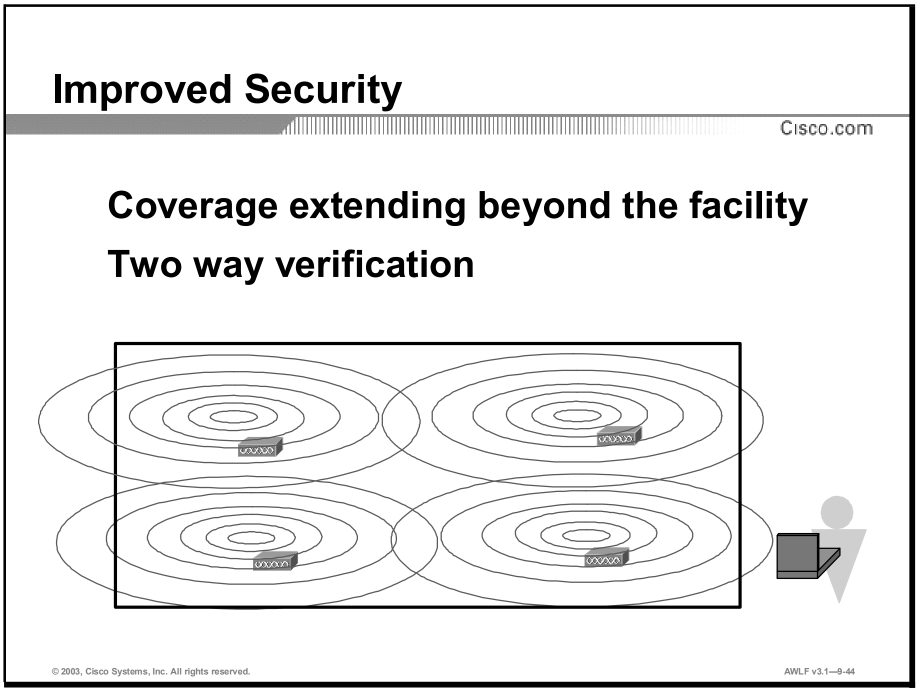
© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—9-43

By providing support for the Extensible authentication protocol (EAP) the 802.1X standards is designed to leverage existing standards. Support for EAP, WLANs can now offer:

- Support for RFC 2284, with password authentication. Users are authenticated based upon username and password that is typically already stored in an active directory on the network. This directory is then connected to a certificate server, such as a RADIUS server or the Cisco access control server (ACS).
- **One-Time Passwords (OTP):** OTP takes a plaintext password and will encrypt it. Then plaintext passwords will never have to be typed on a non-secure connection (telnet and ftp use no encryption and therefore are not considered secure protocols).

EAP support is designed to allow additional authentication methods to be deployed with no changes to the access point or client NIC. Nothing beyond the latest versions of firmware and drivers are required for the Cisco Aironet equipment to take advantage of the benefits offered with EAP.



Improved Security

Coverage extending beyond the facility

Two way verification

© 2003, Cisco Systems, Inc. All rights reserved.

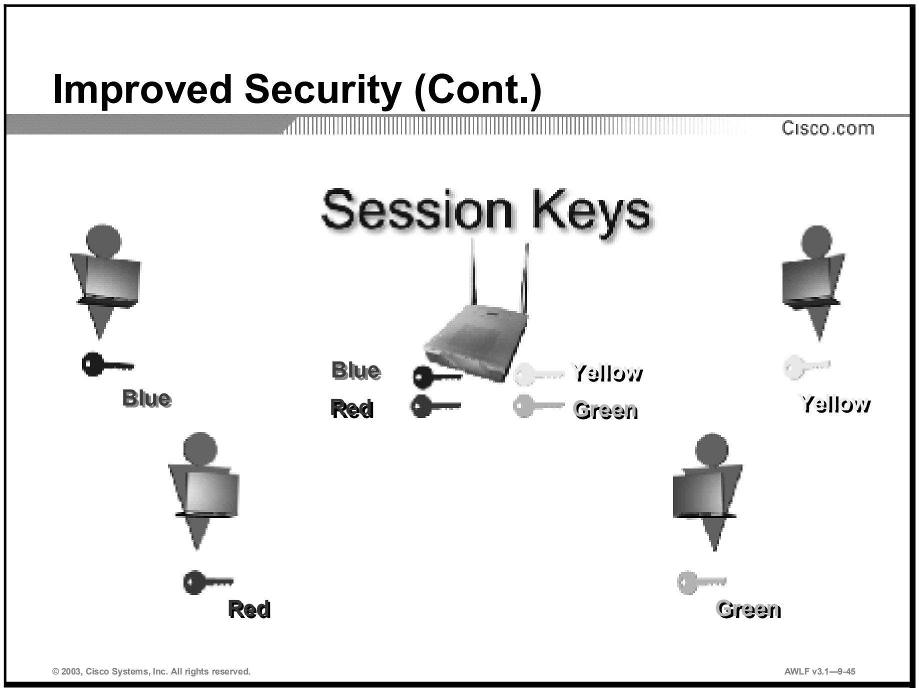
AWLF v3.1—9-44

One of the main concerns with implementing WLAN technology into networks is that WLANs “put my ports” on the outside of the facility, meaning that the wireless signal extends beyond the building, to the parking lot for example. Without any form of security an intruder could potentially use any 802.11 compliant card to access the network. And even when using WEP security, it might be possible for an intruder to capture network traffic outside the building and learn the system WEP keys. Because wireless traffic is broadcasted, and not directed to an individual, anyone with a wireless card could potentially get into the system.

Using the security features on the Cisco Aironet products allows for two-way verification. With RADIUS server support, the client verifies that the access point is an allowed access point while at the same time the access point verifies that the client is allowed. This means a secure channel and secures transmissions.

A user may associate to an access point but would not be granted access to network resources until the user performed a network logon. All attempts to gain access to the network resources will be blocked until the network logon is performed. And because all data is encrypted, a user trying to capture data outside the facility would not be able to use the data.

One of the biggest benefits of 802.1X is that it provides very strong authentication. Stealing or deriving a WEP key or spoofing a MAC address is no longer sufficient for gaining access to the WLAN.



Improved Security (Cont.)

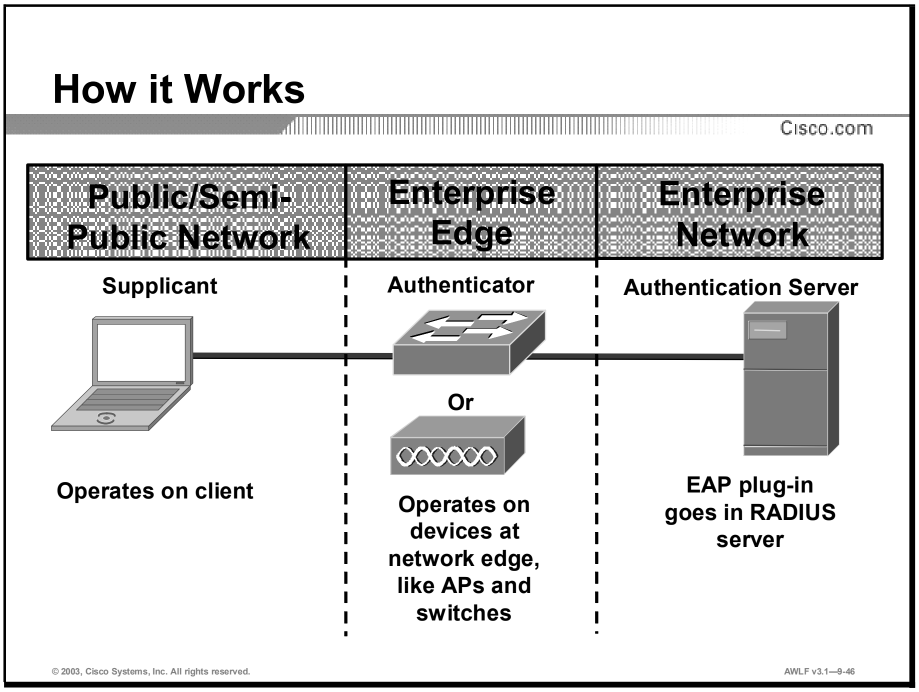
Cisco.com

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—9-45

An unauthorized user would not even be allowed to send any data through the access point. The process a client undergoes while "attaching" with an access point is two part, authentication and association. Authentication is the process of verifying the credentials of a client desiring to join a WLAN. Association is the process of associating a client with a given access point in the WLAN.

Using Cisco Aironet's security features means that each wireless client can be granted a new, dynamic WEP key each time they access the network. Because these keys are dynamic and session based, an intruder cannot learn the system WEP keys and then use them to access the WLAN. WEP keys administered in this fashion are referred to as "session" keys. Each user will have a unique WEP key. The access point will have all of the WEP keys for each associated client, thus allowing it to communicate discreetly with each client. Users who receive information that they are unable to decrypt will discard the information.



How it Works

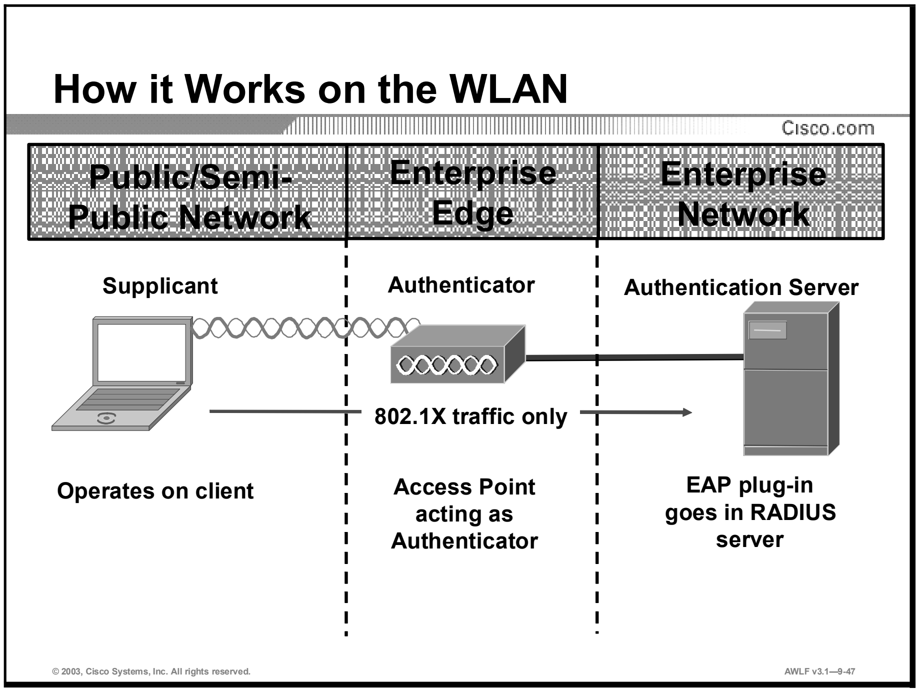
Cisco.com

Public/Semi-Public Network	Enterprise Edge	Enterprise Network
Supplicant	Authenticator	Authentication Server
	Or	
Operates on client	Operates on devices at network edge, like APs and switches	EAP plug-in goes in RADIUS server

AWLF v3.1—9-46

802.1X uses a RADIUS proxy to authenticate clients on the network. This proxy device could be a device like a switch or an access point. This device operates on the “enterprise edge”, meaning that it is the interface between the Enterprise network and the Public or Semi-public network, where security is most needed.

The supplicant sends authentication credentials to the authenticator which in turn sends the information to the authentication server, where the logon request is compared against a user database to determine if, and at what level, the user may be granted access to the network resources.



How it Works on the WLAN

Cisco.com

Public/Semi-Public Network

Enterprise Edge

Enterprise Network

Supplicant

Authenticator

Authentication Server

802.1X traffic only

Operates on client

Access Point acting as Authenticator

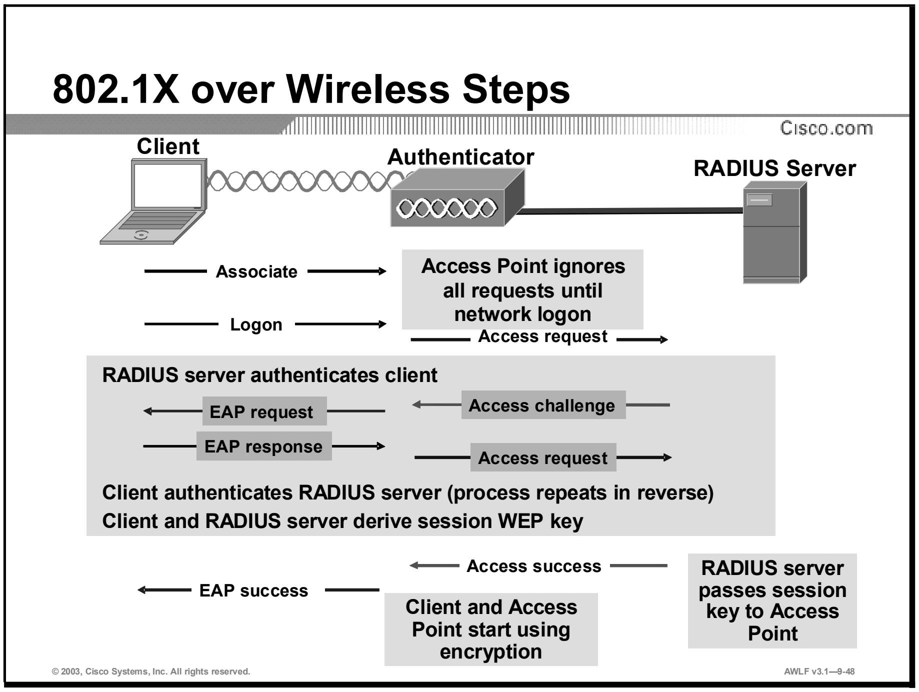
EAP plug-in goes in RADIUS server

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—9-47

The access point, acting as the authenticator at the enterprise edge, will allow the client to associate using Open authentication. The access point will then encapsulate any 802.1X traffic bound for the authentication server, and send it to the server. All other network traffic will be blocked, meaning that all other attempts to access network resources will be blocked.

Upon receiving RADIUS traffic bound for the client, the access point will encapsulate it and send the information to the client. Beyond the server authenticating the client as a valid network user, this allows the client to validate the server as well, insuring that the client is not logging into a “phony” server.



802.1X over Wireless Steps

Client

Authenticator

RADIUS Server

Associate →

Logon →

Access Point ignores all requests until network logon

Access request →

RADIUS server authenticates client

← EAP request

← Access challenge

EAP response →

Access request →

Client authenticates RADIUS server (process repeats in reverse)

Client and RADIUS server derive session WEP key

← Access success

← EAP success

Client and Access Point start using encryption

RADIUS server passes session key to Access Point

AWLF v3.1—9-48

After the client has associated to the access point, the supplicant starts the process for using EAPOL (EAP over LAN) by asking the user for their logon and password.

The client responds with their username and password. Using 802.1X and EAP the supplicant then send the username and a one-way encryption of the password to the access point. The access point then encapsulates the request and sends the request to the RADIUS server.

The RADIUS server then checks the username and password against the database to determine if the client should be authenticated on the network. If the client is to be authenticated, the RADIUS server then issues an access challenge, which is passed to the access point and then sent to the client.

The client sends the EAP response to the access challenge to the RADIUS server via the access point.

If the client sends the proper response then the RADIUS server sends an access success message and session WEP key (EAP over Wireless) to the client via the access point. The same session WEP key is also sent to the access point in success packet.

The client and the access point then begin using session WEP keys. The WEP key used for multicasts is then sent from the access point to the client. It is encrypted using the session WEP key.

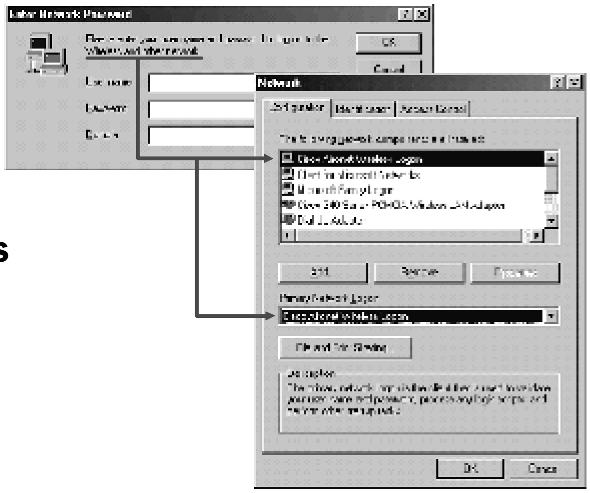
Upon client log off, the access point returns to the initial state, allowing only 802.1X traffic to pass.

Supplicant

Cisco.com

Use with EAP requires a Client

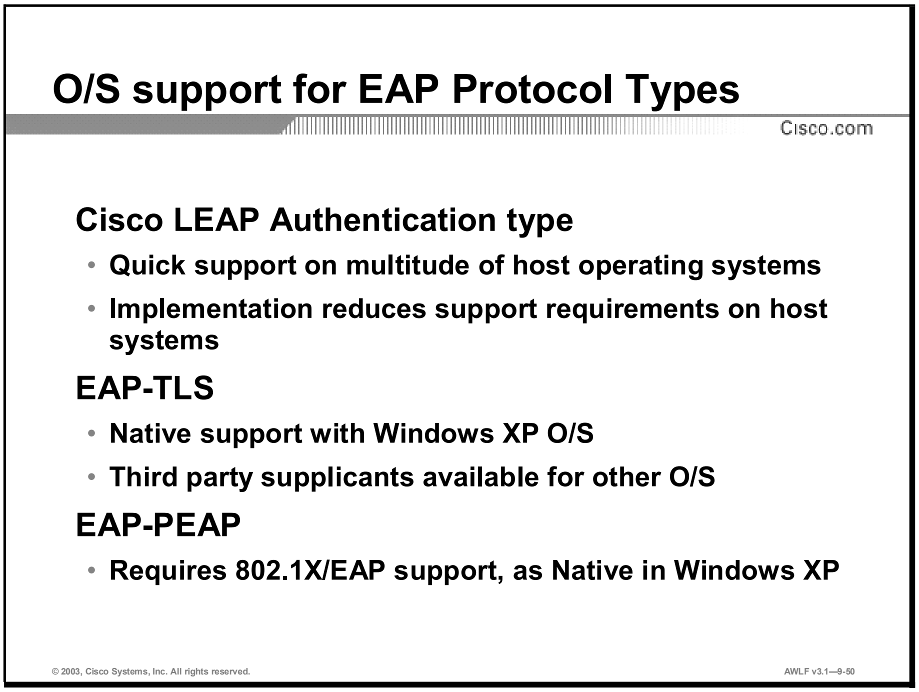
Referred to as a Supplicant



AWLF v3.1—9-49

The client will require a network logon application that will front-end the user's network logon, capturing the username/password. This is done so that the username and password may be encrypted, keeping unwanted users from obtaining usernames and passwords. Cisco provides a logon application just for LEAP, not for other 802.1X types.

The client will also require firmware that will support the LEAP supplicant for authentication with a RADIUS server. This supplicant will pass the username and password to the RADIUS server, and receive the dynamic WEP keys from the RADIUS server and the access point. The supplicant sets and removes the dynamic WEP keys.



O/S support for EAP Protocol Types

Cisco LEAP Authentication type

- Quick support on multitude of host operating systems
- Implementation reduces support requirements on host systems

EAP-TLS

- Native support with Windows XP O/S
- Third party supplicants available for other O/S

EAP-PEAP

- Requires 802.1X/EAP support, as Native in Windows XP

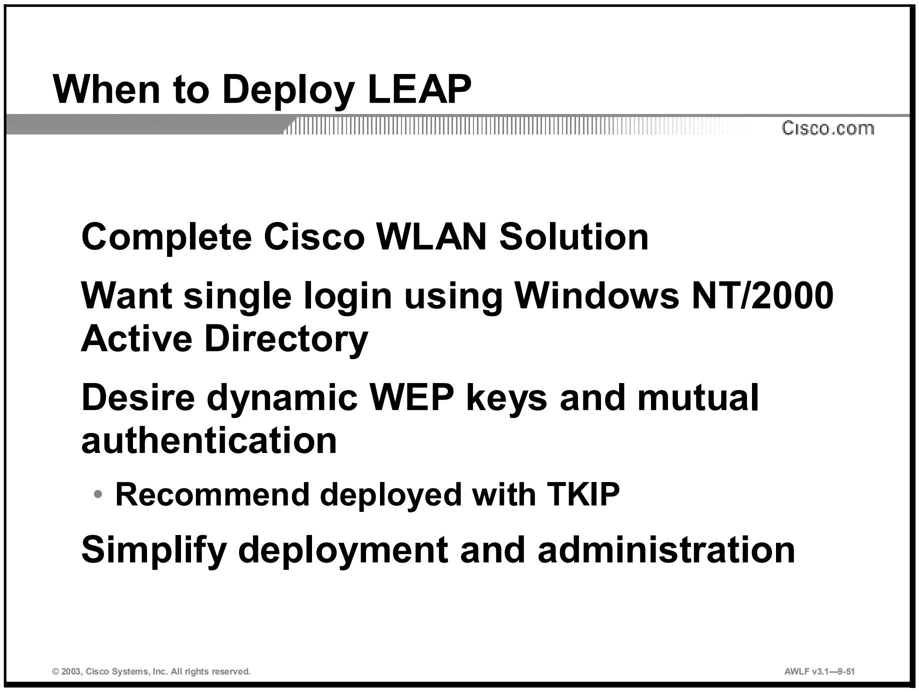
AWLF v3.1—9-50

Currently, Windows XP is the only operating system with native support for EAP. Third party software vendors are writing EAP supplicants for many of the popular operating systems.

LEAP is a password–based 802.1X authentication type that is supported on all client operating systems. The current versions of EAP may not provide the functionality that is needed or may be too demanding and could compromise the performance of the WLAN equipment.

Also, no native EAP support is currently available on legacy operating systems such as Windows 95, 98, Me, CE, Windows NT/2000, and Linux operating systems. All of these systems require LEAP.

The network will also need support in backend for delivery of session key to access points to speak WEP with client. This might be the Windows 2000 RADIUS server or Cisco's ACS.



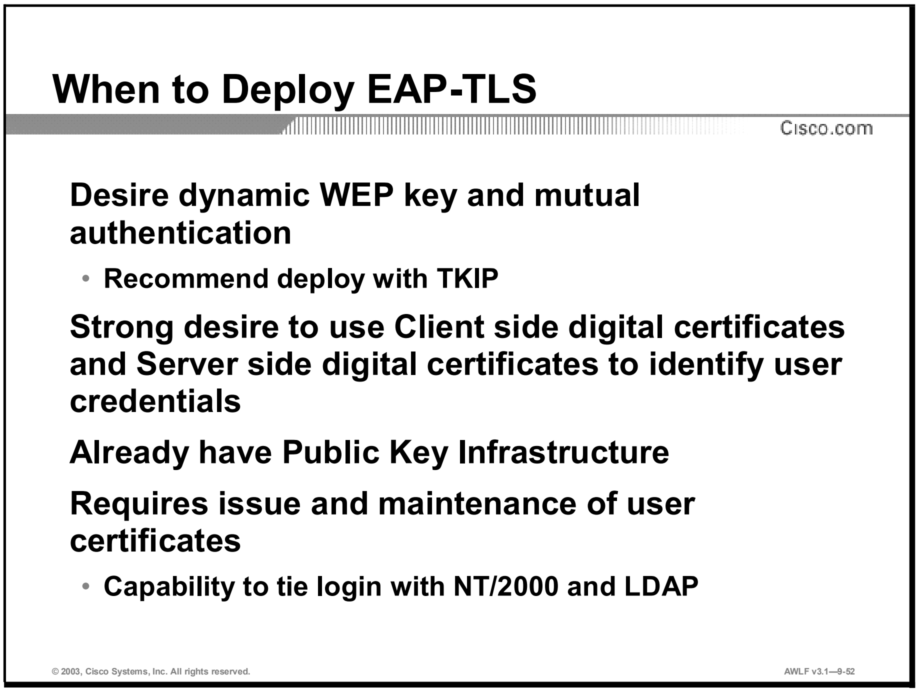
When to Deploy LEAP

Cisco.com

- Complete Cisco WLAN Solution
- Want single login using Windows NT/2000 Active Directory
- Desire dynamic WEP keys and mutual authentication
  - Recommend deployed with TKIP
- Simplify deployment and administration

AWLF v3.1—9-51

Active Directory is an essential component of the Windows 2000 architecture, presents organizations with a directory service designed for distributed computing environments. Active Directory allows organizations to centrally manage and share information on network resources and users while acting as the central authority for network security. In addition to providing comprehensive directory services to a Windows environment, Active Directory is designed to be a consolidation point for isolating, migrating, centrally managing, and reducing the number of directories that companies require.



When to Deploy EAP-TLS

Desire dynamic WEP key and mutual authentication

- Recommend deploy with TKIP

Strong desire to use Client side digital certificates and Server side digital certificates to identify user credentials

Already have Public Key Infrastructure

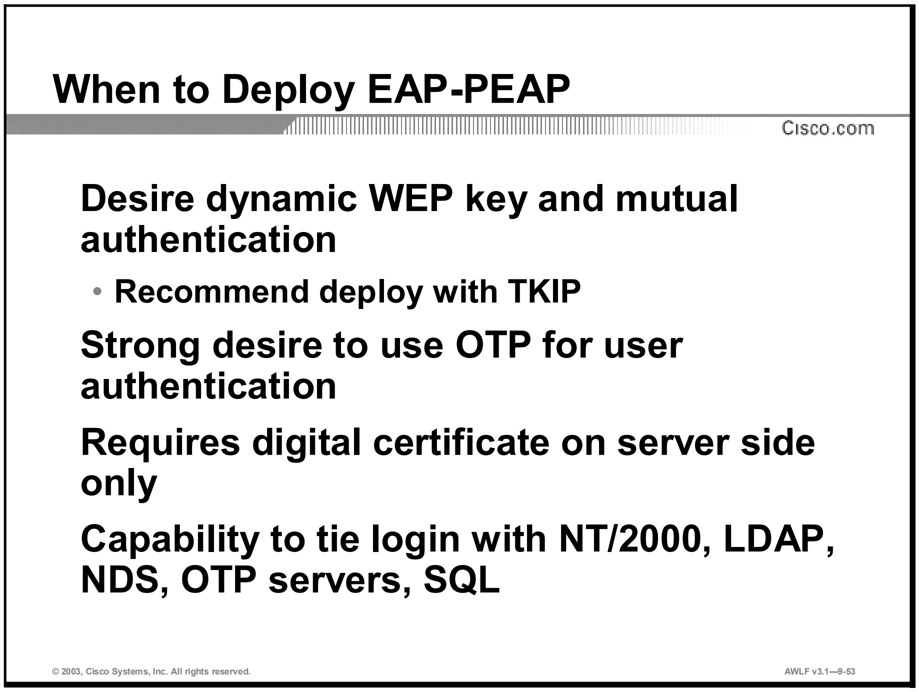
Requires issue and maintenance of user certificates

- Capability to tie login with NT/2000 and LDAP

AWLF v3.1—9-52

- **Public Key Infrastructure** ensures that sensitive electronic communications are private and protected from tampering. It provides assurances in the identities of the participants in those transactions, and prevents their later denying participating in the transaction.
- **Lightweight Directory Access Protocol** (LDAP) lets you use directory services to integrate Network Registrar client and lease information. By building on your existing standard schema for objects stored in LDAP directories, you can handle information about DHCP client entries. Thus, instead of maintaining client information in the DHCP server's database, you can ask the Network Registrar DHCP server to issue queries to one or more LDAP servers for information in response to DHCP client requests.

Note EAP-TLS is a very labor-intensive security option. EAP-TLS requires a digital certificate to configure on all WLAN Clients and on the Server.



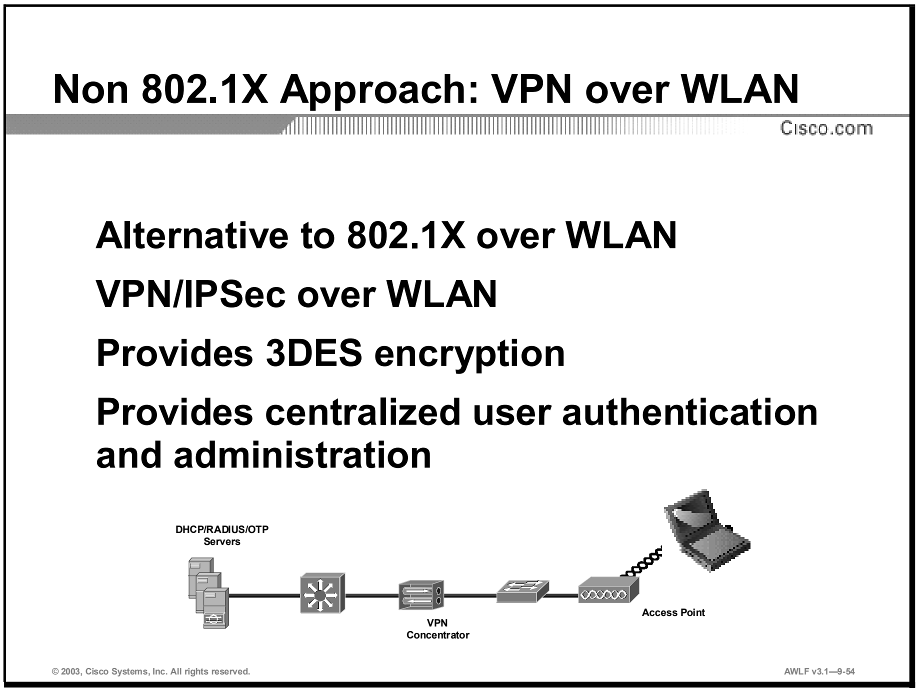
When to Deploy EAP-PEAP

- Desire dynamic WEP key and mutual authentication
  - Recommend deploy with TKIP
- Strong desire to use OTP for user authentication
- Requires digital certificate on server side only
- Capability to tie login with NT/2000, LDAP, NDS, OTP servers, SQL

AWLF v3.1—9-53

Protected EAP is a draft RFC authentication type that is designed to allow hybrid authentication. PEAP employs server-side PKI authentication. For client-side authentication, PEAP can use any other EAP authentication type. Because PEAP establishes a secure tunnel via server-side authentication, non-mutually authenticating EAP types can be used for client-side authentication, such as EAP generic token card (GTC) for one-time passwords (OTP), and EAP-MSCHAPV2 for password based authentication.

PEAP is based on server-side EAP-TLS, and it addresses the manageability and scalability shortcomings of EAP-TLS. Organizations can avoid the issues associated with installing digital certificates on every client machine as required by EAP-TLS and select the method of client authentication that best suits them.



Non 802.1X Approach: VPN over WLAN

Cisco.com

- Alternative to 802.1X over WLAN
- VPN/IPSec over WLAN
- Provides 3DES encryption
- Provides centralized user authentication and administration

DHCP/RADIUS/OTP Servers
VPN Concentrator
Access Point

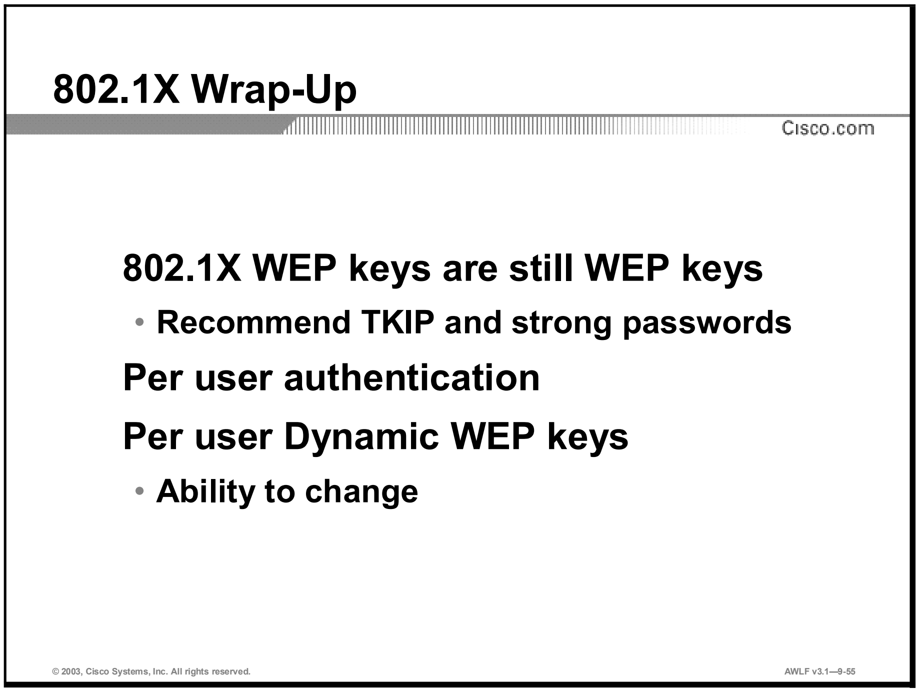
© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—9-54

IPSec is a framework of open standards for ensuring secure private communications over IP networks. IPSec VPNs use the services defined within IPSec to ensure confidentiality, integrity, and authenticity of data communications across public networks, such as the Internet. IPSec also has a practical application to secure WLANs by overlaying IPSec on top of cleartext 802.11 wireless traffic.

When deploying IPSec in a WLAN environment, an IPSec client is placed on every PC connected to the wireless network and the user is required to establish an IPSec tunnel to route any traffic to the wired network. Filters are put in place to prevent any wireless traffic from reaching any destination other than the VPN gateway and DHCP/DNS server. IPSec provides for confidentiality of IP traffic, as well as authentication and anti-replay capabilities. Confidentiality is achieved through encryption using a variant of the Data Encryption Standard (DES), called Triple DES (3DES), which encrypts the data three times with up to three different keys.

The IPSec VPN option in the remote network is recommended when the wireless user requires security from the wireless device to the corporate network. This is the most common configuration for remote workers who may not have IT-managed hardware resources at their remote location. Part-time teleworkers fall into this category. The access point can be set up with almost any configuration that allows connectivity to the broadband device because the security is handled via the VPN client with personal firewall software.



802.1X Wrap-Up

802.1X WEP keys are still WEP keys

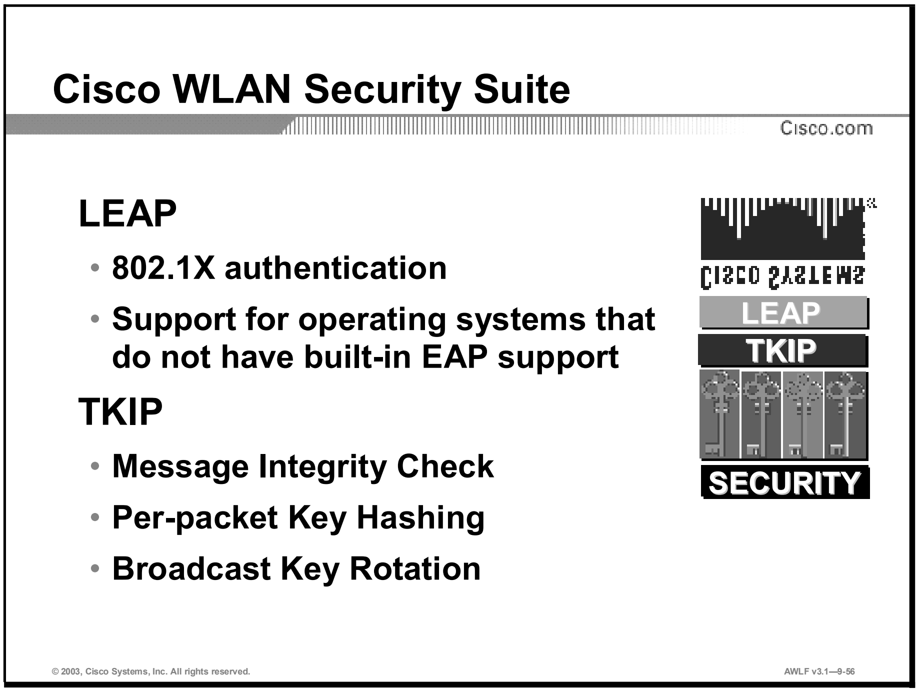
- Recommend TKIP and strong passwords

Per user authentication

Per user Dynamic WEP keys

- Ability to change

AWLF v3.1—9-55



Cisco WLAN Security Suite

Cisco.com

LEAP

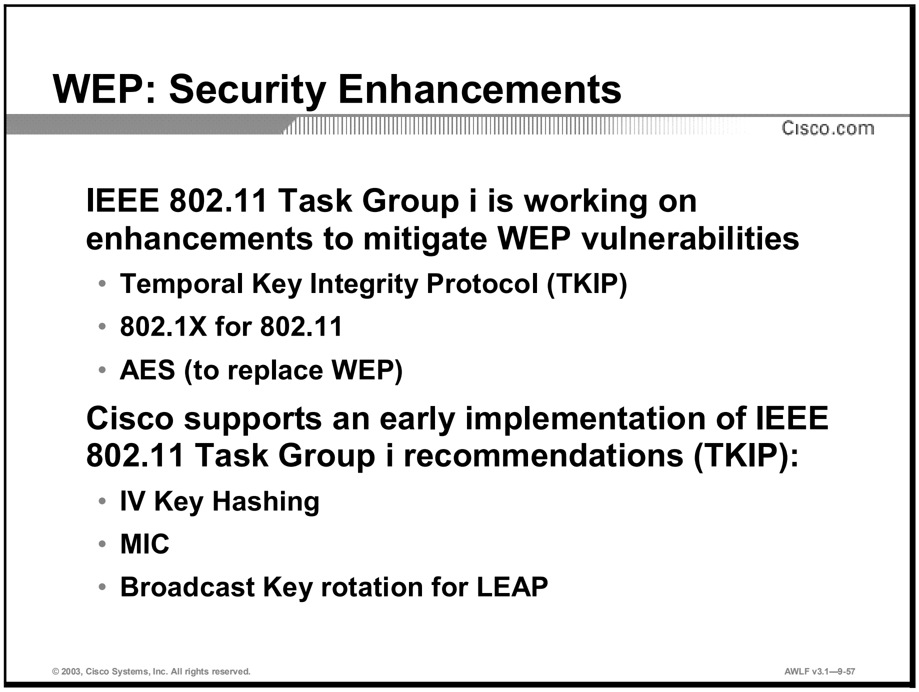
- 802.1X authentication
- Support for operating systems that do not have built-in EAP support

TKIP

- Message Integrity Check
- Per-packet Key Hashing
- Broadcast Key Rotation

AWLF v3.1—9-56

Stronger WEP keys are provided by Temporal Key Integrity Protocol (TKIP) enhancements such as Message Integrity Check (MIC), which prevents bit-flip attacks on encrypted packets. WEP Key hashing protects weak Initialization Vectors (IV) from being exposed by hashing the IV on a per-packet basis. MIC and WEP Key hashing can be enabled using static WEP keys and do not need a Remote Access Dial In User Service (RADIUS) server to function. The Broadcast Key Rotation (BKR) feature is also a TKIP enhancement. BKR protects the multicast traffic of the Access Point from being exploited by dynamically changing the multicast encryption key. The access point generates broadcast WEP keys using a seeded pseudorandom number generator (PRNG). The access point rotates the broadcast key after a configured broadcast WEP key timer expires. This process should generally be in sync with the timeouts configured on the RADIUS servers for user reauthentication. Cisco recommends that broadcast key rotation be enabled when the access point services an 802.1X *exclusive* wireless LAN.



WEP: Security Enhancements

Cisco.com

IEEE 802.11 Task Group i is working on enhancements to mitigate WEP vulnerabilities

- **Temporal Key Integrity Protocol (TKIP)**
- **802.1X for 802.11**
- **AES (to replace WEP)**

Cisco supports an early implementation of IEEE 802.11 Task Group i recommendations (TKIP):

- **IV Key Hashing**
- **MIC**
- **Broadcast Key rotation for LEAP**

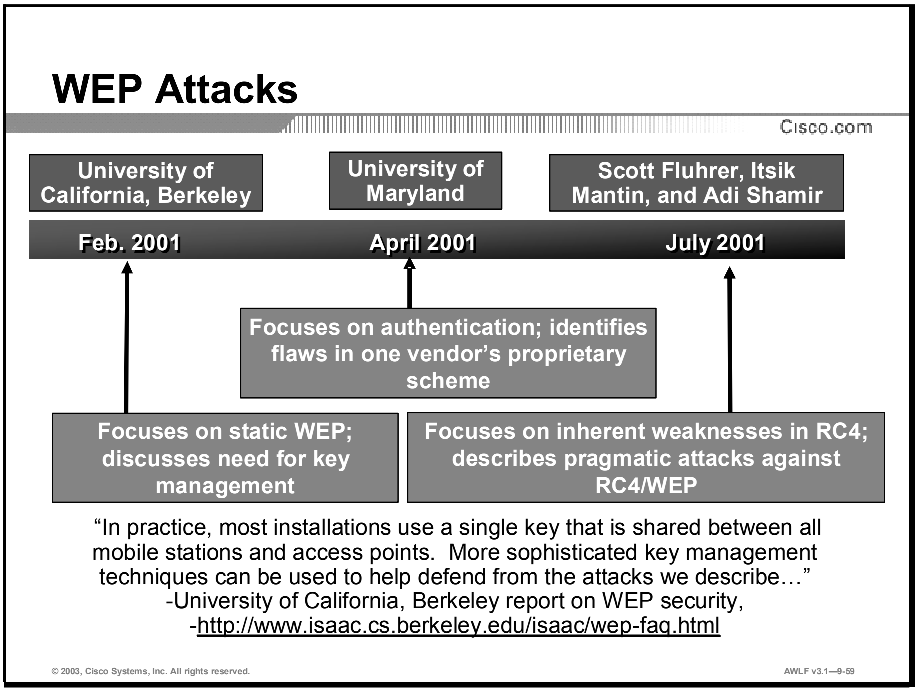
© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—9-57

The next generation of WLAN security is the responsibility of IEEE’s 802.11 Task Group I. These enhancements are being added to mitigate WEP vulnerabilities. Once these enhancements are ratified by IEEE 802.11 Task Group I, the new standard will be called IEEE 802.11I. The enhancements that IEEE 802.11 Task Group I are working on are:

- Temporal Key Integrity Protocol also referred to as WEP key hashing. A security feature that defends against an attack on WEP in which the intruder uses the initialization vector (IV) in encrypted packets to calculate the WEP key. TKIP removes the predictability that an intruder relies on to determine the WEP key by exploiting IVs.
- 802.1X for 802.11 is the new standard for wireless LAN security, as defined by the Institute of Electrical and Electronics Engineers (IEEE). An access point that supports 802.1X and its protocol, Extensible Authentication Protocol (EAP), acts as the interface between a wireless client and an authentication server, such as a Remote Authentication Dial-In User Service (RADIUS) server, to which the access point communicates over the wired network.
- Advanced Encryption Standard (AES) is a FIPS (US Federal Information Processing Standard) encryption standard approved by NIST, the US National Institute of Standards and Technology. AES is a block cipher and will replace DES encryption standard. This next-generation encryption function was approved by the National Institute of Standards and Technology (NIST). AES specifies three key sizes: 128, 192 and 256 bits and uses the Rijndael Algorithm. Assuming that one could build a machine that could recover a DES key in a second (i.e., try 255 keys per second), then it would take that machine approximately 149 thousand-billion (149 trillion) years to crack a 128-bit AES key. To put that into perspective, the universe is believed to be less than 20 billion years old.

WLAN Attacks



WEP Attacks

University of California, Berkeley

University of Maryland

Scott Fluhrer, Itsik Mantin, and Adi Shamir

Feb. 2001

April 2001

July 2001

Focuses on authentication; identifies flaws in one vendor's proprietary scheme

Focuses on static WEP; discusses need for key management

Focuses on inherent weaknesses in RC4; describes pragmatic attacks against RC4/WEP

"In practice, most installations use a single key that is shared between all mobile stations and access points. More sophisticated key management techniques can be used to help defend from the attacks we describe…"
-University of California, Berkeley report on WEP security,
-http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

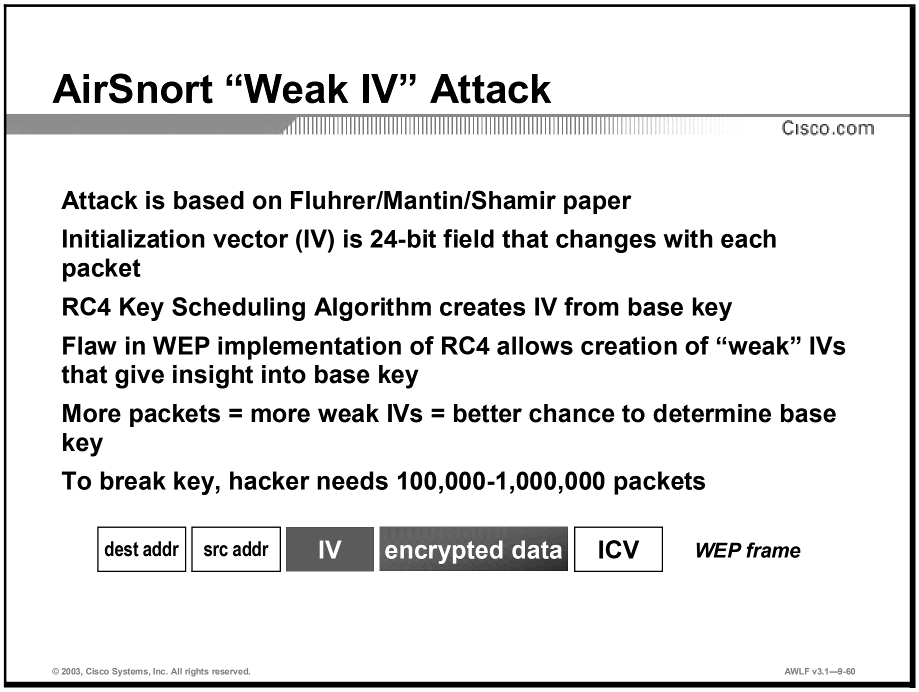
AWLF v3.1—9-59

In 2000-2001, several papers were written that documented a number of weaknesses with the 802.11 authentication method, as well as weaknesses in the data frame encryption (WEP). The main problem identified with WLAN security was that very few WLANs were implementing any form of security at all. Any user with an 802.11 client card could potentially attach to these WLAN, and, as a result, attach to the LAN.

These papers then went on to point out that using Shared Key Authentication, it was possible to capture the challenge text packet that was sent to the client, and then capture the encrypted response, thus allowing someone to derive the WEP key being used.

And finally, it was shown that using a WLAN "sniffer" (a device that can capture WLAN packets), someone could capture enough packets to crack the security and derive the WEP key(s) being used, no matter which method of authentication was being used.

Scott Fluhrer, Itsik Mantin, and Adi Shamir, who are experts on cryptology, authored one of the most recent papers. This paper discusses weaknesses in the Key Scheduling Algorithm of the RC4 stream cipher and describes how to mount attacks on RC4-based WEP keys. This type of attack is implemented using the "AirSnort" tool (a Linux based wireless sniffer).



AirSnort "Weak IV" Attack

Cisco.com

- Attack is based on Fluhrer/Mantin/Shamir paper
- Initialization vector (IV) is 24-bit field that changes with each packet
- RC4 Key Scheduling Algorithm creates IV from base key
- Flaw in WEP implementation of RC4 allows creation of "weak" IVs that give insight into base key
- More packets = more weak IVs = better chance to determine base key
- To break key, hacker needs 100,000-1,000,000 packets

dest addr	src addr	IV	encrypted data	ICV

WEP frame

AWLF v3.1—9-60

The figure shown depicts a WEP encrypted frame. The first 24 bits of the frame are the Initialization Vector (IV). The purpose of the IV is to insure that the same plaintext data frame will never generate the same WEP encrypted data frame. The method of changing the IV is dependent upon vendor implementation (Cisco Aironet changes the IV on a per packet basis).

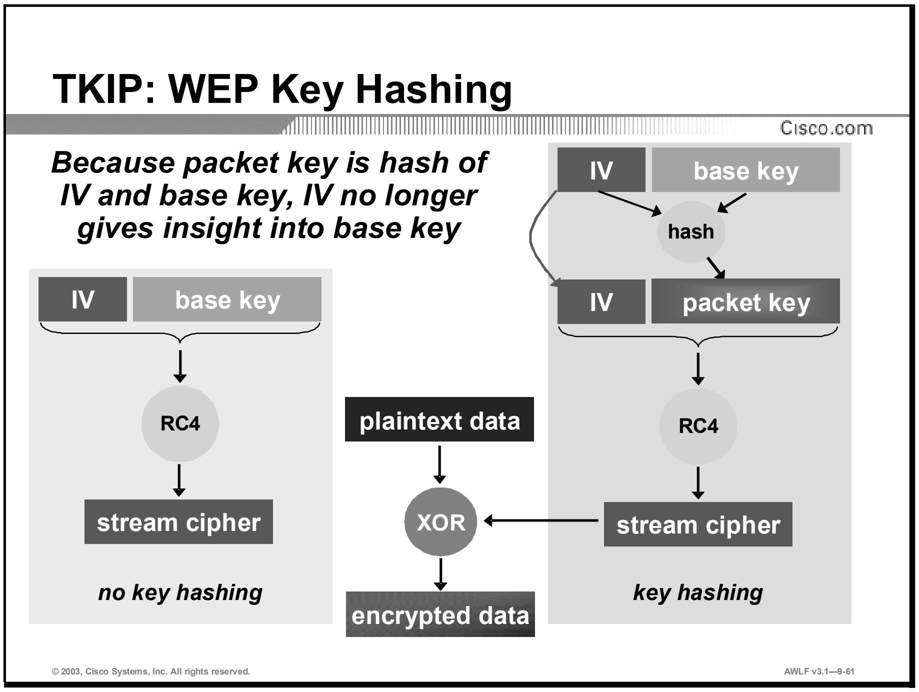
The IV is transmitted as plaintext and a user "sniffing" the WLAN could see the IV. When the same IV is used over and over with the same WEP key, a hacker could capture the frames and derive information about the data in the frame, as well as data about the network.

Using static WEP keys has proven to be highly vulnerable to this type of attack. This is why Cisco recommends that WLANs not use static WEP, and instead use the more advanced security features implementing 802.1X.

Cisco Aironet Access Point firmware includes features to improve RC4/WEP security by hashing WEP keys, thus protecting against weak initialization vectors.

Care must be taken when configuring the WLAN security to protect against this type of attack. Configuring the WEP key timeout on the authentication server does this. This will force wireless clients to re-authenticate, resulting in the generation of a new WEP key. The result of the shorter timeout period is that wireless clients do not use the same WEP key long enough for a hacker to capture the number of frames to hack the WEP key.

For more information on Cisco's response in the Berkeley paper go to: http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1281_pp.htm



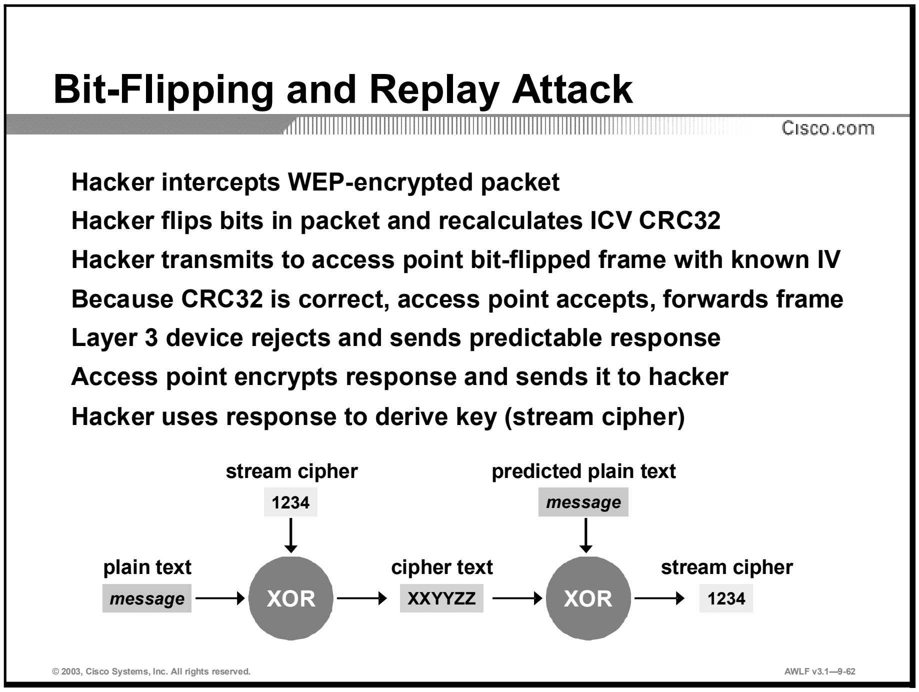
TKIP: WEP Key Hashing

Cisco.com

Because packet key is hash of IV and base key, IV no longer gives insight into base key

AWLF v3.1—9-61

Another advanced security feature on the Cisco Aironet devices is WEP Key hashing. When configured, a Cisco Aironet Access Point or Bridge protects against attack that focus on weak (or predictable) initialization vectors. Because the packet key is hash of the initialization vector and the base key, the initialization vector no longer gives insight into base key.



Bit-Flipping and Replay Attack

Cisco.com

Hacker intercepts WEP-encrypted packet

Hacker flips bits in packet and recalculates ICV CRC32

Hacker transmits to access point bit-flipped frame with known IV

Because CRC32 is correct, access point accepts, forwards frame

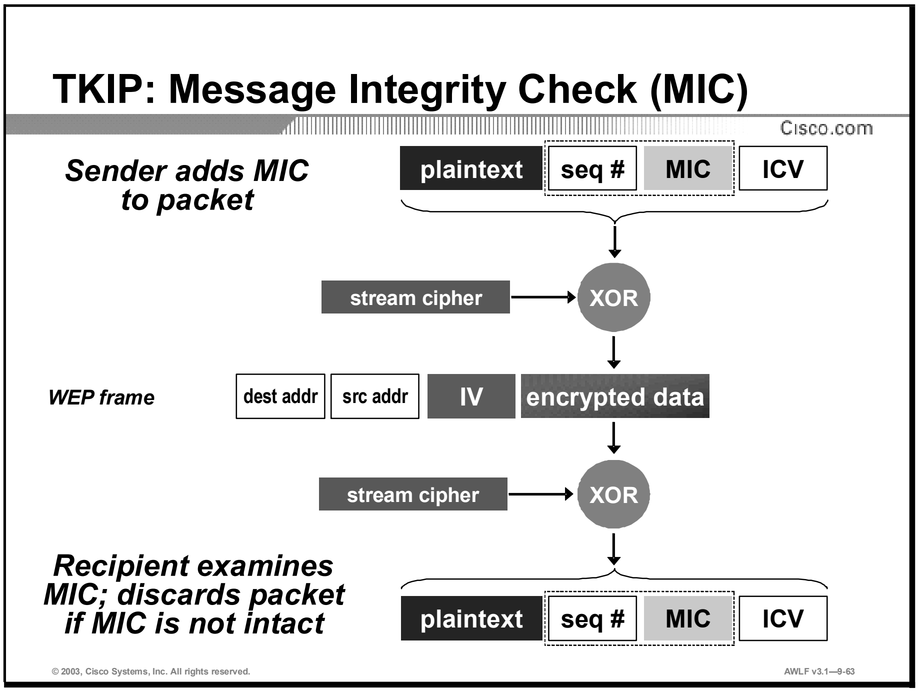
Layer 3 device rejects and sends predictable response

Access point encrypts response and sends it to hacker

Hacker uses response to derive key (stream cipher)

AWLF v3.1—9-62

Another WEP attack is the “bit flip” attack. In this type of attack, a hacker attempts to capture an encrypted message, flips (or tampers) the bits in the message, and then retransmits the message in the hope that the message is accepted as a valid message. If it is, then the access point is communicating with the hacker (instead of the legitimate user) and WLAN security has been compromised.



TKIP: Message Integrity Check (MIC)

Cisco.com

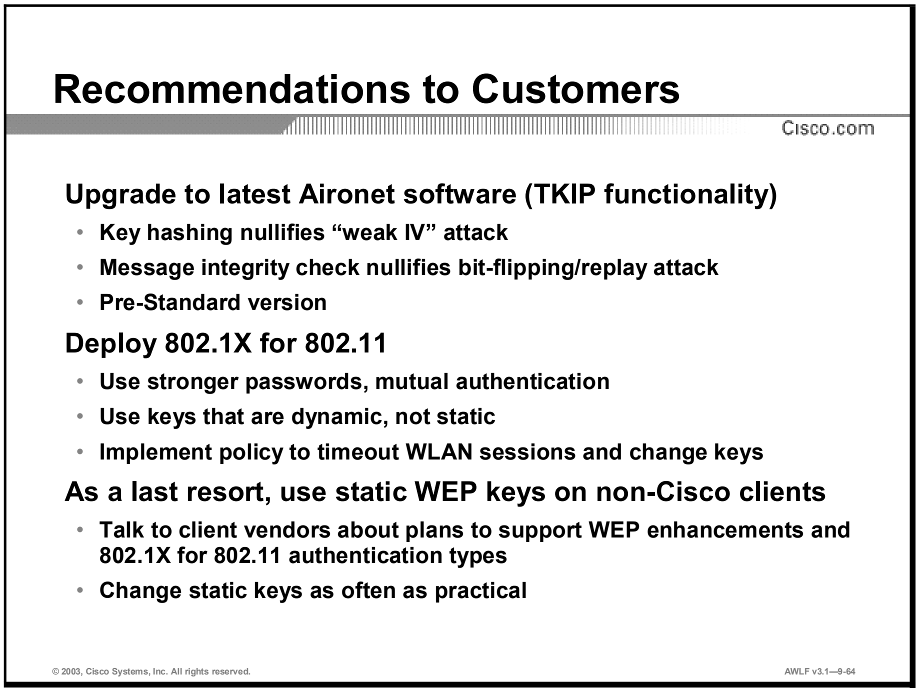
Sender adds MIC to packet

Recipient examines MIC; discards packet if MIC is not intact

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—9-63

The Cisco Aironet Access Point includes a feature called Message Integrity Check (MIC). When configured it adds a few extra bytes to every packet before the packet is encrypted. The recipient of the packet will then decrypt the packet and examine the MIC. If the extra bytes are not intact, then the message has been tampered with and the recipient will then discard the message.



Recommendations to Customers

Upgrade to latest Aironet software (TKIP functionality)

- Key hashing nullifies “weak IV” attack
- Message integrity check nullifies bit-flipping/replay attack
- Pre-Standard version

Deploy 802.1X for 802.11

- Use stronger passwords, mutual authentication
- Use keys that are dynamic, not static
- Implement policy to timeout WLAN sessions and change keys

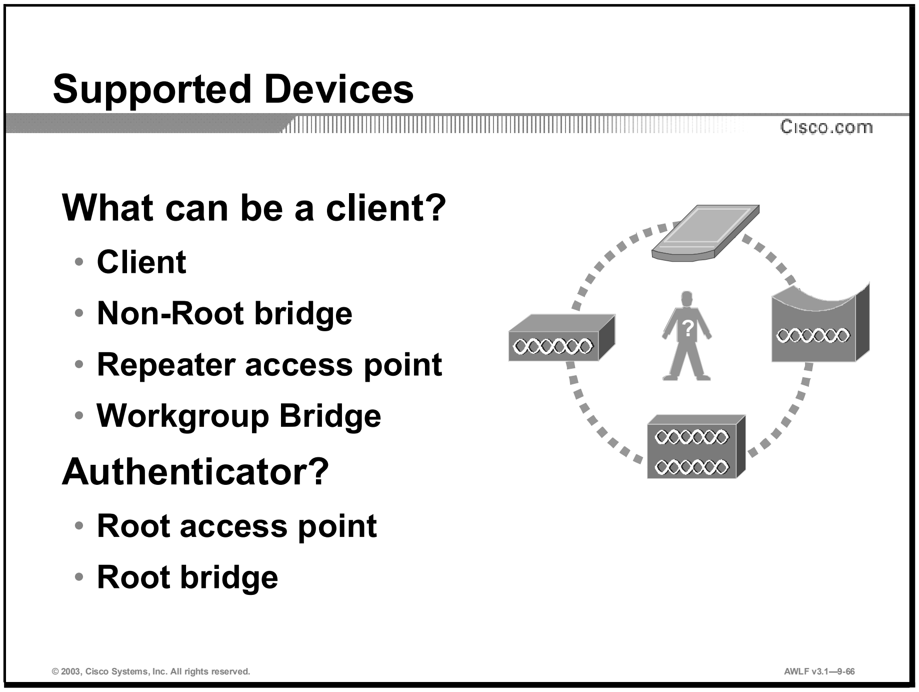
As a last resort, use static WEP keys on non-Cisco clients

- Talk to client vendors about plans to support WEP enhancements and 802.1X for 802.11 authentication types
- Change static keys as often as practical

AWLF v3.1—9-64

Cisco offers a variety of options for installing or improving network security on the WLAN. Not all customers may feel they need to use the more advanced security options. Some customers may feel that the information they send across the WLAN does not need the level of protection that an authentication server and 802.1X (LEAP) can provide. Other customers may want to use all security features available to them. In any case, Cisco Aironet offers a security solution that will meet the customer’s needs.

Configuring the Access Point for Authentication



Supported Devices

What can be a client?

- Client
- Non-Root bridge
- Repeater access point
- Workgroup Bridge

Authenticator?

- Root access point
- Root bridge

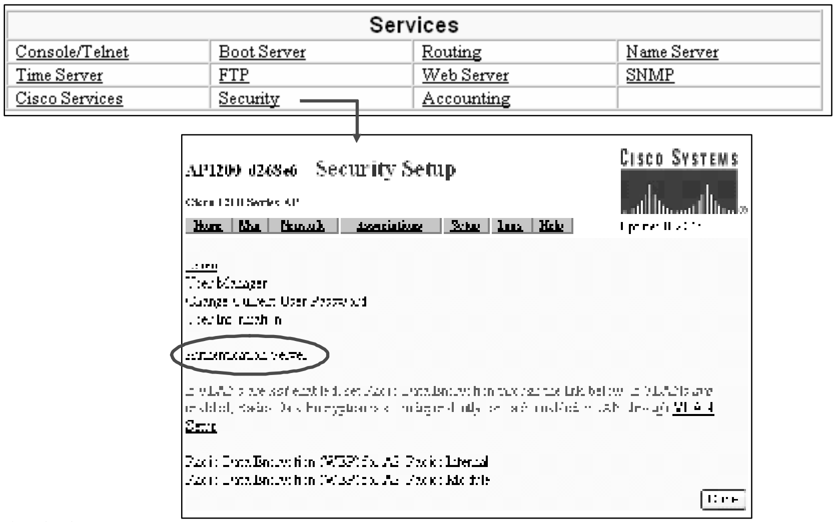
AWLF v3.1—9-66

All of Cisco's WLAN products can be configured to take advantage of LEAP. The WLAN products are classified into two categories, Client and Authenticator.

- **Clients:** A Client card uses the Aironet Client Unity (ACU) to setup and enable security. A **Non-Root Bridge**, **Repeater Access Point** and **Workgroup Bridge** can be configured with a LEAP user name and password. The preset user name and password will respond automatically when they are challenged for LEAP credentials.
- Authenticators: A Root Access Point and Root Bridge can be configured to pass Client and Authentication Server credentials. Until the Client's credentials are confirmed the Client is denied access to the LAN.

Enabling Authentication on Access Point

Cisco.com



Services			
Console/Telnet	Boot Server	Routing	Name Server
Time Server	FTP	Web Server	SNMP
Cisco Services	Security	Accounting	

AP1200 d268e6 Security Setup

Cisco 1200 Series AP

Login
User Manager
Change Current User Password
User Information

Authentication Server

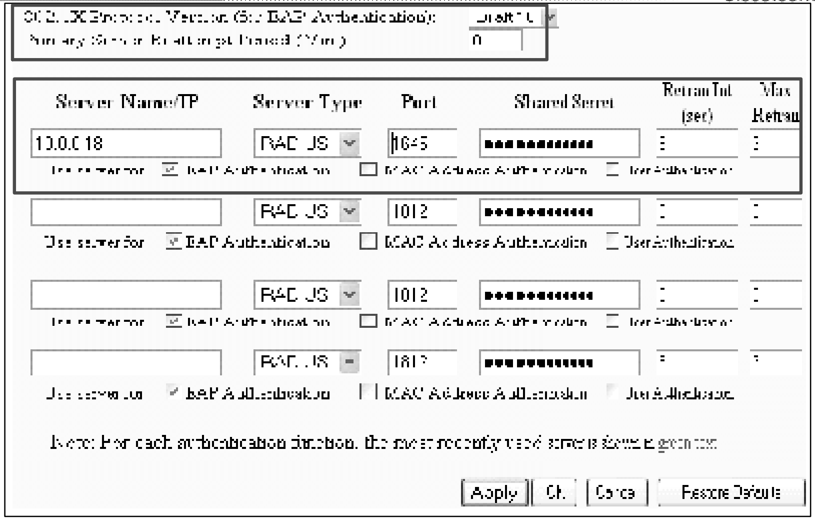
If VLANs are not enabled, set Radio Data Encryption through the links below. If VLANs are enabled, Radio Data Encryption is configured independently for each enabled VLAN through VLAN Setup.

Radio Data Encryption (WEP) for AP Radio Internal
Radio Data Encryption (WEP) for AP Radio Module

AWLF v3.1—9-67

In order to configure the access point for authentication using a radius server, start at the **Security Setup** screen again. Click on the **Authentication Server** link to set the parameters for the server.

Defining an Authenticator



802.1X Protocol Version (for EAP Authentication): Draft 10

Primary Server Reattempt Period (Min.): 0

Server Name/IP	Server Type	Port	Shared Secret	Retran Int (sec)	Max Retran
10.0.0.18	RADIUS	1645	••••••••••••	[illegible]	[illegible]
Use server for: ☑ EAP Authentication	☐ MAC Address Authentication	☐ User Authentication			
	RADIUS	1812	••••••••••••	[illegible]	[illegible]
Use server for: ☑ EAP Authentication	☐ MAC Address Authentication	☐ User Authentication			
	RADIUS	1812	••••••••••••	[illegible]	[illegible]
Use server for: ☑ EAP Authentication	☐ MAC Address Authentication	☐ User Authentication			
	RADIUS	1812	••••••••••••	[illegible]	[illegible]
Use server for: ☑ EAP Authentication	☐ MAC Address Authentication	☐ User Authentication			

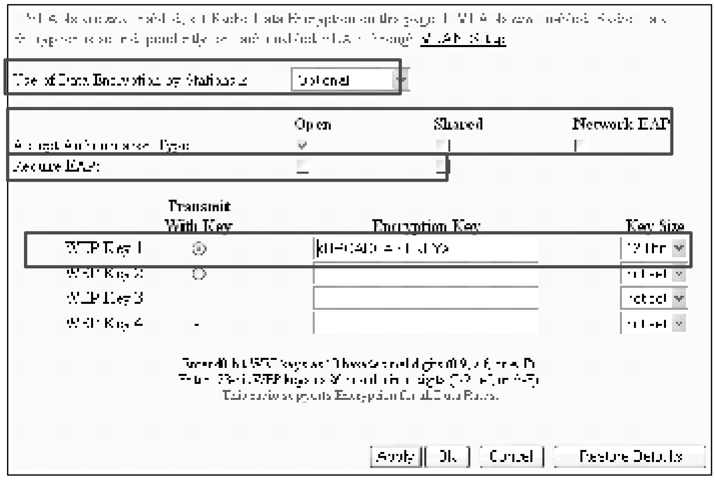
Note: For each authentication function, the most recently used server is shown in green text.

AWLF v3.1—9-68

In order to use an authentication server, the access point must be configured to communicate with the server. From the Authentication Server screen, configure the following:

- **802.1X Protocol Version for EAP Authentication:** This must match on both the APs and the clients.
- **EAP Authentication:** Check here if the access point will be supporting clients that must authenticate using EAP.
- **MAC Address Authentication:** Check here if the access point will be supporting clients that must authenticate by MAC Address.
- **Server Name/IP:** Enter the name or IP address of the Radius server in the Server Name/IP entry field.
- **Port:** Enter the port number your RADIUS server uses for authentication. The default
  - 1812 is the port setting for many RADIUS servers.
  - 1645 is the port setting for Cisco's RADIUS server, the Access Control Server (ACS). Check your server's product documentation to find the correct port setting.
- **Shared Secret:** Enter the shared secret used by your RADIUS server in the Shared Secret entry field. The shared secret on the access point must match the shared secret on the RADIUS server.
- **Retran Int (sec):** Enter the number of seconds the access point should wait before retransmitting authentication challenges upon failure.
- **Max Retran:** Enter the maximum number of retransmits of authentication challenges upon failure.

WEP Configuration on the Access Point



[illegible] VLAN Setup

Use of Data Encryption by Stations is: Optional

	Open	Shared	Network EAP
Accept Authentication Type:	☑	□	□
Require EAP:	□	□	

	Transmit With Key	Encryption Key	Key Size
WEP Key 1	●	[illegible]	128 bit
WEP Key 2	○		not set
WEP Key 3			not set
WEP Key 4			not set

Enter 40-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F).
Enter 128-bit WEP keys as 26 hexadecimal digits (0-9, a-f, or A-F).
This radio supports Encryption for all Data Rates.

AWLF v3.1—9-69

At least one WEP key needs to be set on the access point. This key will be used for multicast packets. After the client has been authenticated with the RADIUS server, the WEP key used for multicasts will be passed to the client and will be encrypted using the session key.

Note It is possible to use EAP without using WEP, but all multicast packets sent by the access point will not be encrypted.

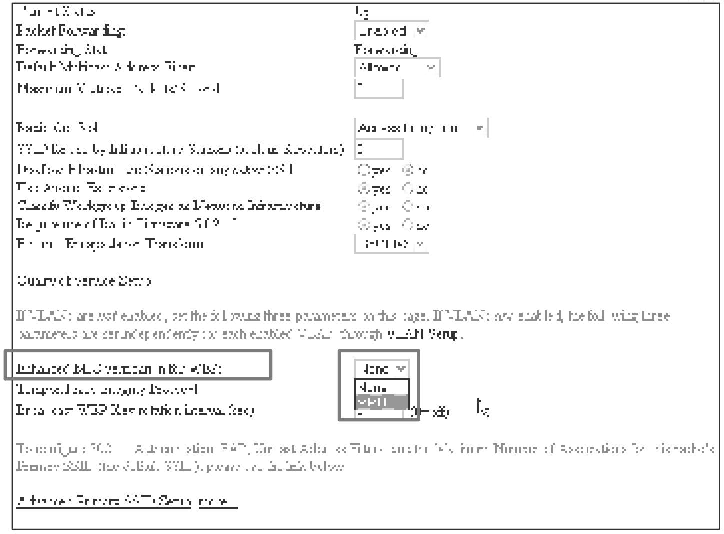
Accept Authentication Type- Check the Network-EAP box to allow clients to authenticate using LEAP (or Host Based EAP).

In order for the access point to require that other types of authentication (Open, Shared Key) use EAP (EAP-TLS, EAP-MD5), check the appropriate box (**Open**, **Shared Key**), and then check the **Require EAP** box below. This will force all clients using that authentication method to authenticate using EAP.

Note This feature is useful in insuring that non-Cisco Aironet devices with EAP enabled can authenticate through the access point.

Configuring the Access Point for MIC

Cisco.com



AWLF v3.1—9-70

Message Integrity Check (MIC)

MIC helps prevent *bit-flip* attacks.

Note MIC must be set up and WEP enabled with full encryption before MIC takes effect.

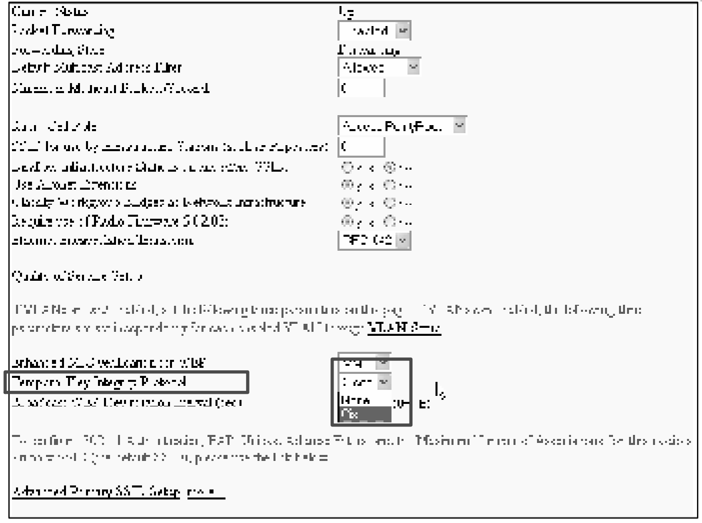
Note To use MIC, the Use Aironet Extensions setting on the access point Radio Advanced screen must be set to yes (the default setting).

Note The access point must be set up for WEP with full encryption before MIC becomes active. If WEP is off or set to optional, MIC is not enabled.

From the access point Radio Advanced screen, select MMH from the Enhanced MIC verification for WEP pull-down menu. Click OK.

MIC is enabled, and only client devices with MIC capability can communicate with the access point.

Configuring the Access Point for WEP Key Hashing



AWLF v3.1—9-71

Temporal Key Integrity Protocol (WEP Key Hashing)

WEP key hashing defends against an attack on WEP in which the intruder uses an unencrypted segment called the initialization vector (IV) in encrypted packets to calculate the WEP key. WEP key hashing removes the predictability that an intruder relies on to determine the WEP key by exploiting IVs. WEP key hashing protects both unicast and broadcast WEP keys.

Note When WEP key hashing is enabled, all WEP-enabled client devices associated to the access point must support WEP key hashing. WEP-enabled devices that do not support key hashing cannot communicate with the access point.

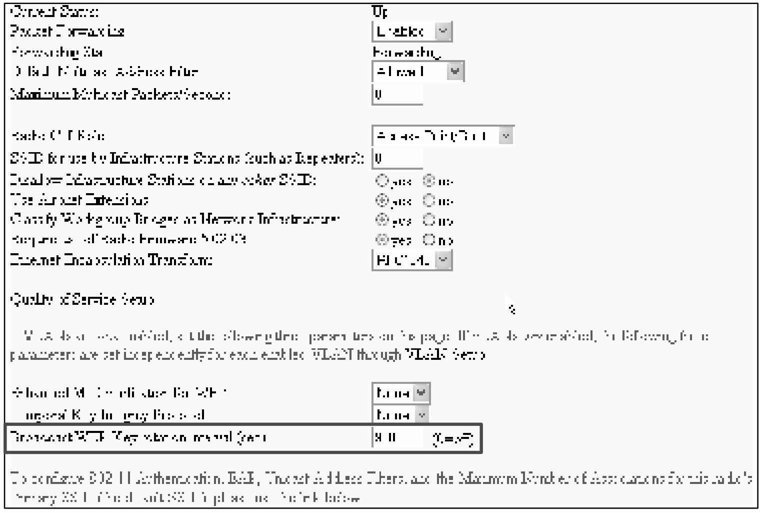
Note To use WEP key hashing, the Use Aironet Extensions setting on the access point Radio Advanced screen must be set to yes (the default setting).

Note When WEP key hashing is enabled, it is not necessary to enable broadcast key rotation. Key hashing prevents intruders from calculating the static broadcast key; therefore broadcast key rotation would only serve as a redundant security measure.

Insure that the access point is set up for WEP (either full or optional encryption). Select Cisco from the Temporal Key Integrity Protocol pull-down menu (this enables hashing of the initialization vector). Click OK. WEP key hashing is enabled.

Enabling Broadcast WEP Key Rotation

Cisco.com



Current State: Up

Packet Forwarding: Enabled

Forwarding State: Forwarding

Default Multicast Address Filter: Allowed

Maximum Multicast Packets/Second: 0

Radio Cell Role: Access Point/Root

SSID for use by Infrastructure Stations (such as Repeaters): 0

Disallow Infrastructure Stations on any other SSID: ○ yes ● no

Use Aironet Extensions: ● yes ○ no

Classify Workgroup Bridges as Network Infrastructure: ● yes ○ no

Require use of Radio Firmware 5.02.19: ● yes ○ no

Ethernet Encapsulation Transform: RFC1042

Quality of Service Setup

If VLANs are not enabled, set the following three parameters on this page. If VLANs are enabled, the following three parameters are set independently for each enabled VLAN through VLAN Setup.

Enhanced MIC verification for WEP: None

Temporal Key Integrity Protocol: None

Broadcast WEP Key rotation interval (sec): 900 (0=off)

To configure 802.11 Authentication, EAP, Unicast Address Filters, and the Maximum Number of Associations for this radio's Primary SSID, click on the SSID Setup link below.

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—9-72

Broadcast WEP Key rotation interval (sec)

Broadcast key rotation is an excellent alternative to WEP key hashing if the WLAN supports wireless client devices that are not Cisco devices or that cannot be upgraded to the latest firmware for Cisco client devices.

Note When broadcast key rotation is enabled, only wireless client devices using LEAP or EAP-TLS authentication can use the access point. Client devices using static WEP (with open, shared key, or EAP-MD5 authentication) cannot use the access point when you enable broadcast key rotation.

It is not necessary to enable broadcast key rotation if WEP key hashing is enabled. Use of both key rotation and key hashing provides redundant protection.

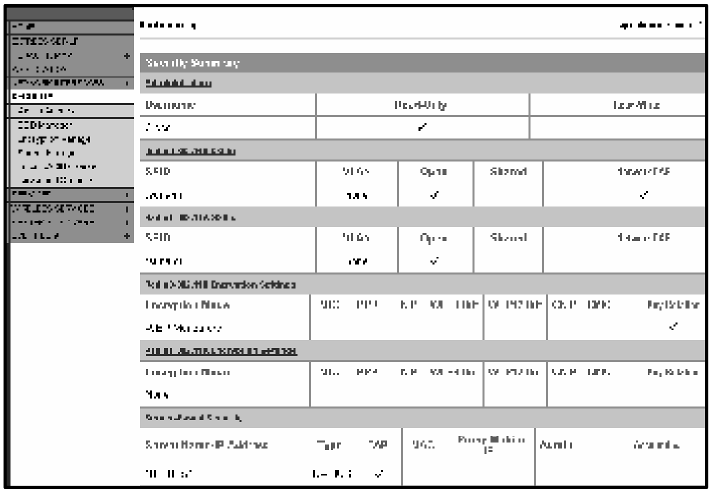
On the access point Radio Advanced screen, enter the rotation interval in seconds in the Broadcast WEP Key rotation interval entry field. If you enter 900, for example, the access point sends a new broadcast WEP key to all associated client devices every 15 minutes. To disable broadcast WEP key rotation, enter 0.

Note Set the rotation interval on every access point using broadcast key rotation. Key rotation interval is not configured on the RADIUS server.

Use a short rotation interval if the traffic on the wireless network contains numerous broadcast or multicast packets. Click OK. Broadcast key rotation is enabled.

Enable Authentication on IOS AP

Cisco.com



Security Summary

Username	Read-Only	Read-Write
[illegible]	✓	

SSID	VLAN	Open	Shared	Network EAP
[illegible]	none	✓		✓

SSID	VLAN	Open	Shared	Network EAP
[illegible]	none	✓		

Encryption Mode	[illegible]	[illegible]	Key Rotation
[illegible]			✓

Encryption Mode	[illegible]	[illegible]	Key Rotation
None			

Server Name/IP Address	Type	EAP	MAC	Proxy Mobile IP	Admin	Accounting
[illegible]	[illegible]	✓				

© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—9-73

In order to enable Authentication and dynamic WEP keying on an IOS AP, it is necessary to enable encryption and authentication settings as well as to define an Authentication Server.

These are configurable from the following Security submenus:

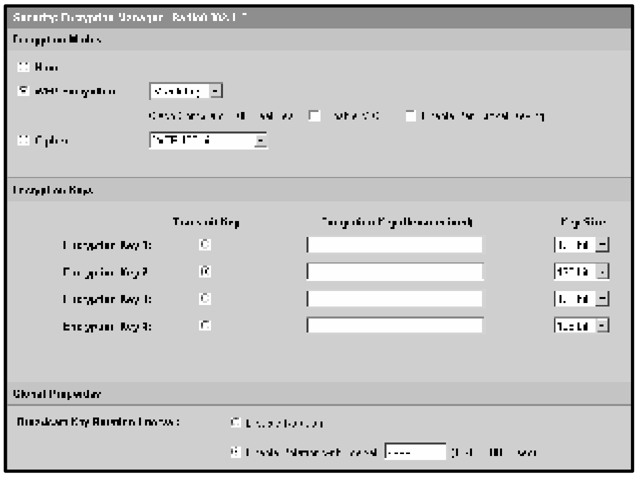
- Encryption Manager
- SSID Manager
- Server Manager

The Security tab on the left menu bar provides a summary view of the configured Security parameters, as well as providing links to the appropriate SSID, Encryption, and Server configuration screens.

Note that these encryption settings are configurable for each radio interface and also may be configured uniquely per VLAN.

Enabling Authentication on IOS AP

Cisco.com



AWLF v3.1—9-74

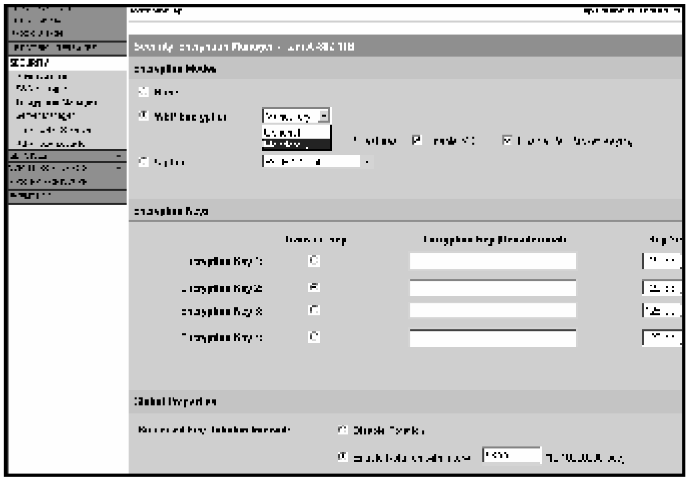
From the AP **Encryption Manager** screen, it is possible to configure WEP Encryption, any required WEP Encryption Keys, and enable Broadcast Key Rotation.

- **WEP Encryption:** Enable or Disable WEP Encryption, and if enabled, set WEP Encryption to Mandatory or Optional.
- **Encryption Keys:** enter **Encryption Key** string in Hex, set **Transmit Key**, and **Key Size**. Encryption key must be entered if using static WEP key clients in addition to dynamically keyed clients.

Under **Global Properties**, it is possible to enter **Broadcast Key Rotation Interval** and to specify the interval at the "**Enable Rotation with Interval**" textbox. Note that broadcast key rotation may not be used when static and dynamic WEP key clients coexist on a single SSID.

Enable Key Hashing and MIC

Cisco.com



AWLF v3.1—9-75

To enable Cisco Per-Packet Keying (a.k.a. key hashing or Cisco Temporal Key Integrity Protocol- TKIP) and Message Integrity Check (MIC), WEP Encryption must be enabled.

Select the appropriate checkboxes for:

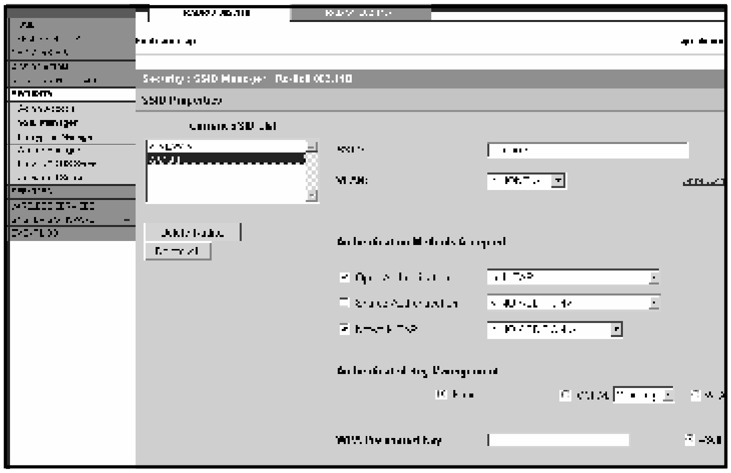
- Enable MIC
- Enable Per Packet Keying

Note	These features are only compatible with Cisco client devices.

Note	Also, Cisco TKIP (CKIP) and MIC (CMIC) may be enabled via the "**Cipher**" dropdown menu for use with Cisco Centralized Key Management protocol.

SSID Configuration for Authentication

Cisco.com


Security : SSID Manager - Radio0-802.11B
SSID Properties
Current SSID List
SSID:
VLAN:
Authentication Methods Accepted:
Network EAP
Authenticated Key Management
WPA Pre-shared Key

AWLF v3.1—9-76

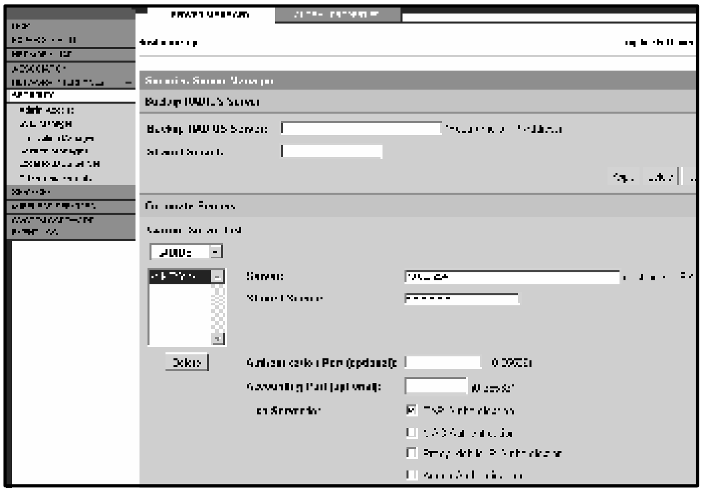
To enable Authentication for dynamic WEP key operation, it is necessary to configure the SSID to use one of the authentication mechanisms which supports dynamic WEP keying.

From **SSID Manager**, select the appropriate SSID to be configured for dynamic WEP.

Under **Authentication Methods Accepted**, select the following options:

- For Cisco client devices using Cisco Aironet Client Utility, select the **Network EAP** checkbox, no additional selections are required.
- For non-Cisco client devices, select **Open Authentication** and select "**with EAP**" from the dropdown menu.
- Also, if using static WEP, or unencrypted clients on the same SSID as the dynamic WEP key clients, make sure to enable "**Open Authentication**".

Enable RADIUS Server for EAP



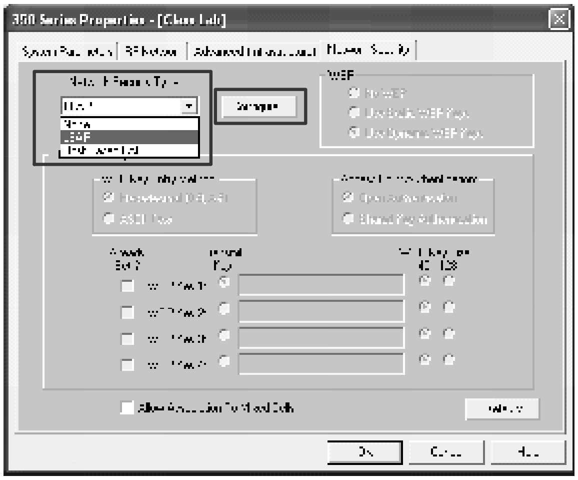
After configuration of Encryption settings and configuring an Authentication mechanism which permits dynamic WEP keying for the appropriate SSID, it is necessary to configure a RADIUS server to authenticate users and to generate the dynamic WEP key for distribution to the AP.

From **Server Manager** submenu, select the RADIUS Server type and enter the appropriate Server IP address or DNS name. Enter **Shared Secret** string for the RADIUS server in the textbox. Specify **EAP Authentication** by selecting the checkbox to specify that the server will be used for EAP Authentication.

Configuring the Client for Authentication

Enabling LEAP on the Client

Cisco.com



AWLF v3.1—9-79

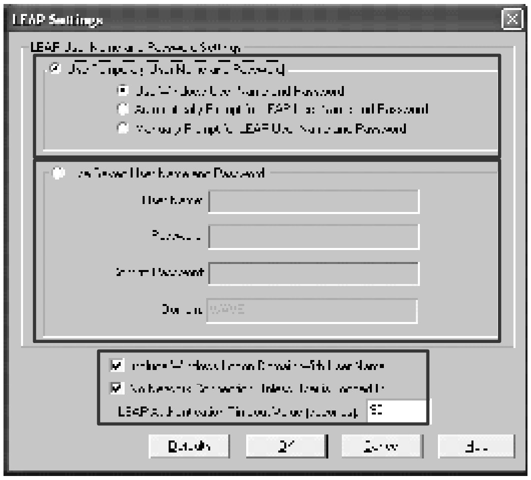
The ACU must be used to configure the client to use Server Based Authentication (EAP, LEAP, etc.). From the Profile Manager, choose the profile you wish to configure for Server Based Authentication, and click the **Edit** button. This will launch the Properties screens for the profile. Click the **Network Security** tab.

Network Security Type:

- **NONE**: Allows you to use Static WEP.
- **LEAP**: Leverages Cisco software and firmware to cause your network logon to trigger server-based authentication using your user name and password. Requires a LEAP-enabled RADIUS server running on the network. You can also choose the LEAP Settings
- **Host Based EAP**: Allows you to use Windows XP's built in EAP, such as EAP-TLS or EAP-MD5 or PEAP. Refer to Windows XP Help for information on how to set up EAP.

To configure LEAP or Host Based EAP Authentication, click the **Configure** button.

Configuring LEAP on the Client



LEAP Settings

LEAP User Name and Password Setting

- ● Use Temporary User Name and Password
  - ● Use Windows User Name and Password
  - ○ Automatically Prompt for LEAP User Name and Password
  - ○ Manually Prompt for LEAP User Name and Password
- ○ Use Saved User Name and Password
  - User Name
  - Password
  - Confirm Password
  - Domain

☑ Include Windows Logon Domain with User Name

☑ No Network Connection Unless User Is Logged In

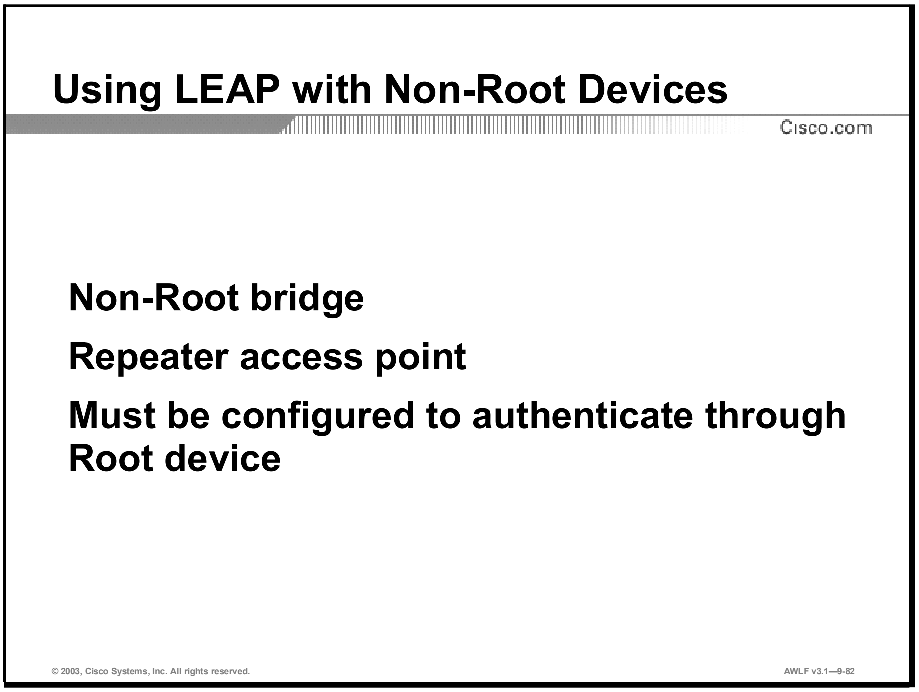
LEAP Authentication Timeout Value (in seconds) 90

AWLF v3.1—9-80

All of Cisco’s WLAN products can be configured to take advantage of LEAP. The WLAN products are classified into two categories, Client and Authenticator.

- Clients: A **Client** card uses the Aironet Client Unity (ACU) to setup and enable security. A **Non-Root Bridge**, **Repeater Access Point** and **Workgroup Bridge** can be configured with a LEAP user name and password. The preset user name and password will respond automatically when they are challenged for LEAP credentials.
- Authenticators: A Root Access Point and Root Bridge can be configured to pass Client and Authentication Server credentials. Until the Client’s credentials are confirmed the Client is denied access to the LAN.

Configuring Non-Root Devices for Authentication



Using LEAP with Non-Root Devices

Non-Root bridge

Repeater access point

Must be configured to authenticate through Root device

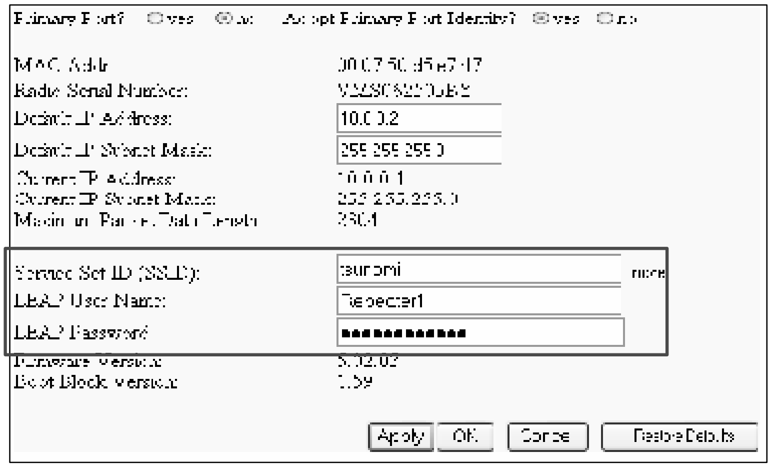
AWLF v3.1—9-82

If a Cisco Aironet Bridge or Access Point is configured as a non-root device, it can be also be configured to authenticate to the network like other wireless client devices. A non-root device can be configured with a username and password, allowing it to authenticate to the network using LEAP. The non-root device can then receive and use dynamic WEP keys.

In order for a non-root device to support LEAP authentication for wireless client devices, it must be configured to authenticate using LEAP, and must be configured with information about the authentication server that will be used to support the wireless client devices.

Configuring a Non-Root device for LEAP Authentication

Cisco.com



Primary Port? ○ yes ● no   Accept Primary Port Identity? ● yes ○ no

MAC Addr	00:07:50:d5:e7:17
Radio Serial Number:	[illegible]
Default IP Address:	10.0.0.2
Default IP Subnet Mask:	255.255.255.0
Current IP Address:	10.0.0.1
Current IP Subnet Mask:	255.255.255.0
Maximum Packet Data Length	2304
Service Set ID (SSID):	tsunami
LEAP User Name:	Repeater1
LEAP Password	●●●●●●●●●●●●●
Firmware Version:	5.02.02
Boot Block Version:	1.59

AWLF v3.1—9-83

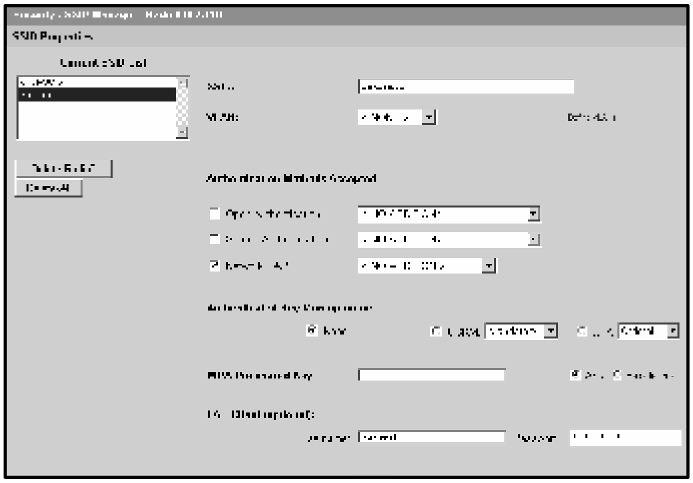
In order to configure a non-root device for LEAP authentication you must do the following:

- Enter the **SSID** (must match access point that non-root device will connect with).
- Enter the **LEAP User Name**.
- Enter **LEAP Password**.
- Click Apply or **OK**.

Note The unit is then set to use LEAP authentication. Ensure that there is a User Account set up for the non-root device in the user database.

Configuring Non-root IOS devices for LEAP Authentication

Cisco.com



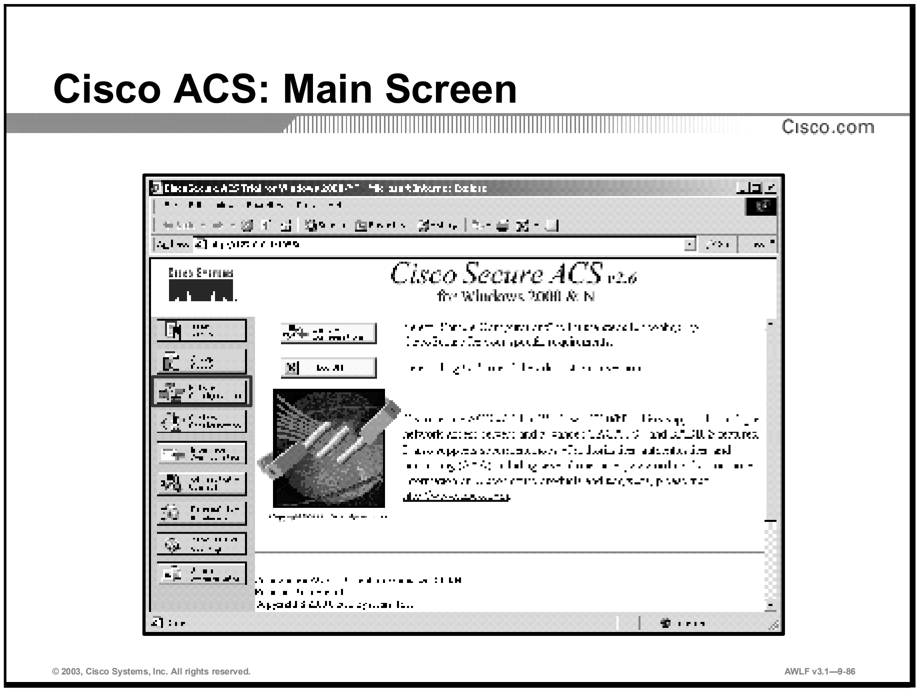
AWLF v3.1—9-84

In order to configure a non-root IOS device (either a repeater or a non-root bridge) for LEAP authentication you must do the following:

- Enter the **SSID** (this must match the root bridge or access point that non-root device will connect with).
- Under **EAP Client**, enter **Username**.
- Also under **EAP Client**, enter **Password**.
- Create a user entry in the EAP/ RADIUS server for this non-root device

Also note that if this non-root device will be used to authenticate other LEAP client devices, it is necessary to configure the SSID for **Network EAP** (or **Open Authentication** & **with EAP**) under **Authentication Methods Accepted**. There will also need to be an entry in the EAP/ RADIUS server for this non-root device as a AAA client/ NAS.

Configuring Cisco ACS



Cisco ACS: Main Screen

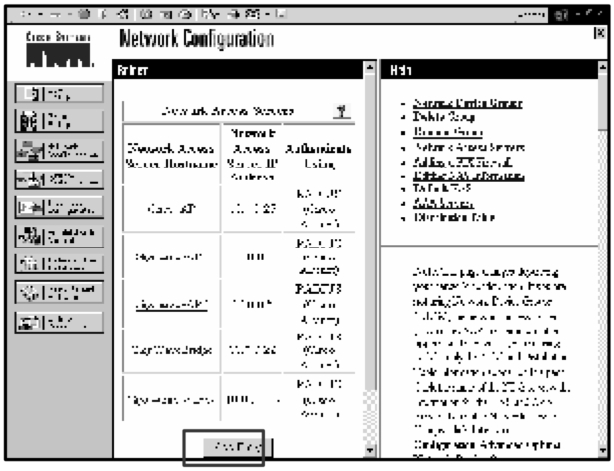
Cisco.com

AWLF v3.1—9-86

To begin configuring Cisco ACS to work with Cisco Aironet Access Points as Network Access Servers (NAS), open the Cisco ACS main screen. From the navigation bar, click the **Network Configuration** button. This will launch the Network Configuration screen.

Network Configuration

Cisco.com


Network Configuration
Network Access Servers
Network Access Server Hostname
Network Access Server IP Address
Authenticate Using

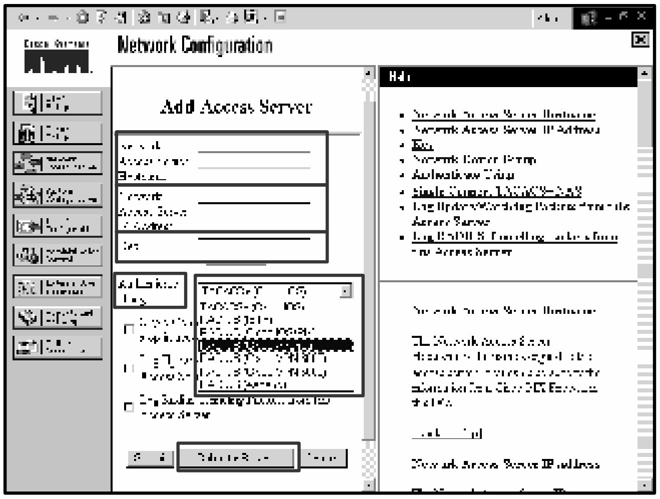
© 2003, Cisco Systems, Inc. All rights reserved.

AWLF v3.1—9-87

The Network Configuration screen lists all NASs that are currently configured. To add a NAS, click the **Add Entry** button. This will launch the Add Access Server screen.

Access Server Setup Example

Cisco.com



AWLF v3.1—9-88

To configure Cisco ACS for use with the Cisco Aironet product as a NAS, perform the following:

Step 1 On the ACS menu (left side of screen) click on the **Network Configuration** button then click **ADD Access Server**. This will bring up the Add Access Server screen.

Each individual access point is considered a Network Access Server (NAS). To configure a NAS, enter the following:

Step 2 **Network Access Server Hostname:** DNS name of the specified access point

Step 3 **Network Access Server IP Address:** IP address of the specified access point

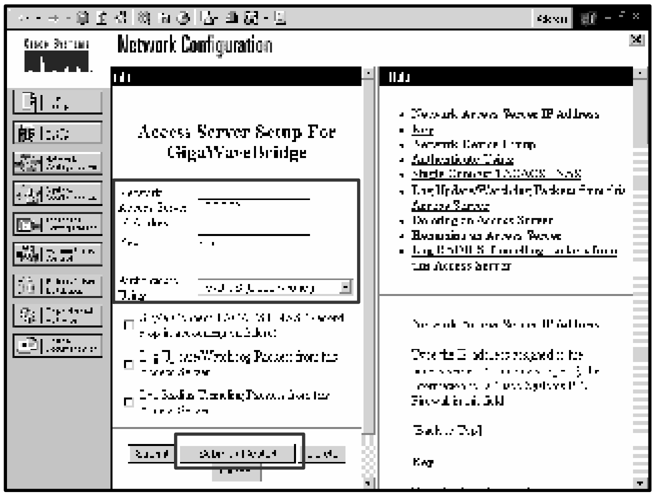
Step 4 **Key:** Shared secret between the server and this individual access point

Step 5 **Authenticate Using:** Must select “RADIUS (Cisco Aironet)”

Each key can be different on a per access point basis but must match the setting in the specified access point.

Access Server Setup Example (Cont.)

Cisco.com

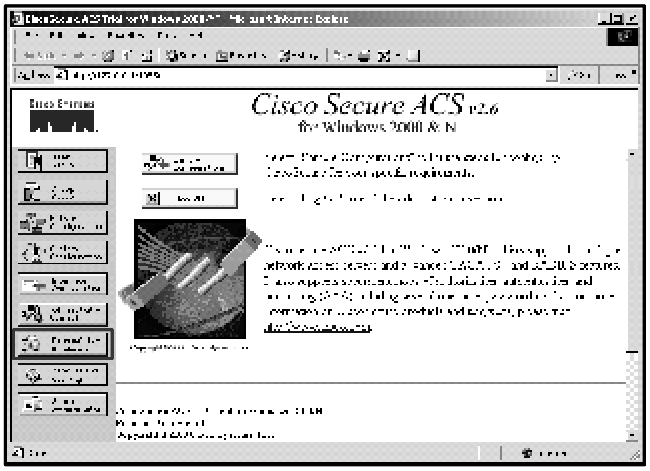

Network Configuration
Access Server Setup For GigaWaveBridge
Network Access Server IP Address
Key
Network Device Group
Authenticate Using
Single Connect TACACS+ NAS
Deleting an Access Server
Key

AWLF v3.1—9-89

Step 6 When finished configuring the Network Access Server (NAS) click the **Submit+Restart** button. Cisco ACS is now ready to receive authentication requests via the NAS.

External User Database

Cisco.com



AWLF v3.1—9-90

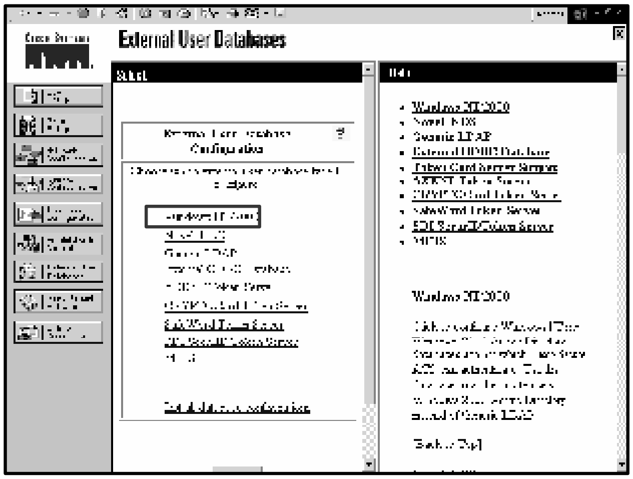
Configuring a Windows NT/2000 External User Database

To configure Cisco Secure ACS to authenticate users against the Windows NT/2000 user database in your network's trusted domains, follow these steps:

Step 7 In the navigation bar, click **External User Databases**.

External User Database: Windows NT/2000

Cisco.com

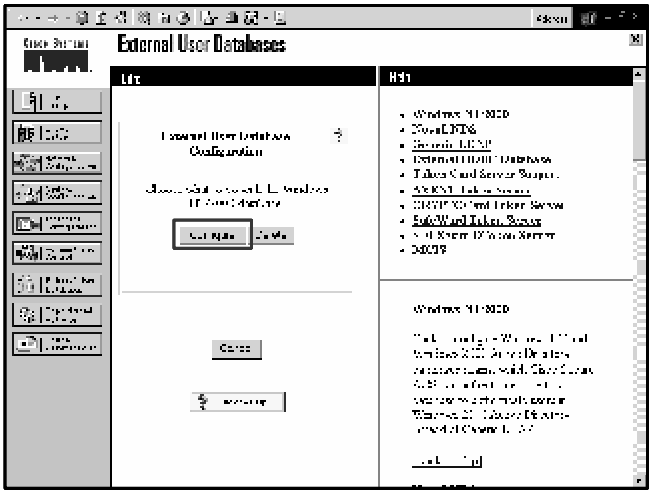


AWLF v3.1—9-91

Step 8 Click **Windows NT/2000**. This will launch the External User Database Configuration screen.

Windows NT/2000 Database (Cont.)

Cisco.com



External User Databases

Edit

External User Database Configuration

Configure

Cancel

Help

- Windows NT/2000
- Novell NDS
- Generic LDAP
- External ODBC Database
- Token Card Server Support
- AXENT Token Server
- CRYPTOCard Token Server
- SafeWord Token Server

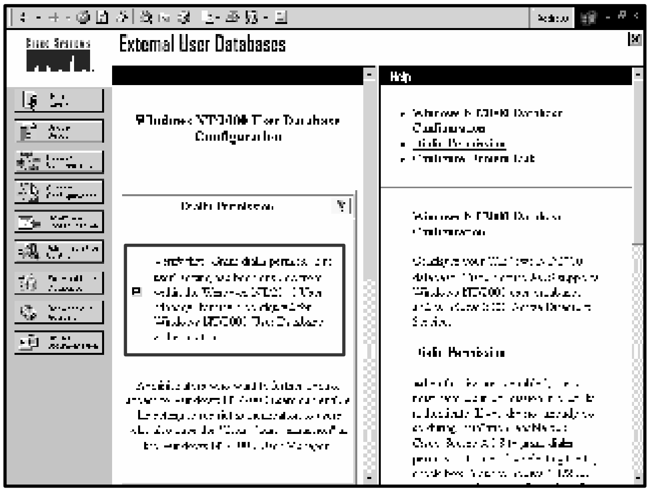
Windows NT/2000

AWLF v3.1—9-92

Step 9 Click **Configure**. The will launch the Windows NT/2000 User Database Configuration screen.

Windows NT/2000 Database (Cont.)

Cisco.com



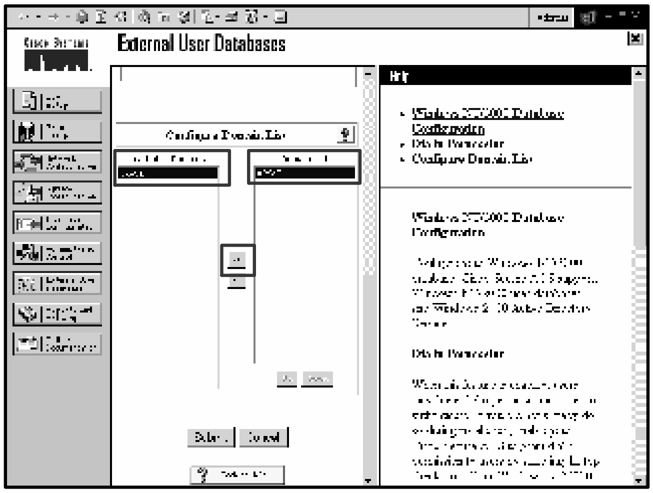
AWLF v3.1—9-93

Step 10 To restrict network access to users who have Windows dial-in permission, select the "**Verify that Grant dial in permission…**" to user check box.

Note Windows dial in permission is enabled in the Dial in section of user properties in Windows NT and on the Dial-in tab of the user properties in Windows 2000.

Windows NT/2000 Database (Cont.)

Cisco.com



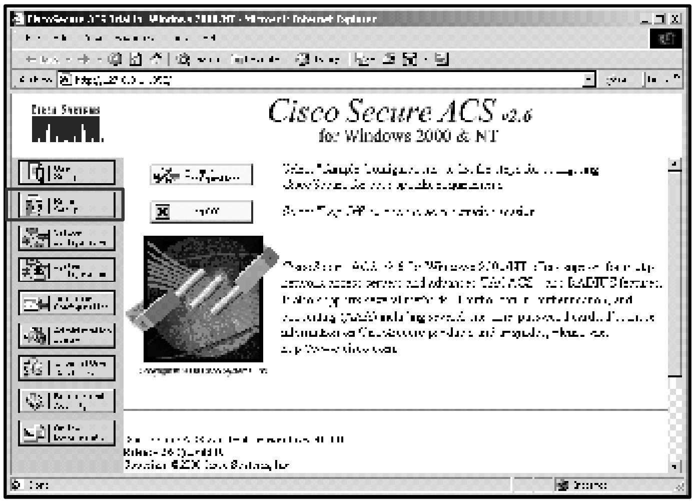
AWLF v3.1—9-94

Step 11 To authenticate explicitly using each trusted Windows domain for usernames that are not domain-qualified, select (highlight) the domains you want Cisco Secure ACS to use to authenticate unqualified usernames in the **Available Domains** list and move them to the **Domain List** by clicking the button with the arrow pointing to the **Domain List** box. Click **Submit**.

Cisco Secure ACS will then save the Windows NT/2000 user database configuration that was created. It is then possible to add it to the **Unknown User Policy** or assign specific user accounts to use this database for authentication.

Session Policy Setup

Cisco.com



Cisco Secure ACS v2.6

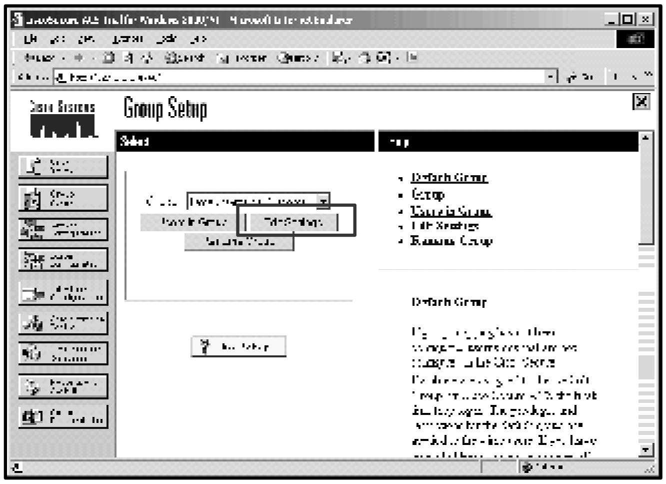
for Windows 2000 & NT

AWLF v3.1—9-95

Step 1 To adjust the timeout value for the client session (requiring re-authentication and new WEP key derivation), click the **Group Setup** button form the ACS main screen. This will launch the Group Setup screen.

Session Policy Setup (Cont.)

Cisco.com

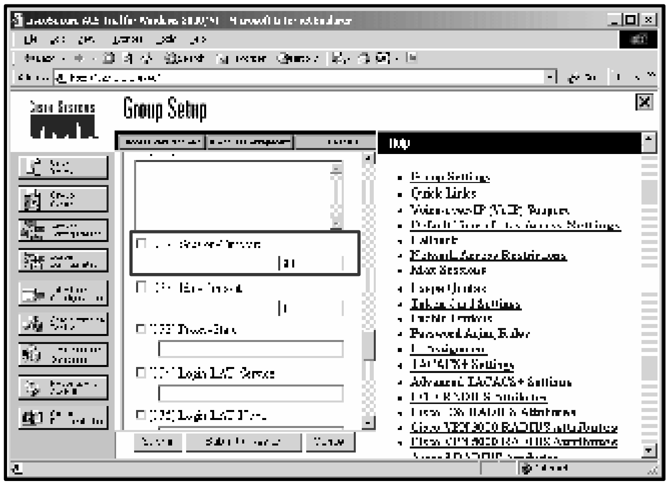


AWLF v3.1—9-96

Step 2 From the Group Setup screen, choose a group (usually the default group) and click the **Edit Settings** button.

Session Policy Setup (Cont.)

Cisco.com



AWLF v3.1—9-97

Step 3 Scroll down through the setup menu and find the **[027] Session Timeout** entry. Enter the timeout value in seconds. The timeout value will depend upon the number of users typically attached to the access point, as well as the amount of traffic the clients will typically be sending. The larger the number of users, or the more traffic the users are sending, the smaller the value needs to be to insure that the WLAN is protected. By setting smaller values it is possible to prevent a hacker from being able to capture enough packets to hack a WEP key.

Recommended values:

- Using WEP only with 802.1X, key rotation time: 15 minutes
- Using WEP and TKIP with 802.1X key rotation time: 240 minutes

Note These values apply to both session keys and broadcast key.

For help in determining the best session key timeout value, consult *Cisco Product Bulletin 1515: Cisco Wireless LAN Security Bulletin*. This can be found at:

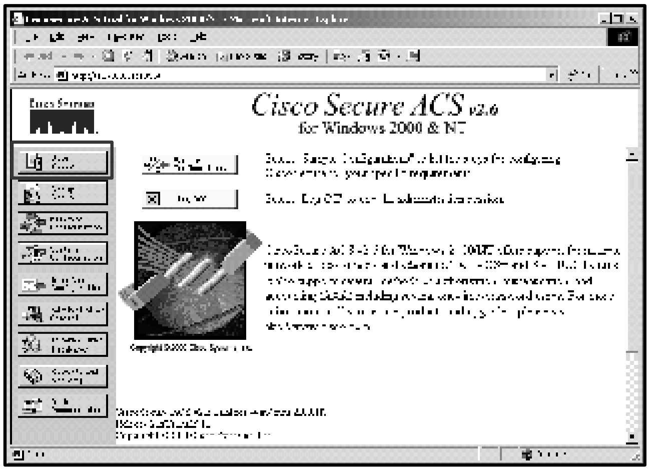
http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a008009246f.html

Step 4 When finished click the **Submit+Restart** button.

User Setup

User Setup in ACS

Cisco.com



AWLF v3.1—9-99

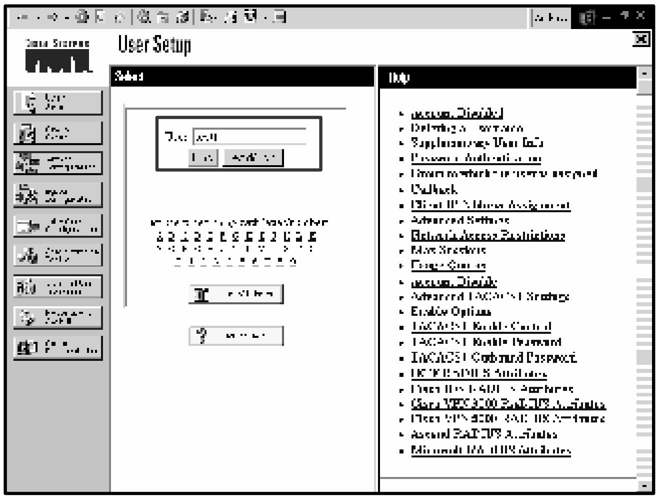
Cisco ACS can use the Cisco Radius server as the User database or an external User Database.

Note If using the Windows NT/2000 database, all users who should have wireless access must have “remote access” enabled under their user profile.

Step 1 To configure accounts on Cisco ACS, click the **User Setup** button from the main screen. This will launch the User Setup screen.

User Setup in ACS (Cont.)

Cisco.com

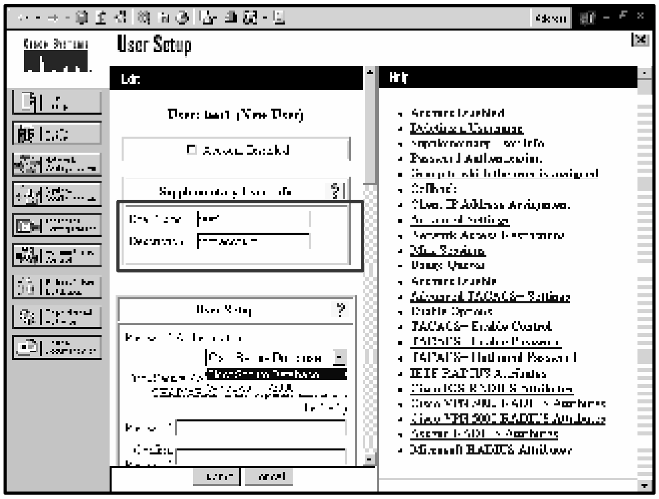


AWLF v3.1—9-100

Step 2 To set up a new user, type the User name into the **User:** box and press **Enter**.

User Setup in ACS: New User

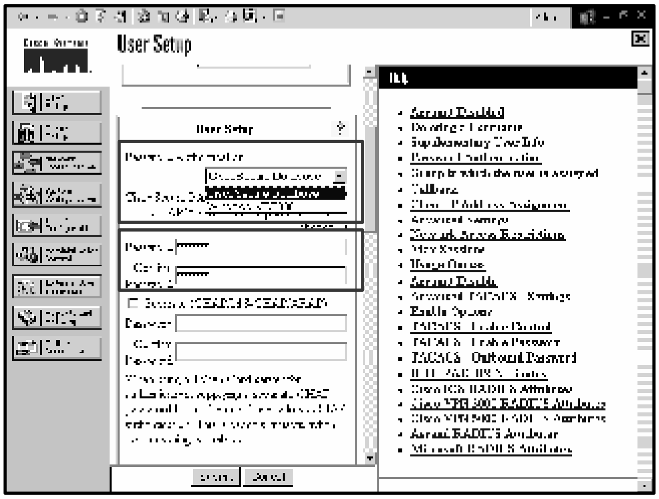
Cisco.com



Step 3 Enter information about the user. At a minimum, the **Real Name** (user’s real name) and **Description** (description of the account) should be entered.

User Setup in ACS: New User (Cont.)

Cisco.com



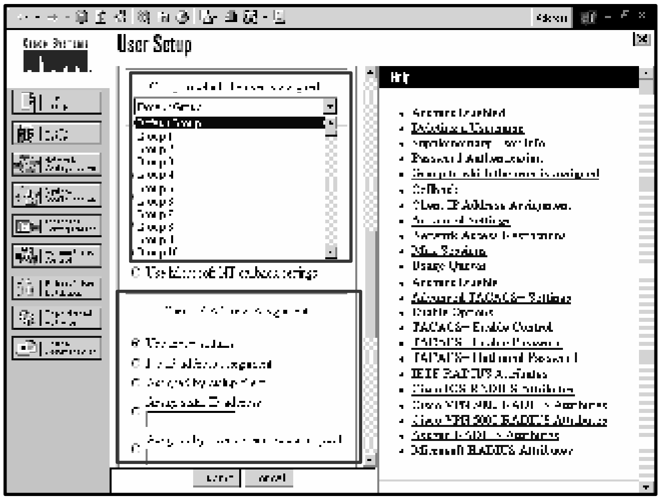
AWLF v3.1—9-102

Step 4 Scroll down to the **Password Authentication** entry and choose **Cisco Secure Database** form the drop down menu. This indicates that the user account will be stored on Cisco ACS.

Step 5 Type the password in the **Password** box. Retype the password in the **Confirm Password** box.

User Setup in ACS: New User (Cont.)

Cisco.com



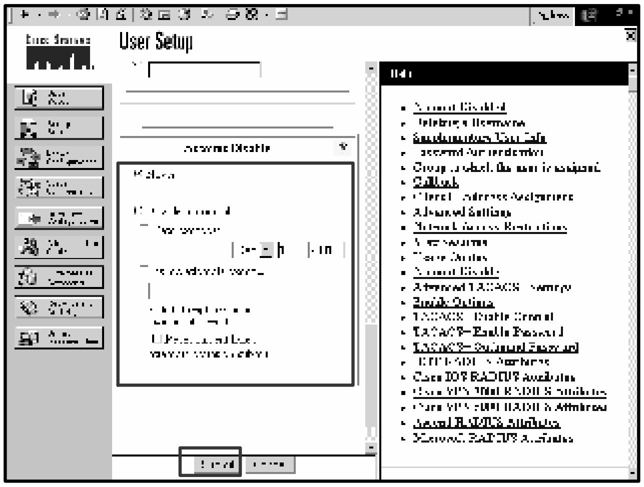
AWLF v3.1—9-103

Step 6 Scroll down to the **Group to which the user is assigned** box. From the dropdown menu, choose which group the user will belong to. Unless otherwise specified, all users are assigned to the **Default Group**.

Step 7 Scroll down to **Client IP Address Assignment**. Choose how the user will be assigned an IP address.

User Setup in ACS: New User (Cont.)

Cisco.com



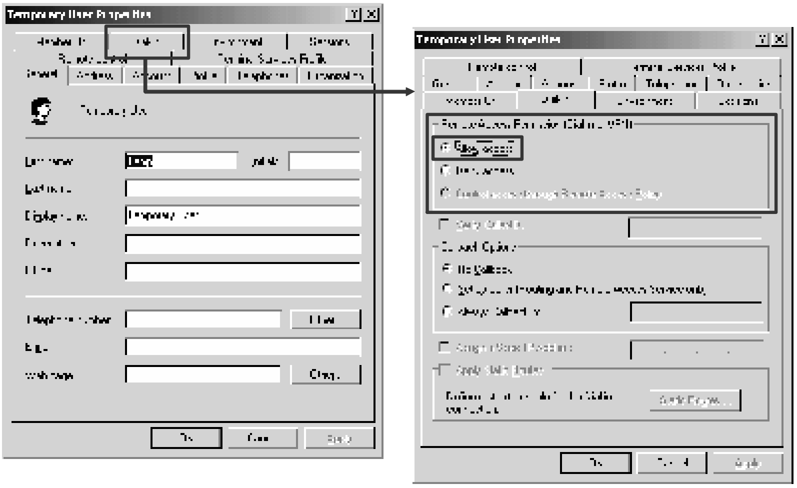
AWLF v3.1—9-104

Step 8 Scroll down to the **Account Disable** box. Choose how and if the account will be disabled. By default the account is never disabled. Using this feature is possible to set up temporary accounts with an expiration date.

Step 9 When finished, click the **Submit** button. The user account is now set up and ready for use.

Windows 2000 User Setup: Dial-In Permission

Cisco.com



AWLF v3.1—9-105

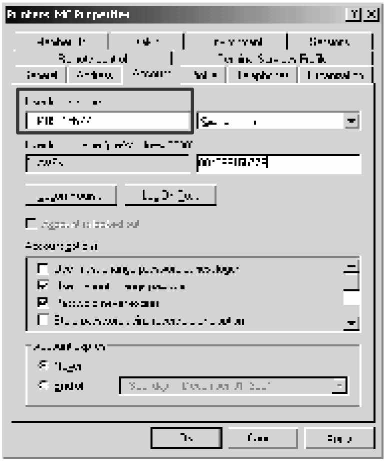
When using an external Windows NT/2000 database, all user accounts must be set up for remote access. In order to do this, open the **Properties** screen for the account, click the **Dial-In** tab, and insure that **Allow Access** radio button is checked under Remote Access Permission (Dial-In or VPN). When finished, click the **OK** or **Apply** button to apply the changes.

MAC Address Authentication

Cisco.com

Use for devices not capable of performing EAP authentication

Username and Password are MAC address

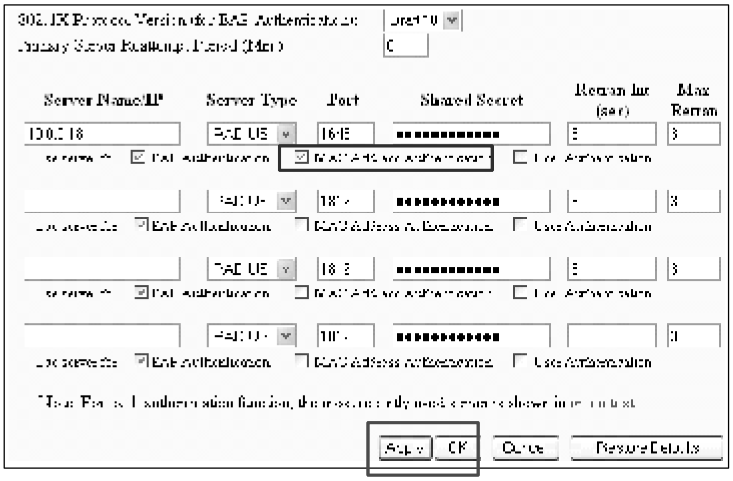


AWLF v3.1—9-106

For wireless clients not capable of using LEAP or other Host-Based EAP authentication, it is possible to authenticate by the client’s MAC address.

MAC Address Authentication: Access Point Setup

Cisco.com



802.1X Protocol Version (for EAP Authentication): Draft 10

Primary Server Reattempt Period (Min): 0

Server Name/IP	Server Type	Port	Shared Secret	Retran Int (sec)	Max Retran
10.0.1.18	RADIUS	1645	●●●●●●●●●●●●●	5	3
	RADIUS	1812	●●●●●●●●●●●●	-	3
	RADIUS	1812	●●●●●●●●●●●●●	5	3
	RADIUS	1812	●●●●●●●●●●●●		0

Row 1 – Use server for: ☑ EAP Authentication ☑ MAC Address Authentication □ User Authentication

Row 2 – Use server for: ☑ EAP Authentication □ MAC Address Authentication □ User Authentication

Row 3 – Use server for: ☑ EAP Authentication □ MAC Address Authentication □ User Authentication

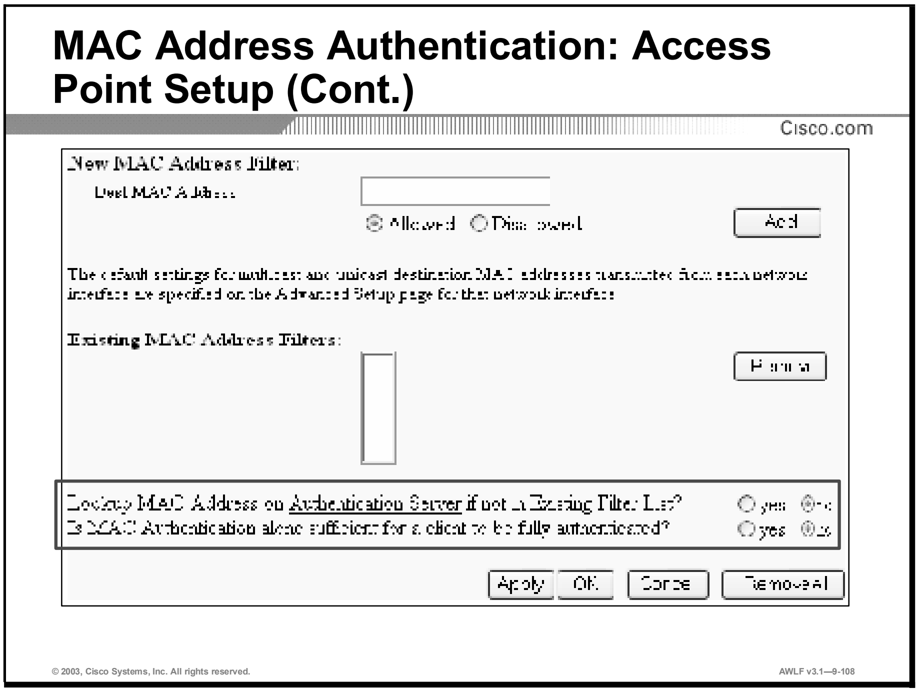
Row 4 – Use server for: ☑ EAP Authentication □ MAC Address Authentication □ User Authentication

[illegible]

AWLF v3.1—9-107

To configure the access point for MAC address authentication:

Step 1 From the Main screen (System Status screen) click the **Setup** link, then click the **Security** link, then click the **Authentication Server** link. This will launch the Authentication Server screen. Insure that the **MAC Address Authentication** box is checked for each of the Network Authentication Servers to be used for MAC Address Authentication. Click **OK** or **Apply** to apply the necessary changes.



MAC Address Authentication: Access Point Setup (Cont.)

Cisco.com

New MAC Address Filter:

Dest MAC Address:

● Allowed ○ Disallowed

The default settings for multicast and unicast destination MAC addresses transmitted from each network interface are specified on the Advanced Setup page for that network interface.

Existing MAC Address Filters:

Lookup MAC Address on Authentication Server if not in Existing Filter List? ○ yes ● no

Is MAC Authentication alone sufficient for a client to be fully authenticated? ○ yes ● no

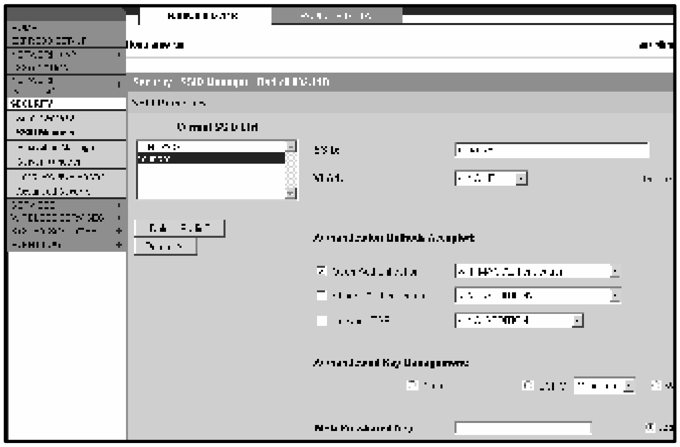
AWLF v3.1—9-108

Step 2 To insure that the access point will check accounts on the authentication server for MAC address authentication, return to the Setup screen, and then click the **Address Filters** link. This will launch the Address Filters screen. Insure that the **yes** radio button is checked for "**Lookup MAC Address on <u>Authentication Server</u> if not in Existing Filter List?** ". Click **OK** or **Apply** to apply the changes.

The access point is now set up for MAC address authentication.

MAC Address Authentication

Cisco.com



AWLF v3.1—9-109

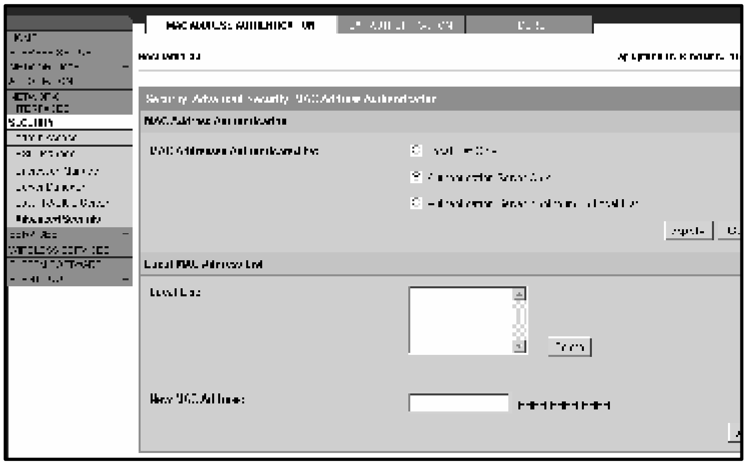
To configure the IOS access point for MAC address authentication:

- From the **Security**> **SSID Manager**, the SSID which is to be used for MAC Authentication must have “**with MAC Authentication**” selected from the appropriate dropdown box.

Note that MAC Authentication may be added to Open, Shared, or Network EAP Authentication.

MAC Address Authentication (Cont.)

Cisco.com



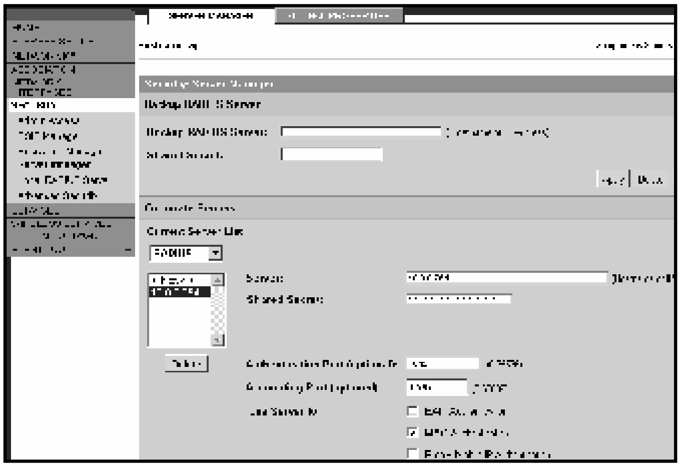
AWLF v3.1—9-110

There are multiple mechanisms for accomplishing MAC authentication at the Access Point. In order to enable one of these methods, select one of the following selections under "**MAC Address Authenticated by**:" and configure the appropriate SSID and Server parameters.

- **Local List Only:** When enabled, the AP will search only the locally configured MAC addresses- those addresses configured on this page- or via CLI "username" and password commands
- **Authentication Server Only:** When enabled, the AP will only use the configured MAC authentication server to authenticate clients
- **Authentication Server if not found in Local List:** When enabled, the AP initially uses Local List to authenticate users and secondarily queries the RADIUS server for MAC address authentication.

MAC Address Authentication (Cont.)

Cisco.com

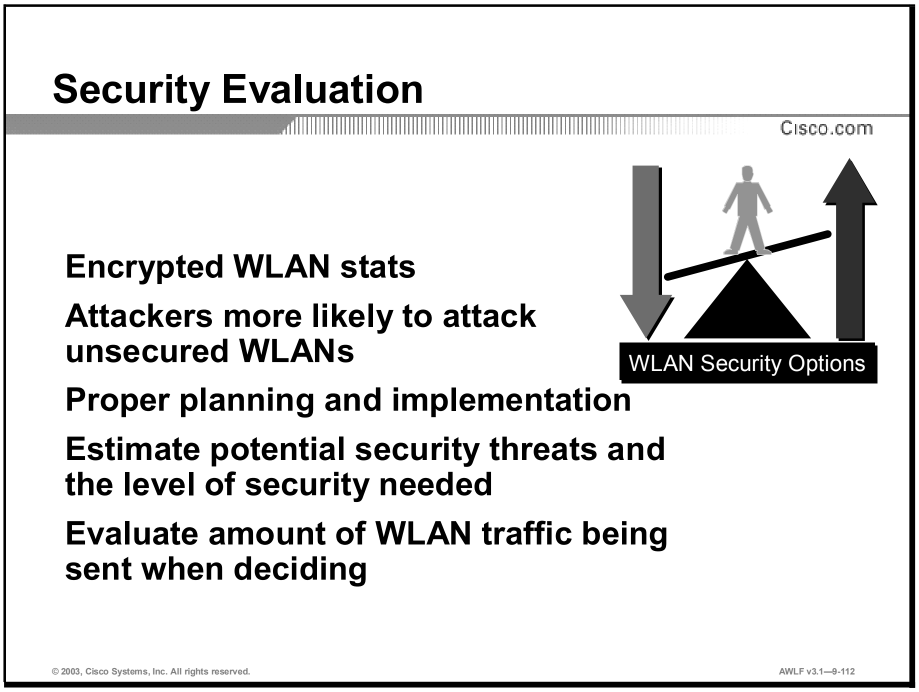


AWLF v3.1—9-111

To configure the access point for communication with a RADIUS server for MAC address authentication:

- From the **Security**> **Server Manager** submenu, select (or enter) the appropriate RADIUS server to be used for MAC address authentication.
- Select **RADIUS** under "**Current Server List**:" and enter the Server's IP address or DNS hostname under "**Server**:" textbox. Enter the **Shared Secret** which matches the shared secret RADIUS key value configured on the server.
- Select the **MAC Authentication** box under "**User Server for**:" menu.

Note	RADIUS server must have entry in user database with the MAC address of the client device as both username and password.



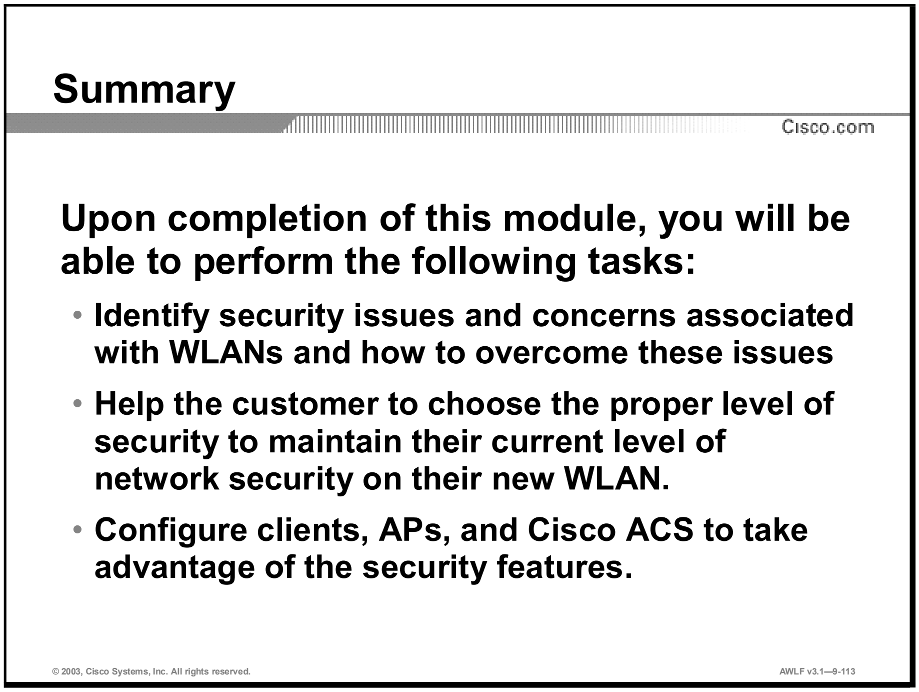
Security Evaluation

WLAN Security Options

- Encrypted WLAN stats
- Attackers more likely to attack unsecured WLANs
- Proper planning and implementation
- Estimate potential security threats and the level of security needed
- Evaluate amount of WLAN traffic being sent when deciding

Summary

This section summarizes the concepts you have learned in this module.



Summary

Upon completion of this module, you will be able to perform the following tasks:

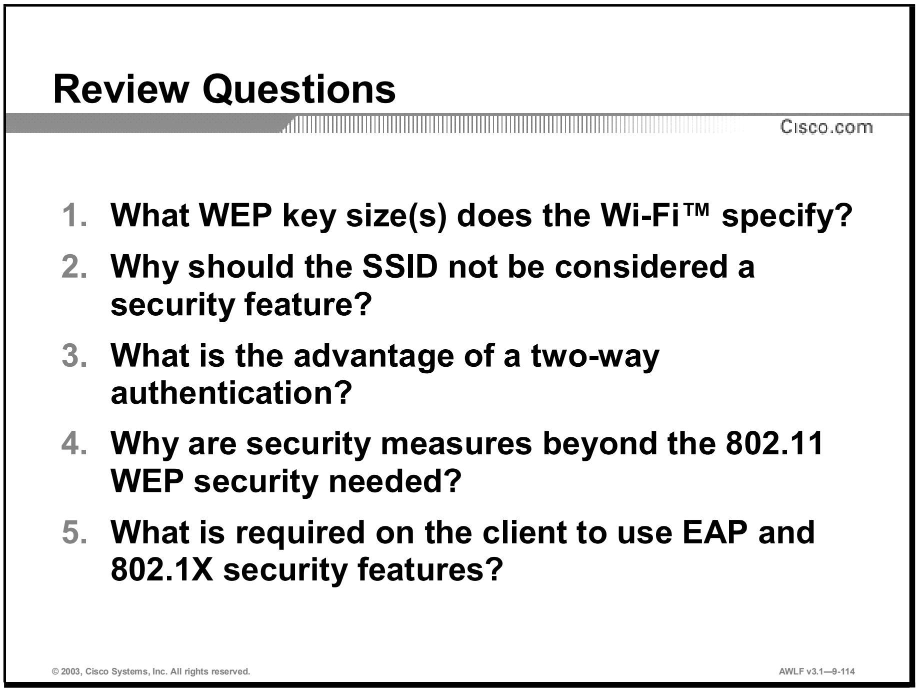
- Identify security issues and concerns associated with WLANs and how to overcome these issues
- Help the customer to choose the proper level of security to maintain their current level of network security on their new WLAN.
- Configure clients, APs, and Cisco ACS to take advantage of the security features.

AWLF v3.1—9-113

Upon completion of this module, you will be able to perform the following tasks:

- Identify security issues and concerns associated with WLANs and how to overcome these issues.
- Help the customer to choose the proper level of security to maintain their current level of network security on their new WLAN.
- Configure clients, APs, and Cisco ACS to take advantage of the security features.

Review Questions



Review Questions

1. What WEP key size(s) does the Wi-Fi™ specify?
2. Why should the SSID not be considered a security feature?
3. What is the advantage of a two-way authentication?
4. Why are security measures beyond the 802.11 WEP security needed?
5. What is required on the client to use EAP and 802.1X security features?

AWLF v3.1—9-114

Answer these review questions.

Module 10

WLAN Management Solutions

Overview

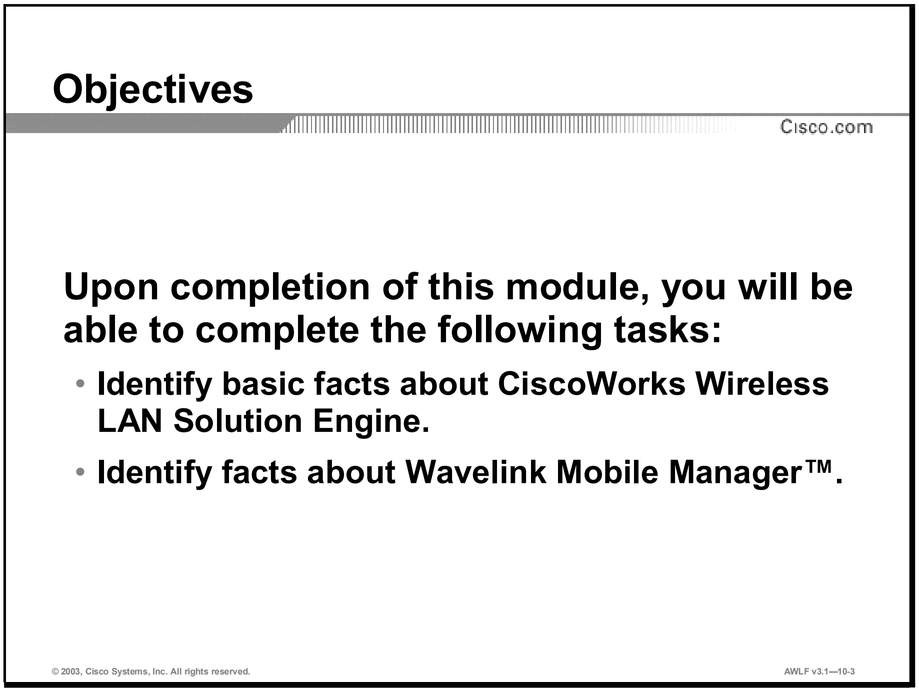
This module provides an overview of WLSE which is a hardware and software solution for managing Cisco wireless devices. It includes the following topics:

It includes the following topics:

- Objectives
- Wireless LAN Challenges
- CiscoWorks Wireless LAN Solution Engine 2.0
- Wavelink Mobile Manager
- Wavelink Avalanche 2.0
- Summary
- Review Questions

Objectives

This section lists the module's objectives.



Objectives

Cisco.com

Upon completion of this module, you will be able to complete the following tasks:

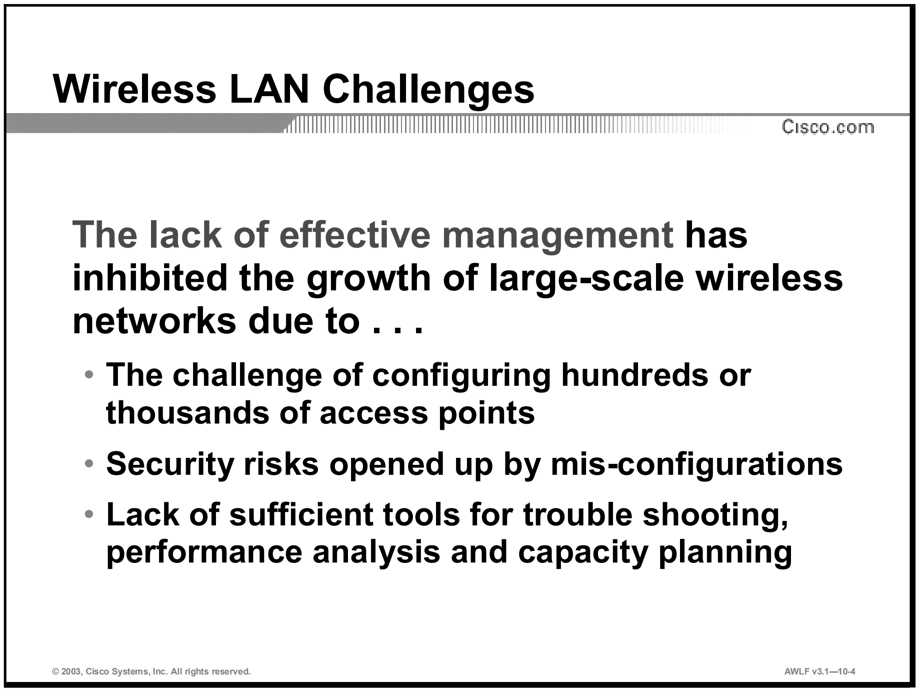
- **Identify basic facts about CiscoWorks Wireless LAN Solution Engine.**
- **Identify facts about Wavelink Mobile Manager™.**

AWLF v3.1—10-3

Upon completion of this module, you will be able to complete the following tasks:

- Identify basic facts about CiscoWorks WLSE.
- Identify facts about Wavelink Mobile Manager™.

Wireless LAN Challenges



Wireless LAN Challenges

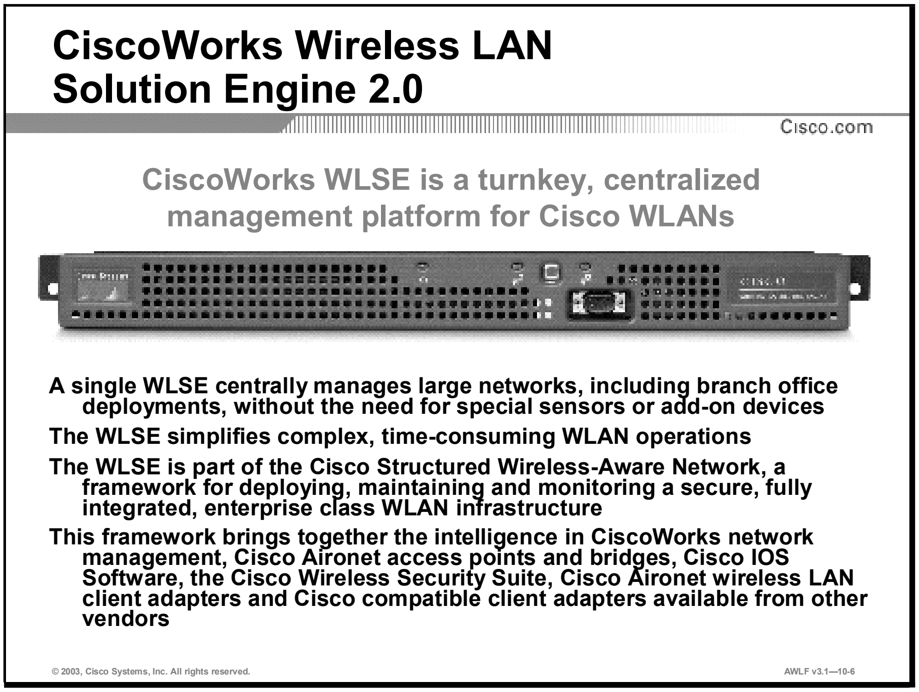
Cisco.com

The lack of effective management has inhibited the growth of large-scale wireless networks due to . . .

- **The challenge of configuring hundreds or thousands of access points**
- **Security risks opened up by mis-configurations**
- **Lack of sufficient tools for trouble shooting, performance analysis and capacity planning**

AWLF v3.1—10-4

CiscoWorks WLSE



CiscoWorks Wireless LAN Solution Engine 2.0

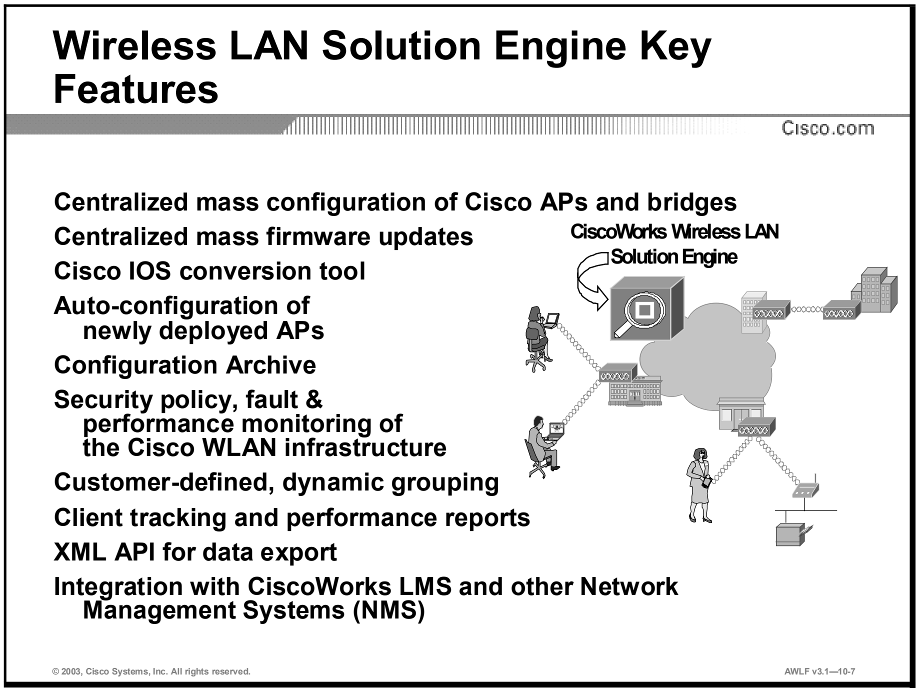
Cisco.com

CiscoWorks WLSE is a turnkey, centralized management platform for Cisco WLANs

- A single WLSE centrally manages large networks, including branch office deployments, without the need for special sensors or add-on devices
- The WLSE simplifies complex, time-consuming WLAN operations
- The WLSE is part of the Cisco Structured Wireless-Aware Network, a framework for deploying, maintaining and monitoring a secure, fully integrated, enterprise class WLAN infrastructure
- This framework brings together the intelligence in CiscoWorks network management, Cisco Aironet access points and bridges, Cisco IOS Software, the Cisco Wireless Security Suite, Cisco Aironet wireless LAN client adapters and Cisco compatible client adapters available from other vendors

AWLF v3.1—10-6

The CiscoWorks WLSE is a centralized, turnkey solution for managing the entire Cisco Aironet® Wireless LAN infrastructure. A single CiscoWorks WLSE gives administrators visibility into the WLAN without the need for any special sensors, add-on devices or so-called wireless switches. Key features like AutoConfig, mass configuration and firmware updating significantly reduce the time and resources needed for administration and trouble shooting, even when hundreds or thousands of access points or large numbers of remote sites are involved.



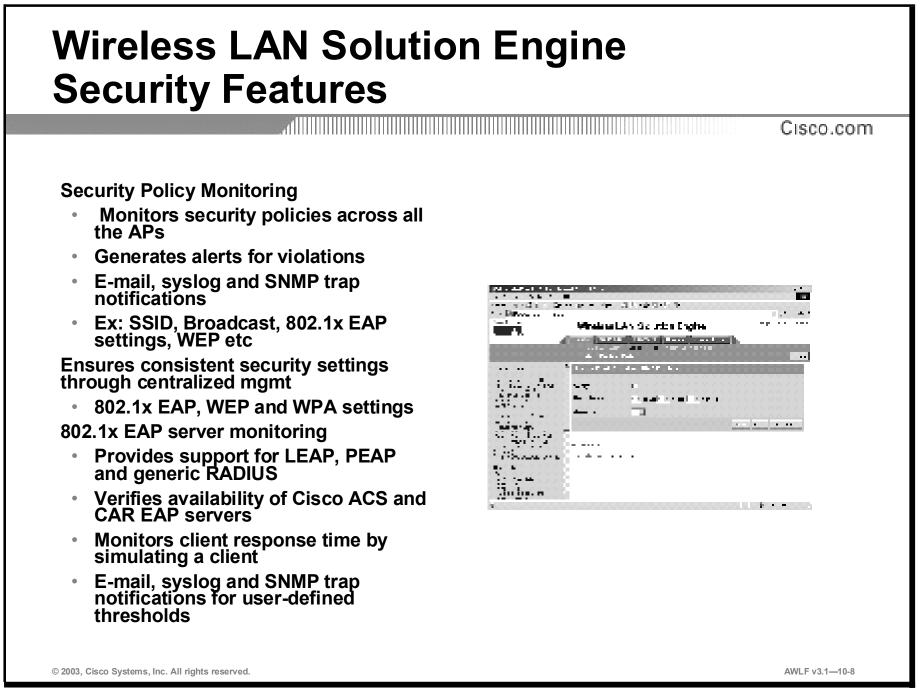
Wireless LAN Solution Engine Key Features

Cisco.com

- Centralized mass configuration of Cisco APs and bridges
- Centralized mass firmware updates
- Cisco IOS conversion tool
- Auto-configuration of newly deployed APs
- Configuration Archive
- Security policy, fault & performance monitoring of the Cisco WLAN infrastructure
- Customer-defined, dynamic grouping
- Client tracking and performance reports
- XML API for data export
- Integration with CiscoWorks LMS and other Network Management Systems (NMS)

AWLF v3.1—10-7

The CiscoWorks WLSE is part of the Cisco Structured Wireless-Aware Network framework for deploying, maintaining and monitoring a secure, fully integrated, enterprise-class wireless LAN infrastructure. This framework brings together intelligence in CiscoWorks network management, Cisco Aironet® Series access points and bridges, Cisco IOS® Software, the Cisco Wireless Security Suite, Cisco Aironet wireless LAN client adapters and Cisco compatible client devices available from other vendors. This unique Cisco framework introduces “wireless aware” capabilities into Cisco IOS Software to extend the WLAN to the same level of security, scalability and reliability that customers have come to expect in a wired LAN.



Wireless LAN Solution Engine Security Features

Cisco.com

Security Policy Monitoring

- Monitors security policies across all the APs
- Generates alerts for violations
- E-mail, syslog and SNMP trap notifications
- Ex: SSID, Broadcast, 802.1x EAP settings, WEP etc

Ensures consistent security settings through centralized mgmt

- 802.1x EAP, WEP and WPA settings

802.1x EAP server monitoring

- Provides support for LEAP, PEAP and generic RADIUS
- Verifies availability of Cisco ACS and CAR EAP servers
- Monitors client response time by simulating a client
- E-mail, syslog and SNMP trap notifications for user-defined thresholds

AWLF v3.1—10-8

Security Policy Monitoring

The CiscoWorks WLSE generates alerts for security policy misconfigurations on Cisco Aironet access points and bridges, thus reducing potential security vulnerabilities and maintaining pre-defined Cisco Wireless Security Suite parameters. For example, when the CiscoWorks WLSE finds an access point or bridge without a Service Set Identifier (SSID) in a valid SSID list, a fault notification can be generated. Other security parameters monitored, include verification that SSID is disabled, that WEP is enabled, that Cisco LEAP, Protected Extensible Authentication Protocol (PEAP) or RADIUS is enabled and that HTTP/Telnet are disabled.

Secure User Interface

The CiscoWorks WLSE web-based graphical user interface supports Secure Socket Layer (SSL); Secure Shell (SSH) is employed for Telnet access.

Wireless LAN Solution Engine Configuration

Cisco.com

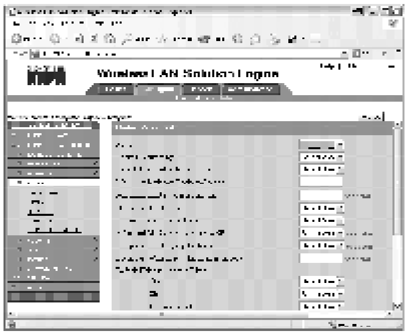
Centralized bulk configuration and firmware image distribution of access points and bridges with user-defined groups

Automatic configuration of newly deployed access points and bridges using a customer defined template

On-demand and scheduled Configuration Archive of 4 prior versions of APs/Bridges

VxWorks to IOS conversion tool

WLSE configuration job can be run immediately, scheduled to run later at a convenient time, or scheduled as a recurring job



AWLF v3.1—10-9

Dynamic Grouping

Groups make the network easier to understand and to operate. Devices may be organized into hierarchical groups defined by the administrator. Groups may span multiple subnets. By default, access points and bridges are grouped by Service Set Identifier (SSID), system location, device type, firmware release, and subnet. Group level polling allows different policies and polling profiles to exist for different sets of devices.

Mass Configuration

Configuring a group with hundreds of devices requires no more effort than configuring just a single device. Configuration tasks may be scheduled or executed on demand. Configuration parameters can be verified before they are applied.

Configuration Archive

The configuration archive stores the last four configuration versions of each device, allowing configurations to be rolled back. A search facility finds configurations by access point name or IP address.

AutoConfig

If desired, newly deployed access points may automatically receive customer-defined, default configurations using DHCP through a feature called “AutoConfig”. This allows administrators to maintain control in rapidly expanding environments. Specific configurations are downloaded based on device type and subnet for authorized MAC addresses.

VLAN Configuration

The CiscoWorks WLSE configures and monitors VLANs on access points, allowing customers to differentiate LAN policies and services, such as security and QoS, for different users. Support for public access is made possible through support for multiple unencrypted VLANs.

Centralized Firmware Updates

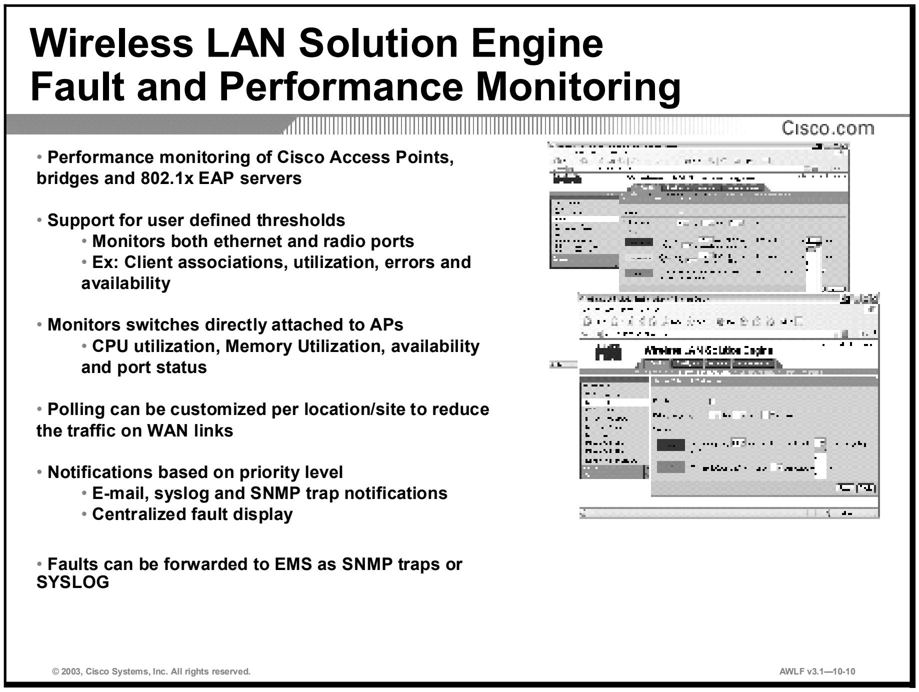
Cisco Aironet access point and bridge firmware may be updated in mass. Updates may be assigned to a specific device or to groups. Tasks may be scheduled or executed on demand. Software images may be imported from the Cisco web site and the CiscoWorks WLSE used as a central repository. Firmware updates can be run using either HTTP or SNMP protocols. Optionally, the CiscoWorks WLSE can update remote sites directly or optionally work with a TFTP server.

Cisco Aironet Conversion Tool for Cisco IOS Software

Cisco Aironet 1200 Series access points running the VxWorks operating system may be upgraded in mass to Cisco IOS Software. As part of the process, previous VxWorks configuration file formats are translated to Cisco IOS Software format.

Auto Discovery

The CiscoWorks WLSE automatically discovers Cisco Aironet access points, bridges and switches connected to the access points using Cisco Discovery Protocol (CDP). Discovery may be scheduled or run on demand. If desired, discovery may be limited by subnet and IP address range. If CDP is disabled, a list of IP addresses and credentials can be imported from a file or from CiscoWorks Resource Manager Essentials (RME). RME synchronization can be automatic. The CiscoWorks WLSE collects statistics and management information for each Cisco access point and bridge in its inventory. The CiscoWorks WLSE itself is also a manageable Cisco device with Cisco Discovery Protocol implementation and supports Cisco MIB-II.



Wireless LAN Solution Engine Fault and Performance Monitoring

- Performance monitoring of Cisco Access Points, bridges and 802.1x EAP servers
- Support for user defined thresholds
  - Monitors both ethernet and radio ports
  - Ex: Client associations, utilization, errors and availability
- Monitors switches directly attached to APs
  - CPU utilization, Memory Utilization, availability and port status
- Polling can be customized per location/site to reduce the traffic on WAN links
- Notifications based on priority level
  - E-mail, syslog and SNMP trap notifications
  - Centralized fault display
- Faults can be forwarded to EMS as SNMP traps or SYSLOG

AWLF v3.1—10-10

Fault Status

The CiscoWorks WLSE provides a centralized, tree view of all access points and user groups. Color coding indicates fault status and group icons reflect the most severe state of its members. Faults may be filtered and sorted by priority to facilitate viewing and acting upon problems.

Fault Notification

Fault notification and forwarding is implemented via SYSLOG messages, SNMP traps and e-mail

The WLSE includes an innovative fault engine that generates faults based on customizable threshold formulas. The fault engine polls the APs and bridges at user configurable intervals and compares the data retrieved against the appropriate threshold formulas.

There are two types of thresholds. (BUILD) The first defines faults that tend to high priority and that network administrators will want to respond to rapidly—for example, RF port is up/down (BUILD).

Fault notifications get generated—can be forwarded to an EMS or as e-mail/e-pager alerts.

(BUILD) Network engineer can then respond, using the WLSE to correct the fault.

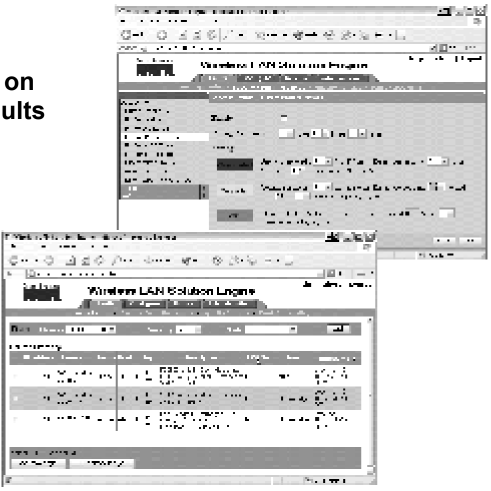
(BUILD) The other type of thresholds are performance related and define states for the managed entity—OK, Degraded, Overloaded. An example is RF Port Utilization. The network administrator configures the parameters that define “degraded” and “overloaded”. In the case of RF Port Utilization, the parameters are based on % utilization and number of polling cycles the condition exists. This monitoring is useful for proactive catastrophe prevention, but also is useful for capacity planning.

If an AP becomes degraded, this may signal that problems are imminent and the network engineer can take proactive action.

If an AP is consistently degraded and/or overloaded, it may also indicate the need for network deployment modification. For example, the network administrator may then determine to deploy more APs, shrink cell sizes, etc. (BUILD)

WLSE: Performance and Fault Monitoring of APs and Bridges

Cisco.com



Customizable thresholds based on SNMP polling can generate faults

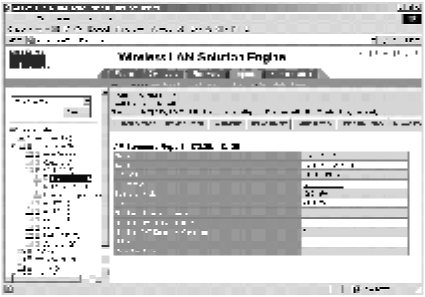
- o SNMP Reachability
- o RF Port Status
- o RF Port Utilization
- o RF Port Packet Errors
- o RF Port WEP Errors
- o RF Port FCS Errors
- o Associated Clients
- o Association Rate
- o Ethernet Port Status
- o Ethernet Port Utilization
- o Ethernet Port Packet Error

AWLF v3.1—10-11

Wireless LAN Solution Engine Device Center with Status

Cisco.com

- Displays status of APs
- Group status reflects the most severe state of its members
- Search by Device name or IP address
- Launch AP and group reports
- View Fault, Config and firmware update status



AWLF v3.1—10-12

Wireless LAN Solution Engine Utilization Reports

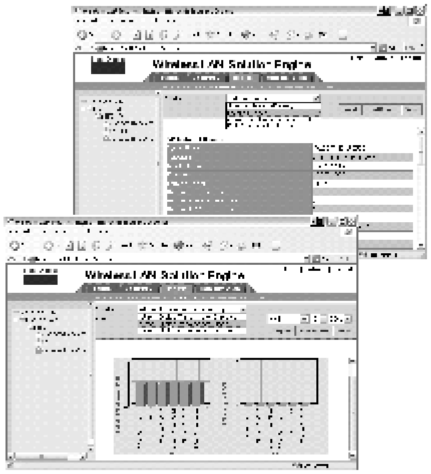
Cisco.com

AP/Bridge reports available for current & trending data:

- Group summary
- Group security
- Group performance: RF Utilization
- Group performance: Ethernet Utilization
- AP/Bridge summary
- AP/Bridge details
- Current Client associations
- EAP Authentication
- AP/Bridge RF transmission statistics
- AP/Bridge Ethernet transmission statistics
- AP/Bridge performance graph/tabular report

All reports exportable in CSV, PDF, XML

Indispensable for capacity planning



AWLF v3.1—10-13

Reporting, Trending & Planning

The CiscoWorks WLSE offers a variety of predefined reports for access points and bridges.

Available reports include summary reports based on criteria such as IP address, SSID, firmware version, and the number of clients, while detailed reports show information about such items as Ethernet & Radio port status, errors, encryption details. Other reports include ACS authentication reports (server, port, and the server priority), client association reports and utilization reports. All reports are available at both the group level and the individual access point or bridge level. Group utilization reports show bandwidth and client association for access points. These reports are useful for capacity planning by monitoring which access points consume the most bandwidth and have the greatest number of clients.

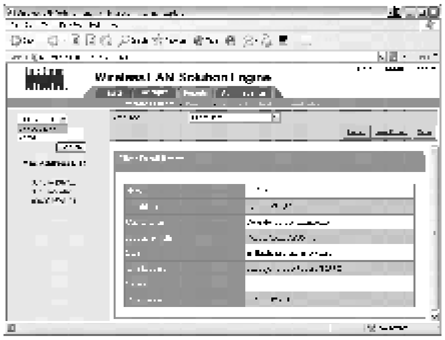
Since wireless clients can be anywhere, packet and error reports aid with trouble shooting. Both current and historical client association reports are accessible by client MAC address and by name, showing access point associations for a given client. Both client detail reports (MAC address, IP address, state, type, and associated access point) and client statistics reports (Errors, packets, signal strength and quality etc.) are provided.

Administrators can specify both aggregation and truncation frequencies for monitored data shown on reports.

All reports can be scheduled and delivered via e-mail. Reports may be exported in CSV/XML/PDF and SOAP/XML formats.

Wireless LAN Solution Engine Client Association Tracking Reports

Cisco.com



Client Reports per AP

- **Client Association Report (Current)**

Client Reports per Group

- **Number of associations (Historical)**

Client Reports per client:

- **Client Detail (Current)**
- **Client Statistics Report (Current)**
- **Client Association (Historical)**

AWLF v3.1—10-14

Discuss reports

Value-add:

- Accelerate client troubleshooting
- Capacity planning
- Resource utilization analysis

Current Client association report:

- client name, IP address, MAC, name of AP/bridge currently associated with, type of wireless device, state (authenticated/associated state)
- Note: association is assumed to be stable (I.e. flipping associations is taken as an error rather than association)

Group Historical Associations Report:

- AP Name (in the group), AP IP Address, Number of associations

Current Client Detail Report

- Name, IP Address, Classification, AP associated with, client authentication/association state, time last seen, software version, MAC address

Current Client Statistics Report

- Name, IP address, time last seen, packets transmitted, octets transmitted, last received signal strength, latest signal quality, sleep time in power save mode, preferred transmission rate, short retries, latest short retries, long retries, received WEP errors, errors in transmitted packets, errors in received packets, announcements sent

Client Association Report (Historical):

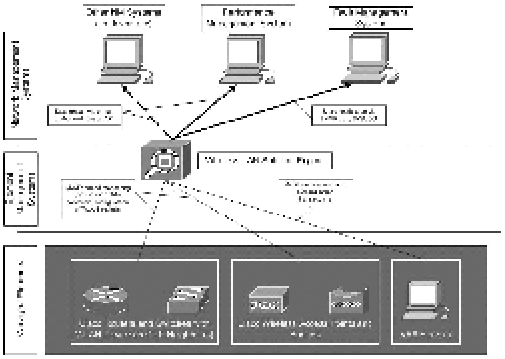
- Client type, AP associated with client IP address, software version, time

Future Enhancements:

- Integrated Cisco client firmware management
- Better client problem diagnosis:
  - Traps like authentication, de-authentication, auth. fail, disassociation, etc. We are making an effort to observe the sequence of some of these traps so we can pre-define some client faults (still under investigation)
  - Polled data (phase II): 802.11 specific values for forwarding tables on an AP/bridge track the state of the client. There are some of these states that won't send a trap so this helps give some advanced diagnosis of client association problems.
- Client Error Report:
  - Client name, IP address, MAC, current state and link to AP report
  - For last 10 errors:
  - Name of AP/bridge trying to associate with
  - Error start time
  - Duration of error
- Export to CiscoWorks User Tracking (under investigation)

Wireless LAN Solution Engine Network Management System/OSS Integration

Cisco.com



WLSE generates northbound SNMP traps/SYSLOG notifications

Allows customers to integrate powerful WLSE features with existing Event Management Systems

AWLF v3.1—10-15

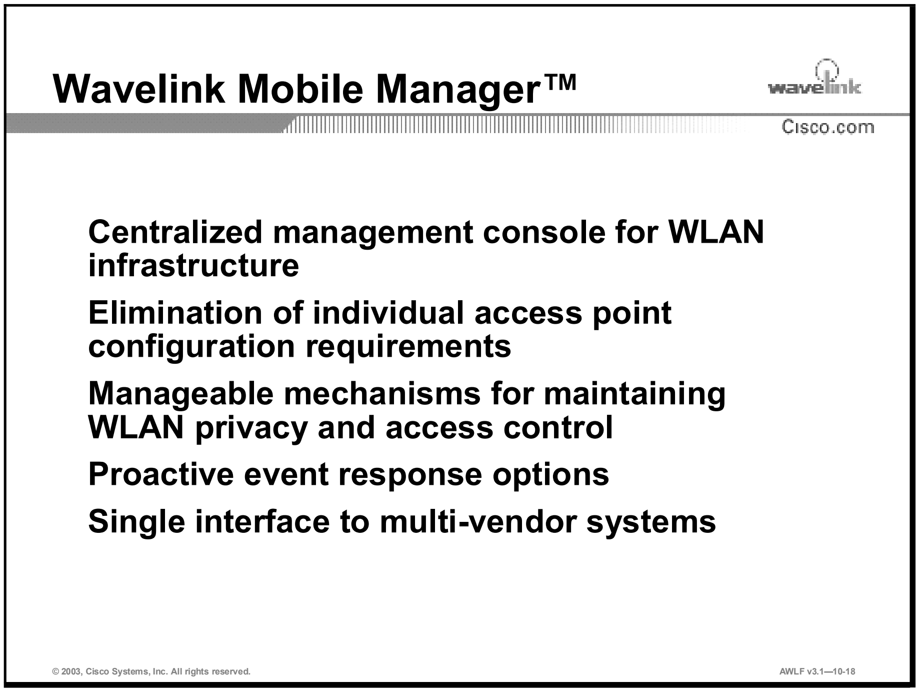
CiscoWorks WLSE Features and Benefits

Cisco.com

- **Centralized configuration and firmware management** ⇨ Reduces Wireless LAN TCO by **saving time and resources** required to manage large numbers of APs
- **Auto Configuration of new APs** ⇨ **Simplifies** large scale deployments
- **Security policy misconfiguration alerts** ⇨ **Minimizes** security vulnerabilities
- **AP utilization and client association reports** ⇨ **Helps** in Capacity Planning and Troubleshooting
- **Proactive monitoring of AP/Bridges and 802.1x EAP servers** ⇨ **Improves** wireless LAN uptime

AWLF v3.1—10-16

Wavelink Mobile Manager



Wavelink Mobile Manager™

wavelink
Cisco.com

Centralized management console for WLAN infrastructure

Elimination of individual access point configuration requirements

Manageable mechanisms for maintaining WLAN privacy and access control

Proactive event response options

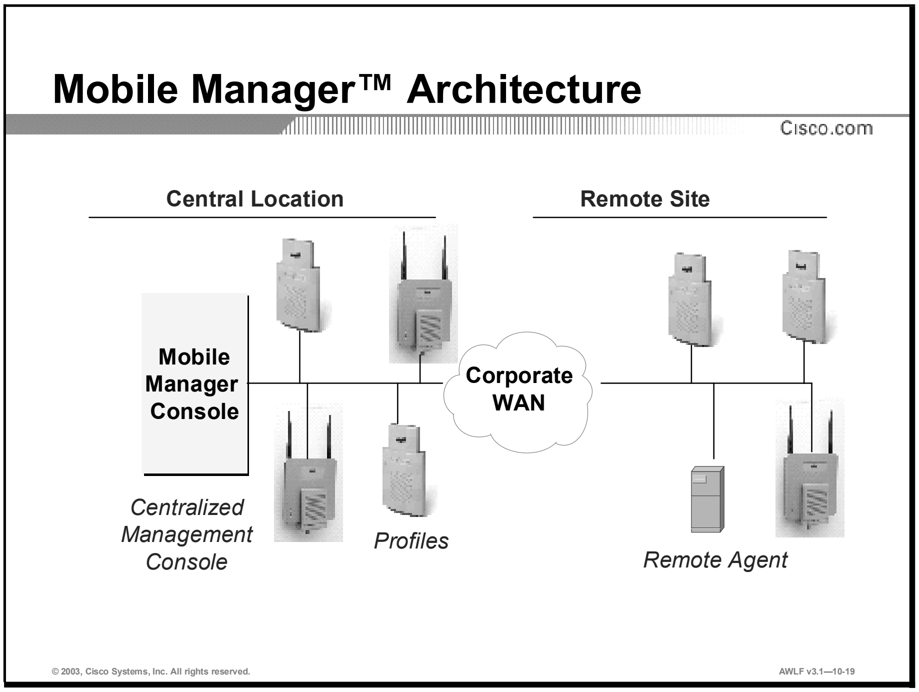
Single interface to multi-vendor systems

AWLF v3.1—10-18

Mobile Manager should be positioned as a WLAN management system for the multiple vendor environments. Mobile Manager helps to eliminate the challenges around configuring a large number of Access Points by using visual tracking of wireless assets down to the mobile client and the ongoing monitoring and updating and maintenance of the WLAN and mobile devices.

Multi-vendor enterprise-wide wireless LAN management eliminates the challenges around:

- Initial configuration costs of large numbers of wireless access points
- Implementing and maintaining wireless LAN security measures
- Wireless asset visibility and monitoring
- On-going attention to updates and maintenance



Mobile Manager™ Architecture

Cisco.com

Central Location

Remote Site

Mobile Manager Console

Corporate WAN

Centralized Management Console

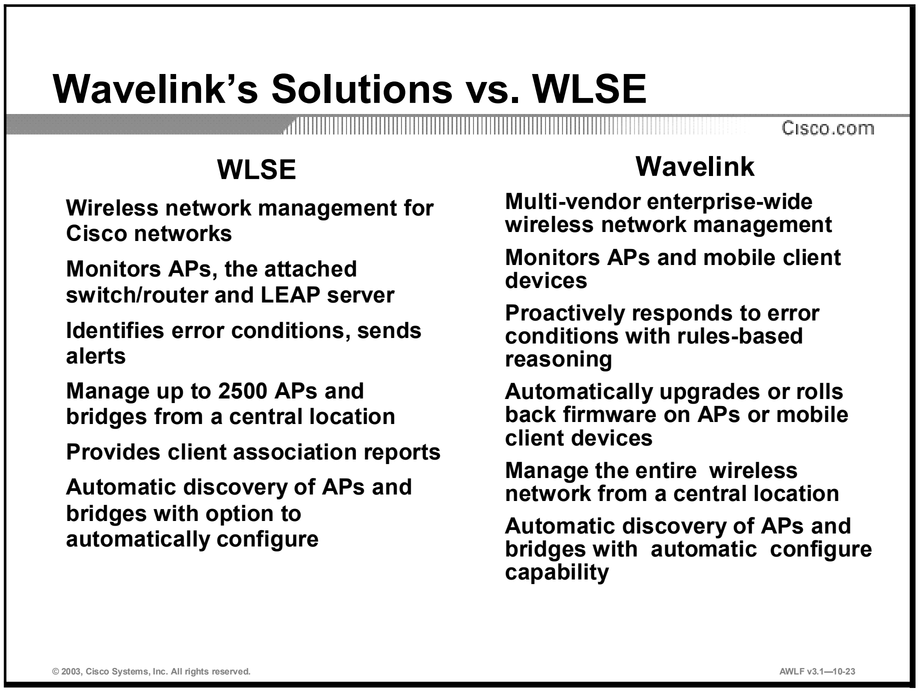
Profiles

Remote Agent

AWLF v3.1—10-19

Mobile Manager is the Wavelink product used to deploy and manage WLAN access Points. In a Cisco environment Mobile Manager takes advantage of the Cisco Discovery Protocol (CDP) broadcast that Cisco Aironet Access Points transmit as soon as they come online. By picking up these broadcast a Mobile Manager Agent will auto discover the Access Point and assign predefined configurations. Many Cisco Aironet Access Points are installed in a Cisco switched environments. Mobile Manager is designed to detect Access Points and Cisco Switches and Routers creating a topographical map of the entire network including Switches, Routers, Access Points and a table of the MAC addresses of the mobile clients attached to each access point.

Mobile Manager is a software solution, both on the Mobile Manager Console and Agent will run on any Windows machine. Profiles contain access point configuration parameters and can be automatically assigned as new access points are brought online. Mobile Manager Profiles will ease the deployment of new access points.



Wavelink's Solutions vs. WLSE

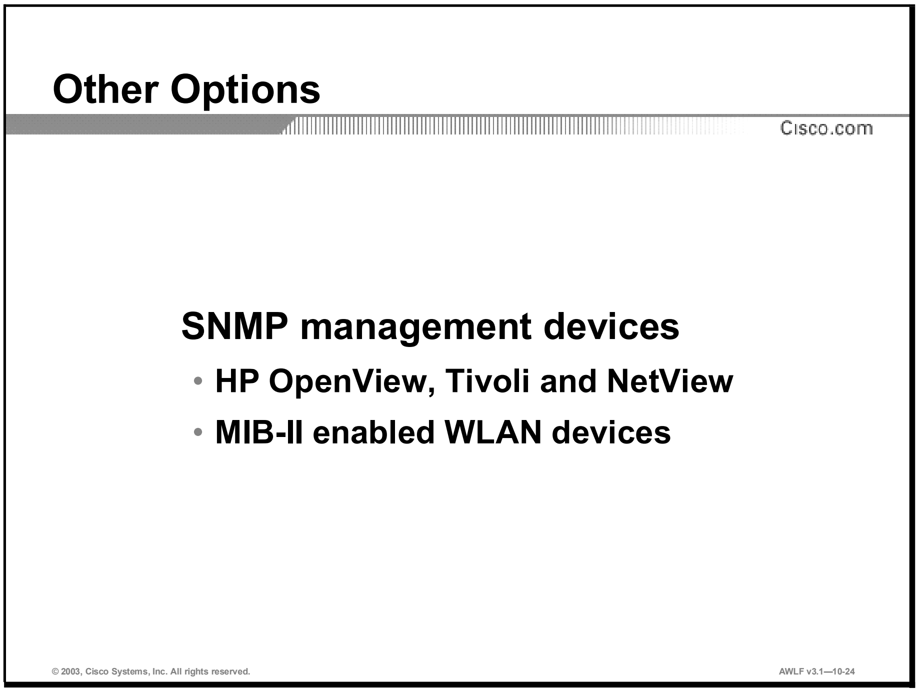
WLSE

- Wireless network management for Cisco networks
- Monitors APs, the attached switch/router and LEAP server
- Identifies error conditions, sends alerts
- Manage up to 2500 APs and bridges from a central location
- Provides client association reports
- Automatic discovery of APs and bridges with option to automatically configure

Wavelink

- Multi-vendor enterprise-wide wireless network management
- Monitors APs and mobile client devices
- Proactively responds to error conditions with rules-based reasoning
- Automatically upgrades or rolls back firmware on APs or mobile client devices
- Manage the entire wireless network from a central location
- Automatic discovery of APs and bridges with automatic configure capability

Wavelink solution is targeted at multiple vendor WLAN installations. Wireless LAN Solution Engine (WLSE) is for a Cisco environment only. Wavelink solution extends the management of software, firmware and drivers to the mobile devices. Wireless LAN Solution Engine (WLSE) manages only the Access Points, LEAP Server and the attached Switch(s) or Router(s). Wavelink solution proactively responds to error conditions. Wireless LAN Solution Engine (WLSE) identifies error conditions and sends alerts. Wavelink has the capability of doing customization of their solution to meet corporate enterprise customization request.



Other Options

Cisco.com

SNMP management devices

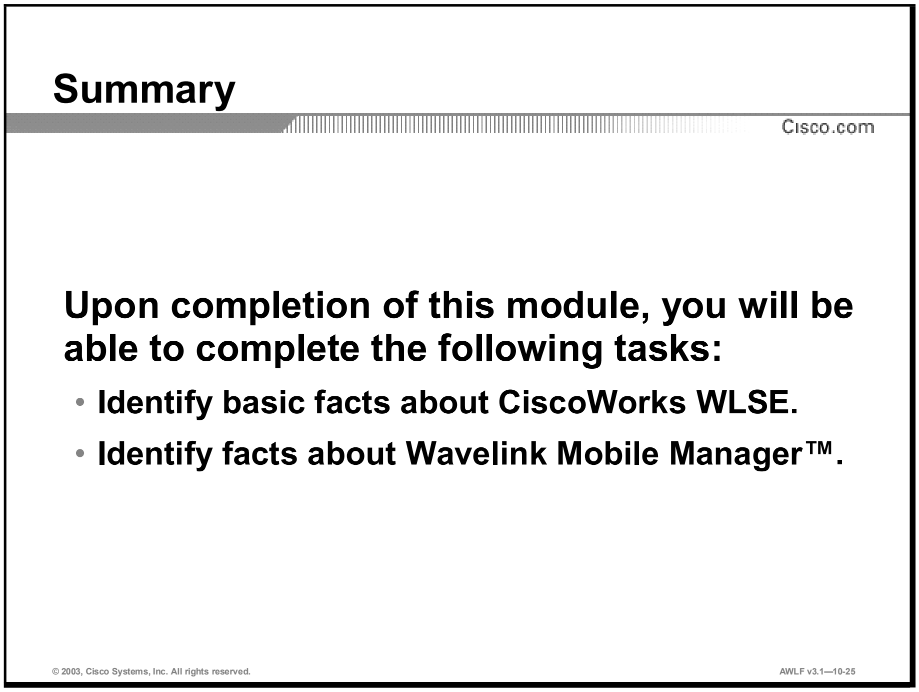
- **HP OpenView, Tivoli and NetView**
- **MIB-II enabled WLAN devices**

© 2003, Cisco Systems, Inc. All rights reserved. AWLF v3.1—10-24

The WLSE does not exist in a management vacuum. All faults generated by the WLSE can be forwarded to a centralized event management system like Tivoli NetView or HP OpenView as a northbound SNMP trap or SYSLOG notification. This allows customers to leverage the powerful fault and performance monitoring feature of the WLSE with powerful applications intelligent event correlation tools.

Summary

This section summarizes the concepts you learned in this module.



Summary

Cisco.com

Upon completion of this module, you will be able to complete the following tasks:

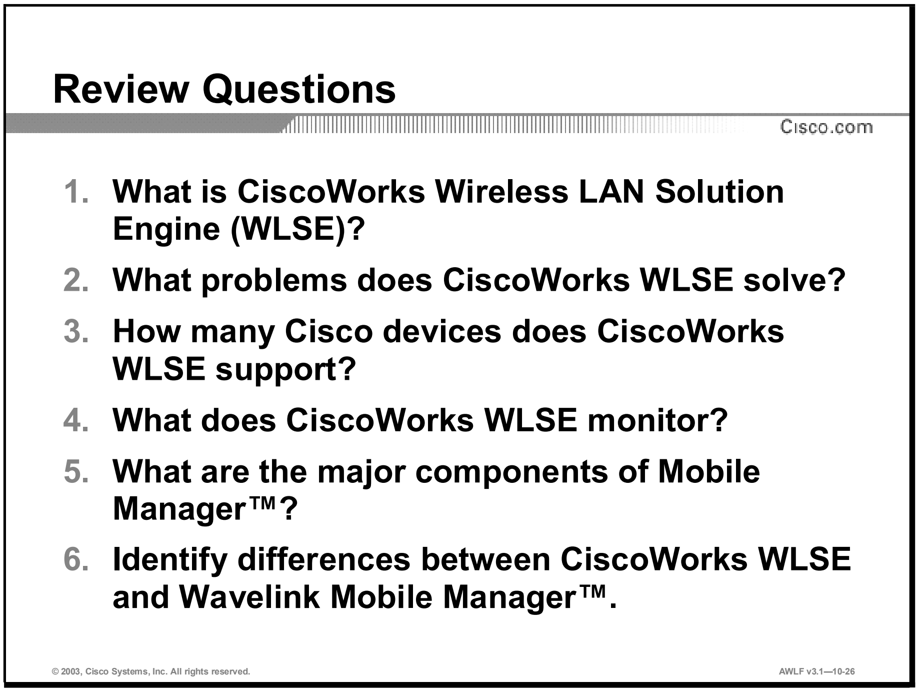
- **Identify basic facts about CiscoWorks WLSE.**
- **Identify facts about Wavelink Mobile Manager™.**

© 2003, Cisco Systems, Inc. All rights reserved. AWLF v3.1—10-25

Upon completion of this module, you will be able to complete the following tasks:

- Identify basic facts about CiscoWorks WLSE.
- Identify facts about Wavelink Mobile Manager.

Review Questions



Review Questions

Cisco.com

1. What is CiscoWorks Wireless LAN Solution Engine (WLSE)?
2. What problems does CiscoWorks WLSE solve?
3. How many Cisco devices does CiscoWorks WLSE support?
4. What does CiscoWorks WLSE monitor?
5. What are the major components of Mobile Manager™?
6. Identify differences between CiscoWorks WLSE and Wavelink Mobile Manager™.

AWLF v3.1—10-26

Answer these review questions.