

Building Cisco Multilayer Switched Networks

Volume 2

Version 3.0

Student Guide

EPGS Production Services: 07.27.06

**Corporate Headquarters**

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

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

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

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • 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



© 2006 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

DISCLAIMER WARRANTY: THIS CONTENT IS BEING PROVIDED "AS IS." CISCO MAKES AND YOU RECEIVE NO WARRANTIES IN CONNECTION WITH THE CONTENT PROVIDED HEREUNDER, EXPRESS, IMPLIED, STATUTORY OR IN ANY OTHER PROVISION OF THIS CONTENT OR COMMUNICATION BETWEEN CISCO AND YOU. CISCO SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. This learning product may contain early release content, and while Cisco believes it to be accurate, it falls subject to the disclaimer above.

Table of Contents

Volume 2

Implementing High Availability in a Campus Environment **5-1**

Overview	5-1
Module Objectives	5-1

Configuring Layer 3 Redundancy with HSRP **5-3**

Overview	5-3
Objectives	5-3
Describing Routing Issues	5-4
Using Default Gateways	5-4
Using Proxy ARP	5-5
Identifying the Router Redundancy Process	5-6
Router Redundancy Providing Continual Access	5-7
Describing HSRP	5-8
Identifying HSRP Operations	5-9
Virtual Router	5-9
Active Router	5-9
ARP Resolution with HSRP	5-10
Standby and Other HSRP Routers in the Group	5-11
HSRP Active and Standby Router Interaction	5-12
Describing HSRP States	5-13
HSRP State Transition	5-14
Standby State	5-16
Active State	5-17
Describing HSRP Configuration Commands	5-18
Enabling HSRP	5-19
Verifying HSRP Configuration	5-20
Verify All HSRP Operations	5-21
Summary	5-22

Optimizing HSRP **5-23**

Overview	5-23
Objectives	5-23
Describing HSRP Optimization Options	5-24
Establishing HSRP Priorities	5-25
Verify the HSRP Standby Priority	5-26
HSRP Standby Preempt	5-27
Hello Message Timers	5-29
HSRP Interface Tracking	5-31
Configuring HSRP Tracking	5-33
Tuning HSRP Operations	5-34
Subsecond Failover	5-34
Preempt Time Aligned with Router Boot Time	5-35
Describing Load Sharing	5-36
Example of Multiple HSRP Groups on the Same Segment	5-37
Addressing HSRP Groups Across Trunk Links	5-38
Example of Load Sharing Across Different IP Subnets	5-39
Describing HSRP Debug Commands	5-40
Debugging HSRP Operations	5-41
Example: HSRP Debugging with Two Active Routers	5-43
Example: HSRP Debugging on Negotiation for Role of Active Router	5-43
Example: HSRP Debugging on First and Only Router on Subnet	5-45
Example: Nonpreempt Configured Router Coming Up with HSRP	5-46
Example: HSRP on Preempt-Configured Router Coming Up	5-47
Summary	5-48

Configuring Layer 3 Redundancy with VRRP and GLBP **5-49**

Overview	5-49
Objectives	5-49
Describing VRRP	5-50
Identifying the VRRP Operations Process	5-52
VRRP Transition Process	5-53
Configuring VRRP	5-55
Describing the GLBP	5-57
GLBP Functions	5-58
Identifying the GLBP Operations Process	5-59
GLBP Implementation	5-64
Summary	5-66
Module Summary	5-67
References	5-67
Module Self-Check	5-68
Module Self-Check Answer Key	5-69

Wireless LANs **6-1**

Overview	6-1
Module Objectives	6-1

Introducing WLANs **6-3**

Overview	6-3
Objectives	6-3
Wireless Data Technologies	6-4
Wireless Technologies	6-5
Wireless LANs	6-6
Wireless LAN Evolution	6-7
WLANs and Other Wireless Technologies	6-8
WLANs and LANs	6-9
Similarities Between WLANs and LANs	6-9
Differences Between WLANs and LANs	6-10
Summary	6-11

Describing WLAN Topologies **6-13**

Overview	6-13
Objectives	6-13
WLAN Topologies	6-14
Wired and Wireless LAN	6-15
Service Set Identifier	6-16
Typical WLAN Topologies	6-17
Wireless Repeater Topology	6-19
Work Group Bridge Topology	6-20
Peer-to-Peer Topology	6-21
WLAN Service Set and Modes	6-22
Roaming Through Wireless Cells	6-23
Client Roaming	6-24
Layer 2 and Layer 3 Roaming	6-25
Wireless VLAN Support	6-26
Enterprise Voice Architecture	6-28
Wireless Mesh Networking	6-29
Wireless Mesh Applications	6-30
AWP Protocol	6-31
Key Market Segments for Outdoor Wireless Technology	6-32
Summary	6-33

Explaining WLAN Technology and Standards**6-35**

Overview	6-35
Objectives	6-35
Unlicensed Frequency Bands	6-36
Radio Frequency Transmission	6-37
Data Transmission over Radio Waves	6-38
WLAN Regulation and Standardization	6-39
IEEE 802.11b Standard	6-40
2.4-GHz Channels	6-41
2.4-GHz Channel Use	6-42
802.11b/g (2.4-GHz) Channel Reuse	6-43
802.11b Access Point Coverage	6-44
IEEE 802.11a Standard	6-45
5-GHz Channels with 802.11h	6-46
802.11a Channel Reuse	6-48
IEEE 802.11g Standard	6-49
802.11g Protection Mechanism	6-50
802.11 Comparison	6-52
2.4 GHz (802.11b)	6-52
2.4 GHz (802.11g)	6-52
5 GHz (802.11a)	6-53
802.11 Standards Comparison	6-54
Range Comparisons	6-55
Ratified 802.11 Standards	6-56
Worldwide Availability	6-57
General Office WLAN Design	6-58
WLAN Best Practices	6-59
WLAN Security	6-60
WLAN Security Threats	6-61
Mitigating the Threats	6-62
Evolution of WLAN Security	6-63
Wireless Client Association	6-64
WPA and WPA2 Authentication	6-65
WPA and WPA2 Encryption	6-66
WLAN Security Summary	6-67
WLAN Security Evaluation	6-68
Summary	6-69

Configuring Cisco WLAN Clients**6-71**

Overview	6-71
Objectives	6-71
Cisco 802.11a/b/g WLAN Client Adapters	6-72
Cisco Aironet Client Adapter Installation	6-73
Cisco Aironet Desktop Utility Installation	6-74
Cisco Site Survey Utility Installation	6-75
Choose Configuration Tool	6-76
Cisco ADU Main Screen	6-77
ADU: Advanced Status Information	6-78
ADU: Main Profile Screen	6-79
ADU: General Settings	6-80
ADU: Security Settings	6-81
ADU: Advanced Profile Settings	6-82
ADU Diagnostics: Advanced Statistics	6-83
ADU Diagnostics: Adapter Information	6-84
ADU Troubleshooting	6-85
Cisco Aironet System Tray Icon	6-86
Cisco Aironet Site Survey Utility: Associated AP Status	6-87
Cisco Aironet Site Survey Utility: AP Scan List	6-89
Windows XP WLAN Configuration	6-91
Comparison of Windows XP and Cisco ADU	6-92

Cisco Aironet Client Administration Utility	6-93
Cisco Wireless IP Phone	6-95
Cisco Compatible Extensions Program for WLAN Client Devices	6-96
Cisco Compatible Extensions: Features and Benefits	6-97
Cisco Compatible Extensions: Versions	6-99
Cisco Compatible Extensions Program	6-100
Summary	6-101

Implementing WLANs **6-103**

Overview	6-103
Objectives	6-103
Cisco WLAN Implementation	6-104
Autonomous WLAN Solution	6-105
Lightweight WLAN Solution Components	6-106
Lightweight WLAN Solution	6-107
Lightweight Access Point Protocol	6-108
Layer 2 and Layer 3 Mode of LWAPP	6-109
Association of Access Point to WLAN Controller	6-110
Cisco Aironet WLAN Controllers	6-111
Comparison of the WLAN Solutions	6-112
Describing WLAN Components	6-113
Cisco Unified Wireless Network	6-114
Cisco Unified Wireless Network Components	6-116
Cisco Aironet Access Points and Bridges	6-118
Power over Ethernet	6-119
PoE Delivery	6-120
Midspan Power Injection	6-121
Power-Sourcing Equipment	6-122
Investment Protection	6-123
PoE Configuration	6-124
Explaining WLAN Antennas	6-126
Omnidirectional Isotropic Antennas	6-127
Omnidirectional Dipole Antennas	6-128
Directional Antennas	6-129
Connectorized 5-GHz Antennas	6-130
Cisco Access Point and Bridge Antennas	6-131
Multipath Distortion	6-132
Definition of Decibel	6-134
Effective Isotropic Radiated Power	6-135
Antenna Cable Loss	6-136
2.4-GHz EIRP Rules for FCC-Governed Countries	6-137
2.4-GHz EIRP Rules for ETSI-Governed Countries	6-138
EIRP Rules Summary	6-139
Summary	6-140

Configuring WLANs **6-141**

Overview	6-141
Objectives	6-141
Autonomous Access Point Configuration	6-142
Autonomous Access Point IP Address	6-143
Role of Autonomous Access Points in a Radio Network	6-144
Autonomous Access Point Configuration via the Web Browser	6-145
Autonomous Access Point Express Setup	6-146
Lightweight WLAN Controller Configuration	6-147
Lightweight WLAN Controller Interfaces	6-148
Cisco WLC Boot Menu	6-149
CLI Wizard Configuration Tool	6-150
WLAN Controller CLI Commands	6-152
Web Wizard Initial Configuration	6-153
WLAN Controller Web Configuration	6-154

WLAN Controller Web Menu Bar	6-155
Summary	6-164
Module Summary	6-165
References	6-165
Module Self-Check	6-166
Module Self-Check Answer Key	6-169
<u>Configuring Campus Switches to Support Voice</u>	7-1
Overview	7-1
Module Objectives	7-1
<u>Planning for Implementation of Voice in a Campus Network</u>	7-3
Overview	7-3
Objectives	7-3
Explaining Converged Network Benefits	7-4
Describing VoIP Network Components	7-6
Explaining Traffic Characteristics of Voice and Data	7-7
Describing VoIP Call Flow	7-9
Explaining Auxiliary VLANs	7-11
Describing QoS	7-12
Explaining the Importance of High Availability for VoIP	7-14
Example: Cisco Reliability and Availability	7-15
Explaining Power Requirements in Support of VoIP	7-16
Summary	7-17
<u>Accommodating Voice Traffic on Campus Switches</u>	7-19
Overview	7-19
Objectives	7-19
QoS and Voice Traffic in the Campus Model	7-20
LAN-Based Classification and Marking	7-21
Layer 2 QoS Marking	7-22
Layer 3 QoS Marking	7-23
Describing QoS Trust Boundaries	7-24
Configuring a Switch for Attachment of a Cisco IP Phone	7-25
Describing Basic Switch Commands to Support Attachment of a Cisco IP Phone	7-26
Example	7-27
What Is Cisco AutoQoS VoIP?	7-28
Configuring Cisco AutoQoS VoIP on a Cisco Catalyst Switch	7-30
Example: Using the Port-Specific Cisco AutoQoS Macro	7-34
Automation with Cisco AutoQoS	7-37
Summary	7-38
Module Summary	7-39
References	7-40
Module Self-Check	7-41
Module Self-Check Answer Key	7-43
<u>Minimizing Service Loss and Data Theft in a Campus Network</u>	8-1
Overview	8-1
Objectives	8-1
<u>Understanding Switch Security Issues</u>	8-3
Overview	8-3
Objectives	8-3
Overview of Switch Security Concerns	8-4
Describing Unauthorized Access by Rogue Devices	8-5
Switch Attack Categories	8-6
Describing a MAC Flooding Attack	8-8
Suggested Mitigation for MAC Flooding Attacks	8-9
Describing Port Security	8-10
Configuring Port Security on a Switch	8-12

Caveats to Port Security Configuration Steps	8-13
How to Verify Port Security	8-14
Verifying Network Access Security	8-14
Example: show port-security Command Output	8-15
Example: show port-security Command for a Specific Interface	8-16
Port Security with Sticky MAC Addresses	8-17
Authentication, Authorization, and Accounting	8-18
Authentication and Authorization Methods	8-19
802.1x Port-Based Authentication	8-20
Configuring 802.1x Port-Based Authentication	8-22
Example	8-23
Summary	8-24

Protecting Against VLAN Attacks **8-25**

Overview	8-25
Objectives	8-25
Explaining VLAN Hopping	8-26
Switch Spoofing	8-27
Double Tagging	8-28
Mitigating VLAN Hopping	8-29
VLAN Access Control Lists	8-30
Configuring VACLs	8-31
Explaining PVLANS	8-33
PVLAN Port Types	8-34
Configuring PVLANS	8-36
Example: PVLAN Configurations	8-37
Example: Configuring PVLAN Ports	8-39
Example: Permitting Routing of Secondary VLAN Ingress Traffic	8-40
Summary	8-41

Protecting Against Spoof Attacks **8-43**

Overview	8-43
Objectives	8-43
Describing a DHCP Spoof Attack	8-44
Describing DHCP Snooping	8-45
Configuring DHCP Snooping	8-46
Verifying the DHCP Snooping Configuration	8-47
IP Source Guard	8-48
Configuring IP Source Guard on the Switch	8-49
Describing ARP Spoofing	8-51
Describing DAI	8-53
Describing Commands to Configure DAI	8-55
Example: DAI Implementation	8-56
Protecting Against ARP Spoofing Attacks	8-57
Summary	8-58

Describing STP Security Mechanisms **8-59**

Overview	8-59
Objectives	8-59
Protecting the Operation of STP	8-60
BPDU Guard	8-60
BPDU Filtering	8-60
BPDU Root Guard	8-60
Describing BPDU Guard Configuration	8-61
BPDU Filtering Applied Globally Versus Per-Port	8-61
Configuring BPDU Guard	8-62
Verifying BPDU Guard	8-62
Describing BPDU Filtering Configuration	8-63
BPDU Filtering Applied Globally Versus Per-Port	8-63
Configuring BPDU Filtering	8-64

Describing Root Guard	8-66
Example: Using Root Guard	8-66
Describing Root Guard Configuration Commands	8-68
Summary	8-70
<i>Preventing STP Forwarding Loops</i>	8-71
Overview	8-71
Objectives	8-71
Describing UDLD	8-72
Describing Loop Guard	8-74
Example: Before Loop Guard	8-75
Example: With Loop Guard	8-76
Configuring UDLD and Loop Guard	8-77
Configuring UDLD	8-78
Verifying and Resetting UDLD	8-79
Example: Displaying the UDLD State	8-80
Configuring Loop Guard	8-81
Preventing STP Failures Caused by Unidirectional Links	8-83
Summary	8-84
<i>Securing Network Switches</i>	8-85
Overview	8-85
Objectives	8-85
Describing Vulnerabilities in the CDP	8-86
Describing Vulnerabilities in the Telnet Protocol	8-87
Describing Vulnerabilities in the SSH	8-88
Describing vty ACLs	8-89
Describing Commands to Apply ACLs to vty	8-90
Example: vty Access	8-90
Best Practices: Switch Security Considerations	8-91
Organizational Security Policies	8-92
Secure Switch Devices	8-92
Secure Switch Protocols	8-94
Mitigating Compromises Launched Through a Switch	8-95
Summary	8-96
Module Summary	8-97
References	8-98
Module Self-Check	8-99
Module Self-Check Answer Key	8-100

Implementing High Availability in a Campus Environment

Overview

A network with high availability provides alternative means by which all infrastructure paths and key servers can be accessed at all times. The Hot Standby Router Protocol (HSRP) is one of those software features that can be configured to provide Layer 3 redundancy to network hosts. HSRP optimization provides immediate or link-specific failover as well as a recovery mechanism. Virtual Router Redundancy Protocol (VRRP) and Gateway Load Balancing Protocol (GLBP) are derivatives of HSRP, providing additional Layer 3 redundancy features such as load balancing.

Module Objectives

Upon completing this module, you will be able to implement high availability technologies and techniques using multilayer switches in a campus environment. This ability includes being able to meet these objectives:

- Explain the procedure to enable and tune HSRP so that extended pings show that HSRP is working correctly
- Describe how to identify technologies and best practices required to increase network availability and verify its function in a multilayer switch
- Describe and configure gateway redundancy protocols (VRRP and GLBP)

Configuring Layer 3 Redundancy with HSRP

Overview

Businesses and consumers that rely on intranet and Internet services for their mission-critical communications require and expect their networks and applications to be continuously available to them. Customers can satisfy their demands for near-100 percent network uptime if they leverage the Hot Standby Router Protocol (HSRP) in Cisco IOS software. HSRP provides network redundancy for IP networks in a manner that ensures that user traffic immediately and transparently recovers from first-hop failures in network edge devices or access circuits. However, routing issues exist with various means of providing redundancy for the default gateway of each segment. Because of this, HSRP has very specific attributes that warrant further description, as does a delineation of HSRP operations on the network. HSRP interfaces transition through a series of states as they find their role in the capacity of active or standby HSRP router.

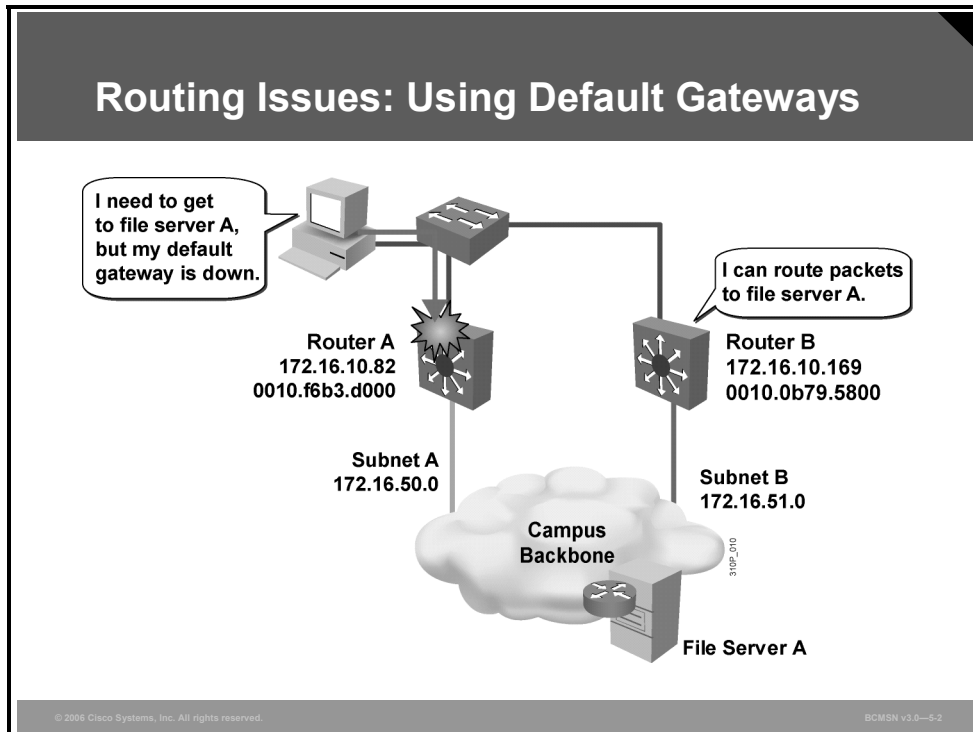
Objectives

Upon completing this lesson, you will be able to explain the procedure to enable and tune HSRP so that extended pings show that HSRP is working correctly. This ability includes being able to meet these objectives:

- Describe routing issues that occur when using default gateways and proxy ARP
- Describe how router device redundancy works
- Describe HSRP
- Describe how HSRP operates to provide a nonstop path redundancy for IP
- Describe the six HSRP states and their functions
- Describe the commands used to configure HSRP
- Explain the procedure to enable HSRP

Describing Routing Issues

This topic describes routing issues that occur when using default gateways and proxy Address Resolution Protocol (ARP).



Using Default Gateways

When a default gateway is configured on most devices, there is no means by which to configure a secondary gateway, even if a second route exists to carry packets off the local segment.

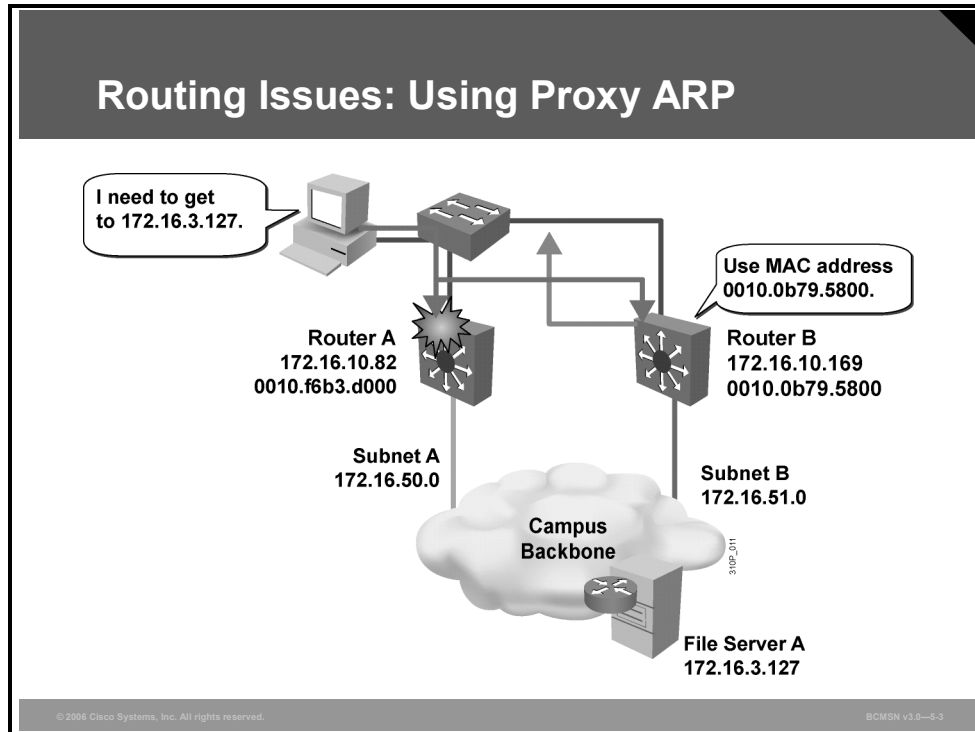
For example, primary and secondary paths between the Building Access submodule and the Building Distribution submodule provide continuous access in the event of a link failure at the Building Access layer. Primary and secondary paths between the Building Distribution layer and the Building Core layer provide continuous operations should a link fail at the Building Distribution layer.

In this example, router A is responsible for routing packets for subnet A, and router B is responsible for handling packets for subnet B. If router A becomes unavailable, routing protocols can quickly and dynamically converge and determine that router B will now transfer packets that would otherwise have gone through router A. Most workstations, servers, and printers, however, do not receive this dynamic routing information.

End devices are typically configured with a single default gateway IP address that does not change when network topology changes occur. If the router whose IP address is configured as the default gateway fails, the local device will be unable to send packets off the local network segment, effectively disconnecting it from the rest of the network. Even if a redundant router exists that could serve as a default gateway for that segment, there is no dynamic method by which these devices can determine the address of a new default gateway.

Using Proxy ARP

This subtopic describes proxy ARP.



Cisco IOS software runs proxy ARP to enable hosts that have no knowledge of routing options to obtain the MAC address of a gateway that is able to forward packets off the local subnet.

For example, if the proxy ARP router receives an ARP request for an IP address that it knows is not on the same interface as the request sender, it will generate an ARP reply packet giving its own local MAC address as the destination MAC address of the IP address that is being resolved. The host that sent the ARP request sends all packets that are destined for the resolved IP address to the MAC address of the router. The router then forwards the packets toward the intended host, perhaps repeating this process along the way. Proxy ARP is enabled by default.

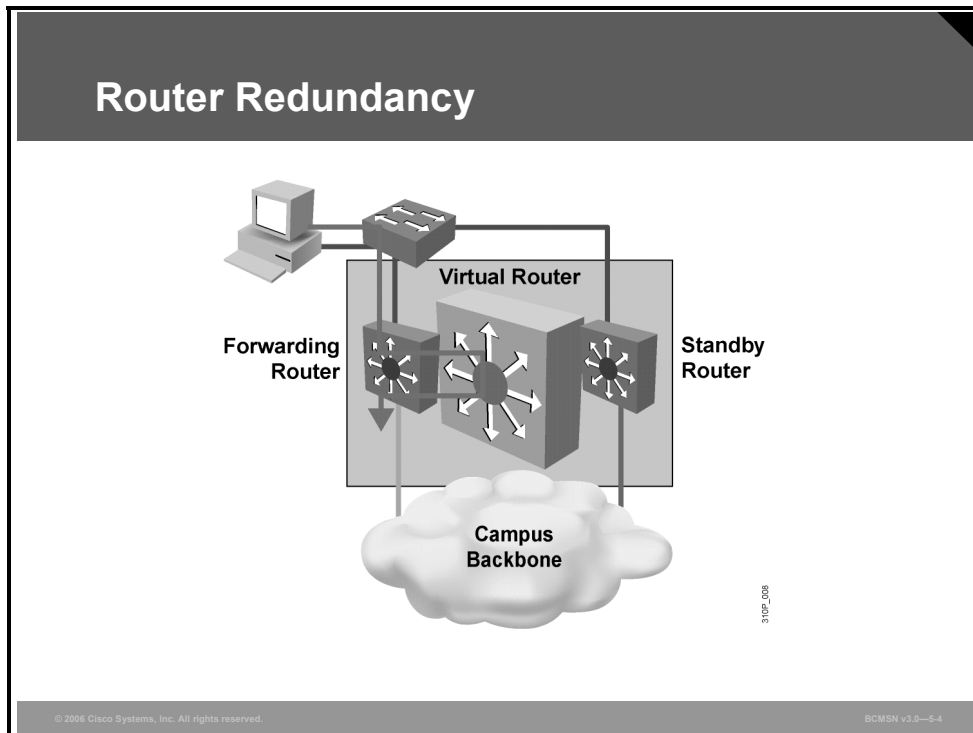
With proxy ARP, the end-user station behaves as if the destination device were connected to its own network segment. If the responsible router fails, the source end station continues to send packets for that IP destination to the MAC address of the failed router, and the packets are therefore discarded.

Eventually, the proxy ARP MAC address will age out of the workstation's ARP cache. The workstation may eventually acquire the address of another proxy ARP failover router, but the workstation cannot send packets off the local segment during this failover time.

For further information on proxy ARP, refer to RFC 1027, *Using ARP to Implement Transparent Subnet Gateways*.

Identifying the Router Redundancy Process

This topic describes how router device redundancy works.



With this type of router redundancy, a set of routers works in concert to present the illusion of a single virtual router to the hosts on the LAN. By sharing an IP address and a MAC (Layer 2) address, two or more routers can act as a single "virtual" router.

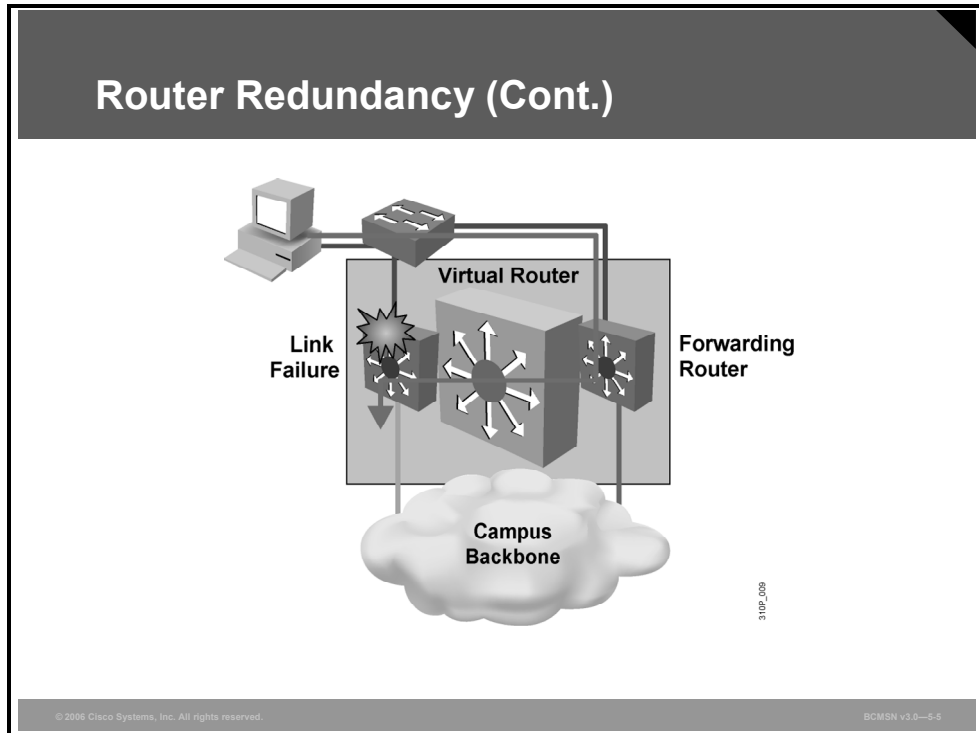
The IP address of the virtual router will be configured as the default gateway for the workstations on a specific IP segment. When frames are to be sent from the workstation to the default gateway, the workstation will use ARP to resolve the MAC address associated with the IP address of the default gateway. The ARP resolution will return the MAC address of the virtual router. Frames sent to the MAC address of the virtual router can then be physically processed by any active or standby router that is part of that virtual router group.

A protocol is used to identify two or more routers as the devices responsible for processing frames sent to the MAC or IP address of a single virtual router. Host devices send traffic to the address of the virtual router. The physical router that forwards this traffic is transparent to the end stations.

The redundancy protocol provides the mechanism for determining which router should take the active role in forwarding traffic and determining when that role must be taken over by a standby router. The transition from one forwarding router to another is transparent to the end devices.

Router Redundancy Providing Continual Access

This subtopic describes how router device redundancy provides continual access.



When the forwarding router or a link fails, this process occurs.

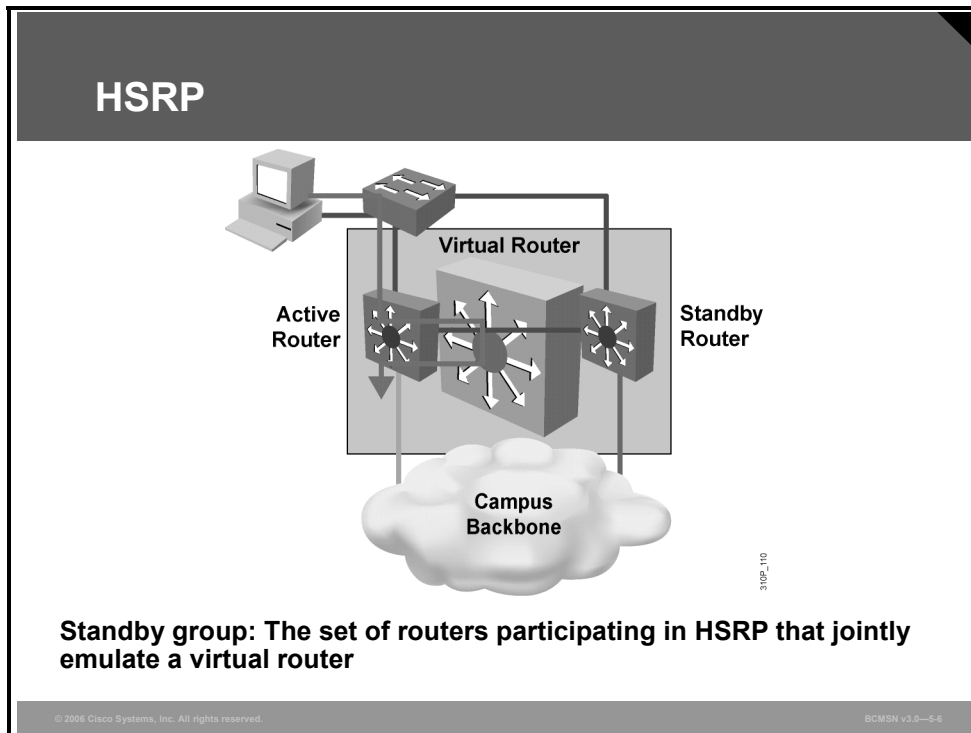
Router Redundancy Process

The table describes the steps that take place when a router fails.

Step	Description
1.	The standby router stops seeing hello messages from the forwarding router.
2.	The standby router then assumes the role of the forwarding router.
3.	Because the new forwarding router assumes both the IP and MAC address of the virtual router, the end stations see no disruption in service.

Describing HSRP

This topic describes HSRP.



HSRP defines a standby group of routers, with one router as the active one. HSRP provides gateway redundancy by sharing IP and MAC addresses between redundant gateways. The protocol consists of virtual MAC and IP addresses that are shared between two routers that belong to the same HSRP group.

HSRP Terminology

The table describes some of the terms used with HSRP.

Term	Definition
Active router	The router that is currently forwarding packets for the virtual router
Standby router	The primary backup router
Standby group	The set of routers participating in HSRP that jointly emulate a virtual router

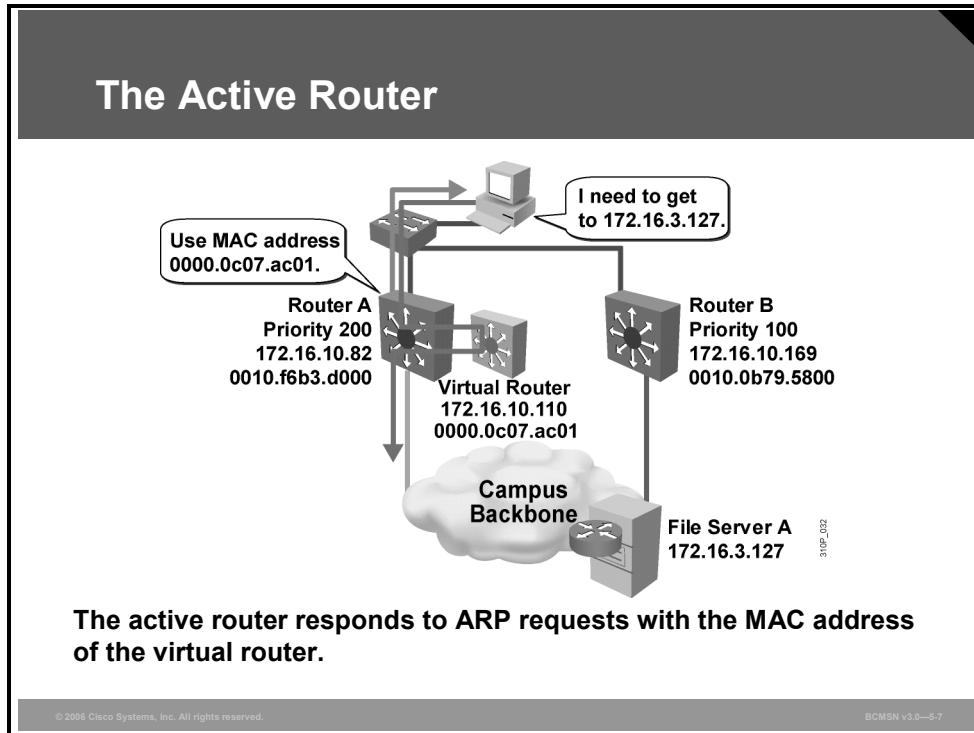
An HSRP group comprises these entities:

- One active router
- One standby router
- One virtual router
- Other routers

HSRP active and standby routers send hello messages to multicast address 224.0.0.2 User Datagram Protocol (UDP) port 1985.

Identifying HSRP Operations

This topic describes how HSRP operates to provide a nonstop path redundancy for IP.



All the routers in an HSRP group have specific roles and interact in specific manners.

Virtual Router

The virtual router is simply an IP and MAC address pair that end devices have configured as their default gateway. The active router will process all packets and frames sent to the virtual router address. The virtual router processes no physical frames.

Active Router

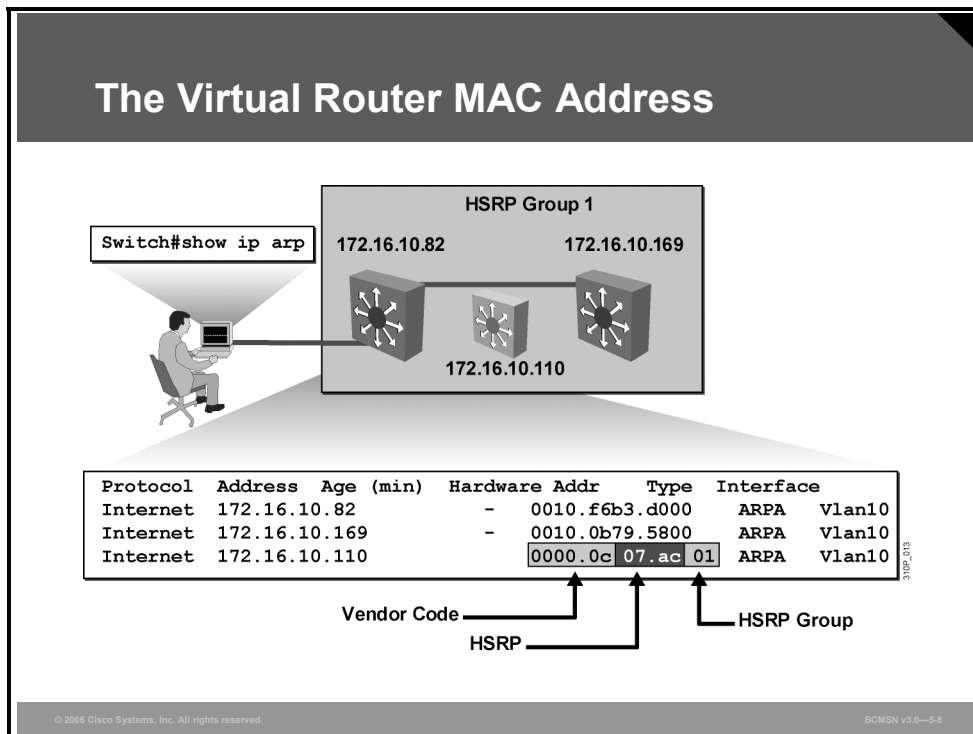
Within an HSRP group, one router is elected to be the active router. The active router physically forwards packets sent to the MAC address of the virtual router.

The active router responds to traffic for the virtual router. If an end station sends a packet to the virtual router MAC address, the active router receives and processes that packet. If an end station sends an ARP request with the virtual router IP address, the active router replies with the virtual router MAC address.

In this example, router A assumes the active role and forwards all frames addressed to the well-known MAC address of 0000.0c07.acxx, where xx is the HSRP group identifier.

ARP Resolution with HSRP

This subtopic describes ARP resolution with HSRP.



The IP address and corresponding MAC address of the virtual router are maintained in the ARP table of each router in an HSRP group. As shown in the figure, the command **show ip arp** displays the ARP cache on a multilayer switch.

Interpretation of show ip arp Output

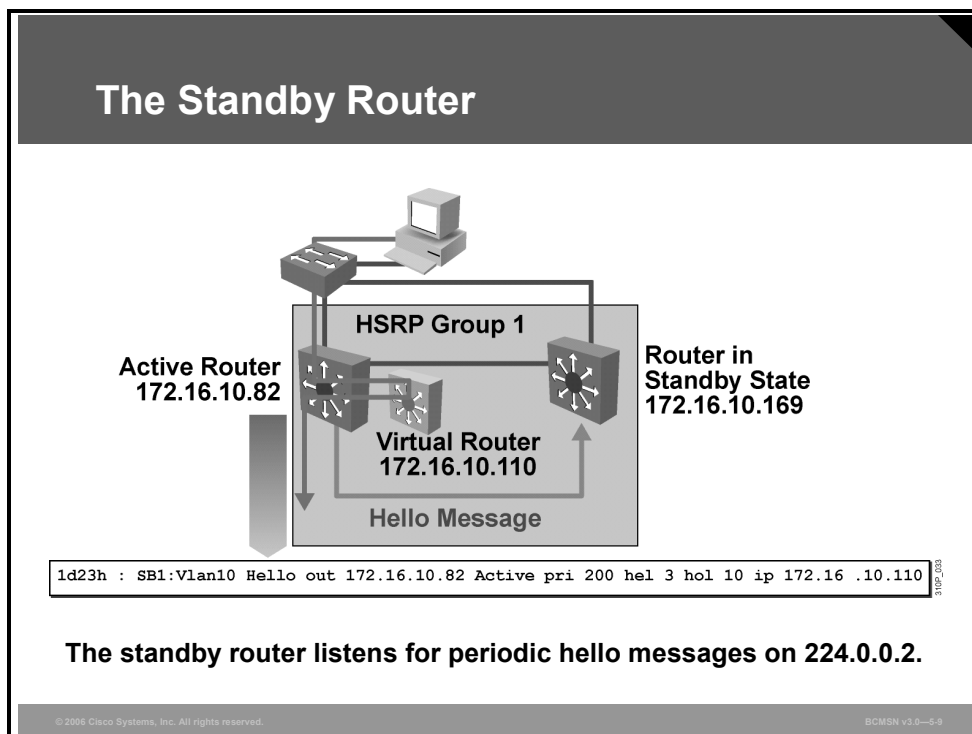
The table describes the command output for the **show ip arp** command.

Field	Definition
Protocol	Protocol for network address in the Address field
Address	The network address that corresponds to hardware address
Age (min)	Age, in minutes, of the cache entry
Hardware Addr	The MAC address that corresponds to network address
Type	Type of encapsulation
Interface	Interface to which this address mapping has been assigned

In the example, the output displays an ARP entry for a router that is a member of HSRP group 1 in VLAN10. The virtual router for VLAN10 is identified as 172.16.10.110. The well-known MAC address that corresponds to this IP address is 0000.0c07.ac01, where 01 is the HSRP group identifier for group 1. The HSRP group number is the standby group number (1) converted to hexadecimal (01).

Standby and Other HSRP Routers in the Group

This subtopic describes the HSRP standby and other router roles in an HSRP group.



The function of the HSRP standby router is to monitor the operational status of the HSRP group and quickly assume packet-forwarding responsibility if the active router becomes inoperable. Both the active and standby routers transmit hello messages to inform all other routers in the group of their role and status. The routers use multicast address 224.0.0.2 UDP port 1985 for these messages.

An HSRP group may contain other routers that are group members but are not in an active or standby state. These routers monitor the hello messages sent by the active and standby routers to ensure that an active and standby router exist for the HSRP group of which they are members. These routers do forward packets addressed to their own specific IP addresses, but they do not forward packets addressed to the virtual router. These routers issue speak messages at every hello interval time.

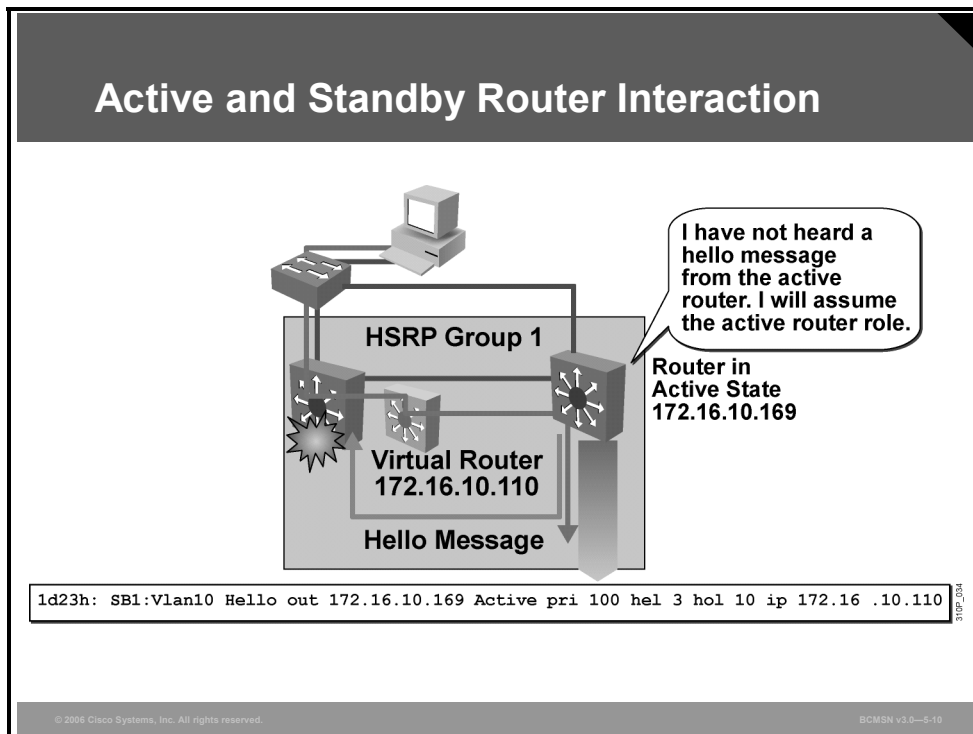
HSRP Terminology

The table describes some of the terms used with HSRP.

Term	Definition
Hello interval time	The interval between successive HSRP hello messages from a given router. Default = 3 seconds.
Hold interval time	The interval between the receipt of a hello message and the presumption that the sending router has failed. Default = 10 seconds.

HSRP Active and Standby Router Interaction

This subtopic describes the interaction between the active and standby routers.



When the active router fails, the other HSRP routers stop seeing hello messages from the active router. The standby router will then assume the role of the active router. If other routers are participating in the group, they then contend to be the new standby router.

In the event that both the active and standby routers fail, all routers in the group contend for the active and standby router roles.

Because the new active router assumes both the IP and MAC addresses of the virtual router, the end stations see no disruption in service. The end-user stations continue to send packets to the virtual router MAC address, and the new active router delivers the packets to the destination.

Describing HSRP States

This topic describes the six HSRP states and their functions.

HSRP States

An HSRP router can be in one of six different states:

- Initial
- Learn
- Listen
- Speak
- Standby
- Active

© 2006 Cisco Systems, Inc. All rights reserved. BCRSN v3.0-5.11

A router in an HSRP group can be in one of these states: initial, learn, listen, standby, or active.

HSRP States

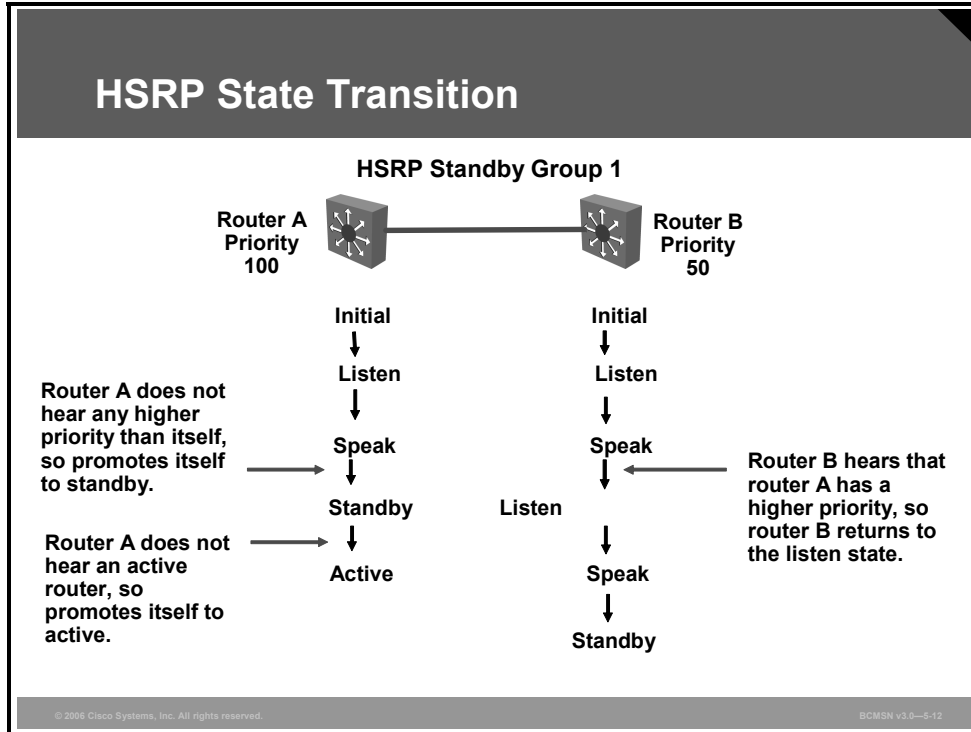
The table describes the different HSRP states.

State	Definition
Initial	The state at the start. The initial state indicates that HSRP does not run. This state is entered via a configuration change or when an interface first comes up.
Learn	The router is neither in the active or standby state, nor does it have enough information to attempt to claim the active or standby role.
Listen	The router knows the virtual IP address, but the router is neither the active router nor the standby router. It listens for hello messages from those routers.
Speak	The router sends periodic hello messages and actively participates in the election of the active or standby router. A router cannot enter speak state unless the router has the virtual IP address.
Standby	The router is a candidate to become the next active router and sends periodic hello messages. With the exclusion of transient conditions, there is, at most, one router in the group in standby state.
Active	The router currently forwards packets that are sent to the group virtual MAC address. The router sends periodic hello messages. With the exclusion of transient conditions, there must be, at the most, one router in the active state in the group.

When a router exists in one of these states, it performs the actions required for that state. Not all HSRP routers in the group will transition through all states. For example, if there were three routers in the HSRP group, the router that is not the standby or active router will remain in the listen state.

HSRP State Transition

This subtopic describes the HSRP state transitions.



All routers begin in the initial state. This is the starting state and indicates that HSRP is not running. This state is entered via a configuration change, such as when HSRP is disabled on an interface, or when an HSRP-enabled interface is first brought up, such as when the **no shutdown** command is issued.

The purpose of the listen state is to determine if there are already active or standby routers for the group.

In the speak state, the routers are actively participating in the election of the active router or standby router or both.

Each router uses three timers in HSRP. The timers time hello messages. When a timer expires, the router transitions to a new HSRP state.

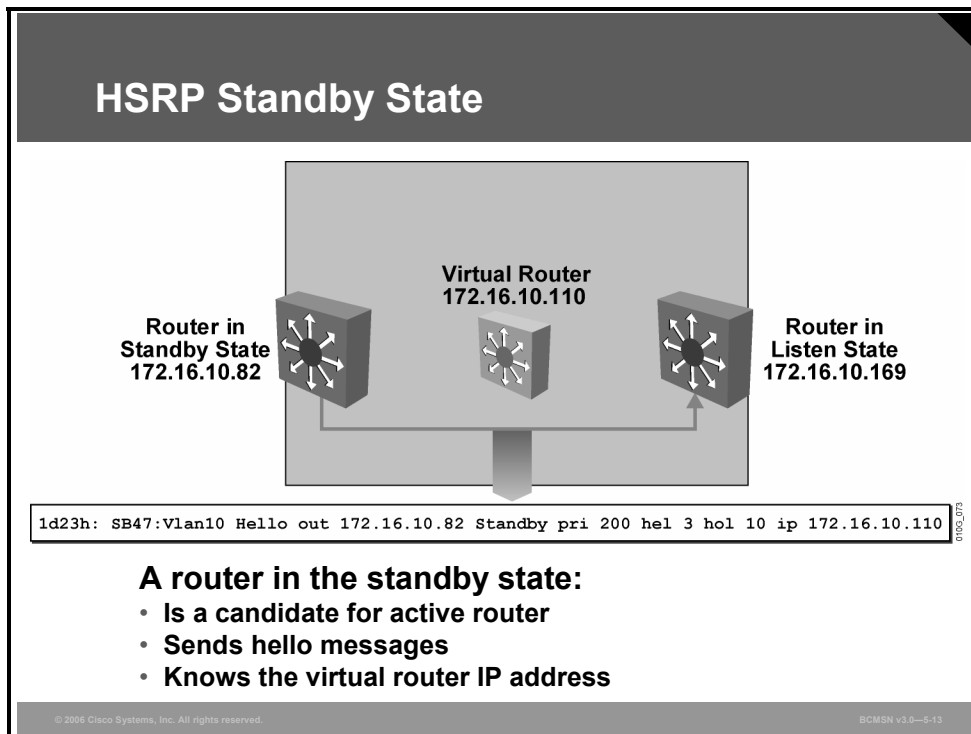
HSRP Timers

The table describes the HSRP timers.

Term	Definition
Active timer	This timer is used to monitor the active router. The timer resets any time a router in the standby group receives a hello packet from the active router. This timer expires in accordance with the hold time value that is set in the corresponding field of the HSRP hello message.
Standby timer	This timer is used to monitor the standby router. The timer resets any time a router in the standby group receives a hello packet from the standby router. This timer expires in accordance with the hold time value that is set in the respective hello packet.
Hello timer	This timer is used to clock hello packets. All HSRP routers in any HSRP state generate a hello packet when this hello timer expires.

Standby State

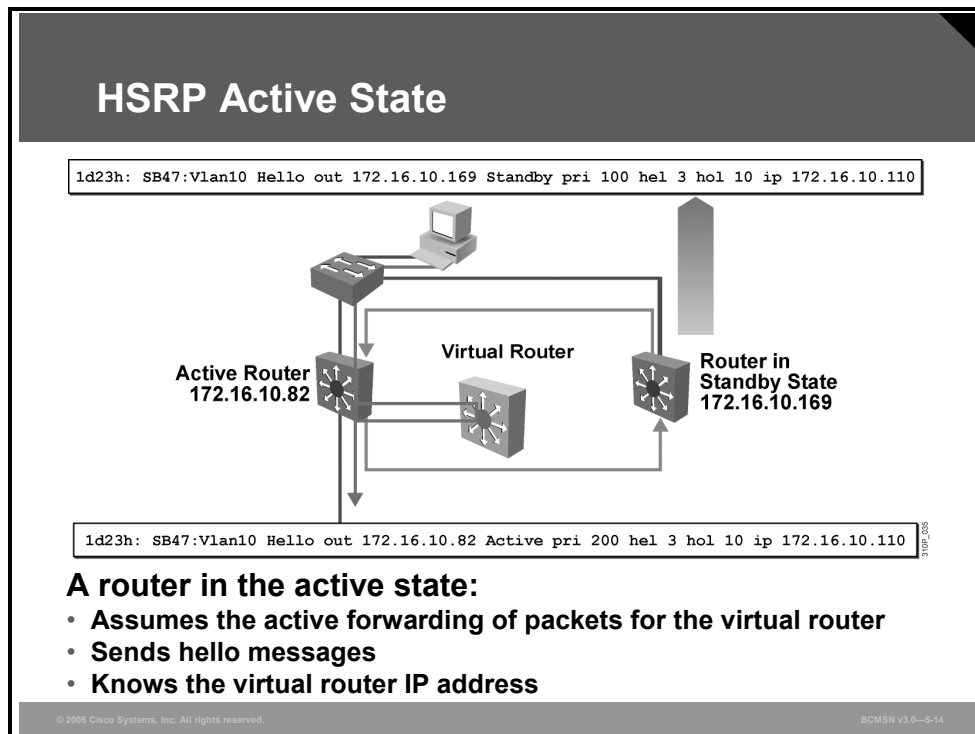
This subtopic describes the HSRP standby state.



In the standby state, because the router is a candidate to become the next active router, it sends periodic hello messages. It will also listen for hello messages from the active router. There will be only one standby router in the HSRP group.

Active State

This subtopic describes the HSRP active state.



In the active state, the router is currently forwarding packets that are sent to the virtual MAC address of the group. It also replies to ARP requests that are directed to the virtual router's IP address. The active router sends periodic hello messages. There must be one active router in each HSRP group.

Describing HSRP Configuration Commands

This topic describes the commands used to configure HSRP.

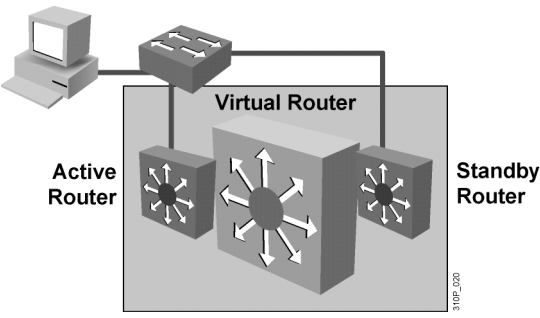
HSRP Configuration Commands

Configure

- standby 1 ip 10.1.1.1

Verify

- show running-config
- show standby



The diagram illustrates HSRP configuration. A PC is connected to a switch. The switch is connected to a Virtual Router, which consists of an Active Router and a Standby Router. The Virtual Router is shown as a central box with arrows pointing outwards, representing the virtual gateway. The Active Router and Standby Router are shown as smaller boxes with arrows pointing outwards, representing the physical routers that provide redundancy for the virtual gateway.

© 2004 Cisco Systems, Inc. All rights reserved.
BCMSN v3.0—5-15

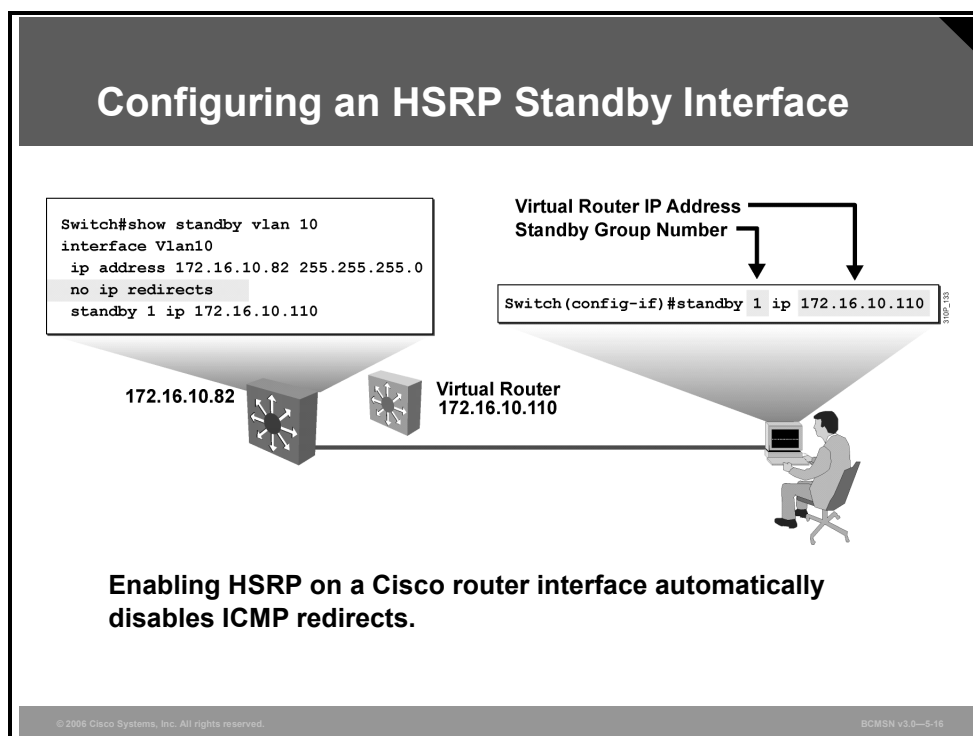
Commands Used to Configure and Verify HSRP

The table describes the minimum commands used to configure HSRP.

Command	Description
Switch(config-if)# standby group-number ip ip-address	Configures HSRP on this interface for this group number. IP address is that of the virtual gateway. Default group number is 0.
Switch(config-if)# no standby group-number ip ip-address	Disables HSRP on the interface.
Switch# show running-config	Displays HSRP parameters configured on each interface.
Switch# show standby [interface] [group] [brief]	Show standby is all that is required. Use other commands to minimize output.

Enabling HSRP

This topic explains the procedure to enable HSRP.



Configure HSRP Group on an Interface

This command enables HSRP on an interface.

```
Switch(config-if)#standby group-number ip ip-address
```

HSRP Group Configuration Command

The table describes the variables in the command used to configure an HSRP group on an interface.

Variable	Definition
<i>group-number</i>	(Optional) Indicates the HSRP group to which this interface belongs. Specifying a unique group number in the standby commands enables the creation of multiple HSRP groups. The default group is 0.
<i>ip-address</i>	Indicates the IP address of the virtual HSRP router.

While running HSRP, the end-user stations must not discover the actual MAC addresses of the routers in the standby group. Any protocol that informs a host of a router actual address must be disabled. To ensure that the actual addresses of the participating HSRP routers are not discovered, enabling HSRP on a Cisco Systems router interface automatically disables Internet Control Message Protocol (ICMP) redirects on that interface.

After the **standby ip** command is issued, the interface changes to the appropriate state. When the router successfully executes the command, the router issues an HSRP message.

To remove an interface from an HSRP group, enter the **no standby group ip** command.

Verifying HSRP Configuration

This subtopic shows the command used to verify the HSRP configuration.

Displaying the Standby Brief Status


```
Switch#show standby brief
                P indicates configured to preempt.
                |
Interface   Grp Prio P State   Active addr   Standby addr   Group addr
Vl11       11 110  Active local     172.16.11.114 172.16.11.115
```

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0-5-17

This example states that interface VLAN11 is a member of HSRP group 11, that the virtual router IP address for the group is 172.16.11.115, and that ICMP redirects are disabled.

```
Switch#show running-config
Building configuration...
```

```
Current configuration:
!
(text deleted)
interface Vlan11
ip address 172.16.11.113 255.255.255.0
no ip redirects
standby 11 ip 172.16.11.115
!
```

Another means of verifying the HSRP configuration is with this command:

```
Switch# show standby brief
```

It displays abbreviated information about the current state of all HSRP operations on this device.

To display the status of the HSRP router, enter one of these commands:

```
Switch#show standby [interface [group]] [active | init | listen |
standby] [brief]
```

```
Switch#show standby delay [type-number]
```

If the optional interface parameters are not indicated, the **show standby** command displays HSRP information for all interfaces.

Verify All HSRP Operations

This example shows the output of the **show standby** command:

```
Switch#show standby Vlan11 11
Vlan11 - Group 11
  Local state is Active, priority 110
  Hellotime 3 holdtime 10
  Next hello sent in 00:00:02.944
  Hot standby IP address is 172.16.11.115 configured
  Active router is local
  Standby router is 172.16.11.114 expires in 00:00:08
  Standby virtual mac address is 0000.0c07.ac01
```

This is an example of the output resulting when you specify the **brief** parameter:

```
Switch#show standby brief
Interface Grp Prio P State Active addr Standby addr Group addr
Vl11      11 110 Active local 172.16.11.114 172.16.11.115
```

Summary

This topic summarizes the key points discussed in this lesson.

Summary

- **Router redundancy allows two or more routers to work as a group to maintain forwarding of IP packets.**
- **A single default gateway or proxy ARP does not provide the redundancy required in a campus network.**
- **HSRP provides router redundancy to end devices.**
- **HSRP operates to provide nonstop path redundancy for IP.**
- **An HSRP-enabled router will exist in a specific state or transition through a series of states.**
- **HSRP is configured using the standby command.**
- **HSRP is enabled per interface.**

Optimizing HSRP

Overview

Hot Standby Router Protocol (HSRP) has options that allow it to be configured to define the order in which active and standby router are selected, for expedited failover, recovery from failover and to specify which interface is to be monitored for HSRP failover.

Specific commands are used to optimize and tune HSRP operations for greatest failover resiliency. There is also a set of commands for verifying and debugging HSRP general and optimized operations.

Objectives

Upon completing this lesson, you will be able to describe how to identify technologies and best practices that are required to increase network availability and verify its function in a multilayer switch. This ability includes being able to meet these objectives:

- Describe the options that can be configured to optimize HSRP
- Explain the procedure to determine which HSRP operations require tuning in their networks
- Describe how a single router can be a member of multiple HSRP-standby groups to facilitate load sharing
- Describe the commands used to debug HSRP operations
- Explain the procedure to debug HSRP operations

Describing HSRP Optimization Options

This topic describes the options that can be configured to optimize HSRP.

HSRP Optimization Options

These options can be configured to optimize HSRP:

- **HSRP standby priority**
- **HSRP standby preempt**
- **Hello message timers**
- **HSRP interface tracking**

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0—5-2

These options are available to optimize the operation of HSRP in the campus network.

HSRP Optimization Options

The table describes the options for HSRP operation.

Option	Description
Standby priority	This option allows the network administrator to control the order in which active routers for that group are selected.
Standby preempt	The preempt option allows a router to regain its role of active router even if there is an existing active router on the segment.
Hello message timer adjustment	This option is used to configure the time between hello packets and the time before other routers declare the active router to be down.
HSRP interface tracking	The standby track interface configuration command ties the router hot standby priority to the availability of its interfaces and is useful for tracking interfaces that are not configured for HSRP.

Establishing HSRP Priorities

In this step the HSRP priority is set and verified.

Configuring HSRP Standby Priority

```
Switch#show standby vlan 10
interface Vlan10
ip address 172.16.10.82 255.255.255.0
no ip redirects

standby 1 priority 150
standby 1 ip 172.16.10.110
```

Assigned Priority
Standby Group Number

Switch(config-if)#standby 1 priority 150

- The router with the highest priority in an HSRP group becomes the active router.
- The default priority is 100.
- In the case of a tie, the router with the highest configured IP address will become active.

© 2006 Cisco Systems, Inc. All rights reserved.
BCMSN v3.0-5-3

Each standby group has its own active and standby routers. The network administrator can assign a priority value to each router in a standby group, allowing the administrator to control the order in which active routers for that group are selected.

To set the priority value of a router, enter this command in interface configuration mode:

```
Switch(config-if)#standby group-number priority priority-value
```

HSRP Standby Priority Configuration Commands

The table describes the variables for the **standby** command.

Variable	Definition
<i>group-number</i>	Indicates the HSRP group. This number can be in the range of 0 to 255.
<i>priority-value</i>	Indicates the number that prioritizes a potential hot standby router. The range is 0 to 255; the default is 100.

During the election process, the router with the highest priority in an HSRP group becomes the active router. In the case of a tie, the router with the highest configured IP address will become active.

To reinstate the default standby priority value, enter the **no standby priority** command.

Note If the routers do not have preempt configured, then a router that boots up significantly faster than the others in the standby group will become the active router, regardless of the configured priority.

Verify the HSRP Standby Priority

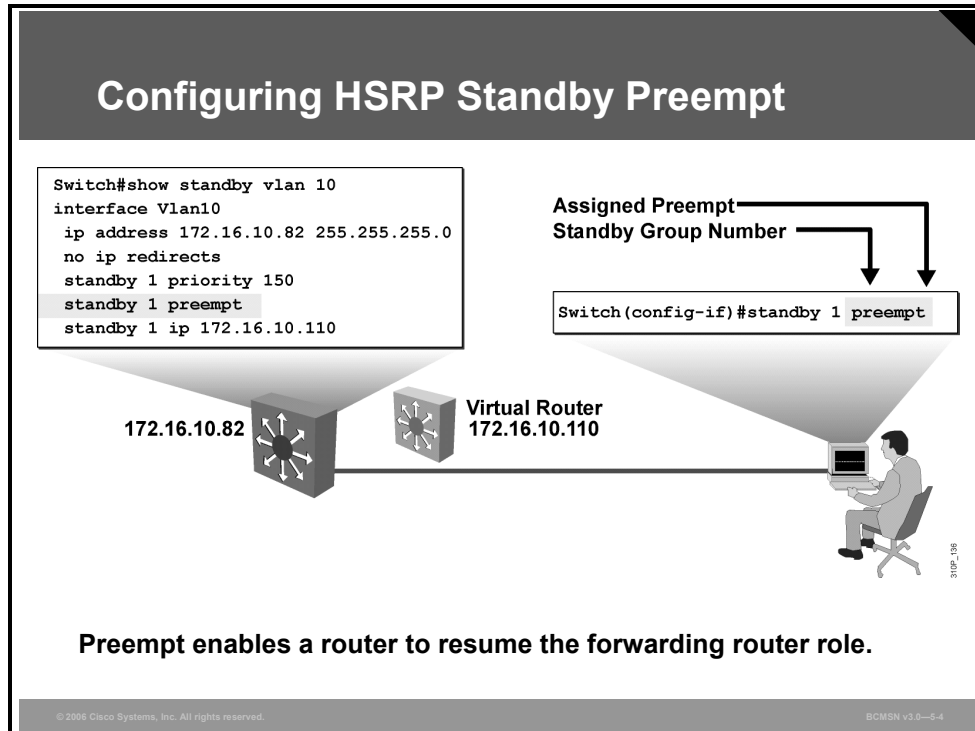
This example states that interface VLAN10 has a priority value of 150 in HSRP group 1. If this priority value is the highest number in that HSRP group, the routing device on which this interface resides is the active router for that group.

```
Switch#show running-config  
Building configuration...
```

```
Current configuration:  
!  
(text deleted)  
interface Vlan10  
ip address 172.16.10.32 255.255.255.0  
no ip redirects  
standby 1 priority 150  
standby 1 ip 172.16.10.110
```

HSRP Standby Preempt

The standby router automatically assumes the active router role when the active router fails or is removed from service. This new active router remains the forwarding router, even when the former active router with the higher priority regains service in the network.



The former active router can be configured to resume the forwarding router role by preempting a router with a lower priority. To enable a router to resume the forwarding router role, enter this command in interface configuration mode:

```
Switch(config-if)#standby [group-number] preempt [{delay} [minimum delay] [sync delay]]
```

When the **standby preempt** command is issued, the interface changes to the appropriate state.

To remove the interface from preemptive status, enter the **no standby group preempt** command.

Example: Displaying HSRP Preempt

This example states that interface VLAN10 is configured to resume its role as the active router in HSRP group 1, assuming that interface VLAN10 on this router has the highest priority in that standby group.

```
Switch#show running-config
Building configuration...

Current configuration:
!
(text deleted)
interface Vlan10
ip address 172.16.10.82 255.255.255.0
no ip redirects
standby 1 priority 150
standby 1 preempt
standby 1 ip 172.16.10.110
```

Hello Message Timers

An HSRP-enabled router sends hello messages to indicate that the router is running and is capable of becoming either the active or the standby router.

Configuring the Hello Message Timers

```
Building configuration...

Current configuration:
(text deleted)
!
interface Vlan10
 ip address 172.16.10.82 255.255.255.0
 no ip redirects
 standby 1 timers 5 15
 standby 1 ip 172.16.10.10
```

Holdtime
Hellotime

```
Switch(config-if)#standby 1 timers 5 15
```

The holdtime parameter value should be at least three times the value of the hellotime parameter.

© 2006 Cisco Systems, Inc. All rights reserved.BCMSN v3.0-6.5

The hello message contains the priority of the router and also hellotime and holdtime parameter values. The hellotime parameter value indicates the interval between the hello messages that the router sends. The holdtime parameter value indicates the amount of time that the current hello message is considered valid. The standby timer includes an **msec** parameter to allow for subsecond failovers. Lowering the hello timer results in increased traffic for hello messages and should be used cautiously.

If an active router sends a hello message, receiving routers consider that hello message to be valid for one holdtime. The holdtime value should be at least three times the value of the hellotime. The holdtime value must be greater than the value of the hellotime.

By default, HSRP hellotime is 3 seconds and holdtime is 10 seconds, which means that failover time could be as much as 10 seconds for clients to start communicating with the new default gateway. In some cases, this interval may be excessive for application support. The hellotime and the holdtime parameters are both configurable. To configure the time between hello messages and the time before other group routers declare the active or standby router to be nonfunctioning, enter this command in interface configuration mode:

```
Switch(config-if)#standby group-number timers [msec] hellotime holdtime
```

Note Hello and dead timer intervals must be identical for all devices within the HSRP group.

Standby Message Timer Configuration Options

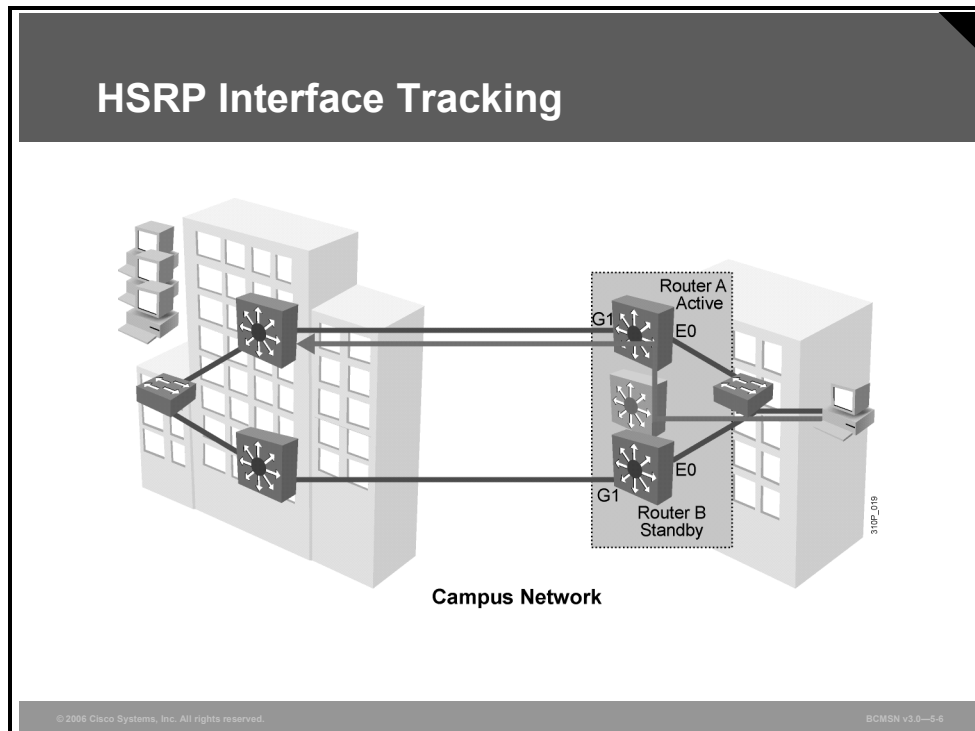
The table describes the options for standby message timer configuration.

Variable	Description
<i>group-number</i>	(Optional) Group number on the interface to which the timers apply. The default is 0.
<i>hellotime</i>	Hello interval in seconds. This is an integer from 1 through 255. The default is 3 seconds.
<i>holdtime</i>	Time, in seconds, before the active or standby router is declared to be down. This is an integer from 1 through 255. The default is 10 seconds.

To reinstate the default standby timer values, enter the **no standby group timers** command.

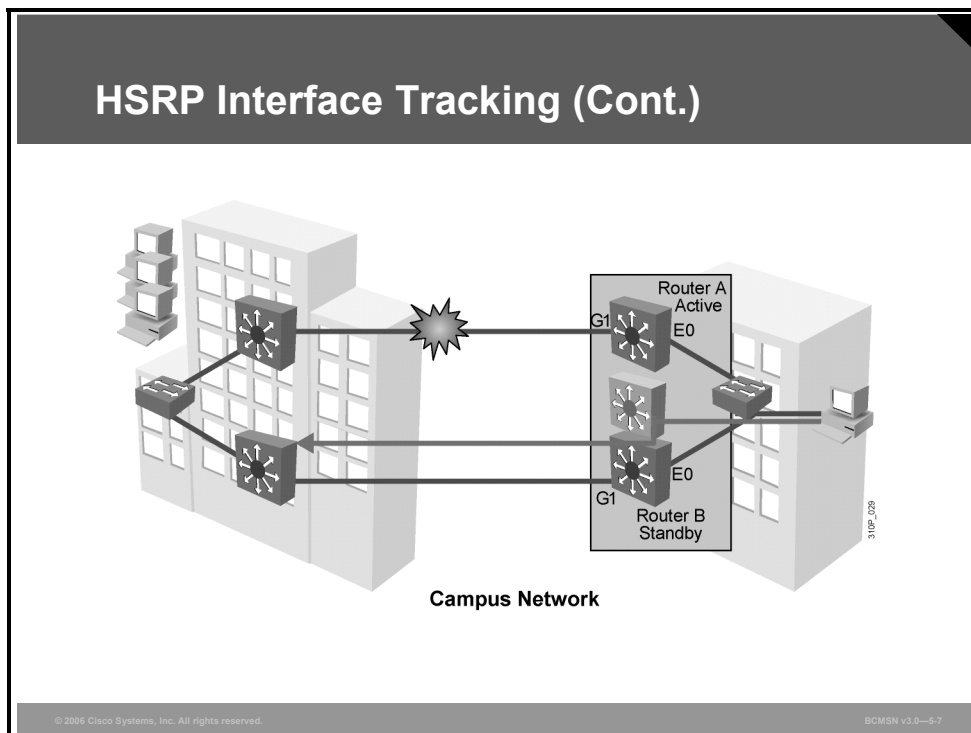
HSRP Interface Tracking

In some situations, the status of an interface directly affects which router needs to become the active router. This is particularly true when each of the routers in an HSRP group has a different path to resources within the campus network.



In this example, router A and router B reside in one building. Each of these routers supports a Gigabit Ethernet link to the other building. Router A has the higher priority and is the active forwarding router for standby group 1. Router B is the standby router for that group. Routers A and B are exchanging hello messages through their E0 interfaces.

HSRP Interface Tracking (Cont.)



The Gigabit Ethernet link between the active forwarding router for the standby group and the other building experiences a failure. Without HSRP enabled, router A would detect the failed link and send an Internet Control Message Protocol (ICMP) redirect to router B. However, when HSRP is enabled, ICMP redirects are disabled.

Therefore, neither router A nor the virtual router sends an ICMP redirect. In addition, although the G1 interface on router A is no longer functional, router A still communicates hello messages out interface E0, indicating that router A is still the active router. Packets sent to the virtual router for forwarding to headquarters cannot be routed.

Interface tracking enables the priority of a standby group router to be automatically adjusted, based on availability of the interfaces of that router. When a tracked interface becomes unavailable, the HSRP priority of the router is decreased. When properly configured, the HSRP tracking feature ensures that a router with an unavailable key interface will relinquish the active router role.

In this example, the E0 interface on router A tracks the G1 interface. If the link between the G1 interface and the other building fails, the router automatically decrements the priority on that interface and stops transmitting hello messages out interface E0. Router B assumes the active router role when no hello messages are detected for the specific holdtime period.

Configuring HSRP Tracking

To configure HSRP tracking, enter the command in the figure in interface configuration mode.

Configuring HSRP Tracking

```
Switch(config-if)#standby [group-number] track type number  
[interface-priority]
```

- **Configures HSRP tracking**

```
Switch(config)#interface vlan 10  
Switch(config-if)#standby 1 track GigabitEthernet 0/7 50  
Switch(config-if)#standby 1 track GigabitEthernet 0/8 60
```

- **Example of HSRP tracking**

Note: Preempt must be configured on all participating devices within the HSRP group.

© 2006 Cisco Systems, Inc. All rights reserved.BCMSN v3.0—5-8

HSRP Tracking Configuration Arguments

The table describes the variables in the HSRP configuration command.

Variable	Description
<i>group-number</i>	(Optional) Indicates the group number on the interface to which the tracking applies. The default number is 0.
<i>type</i>	Indicates the interface type (combined with the interface number) that will be tracked.
<i>number</i>	Indicates the interface number (combined with the interface type) that will be tracked.
<i>interface-priority</i>	(Optional) Indicates the amount by which the hot standby priority for the router is decremented when the interface becomes disabled. The priority of the router is incremented by this amount when the interface becomes available. The default value is 10.

To disable interface tracking, enter the **no standby group track** command.

The command to configure HSRP tracking on a multilayer switch is the same as on the external router, except that the interface type can be identified as a switch virtual interface (**vlan** followed by the *vlan number* assigned to that interface) or by a physical interface.

The internal routing device uses the same command as the external routing device to disable interface tracking.

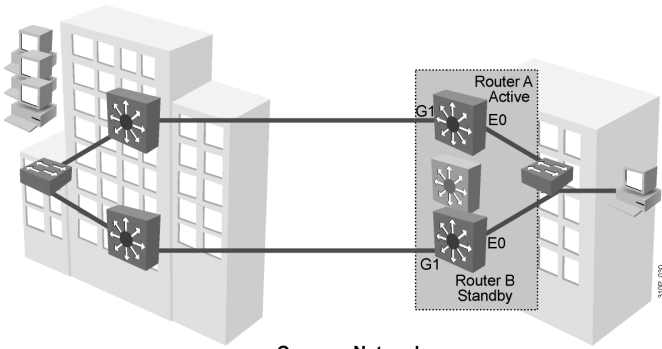
Multiple tracking statements may be applied to an interface. For example, this may be useful if the currently active HSRP interface will relinquish its status only upon the failure of two (or more) tracked interfaces.

Tuning HSRP Operations

This topic explains the procedure to determine which HSRP operations require tuning in a network.

Tuning HSRP

- **Configure hellotime and holdtime to millisecond values.**
- **Configure preempt delay timer so that preempt occurs only after the distribution switch has fully rebooted and established full connectivity to the rest of the network.**



Campus Network

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0-5-9

HSRP timers can be adjusted to tune the performance of HSRP on distribution devices, thereby increasing their resilience and reliability in routing packets off the local VLAN.

Subsecond Failover

The HSRP hellotime and holdtime can be set to millisecond values so that HSRP failover occurs in less than 1 second. Here is an example:

```
Switch(config-if)#standby 1 timers msec 200 msec 750
```

Preempt Time Aligned with Router Boot Time

Preempt is an important feature of HSRP that allows the primary router to resume the active role when it comes back online after a failure or maintenance event. Preemption is a desired behavior because it forces a predictable routing path for the VLAN during normal operations and ensures that the Layer 3 forwarding path for a VLAN parallels the Layer 2 Spanning Tree Protocol (STP) forwarding path whenever possible.

When a preempting device is rebooted, HSRP preempt communication should not begin until the distribution switch has established full connectivity to the rest of the network. This allows the routing protocol convergence to occur more quickly, after the preferred router is in an active state.

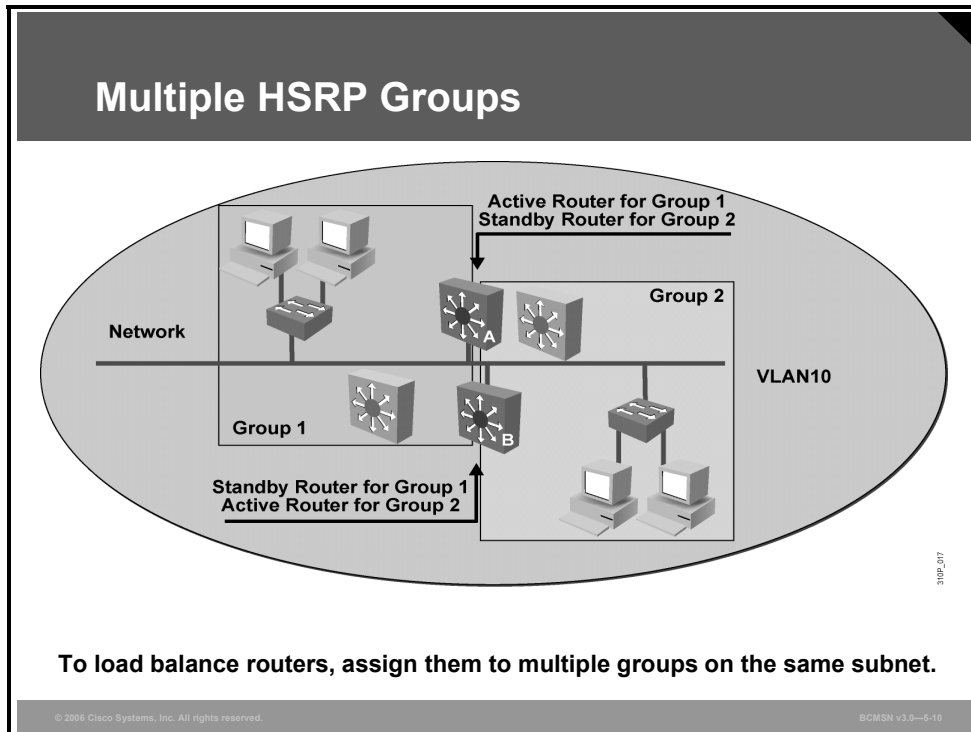
To accomplish this, measure the system boot time and set the HSRP preempt delay to a value 50 percent greater than the boot time. This ensures that the primary distribution switch establishes full connectivity to the network before HSRP communication occurs.

For example, if the boot time for the distribution device is 120 seconds, the preempt configuration would appear as follows:

```
standby 1 preempt
standby 1 preempt delay minimum 180
```

Describing Load Sharing

This topic describes how a single router can be a member of multiple HSRP-standby groups to facilitate load sharing.



With a single HSRP group on a subnet, the active router is forwarding all the packets off that subnet while the standby router is forwarding no packets off that subnet. To facilitate load sharing, and hence have both routers load balancing, a single router may be a member of multiple HSRP groups that exist on the same segment.

Multiple standby groups further enable redundancy and load sharing within networks. While a router is actively forwarding traffic for one HSRP group, the router can be in standby or listen state for another group.

Each standby group emulates a single virtual router. There can be up to 255 standby groups on any LAN, but the maximum standby groups that are necessary should be no more than the number of active routers required. In most cases, the required number will be two.

Caution Increasing the number of groups in which a router participates increases the load on the router. This can have an impact on the performance of the router.

In the figure, both router A and router B are members of groups 1 and 2. However, router A is the active forwarding router for group 1 and the standby router for group 2. Router B is the active forwarding router for group 2 and the standby router for group 1.

Example of Multiple HSRP Groups on the Same Segment

This example shows how multiple HSRP groups can be configured on the same segment to facilitate load sharing.

```
RouterA#show running-config
Building configuration...
```

```
Current configuration:
!
(text deleted)
interface Vlan10
ip address 172.16.10.32 255.255.255.0
no ip redirects
standby 1 priority 150
standby 1 ip 172.16.10.110
standby 2 priority 50
standby 2 ip 172.16.10.120
```

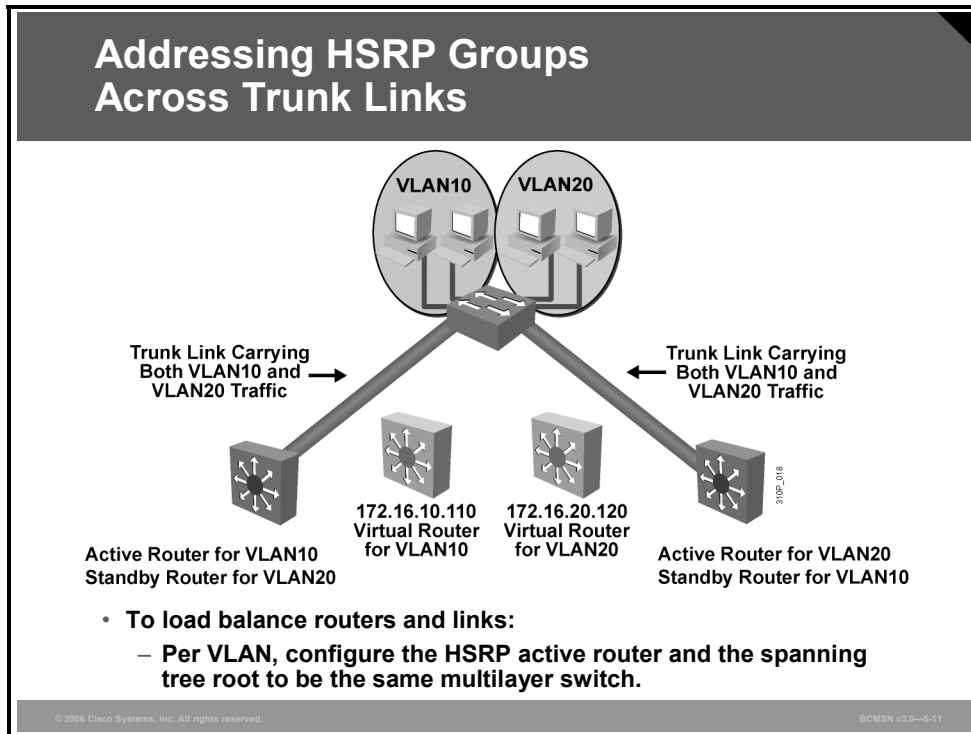
```
RouterB#show running-config
Building configuration...
```

```
Current configuration:
!
(text deleted)
interface Vlan10
ip address 172.16.10.33 255.255.255.0
no ip redirects
standby 1 priority 50
standby 1 ip 172.16.10.110
standby 2 priority 150
standby 2 ip 172.16.10.120
```

```
RouterA#show standby brief
                P indicates configured to preempt.
                |
Interface Grp Prio P State      Active      Standby      Virtual IP
Vl10      1   150 Active    local       172.16.10.33 172.16.10.110
Vl10      2   50 Standby   172.16.10.33 local       172.16.10.120
```

Addressing HSRP Groups Across Trunk Links

This subtopic describes how HSRP devices can provide primary paths for some data and backup paths for other data when VLANs and trunks are deployed in the network.



Routers can simultaneously provide redundant backup and perform load sharing across different IP subnets.

In the figure, two HSRP-enabled routers participate in two separate VLANs, using Inter-Switch Link (ISL) or 802.1Q. Running HSRP over trunking allows users to configure redundancy among multiple routers that are configured as front ends for VLAN IP subnets.

By configuring HSRP over trunks, users can eliminate situations in which a single point of failure causes traffic interruptions. This feature inherently provides some improvement in overall networking resilience by providing load balancing and redundancy capabilities between subnets and VLANs.

For a VLAN, configure the same device to be both the spanning tree root and the HSRP active router. This approach ensures that the Layer 2 forwarding path leads directly to the Layer 3 active router and so achieves maximum efficiency of load balancing on the routers and the trunks.

For each VLAN, a standby group, an IP address, and a single well-known MAC address with a unique group identifier is allocated to the group. Although up to 255 standby groups can be configured, it is advised that the actual number of group identifiers used be kept to a minimum. When you are configuring two distribution layer switches, typically you will require only two standby group identifiers, regardless of how many standby groups are actually created.

Example of Load Sharing Across Different IP Subnets

This example shows how multiple HSRP groups can be configured on two HSRP-enabled routers to participate in two separate VLANs

```
1DSW1#show running-config
```

```
Building configuration...
```

```
Current configuration:
```

```
!  
(text deleted)  
interface Vlan10  
ip address 172.16.10.32 255.255.255.0  
no ip redirects  
standby 1 priority 150  
standby 1 ip 172.16.10.110  
  
interface Vlan20  
ip address 172.16.20.32 255.55.255.0  
no ip redirects  
standby 2 priority 50  
standby 2 ip 172.16.20.120
```

```
RouterB#show running-config
```

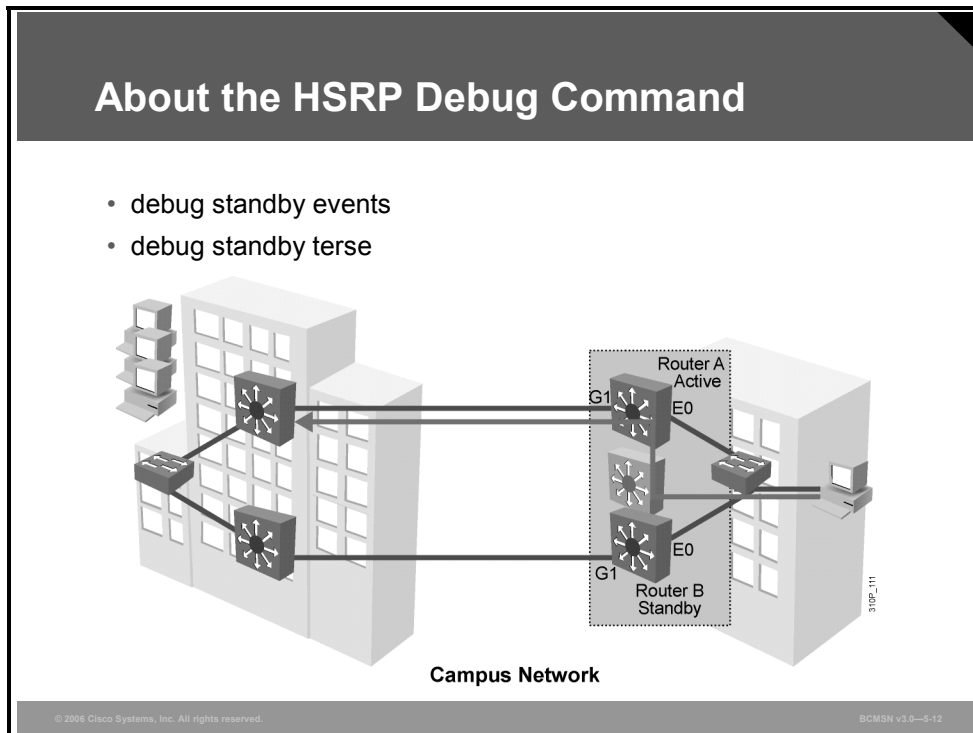
```
Building configuration...
```

```
Current configuration:
```

```
!  
(text deleted)  
interface Vlan10  
ip address 172.16.10.33 255.255.255.0  
no ip redirects  
standby 1 priority 50  
standby 1 ip 172.16.10.110  
  
interface Vlan20  
ip address 172.16.20.33 255.255.255.0  
no ip redirects  
standby 2 priority 150  
standby 2 ip 172.16.20.120
```

Describing HSRP Debug Commands

This topic describes the commands used to debug HSRP operations.



These commands are used to debug HSRP operation.

HSRP Debug Commands

The table describes commands used to debug HSRP.

Command	Description
Switch# debug standby [errors] [events] [packets]	Displays all state changes to HSRP, including all hello packets. Arguments minimize output.
Switch# debug standby terse	Displays all HSRP errors, events, and packets, except hello and advertisement packets.

Debugging HSRP Operations

This topic explains the procedure to debug HSRP operations.

Debugging HSRP

```
DSW111#debug standby
*Mar 4 19:08:08.918: HSRP: V11 Grp 1 Hello out 172.16.1.111 Active pri 150 vIP 172.16.1.113
*Mar 4 19:08:09.287: HSRP: V11 Grp 2 Hello in 172.16.1.112 Active pri 50 vIP 172.16.1.113
*Mar 4 19:08:09.287: HSRP: V11 API active virtual address 172.16.1.113 found
*Mar 4 19:08:09.891: HSRP: V11 API Duplicate ARP entry detected for 172.16.1.113
*Mar 4 19:08:09.891: HSRP: V11 Grp 1 Hello out 172.16.1.111 Active pri 150 vIP 172.16.1.113
*Mar 4 19:08:10.294: HSRP: V11 Grp 2 Hello in 172.16.1.112 Active pri 50 vIP 172.16.1.113
*Mar 4 19:08:10.294: HSRP: V11 API active virtual address 172.16.1.113 found
*Mar 4 19:08:10.294: HSRP: V11 API Duplicate ARP entry detected for 172.16.1.113
*Mar 4 19:08:10.294: HSRP: V11 Grp 1 Hello out 172.16.1.111 Active pri 150 vIP 172.16.1.113
*Mar 4 19:08:10.294: HSRP: V11 Grp 2 Hello in 172.16.1.112 Active pri 50 vIP 172.16.1.113
*Mar 4 19:08:10.294: HSRP: V11 API active virtual address 172.16.1.113 found
*Mar 4 19:08:10.898: HSRP: V11 API Duplicate ARP entry detected for 172.16.1.113
*Mar 4 19:08:10.898: HSRP: V11 Grp 1 Hello out 172.16.1.111 Active pri 150 vIP 172.16.1.113
*Mar 4 19:08:10.965: HSRP: V11 Grp 2 Hello in 172.16.1.112 Active pri 50 vIP 172.16.1.113
*Mar 4 19:08:11.300: HSRP: V11 API active virtual address 172.16.1.113 found
```

- Example of HSRP debug showing standby group number mismatch

The Cisco IOS implementation of HSRP supports the **debug** command. Enabling debug displays HSRP state changes and debug output regarding the transmission and receipt of HSRP packets. To enable HSRP debugging, enter this command in privileged EXEC mode:

```
Switch#debug standby
```

Field Descriptions for the debug standby Command

The table provides a description of debug standby fields.

Field	Description
SB	Abbreviation for "standby"
Ethernet0	Interface on which a Hot Standby packet was sent or received
Hello in	Hello packet received from the specified IP address
Hello out	Hello packet sent from the specified IP address
pri	Priority advertised in the hello packet
hel	Hello interval advertised in the hello packet
hol	Hold-down interval advertised in the hello packet
ip address	Hot Standby group IP address advertised in the hello packet
state	Transition from one state to another
Coup out address	Coup packet sent by the router from the specified IP address

Caution Because debugging output is assigned high priority in the CPU process, this command can render the system unusable.

Example: HSRP Debugging with Two Active Routers

The example shown here and in the slide displays the **debug standby** command output on the 1DSW1.

From the output, it can be seen that 1DSW1 is sending an HSRP Hello on VLAN1 for standby group 1 with a virtual IP address of 172.16.1.113. It can also be seen that 1DSW1 is receiving an HSRP Hello from 172.16.1.112 for the same VLAN and same virtual IP address, but with a different standby group number. Hence both routers are active for the same virtual IP address.

Debug standby has been used to troubleshoot the problem. The standby group number is not consistent, so the two routers have not formed a standby group.

```
1DSW1#debug standby
```

```
*Mar  4 19:08:08.918: HSRP: V11 Grp 1 Hello  out 172.16.1.111 Active  pri 150 vIP
172.16.1.113
*Mar  4 19:08:09.287: HSRP: V11 Grp 2 Hello  in  172.16.1.112 Active  pri  50 vIP 172.16.1.113
*Mar  4 19:08:09.287: HSRP: V11 API active virtual address 172.16.1.113 found
*Mar  4 19:08:09.891: HSRP: V11 API Duplicate ARP entry detected for 172.16.1.113
*Mar  4 19:08:09.891: HSRP: V11 Grp 1 Hello  out 172.16.1.111 Active  pri 150 vIP
172.16.1.113
*Mar  4 19:08:10.294: HSRP: V11 Grp 2 Hello  in  172.16.1.112 Active  pri  50 vIP 172.16.1.113
*Mar  4 19:08:10.294: HSRP: V11 API active virtual address 172.16.1.113 found
*Mar  4 19:08:10.294: HSRP: V11 API Duplicate ARP entry detected for 172.16.1.113
*Mar  4 19:08:10.294: HSRP: V11 Grp 1 Hello  out 172.16.1.111 Active  pri 150 vIP
172.16.1.113
*Mar  4 19:08:10.294: HSRP: V11 Grp 2 Hello  in  172.16.1.112 Active  pri  50 vIP 172.16.1.113
*Mar  4 19:08:10.294: HSRP: V11 API active virtual address 172.16.1.113 found
*Mar  4 19:08:10.898: HSRP: V11 API Duplicate ARP entry detected for 172.16.1.113
*Mar  4 19:08:10.898: HSRP: V11 Grp 1 Hello  out 172.16.1.111 Active  pri 150 vIP
172.16.1.113
*Mar  4 19:08:10.965: HSRP: V11 Grp 2 Hello  in  172.16.1.112 Active  pri  50 vIP 172.16.1.113
*Mar  4 19:08:11.300: HSRP: V11 API active virtual address 172.16.1.113 found
```

Example: HSRP Debugging on Negotiation for Role of Active Router

This example displays the **debug standby** command output as the 1DSW1 router with the IP address 172.16.1.111 initializes and negotiates for the role of active router.

```
*Mar 8 20:34:10.221: SB11: V111 Init: a/HSRP enabled
*Mar 8 20:34:10.221: SB11: V111 Init -> Listen
*Mar 8 20:34:20.221: SB11: V111 Listen: c/Active timer expired (unknown)
*Mar 8 20:34:20.221: SB11: V111 Listen -> Speak
*Mar 8 20:34:20.221: SB11: V111 Hello out 172.16.11.111 Speak pri 100 ip 172.16.11.115
*Mar 8 20:34:23.101: SB11: V111 Hello out 172.16.11.111 Speak pri 100 ip 172.16.11.115
*Mar 8 20:34:25.961: SB11: V111 Hello out 172.16.11.111 Speak pri 100 ip 172.16.11.115
*Mar 8 20:34:28.905: SB11: V111 Hello out 172.16.11.111 Speak pri 100 ip 172.16.11.115
*Mar 8 20:34:30.221: SB11: V111 Speak: d/Standby timer expired (unknown)
*Mar 8 20:34:30.221: SB11: V111 Standby router is local
*Mar 8 20:34:30.221: SB11: V111 Speak -> Standby
*Mar 8 20:34:30.221: SB11: V111 Hello out 172.16.11.111 Standby pri 100 ip 172.16.11.115
*Mar 8 20:34:30.221: SB11: V111 Standby: c/Active timer expired (unknown)
*Mar 8 20:34:30.221: SB11: V111 Active router is local
*Mar 8 20:34:30.221: SB11: V111 Standby router is unknown, was local
*Mar 8 20:34:30.221: SB11: V111 Standby -> Active
*Mar 8 20:34:30.221: %STANDBY-6-STATECHANGE: Vlan11 Group 11 state Standby -> Active
*Mar 8 20:34:30.221: SB11: V111 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
```

To disable the debugging feature, enter either the **no debug standby** command or the **no debug all** command.

Example: HSRP Debugging on First and Only Router on Subnet

In this example, because 1DSW1 (172.16.11.111) is the only router on the subnet, and because it is not configured for preempt, this router will go through five HSRP states before becoming the active router. Notice at time stamp Mar 8 20:34:10.221 that the interface comes up and 1DSW1 enters the listen state.

The router stays in the listen state for the holdtime of 10 seconds. 1DSW1 then goes into the speak state at time stamp Mar 8 20:34:20.221 for 10 seconds. When the router is speaking, it sends its state out every 3 seconds, according to its hello interval. After 10 seconds in speak state, the router has determined that there is no standby router at time stamp Mar 8 20:34:30.221 and enters the standby state.

The router has also determined that there is not an active router; therefore, the router immediately enters the active state at time stamp Mar 8 20:34:30.221. From then on, the active router will send its active state hello message every 3 seconds. Because there are no other routers on this broadcast domain, no hellos are being received.

```
1DSW1(config)#interface vlan 11
1DSW1(config-if)#no shut

*Mar 8 20:34:08.925: %SYS-5-CONFIG_I: Configured from console by console
*Mar 8 20:34:10.213: %LINK-3-UPDOWN: Interface Vlan11, changed state to up
*Mar 8 20:34:10.221: SB: V111 Interface up
*Mar 8 20:34:10.221: SB11: V111 Init: a/HSRP enabled
*Mar 8 20:34:10.221: SB11: V111 Init -> Listen
*Mar 8 20:34:11.213: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan11, changed state to up
*Mar 8 20:34:20.221: SB11: V111 Listen: c/Active timer expired (unknown)
*Mar 8 20:34:20.221: SB11: V111 Listen -> Speak
*Mar 8 20:34:20.221: SB11: V111 Hello out 172.16.11.111 Speak pri 100 ip 172.16.11.115
*Mar 8 20:34:23.101: SB11: V111 Hello out 172.16.11.111 Speak pri 100 ip 172.16.11.115
*Mar 8 20:34:25.961: SB11: V111 Hello out 172.16.11.111 Speak pri 100 ip 172.16.11.115
*Mar 8 20:34:28.905: SB11: V111 Hello out 172.16.11.111 Speak pri 100 ip 172.16.11.115
*Mar 8 20:34:30.221: SB11: V111 Speak: d/Standby timer expired (unknown)
*Mar 8 20:34:30.221: SB11: V111 Standby router is local
*Mar 8 20:34:30.221: SB11: V111 Speak -> Standby
*Mar 8 20:34:30.221: SB11: V111 Hello out 172.16.11.111 Standby pri 100 ip 172.16.11.115
*Mar 8 20:34:30.221: SB11: V111 Standby: c/Active timer expired (unknown)
*Mar 8 20:34:30.221: SB11: V111 Active router is local
*Mar 8 20:34:30.221: SB11: V111 Standby router is unknown, was local
*Mar 8 20:34:30.221: SB11: V111 Standby -> Active
*Mar 8 20:34:30.221: %STANDBY-6-STATECHANGE: Vlan11 Group 11 state Standby -> Active
*Mar 8 20:34:30.221: SB11: V111 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
*Mar 8 20:34:33.085: SB11: V111 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
*Mar 8 20:34:36.025: SB11: V111 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
*Mar 8 20:34:38.925: SB11: V111 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
```

Example: Nonpreempt Configured Router Coming Up with HSRP

Router 1DSW1 (172.16.11.111) is configured with a priority of 100. This priority is higher than the priority of the current active router, 1DSW2 (172.16.11.112), which has a priority of 50. Note that router 1DSW1 is *not* configured with the preempt option. Only when it is configured with preempt will a router with a higher priority immediately become the active router. After router 1DSW1 goes through the HSRP initialization states, it will come up as the standby router.

```
1DSW1(config)#interface vlan 11
1DSW1(config-if)#no shut

*Mar 1 00:12:16.871: SB11: V111 Hello in 172.16.11.112 Active pri 50 ip 172.16.11.115
*Mar 1 00:12:16.871: SB11: V111 Active router is 172.16.11.112
*Mar 1 00:12:16.891: %SYS-5-CONFIG I: Configured from console by console
*Mar 1 00:12:18.619: %LINK-3-UPDOWN: Interface Vlan11, changed state to up
*Mar 1 00:12:18.623: SB: V111 Interface up
*Mar 1 00:12:18.623: SB11: V111 Init: a/HSRP enabled
*Mar 1 00:12:18.623: SB11: V111 Init -> Listen
*Mar 1 00:12:19.619: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan11, changed state to up
*Mar 1 00:12:19.819: SB11: V111 Hello in 172.16.11.112 Active pri 50 ip 172.16.11.115
*Mar 1 00:12:19.819: SB11: V111 Listen: h/Hello rcvd from lower pri Active router
(50/172.16.11.112)
*Mar 1 00:12:22.815: SB11: V111 Hello in 172.16.11.112 Active pri 50 ip 172.16.11.115
*Mar 1 00:12:22.815: SB11: V111 Listen: h/Hello rcvd from lower pri Active router
(50/172.16.11.112)
*Mar 1 00:12:25.683: SB11: V111 Hello in 172.16.11.112 Active pri 50 ip 172.16.11.115
*Mar 1 00:12:25.683: SB11: V111 Listen: h/Hello rcvd from lower pri Active router
(50/172.16.11.112)
*Mar 1 00:12:28.623: SB11: V111 Listen: d/Standby timer expired (unknown)
*Mar 1 00:12:28.623: SB11: V111 Listen -> Speak
*Mar 1 00:12:28.623: SB11: V111 Hello out 172.16.11.111 Speak pri 100 ip 172.16.11.115
*Mar 1 00:12:28.659: SB11: V111 Hello in 172.16.11.112 Active pri 50 ip 172.16.11.115
*Mar 1 00:12:28.659: SB11: V111 Speak: h/Hello rcvd from lower pri Active router (50/172.16.11.112)
*Mar 1 00:12:31.539: SB11: V111 Hello in 172.16.11.112 Active pri 50 ip 172.16.11.115
*Mar 1 00:12:31.539: SB11: V111 Speak: h/Hello rcvd from lower pri Active router (50/172.16.11.112)
*Mar 1 00:12:31.575: SB11: V111 Hello out 172.16.11.111 Speak pri 100 ip 172.16.11.115
*Mar 1 00:12:34.491: SB11: V111 Hello in 172.16.11.112 Active pri 50 ip 172.16.11.115
*Mar 1 00:12:34.491: SB11: V111 Speak: h/Hello rcvd from lower pri Active router (50/172.16.11.112)
*Mar 1 00:12:34.547: SB11: V111 Hello out 172.16.11.111 Speak pri 100 ip 172.16.11.115
*Mar 1 00:12:37.363: SB11: V111 Hello in 172.16.11.112 Active pri 50 ip 172.16.11.115
*Mar 1 00:12:37.363: SB11: V111 Speak: h/Hello rcvd from lower pri Active router (50/172.16.11.112)
*Mar 1 00:12:37.495: SB11: V111 Hello out 172.16.11.111 Speak pri 100 ip 172.16.11.115
*Mar 1 00:12:38.623: SB11: V111 Speak: d/Standby timer expired (unknown)
*Mar 1 00:12:38.623: SB11: V111 Standby router is local
*Mar 1 00:12:38.623: SB11: V111 Speak -> Standby
*Mar 1 00:12:38.623: SB11: V111 Hello out 172.16.11.111 Standby pri 100 ip 172.16.11.115
*Mar 1 00:12:40.279: SB11: V111 Hello in 172.16.11.112 Active pri 50 ip 172.16.11.115
*Mar 1 00:12:40.279: SB11: V111 Standby: h/Hello rcvd from lower pri Active router
(50/172.16.11.112)
*Mar 1 00:12:41.551: SB11: V111 Hello out 172.16.11.111 Standby pri 100 ip 172.16.11.115
*Mar 1 00:12:43.191: SB11: V111 Hello in 172.16.11.112 Active pri 50 ip 172.16.11.115
*Mar 1 00:12:43.191: SB11: V111 Standby: h/Hello rcvd from lower pri Active router
(50/172.16.11.112)
*Mar 1 00:12:44.539: SB11: V111 Hello out 172.16.11.111 Standby pri 100 ip 172.16.11.115
*Mar 1 00:12:46.167: SB11: V111 Hello in 172.16.11.112 Active pri 50 ip 172.16.11.115
*Mar 1 00:12:46.167: SB11: V111 Standby: h/Hello rcvd from lower pri Active router
(50/172.16.11.112)
*Mar 1 00:12:47.415: SB11: V111 Hello out 172.16.11.111 Standby pri 100 ip 172.16.11.115
*Mar 1 00:12:49.119: SB11: V111 Hello in 172.16.11.112 Active pri 50 ip 172.16.11.115
*Mar 1 00:12:49.119: SB11: V111 Standby: h/Hello rcvd from lower pri Active router
(50/172.16.11.112)
*Mar 1 00:12:50.267: SB11: V111 Hello out 172.16.11.111 Standby pri 100 ip 172.16.11.115
```


Example: HSRP on Preempt-Configured Router Coming Up

1DSW1 (172.16.11.11) is configured with a priority of 100. This priority is higher than the priority of the active router, 1DSW2 (172.16.11.112). 1DSW1 is also configured with preempt. Only when a router is configured with preempt will that router with a higher priority transition into the active state.

At time stamp Mar 1 00:16:43.099, the interface VLAN11 on 1DSW1 comes up and transitions into the listen state.

At time stamp Mar 1 00:16:43.295, 1DSW1 receives a hello message from the active router (1DSW2). 1DSW1 determines that the active router has a lower priority.

At time stamp Mar 1 00:16:43.295, 1DSW1 immediately sends out a coup message, indicating that 1DSW1 is transitioning into the active router. 1DSW2 enters the speak state and eventually becomes the standby router.

```
1DSW1(config)#interface vlan 11
1DSW1(config-if)#no shut

*Mar 1 00:16:41.295: %SYS-5-CONFIG_I: Configured from console by console
*Mar 1 00:16:43.095: %LINK-3-UPDOWN: Interface Vlan11, changed state to up
*Mar 1 00:16:43.099: SB: V111 Interface up
*Mar 1 00:16:43.099: SB11: V111 Init: a/HSRP enabled
*Mar 1 00:16:43.099: SB11: V111 Init -> Listen
*Mar 1 00:16:43.295: SB11: V111 Hello in 172.16.11.112 Active pri 50 ip 172.16.11.115
*Mar 1 00:16:43.295: SB11: V111 Active router is 172.16.11.112
*Mar 1 00:16:43.295: SB11: V111 Listen: h/Hello rcvd from lower pri Active router
(50/172.16.11.112)
*Mar 1 00:16:43.295: SB11: V111 Active router is local, was 172.16.11.112
*Mar 1 00:16:43.295: SB11: V111 Coup out 172.16.11.111 Listen pri 100 ip 172.16.11.115
Mar 1 00:16:43.295
*Mar 1 00:16:43.299: %STANDBY-6-STATECHANGE: Vlan11 Group 11 state Listen -> Active
*Mar 1 00:16:43.299: SB11: V111 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
*Mar 1 00:16:43.303: SB11: V111 Hello in 172.16.11.112 Speak pri 50 ip 172.16.11.115
*Mar 1 00:16:44.095: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan11, changed state to up
*Mar 1 00:16:46.187: SB11: V111 Hello in 172.16.11.112 Speak pri 50 ip 172.16.11.115
*Mar 1 00:16:46.207: SB11: V111 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
*Mar 1 00:16:49.095: SB11: V111 Hello in 172.16.11.112 Speak pri 50 ip 172.16.11.115
*Mar 1 00:16:49.195: SB11: V111 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
*Mar 1 00:16:52.079: SB11: V111 Hello in 172.16.11.112 Speak pri 50 ip 172.16.11.115
*Mar 1 00:16:52.147: SB11: V111 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
*Mar 1 00:16:53.303: SB11: V111 Hello in 172.16.11.112 Standby pri 50 ip 172.16.11.115
*Mar 1 00:16:53.303: SB11: V111 Standby router is 172.16.11.112
*Mar 1 00:16:55.083: SB11: V111 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
*Mar 1 00:16:56.231: SB11: V111 Hello in 172.16.11.112 Standby pri 50 ip 172.16.11.115
*Mar 1 00:16:58.023: SB11: V111 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
*Mar 1 00:16:59.223: SB11: V111 Hello in 172.16.11.112 Standby pri 50 ip 172.16.11.115
*Mar 1 00:17:00.983: SB11: V111 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
*Mar 1 00:17:02.211: SB11: V111 Hello in 172.16.11.112 Standby pri 50 ip 172.16.11.115
*Mar 1 00:17:03.847: SB11: V111 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
```

Summary

This topic summarizes the key points discussed in this lesson.

Summary

- **Preempt, timers, and interface tracking are options that can be configured to optimize HSRP.**
- **HSRP preempt can be tuned by adjusting timers that can thereby reduce failover time.**
- **To facilitate load sharing, a single interface on a router can be a member of multiple HSRP groups.**
- **Specific debug commands are used to view HSRP state changes.**
- **Debug can be used to discover the virtual IP address and the priority of the active and standby routers.**

Configuring Layer 3 Redundancy with VRRP and GLBP

Overview

As the name would imply, Virtual Router Redundancy Protocol (VRRP) provides router interface failover in a manner similar to Hot Standby Router Protocol (HSRP) but with added features and IEEE compatibility. The process by which VRRP operates is defined in this lesson. The Gateway Load Balancing Protocol (GLBP) and its operations will be defined and differentiated from both HSRP and VRRP. Specific commands are used to implement and to verify VRRP and GLBP.

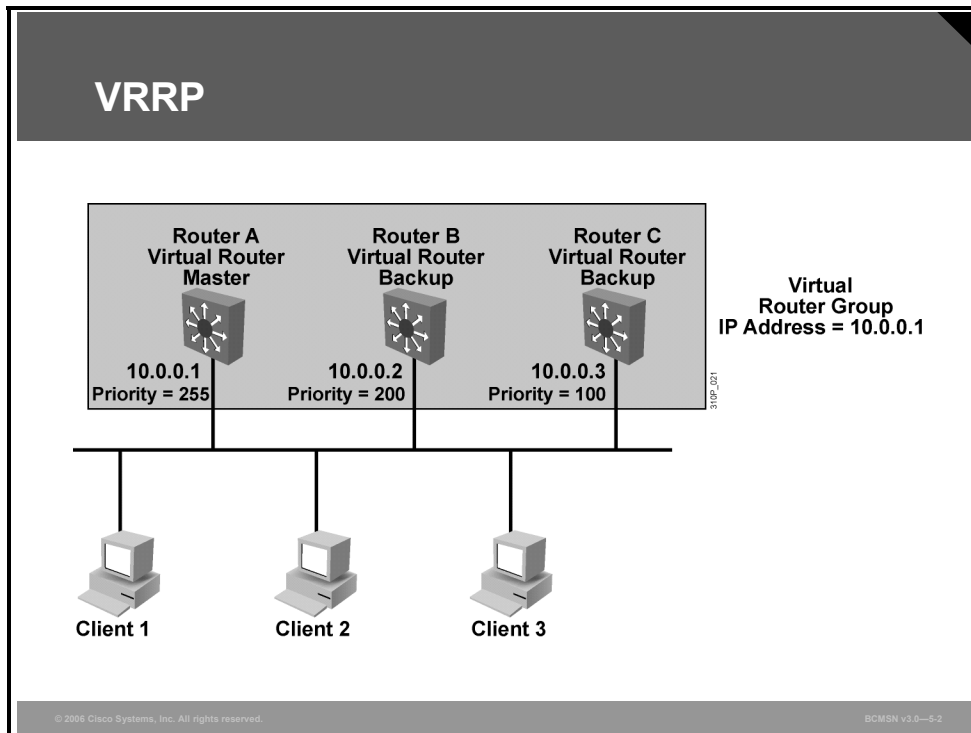
Objectives

Upon completing this lesson, you will be able to describe and configure gateway redundancy protocols (VRRP and GLBP). This ability includes being able to meet these objectives:

- Describe VRRP
- Describe how VRRP supports transitions from a master to a backup router
- Describe the commands used to configure VRRP and GLBP
- Describe GLBP
- Describe how GLBP provides balanced traffic on a per-host basis, using a round-robin scheme

Describing VRRP

This topic describes VRRP.



Like HSRP, VRRP allows a group of routers to form a single virtual router. In an HSRP or VRRP group, one router is elected to handle all requests sent to the virtual IP address. With HSRP, this is the active router. An HSRP group has one active router, at least one standby router, and perhaps many listening routers. A VRRP group has one master router and one or more backup routers.

The LAN workstations are then configured with the address of the virtual router as their default gateway. VRRP differs from HSRP in these ways:

- VRRP is an IEEE standard (RFC 2338) for router redundancy; HSRP is a Cisco Systems proprietary protocol.
- The virtual router, representing a group of routers, is known as a VRRP group.
- The active router is referred to as the master virtual router.
- The master virtual router may have the same IP address as the virtual router group.
- Multiple routers can function as backup routers.
- VRRP is supported on Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces, and on Multiprotocol Label Switching (MPLS) virtual private networks (VPNs) and VLANs.

In the example, routers A, B, and C are members of a VRRP group. The IP address of the virtual router is the same as that of the LAN interface of router A (10.0.0.1). Router A is responsible for forwarding packets sent to this IP address.

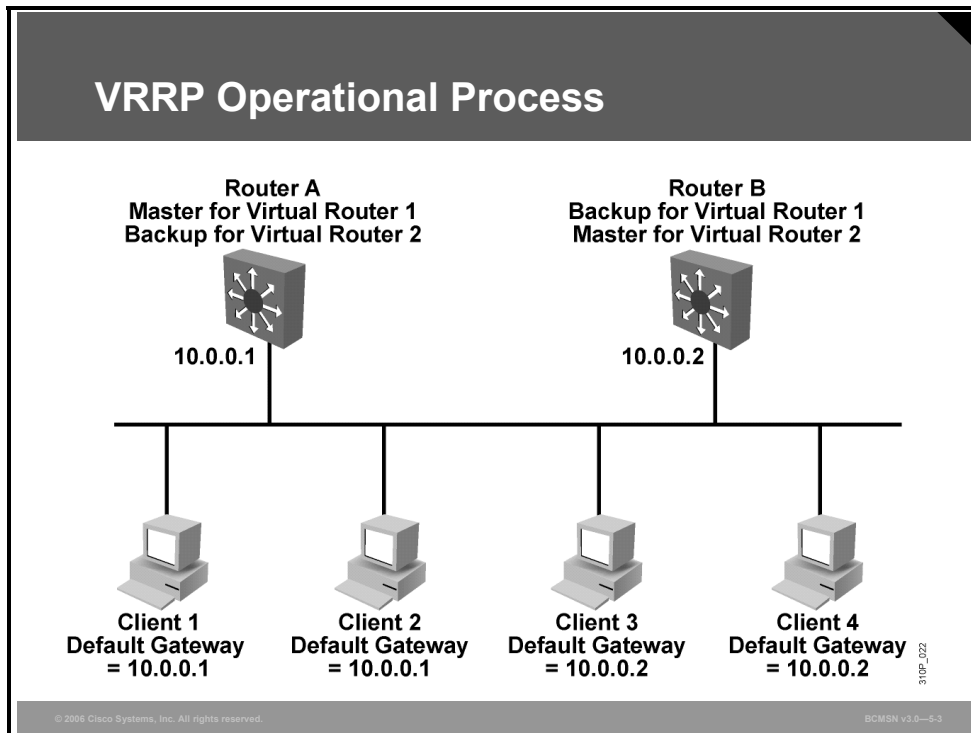
The clients have a gateway address of 10.0.0.1. Routers B and C are backup routers. If the master router fails, the backup router with the highest priority becomes the master router. When router A recovers, it resumes the role of master router.

VRRP offers these redundancy features:

- VRRP provides redundancy for the real IP address of a router or for a virtual IP address shared among the VRRP group members.
- If a real IP address is used, the router with that address becomes the master. If a virtual IP address is used, the master is the router with the highest priority.
- A VRRP group has one master router and one or more backup routers. The master router uses VRRP messages to inform group members that it is the master.

Identifying the VRRP Operations Process

This topic describes VRRP operations.



This figure shows a LAN topology in which VRRP is configured so that routers A and B share the load of being the default gateway for clients 1 through 4. Routers A and B act as backup virtual routers to one another should either one fail.

In this example, two virtual router groups are configured. For virtual router 1, router A is the owner of IP address 10.0.0.1 and is therefore the master virtual router for clients configured with that default gateway address. Router B is the backup virtual router to router A.

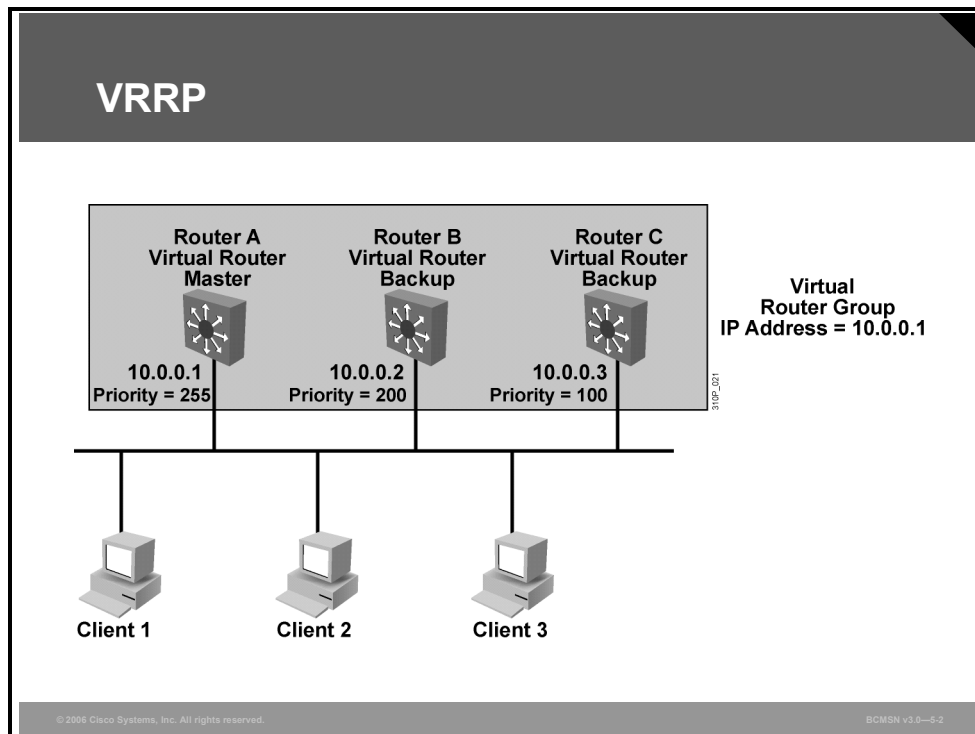
For virtual router 2, router B is the owner of IP address 10.0.0.2 and is the master virtual router for clients configured with the default gateway IP address 10.0.0.2. Router A is the backup virtual router to router B.

Given that the IP address of the VRRP group is that of a physical interface on one of the group members, the router owning that address will be the master in the group. Its priority is set to 255. Backup router priority values can range from 1 to 254; the default value is 100. The priority value zero has special meaning, indicating that the current master has stopped participating in VRRP. This setting is used to trigger backup routers to quickly transition to the master without having to wait for the current master to time out.

With VRRP, only the master sends advertisements (the equivalent of HSRP hellos). The master sends the advertisement on multicast 224.0.0.18 protocol number 112 on a default interval of 1 second.

VRRP Transition Process

This subtopic describes the VRRP transition process.



The dynamic failover, when the active (master) becomes unavailable, uses three timers within VRRP: the advertisement interval, the master down interval, and the skew time.

- The advertisement interval is the time interval between advertisements (in seconds). The default interval is 1 second.
- The master down interval is the time interval for backup to declare the master down (in seconds). The default is $3 \times \text{advertisement interval} + \text{skew time}$.
- The skew time $(256 - \text{priority} / 256)$ ms, ensures that the backup router with the highest priority becomes the new master.

VRRP Transition Process

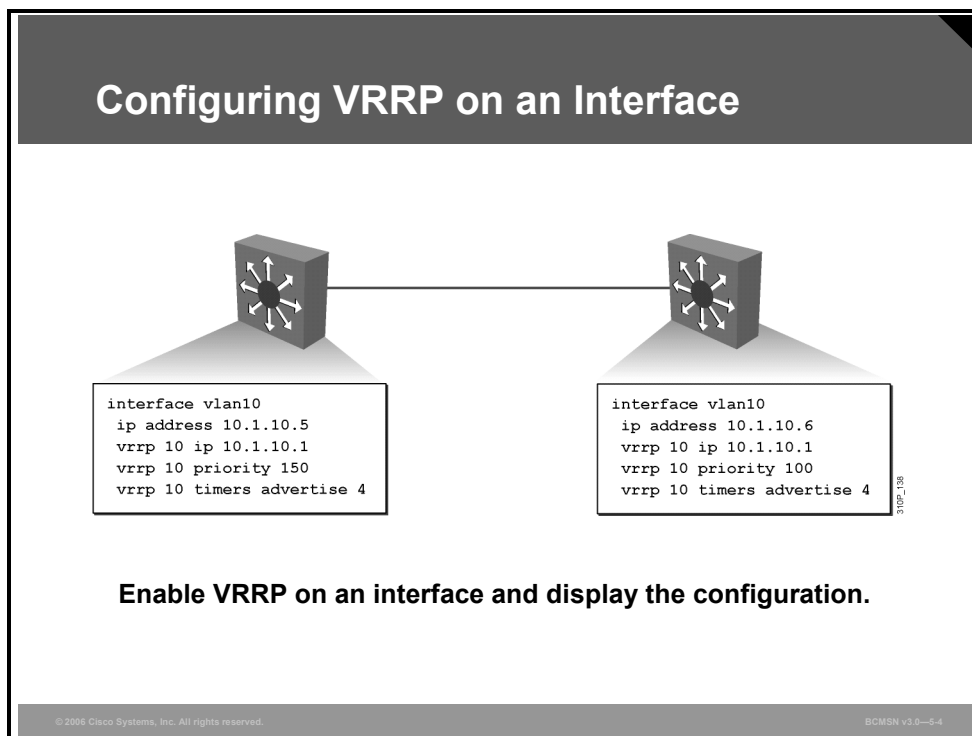
The table lists the steps involved in the VRRP transition.

Step	Description	Notes
1.	Router A is currently the master, so it is sending advertisements by default every 1 second.	Router A is the only device sending advertisements.
2.	Router A fails.	Advertisements stop.
3.	Router B and Router C stop receiving advertisements and wait for their respective master down interval to expire before transitioning to the master state.	By default, the master down interval is 3 seconds plus the skew time.
4.	Because the skew time is inversely proportional to priority, the master down interval of Router B is less than that of Router C. Router B has a master down interval of approximately 3.2 seconds. Router C has a master down interval of approximately 3.6 seconds.	The skew time for Router B equals $(256 - 200) / 256$, which is approximately equal to 0.2 seconds. The skew time for Router C equals $(256 - 100) / 256$, which is approximately equal to 0.6 seconds.
5.	Router B transitions to the master state after 3.2 seconds and starts sending advertisements.	
6.	Router C receives the advertisement from the new master, so it resets its master down interval and remains in the backup state.	

Note In the case of an orderly shutdown of the VRRP master, it sends an advertisement with a priority of 0. This priority setting then triggers the backup router to take over quicker by waiting only the skew time instead of the master down interval. Therefore, in the previous example, Router B would have waited only 0.2 seconds to transition to the master state.

Configuring VRRP

This topic describes the commands used to configure the VRRP and GLBP operations.



VRRP and GLBP are supported on select Cisco Catalyst platforms and, when supported, can be configured using these commands.

VRRP Commands

The table describes VRRP command parameters.

Command	Description
Switch(config-if)# vrrp <i>group-number</i> ip <i>virtual-gateway-addr</i>	Makes the interface a member of the virtual group identified with the IP virtual address.
Switch(config-if)# vrrp <i>group-number</i> priority <i>priority_value</i>	Sets the priority of this router. Highest value will win election as active router. Default is 100. If routers have the same VRRP priority, the gateway with the highest real IP address is elected to become the master virtual router.
Switch(config-if)# vrrp <i>group-number</i> timers advertise <i>timer-value</i>	Master router configures this parameter to advertise value to the other group members. Others configure timers learned to accept.
Switch(config-if)# vrrp <i>group-number</i> timers learn	Configures nonmaster members to learn timer values from master.

VRRP Implementation

The table describes how to configure VRRP.

Step	Description
1.	To enable VRRP on an interface: <code>Switch(config-if)#vrrp group-number ip virtual-gateway-address</code>
2.	To set a VRRP priority for this router for this VRRP group: <code>Switch(config-if)#vrrp group-number priority priority-value</code>
3.	To change timer and indicate if it should advertise (master) or learn (backup): <code>Switch(config-if)#vrrp group-number timers advertise timer-value</code> <code>Switch(config-if)#vrrp group-number timers learn</code>

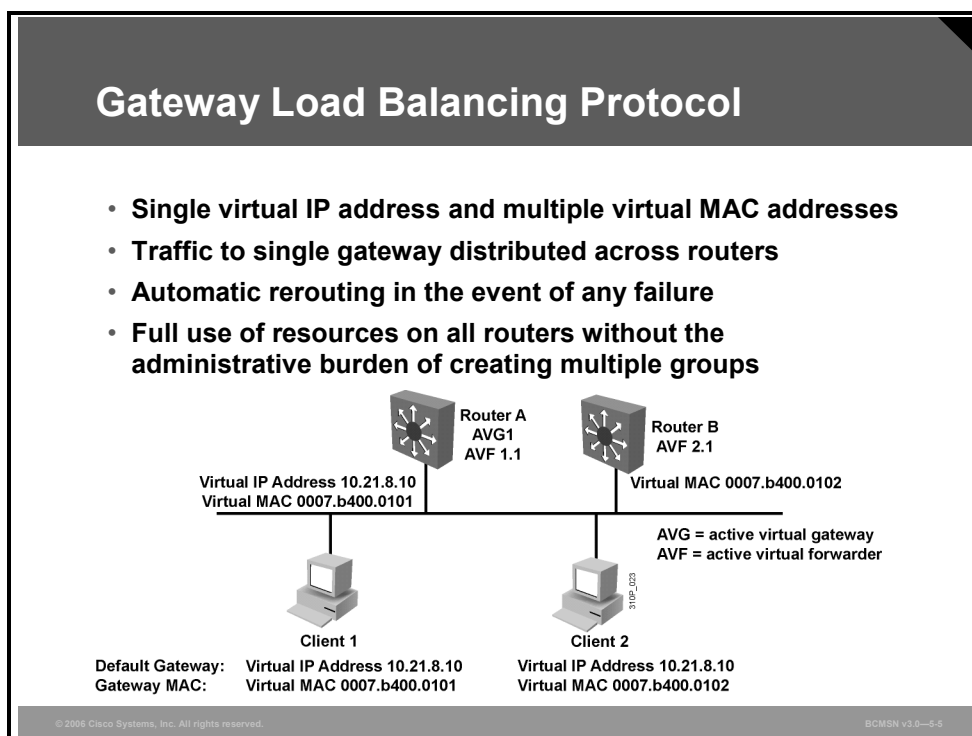
Example: VRRP Implementation

```
SwitchA(config)#interface vlan10
SwitchA(config-if)#ip address 10.1.10.5 255.255.255.0
SwitchA(config-if)#vrrp 10 ip 10.1.10.1
SwitchA(config-if)#vrrp 10 priority 150
SwitchA(config-if)#vrrp 10 timer advertise 4
```

```
SwitchB(config)#interface vlan10
SwitchB(config-if)#ip address 10.1.10.6 255.255.255.0
SwitchB(config-if)#vrrp 10 ip 10.1.10.1
SwitchB(config-if)#vrrp 10 priority 100
SwitchB(config-if)#vrrp 10 timer advertise 4
```

Describing the GLBP

This topic describes GLBP.



Although HSRP and VRRP provide gateway resiliency, for the standby members of the redundancy group, the upstream bandwidth is not used while the device is in standby mode.

Only the active router for HSRP and VRRP groups forwards traffic for the virtual MAC. Resources associated with the standby router are not fully utilized. Some load balancing can be accomplished with these protocols through the creation of multiple groups and through the assignment of multiple default gateways, but this configuration creates an administrative burden.

Cisco designed GLBP to allow automatic selection and simultaneous use of multiple available gateways in addition to automatic failover between those gateways. Multiple routers share the load of frames that, from a client perspective, are sent to a single default gateway address.

With GLBP, resources can be fully utilized without the administrative burden of configuring multiple groups and managing multiple default gateway configurations, as is required with HSRP and VRRP.

GLBP Functions

- **GLBP active virtual gateway (AVG):** Members of a GLBP group elect one gateway to be the AVG for that group. Other group members provide backup for the AVG in the event that the AVG becomes unavailable. The AVG assigns a virtual MAC address to each member of the GLBP group.
- **GLBP active virtual forwarder (AVF):** Each gateway assumes responsibility for forwarding packets that are sent to the virtual MAC address assigned to that gateway by the AVG. These gateways are known as AVFs for their virtual MAC address.
- **GLBP communication:** GLBP members communicate between each other through hello messages sent every 3 seconds to the multicast address 224.0.0.102, User Datagram Protocol (UDP) port 3222.

GLBP Features

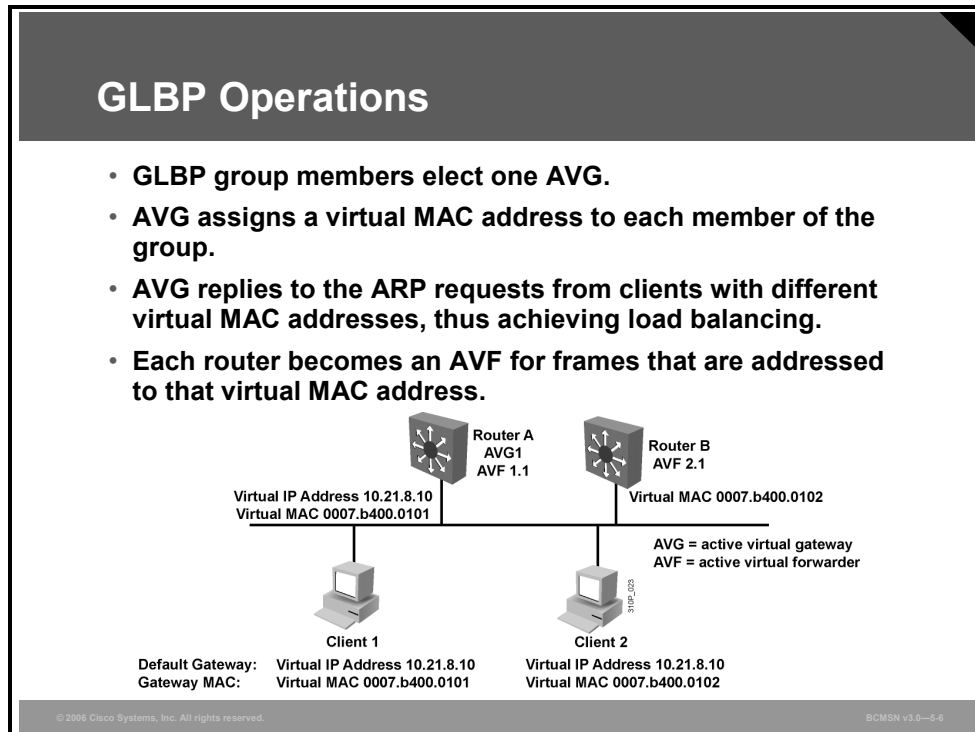
- **Load sharing:** You can configure GLBP in such a way that traffic from LAN clients can be shared by multiple routers, thereby sharing the traffic load more equitably among available routers.
- **Multiple virtual routers:** GLBP supports up to 1024 virtual routers (GLBP groups) on each physical interface of a router and up to four virtual forwarders per group.
- **Preemption:** The redundancy scheme of GLBP enables you to preempt an AVG with a higher priority backup virtual gateway that has become available. Forwarder preemption works in a similar way, except that forwarder preemption uses weighting instead of priority and is enabled by default.
- **Efficient resource utilization:** GLBP makes it possible for any router in a group to serve as a backup, which eliminates the need for a dedicated backup router because all available routers can support network traffic.

GLBP provides upstream load sharing by utilizing the redundant uplinks simultaneously. It uses link capacity efficiently, thus providing peak-load traffic coverage. By making use of multiple available paths upstream from the routers or Layer 3 switches running GLBP, output queues may also be reduced.

Only a single path is used with HSRP or VRRP, while others are idle, unless multiple groups and gateways are configured. The single path may encounter higher output queue rates during peak times, which leads to lower performance from higher jitter rates. The impact of jitter is lessened and over performance is increased because more upstream bandwidth is available, and additional upstream paths are used.

Identifying the GLBP Operations Process

This topic describes how GLBP provides balanced traffic on a per-host basis, using a round-robin scheme.



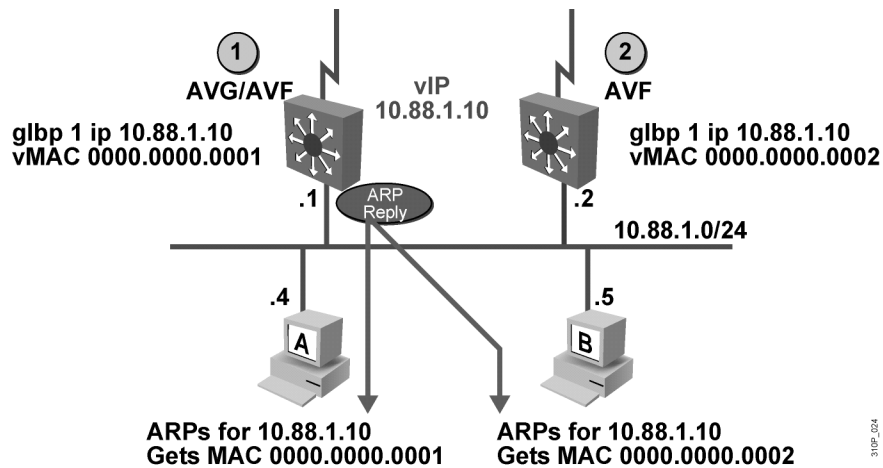
GLBP allows automatic selection and simultaneous use of all available gateways in the group. The members of a GLBP group elect one gateway to be the AVG for that group. Other members of the group provide backup for the AVG if it becomes unavailable. The AVG assigns a virtual MAC address to each member of the GLBP group. All routers become AVFs for frames addressed to that virtual MAC address. As clients send Address Resolution Protocol (ARP) requests for the address of the default gateway, the AVG sends these virtual MAC addresses in the ARP replies. A GLBP group can have up to four group members.

GLBP supports these operational modes for load balancing traffic across multiple default routers servicing the same default gateway IP address:

- **Weighted load-balancing algorithm:** The amount of load directed to a router is dependent upon the weighting value advertised by that router.
- **Host-dependent load-balancing algorithm:** A host is guaranteed to use the same virtual MAC address as long as that virtual MAC address is participating in the GLBP group.
- **Round-robin load-balancing algorithm:** As clients send ARP requests to resolve the MAC address of the default gateway, the reply to each client contains the MAC address of the next possible router in round-robin fashion. All routers' MAC addresses take turns being included in address resolution replies for the default gateway IP address.

GLBP automatically manages the virtual MAC address assignment, determines who handles the forwarding, and ensures that each station has a forwarding path in the event of failures to gateways or tracked interfaces. If failures occur, the load-balancing ratio is adjusted among the remaining AVFs so that resources are used in the most efficient way.

GLBP Operation



© 2006 Cisco Systems, Inc. All rights reserved.

BCMSN v3.0-3.7

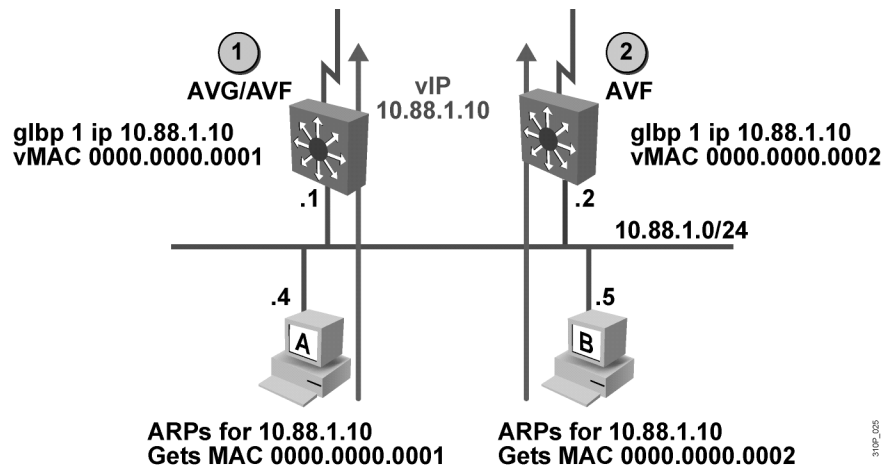
As shown in the figure, by default, GLBP will attempt to balance traffic on a per-host basis, using the round-robin algorithm.

GLBP Per-Host Traffic Balancing

The table describes how GLBP balances traffic using the round-robin algorithm.

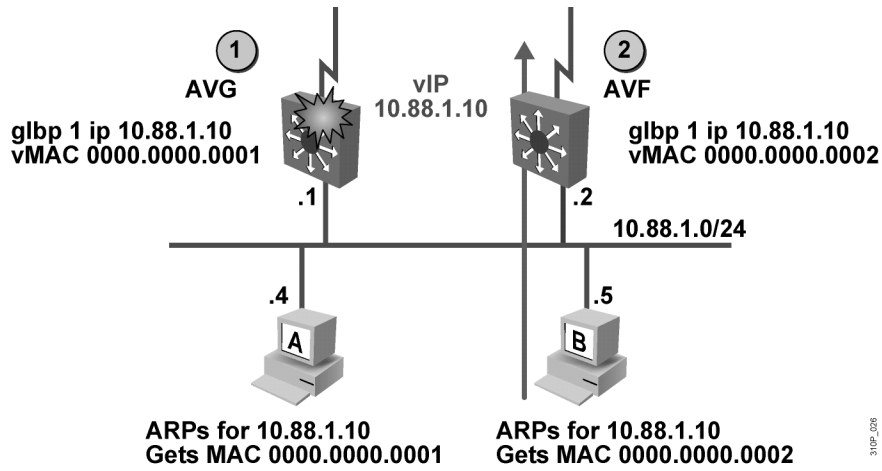
Step	Description
1.	When a client sends an ARP message for the gateway IP address, the AVG returns the virtual MAC address of one of the AVFs.
2.	When a second client sends an ARP message, the AVG returns the next virtual MAC address from the list.

GLBP Operation (Cont.)



Having each resolved a different MAC address for the default gateway, clients A and B will send their routed traffic to separate routers, although they both have the same default gateway address configured. Each GLBP router is an AVF for the virtual MAC address to which it has been assigned.

GLBP Interface Tracking

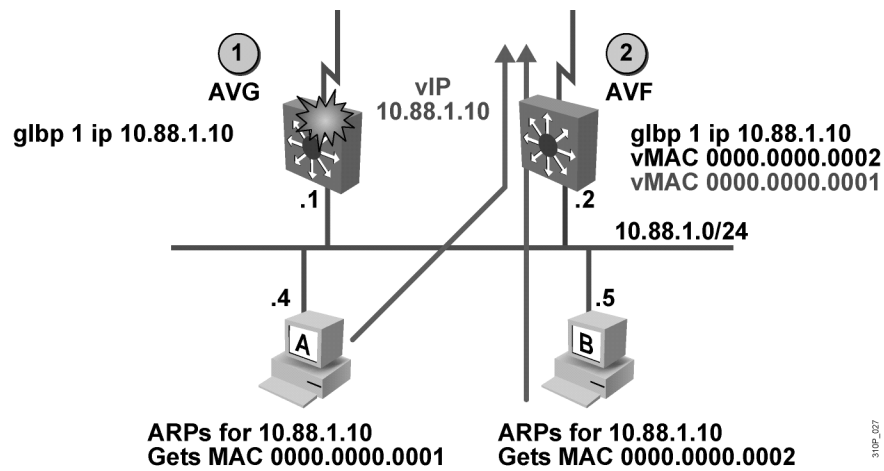


© 2006 Cisco Systems, Inc. All rights reserved.

BCMSN v3.0-5-8

Like HSRP, GLBP can be configured to track interfaces. In the figure, the WAN link from router R1 is lost. GLBP detects the failure.

GLBP Interface Tracking (Cont.)

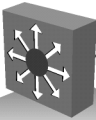


Because interface tracking was configured on R1, the job of forwarding packets for virtual MAC address 0000.0000.0001 will be taken over by the secondary virtual forwarder for the MAC, router R2. Therefore, the client sees no disruption of service nor does the client need to resolve a new MAC address for the default gateway.

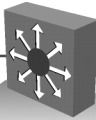
GLBP Implementation

This subtopic describes the process used to implement GLBP.

Configuring GLBP on an Interface



```
interface vlan7
ip address 10.1.7.5
glbp 7 ip 10.1.7.1
glpb 7 priority 150
glbp 7 timers msec 200 msec 700
```



```
interface vlan7
ip address 10.1.7.6
glbp 7 ip 10.1.7.1
glpb 7 priority 100
glbp 7 timers msec 200 msec 700
```

Enable GLBP on an interface and display the configuration.

© 2006 Cisco Systems, Inc. All rights reserved.
BCMSN v3.0—5-11

GLBP Commands

The table describes GLBP command parameters.

Command	Description
Switch(config-if)# glbp <i>group-number</i> ip <i>virtual-gateway-addr</i>	Makes the interface a member of the virtual group identified with the IP virtual address.
Switch(config-if)# glbp <i>group-number</i> priority <i>priority_value</i>	Sets the priority of this router. Highest value will win election as active router. Default is 100. If routers have the same GLBP priority, the gateway with the highest real IP address will become the AVG.
Switch(config-if)# glbp <i>group-number</i> timers <i>hello-value</i> <i>holdtime-value</i>	Adjusts the hellotimer and holdtimer in seconds. Place the argument <i>msec</i> before the values to enter subsecond values.

GLBP Implementation

The table describes the steps needed to configure GLBP.

Step	Description
1.	Enable GLBP on an interface. Switch(config-if)# glbp group-number ip virtual-gateway-address
2.	Set a GLBP priority for this router for this GLBP group. Switch(config-if)# glbp group-number priority priority-value
3.	Change timer values for hello interval and holdtime. Switch(config-if)# glbp group-number timers hello holdtime

Example: GLBP Implementation

```
SwitchA(config)#interface vlan7
SwitchA(config-if)#ip address 10.1.7.5 255.255.255.0
SwitchA(config-if)#glbp 7 ip 10.1.7.1
SwitchA(config-if)#glbp 7 priority 150
SwitchA(config-if)#glbp 7 timers msec 250 msec 750
```

```
SwitchB(config)#interface vlan7
SwitchB(config-if)#ip address 10.1.7.6 255.255.255.0
SwitchB(config-if)#glbp 7 ip 10.1.7.1
SwitchB(config-if)#glbp 7 priority 100
SwitchB(config-if)#glbp 7 timers msec 250 msec 750
```

Summary

This topic summarizes the key points discussed in this lesson.

Summary

- **VRRP provides router redundancy in a manner similar to HSRP.**
- **VRRP supports a master and one or more backup routers.**
- **VRRP and GLBP are configured per interface.**
- **GLBP provides router redundancy and load balancing.**
- **GLBP balances traffic by allocating a virtual MAC address to each AVF.**

Module Summary

This topic summarizes the key points discussed in this module.

Module Summary

- **HSRP is enabled so that redundant routers can provide default gateway functionality.**
- **HSRP can be tuned to provide subsecond failover to a standby router.**
- **VRRP or GLBP can provide Layer 3 router failover in addition to load balancing at the distribution layer.**

© 2006 Cisco Systems, Inc. All rights reserved. BOMSN v3.0—5-1

Device, link, or hardware component redundancy at strategic points in the network leads to high availability. Hot Standby Router Protocol (HSRP) provides router redundancy to network hosts and can be optimized in several ways. Virtual Router Redundancy Protocol (VRRP) and Gateway Load Balancing Protocol (GLBP) were derived from HSRP, providing additional redundancy features.

References

For additional information, refer to these resources:

- Cisco Systems, Inc., *Hot Standby Router Protocol Features and Functionality*:
http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094a91.shtml#hsrpdebug
- Cisco Systems, Inc., *Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services*:
http://www.cisco.com/application/pdf/en/us/guest/products/ps5207/c2001/ccmigration_09186a0080238b7d.pdf

Module Self-Check

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

- Q1) During which three HSRP states do routers send hello messages? (Choose three.) (Source: Configuring Layer 3 Redundancy with HSRP)
- A) initial
 - B) listen
 - C) speak
 - D) active
 - E) standby
- Q2) Which command enables HSRP? (Source: Configuring Layer 3 Redundancy with HSRP)
- A) standby virtual ip 10.1.1.1
 - B) standby ip 10.1.1.1 group 1
 - C) hsrp 1 ip 10.1.1.1
 - D) standby 1 ip 10.1.1.1
- Q3) During the election process, if all routers on VLAN10 have the same HSRP priority, which router will become the active router? (Source: Optimizing HSRP)
- A) the router with the highest configured IP address on any interface
 - B) the router with the lowest configured IP address on interface VLAN10
 - C) the router with the highest configured IP address on interface VLAN10
 - D) the router with the lowest configured IP address on any interface
- Q4) Which command enables preempt with a delay of 2 minutes? (Source: Optimizing HSRP)
- A) **standby 1 preempt delay minutes 2**
 - B) **hsrp 1 delay 120**
 - C) **standby 1 delay preempt 120**
 - D) **standby 1 preempt delay minimum 120**
- Q5) With VRRP, which command would be used in order for advertisements to be generated every 3 seconds? (Source: Configuring Layer 3 Redundancy with VRRP and GLBP)
- A) **vrrp 1 timers 3 10**
 - B) **vrrp 1 timers advertise 3**
 - C) **vrrp 1 timers advertise msec 3**
 - D) **vrrp 1 timers 3**

Module Self-Check Answer Key

- Q1) C, D, E
- Q2) D
- Q3) C
- Q4) D
- Q5) B

Wireless LANs

Overview

This module introduces wireless LANs (WLANs). WLAN is an access technology that has an increasing significance for network access in offices, factories, hotels, airports, and at home. This module explains the differences between wired and wireless LANs, describes WLAN topologies, and teaches you how to implement Cisco Systems WLAN solutions.

Module Objectives

Upon completing this module, you will be able to describe WLANs. This ability includes being able to meet these objectives:

- Describe basic WLAN features and compare WLANs with wired LANs
- Distinguish between the different WLAN topologies
- Explain WLAN technology, standards, and WLAN security
- Use Cisco utilities to configure the Cisco WLAN client
- Distinguish between autonomous and lightweight WLAN implementations, and describe PoE and WLAN antennas
- Configure autonomous and lightweight Cisco WLAN solutions

Introducing WLANs

Overview

This lesson introduces wireless LANs (WLANs). WLAN is an access technology that has an increasing significance for network access in offices, factories, hotels, airports, and at home.

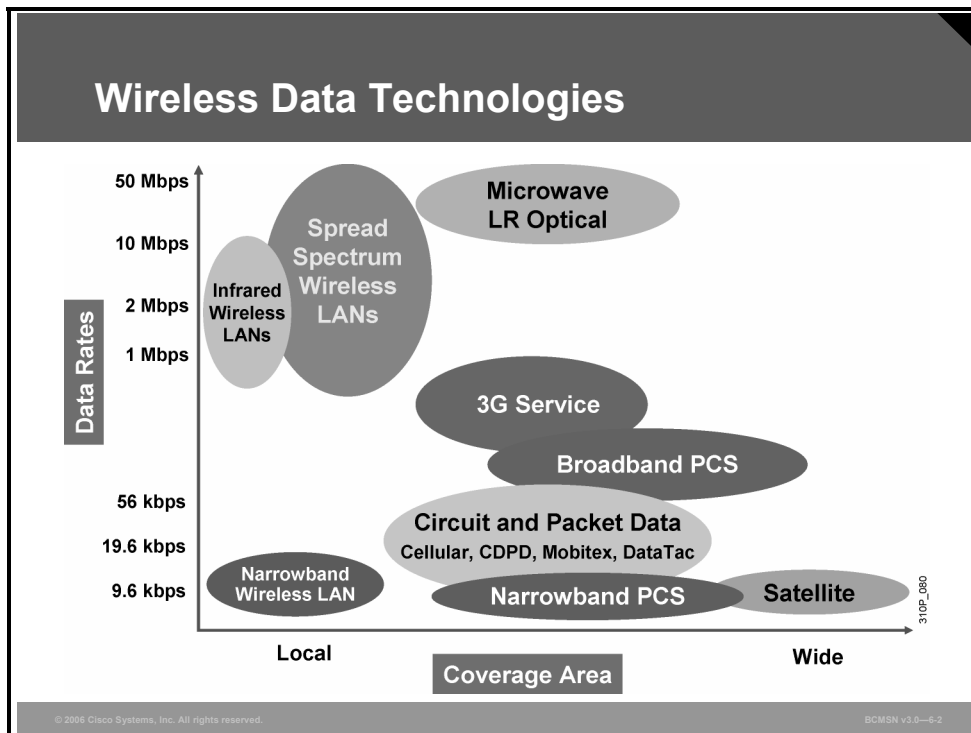
Objectives

Upon completing this lesson, you will be able to describe basic WLAN features and compare WLANs with wired LANs. This ability includes being able to meet these objectives:

- Describe the different wireless data technologies that are currently available
- Describe WLANs
- Distinguish WLANs from other wireless data networks
- Describe similarities and differences between WLANs and wired LANs

Wireless Data Technologies

This topic describes different wireless data technologies.



There are many different types of wireless data communications. Each of these has its particular characteristics. Range, data rate, and cost differ between these technologies.

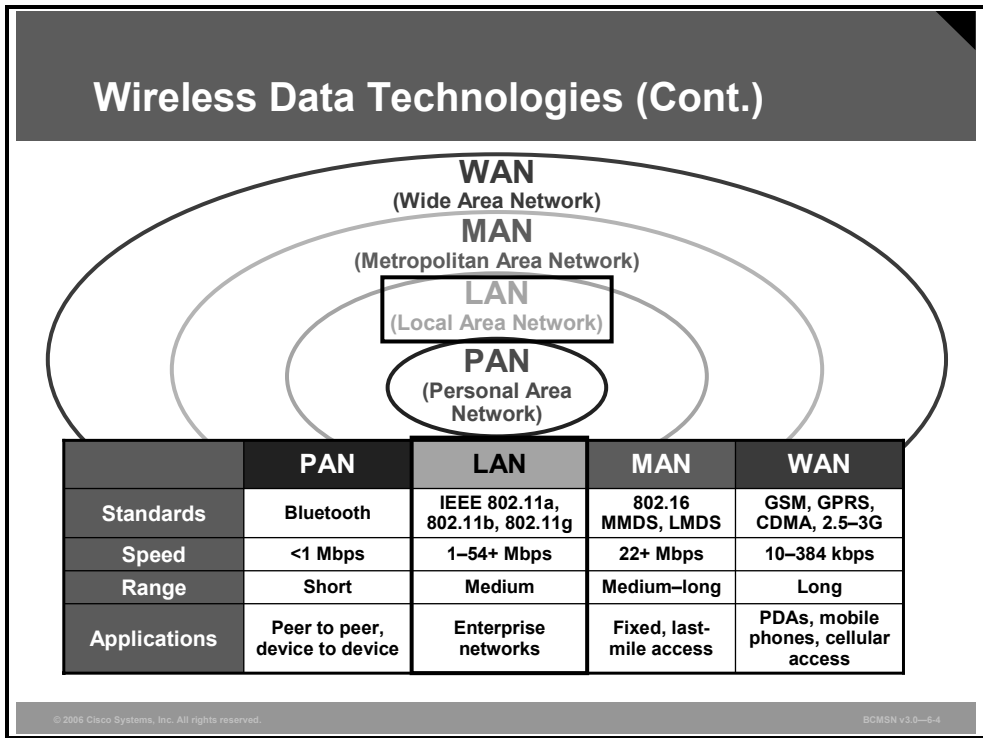
Characteristics of Wireless Data Technologies

This table describes the characteristics of various types of wireless data technologies.

Wireless Technology	Characteristics
Infrared (IR)	Very high data rates, low cost, very short distance
Narrowband	Low data rates, medium cost, limited distance, license required
Spread spectrum	High data rates, medium cost, limited to campus coverage
Personal communication service (PCS)	Low data rates, medium cost, citywide coverage
3G service	Mobile phone data technologies, medium cost, worldwide coverage
Cellular, Cellular Digital Packet Data (CDPD), Mobitex, DataTAC	Low data rates, flat monthly rate, national coverage
Microwave transmissions	Wireless data link using microwaves, medium range, high data rates possible, license required
Long range (LR) optical transmissions	Data link using laser transmission, short range, high data rates

Wireless Technologies

This subtopic distinguishes wireless technologies for different types of networks.



Many different types of wireless technologies for networks are offered today. Each of these technologies provides different coverage. Starting with the smallest coverage area, these networks are as follows:

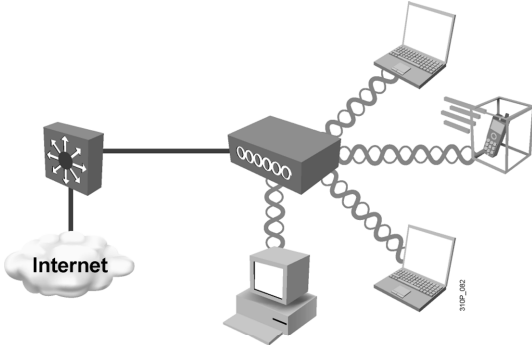
- Personal area network (PAN):** PAN wireless networks are typically designed to cover your personal work space. Radios are typically low powered and do not deliver options in antenna selection, thus limiting the size of the coverage area (typically less than 20 feet of radius). One example of a PAN network is Bluetooth. Good applications of this technology are communications between a PC and its peripherals or between a wireless phone and its headset. In the PAN wireless network, the customer owns 100 percent of the network; therefore there are no airtime charges.
- Local area network (LAN):** LAN wireless networks are designed to be enterprise-based, allowing for complete enterprise applications to be used without wires. Typically, WLANs deliver Ethernet capable speeds (up to 54 Mbps). In the WLAN, the customer owns 100 percent of the network; therefore no airtime charges are incurred.
- Metropolitan area networks (MAN):** MAN wireless networks are deployed inside a metropolitan area, allowing wireless connectivity throughout an urban area. Wireless MANs typically deliver up to broadband speeds (similar to DSL) but are not capable of Ethernet speeds. In the MAN, the wireless networks can either be provided by a licensed carrier that requires the customer to purchase airtime, or they may be built out and supported by one entity, such as a police department. Examples of MANs are multichannel multipoint distribution service (MMDS) and local multipoint distribution service (LMDS).
- Wide area networks (WAN):** The WAN wireless networks are typically slower in speed but have more coverage, sometimes covering rural areas. Due to the vast deployment, all WAN wireless networks require customers to purchase airtime for data transmission. Examples of WANs are general packet radio service (GPRS), code division multiple access (CDMA), and personal digital assistants (PDAs).

Wireless LANs

This topic introduces the concept of WLAN.

Wireless LAN (WLAN)

- **A WLAN is a shared network.**
- **An access point is a shared device and functions like a shared Ethernet hub.**
- **Data is transmitted over radio waves.**
- **Two-way radio communications (half-duplex) are used.**
- **The same radio frequency is used for sending and receiving (transceiver).**



© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0-6-5

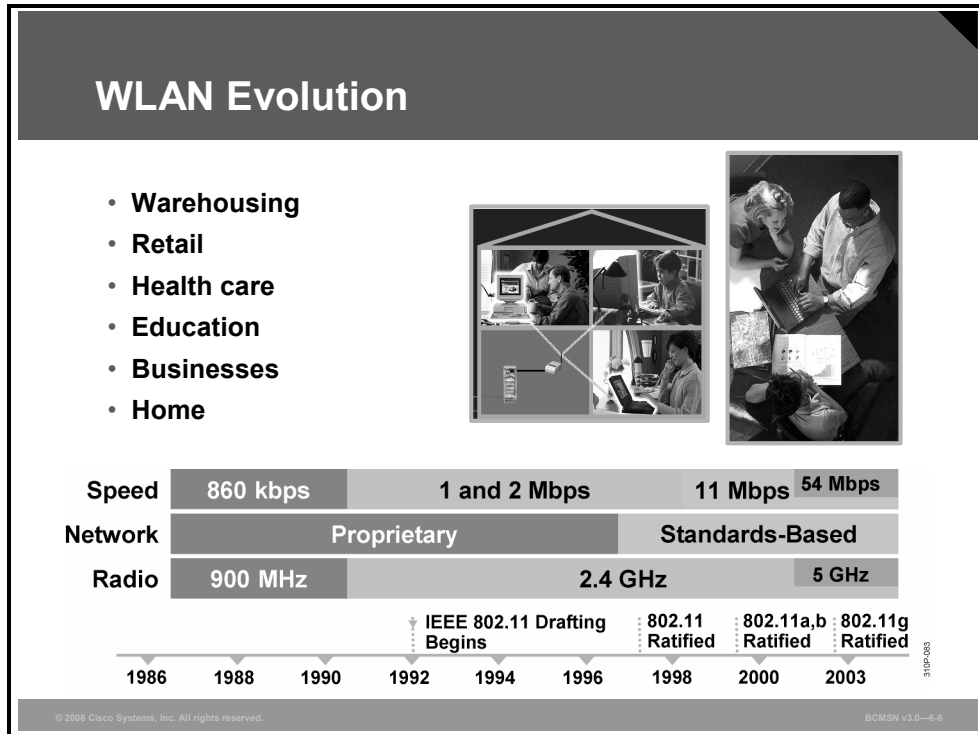
WLANs are similar to Ethernet networks in many ways. A WLAN is a shared network. An access point is a shared device and functions like a shared Ethernet hub. In the wireless cell, only one station can transmit at any time; all other stations listen. A station that wants to transmit must wait until the wireless media is not in use by another station.

This transmission setup is similar to that of a coaxial cable or half-duplex Ethernet and an Ethernet hub. Therefore, the performance of a wireless access point is similar to that of a hub. The average data rate per station is total bandwidth divided by the number of stations. The actual data throughput experienced by the wireless clients will be even less due to wireless-specific issues.

In WLANs, data is transmitted over radio waves. WLAN signals are similar to two-way radio communications. WLAN signals use the same frequency for transmitting and receiving (half-duplex). This setup means that a station that is transmitting cannot receive while it is transmitting. Therefore, only half-duplex transmission is possible. This transmission setup is similar to coaxial cable Ethernet.

Wireless LAN Evolution

This subtopic explains the evolution of WLANs from proprietary systems to the standardized WLAN systems of today.



The WLAN evolution started in the 1980s 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 manufacturers of WLAN products to engineer new products for the 2.4-GHz band.

The move to 2.4 GHz in the 1990s put WLAN products into a “cleaner” radio frequency (RF) environment, making it possible to deploy data collection systems without interference from 900-MHz transmissions. The 2.4-GHz technology was also well received because the throughput grew from 860 kbps to 1 Mbps and 2 Mbps.

When frequency and speeds are increased, distances are decreased, but the new data collection opportunities that the faster throughput helped to create justified the extra access points that were needed. However, end users were still concerned about using a proprietary system. In 1992, the IEEE began drafting the 802.11 standard to eliminate the issue of proprietary technology and design an open standard for WLAN.

In July 1997, the IEEE ratified the 2.4-GHz standard that included DSSS technology at the physical layer. This standard specified 1 Mbps as the standard speed and 2 Mbps as a “turbo” mode.

In September 1999, the IEEE 802.11a standard (5 GHz at 54 Mbps) and the IEEE 802.11b standard (2.4 GHz at 11 Mbps) were ratified by the IEEE. In June 2003, the IEEE ratified the 802.11g standard (2.4 GHz at 54 Mbps). This standard is backward-compatible with 802.11b systems because both standards use the same 2.4-GHz frequency band.

WLANs and Other Wireless Technologies

This topic distinguishes WLANs from other wireless technologies.

What Are WLANs?

They are: <ul style="list-style-type: none">• Local• In building or campus for mobile users• Radio or infrared• Not required to have RF licenses in most countries• Using equipment owned by customers	They are not: <ul style="list-style-type: none">• WAN or MAN networks• Cellular phones networks• Packet data transmission via cellular phone networks<ul style="list-style-type: none">– Cellular digital packet data (CDPD)– General packet radio service (GPRS)– 2.5G to 3G services
--	---

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0-6-7

WLANs are designed for a local network, not a WAN. They are intended for in-building wireless networks, line-of-sight outdoor bridging applications, or a combination of both. They are not designed for city-wide wireless networks.

No license is required for the WLAN in most countries.

A WLAN is not a cellular phone network. It does not provide packet data transmission for cellular phone networks.

WLANS and LANs

This topic compares WLANs and wired LANs.

Similarities Between WLAN and LAN

- **A WLAN is an 802 LAN.**
 - Transmits data over the air vs. data over the wire
 - Looks like a wired network to the user
 - Defines physical and data link layer
 - Uses MAC addresses
- **The same protocols/applications run over both WLANs and LANs.**
 - IP (network layer)
 - IPSec VPNs (IP-based)
 - Web, FTP, SNMP (applications)

© 2006 Cisco Systems, Inc. All rights reserved. BOMS v3.0—6-9

Similarities Between WLANs and LANs

WLANs are 802 LANs. The data in WLANs is sent over radio waves. In wired LANs, the data is sent over wires. But the network interface of WLANs looks similar to wired LANs for the user.

Both WLANs and wired LANs define the physical and data link layers and use MAC addresses. The same protocols and applications can be used over LANs and WLANs. Examples of such protocols are the IP and IP Security (IPSec) protocol for virtual private networks (VPNs). Examples of applications are web, FTP, and Simple Network Management (SNMP) management.

Differences Between WLANs and LANs

This subtopic explains the differences between WLANs and wired LANs.

Differences Between WLAN and LAN

- **WLANs use radio waves as the physical layer.**
 - **WLANs use CSMA/CA instead of CSMA/CD to access the network.**
- **Radio waves have problems that are not found on wires.**
 - **Connectivity issues.**
 - **Coverage problems**
 - **Multipath issues**
 - **Interference, noise**
 - **Privacy issues.**
- **WLANs use mobile clients.**
 - **No physical connection.**
 - **Battery-powered.**
- **WLANs must meet country-specific RF regulations.**

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0-6-9

Here is an explanation of how WLANs differ from LANs.

- In WLANs, radio frequencies are used as the physical layer of the network.
 - WLANs use carrier sense multiple access collision avoidance (CSMA/CA) instead of carrier sense multiple access collision detection (CSMA/CD), which is used by Ethernet LANs. Collision detection is not possible because a sending station cannot receive at the same time that it is transmitting and, therefore, cannot detect a collision. Instead, the Request To Send (RTS) and Clear To Send (CTS) protocols are used to avoid collisions.
 - WLANs use a different frame format than wired Ethernet LANs. Additional information for WLANs is required in the Layer 2 header of the frame.
- Radio waves have problems not found in wires.
 - Connectivity issues in WLANs can be caused by coverage problems, RF transmission, multipath distortion, and interference from other wireless services or other WLANs.
 - Privacy issues are possible because radio frequencies can reach outside the facility.
- In WLANs, mobile clients are used to connect to the network.
 - Mobile clients do not have a physical connection to the network.
 - Mobile devices are often battery powered as opposed to being electrically powered as they are for LANs.
- WLANs must meet country-specific RF regulations.
 - The aim of standardization is to make WLANs available worldwide. Because WLANs use radio frequencies, they must follow country-specific regulations for RF power and frequencies. This requirement does not apply to wired LANs.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

- **Different wireless data technologies with different characteristics are available.**
- **WLANs were introduced to provide local connectivity with higher data rates.**
- **WLANs use half-duplex transmission.**
- **WLANs have similarities and differences compared to wired LANS.**

Describing WLAN Topologies

Overview

This lesson explains different wireless LAN (WLAN) topologies. WLAN topologies refer to the placement and application of WLANs.

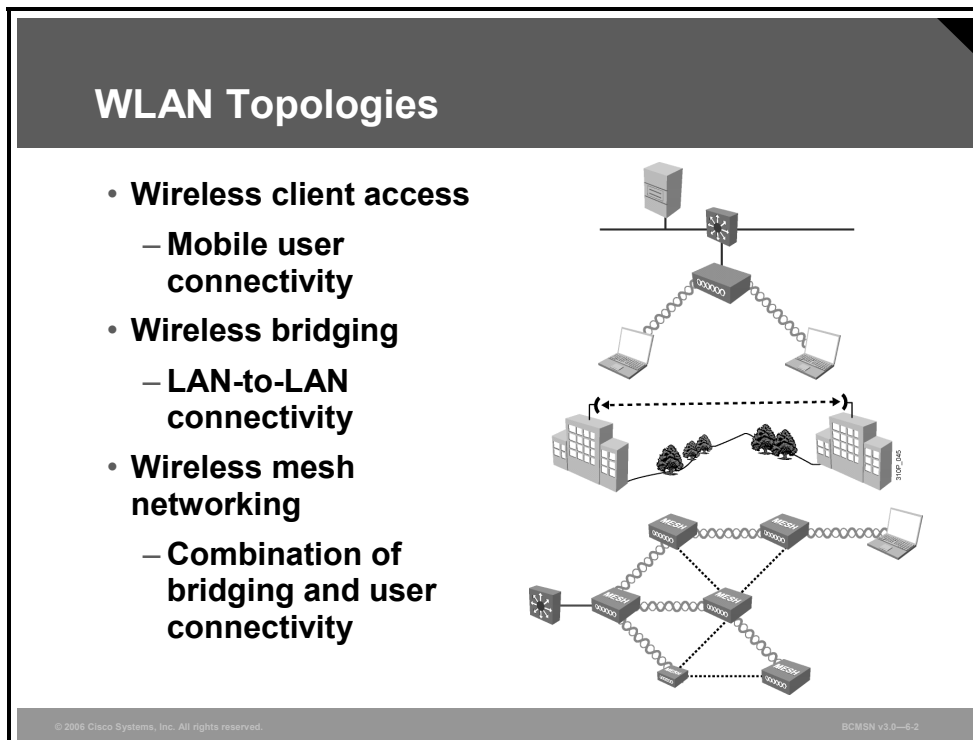
Objectives

Upon completing this lesson, you will be able to distinguish between the different WLAN topologies. This ability includes being able to meet these objectives:

- Describe types of WLAN topologies
- Describe WLAN access topologies
- Explain roaming between wireless cells
- Describe WLAN support for VLANs and QoS
- Describe wireless mesh networking

WLAN Topologies

This topic explains general WLAN topologies.



WLANs replace the Layer 1 transmission medium of a traditional wired network (usually Category 5 cable) with radio transmission over the air. Cisco Aironet wireless products fit into three main categories:

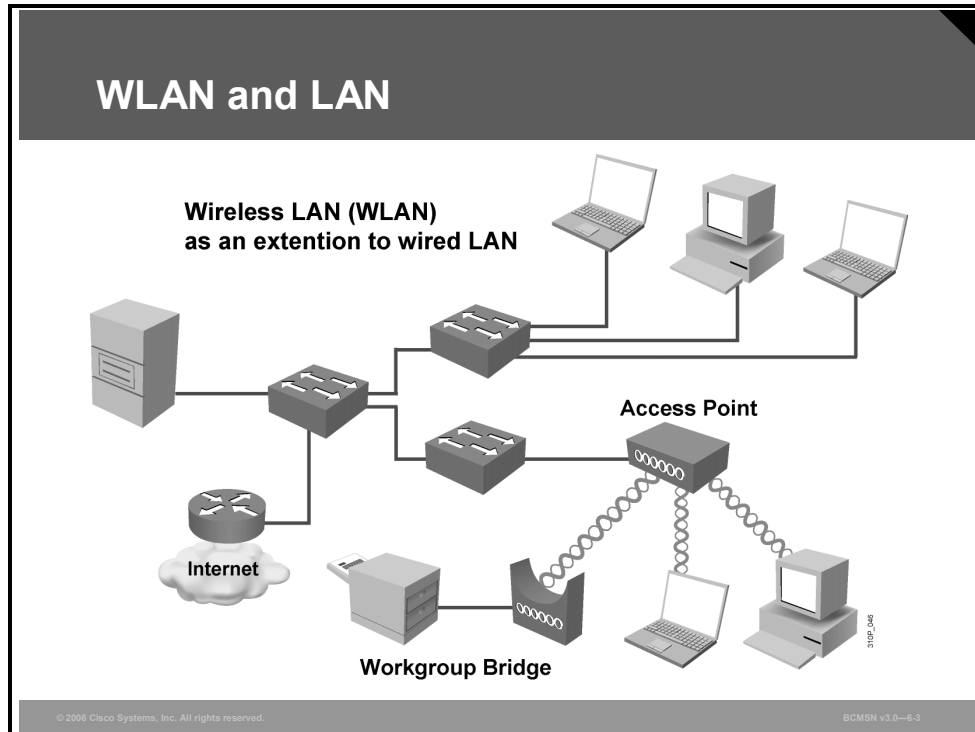
- **Wireless in-building LANs for client access:** Cisco Aironet WLAN products can plug into a wired network and function as an overlay to traditional or wired LANs, or they can be deployed as standalone LANs where wired networking is not feasible. WLANs permit the use of desktop and portable computers or specialty devices in a system where connection to the network is essential.

A computer with a wireless network interface card (NIC) can connect to the wired LAN through the access point. Properly deployed WLANs can provide instant access to the network from anywhere in facility. Users can roam without losing their network connection.

- **Wireless building-to-building bridges:** 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 required for dedicated cable or T1 lines. Wireless bridges also allow wireless NIC connections in the same fashion as access points.
- **Wireless mesh networking:** Mesh networking is a superset of the previously defined categories. Mesh networks provide dynamic, redundant, fault-tolerant links for building and client access.

Wired and Wireless LAN

This subtopic explains WLAN as an extension to wired LAN.



Wired LANs require that users locate in one place and stay there. WLANs are an extension to the wired LAN network. A WLAN can be an overlay to, or substitute for, a traditional wired LAN network.

With Cisco Aironet WLANs, mobile users can:

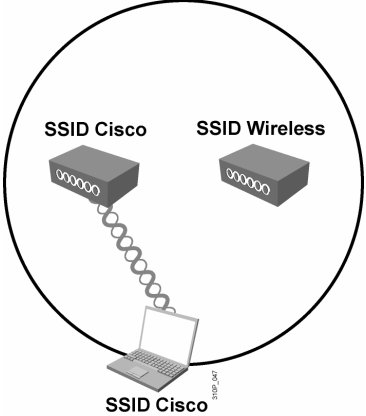
- Move freely around a facility
- Enjoy real-time access to the wired LAN at wired Ethernet speeds
- Access all the resources of wired LANs

Service Set Identifier

This subtopic explains how the Service Set Identifier (SSID) is used in wireless networks.

Service Set Identifier (SSID)

- **SSID is used to logically separate WLANs.**
- **The SSID must match on client and access point.**
- **Access point broadcasts one SSID in beacon.**
- **Client can be configured without SSID.**
- **Client association steps:**
 1. **Client sends probe request.**
 2. **A point sends probe response.**
 3. **Client initiates association.**
 4. **A point accepts association.**
 5. **A point adds client MAC address to association table.**



The diagram illustrates a wireless network setup. Two access points are shown at the top, one labeled 'SSID Cisco' and the other 'SSID Wireless'. Below them, a laptop is shown with the label 'SSID Cisco' next to it. A dotted line connects the 'SSID Cisco' access point to the laptop, indicating a logical connection. The entire setup is enclosed in a large circle.

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0-6-4

The SSID is the name of the wireless cell. It is used to logically separate WLANs. It must match exactly between the client and the access point.

The access point broadcasts the SSID in the beacons. Beacons are broadcasts that the access points send to announce the available services. Therefore, clients can be configured without an SSID (null-SSID), detect all access points, and learn the SSID from the beacons of the access point.

SSID broadcasts can be disabled on the access point, but this approach does not work if the client needs to see the SSID in the beacon.

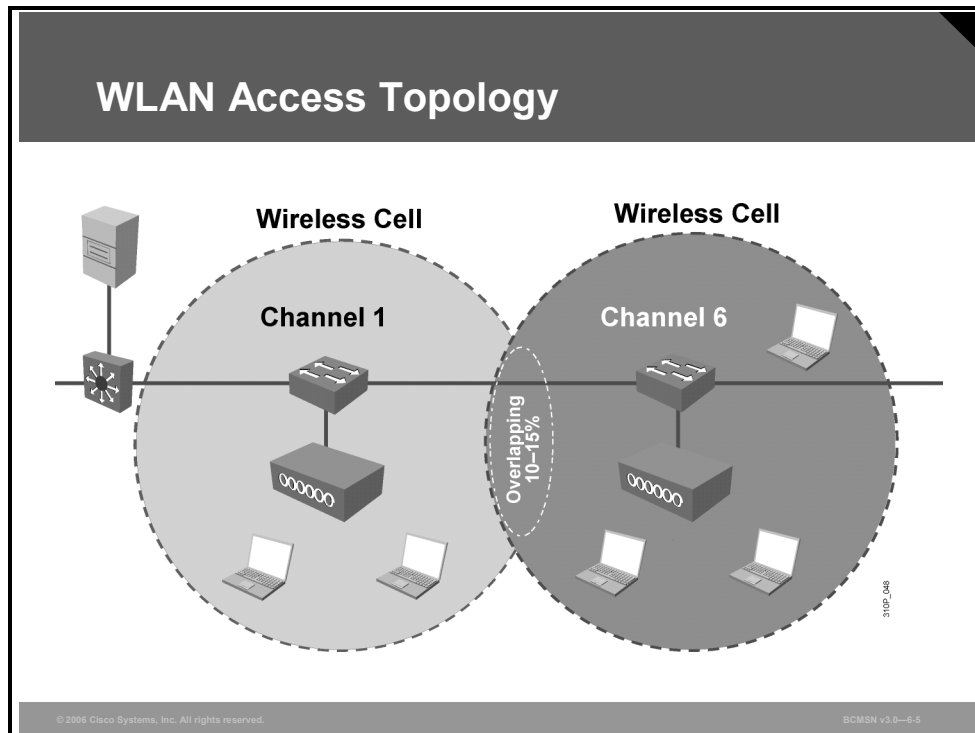
Client Association Steps

The table shows how the client associates to the access point.

Step	Action
1.	Client sends probe request.
2.	Access point sends probe response or beacon.
3.	Client initiates association process.
4.	Access point accepts association of the client.
5.	Access point adds client MAC address to association table.

Typical WLAN Topologies

This topic explains the WLAN topologies used for wireless client access.



This figure shows the WLAN topology for wireless client access.

The basic service area is the area of radio frequency (RF) coverage provided by an access point. This area is also referred to as a “microcell.” To extend the basic service area, or to simply add wireless devices and extend the range of an existing wired system, you can add an access point. As the name “access point” indicates, this device 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 with the access point.

If a single cell does not provide enough coverage, any number of cells can be added to extend the range. This range is known as an extended service area.

It is recommended that the extended service area cells have 10 to 15 percent overlap to allow remote users to roam without losing RF connections. For wireless voice networks, an overlap of 15 to 20 percent is recommended.

Bordering cells should be set to different nonoverlapping channels for best performance.

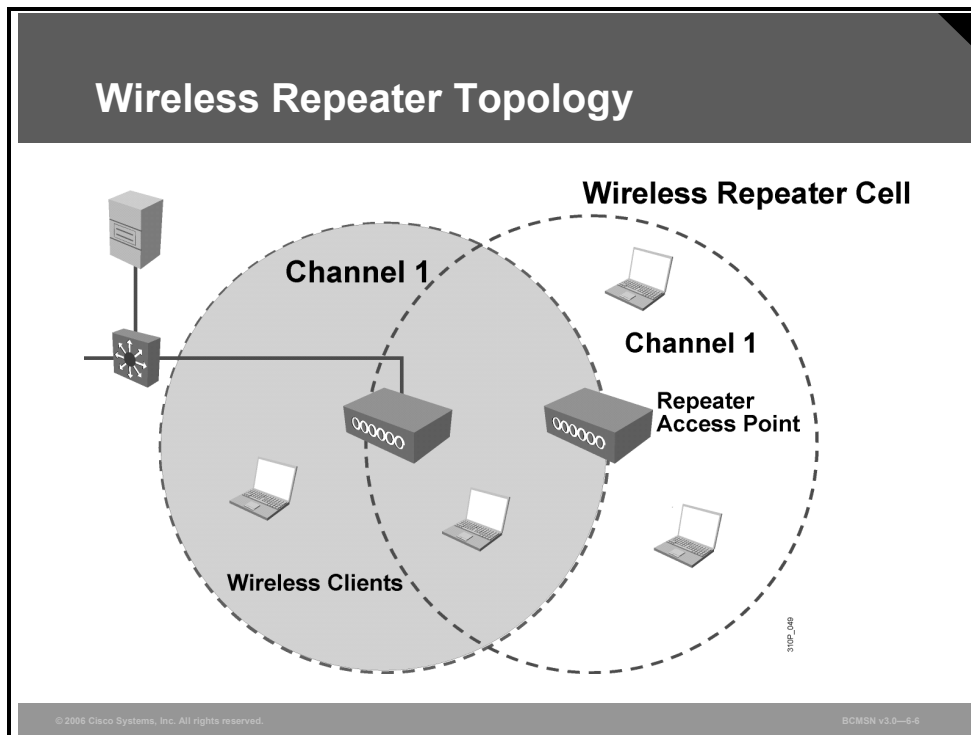
More recently, wireless deployments have moved from “microcell” to “pico cell.” Pico cells further reduce access point coverage area by reducing power and increasing the total number of access points deployed.

The resulting benefits are better coverage, less interference, higher data rates, and fault tolerance through convergence. When an adjacent access point goes down, the neighboring access points expand their coverage by increasing their RF power to cover the area that is lost by the access point that went down.

It is important that not only the access points can reduce their transmit power settings but also the clients can reduce their transmit power. Both access points and clients should use a comparable transmit power so that the client associates to the nearest access point.

Wireless Repeater Topology

This subtopic explains the use of an access point as a wireless repeater.



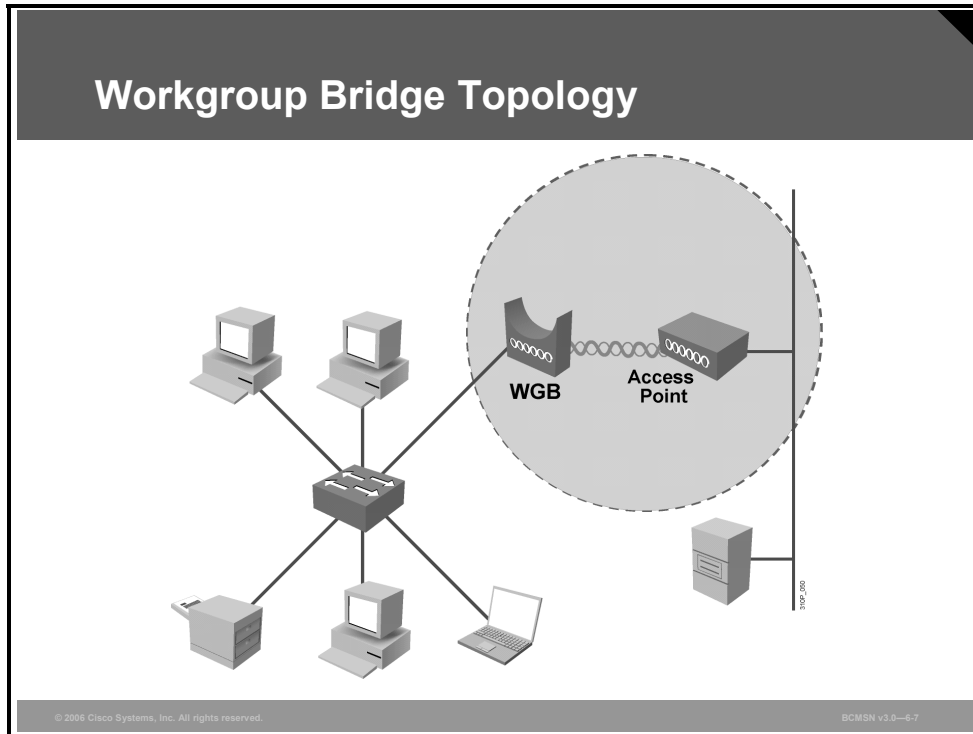
In an environment where you need extended coverage but access to the wired LAN is not practical or available, you can use a wireless repeater. A wireless repeater is simply an access point that is not connected to the wired LAN. This topology requires a 50 percent overlap of the access point on the wired LAN and the wireless repeater. The receive-and-retransmit time involved decreases the throughput by approximately half.

The SSID of the root access point must be configured on the repeater access point. The repeater access point uses the same channel as the root access point.

Note Not all implementations support this feature.

Work Group Bridge Topology

This subtopic explains the workgroup bridge (WGB) topology.



The Cisco Aironet WGB connects to the Ethernet port of a device that does not have a WLAN NIC via Peripheral Component Interconnect (PCI), an available Personal Computer Memory Card International Association (PCMCIA) slot or USB, or the software for a WLAN.

The Cisco Aironet WGB 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 with an autonomous Cisco Aironet Access Point or Cisco Aironet Bridge in access point mode. The Cisco Aironet WGB does not operate with access points of other vendors.

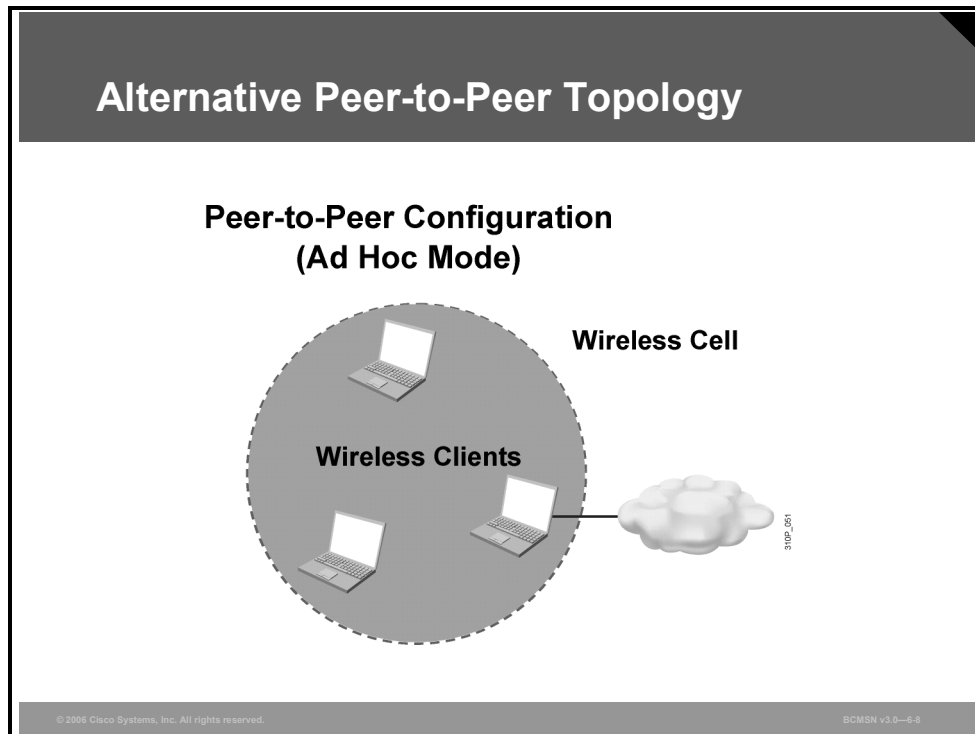
Another configuration of the WGB allows wired machines to be attached to the same radio device. This configuration is ideal for connecting remote workgroups to a wired LAN.

To use a WGB with multiple MAC addresses, you must connect the WGB to a hub with an Ethernet patch cable. All users must connect to the hub. If the WGB is connected directly to an Ethernet client node, then an Ethernet crossover cable must be used.

Note Not all WLAN implementations support this topology.

Peer-to-Peer Topology

This subtopic explains the ad hoc mode of wireless clients as an alternative WLAN topology.



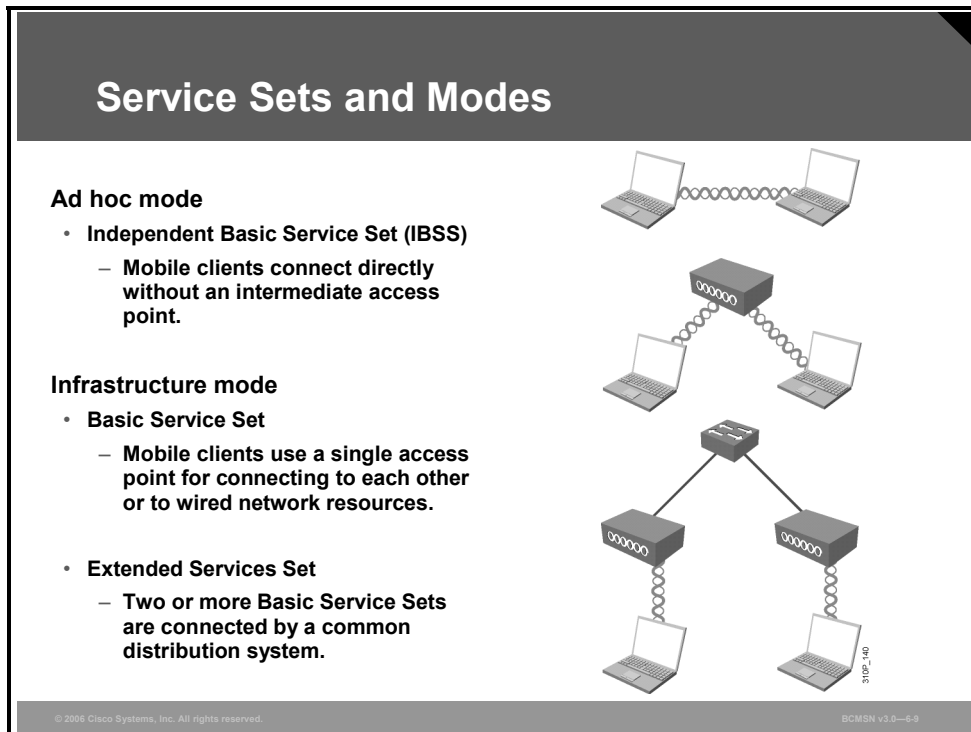
The basic service area can consist of a number of wireless PCs with a wireless network card. Operating systems such as Windows have made this peer-to-peer network easy to set up. This setup can be used for a small office (or home office) to allow a laptop to be connected to the main PC or for several people to simply share files.

The coverage is limited. Everyone must be able to hear everyone else. An access point is not required. A problem is that peer-to-peer networks are difficult to secure.

Note Many clients default to ad hoc mode, which has a negative impact on infrastructure WLANs with regard to both bandwidth use and network security.

WLAN Service Set and Modes

This subtopic summarizes the different WLAN topologies.

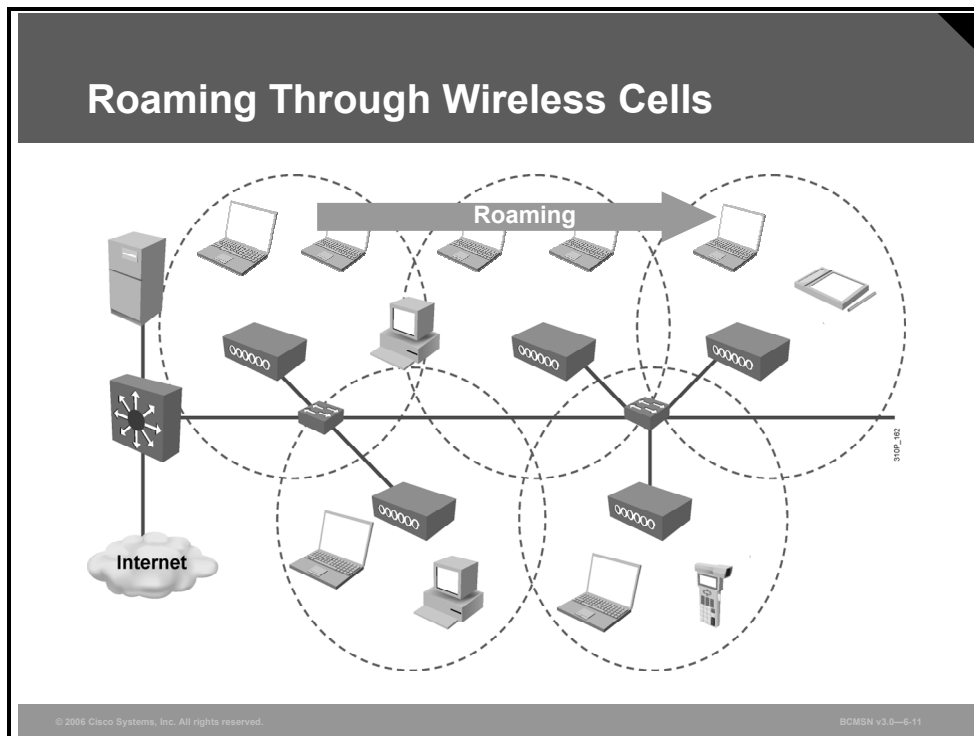


This is a summary of the different WLAN topologies:

- **Ad hoc mode:** This mode is called Independent Basic Service Set (IBSS). Mobile clients connect directly without an intermediate access point.
- **Infrastructure mode:** In infrastructure mode, where clients connect through an access point, there are two modes:
 - **Basic Service Set:** Mobile clients use a single access point for connectivity to each other or to wired network resources.
 - **Extended Services Set:** In this mode, two or more Basic Service Sets are connected by a common distribution system. An Extended Services Set generally includes a common SSID to allow roaming from access point to access point without requiring client configuration.

Roaming Through Wireless Cells

This topic explains roaming in WLANs.



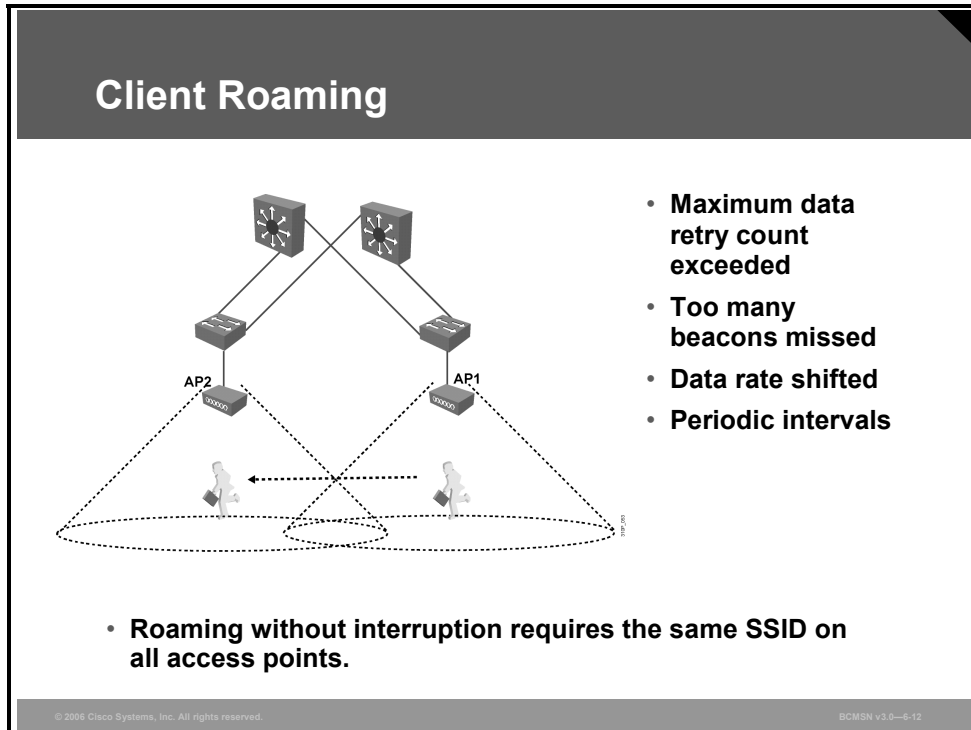
A typical WLAN can include PCs, laptop computers, pen-based computers, printers, and any other device that is normally found on a typical wired network. The WLAN consists of microcells, and the user has the ability to move freely anywhere that the RF coverage permits. Roaming is enabled by complete coverage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

Benefits of Cisco Aironet WLAN products include the following:

- Seamless roaming across access points allows users to maintain a 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.
- Access points with overlapping coverage cells and redundant switches provide fault-tolerant WLAN networks.

Client Roaming

This subtopic explains the reasons for roaming in a WLAN.



Wireless clients associate to another access point if necessary. This process is called roaming between the wireless cells. The wireless client initiates the roaming if one of these conditions is detected:

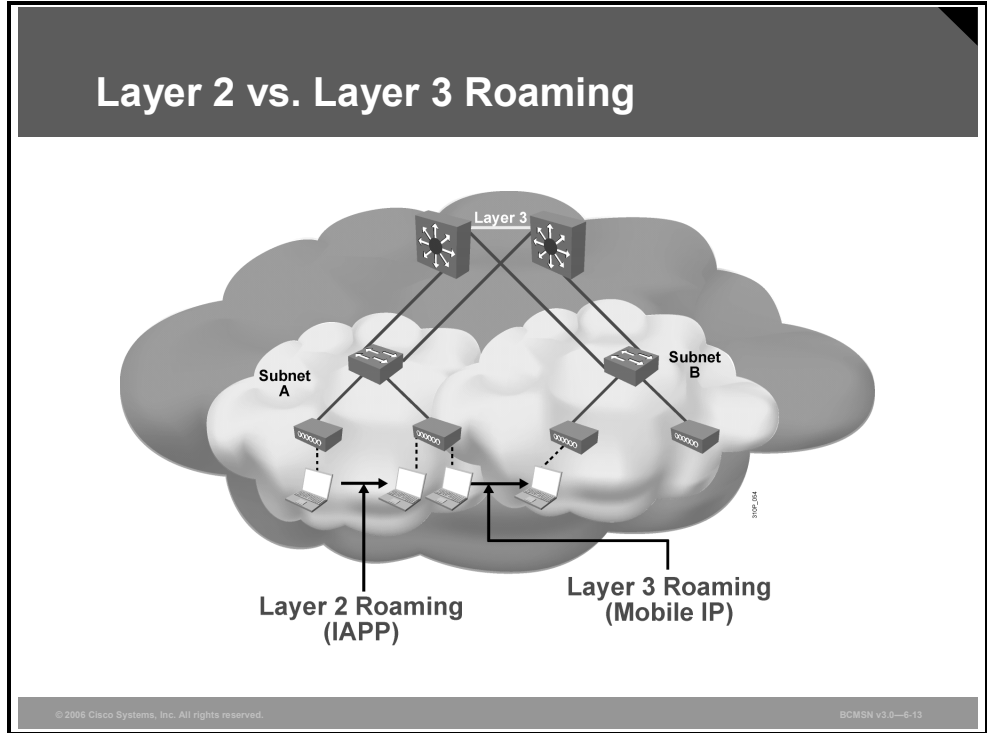
- The maximum data retry count is exceeded.
- The client has missed too many beacons from the access point.
- The client has reduced the data rate.
- The client intends to search for a new access point at periodic intervals.

Roaming without service interruption requires the identical configuration of SSID, VLANs, and IP subnets on all access points. Roaming is initiated by the client. The client searches for another access point with the same SSID and sends a reauthentication request to the new access point.

A short roaming time is important for delay-sensitive applications, such as voice and video.

Layer 2 and Layer 3 Roaming

This subtopic explains roaming between broadcast domains (Layer 2) and IP subnets (Layer 3).



Roaming maintains network connectivity while moving from one access point to another. Roaming between access points that reside on a single IP subnet (or VLAN) is considered Layer 2 (data link layer) roaming. Roaming between access points that reside in different IP subnets is considered Layer 3 (network layer) roaming.

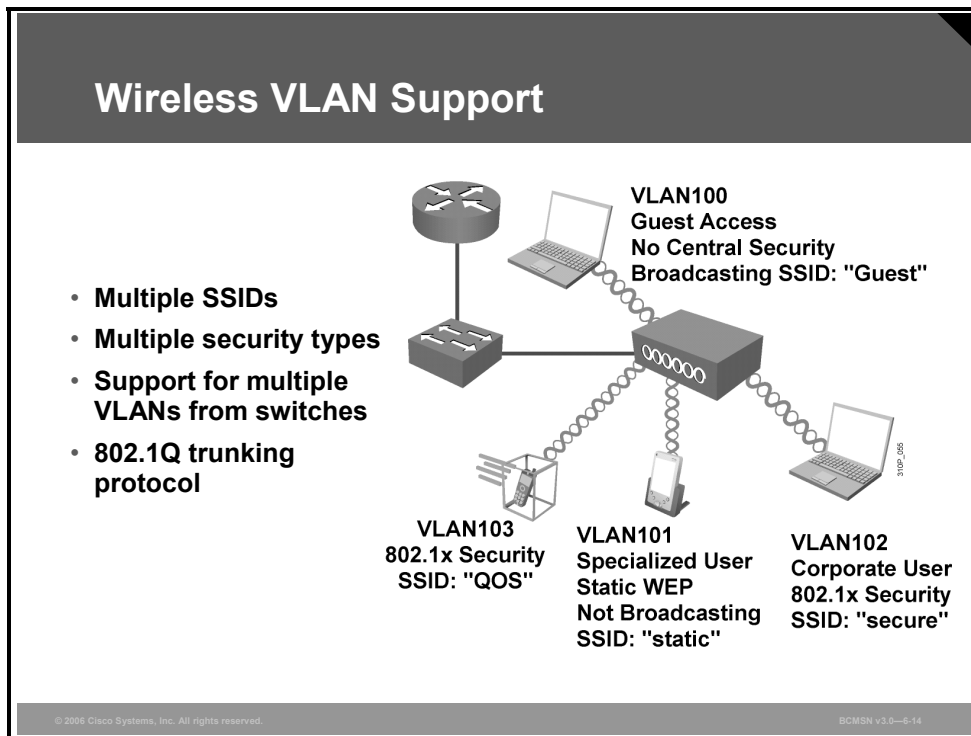
Roaming at Layer 2 is managed by the access points, using a combination of multicast packets that inform the switches in the network that the device has moved. The protocol between the access points is called Inter-Access Point Protocol (IAPP).

Mobile IP is a technology that allows fixed IP addresses in an IP subnet of a network. It relies on devices such as routers, known as home agents and foreign agents, to tunnel traffic for a mobile device.

WLAN implementations allow Layer 3 roaming. Legacy Layer 3 roaming for WLANs was accomplished by Mobile IP, which has been replaced by the advanced feature set of lightweight access point in combination with WLAN controllers.

Wireless VLAN Support

This topic explains the virtualization of access points.



LAN networks are increasingly being divided into workgroups connected via common backbones to form VLAN topologies. VLANs enable efficient traffic separation, provide better bandwidth utilization, and alleviate scaling issues by logically segmenting the physical 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.

Switches use VLANs to separate traffic. Access points can extend VLANs to the wireless LAN by mapping VLANs to SSIDs. The wireless VLANs share the same wireless cell and channel. The result is a virtualization of the access points. The access point appears as multiple different access points. The VLAN deployment example in the figure shows how VLANs may be used to segregate user groups and provide unique access policies.

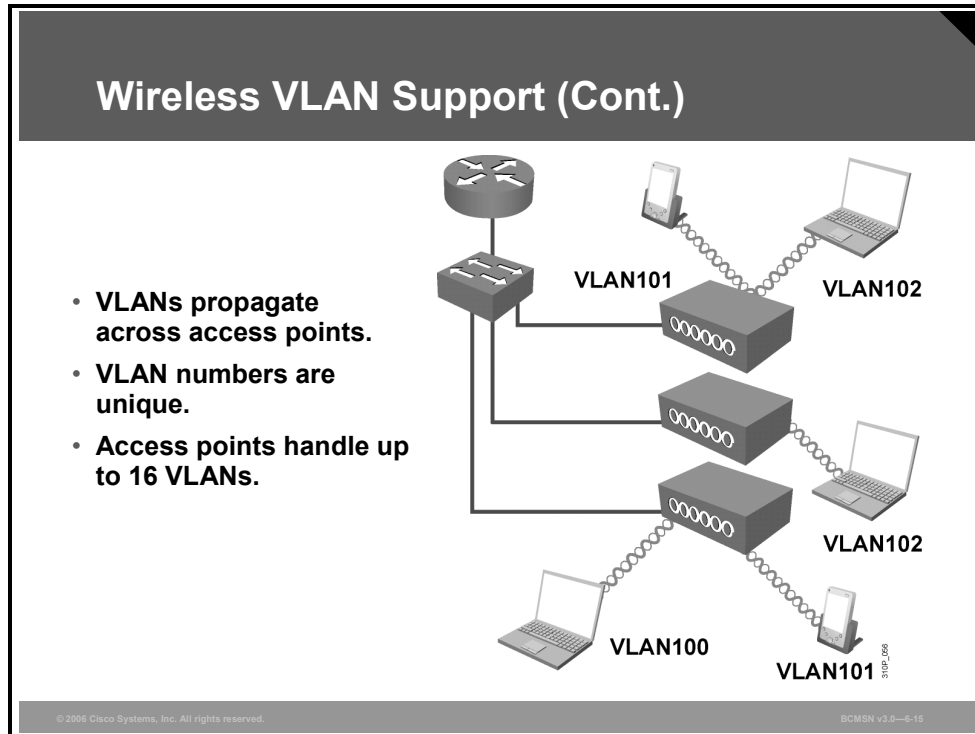
- **VLAN100:** Allows guests who come into your enterprise environment to connect directly to the Internet without having access to your enterprise servers. Without the VLAN function, two access points would be needed to provide isolated connectivity for the guest users and enterprise users.

VLAN100 would be configured with no security and would broadcast its SSID. An access control list (ACL) on the router could also be configured to ensure that traffic with VLAN100 tags goes straight out the firewall.

- **VLAN101:** Allows specialized users (for example, a shipping/receiving clerk) to use a barcode scanner with static Wired Equivalent Privacy (WEP) security because the barcode scanner cannot support dynamic security. VLAN101 would be configured with static WEP security and would be configured not to broadcast its SSID.

- **VLAN102:** Allows enterprise users to take advantage of 802.1x Extensible Authentication Protocol (EAP) types, including Lightweight EAP (LEAP), EAP-Transport Layer Security (EAP-TLS), and Protected Extensible Authentication Protocol (PEAP). VLAN102 would be configured to support 802.1x EAP security.
- **VLAN103:** Allows three enterprise users to take advantage of 802.1x and combine it with secure Quality of Service (QoS) applications, such as WLAN VoIP.

The Cisco Aironet Access Points support only the 802.1Q trunking protocol standard. Cisco switches and routers support both the prestandard Inter-Switch Link (ISL) protocol and 802.1Q.



WLANs can fit nicely into the larger network because VLANs have been enabled on the access points. This approach allows WLAN users to roam from access point to access point, maintaining connectivity to the proper VLAN.

In the figure, the notebook user is able to maintain access to the proper VLAN (VLAN102) and communicate to the router while roaming from access point to access point.

Roaming without service interruption requires the identical configuration of SSID, VLANs, and IP subnets on all access points.

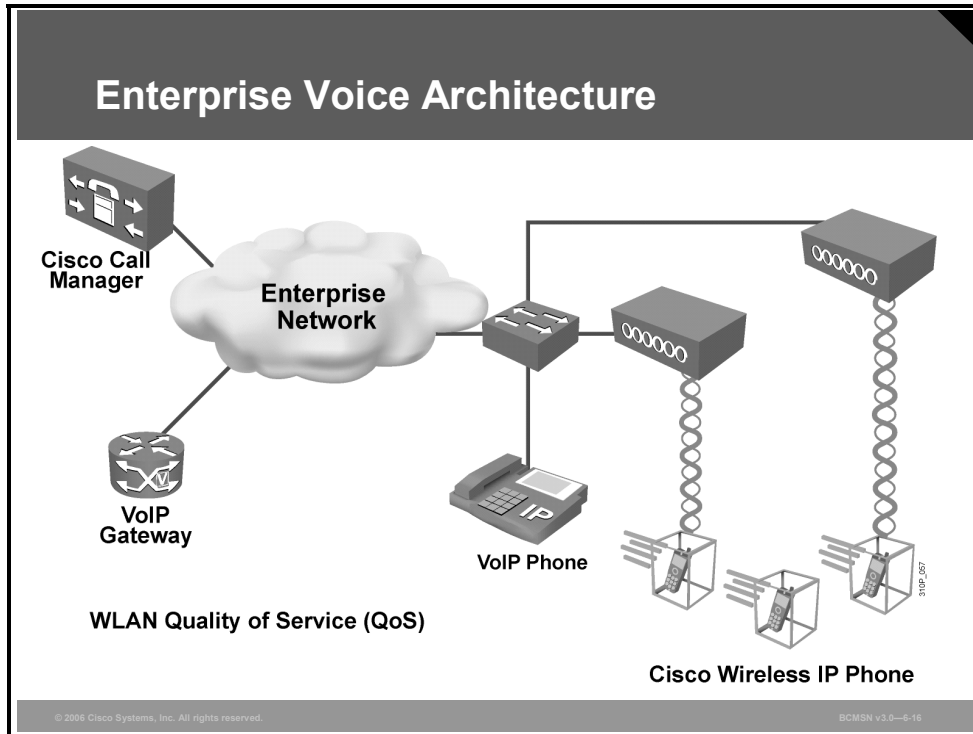
Switches do not allow different VLANs to talk to one another. A router is needed to allow different VLANs to communicate with each other. The VLAN number of the switch and the access point has to match.

The Cisco Aironet Access Points can be configured with 8 to 16 different VLANs (depending on implementation) for system design flexibility.

For client cards that require broadcast SSID support, the access point has to be configured for SSID broadcast per VLAN.

Enterprise Voice Architecture

This subtopic explains the addition of wireless IP phones to a voice network.



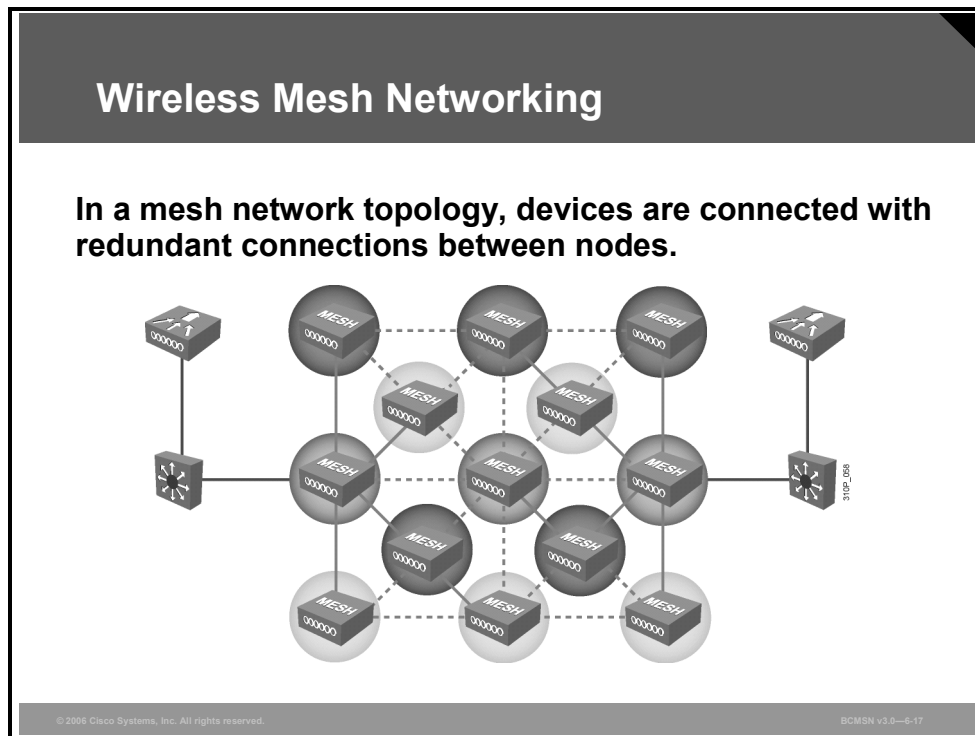
IP phone networks can be extended with wireless IP phones. The new 802.11e standard specifies QoS upstream and downstream for WLAN networks.

Drivers for QoS in WLAN networks include these considerations:

- Converged networks, which combine deployment of data, voice, and video applications over WLAN, are increasing.
- Having the ability to minimize end-to-end delay and jitter for voice and video applications becomes critical in a congested WLAN environment.
- Mobility in clients means that capacity planning alone is insufficient to control quality. QoS is perhaps more important in mobile networks.

Wireless Mesh Networking

This topic describes wireless mesh networking.



A mesh networking infrastructure is decentralized and inexpensive because each node needs to transmit only as far as the next node. Nodes act as repeaters to transmit data from nearby nodes to peers that are too far away to reach. This approach results in a network that can span a large distance, especially over rough or difficult terrain.

Mesh networks are also extremely reliable because each node is connected to several other nodes. If one node drops out of the network because of hardware failure or any other reason, its neighbors simply find another route. Extra capacity can be installed by simply adding more nodes.

Mesh networks allow many possible paths from a given node to other nodes. Paths through the mesh network can change in response to traffic loads, radio conditions, or traffic prioritization.

Wireless mesh networks differ from other wireless networks in that only a subset of the nodes needs to be connected to the wired network. The network can cover more distance by using nodes that are not connected to the wired network. Unlicensed bandwidth and wireless routing allow microcells to interconnect over wireless backhaul links.

Wireless Mesh Applications

This subtopic describes wireless mesh networking details.

Wireless Mesh Networking

- **Mesh access points automatically establish connection to controller.**
 - **Rooftop access points (RAP)** connect via wired connection.
 - **Mesh access points (MAP)** connect via self-configuring backhaul connection.
- **Cisco uses mesh access points.**
- **Adaptive Wireless Path (AWP) protocol establishes best path to root.**
- **Access point authenticates to controller and downloads configuration and radio parameters.**

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0—6-18

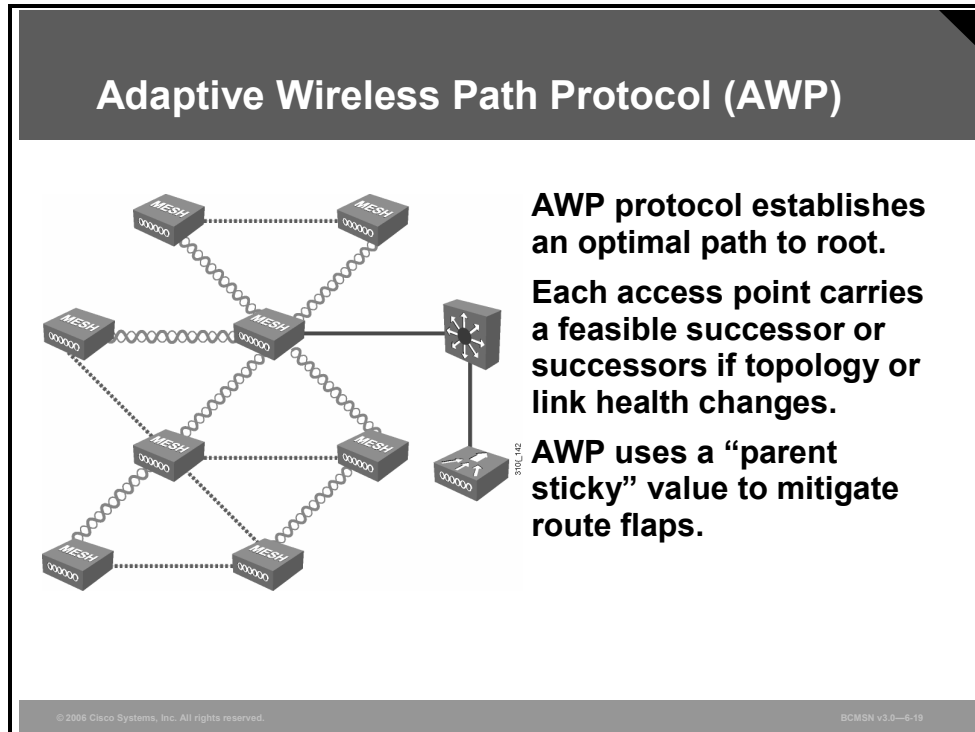
Mesh applications may be used to provide wireless coverage throughout a campus, manufacturing environment, or city. Deploying mesh access points allows the network to extend beyond the typical boundaries that would require each access point to be wired to the LAN.

The Cisco Adaptive Wireless Path (AWP) protocol allows each device to find a way back to the wired rooftop access point and thus to the network.

Access points are authenticated as they join the network, allowing the controller to send configuration parameters.

AWP Protocol

This subtopic explains how the AWP protocol maintains connectivity in a mesh network.



Each access point runs the Cisco AWP protocol. This is a new protocol that was designed from the start, specifically for the wireless environment. This protocol allows access points to communicate with each other to determine the best path back to the wired network. After the optimal path is established, AWP continues to run in the background to establish alternative routes back to the rooftop access points if the topology changes or conditions cause the link strength to diminish.

Cisco AWP takes into consideration factors such as interference and characteristics of the radio so that the mesh can be self-configuring and self-healing. AWP ensures that the mesh network is not disruptive and provides consistent coverage.

The wireless network is a very dynamic environment. When there is interference, or if access points are added or removed, the AWP protocol reconfigures the path back to the rooftop access point.

Because the wireless environment is very dynamic, AWP uses a stickiness factor to mitigate route flaps. This approach ensures that a loss of connection, which causes a temporary disruption, does not allow the mesh to change unnecessarily.

Key Market Segments for Outdoor Wireless Technology

This subtopic describes the key markets for outdoor WLANs.

Key Market Segments for Outdoor Wireless

- Enterprise outdoor**
 - Indoor and outdoor wireless solutions for education customers.
 - Rugged mesh solutions for enterprise customers.
- Public sector**
 - Connecting peripheral devices across the mesh.
 - Establishing hot zones for public safety or municipal departments.
- Service provider**
 - Hot spots become hot zones with Wi-Fi access.

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0—6-20

Enterprise outdoor wireless applications include the following:

- **Universities and health care:** Wi-Fi coverage can be extended throughout the entire campus, providing access to administration, students, and facilities managers.
- **Hospitality:** Indoor and outdoor mesh networks can open up new hospitality markets.
- **Manufacturing:** Wireless applications in this field include shipping and receiving, inventory applications, hand-held scanners, radio frequency identification, and so on.
- **Large corporate campuses:** Wireless applications can be used to create blanket coverage for access and asset tracking.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- **Types of WLAN topologies are client access, bridging, and mesh networking.**
- **Wireless networks are built with multiple wireless cells.**
- **WLAN roaming occurs seamlessly between wireless cells.**
- **WLANs support VLANs and QoS.**
- **WLAN mesh networks extend the wireless network beyond the boundaries of wired LANs.**

Explaining WLAN Technology and Standards

Overview

This lesson explains wireless LAN (WLAN) technology and the WLAN standards. This knowledge is important for the design, configuration, operation, and troubleshooting of WLANs.

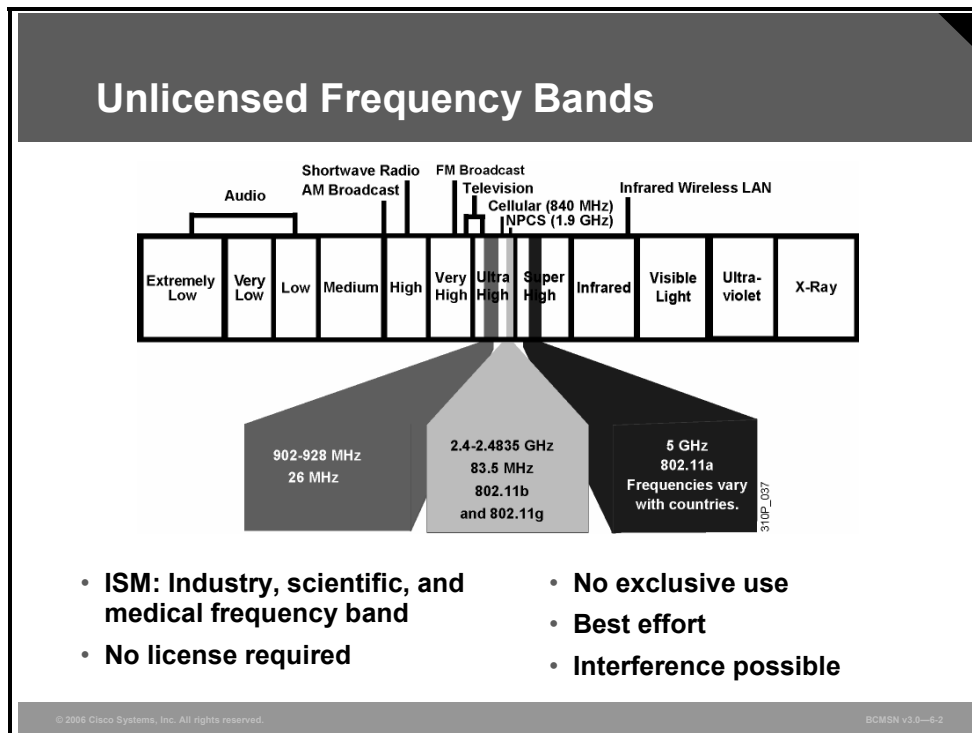
Objectives

Upon completing this lesson, you will be able to explain WLAN technology, standards, and security. This ability includes being able to meet these objectives:

- Describe the WLAN frequency bands and RF transmission
- Describe WLAN regulations, standards, and certification bodies
- Describe the IEEE 802.11b standard
- Describe the IEEE 802.11a standard
- Describe the IEEE 802.11g standard
- Compare the 802.11b, 802.11g, and 802.11a standards for data rates, throughput, and coverage
- Identify best practices for WLAN office design
- Explain the need for WLAN security and describe the available WLAN security solutions

Unlicensed Frequency Bands

This topic describes the frequency bands available for WLANs.



There are three unlicensed bands: 900 MHz, 2.4 GHz, and 5.7 GHz. The 900-MHz and 2.4-GHz bands are referred to as the industrial, scientific, and medical (ISM) bands, and the 5-GHz band is commonly referred to as the Unlicensed National Information Infrastructure (UNII) band.

Frequencies for these bands are as follows:

- **900-MHz band:** 902 MHz to 928 MHz.
- **2.4-GHz band:** 2.400 MHz to 2.483 GHz. (In Japan, this band extends to 2.495 GHz.)
- **5-GHz band:** 5.150 MHz to 5.350 MHz, 5.725 MHz to 5.825 MHz, with some countries supporting middle bands between 5.350 MHz and 5.825 MHz. Not all countries permit 802.11a, and the available spectrum varies widely. The list of countries that permit 802.11a is changing.

The figure shows WLAN frequencies. Next to the WLAN frequencies in the spectrum are other wireless services, such as cellular phones and Narrowband Personal Communication Services. The frequencies used for WLAN are ISM bands.

Unlicensed frequency bands do not require a license to operate wireless equipment. However, there is no exclusive use of a frequency for a user or a service. For example, the 2.4-GHz band is used for WLANs, video transmitters, Bluetooth, microwave ovens, and portable phones. Unlicensed frequency bands offer a best-effort use, and interference and degradations are possible.

Radio Frequency Transmission

This subtopic explains the propagation and behavior of radio waves.

Radio Frequency Transmission

- **Radio frequencies are radiated into the air via an antenna, creating radio waves.**
- **Radio waves are absorbed when they are propagated through objects (e.g., walls).**
- **Radio waves are reflected by objects (e.g., metal surfaces).**
- **This absorption and reflection can cause areas of low signal strength or low signal quality.**

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0—6-3

Radio frequencies are radiated into the air by antennas that create radio waves. When radio waves are propagated through objects, they may be absorbed by some objects (for instance, walls) and reflected by other objects (for instance, metal surfaces). This absorption and reflection may cause areas of low signal strength or low signal quality.

The transmission of radio waves is influenced by these factors:

- **Reflection:** Occurs when radio frequency (RF) waves bounce off objects (for example, metal or glass surfaces).
- **Scattering:** Occurs when RF waves strike an uneven surface (for example, a rough surface) and are reflected in many directions.
- **Absorption:** Occurs when RF waves are absorbed by objects (for example, walls).

Data Transmission over Radio Waves

This subtopic explains the transmission of radio waves.

Radio Frequency Transmission (cont.)

- **Higher data rates have a shorter transmission range.**
 - **The receiver needs more signal strength and better SNR to retrieve information.**
- **Higher transmit power results in greater distance.**
- **Higher frequencies allow higher data rates.**
- **Higher frequencies have a shorter transmission range.**

© 2006 Cisco Systems, Inc. All rights reserved.

BCMSN v3.0-6.4

These rules apply for data transmission over radio waves:

- Higher data rates have a shorter range because the receiver requires a stronger signal with a better signal-to-noise ratio (SNR) to retrieve the information.
- Higher transmit power results in greater range. To double the range, the power has to be increased by a factor of four.
- Higher data rates require more bandwidth. Increased bandwidth is possible with higher frequencies.
- Higher frequencies have a shorter transmission range through higher degradation and absorption. More efficient antennas can compensate for this effect.

WLAN Regulation and Standardization


This topic describes the Wi-Fi certification.

WLAN Regulation and Standardization

Regulatory agencies


- FCC (United States)
- ETSI (Europe)

Standardization

- IEEE 802.11 
- <http://standards.ieee.org/getieee802/>

Certification of equipment

- Wi-Fi Alliance certifies interoperability between products.
- Certifications include 802.11a, 802.11b, 802.11g, dual-band products, and security testing.
- Certified products can be found at <http://www.wi-fi.org>.



Wi-Fi CERTIFIED

Interoperable with:

2.4 GHz Band	11 Mbps	<input checked="" type="checkbox"/>
	54 Mbps	<input checked="" type="checkbox"/>
5 GHz Band	54 Mbps	<input checked="" type="checkbox"/>
Wi-Fi Protected Access™		<input checked="" type="checkbox"/>

www.wi-fi.org

© 2006 Cisco Systems, Inc. All rights reserved. BOMSIN v3.0-6.5

Regulatory agencies control the use of the RF bands. With the opening of the 900-MHz ISM band in 1985, the development of WLANs started. New transmissions, modulations, and frequencies depend on the approval of the regulatory agencies. A worldwide consensus is required. Regulatory agencies include the FCC for the United States (<http://www.fcc.gov>) and the European Telecommunications Standards Institute (ETSI) for Europe (<http://www.etsi.org>).

The IEEE defines standards. 802.11 is part of the 802 networking standardization. You can download ratified standards from the IEEE website (<http://standards.ieee.org/getieee802/>).

The Wi-Fi Alliance offers certification for interoperability between vendors of 802.11 products. This certification provides a comfort zone for the users who are purchasing the products. It also helps to market the WLAN technology by promoting interoperability between vendors.

Certification includes all three 802.11 RF technologies and Wi-Fi Protected Access (WPA), a security model released in 2003, based on the new security standard IEEE 802.11i, which was ratified in 2004. The Wi-Fi promotes and influences WLAN standards. Ratified products can be found on the Wi-Fi website (<http://www.wi-fi.org>).

IEEE 802.11b Standard

This topic describes the characteristics of the 802.11b standard.

802.11b Standard

- **Standard was ratified in September 1999**
- **Operates in the 2.4-GHz band**
- **Specifies direct sequence spread spectrum (DSSS)**
- **Specifies four data rates up to 11 Mbps**
 - 1, 2, 5.5, 11 Mbps
- **Provides specifications for vendor interoperability (over the air)**
- **Defines basic security, encryption, and authentication for the wireless link**
- **Is the most commonly deployed WLAN standard**

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0-6-7

IEEE 802.11b was ratified in 1999. Products were actually introduced into the market before the standard was ratified. It became the unwritten but accepted standard for wireless and was adopted rapidly. It operates in the 2.4-GHz ISM band that is available worldwide. The standard specifies one RF transmission: direct sequence spread spectrum (DSSS). It provides four data rates up to 11 Mbps: 1, 2, 5.5, and 11 Mbps.

The 802.11b standard is the most commonly deployed WLAN standard.

2.4-GHz Channels

This subtopic describes the 2.4-GHz channels.

Channel Identifier	Channel Center Frequency	Channel Frequency Range [MHz]	Regulatory Domain		
			Americas	Europe, Middle East, and Asia	Japan
1	2412 MHz	2401 – 2423	X	X	X
2	2417 MHz	2406 – 2428	X	X	X
3	2422 MHz	2411 – 2433	X	X	X
4	2427 MHz	2416 – 2438	X	X	X
5	2432 MHz	2421 – 2443	X	X	X
6	2437 MHz	2426 – 2448	X	X	X
7	2442 MHz	2431 – 2453	X	X	X
8	2447 MHz	2436 – 2458	X	X	X
9	2452 MHz	2441 – 2463	X	X	X
10	2457 MHz	2446 – 2468	X	X	X
11	2462 MHz	2451 – 2473	X	X	X
12	2467 MHz	2466 – 2478		X	X
13	2472 MHz	2471 – 2483		X	X
14	2484 MHz	2473 – 2495			X

© 2006 Cisco Systems, Inc. All rights reserved. BOMSN v3.0-4-8

There are 11 channels available in the United States. However, only three of these channels are nonoverlapping.

In the ETSI domains, there are 13 available channels, but again there are only three nonoverlapping channels.

In Japan, a fourteenth channel located at the upper end of the band is available, and it is possible to use this along with three other channels for a total of four nonoverlapping channels.

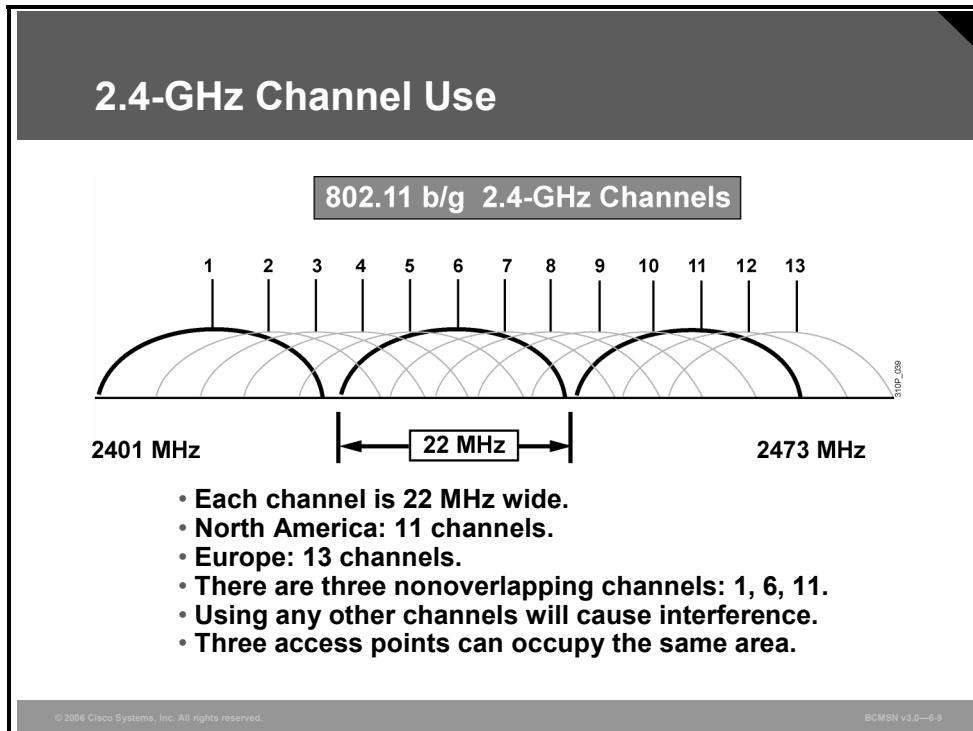
The channels are known by their center frequency. The figure lists the 14 channels. It also shows the lowest and highest frequency used by each 22-MHz wide channel.

Different countries have different regulatory bodies and may have as many as 14 channel sets available. In some countries, the number of nonoverlapping channels is reduced to one.

Regulatory domain information is subject to change. An up-to-date listing of the countries that correspond to these regulatory domains is available at <http://www.cisco.com/go/aironet/compliance>.

2.4-GHz Channel Use

This subtopic describes the use of the 2.4-GHz channels.



In the 2.4-GHz frequency band there are three nonoverlapping channels for the 802.11b standard that do not share any frequency. The existence of these channels means that three access points could operate in the same cell area without sharing the media.

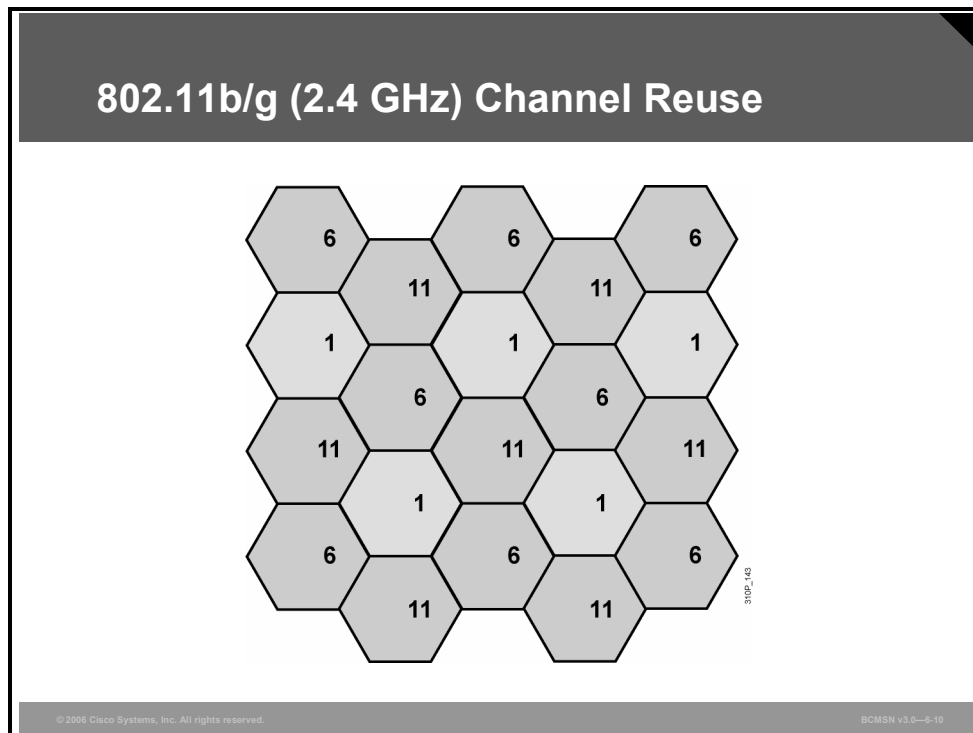
An access point on channel 1 does not share frequencies with an access point on channel 6 because the channels do not have any common frequencies. There is no degradation in throughput when three access points are in the same wireless cell area if the access points are each on a nonoverlapping channel. Three access points in the same cell on three nonoverlapping channels (for example, 1, 6, and 11) provide an aggregated data rate for the cell of 33 Mbps (3 x 11Mbps), with an aggregated throughput of about 16 Mbps (half of the aggregate).

If the same three access points shared the same channel, the aggregate data rate would still be 11 Mbps, but the aggregated throughput would be closer to 6 Mbps. This results from each access point sharing the same cell. There would be minimal interference because each access point can detect transmissions in progress.

If the same three access points operate on interfering, overlapping channels, the throughput of the access points is greatly reduced by interference and can drop below 1 Mbps.

802.11b/g (2.4-GHz) Channel Reuse

This subtopic explains how channels are reused to avoid interference.

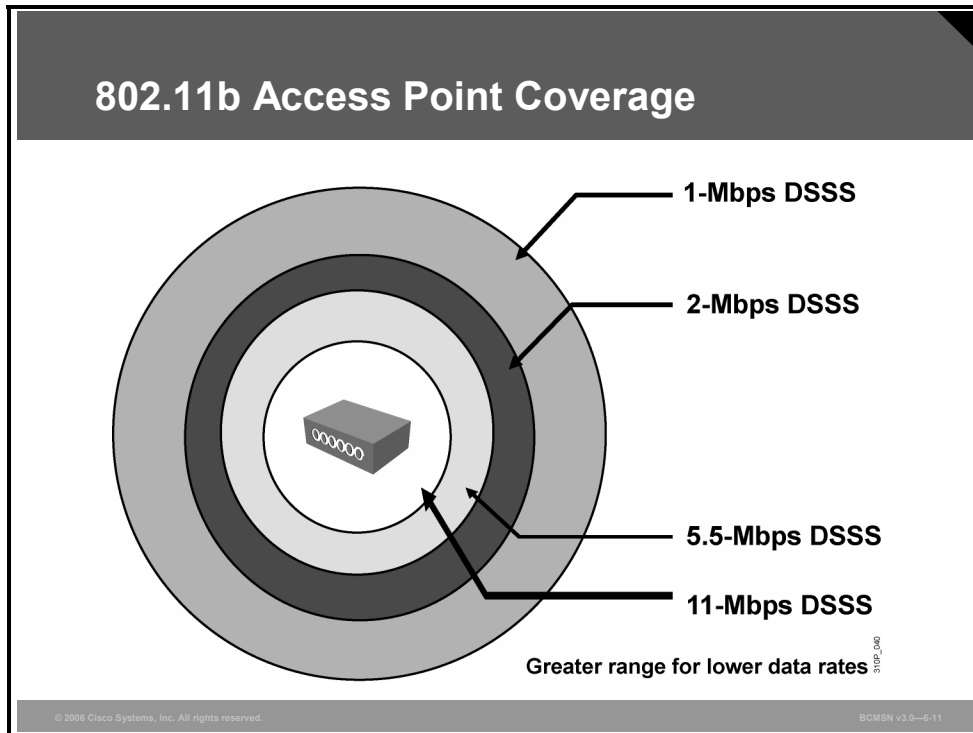


The figure illustrates the three nonoverlapping channels that are available within 802.11b and 802.11g standards.

The goal of access point and 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 never see two radio stations in the same geographic area on the same channel. The same concept holds true for WLAN cells and channels.

802.11b Access Point Coverage

This subtopic describes the coverage of access points.



WLAN clients have the ability to shift data rates while moving. This technique allows the same client operating at 11 Mbps to shift to 5.5 Mbps, 2 Mbps, and finally still communicate in the outside ring at 1 Mbps. This rate shifting happens without losing the 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.

- Higher data rates require stronger signals at the receiver. Therefore, lower data rates have a greater range.
- Wireless clients always try to communicate with the highest possible data rate.
- The client will reduce the data rate only if transmission errors and transmission retries occur.

This approach provides the highest total throughput within the wireless cell.

IEEE 802.11a Standard

This topic describes the IEEE 802.11a standard.

802.11a Standard

- **Standard was ratified September 1999**
- **Operates in the 5-GHz band**
- **Uses orthogonal frequency-division multiplexing (OFDM)**
- **Uses eight data rates of up to 54 Mbps**
 - **6, 9, 12, 18, 24, 36, 48, 54 Mbps**
- **Has from 12 to 23 nonoverlapping channels (FCC)**
- **Has up to 19 nonoverlapping channels (ETSI)**
- **Regulations different across countries**
 - **Transmit (Tx) power control and dynamic frequency selection required (802.11h)**

© 2006 Cisco Systems, Inc. All rights reserved.

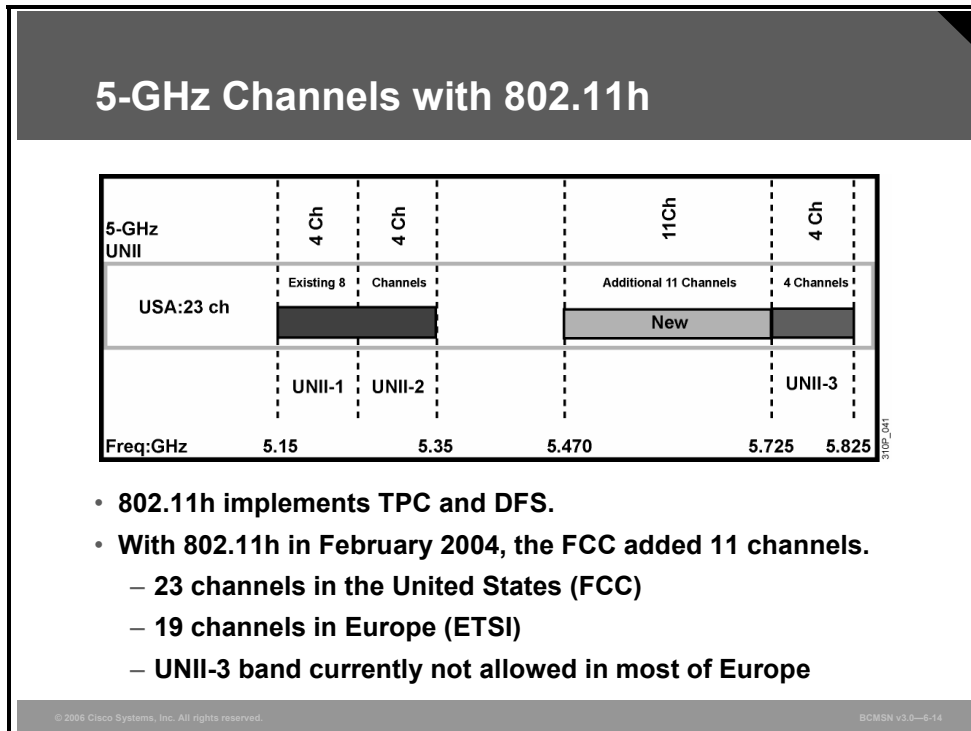
BCMSN v3.0-6-13

The 802.11a standard was ratified at the same time as 802.11b. However, because of limited supplies of silicon and other components, products did not start to appear in the market until late 2000.

The technology provides up to a 54-Mbps data rate and, in most countries, provides eight channels of indoor WLAN use. However, the regulations vary widely across countries and are subject to change. More channels are expected to become available in many countries.

5-GHz Channels with 802.11h

This subtopic describes the new channels available with 802.11h for 5 GHz.



To use the 11 new channels, radios must comply with two features that are part of the 802.11h specification: Transmit Power Control (TPC) and Dynamic Frequency Selection (DFS). DFS dynamically instructs a transmitter to switch to another channel whenever a particular condition (such as the presence of a radar signal) is met.

Prior to transmitting, the DFS mechanism of a device monitors its available operating spectrum, listening for a radar signal. If a signal is detected, the channel associated with the radar signal is vacated or flagged as unavailable for use by the transmitter. The transmitting device continuously monitors the environment for the presence of radar, both before and during operation.

Portions of the 5-GHz band are allocated to radar systems. This allocation allows WLANs to avoid interference with incumbent radar users in instances where they are collocated. Such features can simplify enterprise installations because the devices themselves can (theoretically) automatically optimize their channel reuse patterns.

TPC technology has been used in the cellular telephone industry for many years. Setting the transmit power of the access point and the client adapter can be useful to allow for different coverage area sizes and, in the case of the client, to conserve battery life. In devices that have the ability to set power levels, the settings are usually static and independent of each other (access point and clients).

For example, an access point can be set to a low 5-mW transmit power to minimize cell size, which is useful in areas with high user density. The clients will, however, be transmitting at their previously assigned transmit power settings, which is probably more transmit power than is required to maintain association with the access point. This approach results in unnecessary RF energy transmitting from the clients, creating a higher-than-necessary level of RF energy outside the intended coverage area of the access point.

With TPC, the client and access point exchange information; then the client device dynamically adjusts its transmit power such that it uses only enough energy to maintain association to the access point at a given data rate. The end result is that the client contributes less to adjacent cell interference, allowing for more densely deployed high-performance WLANs. As a secondary benefit, the lower power on the client provides longer battery life; less power is used by the radio.

The Cisco Aironet RM21A and RM22A 5-GHz radio modules for Cisco Aironet 1200 and 1230 Series and the 1130AG and 1240AG Series access points support the 12 channels made up of the UNII-1, UNII-2, and UNII-3 bands. These devices have the hardware capability to support the 11 new channels. However, until the FCC releases a test program, the firmware will not provide the availability to access the additional channels.

The 5-GHz band is divided into several sections. The lower eight channels cover two of the sections known as UNII-1 and UNII-2. Each of these includes 100 MHz of spectrum in which there are four channels. The UNII-1 band has limitations in the United States (and some other countries) that require it to be for indoor use. UNII-2 is permitted for both indoor and outdoor use, and it also permits external antennas. UNII-3 was designated for outdoor use and was primarily set aside for bridging.

Rule changes are underway and, with the adoption of 802.11h, will provide up to an additional 12 channels in many countries, in addition to using the UNII-3 band for WLANs. The number of WLAN channels will then increase from 8 to as many as 24.

If a 6-dBi antenna is used, then the radiated power is as follows:

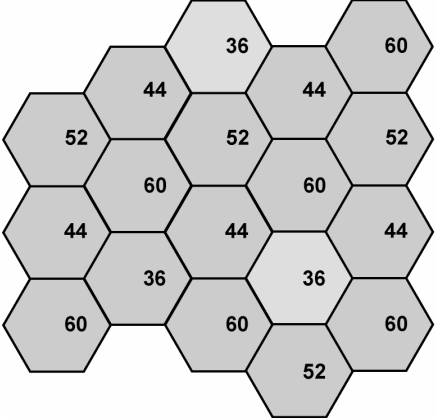
- **UNII-1:** 50 mW in the United States and Japan, 200 mW in Europe, 4 channels (5.15 GHz to 5.25 GHz), indoor access, flexible antenna
- **UNII-2:** 250 mW in the United States, 4 channels (5.25 GHz to 5.35 GHz), indoor and outdoor use, flexible antenna
- **HiperLAN:** 200 mW in Europe, 8 channels (5.15 GHz to 5.35 GHz), indoor use only
- **HiperLAN II:** 1 W in Europe, 11 channels (5.470 GHz to 5.725 GHz), indoor and outdoor use, flexible antenna
- **UNII- 3:** 1 W in the United States, 4 channels (5.725 GHz to 5.825 GHz), indoor and outdoor use, flexible antenna

802.11a Channel Reuse

This subtopic explains how channels are assigned manually or via DFS.

802.11a Channel Reuse

- **802.11h DFS not available**
 - **Manual channel assignment required**
- **802.11h DFS implemented**
 - **Channel assignment done by Dynamic Frequency Selection (DFS)**
 - **Only frequency bands can be selected**



SIP-144

© 2006 Cisco Systems, Inc. All rights reserved.BCMSN v3.0—6-15

The figure illustrates the channel deployment of 802.11a products throughout a given area. The cells are easier to deploy because there are 12 different channels to work with. It is recommended that neighboring cells not be placed on neighboring frequencies.

802.11h DFS replaces manual channel assignment. Only frequency bands can be selected.

DFS changes the channel if other transmissions, such as radar or satellite communication, are detected on the current channel.

With 802.11h, up to 23 channels are available in the United States, and 19 channels are available in Europe (if 5 GHz is allowed).

IEEE 802.11g Standard

This topic describes the IEEE 802.11g standard.

802.11g Standard

- **Standard was ratified June 2003**
- **Operates in the 2.4-GHz band as 802.11b**
 - Same three nonoverlapping channels: 1, 6, 11
- **DSSS (CCK) and OFDM transmission**
- **12 data rates of up to 54 Mbps**
 - 1, 2, 5.5, 11 Mbps (DSSS / 802.11b)
 - 6, 9, 12, 18, 24, 36, 48, 54 Mbps (OFDM)
- **Full backward compatibility to 802.11b standard**

The diagram illustrates a central 802.11g access point (represented by a box with '000000' on top) connected to two laptops. The left laptop is labeled '802.11g' and '54 Mbps', while the right laptop is labeled '802.11b' and '11Mbps'. This shows that the 802.11g standard can support both its own higher data rates and the lower data rates of the 802.11b standard.

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0-6-17

The 802.11g WLAN standard was ratified in June 2003. The aim was to provide higher data rates than the 802.11b standard. By using the 2.4-GHz band, backward compatibility was possible with existing 802.11b WLANs.

The 802.11g standard uses the same three nonoverlapping channels: 1, 6, and 11. There are 11 channels for North America, 13 channels for ETSI, and 14 channels for Japan.

The 802.11g standard provides full backward compatibility with 802.11b. 802.11g uses orthogonal frequency-division multiplexing (OFDM) modulation for 802.11g data rates and complementary code keying (CCK) modulation for 802.11b data rates.

802.11g Protection Mechanism

This subtopic describes the mechanism for compatibility between 802.11b and 802.11g.

802.11g Protection Mechanism

- **Problem: 802.11b stations cannot decode 802.11g radio signals.**
- **802.11b/g access point communicates with 802.11b clients with max. 11 Mbps.**
- **802.11b/g access point communicates with 802.11g clients with max. 54 Mbps.**
- **802.11b/g access point activates RTS/CTS to avoid collisions when 802.11b clients are present.**
- **802.11b client learns from CTS frame the duration of the 802.11g transmission.**
- **Reduced throughput is caused by additional overhead.**

The diagram illustrates an 802.11g access point at the top. Two laptops are connected to it. The laptop on the left is labeled '802.11g' and has a lightning bolt icon next to it with '54 Mbps' written above it. The laptop on the right is labeled '802.11b' and has a lightning bolt icon next to it with '11Mbps' written above it. The access point is labeled '802.11g'.

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0—6-18

Because of the backward compatibility of 802.11g, it is likely that both 802.11b and 802.11g clients associate to an 802.11g access point. The 802.11g protection mechanism allows the coexistence of 802.11b and 802.11g clients in an 802.11g wireless cell.

- If an access point has an 802.11b client associated to it, then the protection mechanism is on.
- The protection mechanism will turn off after 30 seconds without 802.11b client associations.
- The 802.11g specification is a superset of 802.11b and is designed to maintain compatibility with 802.11b.

The 802.11g uses the same frequencies as 802.11b, depending on regulatory domains. (Japan has not approved OFDM for channel 14). The 802.11g standard combines the modulations of 802.11b with the modulation of OFDM for 802.11g data rates. The 802.11g specification supports the data rates of 1, 2, 5.5, and 11 Mbps for 802.11b and adds the data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps for 802.11g.

The access point transacts with 802.11b clients at their highest capable data rate, given their configuration and position in the coverage cell, and does the same for 802.11g clients. This means that an 802.11b client can receive packets at the 11-Mbps data rate while an 802.11g client right next to the 802.11b client can receive packets at the 54-Mbps data rate.

When 802.11b clients and 802.11g clients are in the same cell, the 802.11g specification requires a protection mechanism that involves the use of the 802.11 Request to Send/Clear to Send (RTS/CTS) protocol. CTS packets can be sent from the access points without RTS packets. It is the protection mechanism of 802.11g that slows the throughput of 802.11g clients when there are 802.11b clients in the coverage cell.

The protection mechanism is not active when the cell has only 802.11g clients. With the protection mechanism active, the access point still transmits to the clients at rates up to their capabilities. The protection mechanism slows 802.11g throughput but provides for the fewest collisions of packets.

When RTS/CTS is in use, most stations will hear the RTS, and all stations will hear the CTS. In either case, each node receives information indicating the length of the subsequent OFDM packet and acknowledgment (ACK) transmission. Every station has an internal timer referred to as the network allocation vector, which is set to have the same duration as the OFDM packet exchange.

The network allocation vector acts in parallel with conventional carrier sensing and is referred to as a virtual carrier sense mechanism. The channel is not considered idle unless no active signal is detected and the network allocation vector timer has expired. After both criteria are met, stations can once again begin to contend for channel access.

In this manner, 802.11b and 802.11g radios can operate in a mixed environment with 802.11g access points. It should also be noted that every 802.11g client and access point must be capable of falling back and operating exactly like a legacy 802.11b device.

Therefore, migration to 802.11g technology can be smooth and painless. As new 802.11g access points are brought online, legacy 802.11b access points can remain in service and will be fully interoperable with newer 802.11g clients.

802.11 Comparison

This topic identifies the RF advantages and disadvantages of each 802.11 standard.

802.11 RF Comparison			
	802.11b – 2.4 GHz	802.11g – 2.4 GHz	802.11a – 5 GHz
Pro	<ul style="list-style-type: none"> • Most commonly deployed WLAN standard 	<ul style="list-style-type: none"> • Higher throughput • OFDM technology reduces multipath issues 	<ul style="list-style-type: none"> • Highest throughput • OFDM technology reduces multipath issues • Provides up to 23 nonoverlapping channels
Con	<ul style="list-style-type: none"> • Interference and noise from other services in the 2.4-GHz band • Only 3 nonoverlapping channels • Distance limited by multipath issues 	<ul style="list-style-type: none"> • Interference and noise from other services in the 2.4-GHz band • Only three nonoverlapping channels • Throughput degraded in the presence of 802.11b clients 	<ul style="list-style-type: none"> • Lower market penetration

2.4 GHz (802.11b)

The 802.11b standard, the 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 most applications.

Interoperability between many of the products on the market is ensured through the Wi-Fi Alliance certification program. Therefore, if your network requirements include supporting a wide variety of devices from different vendors, 802.11b is probably your best choice.

2.4 GHz (802.11g)

The 802.11g standard was ratified in June 2003. The 802.11g standard delivers the same 54-Mbps maximum data rate as the 802.11a standard, yet it offers an additional and compelling advantage: backward compatibility with 802.11b equipment.

This compatibility means that 802.11b client cards will work with 802.11g access points and that 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 is an affordable choice for organizations with existing 802.11b wireless infrastructures.

Note that 802.11b products cannot be “software upgraded” to 802.11g. This limitation is due to the fact that 802.11g radios use a different chipset 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. Both 802.11g and 802.11b operate in the same unlicensed band. As a result, they share the same three channels, which can limit wireless capacity and scalability.

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 12 nonoverlapping frequency channels. This provision results 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 devices (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. If an organization with 802.11b equipment wants the extra channels and network speed supported by 802.11a technology, the organization must upgrade to a product that supports the technology.

Some products support dual-band operation, and it is important to note that 2.4-GHz and 5-GHz equipment can operate in the same physical environment without interference.

802.11 Standards Comparison

This subtopic summarizes the 802.11 standards.

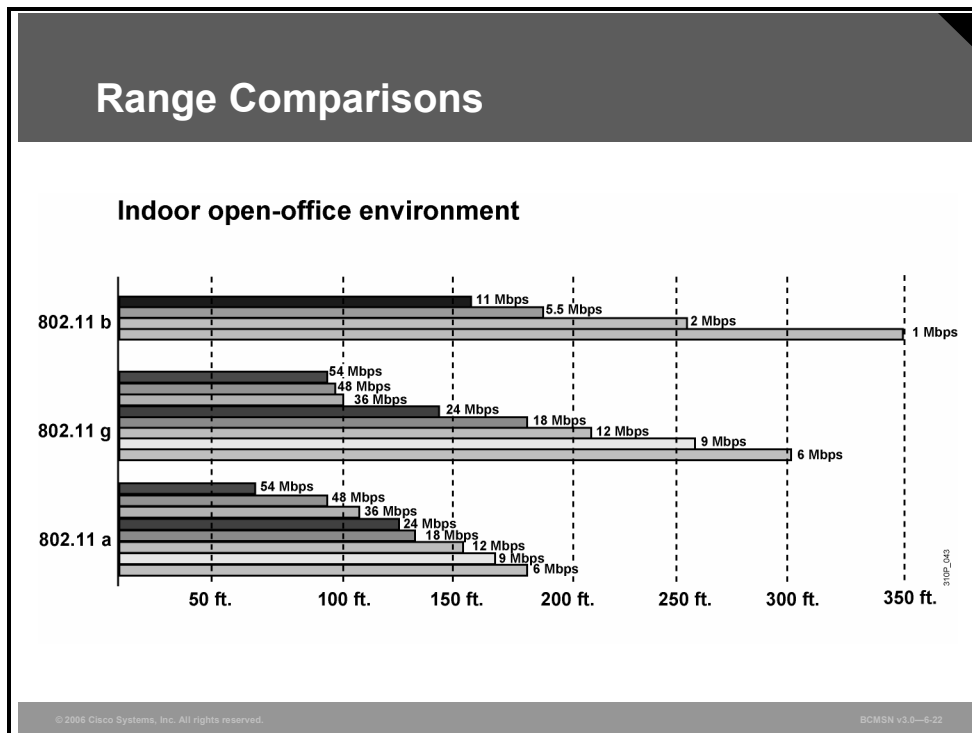
802.11 Standards Comparison				
	802.11b	802.11g		802.11a
Ratified	1999	2003		1999
Frequency band	2.4 GHz	2.4 GHz		5 GHz
No of channels	3	3		Up to 23
Transmission	DSSS	DSSS	OFDM	OFDM
Data rates [Mbps]	1, 2, 5.5, 11	1, 2, 5.5, 11	6, 9, 12, 18, 24, 36, 48, 54	6, 9, 12, 18, 24, 36, 48, 54
Throughput [Mbps]	Up to 6	Up to 22		Up to 28

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0—6-21

The figure summarizes the features of the 802.11 WLAN standards, including frequency band, data rates, and throughput.

Range Comparisons

This subtopic describes the dependency of range, data rate, and frequency.



The 802.11b and 802.11g ranges are based on default power settings with 2.2-dBi 2.4-GHz antennas on the access points and 0-dBi antennas on the clients. The 802.11a ranges are based on default power settings with 5-dBi omni on the access point and 6-dBi omni on the client.

The figure compares the range of the different data rates and the different WLAN standards in an open-office environment. Actual distances can be different because of absorption and reflection. The size of a wireless cell depends on the data rate. It is possible to limit the range by disabling lower data rates. To limit the range to 150 feet, data rates of 5.5, 2, and 1 Mbps (802.11b/g) and 6, 9, 12, and 18 Mbps (802.11g) could be disabled.

The figure shows the relative range of the different wireless standards and data rates. The absolute range depends on the environment, the equipment used, the access point configuration, antenna, and wireless client.

Ratified 802.11 Standards

This subtopic describes the ratified 802.11 standards.

Ratified IEEE 802.11 Standards

- 802.11: WLAN 1 and 2 Mbps at 2.4 GHz**
- 802.11a: WLAN 54-Mbps at 5 GHz**
- 802.11b: WLAN 11-Mbps at 2.4 GHz**
- 802.11d: Multiple regulatory domains**
- 802.11e: Quality of service**
- 802.11f: Inter-Access Point Protocol (IAPP)**
- 802.11g: WLAN 54-Mbps at 2.4 GHz**
- 802.11h: Dynamic Frequency Selection (DFS)
Transmit Power Control (TPC) at 5 GHz**
- 802.11i: Security**
- 802.11j: 5-GHz channels for Japan**

<http://standards.ieee.org/getieee802/>

© 2006 Cisco Systems, Inc. All rights reserved.BCMSN v3.0—6-23

The 802.11a, 802.11b, and 802.11g specifications all relate to WLAN physical layer standards.

Cisco Aironet Access Points support the 802.11d standard for world mode. World mode enables the access point to inform an 802.11d client device which radio setting the device should use to conform to local regulations.

The IEEE 802.11e standard was developed to enhance the current 802.11 MAC standard. The 802.11e standard expands support for applications with quality of service (QoS) requirements and improves the capabilities and efficiency of the WLAN datalink layer. This standard will assist with voice, video, and other time-sensitive applications. It was ratified in October 2005.

The IEEE 802.11f standard is a recommended practice guideline that defines a protocol for intercommunication between access points. It assists in roaming and handoff of traffic. Most vendors have implemented their own proprietary Inter-Access Point Protocol (IAPP) for use with their access points.

The IEEE 802.11h standard is supplementary to the MAC layer to comply with European regulations for 5-GHz WLANs. Most European radio regulations for the 5-GHz band require products to have TPC and DFS. TPC limits the transmitted power to the minimum that is needed to reach the farthest user. DFS selects the radio channel at the access point to minimize interference with other systems, particularly radar.

The IEEE 802.11i standard specifies the improved security, encryption, and authentication for WLANs and the enhancements to the current 802.11 MAC standard to provide improvements in security.

The IEEE 802.11j standard adds channel selection for the 5-GHz band in Japan, to conform to Japanese rules on operational mode, operational rate, radiated power, spurious emissions, and channel sense.

Worldwide Availability

This subtopic describes the worldwide compliance with RF regulations of Cisco Systems WLAN products.

Worldwide Availability

310P_006

<http://www.cisco.com/go/aironet/compliance>

© 2006 Cisco Systems, Inc. All rights reserved.BCMSN v3.0—6-24

In most parts of the world, Cisco products can be deployed without a user license (that is, unlicensed). In most countries, there is more than 80 MHz of available spectrum.

The 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 5.150 GHz to 5.825 GHz, as does the maximum power, which is determined by the local regulating country.

The Cisco Aironet products and the specific countries for which each product is currently certified for order and shipment are listed in the Wireless LAN Compliance Status at www.cisco.com/go/aironet/compliance. This document is important because not all products or versions of Cisco WLAN products are certified in all countries.

General Office WLAN Design

This topic explains the WLAN design for an office.

General Office WLAN Design

- **Eight 802.11g access points deployed**
- **7 users per access point with no conference rooms provides 3.8 Mbps throughput per user**
- **7 users + 1 conference room (10 users) = 17 total users, provides 1.5 Mbps throughput per user**

54 Cubes—4 Conference Rooms

120 Feet

95 Feet

© 2006 Cisco Systems, Inc. All rights reserved. BCM5N v3.0—6-25

In this general office design, 802.11g products with a maximum data rate of 54 Mbps are deployed. Throughput is data rate minus overhead. The throughput is about 50 percent of the data rate or less.

- 7 users per access point with no conference rooms provides 3.8 Mbps throughput per user
- 7 users + 1 conference room (10 users) = 17 total users; provides 1.5 Mbps throughput per user

WLAN Best Practices

This subtopic describes the best practices for scaling wireless cells.

WLAN as a Shared Medium: Best Practices

- 2.4-GHz 802.11b bandwidth calculations**
 - 25 users per cell; general office maximum users limited by bandwidth
 - Peak true throughput 6.8 Mbps
 - $6.8 \text{ Mbps} * 1024/25 = 278.5 \text{ kbps per user}$
- 2.4-GHz 802.11g bandwidth calculations**
 - 20 users per cell; general office maximum users limited by bandwidth
 - Peak true throughput 32 Mbps
 - $32 \text{ Mbps} * 1024/20 = 1683 \text{ kbps per user}$
- 5-GHz 802.11a bandwidth calculations**
 - 15 users per cell; general office users limited by coverage, not bandwidth
 - Peak true throughput 32 Mbps
 - $32 \text{ Mbps} * 1024/15 = 2188 \text{ kbps per user}$

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0—6-26

The figure shows the throughput calculations for 802.11b, 802.11g, and 802.11a wireless cells.

- 802.11b
 - 25 users per wireless cell
 - 278.5 kbps peak throughput per user
- 802.11g
 - 20 users per wireless cell
 - 1683 kbps peak throughput per user
- 802.11a
 - 15 users per wireless cell
 - 2188 kbps peak throughput per user

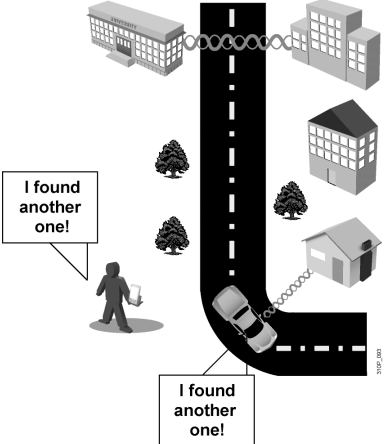
Higher data rates and the higher frequency of 802.11a result in smaller wireless cells. This approach means that fewer users in an office are within a wireless cell, which results in a higher average throughput per user.

WLAN Security

This topic describes the needs and solutions for security in the WLANs.

Why WLAN Security?

- **Wide availability and low cost of IEEE 802.11 wireless equipment**
- **802.11 standard ease of use and deployment**
- **Availability of sniffers**
- **Statistics on WLAN security**
- **Media hype about hot spots, WLAN hacking, war driving**
- **Nonoptimal implementation of encryption in standard Wired Equivalent Privacy (WEP) encryption**
- **Authentication vulnerability**



The illustration shows a person on the left and a car on the right, both with speech bubbles that say "I found another one!". They are positioned around a large, stylized letter 'L' that represents a road. The road is black with white dashed lines. Buildings and trees are scattered around the road, and a signal icon is shown near the car.

© 2004 Cisco Systems, Inc. All rights reserved. BCM5N v3.0-4-28


With the cost of 802.11b systems decreasing, it is inevitable that hackers will have many more unsecured WLANs to choose from. 802.11b sniffers enable network engineers to passively capture data packets so that they can be examined to correct system problems. But sniffers can also be used by hackers to capture data packets.

“War driving” is a phrase that describes the use of a cellular scanning device to look for cell phone numbers to exploit. Recently, the definition of war driving has been expanded to include someone driving around with a laptop and an 802.11b client card, looking for an 802.11b system to exploit.

Numerous open-source applications have reportedly been used to collect and exploit vulnerabilities in the 802.11 standard security mechanism, Wired Equivalent Privacy (WEP). With basic WEP encryption (or with no encryption) enabled, it is possible to collect data and obtain sensitive network information such as user login information, account numbers, and personnel records.

WLAN Security Threats

This subtopic lists the threats to WLAN security.

WLAN Security Threats		
"WAR DRIVERS"	HACKERS	EMPLOYEES
Find "Open" Networks; Use Them to Gain Free Internet Access	Exploit Weak Privacy Measures to View Sensitive WLAN Info and Even Break into WLANs	Plug Consumer-Grade APs/Gateways into Company Ethernet Ports to Create Own WLANs
		

© 2006 Cisco Systems, Inc. All rights reserved. BCM5N v3.0-6-29

These are some of the threats to WLAN security:

- War drivers trying to find open access points for free Internet access
- Hackers trying to exploit weak encryption to access sensitive data via the WLAN
- Employees installing access points for home use without the necessary security configuration on the enterprise network

Mitigating the Threats

This subtopic explains how the threats to WLAN security can be mitigated.

Mitigating the Threats		
Control and Integrity	Privacy and Confidentiality	Protection and Availability
Authentication	Encryption	Intrusion Detection System (IDS)
Ensure that legitimate clients associate with trusted access points.	Protect data as it is transmitted and received.	Track and mitigate unauthorized access and network attacks.

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0—6-30

To secure a WLAN, these steps are required:

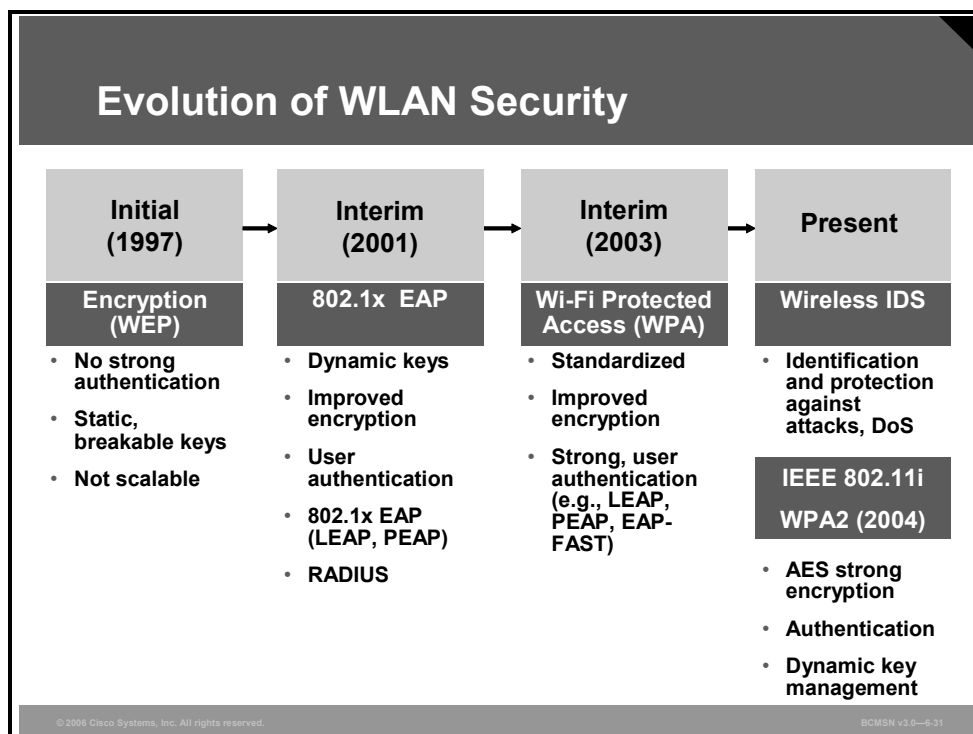
- Authentication to ensure that legitimate clients and users access the network via trusted access points
- Encryption for providing privacy and confidentiality
- Protection from security risks and availability with intrusion detection and intrusion protection systems for WLANs

Authentication and encryption protect the wireless data transmission.

Intrusion detection systems monitor the wireless and wired network to detect and mitigate network attacks.

Evolution of WLAN Security

This subtopic describes the evolution of WLAN security.



Initially, IEEE 802.11 security relied on static keys for both encryption and authentication. The authentication method was not strong, and the keys were eventually compromised. Because the keys were administered statically, this method of security was not scalable to large enterprise environments.

Cisco introduced enhancements that allowed for the use of IEEE 802.1x authentication protocols and dynamic keys and 802.1x Extensible Authentication Protocol (EAP) authentication. Cisco also introduced methods to overcome the exploitation of the encryption keys with key hashing (per-packet keying) and message integrity checks. These methods are today known as Cisco Key Integrity Protocol (CKIP) and Cisco Message Integrity Check (CMIC).

The 802.11 committee began the process of upgrading the security of the WLAN. The Wi-Fi Alliance introduced WPA as an interim solution. This standard was a subset of the expected 802.11i security standard for WLANs that use 802.1x authentication and improved encryption.

WPA consists of user authentication, message integrity checks, Temporal Key Integrity Protocol (TKIP), and dynamic keys. It is similar to the Cisco enhancements but implemented differently. WPA also includes a passphrase or preshared key user authentication for home users, which is not recommended for enterprise security.

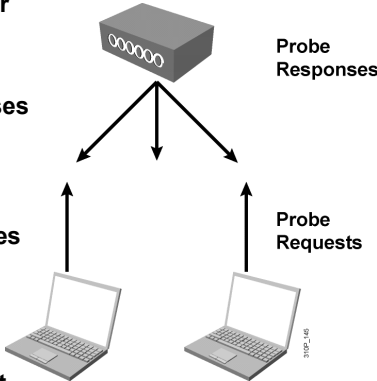
Today IEEE 802.11i has been ratified and Advanced Encryption Standard (AES) has replaced WEP as the latest and most secure method of encrypting data. Wireless intrusion detection systems are available to identify and protect the WLAN from attacks. The Wi-Fi Alliance certifies 802.11i devices under WPA2.

Wireless Client Association

This subtopic describes the association process of wireless clients.

Wireless Client Association

- **Access points send out beacons announcing SSID, data rates, and other information.**
- **Client scans all channels.**
- **Client listens for beacons and responses from access points.**
- **Client associates to access point with strongest signal.**
- **Client will repeat scan if signal becomes low to reassociate to another access point (roaming).**
- **During association SSID, MAC address and security settings are sent from the client to the access point and checked by the access point.**



The diagram illustrates the wireless client association process. At the top, a central access point (AP) is shown with three arrows pointing downwards to two laptops below. The arrows from the AP to the laptops are labeled 'Probe Responses'. From each laptop, an arrow points upwards back to the AP, labeled 'Probe Requests'. The AP is depicted as a rectangular box with a series of vertical lines on its front face, representing an antenna array. The laptops are shown from a three-quarter perspective, with their screens open.

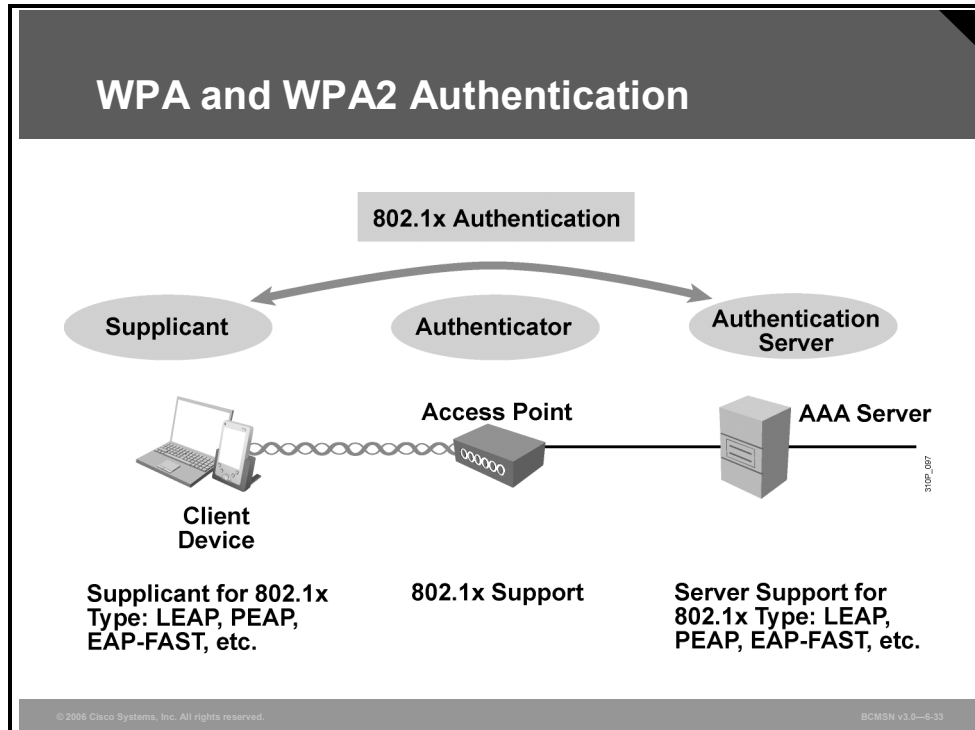
© 2006 Cisco Systems, Inc. All rights reserved.BCMSN v3.0—6-32

Access points send out beacons announcing one or more Service Set Identifiers (SSIDs), data rates, and other information. The client scans all the channels and listens for beacons and responses from the access points. The client associates to the access point that has the strongest signal.

If the signal becomes low, the client repeats the scan to associate with another access point (roaming). During association, the SSID, MAC address, and security settings are sent from the client to the access point and checked by the access point.

WPA and WPA2 Authentication

This subtopic describes WPA and WPA2 authentication.

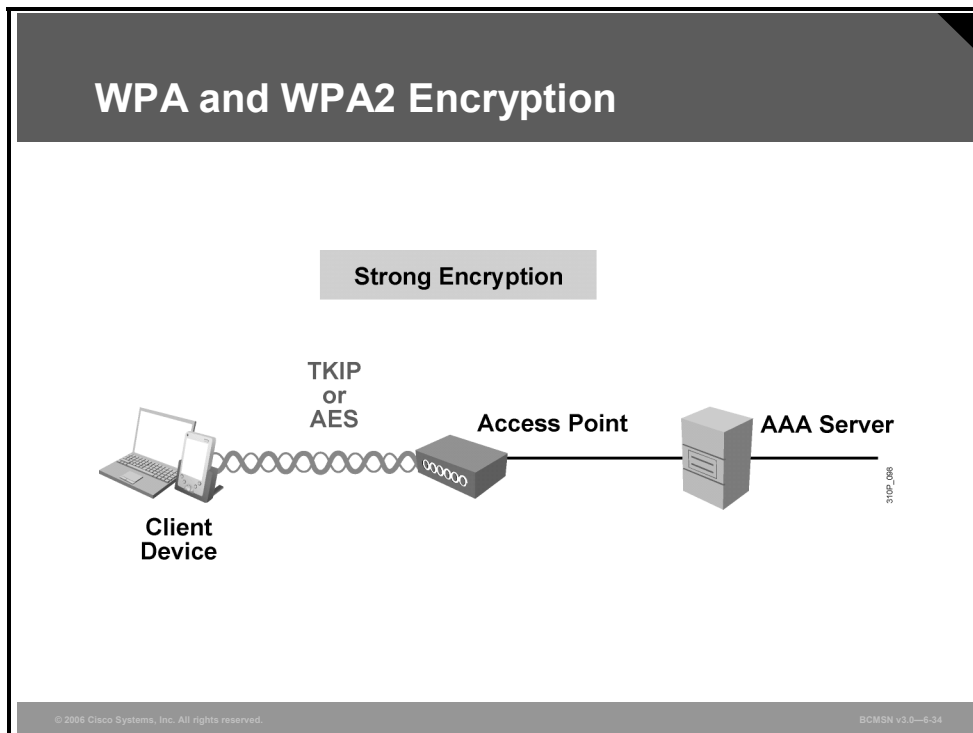


User authentication is done via the 802.1x protocol. A supplicant for 802.1x or EAP is needed on the WLAN client. The access point is the authenticator, which communicates via RADIUS with the authentication, authorization, and accounting (AAA) server, such as Cisco Secure ACS. Lightweight access points communicate with the WLAN controller, which acts as the authenticator.

The client and the authentication server implement different versions of EAP. The EAP messages pass through the access point as the authenticator.

WPA and WPA2 Encryption

This subtopic describes WPA and WPA2 encryption.

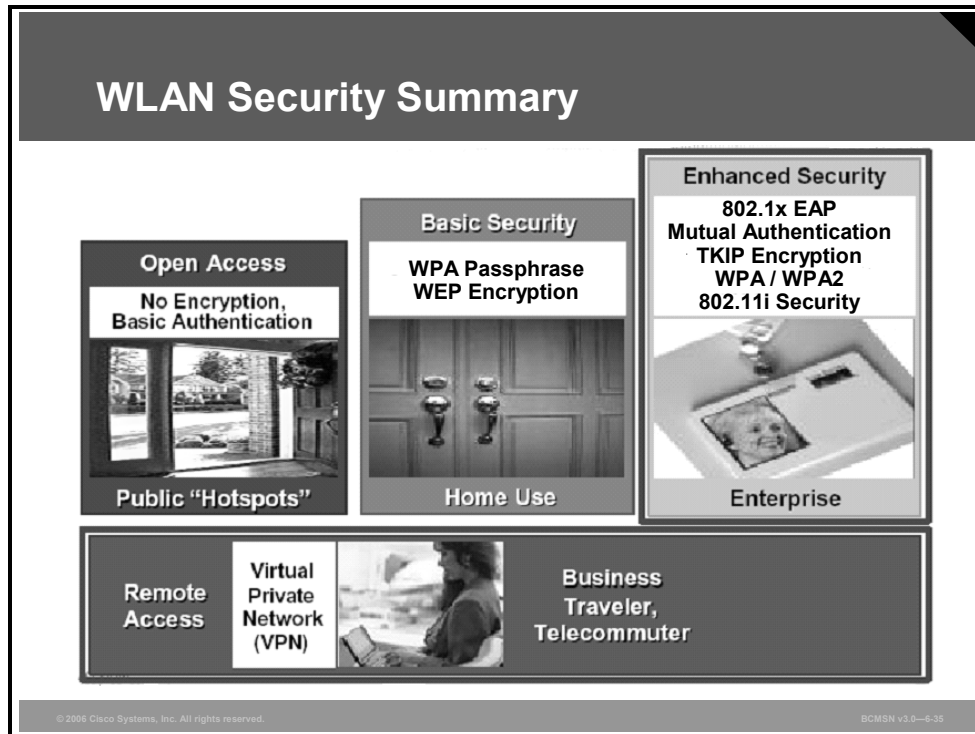


After authentication of the WLAN client, the data is sent encrypted. The basic encryption algorithm RC4 was originally used in WEP.

TKIP made the RC4 encryption more secure through increased size of initialization vector and per-packet key mixing while maintaining hardware compatibility. AES replaces the RC4 with a more cryptographically robust algorithm. WPA uses TKIP whereas WPA2 use AES or TKIP.

WLAN Security Summary

This subtopic summarizes the security issues in WLANs.



There are different security requirements for different types of WLANs.

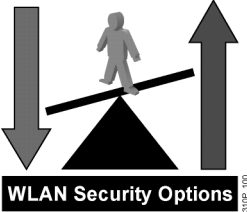
- For open access at hotspots, no encryption is required; only basic authentication is used.
- For the home user, at least basic security with WPA passphrase or preshared keys is recommended.
- For enterprises, enhanced security with 802.1x EAP authentication and TKIP or AES encryption is recommended. This is standardized as WPA or WPA2 and 802.11i security.

WLAN Security Evaluation

This subtopic describes how to evaluate security for your WLAN.

Security Evaluation

- Evaluate effectiveness of encrypted WLAN statistics.
- Focus on proper planning and implementation.
- Estimate potential security threats and the level of security needed.
- Evaluate amount of WLAN traffic being sent when selecting security methods.
- Evaluate tools and options applicable to WLAN design.



© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0—6-36

Security for a WLAN is just like security for any other network. Network security is a multilayered solution that requires commonsense evaluation and implementation. Obvious security fixes should be implemented first, such as limiting administrative access and disabling open access.

WLAN security is closely tied to the volume of traffic that traverses the network. Therefore, the use of statistics to evaluate the relative vulnerability of the network is a valuable step toward assessing WLAN security.

Attackers are more likely to attack unsecured WLANs. Proper planning and implementation is required:

- Estimate potential security threats and the level of security needed.
- Evaluate the amount of WLAN traffic being sent when selecting security methods.
- Evaluate tools and options that are applicable to WLAN design.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- **The 2.4-GHz and 5-GHz frequency bands are used by WLAN 802.11 standards.**
- **The throughput per user depends on the data rate and the number of users per wireless cell.**
- **802.11b has data rates of up to 11 Mbps at 2.4 GHz.**
- **802.11a has data rates of up to 54 Mbps at 5 GHz.**
- **802.11g has data rates of up to 54 Mbps at 2.4 GHz.**
- **802.11a has a shorter range than 802.11g.**
- **For maximum efficiency, limit the number of users per cell.**
- **Different WLAN security types with authentication and encryption satisfy the security requirements of enterprise and home users.**

Configuring Cisco WLAN Clients

Overview

This lesson describes the Cisco 802.11a/b/g wireless LAN (WLAN) client and utilities to configure the client adapter.

Objectives

Upon completing this lesson, you will be able to use Cisco Systems utilities to configure the Cisco WLAN client. This ability includes being able to meet these objectives:

- Install the Cisco WLAN client adapter and the Cisco Aironet Desktop Utility
- Use the Cisco ADU to configure the Cisco 802.11a/b/g WLAN client adapter
- Use the Cisco ADU for diagnostics and troubleshooting of the WLAN client adapters
- Use the Cisco Aironet Site Survey Utility to get information about available WLANs
- Describe the WLAN configuration through Windows XP
- Describe the Cisco ACAU
- Describe the Cisco Wireless IP Phone
- Describe the features and benefits of the Cisco Compatible Extensions program

Cisco 802.11a/b/g WLAN Client Adapters

This topic describes the Cisco 802.11a/b/g WLAN client adapters.

Cisco 802.11a/b/g WLAN Client Adapters

802.11a/b/g dual-band client adapters

- Supports all three current standards
 - 54 Mbps in 2.4 and 5 GHz bands
 - 802.11b support provides investment protection
- CardBus or PCI card
- Supported operating systems
 - Windows 2000 and Windows XP
- Utilities
 - ADU: Aironet Desktop Utility
 - ACM: Aironet Client Monitor
 - ACAU: Aironet Client Administration Utility



The image shows three Cisco Aironet 802.11a/b/g WLAN client adapters: a CardBus adapter, a PCI card, and a desktop antenna adapter. The CardBus adapter is a small, thin device with a black plastic casing and a gold-plated edge connector. The PCI card is a larger, rectangular circuit board with a gold-plated edge connector and various components. The desktop antenna adapter is a black plastic device with a vertical antenna and a USB connector.

© 2004 Cisco Systems, Inc. All rights reserved. BCM5N v3.0-4-2

The Cisco 802.11a/b/g wireless client adapters are supported only by Windows 2000 and Windows XP.

The Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) support IEEE 802.11a, IEEE 802.11b, and IEEE 802.11g (2.4 GHz and 5 GHz).

A description of the appearance of LED 0 and LED 1 for the CardBus and Peripheral Component Interconnect (PCI) cards follows:

- **Power save mode:** Slow blink, off
- **Awake from power save mode:** On, off (can be used to indicate power is applied; the hardware automatically enters this state after exiting from power save mode before any other activity)
- **Looking for network association:** Alternate blink between LED 1 and LED 0
- **Associated or joined with network, no activity:** Slow simultaneous blink
- **Associated or joined with network, activity:** Fast simultaneous blink (blink rate increases with activity)

Cisco Aironet Client Adapter Installation

This subtopic describes the installation of the WLAN adapter.

Client Adapter Installation Wizard

- **Requires a forced reboot at the completion of the install (prompts in the beginning as a warning).**
 - Protection to ensure that machine is left in a stable state.
- **Shows multiple status screens.**
 - Drivers, ADU, firmware, LEAP, and so on.
- **Card must be inserted at the beginning of the setup and must be identified by the computer as new hardware. (If it is not identified as new hardware, reboot the laptop.)**

© 2006 Cisco Systems, Inc. All rights reserved.BOMSN v3.0-6.3

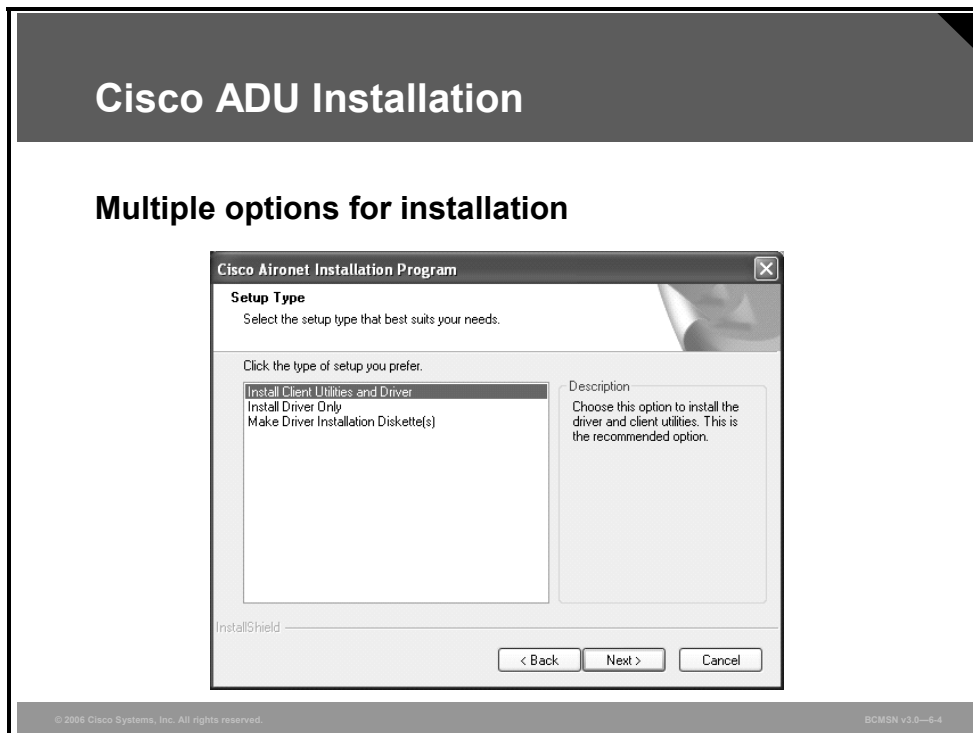
The installation wizard tool is in the file WinClient-802.11a-b-g-Ins-Wizard-v26.exe. Check <http://www.cisco.com> for later versions of this software.

Installation requires a reboot at completion. This forced reboot can be suppressed by administrators who are installing other applications simultaneously; however, a reboot is strongly recommended at the end of the installations, and additional testing is also recommended.

If a card is not inserted during initial installation, drivers will be loaded in addition to utilities. After a card has been inserted, the rest of the installation takes place automatically.

Cisco Aironet Desktop Utility Installation

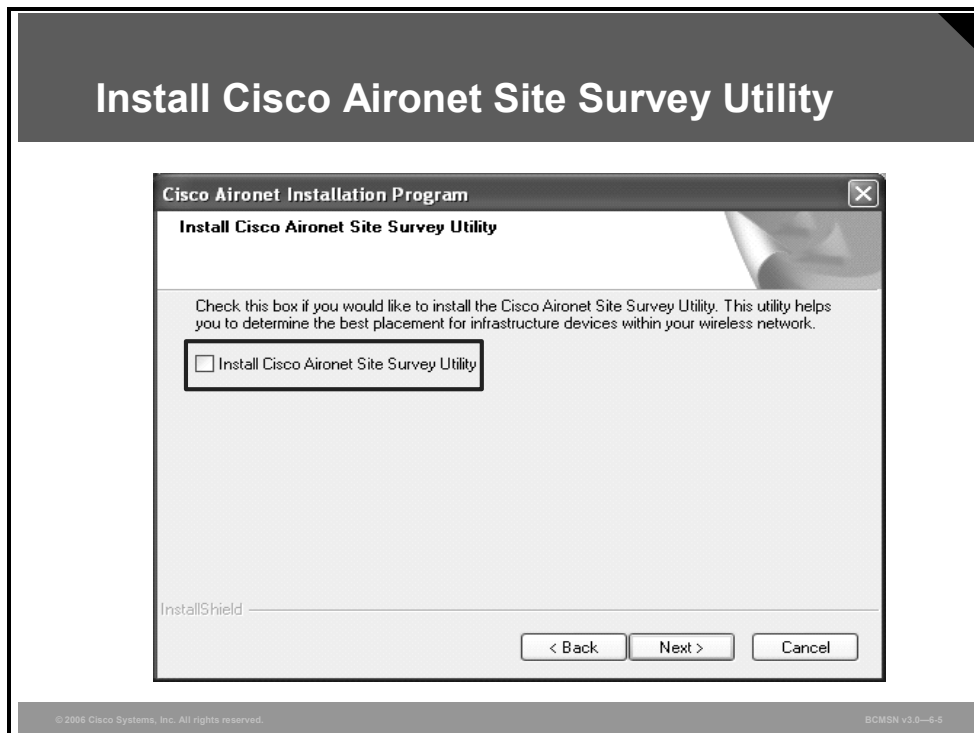
This topic describes Cisco Aironet Desktop Utility (ADU) installation.



The setup utility allows you to install the driver, desktop utility, or both.

Cisco Site Survey Utility Installation

This subtopic describes the Site Survey Utility installation.

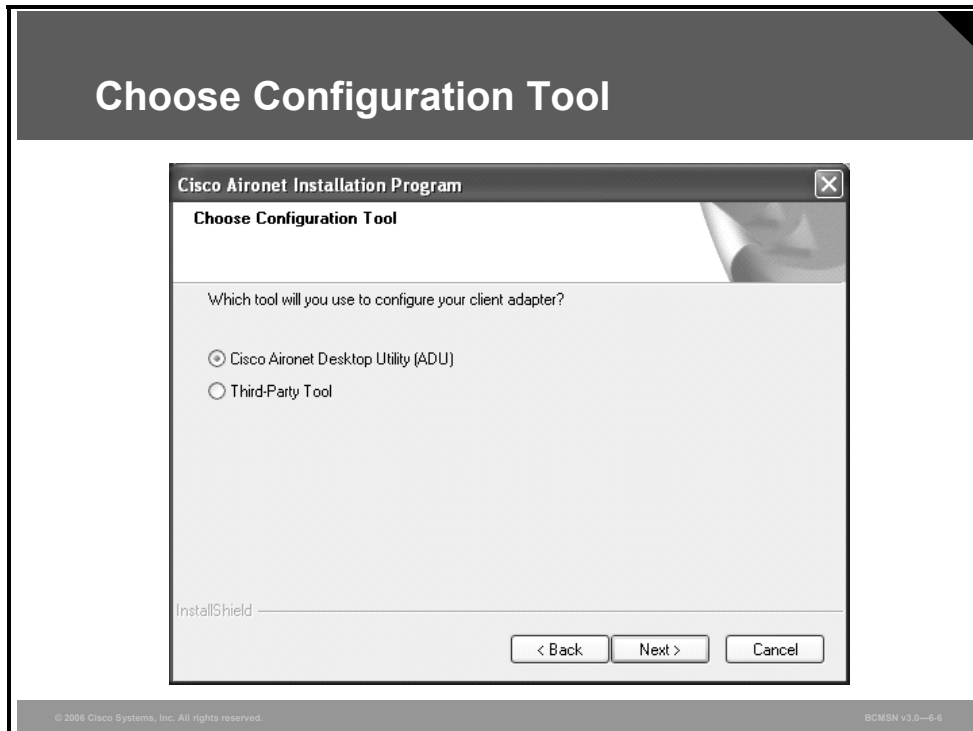


The figure shows one step in the Cisco Aironet installation process.

The Site Survey Utility for the 802.11 a/b/g card is an additional program that can be installed with the ADU. This new Cisco Aironet Site Survey Utility is available with ADU release 2.0.X and later. To install, make sure that you select the **Install Cisco Aironet Site Survey Utility** checkbox.

Choose Configuration Tool

This subtopic describes how to choose the WLAN adapter configuration tool.



On Windows XP, you can configure your Cisco Aironet Wireless LAN Client Adapter through the Cisco ADU or a third-party tool, such as the Microsoft Wireless Configuration Manager.

Because third-party tools may not provide all the functionality available in ADU, Cisco recommends that you use ADU. (Please note that a patch from Microsoft might be required to use the Microsoft tool with Wi-Fi Protected Access [WPA] security.)

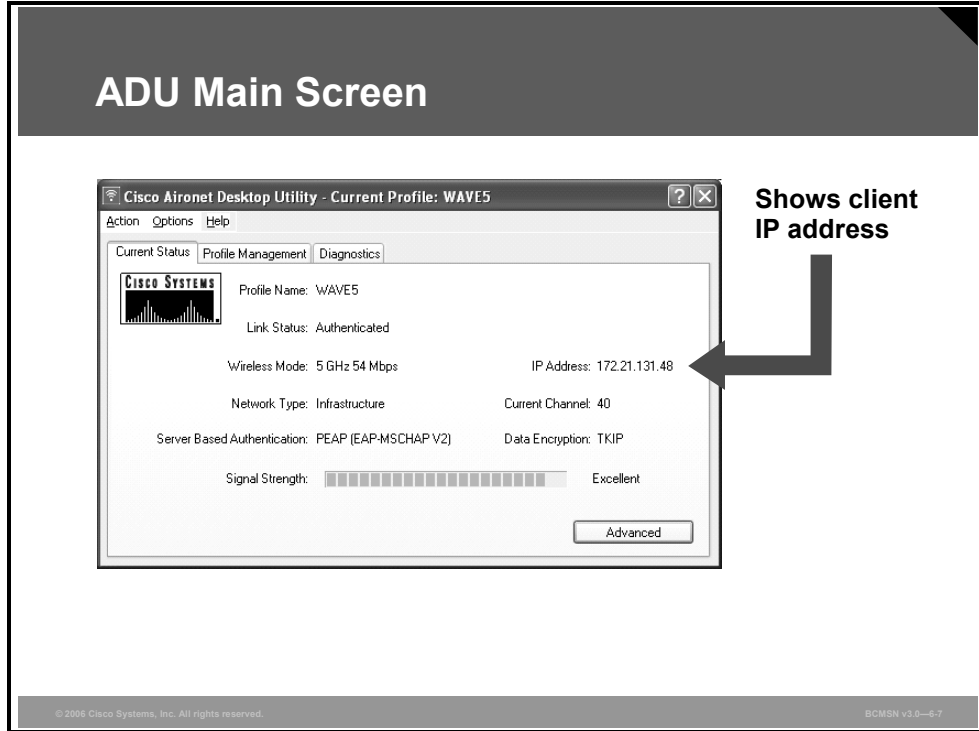
On the next screen, select whether you want to use ADU or a third-party tool to configure your client adapter.

By enabling the third-party tool, you allow the client card to be controlled by another service, such as Windows XP Wireless Zero Config.

Note If you select a third-party tool, some of the ADU features will not be available. To activate those features, you must reinstall ADU.

Cisco ADU Main Screen

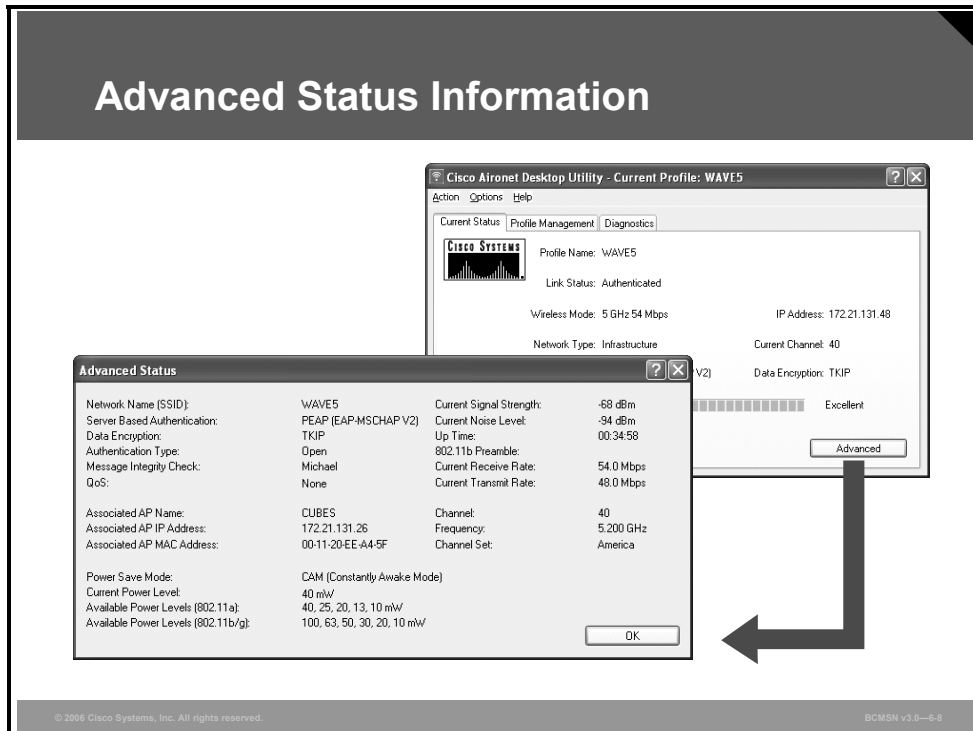
This subtopic describes the main screen of the Cisco ADU.



ADU works with AIR-CB21AG and AIR-PI21AG. The figure shows the main status screen of the ADU on the Current Status tab. This screen shows signal strength, association, IP address, and channel. For more details, click the **Advanced** button.

ADU: Advanced Status Information

This subtopic describes the advanced status information within ADU.

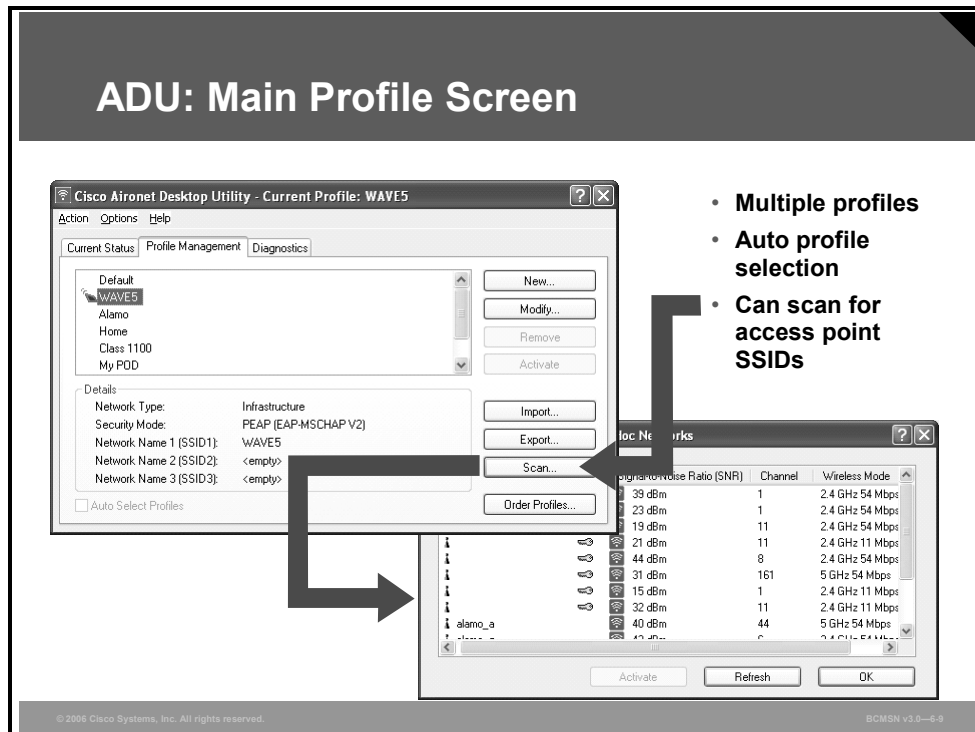


The ADU main page does not list information about associated access points; however, selecting the Advanced button displays the Advanced Status tab, which provides that information.

Current signal strength and noise level can be shown in either dBm or percent. You can change this setting from the Options menu.

ADU: Main Profile Screen

This subtopic describes the main screen for profile configuration.

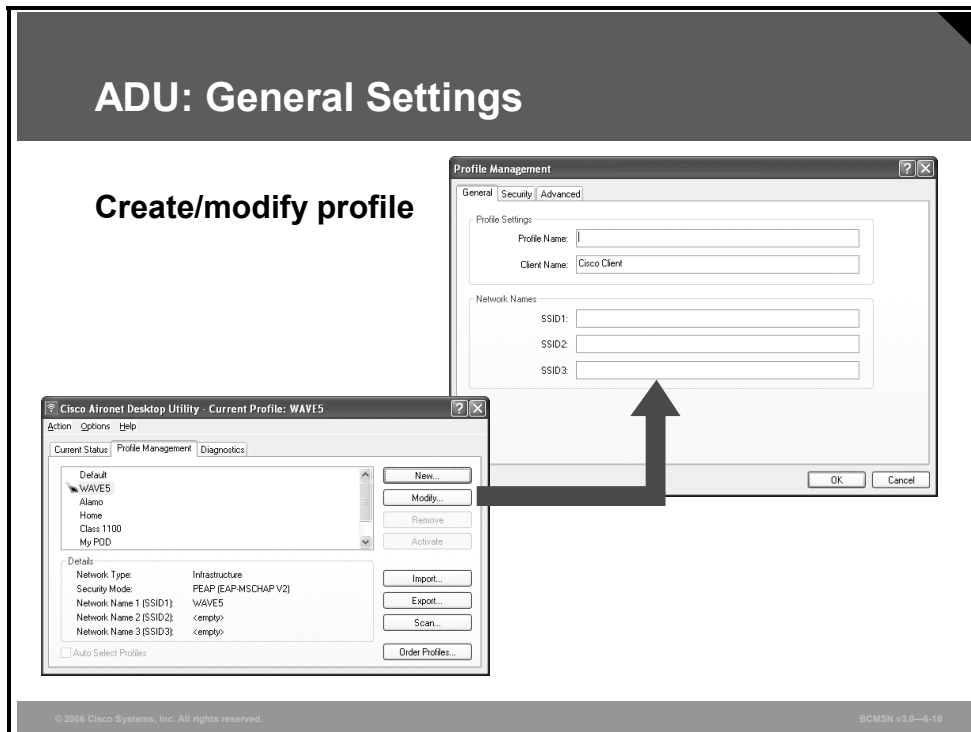


The Profile Management tab offers these features:

- Create up to 16 profiles; each profile can be imported or exported.
- Set auto profile selection and weight the profiles according to your preferences.
- Scan the card to get a list of all open Service Set Identifiers (SSIDs), and directly connect to one of them.

ADU: General Settings

This subtopic describes the configuration of profiles within ADU.

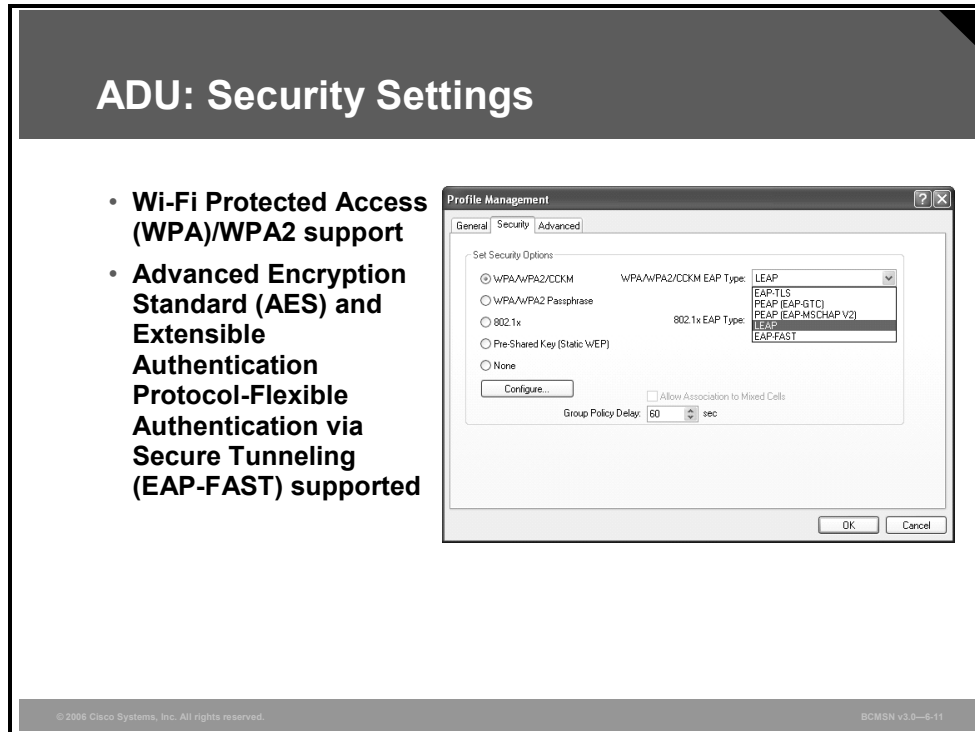


The figure shows how to create and modify profiles. The General tab includes these settings:

- Profile name
- Wireless computer name (default: Windows computer name)
- Up to three SSIDs

ADU: Security Settings

This subtopic describes the security settings for profiles within ADU.



- **Wi-Fi Protected Access (WPA)/WPA2 support**
- **Advanced Encryption Standard (AES) and Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) supported**

The figure shows how to configure and modify security in the profiles. WPA and WPA2 are supported as of version 2.0.X.

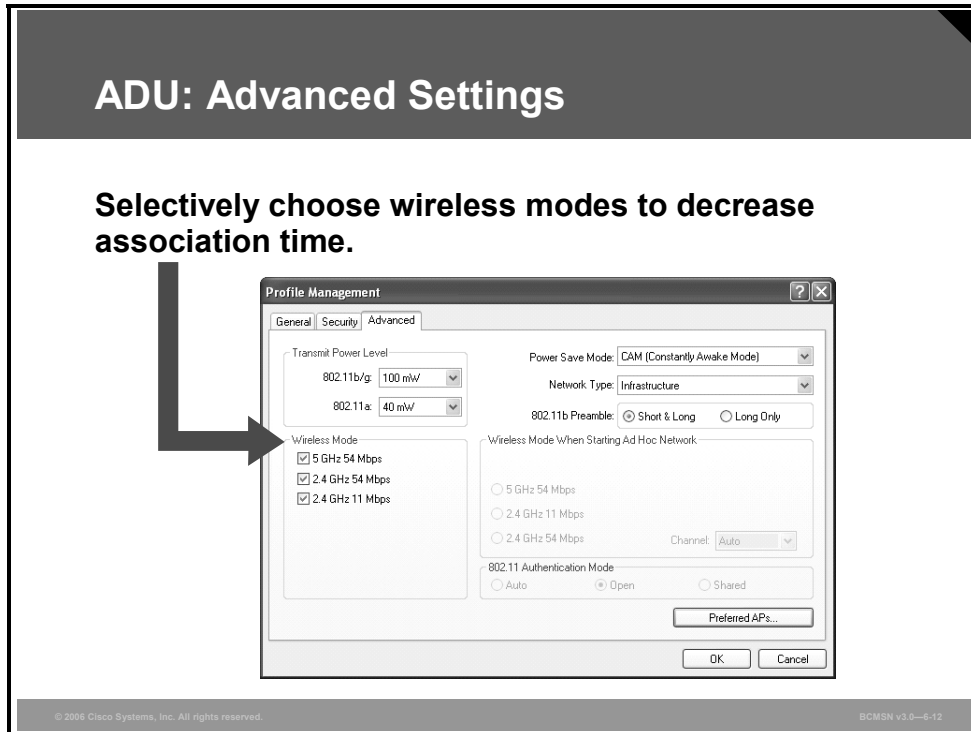
Static WEP keys are selected as Pre-Shared Key (Static WEP).

WPA/WPA2 Passphrase selects WPA/WPA2 Pre-shared Keys (PSK).

Additional parameters for the selected security method have to be configured by clicking the Configure button.

ADU: Advanced Profile Settings

This subtopic describes advanced settings within the ADU profile management.

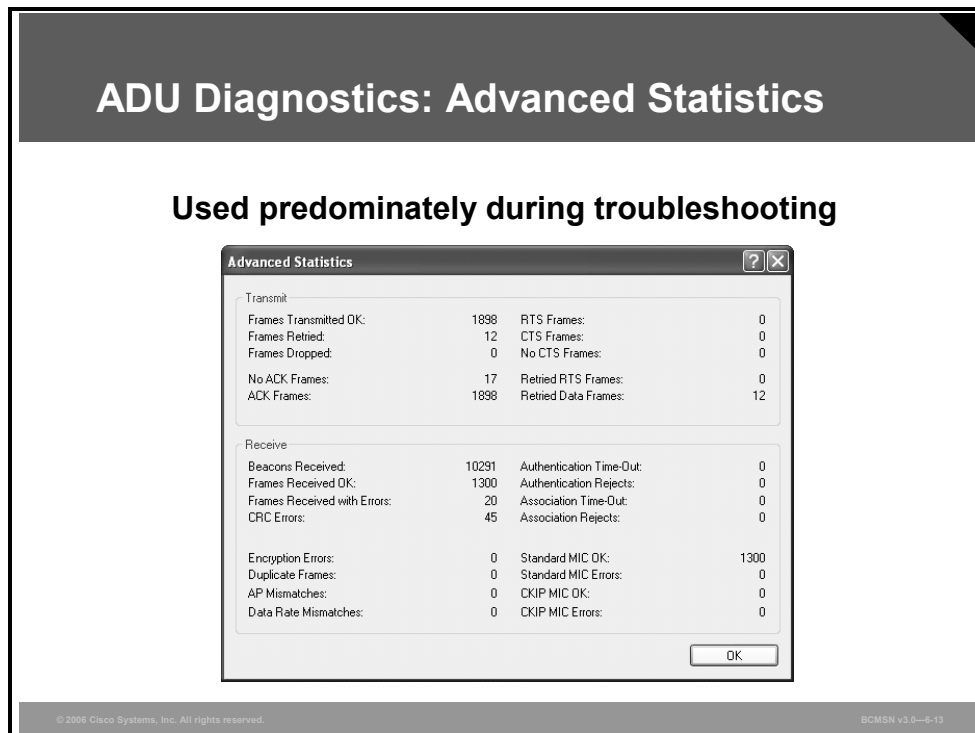


Selectively choose wireless modes to decrease association time.

To increase connection speed, disable different wireless modes that are known to be unavailable. The maximum transmit power of the Cisco client adapter for IEEE 802.11a is 40 mW; for IEEE 802.11b/g, it is 100 mW.

ADU Diagnostics: Advanced Statistics

This topic describes the advanced statistics within ADU.

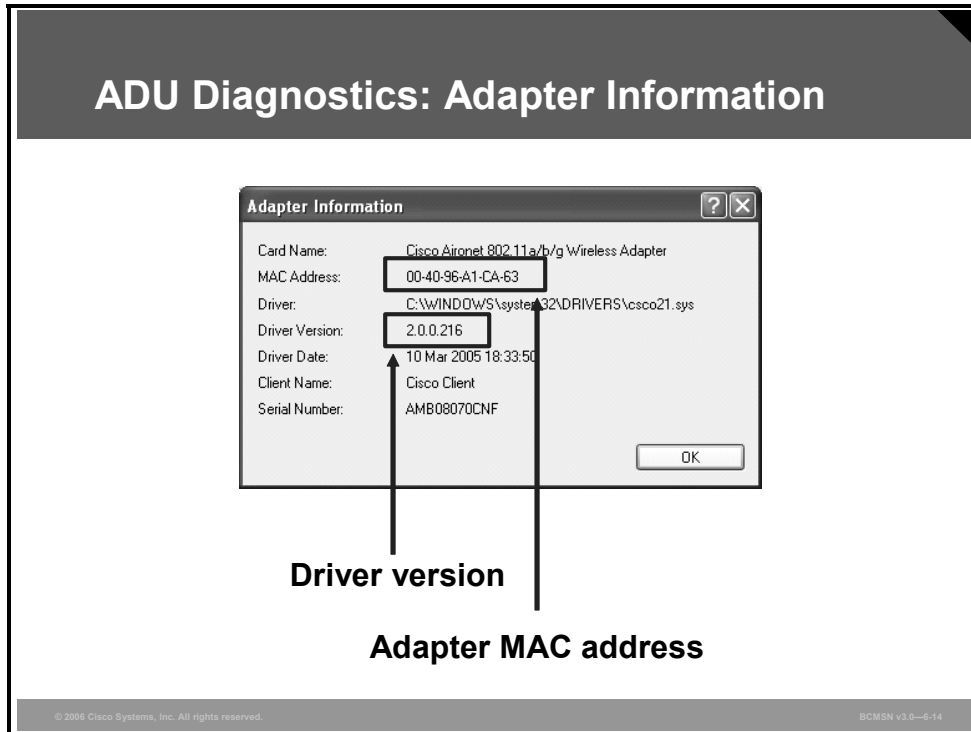


On the Diagnostics tab on the main screen of ADU, you can select Advanced Statistics to see detailed receive and transmit statistics of the adapter. This information is often used for troubleshooting.

The Advanced Statistics dialog box shows the transmit and receive statistics and encryption errors.

ADU Diagnostics: Adapter Information

This subtopic describes the adapter information within ADU.



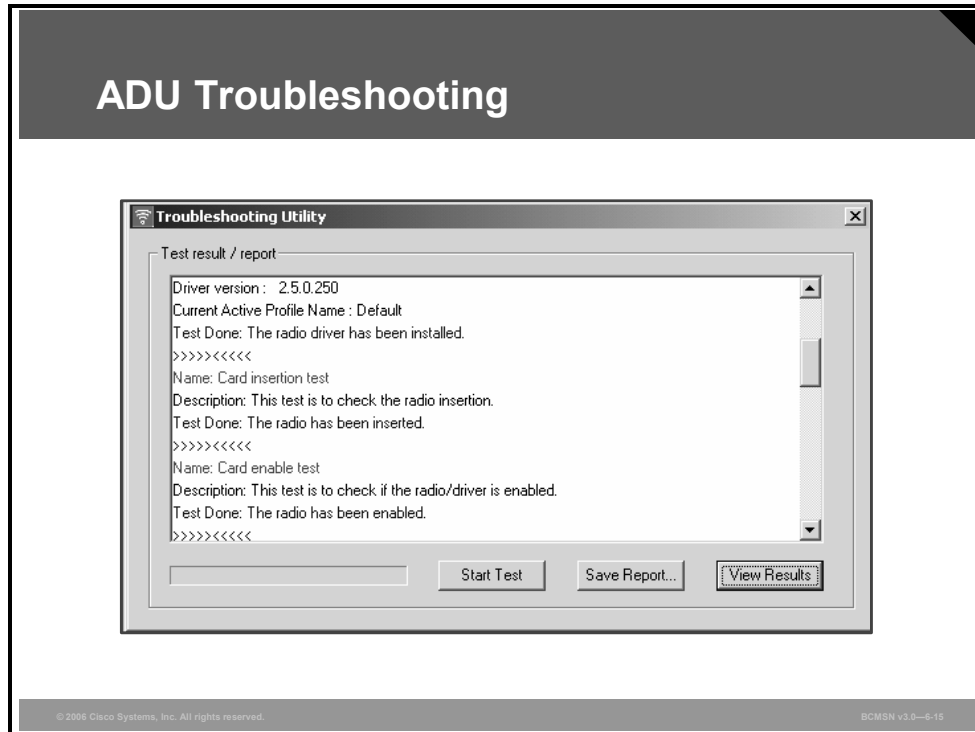
On the Diagnostics tab on the main screen of ADU, you can select Adapter Information.

The Adapter Information dialog box includes this information:

- WLAN adapter type
- Client adapter MAC address
- Driver file and version
- Adapter serial number

ADU Troubleshooting

This subtopic describes the troubleshooting utility of ADU.

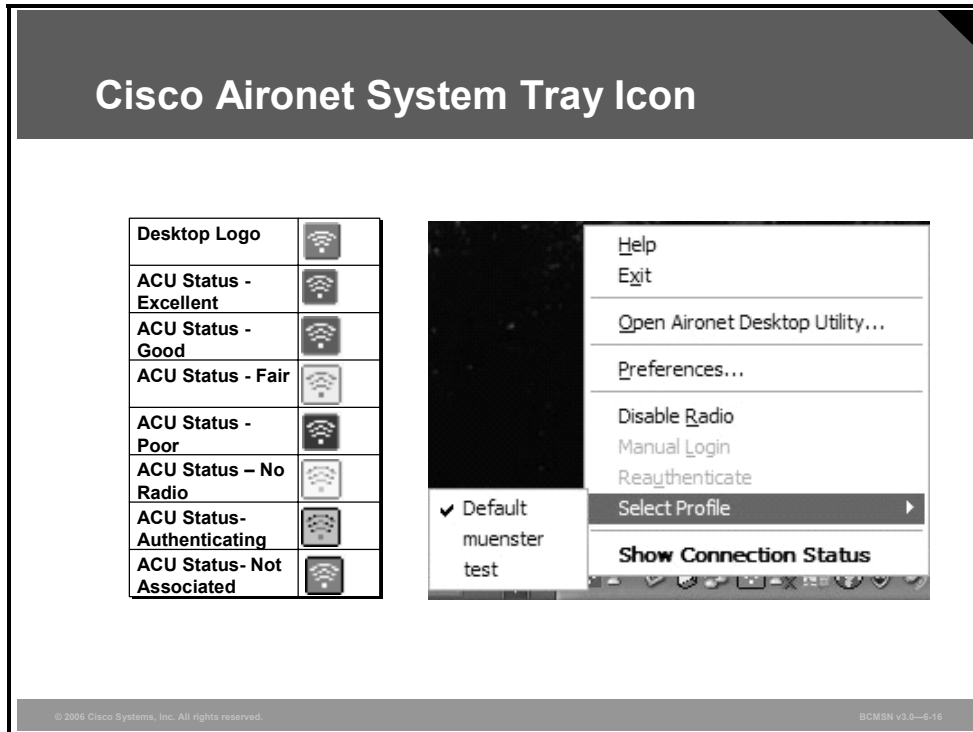


You can start the ADU troubleshooting utility from the Diagnostics tab of the main screen or from the system tray icon. This utility tests the card, driver, radio, association, and network connectivity.

Click the **Start Test** button to execute the test. Click **View Results** to display the detailed results.

Cisco Aironet System Tray Icon

This subtopic describes the system tray icon for the WLAN client adapter.

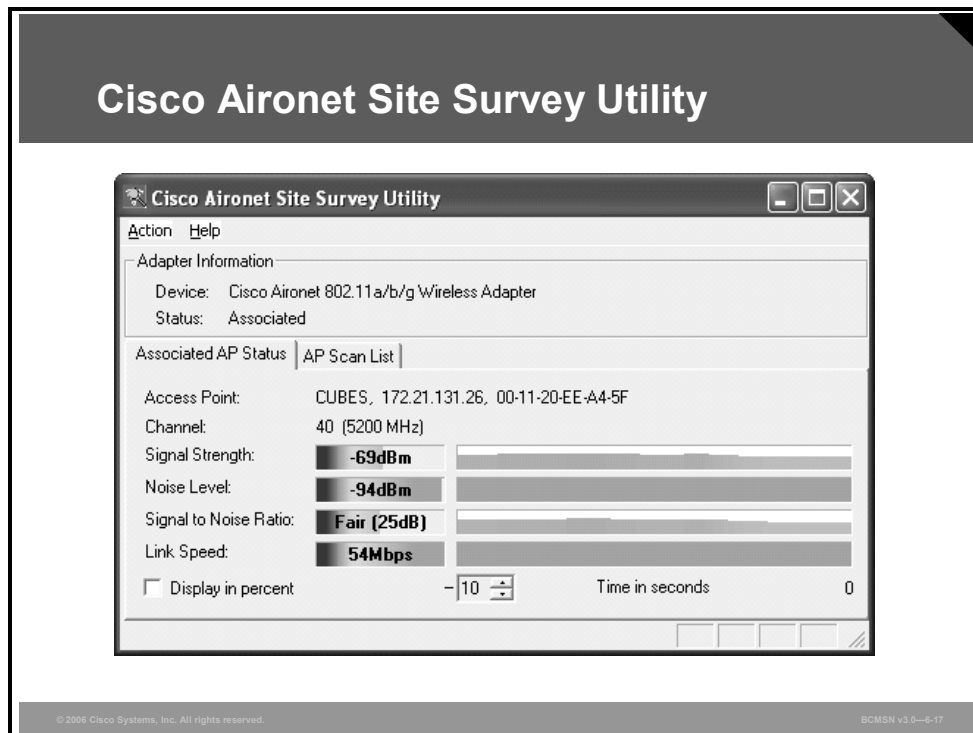


The Aironet Monitor provides a system tray icon, which allows you to open the ADU, disable and enable the radio, select profiles, and display the connection status and IP address.

If security with authentication is configured in the active profile login, reauthentication can be initiated from the system tray icon.

Cisco Aironet Site Survey Utility: Associated AP Status

This topic describes the Associated AP Status tab of the Cisco Aironet Site Survey Utility.



The Site Survey Utility monitors transmitted network traffic, and the link speed reflects the current transmit rate of data packets.

The Associated AP Status tab includes this information:

- **Adapter Information:** Identifies the selected network adapter and the current association status. The association status options are Associated, Not Associated, and Device Not Present.
- **Access Point:** Identifies the name, IP address, and MAC address of the access point.
- **Channel:** Identifies the channel number and frequency.
- **Signal Strength:** Shows how strong the signal is for all received packets. The higher the value and the more green the bar graph, the stronger the signal. The trend graph provides a visual interpretation of the current signal strength. Differences in signal strength are indicated by these colors: green (strongest), yellow (middle of the range), and red (weakest).
- **Signal Quality:** Shows how clear the signal is for all received packets. The higher the value and the more green the bar graph, the clearer the signal. The trend graph provides a visual interpretation of the current signal quality. Differences in signal quality are indicated by these colors: green (highest quality), yellow (average), and red (lowest quality).

Note The Signal Quality setting appears only if the Display in percent check box is selected.

- **Noise Level:** Shows the level of background radio frequency (RF) energy. The lower the value and the more green the bar graph, the less the background noise. The trend graph provides a visual interpretation of the current level of background noise. Differences in background noise are indicated by these colors: green (low noise), yellow (middle of the range), and red (high noise).

Note The Noise Level setting appears only if the Display in percent check box is not checked.

- **Signal to Noise Ratio:** Shows the percentage of beacon packets received versus those expected to be received. The higher the value and the more green the bar graph, the clearer the signal. For example, if the access point sends out 10 beacons per second, you would expect the client adapter to receive 50 beacon packets in 5 seconds. If it receives only 40 packets, the percentage of beacons received would be 80 percent.

Note The Signal to Noise Ratio setting appears only if the Display in percent check box is checked.

- **Overall Link Quality:** Shows the ability of the client adapter to communicate with the access point. Possible values are Poor, Fair, **Good**, or Excellent.

Note The Overall Link Quality setting appears only if the Display in percent check box is checked.

- **Link Speed:** Shows a trend graph providing a visual interpretation of the current rate at which your client adapter is transmitting packets. Possible values are 1, 2, 5.5, or 11 Mbps (IEEE 802.11b); 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps (802.11g); 6, 9, 12, 18, 24, 36, 48, or 54 Mbps (IEEE 802.11a).

Display in percent: The default is to display the fields in dB or dBm. If you would rather view the values as a percentage, check the **Display in percent** check box. The decibels display unit is recommended for a more precise view. The fields that appear on this screen vary, depending on which method of display you choose.

- The trend graph provides a graphical representation of activity in the past 10 to 60 seconds. Use the up and down arrows to select the desired number of seconds.

The Cisco Aironet Site Survey Utility works with all Cisco Aironet Wireless Adapters.

Cisco Aironet Site Survey Utility: AP Scan List

This subtopic describes the AP Scan List tab of the Cisco Aironet Site Survey Utility.

Cisco Aironet Site Survey Utility (Cont.)

Cisco Aironet Site Survey Utility

Action Help

Adapter Information

Device: Cisco Aironet 802.11a/b/g Wireless Adapter

Status: Associated

Associated AP Status: AP Scan List

Pause List Update View AP Details Log Snapshot

Network Name	MAC Address	RSSI	Data Enc.	Type	Ch. (Freq.)	Max Rate	AP Name	Load	CCX	Other Info.
↑	00:11:21:F...	-61	Secure	G	1 (2412)	54*	CUBES	0	2	Qos, R...
↑	00:12:00:6...	-77	Secure	G	1 (2412)	54*	Ex_Conf	0	2	Qos, R...
↑	00:02:6F:0...	-57	Secure	B	11 (2462)	11				
↑	00:12:00:6...	-73	Secure	G	11 (2462)	54*	CiscoLab	0	2	Qos, R...
↑	00:12:44:B...	-56	Secure	G	8 (2447)	54	training...	0	2	Qos
↑	00:12:44:B...	-61	Secure	A	161 (58...	54	training...	0	2	Qos
↑	00:01:64:4...	-70	Secure	B	11 (2462)	11*	WARE...	0		
↑ alamo_a	00:0C:30:8...	-66	Open	A	44 (5220)	54	alamo1...	0	2	Qos
↑ alamo_g	00:12:00:C...	-54	Open	G	6 (2437)	54	alamo1...	0	2	Qos
↑ WAVE5	00:11:20:E...	-72	Secure	A	64 (5320)	54	CiscoLab	0	2	Qos, R...
↑ WAVE5	00:11:20:E...	-85	Secure	A	36 (5180)	54	Ex_Conf	0	2	Qos, R...
Open WAVE5	00:11:20:E...	-70	Secure	A	40 (5200)	54	CUBES	0	2	Qos, R...

© 2006 Cisco Systems, Inc. All rights reserved. BCM5N v3.0—6-18

The AP Scan List tab includes this information:

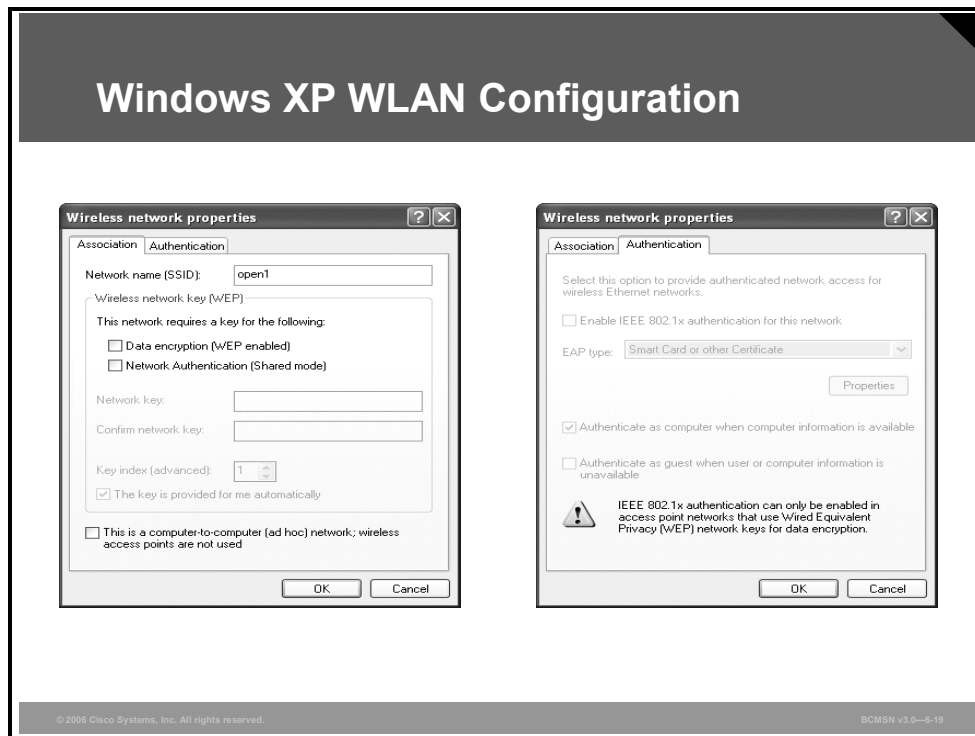
- **Network Name:** Identifies the SSID of the access point.
- **MAC Address:** Identifies the MAC address of the access point.
- **RSSI:** Identifies the received signal strength in dBm.
- **Data Enc.:** Indicates whether the data exchanged with this access point is encrypted. The possible values are Secure (encrypted) and Open (unencrypted).
- **Type:** Indicates whether the band of the access point radio is 802.11a, 802.11b, or IEEE 802.11g.
- **Ch. (Freq.):** Displays the channel number that is being used and the frequency of that channel (given in megahertz). Possible values depend on the client adapter radio and regulatory domain.
- **Max Rate:** Identifies the maximum data rate that is currently available on this access point.
- **AP Name:** Identifies the name of the access point (AP).
- **Load:** Identifies the access point load.
- **CCX:** Identifies which version of Cisco Compatible Extensions is supported by the access point. This parameter may be blank if the access point is not broadcasting its CCX version number.

- **Other Info:** Some of these columns may appear, depending on what is transmitted by the access point.
 - **Ad-Hoc:** Identifies the device as another client adapter operating in ad hoc mode.
 - **Power:** Indicates the presence of the cell power limit information element (IE). Broadcasting the cell power limit IE allows access points to limit the transmitting power used by clients.
 - **QoS:** Indicates that quality of service (QoS) is enabled. If QoS appears in the Other Info. column, you can open the AP Detailed Information window to get the QoS configuration.
 - **RM-Normal:** Indicates the presence of the radio management (RM) information. A value of 1 means normal. Other values may be displayed as RM-Status (123) for a status value of 123.
 - **RM-Source:** Indicates the presence of the radio management extensions and includes the MAC address of the RM source.
 - **SSIDL:** Indicates the presence and number of Service Set Identifier List IE (SSIDL IE) and the number of hidden SSIDs configured on that access point. An SSIDL broadcasts information about lists of hidden SSIDs on an access point.
 - **Pause List Update:** Click **Pause List Update** to halt the current AP scan list. If you click the button again, it will resume updating.
 - **View AP Details:** Launches the AP Detailed Information window for the currently selected row of the table.
 - **Log Snapshot:** Transfers the current contents of the table into the AP Scan List log. The scan log is a text file named SST_APScanLog.txt. It is located in the same directory as the main executable (SST.EXE).
 - **Count:** Indicates the number of rows currently displayed in the table.

If updating is in a paused state, the old data that is currently displayed in the log will be added, rather than the latest data available.

Windows XP WLAN Configuration

This topic shows the Windows XP WLAN configuration windows.



The figure shows the Windows XP WLAN configuration tool. This tool allows configuration of SSID and security settings.

Comparison of Windows XP and Cisco ADU

This subtopic compares the Windows XP and Cisco ADU for WLAN adapter configuration.

Comparison of Windows XP and Cisco ADU		
Feature	Windows XP	Cisco ADU
Configuration parameters	Limited	Extensive
Create profiles	Yes	Yes
Enable/disable radio	No	Yes
Static WEP	Yes	Yes
LEAP	No	Yes
EAP-TLS or PEAP	Yes	Yes
Status window	Limited	Extensive
Troubleshooting	No	Yes
Statistics	No	Yes

© 2006 Cisco Systems, Inc. All rights reserved. BCM5N v3.0—6-20

The full functionality of the WLAN adapter is available only via the ADU. Windows can be used to configure the WLAN adapter, but it has limited functionality.

Wireless networks with SSID-broadcasting disabled are not visible or accessible without the ADU. ADU allows you to disable the radio of the WLAN card, whereas Windows can disable the whole WLAN network information card (NIC).

Cisco Aironet Client Administration Utility

This topic describes the Cisco Aironet Client Administration Utility (ACAU).

Aironet Client Administration Utility (ACAU)

- **Creates file with profiles and settings**
- **Profiles imported during the installation of ADU and firmware**
 - **For AIR-CB21AG and AIR-PI21AG**
 - **Installs across network**
 - **Encrypted setup files**
 - **Windows 2000 and Windows XP only**

© 2006 Cisco Systems, Inc. All rights reserved.BCMSN v3.0-6-21

The Cisco Wireless Utility Auto Installer enables an administrator to install the Cisco ADU and the driver for the Cisco client adapter across a network, eliminating the need to install and configure the ADU on each wireless client. The auto installer runs in silent batch mode and installs and configures the ADU (thereby configuring the Cisco Aironet client adapter) on a computer that is running the Windows operating system.

The auto installer allows the administrator to selectively install and configure certain parameters, as follows:

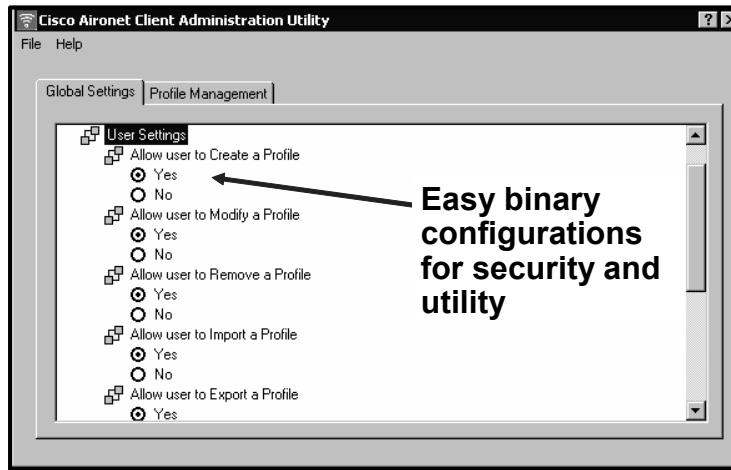
- The drive and directory where the ADU will be stored on the computer
- The folder where the ADU will be installed on the computer
- The drive and directory where client card firmware and drivers will be stored on the computer
- Profiles that will be installed on the computer with the software

Each profile allows the administrator to selectively configure these parameters on the ADU:

- Radio settings
- Wireless network settings
- Network security settings (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 ensure that network security is not compromised while performing auto installs.

Aironet Configuration Administration Utility




The figure shows the ACAU configuration of the general settings used by the ADU.

Cisco Wireless IP Phone

This topic describes the Cisco Wireless IP Phone.

Cisco Wireless IP Phone

- **For workers who need to communicate while moving about their workplace or campus**
- **Same features as Cisco wired IP Phones**
- **Graphical, menu-driven user interface**
- **Multiline appearance (up to six extensions)**
- **Phone book with speed dials**
- **LEAP security**
- **Auto VLAN configuration and Cisco CallManager registration**



© 2006 Cisco Systems, Inc. All rights reserved. BCM5N v3.0-6-23

The Cisco Wireless IP Phone solution enables enterprise users to globally answer business-critical calls anywhere on a corporate campus.

The Cisco Wireless IP Phone is equally adaptable for all mobile professionals, from managers on the move or in an office environment to associates working in the warehouse, on the sales floor, or in the call center. Users can also increase their availability as ever-broadening ranges of industries adopt WLANs.

The solution allows enterprises the flexibility to add coverage and capacity as needed to meet user needs. In addition, the Cisco wireless IP communications solution operates seamlessly with existing Cisco wired IP communications solutions on a single intelligent network. As with the other Cisco wireless offerings, the phone can use Lightweight EAP (LEAP) as an authentication mechanism to improve security.

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. The Cisco Wireless IP Phone is managed in the same way by the Cisco CallManager and Cisco CallManager Express as other Cisco IP Phones.

Refer to the Cisco Wireless IP Phone deployment guide for additional information.

Cisco Compatible Extensions Program for WLAN Client Devices

This topic describes the Cisco Compatible Extensions program for WLAN client devices.

Cisco Compatible Extensions

- No-cost licensing of technology for use in WLAN adapters and devices
- Independent testing to ensure interoperability with Cisco infrastructure
- Marketing of compliant products by Cisco and product suppliers under “Cisco Compatible” brand

Approved Suppliers

Silicon Suppliers

www.cisco.com/go/ciscocompatible/wireless

© 2006 Cisco Systems, Inc. All rights reserved. BCM5N v3.0—6-24

This program is known as Cisco Compatible Extensions for WLAN devices. This program will issue an evolving set of specifications for interoperability, and also will facilitate testing of vendor clients.

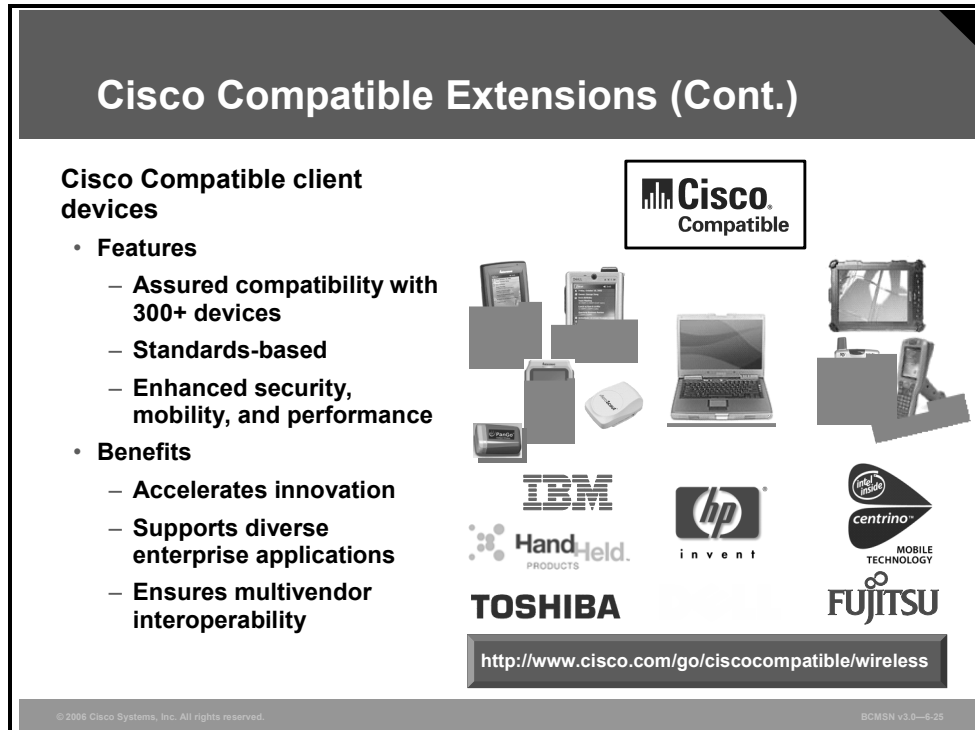
The Cisco Compatible Extensions program for WLAN devices provides tested compatibility with licensed Cisco infrastructure innovations. Compatibility is assured through extensive, independent testing of third-party devices.

The Cisco Compatible Extensions program enables the widespread availability of wireless client devices that take advantage of the Cisco Aironet wireless network, accelerating the availability of innovative features while maintaining interoperability.

Approved devices are listed at www.cisco.com/go/ciscocompatible/wireless and can also be found by looking for products displaying the Cisco Compatible logo.

Cisco Compatible Extensions: Features and Benefits

This subtopic describes features and benefits of the Cisco Compatible Extensions program.



Cisco Compatible Extensions (Cont.)

Cisco Compatible client devices

- **Features**
 - Assured compatibility with 300+ devices
 - Standards-based
 - Enhanced security, mobility, and performance
- **Benefits**
 - Accelerates innovation
 - Supports diverse enterprise applications
 - Ensures multivendor interoperability

Cisco Compatible

IBM
Hand Held PRODUCTS
TOSHIBA

hp invent

centrino MOBILE TECHNOLOGY
FUJITSU

<http://www.cisco.com/go/ciscocompatible/wireless>

© 2006 Cisco Systems, Inc. All rights reserved. BCM5N v3.0—6-25

The figure shows an array of client devices that are Cisco Compatible certified. More than 300 wireless devices are Cisco Compatible certified today (and more are being added). Over 90 percent of notebooks that are available today are Cisco Compatible certified.

Cisco Compatible client devices are sold and supported by their manufacturers, not Cisco.

In the Cisco Compatible Extensions program, Cisco licenses a specification with the latest WLAN standards and Cisco innovations.

- A program participant, such as a maker of a WLAN client adapter or client device, implements support for all features and then submits the product to an independent lab for rigorous testing.
- Only by passing all tests via third-party certification does the device earn the right to be called Cisco Compatible.

When IT managers select Cisco Compatible client devices, they can confidently deploy their WLANs, even if their WLANs serve a variety of different client device types.

With the Cisco Compatible Extensions program, Cisco is able to deliver next-generation WLAN features today. No other WLAN vendor has the ability to take advantage of enhancements today, providing the ability to confidently deploy robust, scalable, secure, and manageable solutions.

These are some of the features of the Cisco Compatible Extensions program:

- Assured compatibility out of the box
- Extensive, independent testing of third-party devices
- Standards based
- Strong wireless security with WPA2
- No-cost licensing of Cisco Aironet innovations

These are some of the benefits of the Cisco Compatible Extensions program:

- Innovative Cisco features
- Availability of prestandard features
- Planned upgrade paths
- Support for diverse enterprise applications
- Interoperability

Approved devices are listed at www.cisco.com/go/ciscocompatible/wireless and can also be found by looking for products displaying the Cisco Compatible logo.

Cisco Compatible Extensions: Versions

This subtopic compares the different versions of the Cisco Compatible Extensions specification.

Cisco Compatible Extensions Features				
	V1	V2	V3	V4
Security	<ul style="list-style-type: none"> • WEP • IEEE 802.1x • LEAP • Cisco TKIP 	<ul style="list-style-type: none"> • PEAP-GTC • WPA 	<ul style="list-style-type: none"> • WPA2 • EAP-FAST 	<ul style="list-style-type: none"> • NAC (wireless) • EAP-TLS • PEAP-MSCHAP
VLANs and QoS	<ul style="list-style-type: none"> • Multiple SSIDs/VLANs on AP 	<ul style="list-style-type: none"> • eDCF 	<ul style="list-style-type: none"> • Wi-Fi Multimedia (WMM) 	<ul style="list-style-type: none"> • MBSSID • Call Admission Control (CAC)
Voice over IP				<ul style="list-style-type: none"> • U-APSD • TSPEC CAC • Voice metrics
Performance and Management		<ul style="list-style-type: none"> • AP-assisted roaming • CCKM with LEAP • RF scanning and reporting • Transmit power sync 	<ul style="list-style-type: none"> • CCKM with EAP-FAST • Proxy ARP information element • Single sign-on: LEAP, EAP-FAST 	<ul style="list-style-type: none"> • CCKM with other EAP types • AP-directed roaming • Location • Keep Alive link test

WLAN access points manufactured by Cisco have features and capabilities beyond those in related standards such as IEEE 802.11 suite of standards, Wi-Fi recommendations, and the 802.1x security suite. It is possible to group these features into several categories.

First and foremost, a number of security features substantially differentiate Cisco access points and clients in the marketplace. In addition, a number of features provide higher performance.

For example, Cisco access points transmit a specific information element (IE) to which the clients adapt for enhanced performance.

Similarly, a number of features are implemented by means of proprietary IEs, which Cisco clients use in specific ways to carry out tasks above and beyond the standard. Other examples of feature categories are roaming and power saving.

The figure lists the features introduced in versions 1 through 4 of the Cisco Compatible Extensions program. With new developments, the specifications will be extended.

Cisco Compatible Extensions Program

This subtopic describes the Cisco Compatible Extensions program.

Cisco Compatible Extensions Program

- **Develops interoperability with semiconductor and client vendors**
- **Provides additional functionality and performance improvement while working with Cisco access points and Cisco wireless infrastructure**
 - **Objective: The Cisco Compatible Extensions program provides customers with a broad range of WLAN client devices that have tested interoperability with Cisco Aironet innovations.**
 - **Phase 1:**
 - **Specification: Cisco provides specification to WLAN silicon providers.**
 - **Phase 2:**
 - **Interoperability test: Devices are tested by approved third-party vendor for the specification.**
 - **Phase 3:**
 - **Compatibility: Approved products are marketed.**

© 2006 Cisco Systems, Inc. All rights reserved.BCMSN v3.0—6-27

It is desirable that clients manufactured by qualified vendors and access points manufactured by Cisco interoperate beyond Wi-Fi and similar industry requirements. There are two advantages gained by this interoperability:

First, by recognition of and adaptation to these features, other clients can take advantage of the proprietary Cisco features. This provides additional functionality and performance improvement while working with Cisco access points.

Second, by designing clients that are transparent to legacy proprietary features intended for uses that are specific to Cisco, compliant clients do not lose performance and do not become inoperable while interworking with Cisco access points.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- The installation wizard for the Cisco 802.11a/b/g WLAN client adapter installs driver and utilities.
- The Cisco 802.11a/b/g client adapter is configured via Cisco ADU.
- Cisco ADU can be used for troubleshooting the client adapter.
- The Cisco Aironet Site Survey Utility provides information about available WLANs.
- Cisco ADU provides more features than Windows XP for the Cisco client adapter configuration.
- Cisco ACAU provides preconfiguration of WLAN profiles for software distribution.
- The Cisco Wireless IP Phone provides integration of IP telephony into WLANs.
- The Cisco Compatible Extensions program enhances WLAN features for WLAN adapters from multiple vendors.

Implementing WLANs

Overview

This lesson describes wireless LAN (WLAN) implementations. Both autonomous and lightweight WLAN solutions are described. Other topics include PoE (Power over Ethernet) and WLAN antennas.

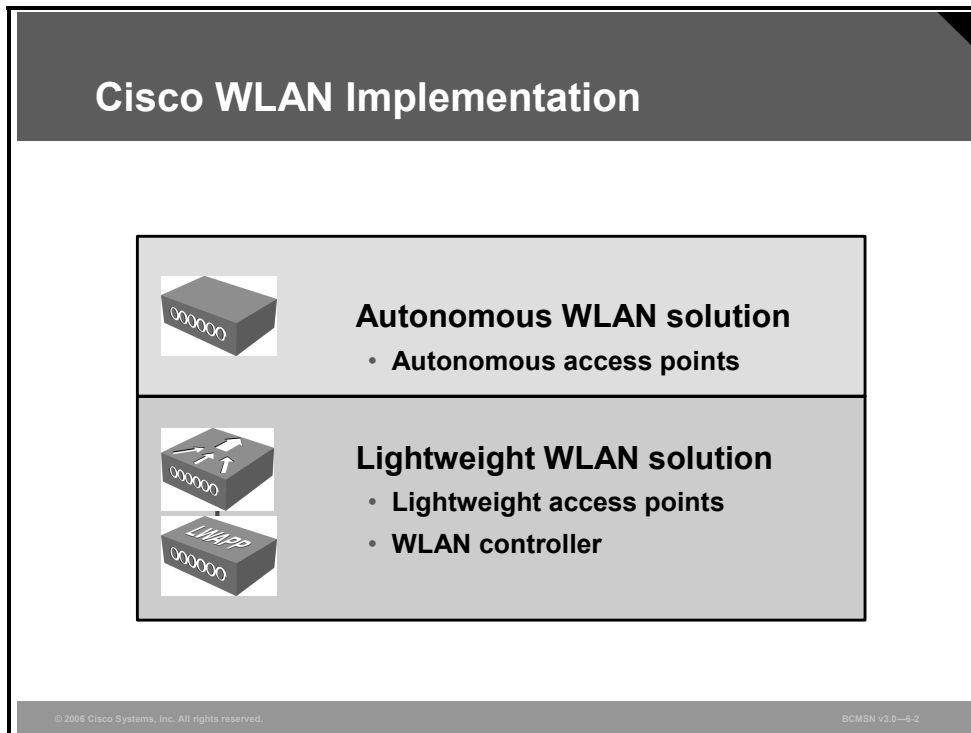
Objectives

Upon completing this lesson, you will be able to distinguish between autonomous and lightweight WLAN implementations and describe PoE and WLAN antennas. This ability includes being able to meet these objectives:

- Describe the implementation of the Cisco autonomous and lightweight WLAN solution that is part of the Cisco implementation of WLANs
- Describe how LWAPP is used in the Cisco lightweight WLAN implementation
- Describe the components of the Cisco WLAN implementations
- Describe Cisco Unified Wireless Networks
- Describe Cisco Aironet access points and bridges
- Describe PoE for access points and IP phones
- Identify the types of antennas to use in WLAN environments
- Explain multipath distortion
- Describe the decibel calculation
- Explain the established EIRP guidelines

Cisco WLAN Implementation

This topic describes how Cisco Systems implements WLANs.

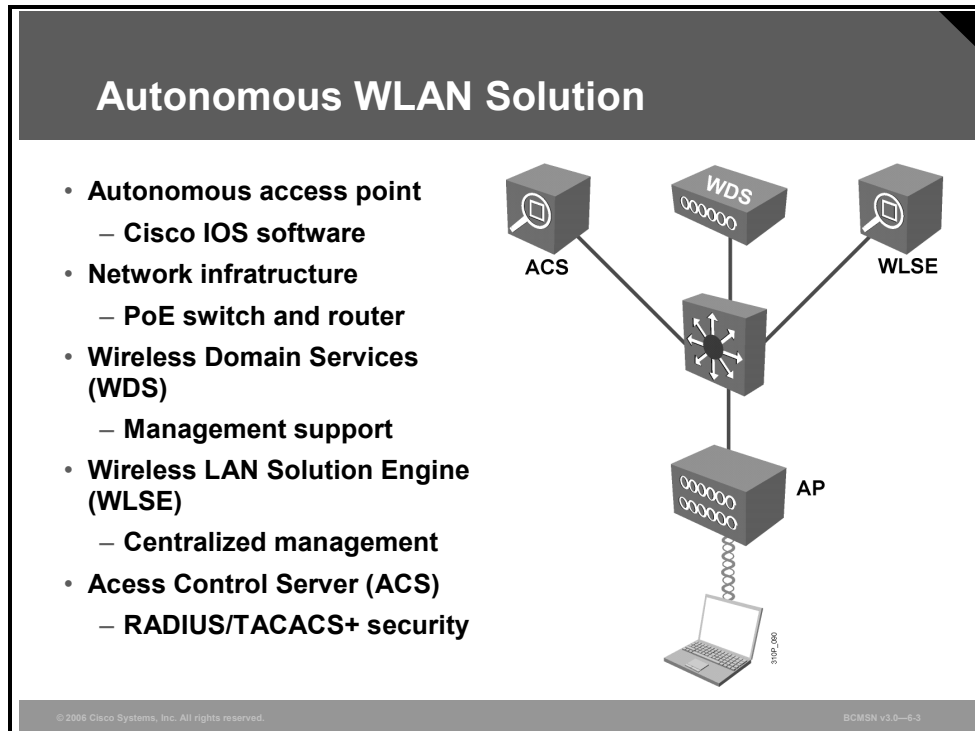


Cisco offers two WLAN implementations:

- The autonomous WLAN solution is based on autonomous access points.
- The lightweight WLAN solution is based on lightweight access points and WLAN controllers.

Autonomous WLAN Solution

This subtopic describes the Cisco autonomous WLAN solution.

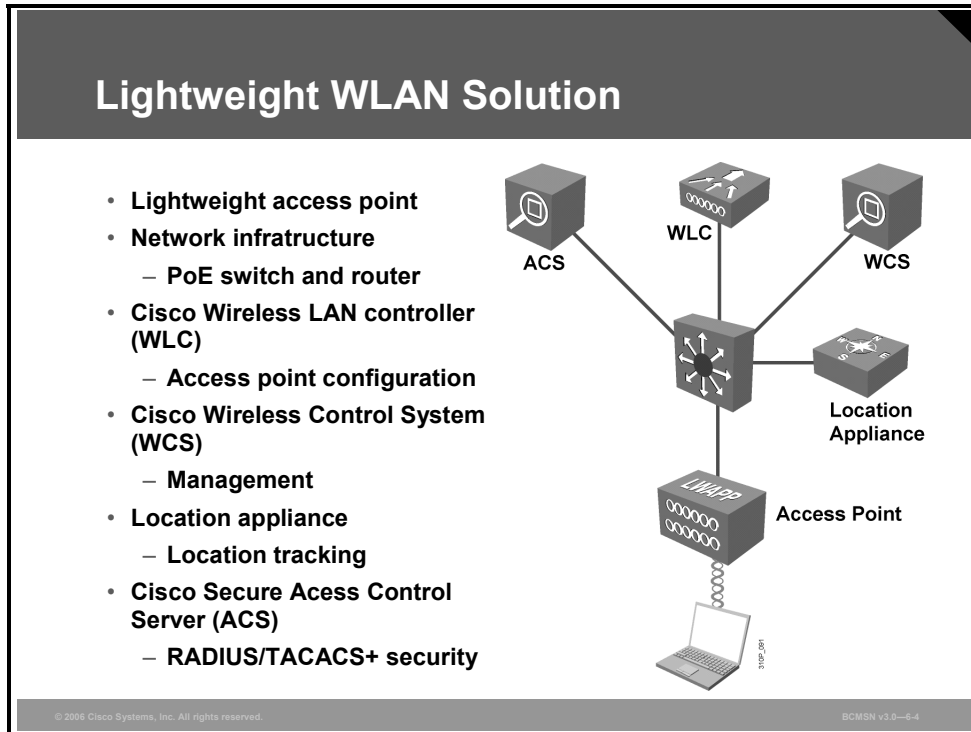


The figure shows the components of the distributed WLAN solution:

- Autonomous access points that use Cisco IOS software.
- Network infrastructure with router and switches. Switches can be used to supply power to the access points (PoE).
- Wireless Domain Services (WDS) for radio frequency (RF) management and fast, secure roaming.
- CiscoWorks Wireless LAN Solution Engine (WLSE) for management (optional).
- Cisco Secure Access Control Server (ACS) for security using RADIUS and TACACS+ protocol.

Lightweight WLAN Solution Components

This subtopic describes the Cisco centralized WLAN solution.

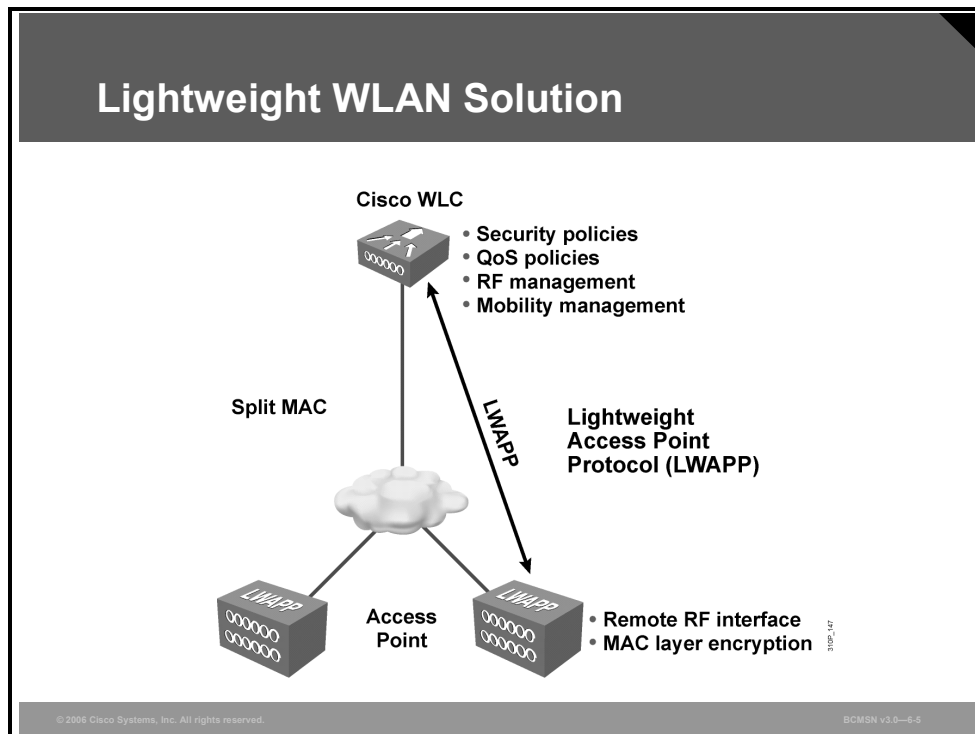


The figure shows the components of the lightweight WLAN solution:

- Lightweight access points
- Network infrastructure with router and switches. Switches can be used to supply power to the access points (PoE)
- Cisco Wireless LAN Controller (WLC) for the configuration of the access points
- Cisco Wireless Control System (WCS) for management (optional)
- Cisco Wireless Location Appliance for location tracking
- Cisco Secure ACS for security using RADIUS and TACACS+ protocol

Lightweight WLAN Solution

This subtopic describes the Cisco lightweight WLAN solution.



The lightweight architecture splits the processing of the 802.11 protocol between two devices, the access point and a centralized Cisco WLC. The processing of the 802.11 data and management protocols and the access point functionality is also divided between the two devices. This approach is called split MAC.

The access point handles the portions of the protocol that have real-time requirements:

- The frame exchange handshake between a client and access point when transferring a frame over the air
- The transmission of beacon frames
- The buffering and transmission of frames for clients in power save operation
- The response to probe request frames from clients
- Forwarding notification of received probe requests to the controller
- Providing real-time signal quality information to the controller with every received frame
- Monitoring each radio channel for noise, interference, and presence of other WLANs
- Monitoring for the presence of other access points

All remaining functionality is handled in the Cisco Aironet WLC, where time-sensitivity is not a concern and controller-wide visibility is required.

These are some of the MAC-layer functions provided in the WLAN controller:

- 802.11 authentication
- 802.11 association and reassociation (mobility)
- 802.11 frame translation and bridging

Lightweight Access Point Protocol

This topic describes how the Lightweight Access Point Protocol (LWAPP) is used in WLANs.

Lightweight Access Point Protocol

- **Real-time frame exchange and certain real-time portions of MAC management are accomplished within the access point.**
- **Authentication, security management, and mobility are handled by WLAN controllers.**
- **Data and control messages are exchanged between the access point and the WLAN controller using LWAPP.**
- **Control messages are encrypted.**
- **All client data traffic is sent via the WLAN controller.**

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0—6-6

The control traffic between the access point and the controller is encapsulated with the LWAPP. The control traffic is encrypted via the Advanced Encryption Standard (AES).

The data traffic between the access point and controller is also encapsulated with LWAPP. The data traffic is not encrypted. It is switched at the WLAN controller, where VLAN tagging and quality of service (QoS) are also applied.

Layer 2 and Layer 3 Mode of LWAPP

This subtopic describes the Layer 2 and Layer3 mode of LWAPP.

LWAPP

Layer 2 mode

- Layer 2 LWAPP is in an Ethernet frame.
- The WLAN controller and the access point must be in the same broadcast domain and IP subnet.

Layer 3 mode

- Layer 3 LWAPP is in a UDP/IP frame.
- The WLAN controller and access point can be in the same or different broadcast domains and IP subnets.
- The access point must obtain an IP address via DHCP.

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0-6-7

The access point and WLAN controller are connected via a network. If it is a switched network, Layer 2 or Layer 3 mode can be used. If it is a routed network, Layer 3 mode is used.

Layer 2 LWAPP is in an Ethernet frame. For Layer 2 mode, the WLAN controller and access point must be in the same broadcast domain and IP subnet.

Layer 3 LWAPP is in a User Datagram Protocol (UDP)/IP packet. The WLAN controller and access point can be in the same or different broadcast domains and IP subnets. For Layer 3 mode, the access points need IP addresses. They must obtain IP addresses via DHCP.

Association of Access Point to WLAN Controller

This subtopic describes the association of access points to the WLAN controller.

Association of Access Point to WLAN Controller

- **Access points use LWAPP in Layer 2 and Layer 3 mode to associate to the WLAN controller.**
- **In Layer 3 mode, the access point sends an LWAPP discovery request to the controller management IP address via a directed broadcast.**
- **The controller responds with a discovery response from the manager IP address that includes the number of access points currently associated to the access point manager interface.**
- **The access point chooses the access point manager IP address with the least number of access points and sends the join request.**
- **All subsequent communication is to the WLAN controller access point manager IP address.**

© 2006 Cisco Systems, Inc. All rights reserved.

BCMSN v3.0—6-8

Lightweight access points first search for a WLAN controller using LWAPP in Layer 2 mode. Then the access point searches for a WLAN in Layer 3 mode.

The access point requests an IP address via DHCP. The access point then sends a LWAPP discovery request to the management IP address of the WLAN controller via a broadcast.

The WLAN controller responds with a discovery response from the manager IP address. This response includes the number of access points that are currently associated to that access point manager interface and the access point manager IP address.

The access point chooses the access point manager with the least number of associated access points and sends the join request.

All subsequent LWAPP communication is done to the access point manager IP address of the WLAN controller.

Cisco Aironet WLAN Controllers

This subtopic describes the Cisco Aironet WLCs.

Cisco Aironet WLCs

- Scalability
- Integrated Radio Resource Management (RRM)
- Zero-configuration deployment
- Multilayered security
- Intrusion detection, location, and containment
- Mobility management
- Reliability
- Intuitive management interfaces



The image shows two Cisco Aironet Wireless LAN Controllers. The top device is the WLC 2000, a small, single-unit device. The bottom device is the WLC 4400, a larger, rack-mountable device with two units stacked. Both devices are black with a silver front panel.

© 2006 Cisco Systems, Inc. All rights reserved. BCM5N v3.0-6.0

The Cisco 2000 Series delivers WLAN services to small and medium-sized enterprise environments. It supports up to six lightweight access points, making it a cost-effective solution for smaller buildings.

With integrated DHCP services and zero-touch access point configuration, the Cisco 2000 Series is also ideal for environments with limited onsite IT support, such as branch offices within a distributed enterprise.

The Cisco 4400 Series Wireless LAN Controller is designed for medium to large facilities. It is available in two models:

- Cisco 4402
 - Two Gigabit Ethernet ports
 - Configurations that support 12, 25, and 50 access points
 - One expansion slot
- Cisco 4404
 - Four Gigabit Ethernet ports
 - Support for 100 access points
 - Two expansion slots

In addition, each Cisco 4400 Wireless LAN Controller supports an optional redundant power supply to ensure maximum availability.

WLAN controllers are also available for the Cisco Catalyst 6500 and Cisco Integrated Services Routers (ISRs).

Comparison of the WLAN Solutions

This subtopic compares the autonomous and lightweight WLAN solutions.

Comparison of the WLAN Configuration	
Autonomous WLAN solution	Lightweight WLAN solution
<ul style="list-style-type: none">• Autonomous access points• Configuration of each access point• Independent operation• Centralized management via WLSE• Access point redundancy	<ul style="list-style-type: none">• Lightweight access points• Configuration via WLC• Dependent on WLC• Centralized management via WCS• WLC redundancy

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0—6-18

The two WLAN solutions have different characteristics and advantages.

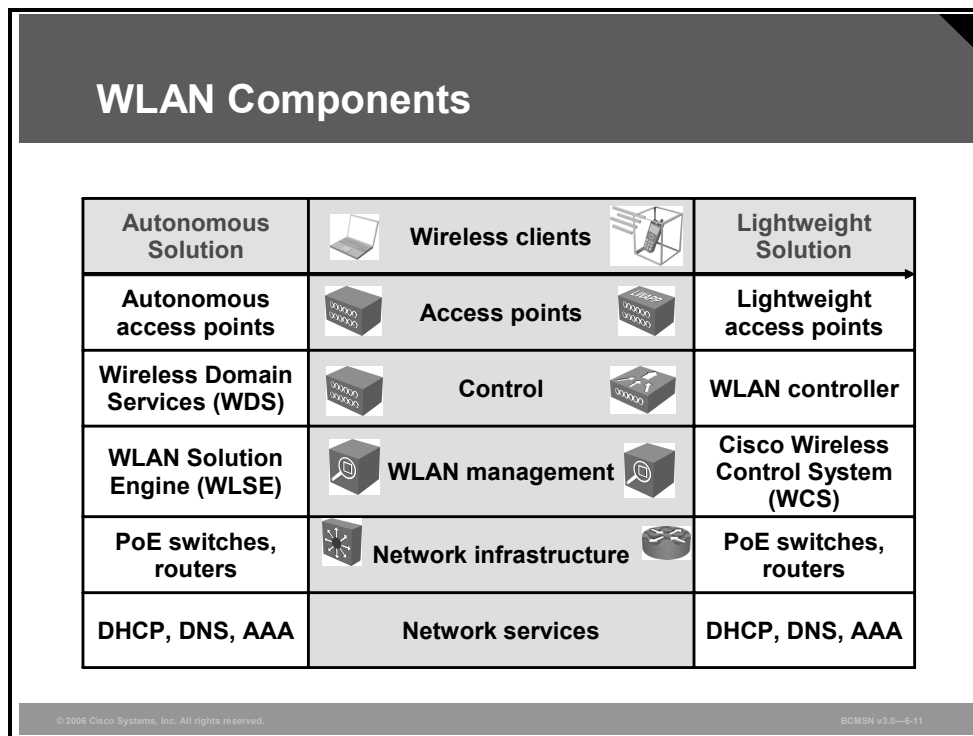
Autonomous access points are configured per access point. Their Cisco IOS software operates independently. Centralized configuration, monitoring, and management can be done via the CiscoWorks WLSE. Autonomous access points can be installed with redundancy per access point.

Lightweight access points are configured via the WLAN controller. They depend on the WLAN controller for control and data transmission. Only in Remote-Edge Access Point mode does a lightweight access point not depend on the WLAN controller for data transmission.

Monitoring and security is implemented by the WLAN controller. Centralized configuration, monitoring, and management can be done via the Cisco WCS. WLAN controllers can be installed with redundancy within WLAN controller groups.

Describing WLAN Components

This topic explains the hierarchy of components that are required to build a WLAN.

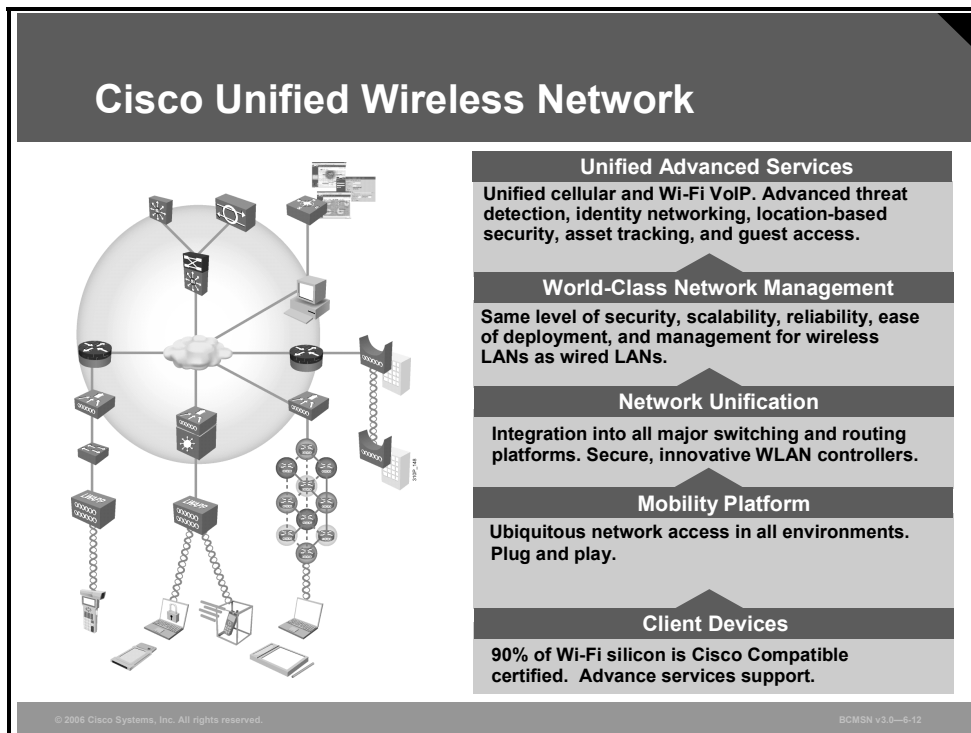


A WLAN consists of these components:

- Wireless clients are connected to the network (for example, notebooks).
- Access points build the WLAN infrastructure.
 - Autonomous access points
 - Lightweight access points
- Lightweight access points are configured using WLAN controllers.
- WLAN management is used to administer and monitor large deployments of WLANs.
- Network infrastructure is provided by switches and routers to connect access points, controllers, management, and servers.
- Network services such as DHCP; and Domain Name System (DNS); and authentication, authorization, and accounting (AAA) are required for both the wireless network and the user.
- Cisco Aironet bridges operate at the MAC address layer (data link layer).

Cisco Unified Wireless Network

This topic describes the Cisco Unified Wireless Network.



The Cisco Unified Wireless Network is an end-to-end unified wired and wireless network that cost-effectively addresses WLAN security, deployment, management, and control issues. The unique Cisco approach addresses all layers of the WLAN network, from client devices and access points to the network infrastructure, network management, and the delivery of advanced wireless services.

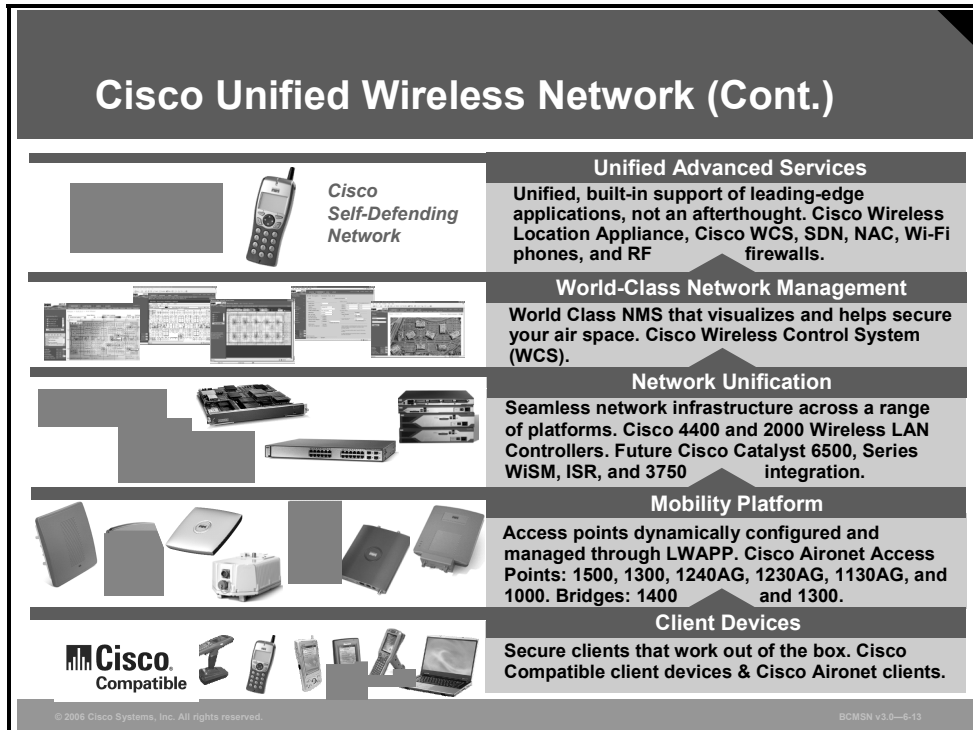
The Cisco Unified Wireless Network is composed of five interconnected elements that work together as building blocks to deliver a unified enterprise-class wireless solution.

- **Client devices:** Cisco is leading the development of interoperable, standards-based client devices through its Cisco Compatible Extensions program. This Cisco Compatible Extensions program helps to ensure the widespread availability of client devices from a variety of suppliers that are interoperable with a Cisco WLAN infrastructure. Cisco Compatible client devices deliver “out-of-the-box” wireless mobility, QoS, network management, and enhanced security.
- **Mobility platform:** Cisco Aironet lightweight access points provide ubiquitous network access for a variety of indoor and outdoor wireless environments, including wireless mesh. The Cisco solution supports a wide array of deployment options, such as single or dual radios, integrated or remote antennas, and ruggedized metal enclosures. They operate as “plug-and-play” wireless devices with zero-touch configuration.
- **Network unification:** The Cisco Unified Wireless Network includes a solid migration path into all major Cisco switching and routing platforms via Cisco WLCs. Cisco WLCs are responsible for system-wide WLAN functions, such as integrated intrusion protection system (IPS), real-time RF management, clustering, zero-touch deployment, and $N+1$ redundancy.

- **World-class network management:** The Cisco Unified Wireless Network delivers the same level of security, scalability, reliability, ease of deployment, and management for WLANs that organizations expect from their wired LANs. The industry-leading Cisco WCS is a world-class WLAN management interface. Cisco WCS brings ease of use to WLAN management. It provides a powerful foundation that allows IT managers to design, control, and monitor their enterprise wireless networks from a centralized location, simplifying operations and reducing the total cost of ownership.
- **Unified advanced services:** The Cisco Unified Wireless Network cost-effectively supports new mobility applications, emerging Wi-Fi technologies, and advanced threat detection and prevention capabilities. Cisco services are more comprehensive than the services of other wireless point-product vendors. The Cisco solution supports these features:
 - Advanced features, such as wireless VoIP and future unified cellular and Wi-Fi VoIP
 - Emerging technologies, such as location services for critical applications like high-value asset tracking, IT management, and location-based security
 - Advanced wireless security features, such as Network Admission Control, Self-Defending Network, identity based networking, intrusion detection systems, and guest access for end-to-end network security.

Cisco Unified Wireless Network Components

This subtopic describes components of Cisco Unified Wireless Networks.



These Cisco WLAN products support the five interconnecting elements of the Cisco Unified Wireless Network and business-class WLANs.

- **Client devices:** Cisco Compatible or Cisco Aironet client devices are strongly recommended for the Cisco Unified Wireless Network. With over 90 percent of shipping client devices certified as Cisco Compatible, almost any client device that you select should be Cisco Compatible certified.

Cisco Compatible client devices interoperate with and support innovative and unique Cisco Unified Wireless Network features, such as fast secure roaming, integrated IPS, location services, and a variety of extensible authentication types.

- **Mobility platform:** Cisco offers access points and bridges for the carpeted enterprise, ruggedized environments, and challenging environments like the outdoors. Cisco Aironet lightweight access points are dynamically configured and managed through LWAPP. Cisco Aironet autonomous access points that have been converted to operate as lightweight access points running the LWAPP are supported.
- **Network unification:** The Cisco Unified Wireless Network leverages the customer's existing wired network and investment in Cisco products. It supports a seamless network infrastructure across a range of platforms. Wired and wireless unification occurs with the Cisco WiSM 4400 and 2000 Series WLAN controllers.

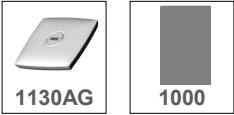
- **World-class network management:** Cisco delivers a world-class network management system (NMS) that visualizes and helps secure your air space. Cisco WCS supports WLAN planning and design, RF management, location tracking, and IPS, in addition to WLAN systems configuration, monitoring, and management. This platform easily manages multiple controllers and their associated lightweight access points.
- **Unified advanced services:** Cisco provides unified support of leading-edge applications. Cisco offers advanced services that are industry leading, innovative, and comprehensive. The Cisco Unified Wireless Network advanced services are delivered by wireless lightweight access points, location appliances, and wireless IP phones.

Cisco Aironet Access Points and Bridges

This topic provides an overview of the access points and bridges for WLAN implementation.


Cisco Aironet Access Points and Bridges

Indoor Access Points




1130AG 1000

Indoor Rugged Access Points



1240AG 1230AG

Outdoor Access Points/Bridges



1500 1400 1300

Mobility Platform

Features

- Industry's best range and throughput
- Enterprise-class security
- Many configuration options
- Simultaneous air monitoring and traffic delivery
- Wide area networking for outdoor areas

Benefits

- Zero-touch management
- No dedicated air monitors
- Support for all deployment scenarios (indoor and outdoor)
- Secure coverage to advanced services

© 2006 Cisco Systems, Inc. All rights reserved. BCM5N v3.0-6-14

Cisco offers different access points and bridges for different physical environments. In addition to lightweight and autonomous access points, Cisco has integrated access points into the ISR with either built-in or access point network modules, depending on the ISR model.

All Cisco Aironet lightweight access points connect to Cisco WLCs, so customers can mix and match access points within their network, yet still take advantage of all the rich Cisco Unified Wireless Network capabilities in an integrated manner. Autonomous access points are manageable via CiscoWorks WLSE or CiscoWorks WLSE Express.

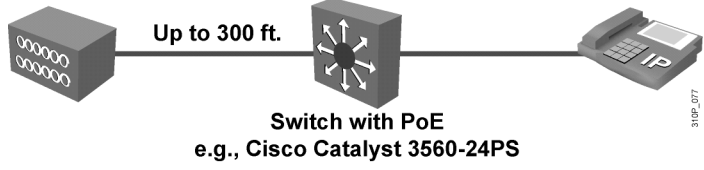
Cisco has products for the carpeted enterprise, ruggedized environments, and challenging environments such as the outdoors. For example:

- Cisco Aironet 1130AG Series Access Point is for the carpeted enterprise that has little environmental variability and operates within a controlled environment.
- Cisco Aironet 1240AG Series Access Point is for challenging environments that need a ruggedized enclosure such as manufacturing, loading docks, and warehouses.
- Cisco Aironet 1500 Lightweight Outdoor Mesh Access Point is for cost-effective, scalable deployment of secure outdoor WLANs for network connections within a campus area, outdoor infrastructure for mobile users, or public access for outdoor areas. The 1500 Series supports autoconfiguring and self-healing wireless mesh deployments.
- Cisco Aironet 1300 Series Outdoor Access Point/Bridge or Cisco Aironet 1400 Series Wireless Bridges offer high-speed, high-performance outdoor bridging for line-of-sight applications. They both have a ruggedized enclosure for harsh outdoor environments with extended operating temperature range. Both are available in an autonomous version only. Cisco Aironet 1300 Series Outdoor Access Point/Bridge can be deployed as an autonomous access point, bridge, or workgroup bridge. It has a ruggedized enclosure and provides high-speed and cost-effective wireless connectivity between multiple fixed or mobile networks and clients.

Power over Ethernet

This topic describes PoE for access points and IP phones.

Power over Ethernet (PoE)



Switch with PoE
e.g., Cisco Catalyst 3560-24PS

- **Sending operating power over Ethernet Category 5 cable**
- **Power-sourcing equipment (PSE)**
 - **Switches, power injector**
- **Powered devices**
 - **Access points, IP phones**
- **Up to 15.4W power per port**
- **Distances up to 100 meters**
- **Alternative: AC power adapter**

© 2006 Cisco Systems, Inc. All rights reserved.BCMSN v3.0-6-16

To decrease the cost and complexity of the installation, the access points can be powered over an Ethernet cable, eliminating the need to run expensive AC power to remote access point installation locations.

No electrician is required. Anyone qualified to run Category 5 cable can install the cabling that is required to power Cisco Aironet access points. The standard Category 5 cable requirements still apply (maximum 328 feet or 100 meters).

Power-sourcing equipment (PSE) can be switches, routers with switch modules, and power injectors.

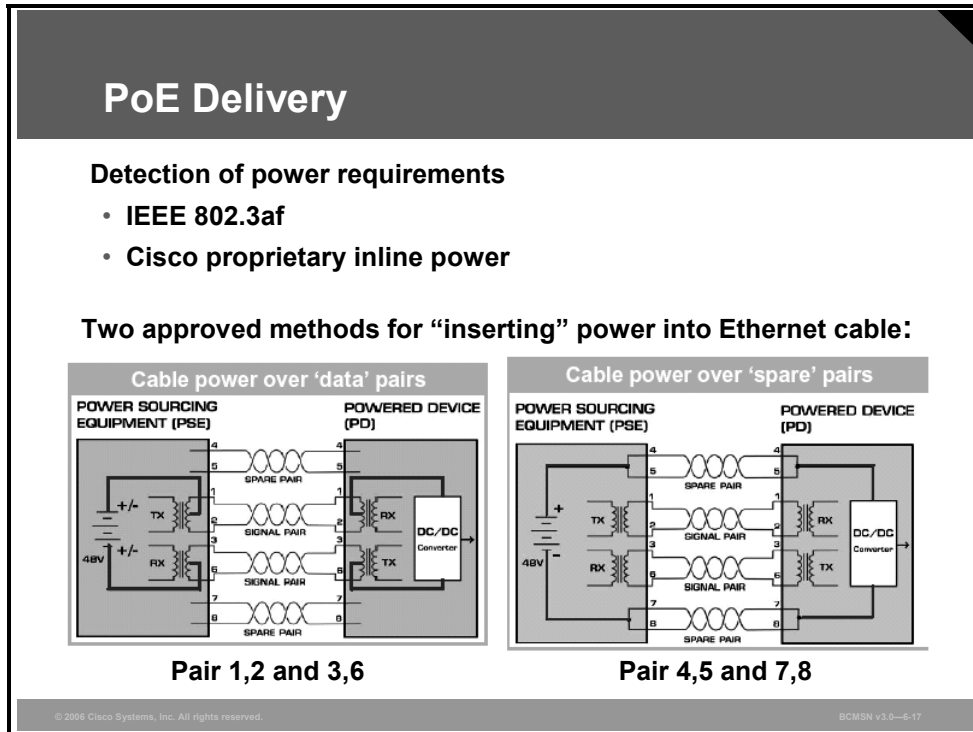
Powered devices are access points and other devices.

New PoE switches, such as the Catalyst 3560-24PS switch, can supply power of up to 15W per port.

Up to 15W power is required for dual-mode access points

PoE Delivery

This subtopic describes the power detection and cabling of PoE.



IEEE 802.3af and Cisco use different methods to detect when power is required. The first step is to detect that the device requires power. The second step is to classify power requirements. Cisco uses Cisco Discovery Protocol (CDP) in the powered device to inform the switch about the amount of power used.

The figure shows how power is transported over the Ethernet cable. PoE can be supplied over these wires:


- Ethernet pair 1,2 and 3,6
- Ethernet pair 4,5 and 7,8

The IEEE 802.3af mandates that for powered devices, both methods have to be supported.

Midspan Power Injection

This subtopic describes midspan power injection.

Midspan Power Injection



- Uses pairs 4,5 and 7,8
- Requires eight-wire cabling
- Does not extend 100-m total length limit
- Not possible for 1000TX

© 2006 Cisco Systems, Inc. All rights reserved.BCMSN v3.0-5-18

Midspan power injectors add power to Ethernet cables between switches and devices. The spare pairs 4,5 and 7,8 are used, which requires eight-wire cabling.



This technique does not extend the 100-meter FastEthernet cable limit. This approach is not possible for 1000TX Gigabit Ethernet, which already uses all eight wires and, therefore, has no spare wires available.

Power-Sourcing Equipment

This subtopic describes PSE.

Power-Sourcing Equipment

- **Power injector**
 - **AIR-PWRINJ3/AIR-PWRINJ-FIB**
- **Powering switch**
 - **Cisco Catalyst 3560-PS/3750-PS**
 - **Cisco Express CE500-LC/CE500-PC**
 - **Cisco Catalyst 4500/6500 switch with inline power line cards**
 - **Router module NM-16ESW-PWR**
 - **Router card HWIC-4ESW-POE**
 - **Router with PoE support**

© 2004 Cisco Systems, Inc. All rights reserved. BCMSN v3.0—6-18

Power can be supplied by these PSEs:

- Power injector
 - AIR-PWRINJ3 / AIR-PWRINJ-FIB
- Powering switch
 - Cisco Catalyst 3560-PS
 - Cisco Catalyst 3750-PS
 - Cisco Express CE500-LC / CE500-PC
 - Cisco Catalyst 4500 / 6500 switch with inline power line cards
 - Router module NM-16ESW-PWR (Cisco Router Series 2600/2800/3600/3700/3800)
 - Router card HWIC-4ESW-POE (Cisco Router 2800/3800)
 - Router with PoE support (Cisco Router 1801/1811/1812)

ISRs need an optional power supply upgrade that supplies 48-volt power.

Investment Protection

This subtopic describes the investment protection by support of both PoE methods.

Investment Protection

- **Cisco has shipped over 18 million ports with PoE installed.**
- **New Cisco devices (PSEs and powered devices) support both PoE methods.**
 - **IEEE 802.3af**
 - **Cisco proprietary PoE**
- **Examples:**
 - **Access points 1131AG, 1242AG**
 - **Switches: 3560, 3750**
 - **Router: 1812, HWIC-4ESW-POE**
- **Automatic detection; no configuration is required.**

© 2006 Cisco Systems, Inc. All rights reserved.BCMSN v3.0-6.20

Cisco has shipped more than 18 million ports with PoE installed. New Cisco PSEs and powered devices support both PoE methods:

- IEEE 802.3af
- Cisco proprietary PoE

These are examples of such Cisco devices:

- **Access points:** Cisco Aironet 1131AG, Cisco Aironet 1242AG
- **Switches:** Cisco Catalyst 3560 and 3750 Series
- **Router:** Cisco 1812, HWIC-4ESW-POE

The devices automatically detect the supported PoE method; no configuration is required.

PoE Configuration

This subtopic describes the configuration of PoE switch ports.

PoE Switch

```
switch(config-if)# power inline {auto | never}
```

- **PoE configuration**

```
switch# show power inline [interface]
```

- **Display PoE statistics**

```
switch# show power inline
Available:370.0(w) Used:61.6(w) Remaining:308.4(w)
Interface Admin Oper Power Device Class Max
              (Watts)
-----
Gi0/1      auto  off  0.0   n/a    n/a  15.4
Gi0/2      auto  on   15.4  Ieee PD 3    15.4
Gi0/3      auto  off  0.0   n/a    n/a  15.4
Gi0/4      auto  on   15.4  Ieee PD 3    15.4
Gi0/5      auto  off  0.0   n/a    n/a  15.4
Gi0/6      auto  on   15.4  Ieee PD 3    15.4
Gi0/7      auto  off  0.0   n/a    n/a  15.4
Gi0/8      auto  on   15.4  Ieee PD 3    15.4
```

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0—6-21

Switch port configuration for PoE:

- Enables and disables PoE
 - Auto (default)
 - Power detection enabled
 - Power is supplied if required by device
 - Never
 - Power disabled
- Port shutdown turns power off

The command **show power inline** displays the configuration and statistics about the used power drawn by connected powered devices and the capacity of the power supply.

PoE Switch Port Status

The screenshot displays the Catalyst 3560 Series Device Manager interface for a switch named 'WLAN-SW1'. The top navigation bar includes options for Refresh, Print, Smartports, Software Upgrade, Legend, and Help. The session is identified as 'Standard' and 'Secured'. The main content area shows a 'View: PoE' dropdown and a visual representation of the switch's ports. Below this, a 'Port Status' table provides detailed information for each port.

Port	Description	Status	VLAN	Speed	Duplex	PoE
Gi0/1	1WLC1	●	111	100	full	Off
Gi0/2	1AP1	●	111	100	full	15.4 On
Gi0/3	1WLC2	●	112	100	full	Off
Gi0/4	1AP2	●	112	100	full	15.4 On
Gi0/5	2WLC1	●	121	100	full	Off
Gi0/6	2AP1	●	121	100	full	15.4 On
Gi0/7	2WLC2	●	122	100	full	Off
Gi0/8	2AP2	●	122	100	full	15.4 On
Gi0/9		●	1			Off
Gi0/10		●	1			Off
Gi0/11		●	1			Off
Gi0/12		●	1			Off
Gi0/13		●	1			Off
Gi0/14		●	1			Off
Gi0/15		●	1			Off
Gi0/16		●	1			Off

The Catalyst switch device manager displays the port status and the PoE statistics.

Explaining WLAN Antennas

This topic explains WLAN antennas.

Antenna Concepts

Directionality

- Omnidirectional antennas (360 degree coverage)
- Directional antennas (limited range of coverage)

Gain

- Measured in dBi (gain over theoretical isotropic)
- More gain means focusing in certain directions, limited range of coverage

Polarization

- Vertical polarization for WLAN

© 2006 Cisco Systems, Inc. All rights reserved. BCM5N v3.0—6-24

To understand wireless networks and how to set them up and optimize them for best performance, some knowledge of antennas is essential.

There are several key terms that you need to understand.

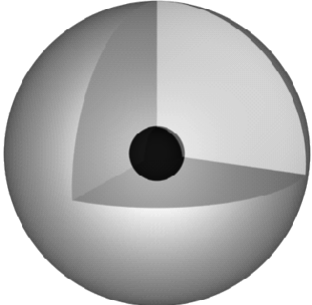
- **Directionality:** The coverage around the antenna. An omnidirectional WLAN antenna transmits and receives signals in all horizontal directions equally. A directional antenna focuses the signal from the access point into a smaller coverage area, resulting in a stronger signal in this direction.
- **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.
- **Polarization:** The physical orientation of the element on the antenna that actually emits the RF energy. All Cisco Aironet antennas are set for vertical polarization. A vertical dipole antenna is vertically polarized.

Omnidirectional Isotropic Antennas

This subtopic describes the omnidirectional isotropic antenna.

Antenna Theory

- **A theoretical isotropic antenna has a perfect 360-degree vertical and horizontal beamwidth.**
- **Reference for all antennas.**

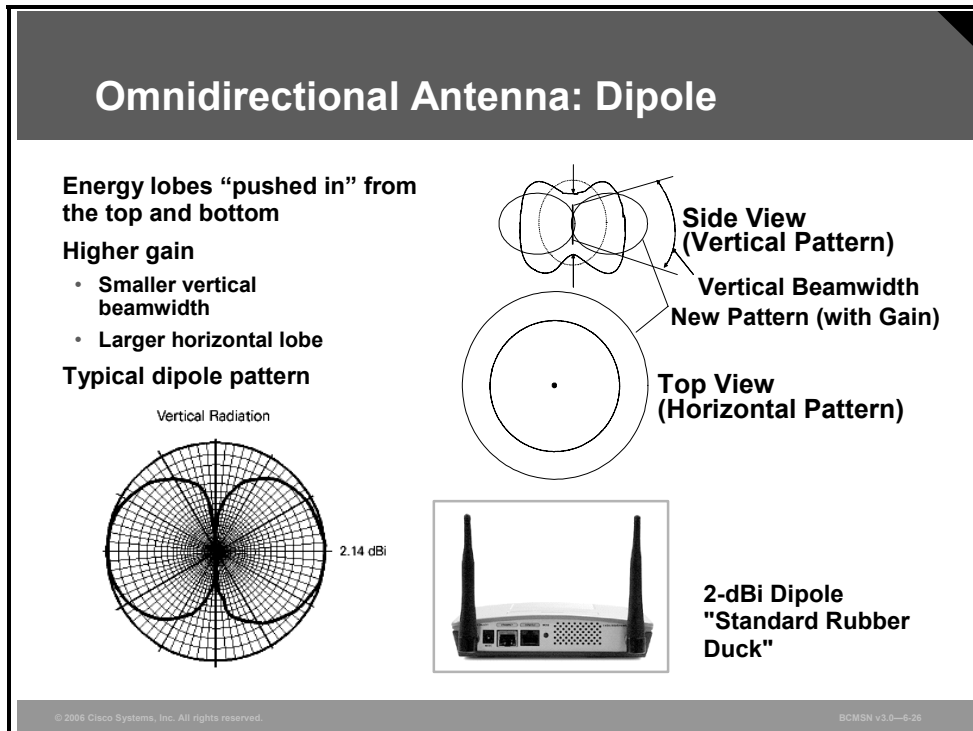


© 2006 Cisco Systems, Inc. All rights reserved. BCM5N v3.0-6-25

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. The coverage of an isotropic antenna can be thought of as a balloon. It transmits equally in all directions.

Omnidirectional Dipole Antennas

This subtopic describes the omnidirectional dipole antenna.



When an omnidirectional antenna is designed to have gain, the result is a loss of coverage in certain areas.

Imagine the radiation pattern of an isotropic antenna as a balloon that 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 yields a higher gain because the antenna appears to extend to a larger coverage area. The higher the gain on an antenna, the smaller the horizontal and vertical beamwidth.

The 2-dBi Rubber Duck dipole antenna for 2.4-GHz frequency band is an example of an omnidirectional antenna. The figure shows the vertical radiation pattern.

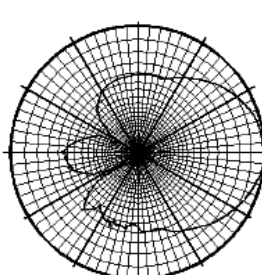
Directional Antennas

This subtopic describes directional antennas.

Directional Antenna

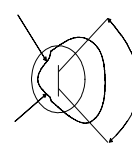
Lobes are pushed in a certain direction, causing the energy to be condensed in a particular area. Very little energy is in the back side of a directional antenna.

Vertical Radiation

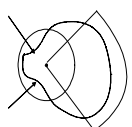


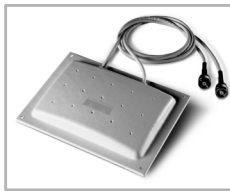
5.2 dBi

**Side View
(Vertical Pattern)**



**Top View
(Horizontal Pattern)**





**6.5-dBi Diversity
Patch Wall Mount
– 55 degrees**

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0-4.27

A directional antenna redirects the energy in a single direction.

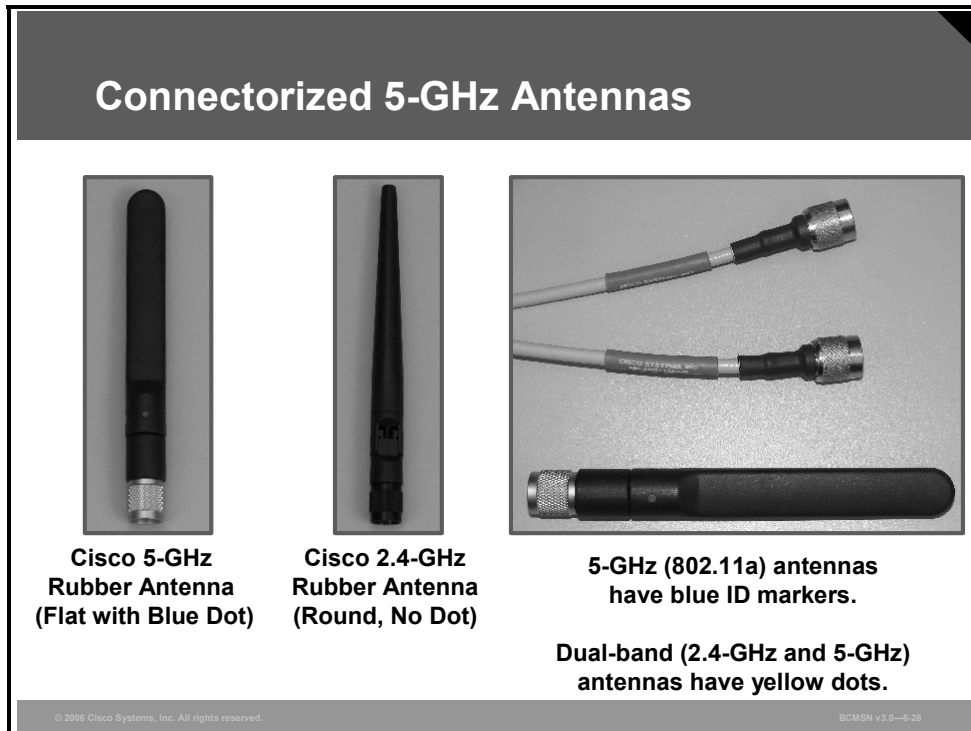
Consider the difference between an adjustable-beam focus flashlight and a regular flashlight. They have the same two batteries and the same bulb, but the intensity and width of the light beam can be changed. The adjustment is controlled by moving the back reflector and directing the light in tighter or wider angles. 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.

The 6.5-dBi Diversity Patch Wall Mount Antenna for 2.4-GHz frequency band is an example of a directional and diversity antenna. The figure shows the vertical radiation pattern.

Connectorized 5-GHz Antennas

This subtopic describes antennas for 5-GHz WLANs.



Cisco connectorized 5-GHz (802.11a) radios use the same RP-TNC radio connector as 2.4-GHz (802.11b/g) radios. Although it is possible that someone might connect the wrong antenna to the unit, Cisco is now using the color blue to denote 5 GHz to minimize the possibility of this error occurring.

The RP-TNC connector is an excellent connector (both physically and electrically) and, therefore, is the Cisco connector of choice for WLAN applications.

Accidentally connecting the wrong antenna will not damage the unit, but it will result in reduced performance.


In addition, Cisco offers multiband antennas for the 2.4-GHz and 5-GHz frequency bands, which have a yellow dot.

Cisco Access Point and Bridge Antennas

This subtopic lists Cisco antennas for access points and bridges.

Cisco Access Point/Bridge Antennas

Frequency	Antenna	Horizontal Beamwidth	Vertical Beamwidth
2.4 GHz	2.2-dBi dipole	360°	65°
2.4 GHz	5.2-dBi omni	360°	38°
2.4 GHz	6-dBi diversity patch	80°	55°
2.4 GHz	9-dBi patch	60°	60°
2.4 GHz	10-dBi Yagi	47°	55°
2.4 GHz	13.5-dBi Yagi	30°	25°
2.4 GHz	21-dBi dish	12.5°	12.5°
5 GHz	3.5-dBi dipole	360°	40°
5 GHz	6-dBi omni	360°	17°
5 GHz	7-dBi patch	70°	50°



© 2006 Cisco Systems, Inc. All rights reserved.
BCMSN v3.0-6-29

The figure shows a table of 2.4-GHz and 5-GHz antennas. All antennas have RP-TNC connectors. Sector antennas, integrated antennas, and omni antennas are vertically polarized. This is only a subset of available antennas.

In addition, Cisco offers multiband antennas for the 2.4-GHz and 5-GHz frequency bands.

Multipath Distortion

This topic describes multipath distortion.

Multipath Distortion

- **Multipath distortion (a form of radio degradation) occurs when radio signals bounce off metal objects in a room, such as metal cabinets or ceiling lights.**
- **OFDM overcomes multipath distortion through parallel frequency use.**
- **Multiple signals at receiver cause distortion of the signal.**
- **As radio waves bounce, they arrive at the receiver slightly delayed, combining with the original signal, causing distortion.**
- **Diversity systems use two antennas in different positions to reduce the degradation.**

Ceiling

Obstruction

Floor

Received Signals

Time →

Combined Results

Time →

310P

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0—6-30

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 objects, so do RF waves. RF waves can take more than one path when going from a transmitting (Tx) antenna to a receiving (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. One indication that you are getting multipath interference is the drastically fluctuating signal strength and signal quality when you move the client only very minor amounts (inches).

When an antenna transmits, it radiates RF energy in more than one definite direction. This transmission causes RF to move between the transmitting and receiving antenna in the most direct (desired) path and to take other routes that include reflecting or bouncing off metallic and other RF reflective surfaces. The process of reflecting the RF waves causes several things to occur:

- The reflected waves travel farther than the desired direct RF wave, which causes them to get to the receiving antenna later.
- Because of the longer transmission route, the signal loses more RF energy while traveling than the direct route signal.
- The signal loses some energy as a result of the reflection or bounce.

When these reflected signals are combined at the receiver, although RF energy (signal strength) may be high, the data would be unrecoverable. In the end, the desired wave is combined with many reflective waves in the receiver. As these different waveforms combine, they cause distortion to the desired waveform, which can affect the decoding capability of the receiver, resulting in poor performance. It is also possible that the radio signals can cancel each other out, causing what is known as a radio null, or dead spot.

Changing the location of the antenna can change these reflections and diminish the chance of multipath interference and nulls. Diversity systems use two antennas, and the access point samples each of the antennas, choosing the antenna with the best performance.

The pattern in which signals reflect is greatly affected by the physical wavelength of the signal. Because the wavelength is inversely proportional to the frequency, each frequency has differing multipath effects (fading). In a location where one frequency has a large multipath interference issue, another, even close frequency, will typically not have multipath interference.

Because orthogonal frequency-division multiplexing (OFDM) is based on many different frequencies, all operating in parallel, the odds are good that some of the information in at least some of the frequencies will be communicated successfully. This approach provides much greater performance in multipath environments.

Definition of Decibel

This topic describes the decibel (dB) calculation.

Definition of Decibel

Decibel (dB)

- **Ratio of one value to another**
- **dBm = Power based on 1 milliwatt**
- **0 dBm = 1 mW**
- **dBi = Antenna gain based on isotropic antenna**

[dB] = 10 log ₁₀ (Ratio)	
0 dB	1:1
10 dB	10:1
+3 dB	Multiply by 2
-3 dB	Divide by 2
+10 dB	Multiply by 10
-10 dB	Divide by 10
13 dB = 10 + 3	20 = 10 * 2
20 dB = 10 + 10	100 = 10 * 10
17 dB = 20 - 3	50 = 100 / 2

© 2004 Cisco Systems, Inc. All rights reserved.BCMSN v3.0-6-31

Antennas and RF power measurements use units based on decibels.

A decibel (dB) is the ratio between two signal levels. This measurement is named after Alexander Graham Bell. Descriptions of the different types of decibel measurements follow.

- **dB Milliwatt (dBm):** 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 (for instance -83 dBm).
- **dB Isotropic (dBi):** 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.

These values were all estimated using 0 dBm = 1 mW as a starting point.

- Add 3 dB to any number = double power
- Subtract 3 dB = one-half power
- Add 10 dB = 10x power
- Subtract 10 dB = divide power by 10

Example:

0 dBm = 1 mW, and 14 dBm = 25 mW

0 dBm = 1 mW,

therefore 10 dBm = 10 mW,

therefore 20 dBm = 100 mW,

subtracting 3 dB (17 dBm = 50 mW)

subtract 3 more (14 dBm = 25mW)

Effective Isotropic Radiated Power

This topic describes Effective Isotropic Radiated Power (EIRP).

Effective Isotropic Radiated Power

The diagram shows a transmitter labeled 'Bridge or Access Point' connected to an antenna. An arrow labeled 'Cable Loss -dB' points from the transmitter to the antenna. Another arrow labeled 'Antenna Gain (dBi)' points from the antenna to the right. A final arrow labeled 'EIRP' points to the right from the antenna. The transmitter is also labeled 'Transmitter Power (dBm)'.

- **Transmit power is rated in dBm or mW.**
- **Power coming off an antenna is Effective Isotropic Radiated Power (EIRP).**
- **FCC and ETSI use EIRP for power limits in regulations for 2.4-GHz and 5-GHz WLANs.**
- **EIRP [dBm] = Power [dBm] – cable_loss [db] + antenna_gain [dBi]**

© 2006 Cisco Systems, Inc. All rights reserved.BCMSN v3.0-4-32

EIRP is defined as the effective power in front of the antenna. The EIRP of a transmitter is the power that the transmitter would appear to have if the transmitter were an isotropic radiator (that is, 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). Transmit power is rated in dBm or mW:

$$\text{EIRP} = \text{transmitter power} + \text{antenna gain} - \text{cable loss}$$

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 have different standards. Check with authorities in the country of installation to determine maximum EIRP.

EIRP is what the FCC and European Telecommunications Standards Institute (ETSI) uses for power limits in regulations for 2.4-GHz and 5-GHz WLANs.

Antenna Cable Loss

This subtopic describes antenna cable loss.


Antenna Cable Loss

Use cable that is supplied with the antenna, avoiding long cable runs when possible.


Cisco offers these cables:

- **LMR400-style cables**
 - 20 and 50 feet
 - Total loss of 1.3 and 3.4 dB, respectively
- **LMR600-style cables**
 - 100 and 150 feet
 - Total loss of 4.4 and 6.6 dB, respectively

LMR400

3/8" 

LMR600

1/2" 

Cable Type	2.4-GHz Loss (db/100 feet)	5.8-GHz Loss (db/100 feet)
LMR400	6.6	10.8
LMR600	4.4	7.25

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0—6-33

RF energy is carried between the antennas and the radio equipment through a coaxial cable. An antenna cable introduces signal loss in the antenna system for both the transmitter and receiver. Loss of signal strength is directly proportional to the length of the cable segment.

As the diameter of the cable increases, signal loss is decreased, but at a much higher purchase cost. As signal frequency increases (higher-numbered channel), signal loss increases.

To reduce signal loss, minimize the cable length and use only low-loss or ultralow-loss antenna cable to connect radio devices to antennas.

2.4-GHz EIRP Rules for FCC-Governed Countries

This subtopic describes the EIRP rules for FCC countries.

2.4-GHz EIRP Rules for FCC-Governed Areas

Point-to-Multipoint				
	Transmitter Power	Transmitter dBm	Maximum Gain	EIRP
FCC Maximum	1 W	30 dBm	6 dBi	36 dBm
Cisco Maximum	100 mW	20 dBm	16 dBi	36 dBm
Reduced Tx Power	20 mW	13 dBm	23 dBi	36 dBm

The above values reflect the 1:1 rule.

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 1-dBi.

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0-6-34

The output of the radio is measured in dBm. The figure shows the dBm ratings for Cisco Aironet Wireless equipment and the resulting EIRP when this equipment is used with a 6-dBi patch antenna and the FCC maximum of 36 dBm for multipoint wireless links.

The maximum EIRP allowed by the FCC for a Part 15 2.4-GHz 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.

Therefore, 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.

The highest gain antenna approved by Cisco for the 2.4-GHz frequency band is the 21-dBi Parabolic Dish Antenna.

2.4-GHz EIRP Rules for ETSI-Governed Countries

This subtopic describes the EIRP rules for ETSI countries.

2.4-GHz EIRP Rules for ETSI-Governed Areas				
	Transmitter Power	Transmitter dBm	Maximum Gain	EIRP
ETSI Maximum	50 mW	17 dBm	3 dBi	20 dBm
Cisco Maximum	50 mW	17 dBm	2.2 dBi	19.2 dBm
Reduced Tx Power	20 mW	13 dBm	7 dBi	20 dBm
Reduced Tx Power	10 mW	10 dBm	10 dBi	20 dBm
Reduced Tx Power	1 mW	0 dBm	20 dBi	20 dBm

- **Currently ETSI allows 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.**
- **Reduce transmit power below maximum of 17 dBm by 1 dBm and increase antenna/cable system gain by 1 dBi.**

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0—6-35

The figure shows the ETSI standards. Here is an excerpt from the document ETSI EN 300 328-1 V1.2.2 (2000-07):

The effective radiated power is defined as the total power of the transmitter. The effective radiated power shall be equal to or less than 20 dBm (100 mW) EIRP. This limit shall apply for any combination of power level and intended antenna assembly. To stay in the limit of the EIRP in Europe, you have to reduce the conducted power of the Aironet devices when you use antennas with more than 3-dBi gain.

EIRP Rules Summary

This subtopic gives a summary of the EIRP regulations.

EIRP Rules: Summary							
Frequency [GHz]	No. of Channels (26 total)	Channel Identifier	Usage	FCC			ETSI
				TX Power	Ant. Gain	EIRP	EIRP
2.400 – 2.483	3	1, 6, 11	Indoor Outdoor	30 dBm	6 dBi	36 dBm	20 dBm
5.150 – 5.250	4	36 – 48	Indoor only	16 dBm	6 dBi	22 dBm	23 dBm
5.250 – 5.350	4	52 – 64	Indoor Outdoor	24 dBm	6 dBi	30 dBm	23 dBm
5.470 – 5.725	11	100 – 140	Indoor Outdoor	24 dBm	6 dBi	30 dBm	30 dBm
5.725 – 5.825	4	149 – 161	Indoor Outdoor	30 dBm	6 dBi	36 dBm	n/a

• 5.725 MHz and above currently not allowed in most of Europe

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0-5-36

The table summarizes the EIRP limits for 2.4-GHz and 5-GHz WLANs in FCC and ETSI regulation domains.

Here is an excerpt from FCC Title 47 Section 15.407:

■ Power limits:

- 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 $4 \text{ dBm} + 10\log B$, 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.

- 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 $11 \text{ dBm} + 10\log B$, 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.

Summary

This topic summarizes the key points covered in this lesson.

Summary

- **Autonomous and lightweight WLAN solutions are the Cisco implementations of WLAN.**
- **LWAPP is the protocol used between lightweight access points and WLAN controllers.**
- **WLAN components include clients, access points, controllers, management systems, infrastructure devices, and security server.**
- **The Cisco Unified Wireless Network provides a unified enterprise-class wireless solution.**
- **Cisco Aironet access points are available for indoor or outdoor use.**
- **Access points and IP phones can be powered over Ethernet cable.**
- **Characteristics of antennas are directionality, gain, and polarisation.**
- **Multipath distortion can cause low quality data transmission.**
- **Antenna and RF power is measured in decibels.**
- **EIRP limits are defined by FCC and ETSI regulations.**

Configuring WLANs

Overview

This lesson describes the configuration of Cisco Systems wireless LAN (WLAN) autonomous and lightweight access points and Cisco Wireless LAN Controllers (WLCs).

Objectives

Upon completing this lesson, you will be able to configure autonomous and lightweight Cisco WLAN solutions. This ability includes being able to meet these objectives:


- List the different methods that can be used to configure autonomous access points
- Describe the role performed by autonomous access points and bridges in a radio network
- Describe how to configure an autonomous access point
- Describe how to configure a WLAN controller
- Describe how to perform the initial configuration of WLAN controllers via the command line and web browser
- Describe how to configure WLAN controllers via the web browser

Autonomous Access Point Configuration

This topic describes how to configure autonomous access points.

Autonomous Access Point Configuration

- **Configuration**
 - **Web browser (preferred)**
 - **Cisco IOS command line**
 - **Serial console**
 - **Telnet or SSH**
 - **CiscoWorks WLSE (optional)**
- **IP address required except for serial console**



The diagram illustrates the configuration process. A laptop is shown at the top, with a downward-pointing arrow leading to a Cisco autonomous access point (AP) at the bottom. The AP is a small, rectangular device with a Cisco logo and the text '3504 004' on its side.

© 2004 Cisco Systems, Inc. All rights reserved. BCMSN v3.0—4-3

You can configure an autonomous access point in any of these ways:

- Using the Cisco IOS command-line interface (CLI) via serial console.
- Using the Cisco IOS command line via Telnet or Secure Shell Protocol (SSH).
- Using a web browser (the preferred configuration method).
- Using the CiscoWorks Wireless LAN Solution Engine (WLSE). The optional Cisco WLSE allows centralized configuration and monitoring of the Cisco Aironet autonomous access points and provides radio frequency (RF) management, rogue access-point detection, and interference detection.

The WLAN configuration requires an IP address on the access point, except for the serial console.

Autonomous Access Point IP Address

This subtopic describes how to set the IP address for the autonomous access point.

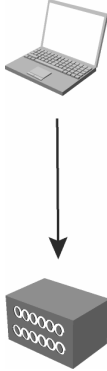
Autonomous Access Point IP Address

Set IP address on access point.

- DHCP (default)
- Serial console

Find IP address of access point.

- DHCP server
- Serial console
- CDP (switch)
- Other access point



The diagram illustrates the connection between a laptop and an access point. A laptop is shown at the top, with a vertical arrow pointing downwards to a rectangular access point device at the bottom. The access point has several ports on its side and the text 'RTP, DM' is visible on its right side.

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0-6.4

The IP address on an autonomous access point can be set in these ways:

- Using a DHCP server
- Using the CLI via the serial console

The IP address of the access point can be found in these ways:

- Checking the DHCP server for the LAN MAC address of the access point
- Using the serial console
- Checking the Cisco Discovery Protocol (CDP) table on the next-hop switch or router
- Checking the network map on other access points in the broadcast domain

Role of Autonomous Access Points in a Radio Network

This topic describes the role performed by autonomous access points and bridges in a radio network.

Role of Autonomous Access Points in a Radio Network

Cisco Aironet 1100, 1200, and 1300 Series

- Access point (fallback to radio island)
- Access point (fallback to radio shutdown)
- Access point (fallback to repeater)
- Repeater (nonroot access point)
- Root bridge
- Nonroot Bridge
- Root bridge with wireless clients
- Nonroot Bridge With Wireless Clients
- Workgroup bridge
- Scanner

Bridge modes not supported on the Cisco 1100 Series

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0—6.6

The Cisco Aironet 1100, 1200, and 1300 Series autonomous access points and bridges can perform these functions in a WLAN network:

- Access point
- Repeater (nonroot access point)
- Bridge (root and nonroot)
- Workgroup bridge
- Scanner

This ability to perform different functions in a network allows flexible use of the wireless equipment.

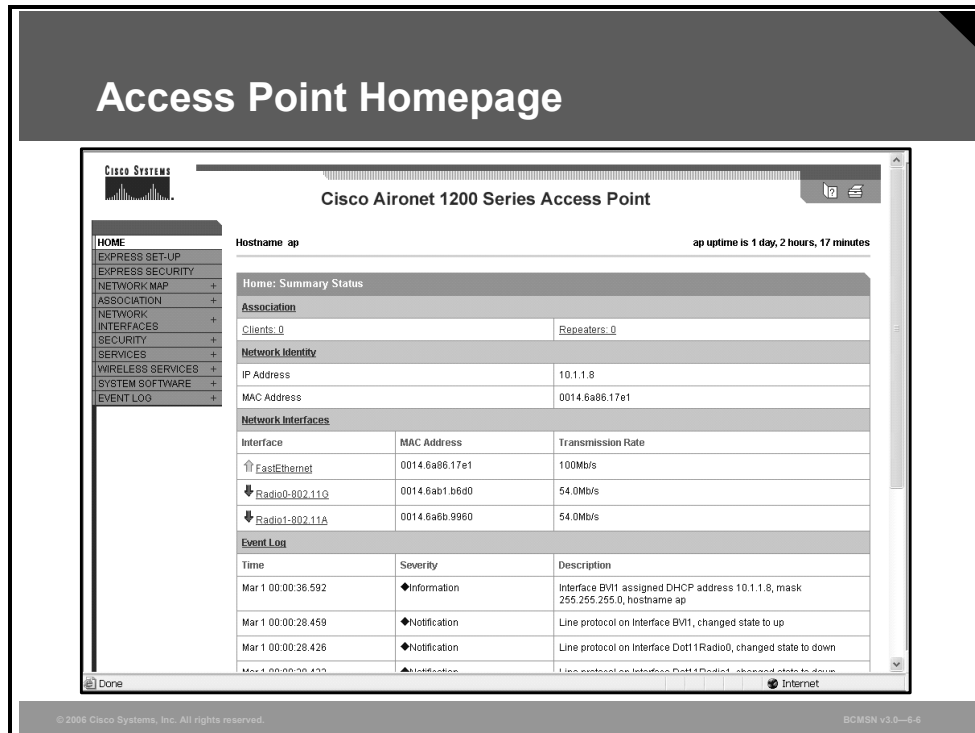
Bridge modes are not supported on the Cisco Aironet 1100 Series. The 1100 Series access points can be used as workgroup bridges.

Root devices accept associations from nonroot devices. Only nonroot devices can initiate connections such as clients to root devices. Therefore, it is important to configure the role of the device.

Access point and bridging can be combined in one device with two radios (2.4 and 5 GHz).

Autonomous Access Point Configuration via the Web Browser

This topic describes the configuration of an autonomous access point via the web browser.



The figure shows the home page of an autonomous access point. The home page is displayed when you connect to the access point. You can access configuration options from the menu on the left. You can return to the home page on the Cisco IOS access point at any time by clicking **Home** on the menu. The home page provides a quick summary of the access point and bridge status. This information is included:

- **Network Identity:** This area summarizes the configuration of the access point Bridge-Group Virtual Interface (BVI) and Ethernet MAC address.
- **Network Interfaces:** This area shows basic information on the access point network interfaces. The title is a link to the Network Interfaces page, which provides more information on data traffic through the ports. The access point radios are Radio0-802.11b/g (2.4 GHz) and Radio1-802.11a (5 GHz).
 - **Interface:** Displays current interface status
 - **MAC Address:** Displays the MAC address of each interface
 - **Transmission Rate:** Gives the operational data rate of each interface
- **Event Log:** After the access point has started running, the Event Log area displays the recent events that have been logged.
 - **Time:** Shows the time of the event, expressed in system uptime or wall-clock time
 - **Severity:** Indicates the level of each event or alarm that is processed by the access point
 - **Description:** Gives a brief description of the error or alarm event

Autonomous Access Point Express Setup

This subtopic describes the settings on the Express Setup web page.

Express Setup

Cisco Aironet 1130AG Series Access Point

Hostname ap ap uptime is 9 minutes

Express Set-Up

Host Name:

MAC Address: 000b.fcfb.7d2f

Configuration Server Protocol: DHCP Static IP

IP Address:

IP Subnet Mask:

Default Gateway:

SNMP Community:

Read-Only Read-Write

Radio0-802.11G

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

Optimize Radio Network for: Throughput Range Default Custom

© 2006 Cisco Systems, Inc. All rights reserved. BCM5N v3.0-6.7

Initial configuration of access point: hostname, IP address, SNMP

The Express Setup page allows configuration of the basic parameters of the access point. These parameters may be set for either of the radio interfaces of the access point or as follows:

- **Host Name:** A unique identifier that stations must use to be able to communicate with an access point. The host name can be any alphanumeric entry up to a maximum of 32 characters.
- **IP Address:** The IP address can be assigned either dynamically from a central server or statically from a system administrator.
- **SNMP Community:** The Simple Network Management Protocol (SNMP) community name required by the trap destination before it records traps sent by the device.

In addition, parameters for the radio interfaces can be configured. Radio interfaces are enabled from the Network Interfaces option in the menu on the left.

Service Set Identifiers (SSIDs) can be configured from the Express Security or the Security menu option.

Lightweight WLAN Controller Configuration

This topic describes how to configure a lightweight WLAN controller.

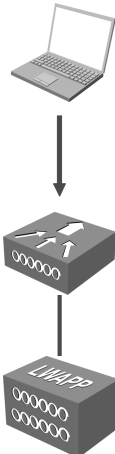
Lightweight WLAN Controller Configuration

Initial setup

- **Command line via serial console**
- **Web browser via service port**
 - No service port on the Cisco WLC 2006

Ongoing configuration

- **Requires IP address to be configured on controller**
- **Web browser**
- **Command line via serial console, Telnet, or SSH**
- **Cisco WCS (optional)**
- **DHCP server for access points required (Layer 3 mode)**



The diagram illustrates the configuration process. At the top, a laptop is shown with a downward arrow pointing to a Cisco WLC 2006 controller. Below this controller, another downward arrow points to a second Cisco WLC 2006 controller, representing a central configuration point.

© 2006 Cisco Systems, Inc. All rights reserved.RCMSN v3.0-6.0

The initial configuration of the WLAN controller can be done in these ways:

- Using the CLI via serial console
- Using the web browser via the service port

The service port and the initial configuration via web browser are not available on the Cisco 2000 Series Wireless LAN Controllers.

The WLAN configuration requires the configuration of IP addresses on the WLAN controller. The WLAN configuration can be done in these ways:

- Using a web browser.
- Using the CLI via serial console, Telnet, or SSH.
- Using the Cisco Wireless Control System (WCS). Cisco WCS allows centralized configuration of the Cisco WLCs.

Lightweight WLAN Controller Interfaces

This subtopic lists the lightweight WLAN controller interfaces.

Lightweight WLAN Controller Interfaces					
Interface Type	Service	Management	AP-Manager	Virtual	User
Category	Static	Static	Static	Static	Dynamic
IP Address	Subnet A	Subnet B	Subnet B	Unique IP for mobility group	User subnets
No. of interfaces	0 or 1	1 per controller	1 or more	1	0 or more
Function	Initial configuration Out-of-band configuration	Ongoing configuration In-band configuration	Layer 3 LWAPP	Mobility DHCP relay Web authentication IPSec	User data
LWAPP	N/A	Layer 2	Layer 3	N/A	None
802.1Q VLAN	N/A	Native/ untagged	Native/ untagged	N/A	User VLANs

© 2006 Cisco Systems, Inc. All rights reserved. BCM5N v3.0—6-18

The figure lists the interfaces on a Cisco WLC.

Service port: The service port is used for out-of-band management including initial setup of the WLAN controller. It has to be connected to a different subnet than the other interfaces. On the Cisco 2006 WLC, no service port is available.

Management interface: The management interface is used by the lightweight access points to associate to the WLAN controller. There is one management interface per WLAN controller.

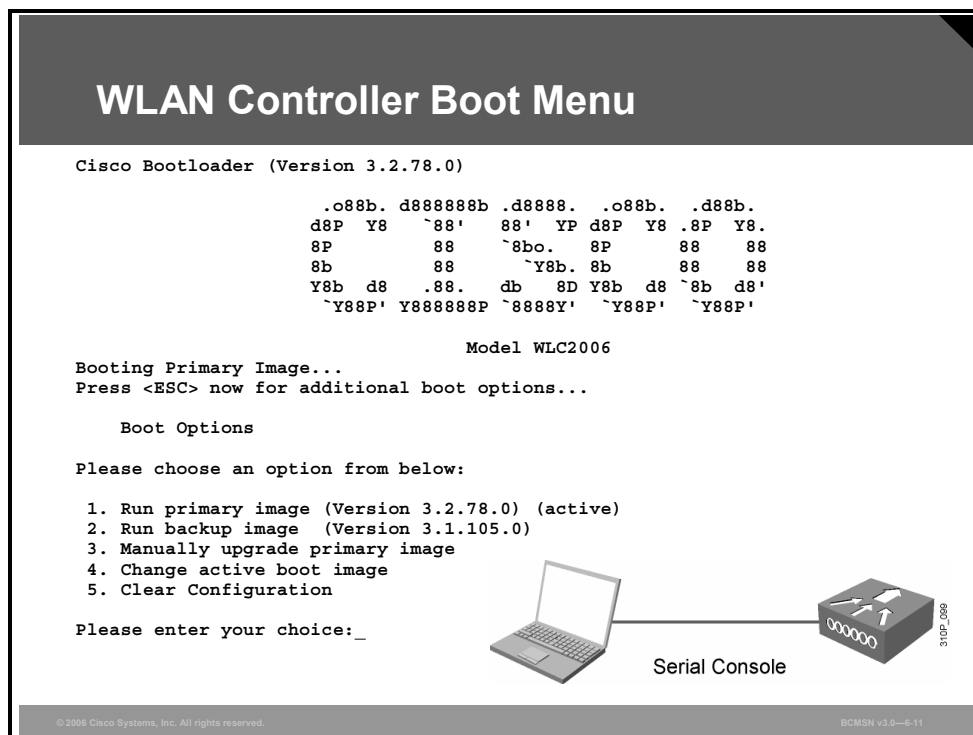
AP-manager interface: The access point management interface is used for all Lightweight Access Point Protocol (LWAPP) traffic between the lightweight access points and the WLAN controller. You can configure more than one management interface per WLAN controller.

Virtual interface: The virtual interface is a unique IP address per mobility group. This address is used for communication between the access point and the controller for mobility, DHCP relay, web authentication, and IP Security (IPsec). A mobility group is a group of WLAN controllers that are implementing Layer 3 roaming.

User interface: The user interfaces carry the data traffic into different VLANs. One user interface is configured per VLAN. The SSIDs are mapped to the VLANs.

Cisco WLC Boot Menu

This topic describes initial configuration of WLAN controllers via the command line.



On the console port, you see the boot messages of the WLAN controller during the boot process. Press the **ESC** key for these additional boot options. The figure shows the menu options.

- Enter **1** to continue to boot the primary image (default).
- Enter **2** to boot the backup image (image used before last software upgrade).
- Enter **3** for manual upgrade of image files.
- Enter **4** to set the backup image as the primary image.
- Enter **5** to clear the configuration and start the CLI setup wizard.

Note Option 3 is for recovery only. Do not use this option unless you have the required files and are instructed to do so by the Cisco Technical Assistance Center (TAC).

CLI Wizard Configuration Tool

This subtopic describes how to use the CLI wizard configuration tool.

```
CLI Wizard Configuration Tool

Booting Primary Image...
Press <ESC> now for additional boot options...
Detecting hardware . . . .

< Output omitted >

(Cisco Controller)

Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco 33:ef:80]: 1WLC1
Enter Administrative User Name (24 characters max): cisco
Enter Administrative Password (24 characters max): *****

Management Interface IP Address: 192.168.111.206
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 192.168.111.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 192.168.111.1

AP Manager Interface IP Address: 192.168.111.3

AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (192.168.111.1):

< continued .. >
```

The figure shows the first part of the initial configuration of a Cisco 2006 WLC via the serial console.

- The minus key (–) can be used to return to the previous question.
- Commands are case-sensitive, and uppercase options are default values.
- The controller name supports up to 32 printable ASCII characters.
- The user name and password for administration is configured.
- The management interface IP address, netmask, default gateway, VLAN, port number, and DHCP server are configured.
- The AP-manager interface is configured with an IP address that is in the same subnet as the management interface.

CLI Wizard Configuration Tool (Cont.)

```
< continued .. >

Virtual Gateway IP Address: 1.1.1.11

Mobility/RF Group Name: group1

Network Name (SSID): wlan1
Allow Static IP Addresses [YES] [no]: no

Configure a RADIUS Server now? [YES] [no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.

Enter Country Code (enter 'help' for a list of countries) [US]:

Enable 802.11b Network [YES] [no]:
Enable 802.11a Network [YES] [no]:
Enable 802.11g Network [YES] [no]:
Enable Auto-RF [YES] [no]:

Configuration saved!
Resetting system with new configuration...

Cisco Bootloader (Version 3.2.78.0)

Booting Primary Image...
```

© 2006 Cisco Systems, Inc. All rights reserved.

BCM59 v3.0-6-13

The figure shows the remainder of the CLI configuration.

- The virtual gateway IP address must be an unassigned, unreachable IP address.
- Static IP defines if a DHCP server must be used by WLAN clients or if they may configure a static address to use the WLAN.
- The initial WLAN defaults to 802.1x security to ensure that there is no accidental access.
- The country code defines which channels, frequencies, and power output will be available per the country regulations.
- Auto-RF enables auto-RF functions.
- The configuration is saved, and the controller is rebooted after the final value of the CLI wizard.

WLAN Controller CLI Commands

This subtopic describes some CLI commands that can be used for the WLAN controller configuration.

WLAN Controller CLI Commands

```
(Cisco Controller) > config network webmode enable
```

- **Enables Web access via SSL, required for web management**

```
(Cisco Controller) > config network telnet enable
```

- **Enables CLI access via Telnet**

```
(Cisco Controller) > config prompt name  
(name) >
```

- **Configures the prompt, usually set to the system name**

© 2006 Cisco Systems, Inc. All rights reserved.BCMSN v3.0—6-14

The figure shows three CLI configuration commands.


- The **config network webmode enable** command enables web mode, which allows HTTP access to the WLAN controller. Secure Socket Layer (SSL) (HTTPS) access is enabled by default.
- The **config network telnet enable** command enables Telnet, which allows Telnet access to the CLI of the WLAN controller. SSH access is enabled by default.
- The **config prompt name** command configures the system prompt, which usually is configured with the system name.

Web Wizard Initial Configuration

This topic describes the web wizard for the initial configuration of the WLAN controller.

Controller Web Configuration Wizard Login

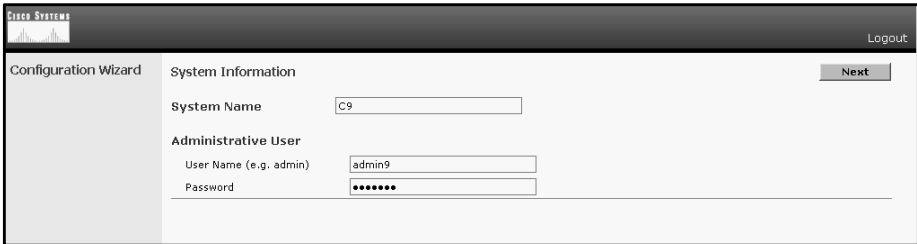
- Initial setup via web browser through service port
- Not available on Cisco 2006 WLC
- Default IP address 192.168.1.1/24
- Username: admin
- Password: admin



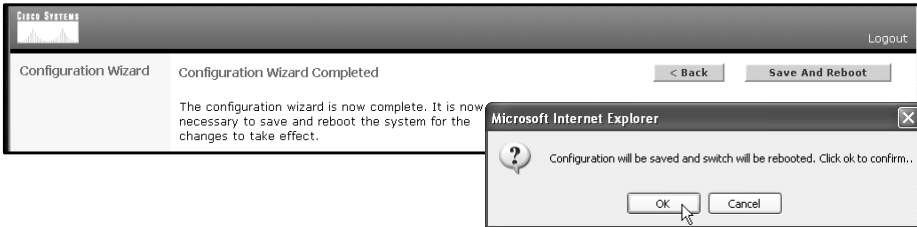
© 2006 Cisco Systems, Inc. All rights reserved. BCM5N v3.0-6-15

The Cisco 4400 Series WLAN controller supports the initial configuration via web browser through the service port. The default IP address of the unconfigured controller is 192.168.1.1/24 with admin as the default user and password.

Controller Initial Web Configuration Wizard



The wizard prompts for the initial setup parameters (similar to the CLI setup dialog).



© 2006 Cisco Systems, Inc. All rights reserved. BCM5N v3.0-6-16

WLAN Controller Web Configuration

This subtopic describes the ongoing configuration of the WLAN controller via the web interface.



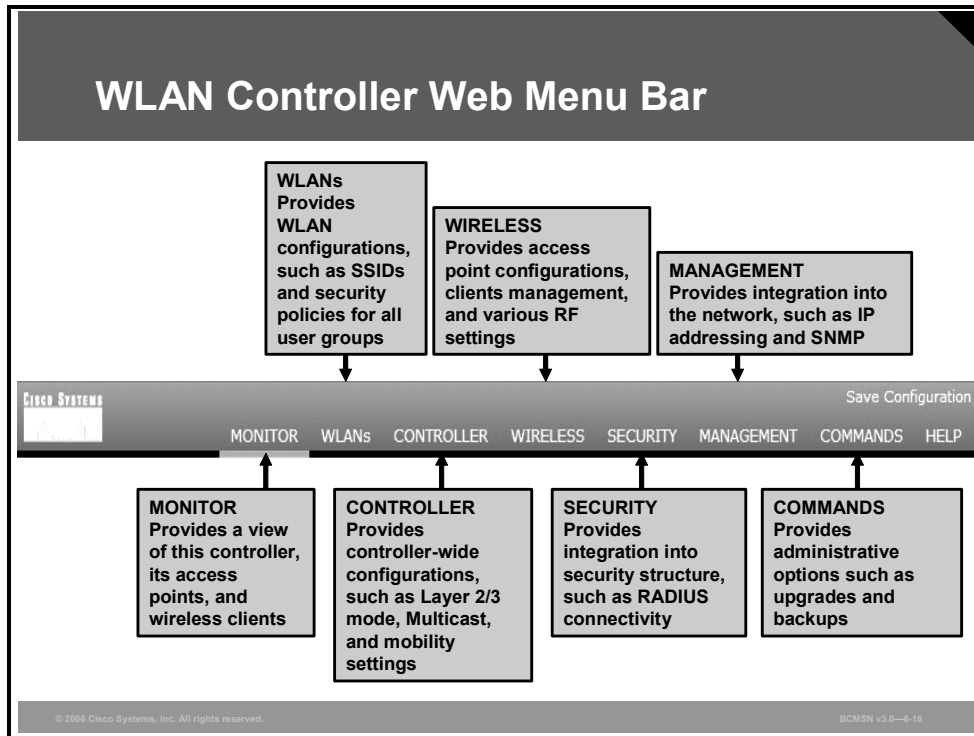
Cisco recommends using Internet Explorer 6.0 with Service Pack 1 (SP1) or higher for full-switch web-interface functionality. There are known issues with Opera, Mozilla, and Netscape.

You can connect using either **http://<controller IP address>** or **https://<controller IP address>**, but HTTP is disabled by default. You can disable either HTTP or HTTPS access. If you receive the error message “The page cannot be displayed,” check to see if the corresponding access method has been disabled.

The WLAN controller web interface has a default inactivity timeout of 10 minutes.

WLAN Controller Web Menu Bar

This subtopic describes the menu bar of the WLAN controller web interface.



The figure shows the tabs and the settings available for each tab.

Monitor > Summary

Monitor

Summary

Controller Summary

Management IP Address	192.168.111.2
Software Version	3.2.78.0
System Name	1WLC1
Up Time	0 days, 0 hours, 18 minutes
System Time	Wed Mar 1 16:11:57 2006
802.11a Network State	Enabled
802.11b/g Network State	Enabled

Access Point Summary

	Total	Up	Down	
802.11a Radios	1	1	0	Detail
802.11b/g Radios	1	1	0	Detail
All APs	1	1	0	Detail

Client Summary

Current Clients	0	Detail
Excluded Clients	0	Detail
Disabled Clients	0	Detail

Rogue Summary

Active Rogue APs	4	Detail
Active Rogue Clients	0	Detail
Adhoc Rogues	0	Detail
Rogues on Wired Network	0	

Top WLANs

WLAN	# of Clients by SSID	
wlan11	0	Detail

Most Recent Traps

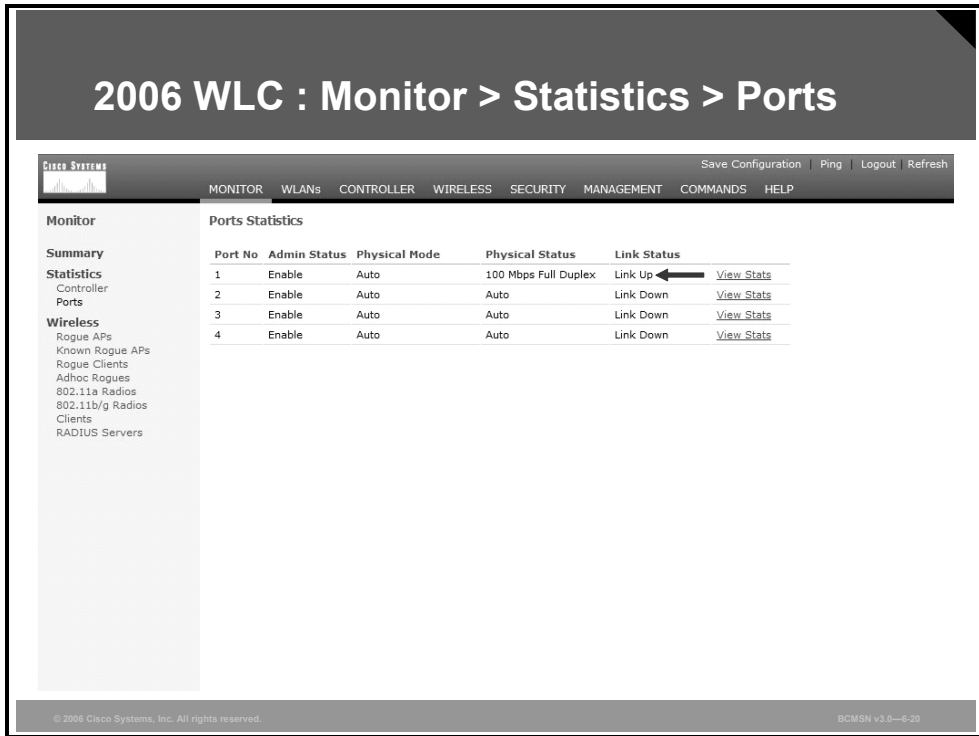
- Rogue AP : 00:0d:bd:01:15:e5 detected on Base Radio
- Rogue AP : 00:40:96:55:d7:a8 detected on Base Radio
- Rogue AP : 00:0d:65:bb:73:4e detected on Base Radio
- Rogue AP : 00:0d:bd:01:0c:f1 detected on Base Radio
- RF Manager updated TxPower for Base Radio MAC: 00:c

[View All](#)

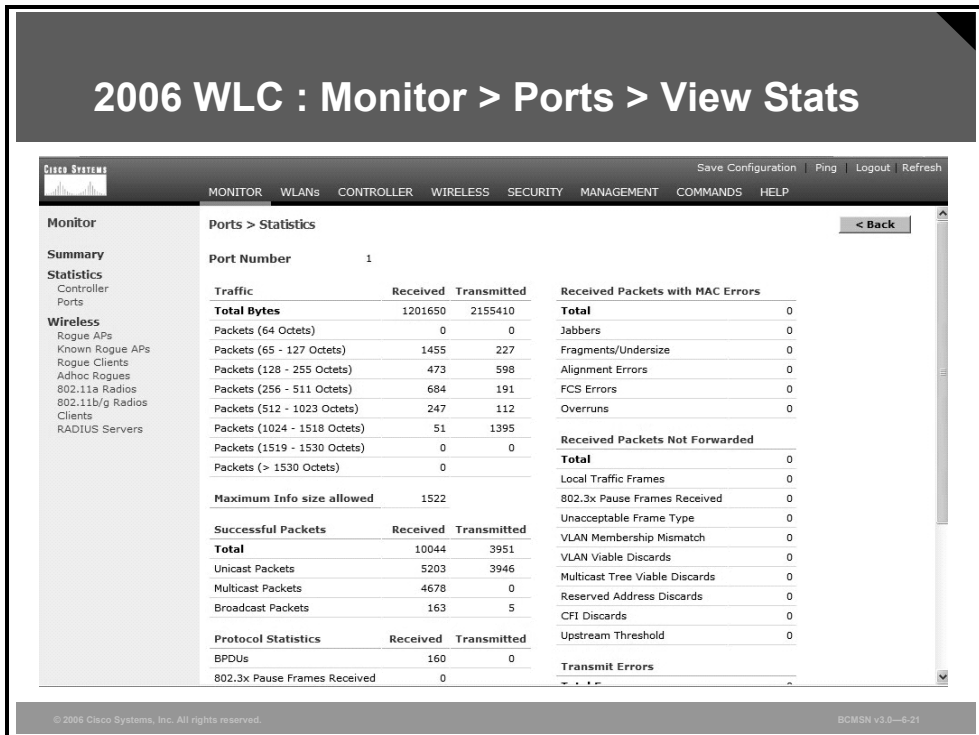
This page refreshes every 30 seconds.

© 2006 Cisco Systems, Inc. All rights reserved. BCM5N v3.0-6-18

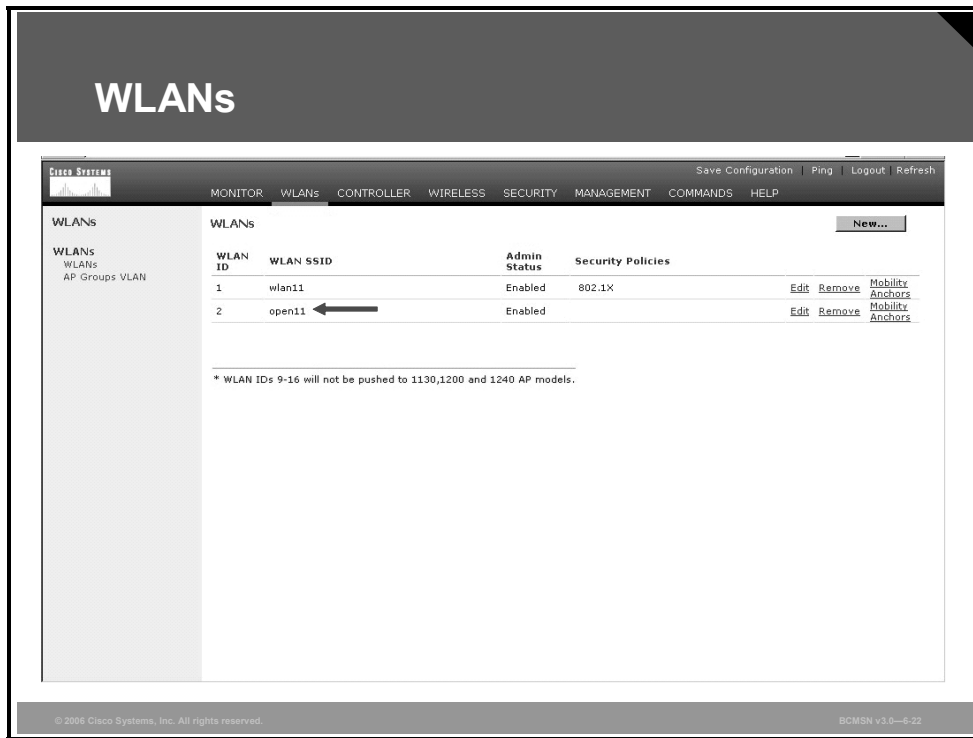
The figure shows the home page of the lightweight access point, which is displayed when you connect to the WLAN controller. The figures that follow show screen shots from the web interface of the WLAN controller.



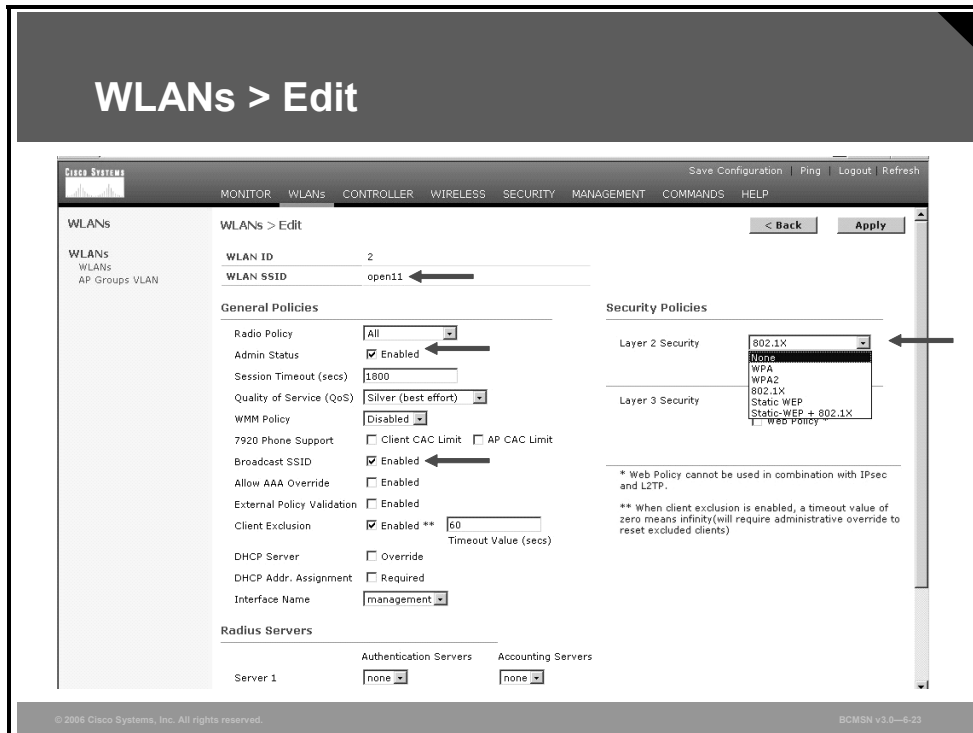
The figure shows the physical ports of a Cisco 2006 WLC.



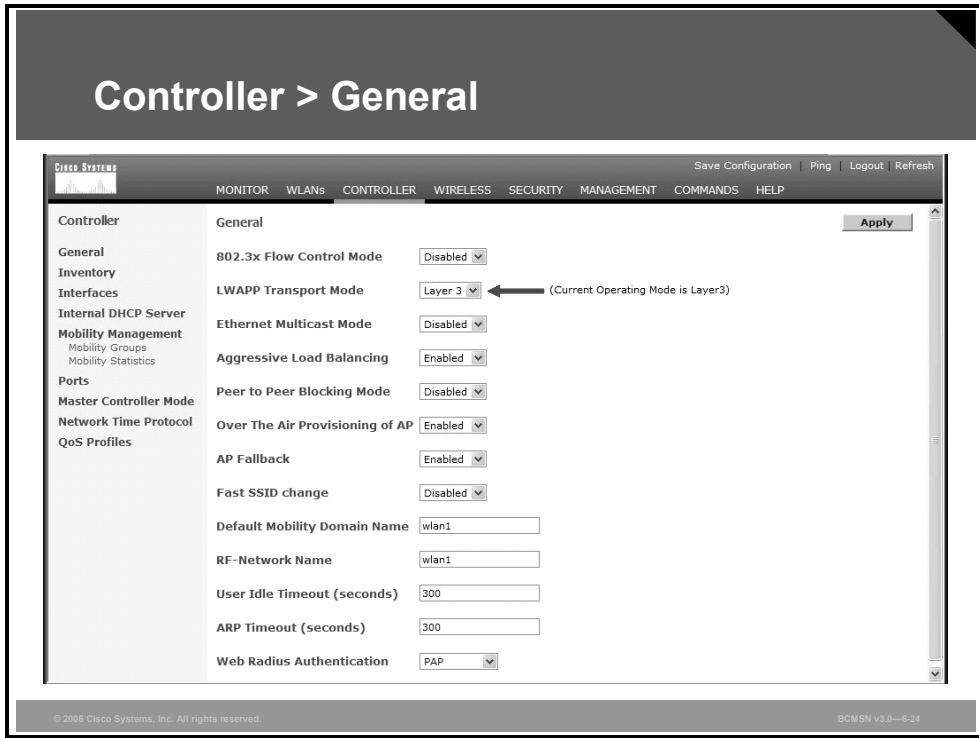
The figure shows the statistics of physical port 1 of a Cisco 2006 WLC.



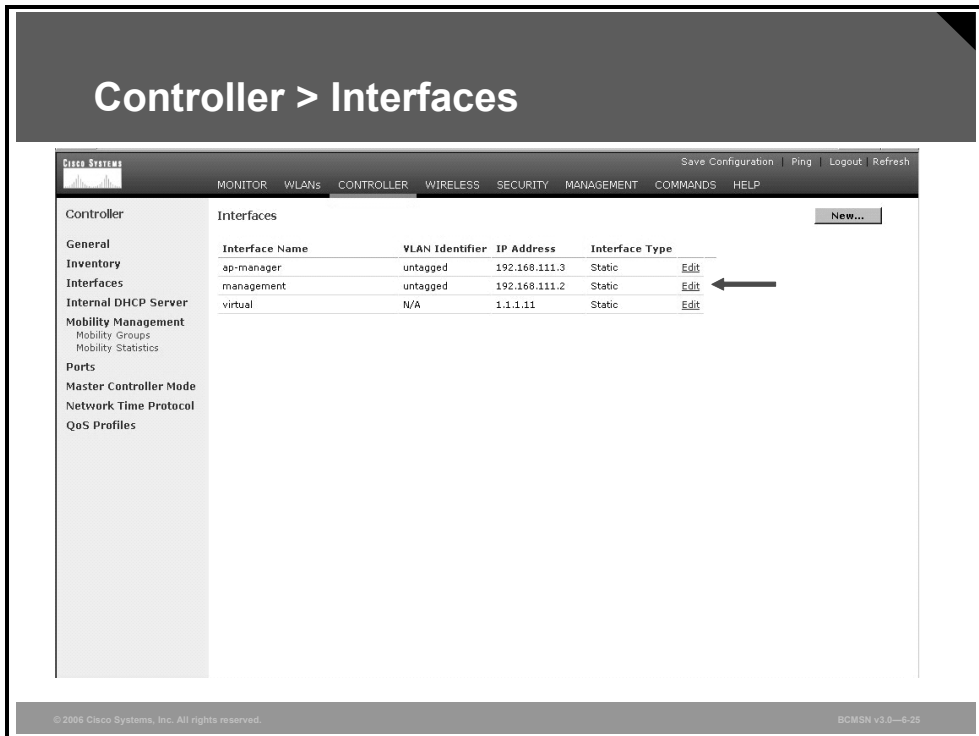
The figure shows the configured SSIDs (WLANs).



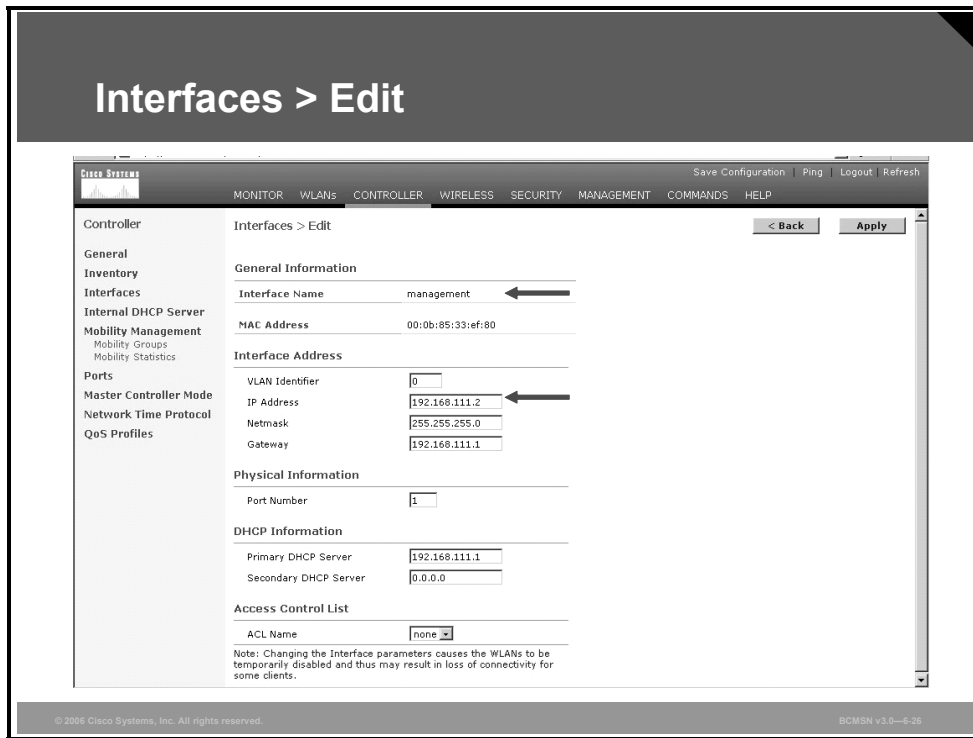
The figure shows details of the configured SSID “wlan11.”



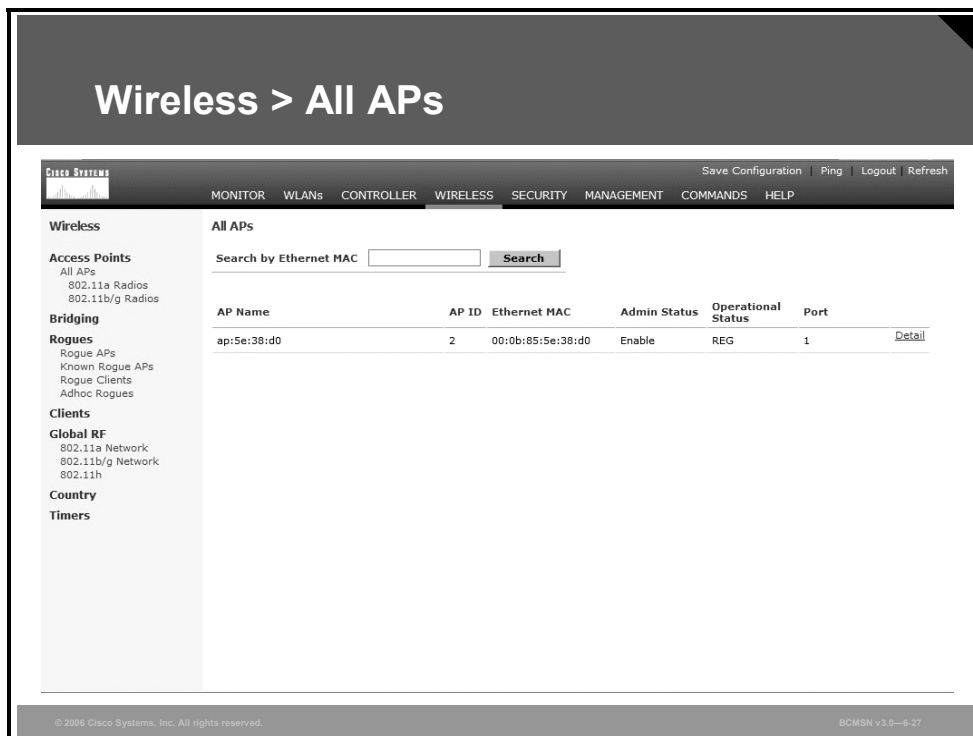
The figure shows general configuration of a Cisco 2006 WLC. The controller operates in Layer 3 LWAPP transport mode.



The figure shows the logical interfaces of a Cisco 2006 WLC.



The figure shows the configuration of the management interface of the controller.



The figure shows access points registered to the WLAN controller.

Wireless > All APs > AP Detail

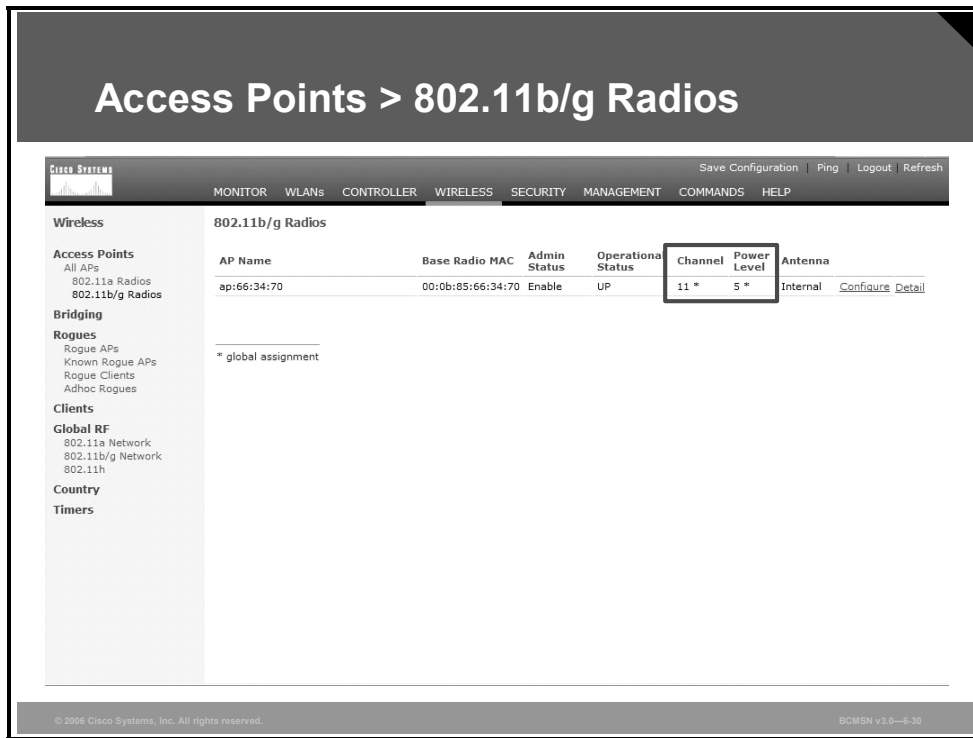
The screenshot displays the Cisco Wireless Management interface for an AP. The left sidebar shows navigation options like 'All APs', 'Rogue APs', and 'Global RF'. The main content area is titled 'All APs > Details' and is divided into several sections: 'General', 'Versions', 'Inventory Information', and 'Radio Interfaces'. The 'General' section contains fields for AP Name, Ethernet MAC Address, Base Radio MAC, Regulatory Domain, AP IP Address, AP Static IP, AP ID, Admin Status, AP Mode, Operational Status, Port Number, AP Group Name, Location, and controller information. The 'Versions' section shows S/W and Boot versions. 'Inventory Information' lists AP Model, Serial Number, and Certificate Type. 'Radio Interfaces' shows 2 interfaces. At the bottom, there are copyright notices for Cisco Systems and BCMSS v3.0-4-29.

The figure shows details of an access point with name and IP address.

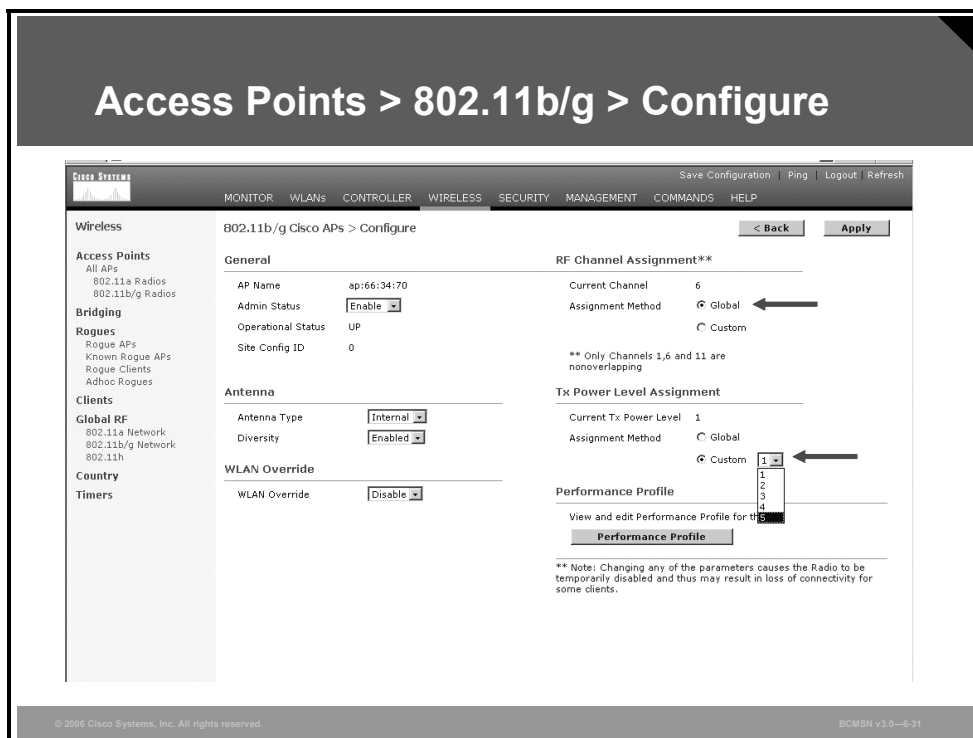
Wireless > All APs > AP Detail (Cont.)

This screenshot shows the bottom portion of the AP Detail page. It includes a table for 'Radio Interfaces' with columns for 'Radio Interface Type', 'Admin Status', 'Oper Status', and 'Regulatory Domain'. Below this are two sections: 'Hardware Reset' with a 'Reset AP Now' button, and 'Set to Factory Defaults' with a 'Clear Config' button. The interface also shows the 'AP IP Address' field and other configuration options. Copyright notices for Cisco Systems and BCMSS v3.0-4-29 are visible at the bottom.

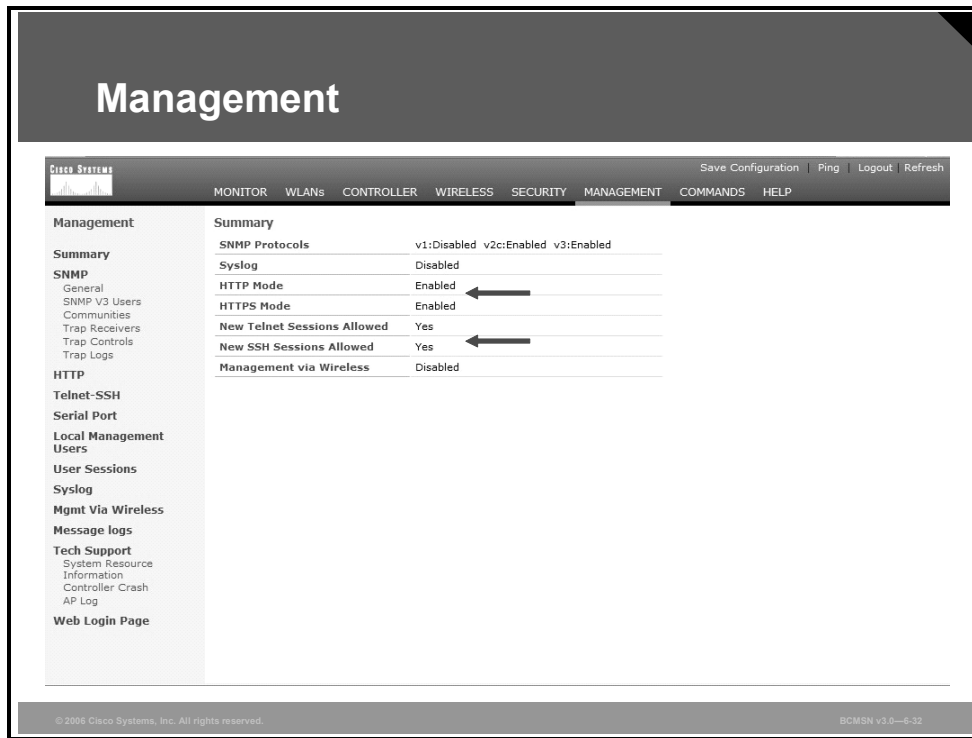
You can use the buttons at the bottom of the screen to reset this access point or clear the configuration of this access point.



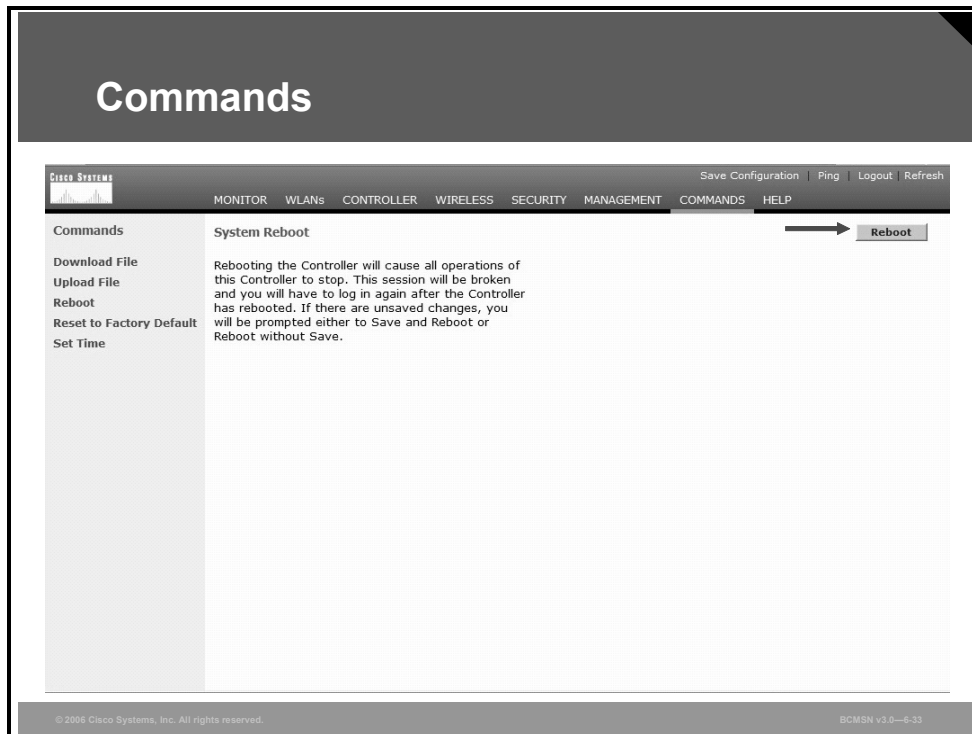
The figure shows the access points with an 802.11b/g radio and the current channel and power level.



The figure shows details of the 802.11b/g radio of this access point. This page allows you to configure channel and power level, if required.



The figure shows an overview of the management settings for this WLAN controller. From the menu on the left, you can configure management options, such as SNMP, HTTP, SSH, and logging.



The Commands menu gives you options to upgrade software, save configurations, reboot the WLAN controller, and clear the configuration of the WLAN controller.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- **Autonomous access points can be configured via console, CLI, Web browser and management system.**
- **An autonomous access points can act as a bridge, repeater, access point, or scanner.**
- **Autonomous access points can be configured easily via a web browser.**
- **Wireless LAN controllers can be initialized via CLI or Web browser.**
- **Wireless LAN controllers can be configured via CLI or Web browser.**
- **Wireless LAN configuration includes SSIDs, VLANs, access points, security, and management.**

Module Summary

This topic summarizes the key points that were discussed in this module.

Module Summary

- **WLANs are shared networks that provide access to networks for multiple users at high data rates.**
- **Types of WLAN topologies are client access, bridging, and mesh networking.**
- **WLAN standard 802.11b/g provides data rates of up to 54 Mbps at 2.4 GHz and 802.11a provides data rates of up to 54 Mbps at 5 GHz.**
- **WLAN components can be configured via CLI, web browser, and management system.**
- **Autonomous and lightweight WLAN solutions are the Cisco WLAN implementations.**
- **WLAN configuration includes SSIDs, VLANs, access points, security, and management.**

© 2006 Cisco Systems, Inc. All rights reserved.BOMSIN v3.0—6-1

This module introduces wireless LAN (WLAN) network access and describes typical WLAN topologies. WLAN technologies and the 802.11 standards are discussed. Cisco Systems autonomous and lightweight solutions for WLANs are described, and configuration of Cisco components of WLANs is outlined. Other concepts that are important to WLAN implementations, such as WLAN network components, Power over Ethernet (PoE), and WLAN antennas are explained.

References

For additional information, refer to these resources:

- Cisco Press:
<http://www.ciscopress.com>
- Cisco Systems, Inc., *Wireless: Introduction*,
<http://www.cisco.com/go/wireless>

Module Self-Check

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

- Q1) What are two similarities between WLANs and wired LANs? (Choose two.) (Source: Introducing WLANs)
- A) Both use MAC addresses.
 - B) Both use the same frame format.
 - C) Both can run the same applications.
 - D) Both use the same physical layer.
- Q2) What are two differences between WLANs and wired LANs? (Choose two.) (Source: Introducing WLANs)
- A) WLAN uses CSMA/CA and wired LAN uses CSMA/CD.
 - B) WLANs have problems not found on wired LANs.
 - C) WLAN uses CSMA/CD and wired LAN uses CSMA/CA.
 - D) WLANs and wired LANs run different applications.
- Q3) Which topology is *not* used for WLANs? (Source: Describing WLAN Topologies)
- A) client access
 - B) bridging
 - C) personal area networking
 - D) mesh networking
- Q4) Which two statements are *not* true about SSIDs? (Choose two.) (Source: Describing WLAN Topologies)
- A) SSIDs on client and access point have to match.
 - B) SSIDs are not case sensitive.
 - C) A client can be configured without an SSID.
 - D) SSIDs on all access points have to be identical.
- Q5) Which frequency bands are unlicensed? (Source: Explaining WLAN Technology and Standards)
- A) 2.4-GHz, 3.5-GHz, and 5-GHz
 - B) 900-MHz, 2.4-GHz, and 5-GHz
 - C) 2.4-GHz, 4.9-GHz, and 5-GHz
- Q6) Which two data rates are supported by the 802.11b standard? (Choose two.) (Source: Explaining WLAN Technology and Standards)
- A) 1 Mbps
 - B) 24 Mbps
 - C) 11 Mbps
 - D) 108 Mbps
- Q7) Which data rate is *not* supported by the 802.11g standard? (Source: Explaining WLAN Technology and Standards)
- A) 1 Mbps
 - B) 24 Mbps
 - C) 11 Mbps
 - D) 108 Mbps

- Q8) Which two types of encryption are available for WLANs? (Choose two.) (Source: Explaining WLAN Technology and Standards)
- A) TKIP
 - B) SNMP
 - C) AES
 - D) EAP
- Q9) The Cisco Aironet a/b/g card comes in which two formats? (Choose two.) (Source: Configuring Cisco WLAN Clients)
- A) Compact flash
 - B) PCMCIA
 - C) PCI
 - D) CardBus
- Q10) Which two operating systems are supported for CB21AG utilities (GUI)? (Choose two.) (Source: Configuring Cisco WLAN Clients)
- A) Windows 98
 - B) Linux
 - C) Windows 2000
 - D) Windows XP
- Q11) Which two wireless components are used for the autonomous WLAN solution? (Choose two.) (Source: Implementing WLANs)
- A) WLC
 - B) ACS
 - C) WLSE
 - D) WCS
- Q12) Which protocol supports “split MAC” operation for the Cisco lightweight WLAN solution? (Source: Implementing WLANs)
- A) CCKM
 - B) LWAPP
 - C) WLCCP
 - D) SNMP
- Q13) What is the maximum EIRP for 2.4-GHz point-to-multipoint communication in the United States? (Source: Implementing WLANs)
- A) 30 dBm
 - B) 36 dBm
 - C) 20 dBm
 - D) 17 dBm
- Q14) What causes multipath distortion? (Source: Implementing WLANs)
- A) reflected radio waves
 - B) radio waves reflected back at 180 degrees
 - C) direct radio waves and reflected radio waves received simultaneously
 - D) reflected radio waves in indoor environments

- Q15) Which two devices can be used to configure a WLAN using lightweight access points?
(Choose two.) (Source: Configuring WLANs)
- A) WCS
 - B) WLSE
 - C) WLC
 - D) access point
- Q16) Which two ways can be used to do the initial configuration of a wireless LAN controller? (Choose two.) (Source: Configuring WLANs)
- A) console port
 - B) Telnet
 - C) web browser
 - D) SNMP

Module Self-Check Answer Key

- Q1) A, C
- Q2) A, B
- Q3) C
- Q4) B, D
- Q5) B
- Q6) A, C
- Q7) D
- Q8) A, C
- Q9) C, D
- Q10) C, D
- Q11) B, C
- Q12) B
- Q13) B
- Q14) C
- Q15) A, C
- Q16) A, C

Configuring Campus Switches to Support Voice

Overview

When migrating to a VoIP network, all network requirements, including power and capacity planning, must be examined. In addition, congestion avoidance techniques should be implemented. This module will highlight the basic issues and define initial steps to take to ensure that the VoIP implementation works correctly.

Module Objectives

Upon completing this module, you will be able to describe and configure switch infrastructure to support voice. This ability includes being able to meet these objectives:

- Describe the best practices for implementing voice in a campus network
- Explain how to configure switches to support voice traffic

Planning for Implementation of Voice in a Campus Network

Overview

IP telephony services are often provided over the campus infrastructure. To have data and voice application traffic harmoniously coexist, mechanisms must be set in place to differentiate traffic and to offer priority processing to delay sensitive voice traffic. Quality of service (QoS) policies mark and qualify traffic as it traverses the campus switch blocks. Specific VLANs keep voice traffic separate from other data to ensure that it is carried through the network with special handling and with minimal delay. Specific design and implementation considerations should be made at all campus switches supporting VoIP.

Objectives

Upon completing this lesson, you will be able to describe the best practices for implementing voice in a campus network. This ability includes being able to meet these objectives:

- Explain why an organization would want to run VoIP on the network
- Describe the main components of a VoIP network, including IP-enabled PBX, user end-devices, gateways and gatekeepers, and the IP network
- Compare the uniform bandwidth consumption of voice traffic to the intermittent bandwidth consumption of data traffic
- Describe a VoIP call flow through a network and where contention for bandwidth between data traffic and voice traffic will occur
- Explain an auxiliary VLAN
- Identify a solution for latency, jitter, bandwidth, packet loss, reliability, and security
- Explain the importance of high availability in the campus network to support a VoIP implementation, including such regulations as E911 that require 99.999 percent system availability for phones
- Explain the need to add a UPS to wiring closets that do not already have them and to provision switches with inline power for IP phones

Explaining Converged Network Benefits

This topic explains why an organization would want to run VoIP on the network.

Benefits of a Converged Network

- **More efficient use of bandwidth and equipment**
- **Lower transmission costs**
- **Consolidated network expenses**
- **Increased revenue from new services**
- **Service innovation**
- **Access to new communications devices**
- **Flexible new pricing structures**

© 2004 Cisco Systems, Inc. All rights reserved.

BCMSN v3.0-7.2

The benefits of packet telephony versus circuit-switched telephony are as follows:

- **More efficient use of bandwidth and equipment:** Traditional telephony networks use a 64-kbps channel for every voice call. Packet telephony shares bandwidth among multiple logical connections and offloads traffic volume from existing voice switches.
- **Lower costs for telephony network transmission:** A substantial amount of equipment is needed to combine 64-kbps channels into high-speed links for transport across the network. Packet telephony statistically multiplexes voice traffic alongside data traffic. This consolidation represents substantial savings on capital equipment and operations costs.
- **Consolidated voice and data network expenses:** Data networks that function separately from voice networks become major traffic carriers. The underlying voice networks are converted to utilize the packet-switched architecture to create a single integrated communications network with a common switching and transmission system. The benefit is significant cost savings on network equipment and operations.
- **Increased revenues from new services:** Packet telephony enables new integrated services, such as broadcast-quality audio, unified messaging, and real-time voice and data collaboration. These services increase employee productivity and profit margins well above those of basic voice services. In addition, these services enable companies and service providers to differentiate themselves and improve their market position.
- **Greater innovation in services:** Unified communications use the IP infrastructure to consolidate communication methods that were previously independent; for example, fax, voice mail, e-mail, wireline telephones, cellular telephones, and the web. The IP infrastructure provides users with a common method to access messages and initiate real-time communications—independent of time, location, or device.

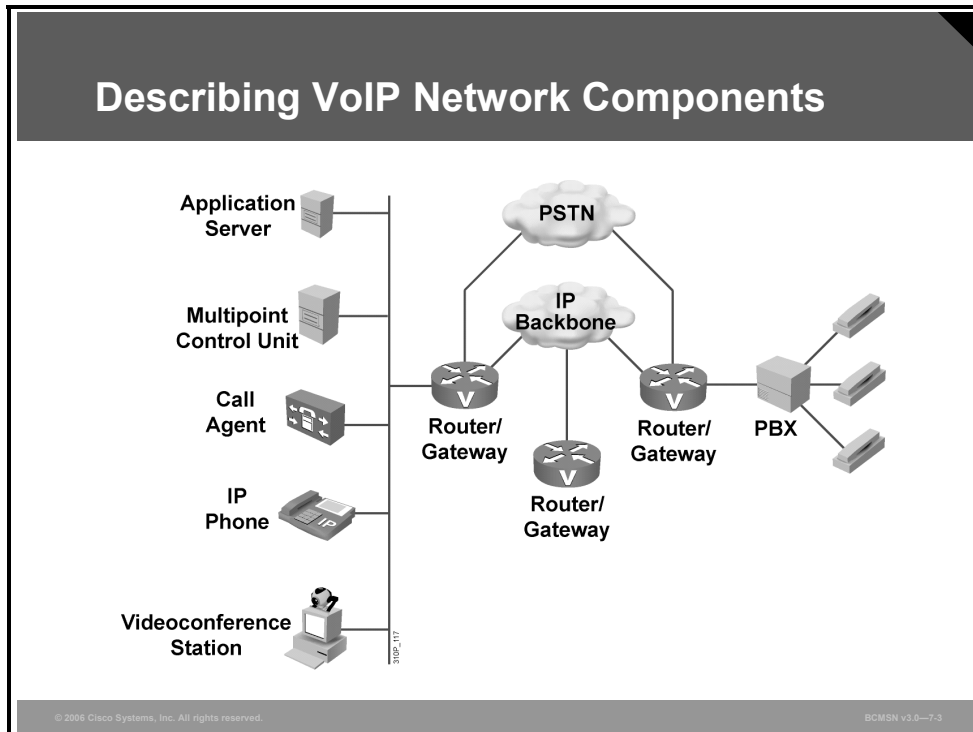
- **Access to new communications devices:** Packet technology can reach devices that are largely inaccessible to the time-division multiplexing (TDM) infrastructures of today. Examples of such devices are computers, wireless devices, household appliances, personal digital assistants, and cable set-top boxes.

Intelligent access to such devices enables companies and service providers to increase the volume of communications they deliver, the breadth of services they offer, and the number of subscribers they serve. Packet technology, therefore, enables companies to market new devices, including videophones, multimedia terminals, and advanced IP phones.

- **Flexible new pricing structures:** Companies and service providers with packet-switched networks can transform their service and pricing models. Because network bandwidth can be dynamically allocated, network usage no longer needs to be measured in minutes or distance. Dynamic allocation gives service providers the flexibility to meet the needs of their customers in ways that bring them the greatest benefits.

Describing VoIP Network Components

This topic describes the main components of a VoIP network, including IP-enabled PBX, user end-devices, gateways and gatekeepers, and the IP network.



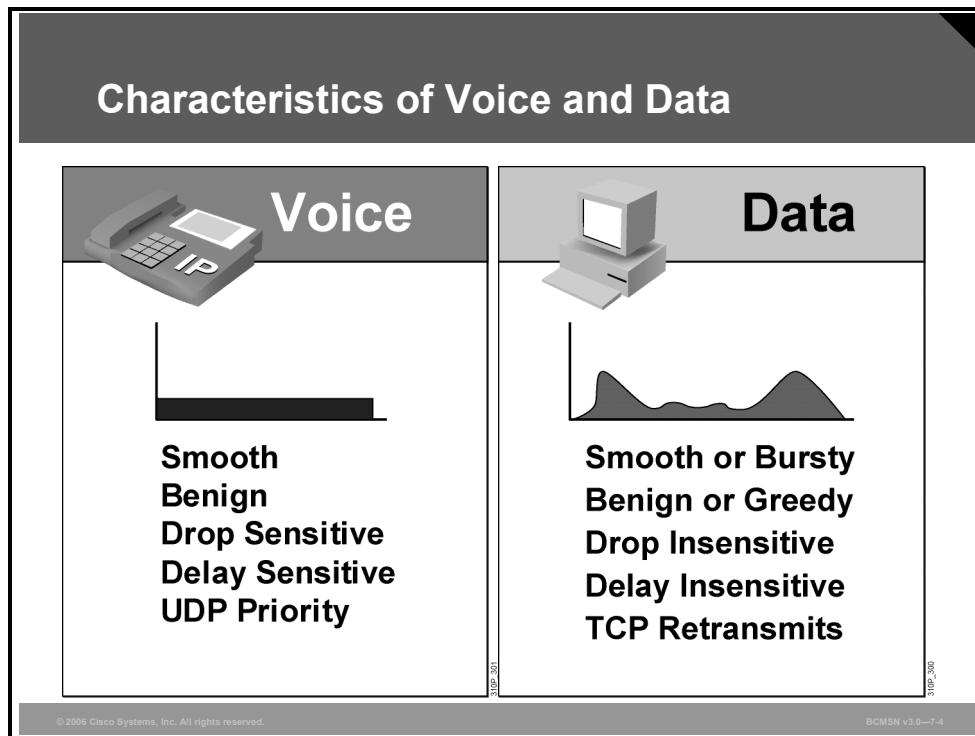
These are the basic components of a VoIP network:

- **IP phones:** Provide IP voice to the desktop.
- **Gatekeeper:** Provides connection admission control (CAC), bandwidth control and management, and address translation.
- **Gateway:** Provides translation between VoIP and non-VoIP networks, such as the public switched telephone network (PSTN). It also provides physical access for local analog and digital voice devices, such as telephones, fax machines, key sets, and PBXs.
- **Multipoint control unit:** Provides real-time connectivity for participants in multiple locations to attend the same videoconference or meeting.
- **Call agent:** Provides call control for IP phones, CAC, bandwidth control and management, and address translation.
- **Application servers:** Provide services such as voice mail, unified messaging, and Cisco CallManager Attendant Console.
- **Videoconference station:** Provides access for end-user participation in videoconferencing. The videoconference station contains a video capture device for video input and a microphone for audio input. The user can view video streams and hear the audio that originates at a remote user station.

Other components, such as software voice applications, interactive voice response (IVR) systems, and softphones, provide additional services to meet the needs of enterprise sites.

Explaining Traffic Characteristics of Voice and Data

This topic describes voice and data traffic characteristics in the campus network.



Voice traffic has extremely stringent QoS requirements. Voice traffic generally generates a smooth demand on bandwidth and has minimal impact on other traffic, as long as voice traffic is managed.

Although voice packets are typically small (60 to 120 bytes), they cannot tolerate delay or drops. The result of delays and drops is poor, and often unacceptable, voice quality. Because drops cannot be tolerated, User Datagram Protocol (UDP) is used to package voice packets; TCP retransmit capabilities have no value.

For voice quality, the delay should be no more than 150 ms (one-way requirement) and less than 1 percent packet loss.

A typical voice call requires 17 kbps to 106 kbps of guaranteed priority bandwidth, plus an additional 150 bps per call for voice-control traffic. Multiplying these bandwidth requirements by the maximum number of calls expected during the busiest time period indicates the overall bandwidth required for voice traffic.

The QoS requirements for data traffic vary greatly.

Different applications (for example, a human resources application versus an ATM application) may make greatly different demands on the network. Even different versions of the same application may have varying network traffic characteristics.

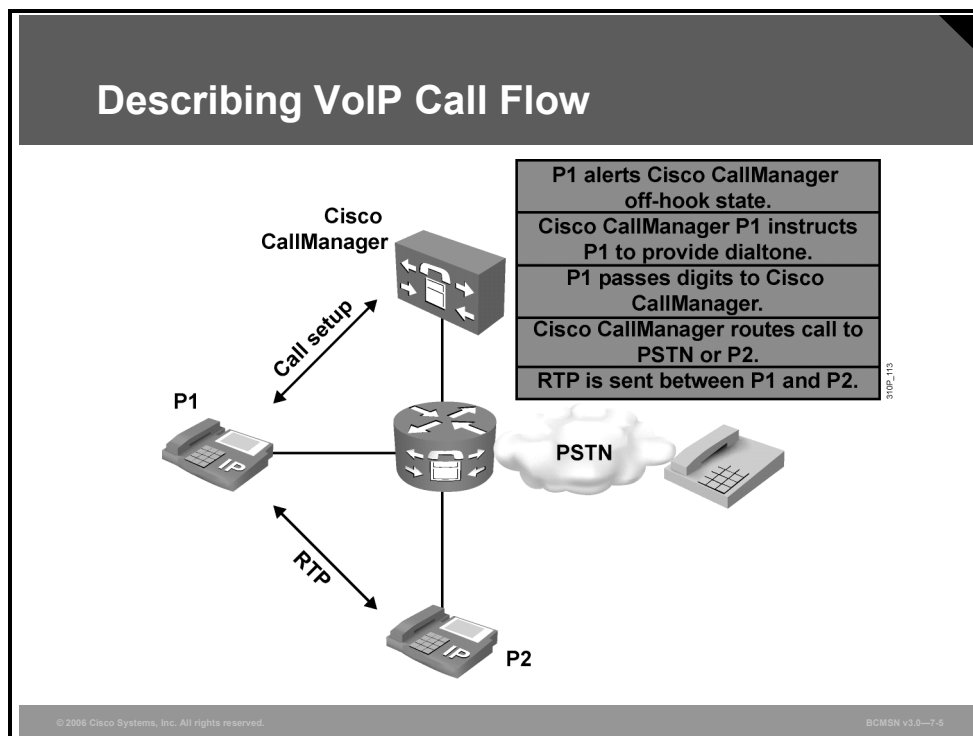
Data traffic can demonstrate either smooth or bursty characteristics, depending upon the application, but it differs from voice and video in terms of delay and drop sensitivity. Almost all data applications can tolerate some delay and generally can tolerate high drop rates.

Because data traffic can tolerate drops, the retransmit capabilities of TCP become important and, as a result, many data applications use TCP.

In enterprise networks, important (business-critical) applications are usually easy to identify. Most applications can be identified based on TCP or UDP port numbers. Some applications use dynamic port numbers that, to some extent, make classifications more difficult. Cisco IOS software supports network-based application recognition (NBAR), which can be used to recognize dynamic port applications.

Describing VoIP Call Flow

This topic describes a VoIP call flow through a network.



VoIP calls can contend with normal client data for bandwidth. If both the client PC and the VoIP phone are on the same VLAN, each will try to use the available bandwidth without consideration of the other device. To avoid this issue, use two VLANs to allow separation of VoIP and client data. After data is separated, QoS can be applied to prioritize the VoIP traffic as it traverses the network.

A major component of designing a successful IP telephony network is properly provisioning the network bandwidth. The required bandwidth can be calculated by adding the bandwidth requirements for each major application, including voice, video, and data. This sum represents the minimum bandwidth requirement for any given link, and it should not exceed approximately 75 percent of the total available bandwidth for the link.

From a traffic standpoint, an IP telephony call consists of two traffic types:

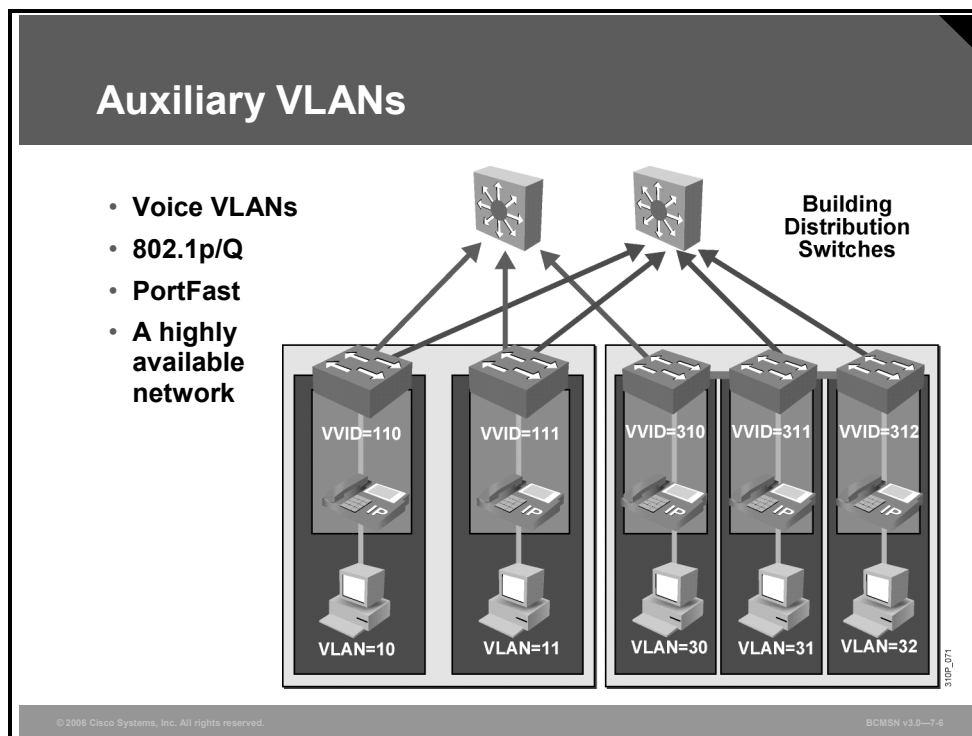
- **Voice carrier stream:** This consists of Real-Time Transport Protocol (RTP) packets that contain the actual voice samples.
- **Call control signaling:** This consists of packets belonging to one of several protocols—those used to set up, to maintain, to tear down, or to redirect a call, depending upon call endpoints. Examples are H.323 or Media Gateway Control Protocol (MGCP).

A VoIP packet consists of the voice payload, IP header, UDP header, RTP header, and Layer 2 link header. The IP header is 20 bytes, the UDP header is 8 bytes, and the RTP header is 12 bytes. The link header varies in size according to the Layer 2 media used; Ethernet requires 14 bytes of header. The voice payload size and the packetization period are device dependent.

Coder-decoders (codecs) are used to convert the analog signal to a digital format. G.711 is a common codec used for normal voice digitization. It is also the only type supported for the Cisco Conference Connection and Personal Assistant applications. G.729 is a codec that provides compression of the voice traffic down to 8 kbps. Cisco VoIP equipment supports these two common codecs, G.711 and G.729, along with several other common industry standards.

Explaining Auxiliary VLANs

This topic explains auxiliary VLANs.



Some Cisco Catalyst switches offer a unique feature called “auxiliary VLAN.” The auxiliary VLAN feature allows you to overlay a voice topology onto a data network. You can segment phones into separate logical networks, even though the data and voice infrastructure are physically the same.

The auxiliary VLAN feature places the phones into their own VLANs without any end-user intervention. Furthermore, these VLAN assignments can be seamlessly maintained, even if the phone is moved to a new location.

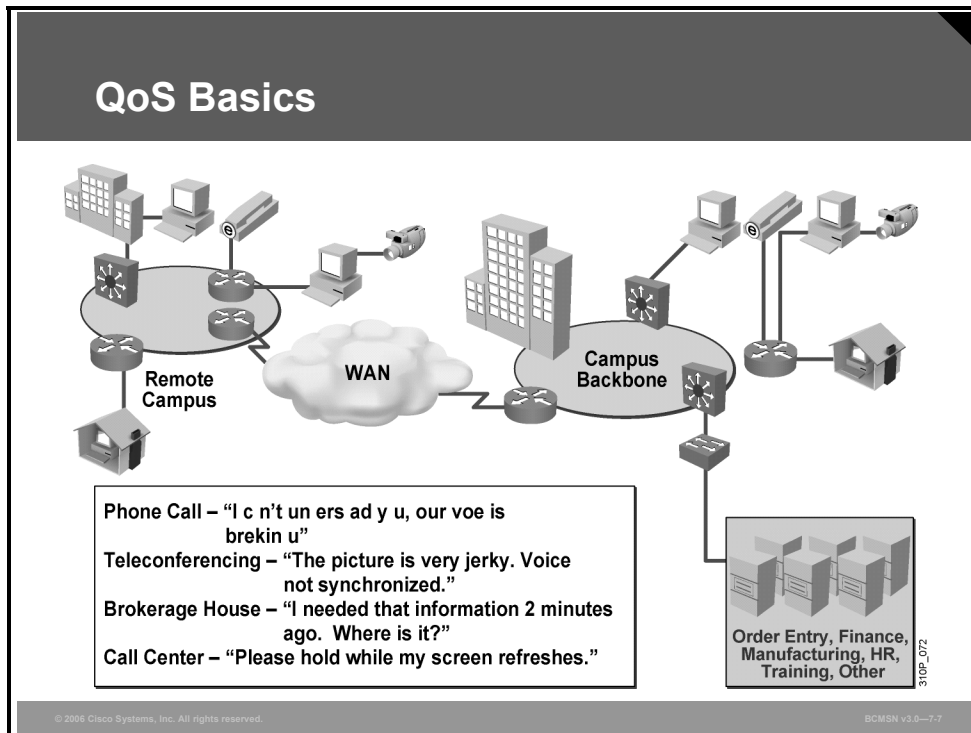
The user simply plugs the phone into the switch, and the switch will provide the phone with the necessary VLAN information. By placing phones into their own VLANs, network administrators gain the advantages of network segmentation and control. Furthermore, network administrators can preserve their existing IP topology for the data end stations. IP phones can be easily assigned to different IP subnets using standards-based DHCP operation.

With the phones in their own IP subnets and VLANs, network administrators can more easily identify and troubleshoot network problems. In addition, network administrators can create and enforce QoS or security policies.

With the auxiliary VLAN feature, Cisco Systems enables network administrators to gain all the advantages of physical infrastructure convergence while maintaining separate logical topologies for voice and data terminals. This creates the most effective way to manage a multiservice network.

Describing QoS

This topic describes the features and attributes of QoS.



Network managers must be prepared for increasing amounts of traffic, requiring more bandwidth than is currently available. This is especially important when dealing with voice traffic. Almost any network can take advantage of QoS for optimum efficiency, whether it is a small corporate network, an Internet service provider, or an enterprise network.

QoS is the application of features and functionality required to actively manage and satisfy the networking requirements of applications that are sensitive to loss, delay, and delay variation (jitter). QoS allows preference to be given to critical application flows for the available bandwidth. QoS tools enable manageability and predictable service for a variety of networked applications and traffic types in a complex network.

The Cisco IOS implementation of QoS software provides these benefits:

- **Priority access to resources:** QoS allows administrators to control which traffic is allowed to access specific network resources such as bandwidth, equipment, and WAN links. Critical traffic may take possession of a resource because the QoS implementation drops low-priority frames.
- **Efficient management of network resources:** If network management and accounting tools indicate that specific traffic is experiencing latency, jitter, and packet loss, then QoS tools can be used to adjust how that traffic is handled.

- **Tailored services:** The control provided by QoS enables Internet service providers to offer carefully tailored grades of service to their customers. For example, a service provider can offer one service level agreement (SLA) to a customer website that receives 3000 to 4000 hits per day and another to a site that receives only 200 to 300 hits per day.
- **Coexistence of mission-critical applications:** QoS technologies ensure that mission-critical business applications receive priority access to network resources while providing adequate processing for applications that are not delay sensitive. Multimedia and voice applications tolerate little latency and require priority access to resources. Other delay-tolerant traffic traversing the same link, such as Simple Mail Transfer Protocol (SMTP) over TCP, can still be adequately serviced.

Explaining the Importance of High Availability for VoIP

The traditional telephony network strives to provide 99.999 percent uptime to the user. This corresponds to 5.25 minutes per year of downtime. Many data networks cannot make the same uptime claim. This topic describes methods that you can use to improve reliability and availability in data networks.

High Availability for VoIP

- **Traditional telephony networks claim 99.999 percent uptime.**
- **Data networks must consider reliability and availability requirements when incorporating voice.**
- **Methods to improve reliability and availability include:**
 - **Redundant hardware**
 - **Redundant links**
 - **UPS**
 - **Proactive network management**

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0—7.8

To provide telephony users the same—or close to the same—level of service as they experience with traditional telephony, the reliability and availability of the data network takes on new importance.

Reliability is a measure of how resilient a network can be. Efforts to ensure reliability may include choosing hardware and software with a low mean time between failure, or installing redundant hardware and links. Availability is a measure of how accessible the network is to the users.

When a user wants to make a call, for example, the network should be accessible to that user at any time a call is required. Efforts to ensure availability may include installing proactive network management to predict failures before they happen and taking steps to correct problems in the design of the network as it grows.

When the data network goes down, it may not come back up for minutes or even hours. This delay is unacceptable for telephony users. Local users with network equipment, such as voice-enabled routers, gateways, or switches for IP phones, now find that their connectivity is terminated. Administrators must, therefore, provide an uninterruptible power supply (UPS) to these devices in addition to providing network availability.

Previously, depending on the type of connection the user had, users received their power directly from the telephone company central office or through a UPS that was connected to their keyswitch or PBX in the event of a power outage. Now the network devices must have protected power to continue to function and provide power to the end devices.

Network reliability comes from incorporating redundancy into the network design. In traditional telephony, switches have multiple redundant connections to other switches. If either a link or a switch becomes unavailable, the telephone company can route the call in different ways. This is why telephone companies can claim a high availability rate.

High availability encompasses many areas of the network. In a fully redundant network, these components need to be duplicated:

- Servers and call managers
- Access layer devices, such as LAN switches
- Distribution layer devices, such as routers or multilayer switches
- Core layer devices, such as multilayer switches
- Interconnections, such as WAN links and PSTN gateways, even through different providers
- Power supplies and UPSs

Example: Cisco Reliability and Availability

In some data networks, a high level of availability and reliability is not critical enough to warrant financing the hardware and links required to provide complete redundancy. If voice is layered onto the network, these requirements need to be revisited.

With Cisco Architecture for Voice, Video and Integrated Data (AVVID) technology, the use of Cisco CallManager clusters provides a way to design redundant hardware in the event of Cisco CallManager failure.

When using gatekeepers, you can configure backup devices as secondary gatekeepers in case the primary gatekeeper fails. You must also revisit the network infrastructure. Redundant devices and Cisco IOS services, such as Hot Standby Router Protocol (HSRP), can provide high availability.

For proactive network monitoring and trouble reporting, a network management platform such as CiscoWorks2000 provides a high degree of responsiveness to network issues.

Explaining Power Requirements in Support of VoIP

This topic discusses power considerations in a voice network.

Power Requirements in Support of VoIP

- **Inline power or power patch panel for IP phones**
 - **May require special modules**
- **UPS and generator backup, with autorestart and monitoring**
- **A 4-hour service-response contract for system problems**
- **Recommended equipment operating temperatures maintained 24/7**

Note: There are several power levels defined for VoIP, ranging from 4.0w to 15.4w, depending on the VoIP phone used.

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0-7.8

Accurate calculations of power requirements are critical for an effective IP telephony solution. Power can be supplied to the IP phones directly from Cisco Catalyst switches with inline power capabilities or by inserting a Cisco Catalyst Inline Power Patch Panel. In addition to IP phones, failover power and total load must be considered for all devices in the IP telephony availability definition, including Building Distribution and Campus Backbone submodules, gateways, Cisco CallManager, and other servers and devices. Power calculations, therefore, must be network-based rather than device-based. As with wireless VoIP, phones are best implemented with Power over Ethernet (PoE).

To provide highly available power protection, you need either a UPS with a minimum battery life to support 1 hour of operation and a 4-hour response for power system failures or a generator with an onsite service contract. This solution must include UPS or generator backup for all devices associated with the IP telephony network. In addition, consider UPS systems that have autorestart capability and a service contract for 4-hour support response.

These are some recommendations for IP telephony high-availability power and environment:

- UPS and generator backup
- UPS systems with autorestart capability
- UPS system monitoring
- A 4-hour service response contract for UPS system problems
- Recommended equipment operating temperatures maintained at all times

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- **Converged networks reduce costs and increase productivity.**
- **VoIP equipment consists of a VoIP phone and a network infrastructure capable of supporting VoIP.**
- **Auxiliary VLANs provide the ability to apply QoS to voice traffic without affecting the flow of data from the client PC.**
- **To ensure high quality VoIP, implementation of QoS is required.**
- **High availability networks must be created to avoid network congestion and overcome a lack of redundancy and poor engineering.**
- **For ease of implementation, most VoIP phones get power through the same cable on which data is sent. This is called “in-line power.”**

Accommodating Voice Traffic on Campus Switches

Overview

VoIP traffic and data will share the same infrastructure. To avoid congestion and subsequent intermittent VoIP communications, quality of service (QoS) must be configured as close to the end device as possible. To accomplish this, QoS trust boundaries must be configured. Several options are available to accomplish this task. This module will provide a brief overview of those options.

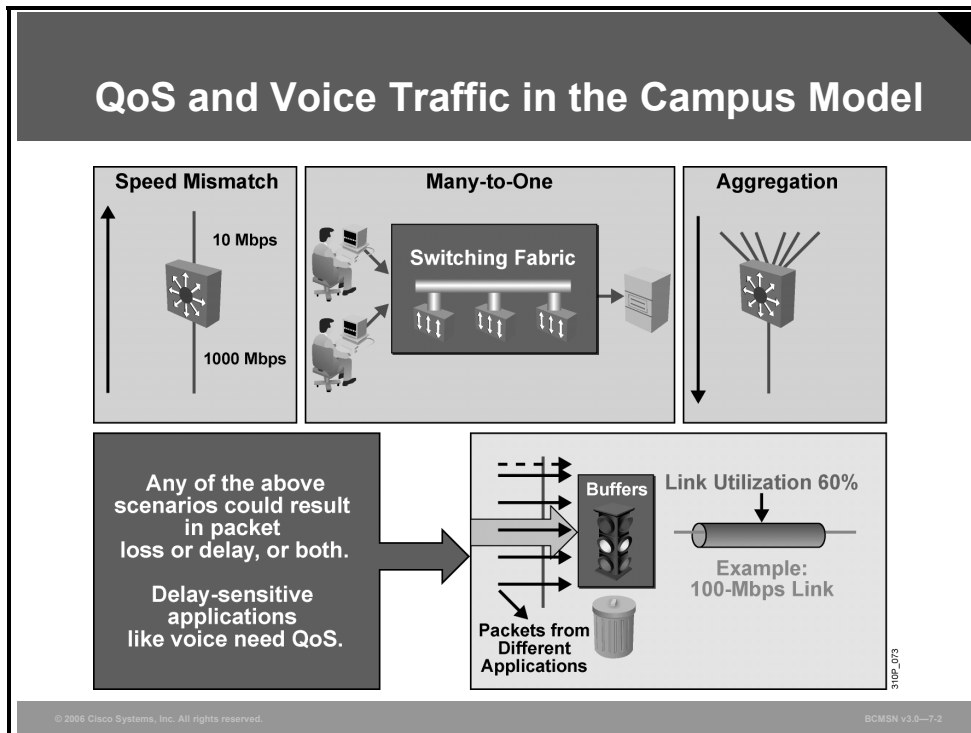
Objectives

Upon completing this lesson, you will be able to explain how to configure switches to support voice traffic. This ability includes being able to meet these objectives:

- Describe how QoS is applied for voice traffic
- Describe LAN-based classification and marking using a Layer 2 Cisco Catalyst workgroup switch
- Describe QoS trust boundaries and their significance in LAN-based classification and marking
- Explain the procedure to configure an access switch for the attachment of a Cisco IP Phone
- Describe basic commands to be considered when voice traffic will traverse a switch
- Explain the use of Cisco AutoQoS in Cisco Catalyst switches
- Describe the commands that enable Cisco AutoQoS on Cisco Catalyst switches

QoS and Voice Traffic in the Campus Model

This topic describes how QoS is applied for voice traffic in the campus model



Regardless of the speed of individual switches or links, speed mismatches, many-to-one switching fabrics, and aggregation may cause a device to experience congestion, which can result in latency. If congestion occurs and congestion management features are not in place, then some packets will be dropped, causing retransmissions that inevitably increase overall network load. QoS can mitigate latency caused by congestion on campus devices.

QoS is implemented by classifying and marking traffic at one device while allowing other devices to prioritize or to queue the traffic according to those marks applied to individual frames or packets. The table lists the campus devices involved in QoS marking or prioritizing.

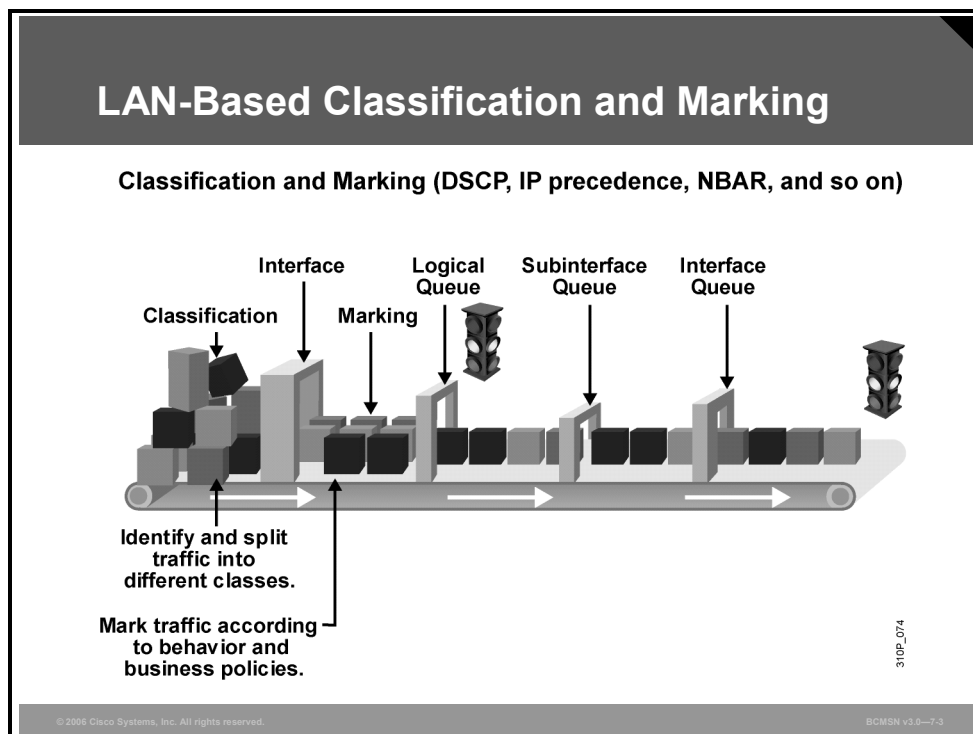
QoS Application in the Campus Network

The table describes how QoS is applied in the campus network.

Campus Device	QoS Application
Access Layer	Initial point at which traffic enters the network. Traffic can be marked (or remarked) at Layers 2 and 3 by the access switch as it enters the network or "trusted" that it is entering the network with an appropriate tag.
Distribution Layer	Marks of traffic inbound from the access layer can be trusted or reset, depending on the ability of the access layer switches. Priority access into the core is provided based on Layer 3 QoS tags.
Core	No traffic marking occurs at the core. Layer 2 or 3 QoS tags are trusted from distribution layer switches and used to prioritize and to queue the traffic as it traverses the core.

LAN-Based Classification and Marking

This topic describes LAN-based classification and marking using a Layer 2 Cisco Catalyst workgroup switch.



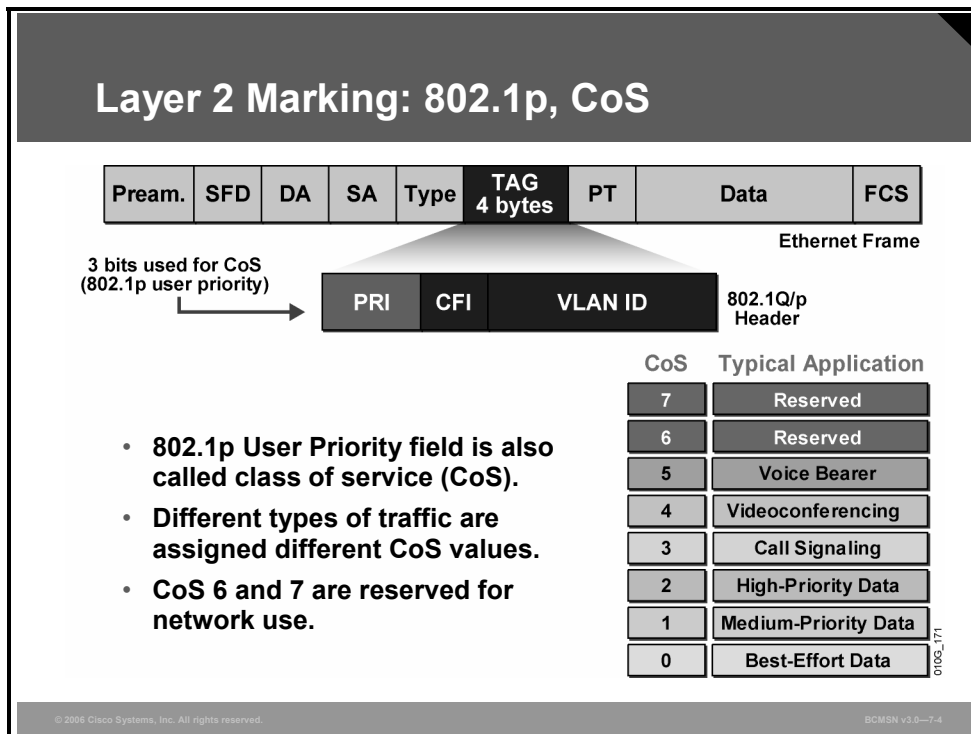
Classification and marking is the process of identifying traffic for proper prioritization as that traffic traverses the network. Traffic is classified by examining information at various layers of the Open Systems Interconnection (OSI) model. All traffic classified in a certain manner will receive an associated mark or QoS value. IP traffic can be classified according to any values configurable in an access control list (ACL) or any of these criteria:

- **Layer 2 parameters:** MAC address, Multiprotocol Label Switching (MPLS), ATM cell loss priority (CLP) bit, Frame Relay discard eligible (DE) bit, ingress interface
- **Layer 3 parameters:** IP precedence, DiffServe Code Point (DSCP), QoS group, IP address, ingress interface
- **Layer 4 parameters:** TCP or User Datagram Protocol (UDP) ports, ingress interface
- **Layer 7 parameters:** Application signatures, ingress interface

All traffic classified or grouped according to these criteria will be marked according to that classification. QoS marks or values establish priority levels or priority classes of service for network traffic as it is processed by each switch. Once traffic is marked with a QoS value, then QoS policies on switches and interfaces will handle traffic according to the values contained in individual frames and packets. As a result of classification and marking, traffic will be prioritized accordingly at each switch to ensure that delay-sensitive traffic receives priority processing as the switch manages congestion, delay, and bandwidth allocation.

Layer 2 QoS Marking

This subtopic describes how QoS values are carried in the Layer 2 header.



QoS Layer 2 classification occurs by examining information in the Ethernet or 802.1Q header, such as destination MAC address or VLAN ID. QoS Layer 2 marking occurs in the Priority field of the 802.1Q header. LAN Layer 2 headers have no means of carrying a QoS value, so 802.1Q encapsulation is required if Layer 2 QoS marking is to occur. The Priority field is 3 bits long and is also known as the 802.1p User Priority or class of service (CoS) value.

This 3-bit field supports CoS values ranging from 1 to 7, 1 being associated with delay-tolerant traffic such as TCP/IP. Voice traffic, which by nature is not delay tolerant, receives higher default CoS values, such as 3 for Call Signaling. A CoS value of 5 is given to voice bearer traffic, which is the phone conversation itself, in which voice quality is impaired if packets are dropped or delayed.

As a result of Layer 2 classification and marking, these QoS operations can occur:

- **Input queue scheduling:** When a frame enters a port, it can be assigned to one of a number of port-based queues before being scheduled for switching to an egress port. Typically, multiple queues are used where traffic requires different service levels.
- **Policing:** Policing is the process of inspecting a frame to see if it has exceeded a predefined rate of traffic within a certain time frame that is typically a fixed number internal to the switch. If a frame is determined to be in excess of the predefined rate limit, it can either be dropped, or the CoS value can be marked down.
- **Output queue scheduling:** The switch will place the frame into an appropriate outbound (egress) queue for switching. The switch will perform buffer management on this queue by ensuring that the buffer does not overflow.

Layer 3 QoS Marking

This subtopic describes QoS information carried in Layer 3 headers.

Layer 3 Marking: IP Precedence, DSCP

Version Length	ToS Byte	Len	ID	Offset	TTL	Proto	FCS	IP SA	IP DA	Data
----------------	----------	-----	----	--------	-----	-------	-----	-------	-------	------

IPv4 Packet

7	6	5	4	3	2	1	0		
IP Precedence			Unused					←	Standard IPv4
DiffServ Code Point (DSCP)			←		Flow Ctrl			←	DiffServ Extensions

- **IPv4**
 - Three most significant bits of ToS byte are called IP precedence.
 - Other bits are unused.
- **DiffServ**
 - Six most significant bits of ToS byte are called DiffServ Code Point (DSCP).
 - DSCP is backward compatible with IP precedence.
 - Remaining two bits are used for flow control.

© 2006 Cisco Systems, Inc. All rights reserved.
BOMSN v3.0—7.6

QoS Layer 3 classification results from the examination of header values such as destination IP address or protocol. QoS Layer 3 marking occurs in the Type of Service (ToS) byte in the IP header. The first three bits of the ToS byte are occupied by IP precedence, which correlates to the three CoS bits carried in the Layer 2 header.

The ToS byte can also be used for DSCP marking. DSCP allows prioritization hop by hop as packets are processed on each switch and interface. The ToS bits are used by DSCP values as shown in the table. The first three DSCP bits, correlating to IP precedence and CoS, identify the DSCP CoS for the packet.

ToS Byte:	P2	P1	P0	T3	T2	T1	T0	Zero
DS Byte:	DS5	DS4	DS3	DS2	DS1	DS0	ECN1	ECN0
	(Class Selector)			(Drop Precedence)				

The next three DSCP bits establish a drop precedence for the packet. Packets with a high DSCP drop precedence value will be dropped before those with a low value if a device or a queue becomes overloaded and must drop packets. Voice traffic will be marked with a low DSCP drop precedence value to minimize voice packet drop.

Each 6-bit DSCP value is also given a DSCP name. DSCP classes 1-4 are Assured Forwarding (AF) classes.

Describing QoS Trust Boundaries

This topic describes QoS trust boundaries.

Classification Tools: Trust Boundaries

1
2
3

- A device is “trusted” if it correctly classifies packets.
- For scalability, classification should be done as close to the edge as possible.
- The outermost trusted devices represent the “trust boundary.”

1 and 2 are optimal; 3 is acceptable (if the access switch cannot perform classification).

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0-7-6

In a campus QoS implementation, boundaries are defined where the existing QoS values that are attached to frames and to packets are to be accepted or altered. These “trust boundaries” are established by configuring trust levels on the ports of key peripheral network devices where QoS policies will be enforced as traffic makes its way into the network. At these boundaries, traffic will be allowed to retain its original QoS marking or will have new marking ascribed as a result of policies associated with its entry point into the network.

Trust boundaries establish a border for traffic entering the campus network. As traffic traverses the switches of the campus network, it is handled and prioritized according to the marks received or trusted when the traffic originally entered the network at the trust boundary.

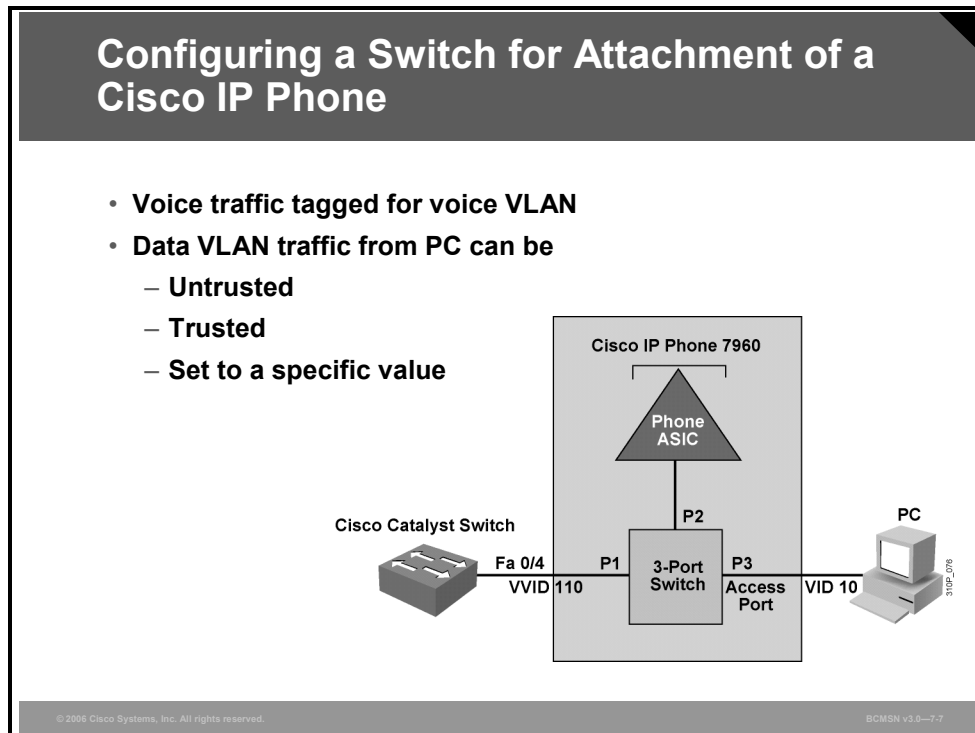
At the trust boundary device, QoS values are trusted if they are considered to accurately represent the type of traffic and precedence processing that the traffic should receive as it enters the campus network.

If untrusted, the traffic is marked with a new QoS value that is appropriate for the policy that is in place at the point where the traffic enters the campus network. Ideally, the trust boundary exists at the first switch that receives traffic from a device or IP phone. It is also acceptable to establish the trust boundary as all the traffic from an access switch enters a Building Distribution layer port.

Note Best practices suggest classifying and marking traffic as close to the traffic source as possible.

Configuring a Switch for Attachment of a Cisco IP Phone

This topic explains the procedure to configure an access switch for the attachment of a Cisco IP Phone.



These commands are used to configure and to verify basic features used to manage voice traffic on Cisco Catalyst switch ports.

Step	Description
1.	Enable voice VLAN on a switch port and associate a VLAN ID. <code>Switch(config-if)# switchport voice vlan vlan-id</code>
2.	Trust the CoS value of frames as they arrive at the switch port. <code>Switch(config-if)# mls qos trust cos</code>
3.	Make this trust conditional on a Cisco IP Phone being attached. <code>Switch(config-if)# mls qos trust device cisco-phone</code> Or Set the CoS value to frames coming from the PC attached to the IP phone. <code>Switch(config-if)# switchport priority extend cos cos_value</code>
3.	Display voice parameters configured on the interface. <code>Switch# show interfaces interface-id switchport</code>
4.	Display QoS parameters configured on the interface. <code>Switch# show mls qos interface interface-id</code>

Describing Basic Switch Commands to Support Attachment of a Cisco IP Phone

This topic describes Cisco Catalyst switch commands associated with attachment of a Cisco IP Phone.

Basic Switch Commands to Support Attachment of a Cisco IP Phone

Configure voice VLAN

- switchport voice vlan 110

Configure trust and CoS options

- mls qos trust cos
- mls qos trust device cisco-phone
- mls qos extend trust
- switchport priority extend cos cos_value

Verify configuration

- show interfaces fa 0/4 switchport
- show mls qos interface fa 0/4

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0—7-8

These commands are used to configure and verify two basic required functions on a switch port connected to an IP phone with a PC connected to that phone.

Example

This example shows configuration of QoS.

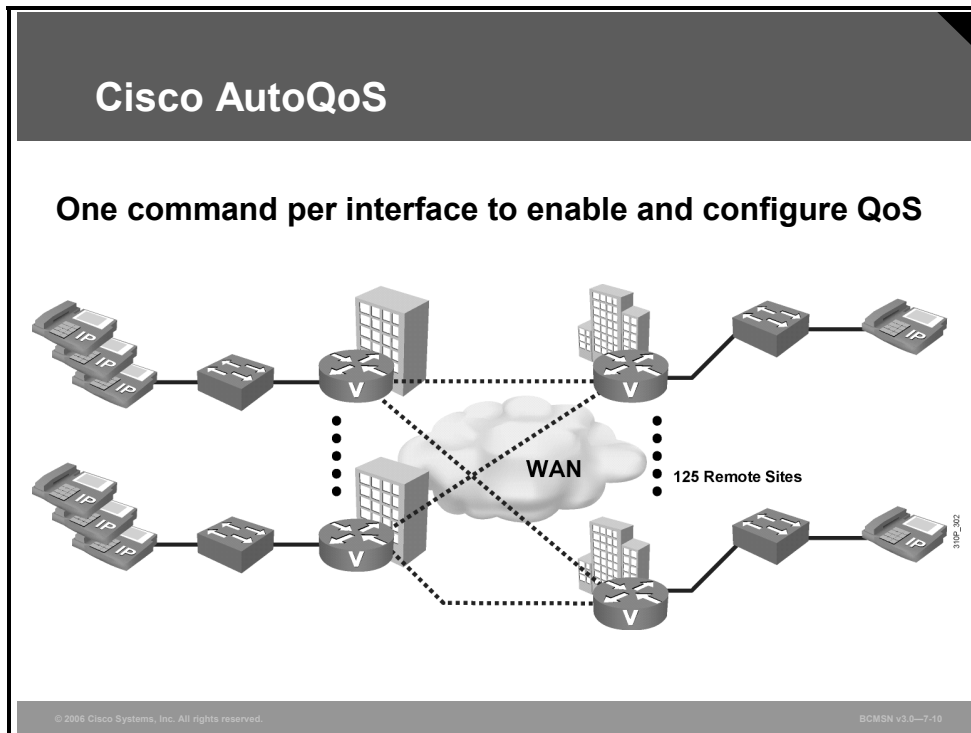
Configuration Example

```
Switch(config)# mls qos
Switch(config)# interface fastethernet 0/4
Switch(config-if)# switchport voice vlan 110
Switch(config-if)# switchport access vlan 10
Switch(config-if)# mls qos trust cos
Switch(config-if)# mls qos trust device cisco-phone
Switch(config-if)# ctrl-Z
Switch# show interfaces fastethernet 0/4

Switch# show mls qos interface fastethernet 0/4
FastEthernet0/4
trust state: trust cos
trust mode: trust cos
COS override: dis
default COS: 0
pass-through: none
trust device: cisco-phone
```

What Is Cisco AutoQoS VoIP?

This topic explains the use of Cisco AutoQoS in Cisco Catalyst switches.



Cisco AutoQoS gives customers the ability to deploy QoS features for converged IP telephony and data networks much more quickly and efficiently. Cisco AutoQoS generates traffic classes and policy map command-line interface (CLI) templates. Cisco AutoQoS simplifies and automates the Modular QoS CLI (MQC) definition of traffic classes and the creation and configuration of traffic policies. Therefore, when Cisco AutoQoS is configured at the interface, the traffic receives the required QoS treatment automatically. In-depth knowledge of the underlying technologies, service policies, link efficiency mechanisms, and Cisco QoS best practice recommendations for voice requirements is not required to configure Cisco AutoQoS.

Cisco AutoQoS can be extremely beneficial for these scenarios:

- Small to medium-sized businesses that must deploy IP telephony quickly but lack the experience and staffing to plan and deploy IP QoS services
- Large customer enterprises that need to deploy Cisco Systems telephony solutions on a large scale, while reducing the costs, complexity, and timeframe for deployment, and ensuring that the appropriate QoS for voice applications is being set in a consistent fashion
- International enterprises or service providers requiring QoS for VoIP where little expertise exists in different regions of the world and where provisioning QoS remotely and across different time zones is difficult
- Service providers requiring a template-driven approach to delivering managed services and QoS for voice traffic to large numbers of customer premise devices

Cisco AutoQoS (Cont.)

- **Application classification**
 - Automatically discovers applications and provides appropriate QoS treatment
- **Policy generation**
 - Automatically generates initial and ongoing QoS policies
- **Configuration**
 - Provides high-level business knobs, and multi-device/domain automation for QoS
- **Monitoring and reporting**
 - Generates intelligent, automatic alerts and summary reports
- **Consistency**
 - Enables automatic, seamless interoperability among all QoS features and parameters across a network topology—LAN, MAN, and WAN



Cisco AutoQoS simplifies and shortens the QoS deployment cycle. Cisco AutoQoS helps in all five major aspects of successful QoS deployments:

- **Application classification:** Cisco AutoQoS leverages intelligent classification on routers using Cisco network-based application recognition (NBAR) to provide deep and stateful packet inspection. Cisco AutoQoS uses Cisco Discovery Protocol (CDP) for voice packets to ensure that the device attached to the LAN is really an IP phone.
- **Policy generation:** Cisco AutoQoS evaluates the network environment and generates an initial policy.

The first release of Cisco AutoQoS provides the necessary Cisco AutoQoS VoIP feature to automate QoS settings for VoIP deployments. This feature automatically generates interface configurations, policy maps, class maps, and ACLs. Cisco AutoQoS VoIP will automatically employ Cisco NBAR to classify voice traffic and mark the traffic with the appropriate DSCP value. Cisco AutoQoS VoIP can be instructed to rely on, or trust, the DSCP markings previously applied to the packets.

- **Configuration:** With one command, Cisco AutoQoS configures the port to prioritize voice traffic without affecting other network traffic, while still offering the flexibility to adjust QoS settings for unique network requirements.

Not only will Cisco AutoQoS automatically detect Cisco IP Phones and enable QoS settings, it will disable the QoS settings to prevent malicious activity when a Cisco IP Phone is relocated or moved.

- **Monitoring and reporting:** Cisco AutoQoS provides visibility into the CoSs deployed via system logging and Simple Network Management Protocol (SNMP) traps, with notification of abnormal events (that is, VoIP packet drops).
- **Consistency:** When deploying QoS configurations using Cisco AutoQoS, the configurations that are generated are consistent among router and switch platforms. This level of consistency ensures seamless QoS operation and interoperability within the network.

Configuring Cisco AutoQoS VoIP on a Cisco Catalyst Switch

This topic describes the commands that enable Cisco AutoQoS on Cisco Catalyst switches.

Configuring Cisco AutoQoS

- **Single command at the interface level configures interface and global QoS.**
 - **Support for Cisco IP Phone and Cisco IP Communicator.**
 - **Support for Cisco IP Communicator currently exists only on the Cisco Catalyst 6500.**
 - **Trust boundary is disabled when Cisco IP Phone is moved.**
 - **Buffer allocation and egress queuing are dependent on interface type (Gigabit Ethernet/Fast Ethernet).**
- **Supported on static, dynamic-access, voice VLAN access, and trunk ports.**
- **CDP must be enabled for Cisco AutoQoS to function properly.**

© 2006 Cisco Systems, Inc. All rights reserved.

BCMSN v3.0—7-12

To configure the QoS settings and the trusted boundary feature on the Cisco IP Phone, CDP version 2 or later must be enabled on the port. If the trusted boundary feature is enabled, a syslog warning message is displayed if CDP is not enabled or if CDP is running version 1.

CDP needs to be enabled for only the **ciscoipphone** QoS configuration; CDP does not affect the other components of the automatic QoS features. When the **ciscoipphone** keyword with the port-specific automatic QoS feature is used, a warning is displayed if the port does not have CDP enabled.

When executing the port-specific automatic QoS command with the **ciscoipphone** keyword but without using the trust option, the trust-device feature is enabled. The trust-device feature is dependent on CDP. If CDP is not enabled or not running version 2, a warning message is displayed, as follows:

```
Console> (enable) set port qos 4/1 autoqos voip ciscoipphone
Warning: CDP is disabled or CDP version 1 is in use. Ensure
that CDP version 2 is enabled globally, and also ensure that
CDP is enabled on the port(s) you wish to configure autoqos
on.
Port 4/1 ingress QoS configured for ciscoipphone.
It is recommended to execute the "set qos autoqos" global
command if not executed previously.
Console> (enable)
```


Configuring Cisco AutoQoS: Cisco Catalyst OS

```
Console> (enable)
```

```
set qos autoqos
```

- **Global configuration command.**
- **All the global QoS settings are applied to all ports in the switch.**
- **Prompt displays the CLI for the port-based automatic QoS commands currently supported.**

```
Console>(enable)set qos autoqos
QoS is enabled
.....
All ingress and egress QoS scheduling parameters configured on all
ports.CoS to DSCP, DSCP to COS, IP Precedence to DSCP and policed
dscp maps configured.
Global QoS configured, port specific autoqos recommended:
set port qos <mod/port> autoqos trust <cos|dscp>
set port qos <mod/port> autoqos voip <ciscoipphone|ciscosoftphone>
```

© 2006 Cisco Systems, Inc. All rights reserved.

BCMSN v3.0--7-13

When the global automatic QoS macro is executed, all the global QoS settings are applied to all ports in the switch. After completion, a prompt will appear, showing the CLI for the port-based automatic QoS commands that are currently supported.

Configuring Cisco AutoQoS: Cisco Catalyst OS (Cont.)

Console> (enable)

```
set port qos <mod/port> autoqos trust [cos|dscp]
```

- **trust dscp and trust cos are automatic QoS keywords used for ports requiring a “trust all” type of solution.**
- **trust dscp should be used only on ports that connect to other switches or known servers because the port will be trusting all inbound traffic marking Layer 3 (DSCP).**
- **trust cos should only be used on ports connecting other switches or known servers because the port trusts all inbound traffic marking in Layer 2 (CoS).**
- **The trusted boundary feature is disabled and no QoS policing is configured on these types of ports.**

© 2006 Cisco Systems, Inc. All rights reserved.

BCMSN v3.0—7-14

The port-specific automatic QoS macro handles all inbound QoS configurations that are specific to a particular port.

The QoS ingress port-specific settings include port trust, default class of service (CoS), classification, and policing, but these settings do not include scheduling. Input scheduling is programmed through the global automatic QoS macro. The port-specific automatic QoS macro, together with the global automatic QoS macro, properly configures all QoS settings for a specific QoS traffic type.

Any existing QoS ACLs that are already associated with a port are removed when Cisco AutoQoS modifies ACL mappings on that port. The ACL names and instances are not changed.

Configuring Cisco AutoQoS: Cisco Catalyst OS (Cont.)

Console> (enable)

```
set port qos <mod/port> autoqos voip [ciscosoftphone |  
ciscoipphone] [trust]
```

ciscosoftphone

- The trusted boundary feature must be disabled for Cisco IP Communicator ports.
- QoS settings must be configured to trust the Layer 3 markings of the traffic that enters the port.
- Only available on Cisco Catalyst 6500.

ciscoipphone

- The port is set up to use trust-cos as well as to enable the trusted boundary feature.
- Combined with the global automatic QoS command, all settings are configured on the switch to properly handle the signaling and voice bearer and PC data entering and leaving the port.
- CDP must be enabled for the ciscoipphone, QoS configuration.

Note: IP Communicator is a softphone, which is an application running on a PC emulating a handset.

© 2006 Cisco Systems, Inc. All rights reserved.

BCMSN v3.0-7-15

The port-specific automatic QoS macro accepts a *mod/port* combination and must include a Cisco Architecture for Voice, Video and Integrated Data (AVVID) type of keyword. The **ciscoipphone**, **ciscosoftphone**, and **trust** keywords are supported.

With the **ciscoipphone** keyword, the port is set up to use **trust-cos** and to enable the trusted boundary feature. Combined with the global automatic QoS command, all settings are configured on the switch to properly handle the signaling, voice bearer, and PC data entering and leaving the port.

In addition to the switch-side QoS settings that are covered by the global automatic QoS command, the IP phone has a few QoS features that need to be configured for proper labeling to occur. QoS configuration information is sent to the IP phone through CDP from the switch. The QoS values that need to be configured are the trust settings of the “PC port” on the IP phone (trusted or untrusted), and the CoS value that is used by the IP phone to remark packets in case the port is untrusted (*ext-cos*).

Cisco IP Communicator is an application that runs on a PC to emulate a phone. This type of application is often referred to as a “soft phone”. Only the Cisco Catalyst 6500 switch supports Cisco AutoQoS for Cisco IP Communicator. On the ports that connect to a PC running Cisco IP Communicator, QoS settings must be configured to trust the Layer 3 markings of the traffic that enters the port.

Trusting all Layer 3 markings is a security risk because PC users could send nonpriority traffic with DSCP 46 and gain unauthorized performance benefits. Although not configured by Cisco AutoQoS, policing on all inbound traffic can be used to prevent malicious users from obtaining unauthorized bandwidth from the network.

Policing is accomplished by rate-limiting the DSCP 46 (Expedited Forwarding [EF]) inbound traffic to the codec rate used by the Cisco IP Communicator application (worst case G.722).

Any traffic that exceeds this rate is marked down to the default traffic rate (DSCP 0 - Best Effort). Signaling traffic (DSCP 24) is also policed and marked down to zero if excess signaling traffic is detected. All other inbound traffic types are reclassified to default traffic (DSCP 0 - Best Effort).

Note You must disable the trusted boundary feature for Cisco IP Communicator ports.

Example: Using the Port-Specific Cisco AutoQoS Macro

This example shows how to use the **ciscoipphone** keyword:

```
Console> (enable) set port qos 3/1 autoqos help  
Usage: set port qos <mod/port> autoqos trust <cos|dscp>  
set port qos <mod/port> autoqos voip  
<ciscoipphone|ciscosoftphone>  
Console> (enable) set port qos 3/1 autoqos voip ciscoipphone  
Port 3/1 ingress QoS configured for Cisco IP Phone.  
It is recommended to execute the "set qos autoqos" global  
command if not executed previously.  
Console> (enable)
```

This example shows how to use the **ciscosoftphone** keyword:

```
Console> (enable) set port qos 3/1 autoqos voip ciscosoftphone  
Port 3/1 ingress QoS configured for Cisco Softphone.  
It is recommended to execute the "set qos autoqos" global  
command if not executed previously.  
Console> (enable)
```

This example shows how to use the **trust cos** keyword:

```
Console> (enable) set port qos 3/1 autoqos trust cos  
Port 3/1 QoS configured to trust all incoming CoS marking.  
It is recommended to execute the "set qos autoqos" global  
command if not executed previously.  
Console> (enable)
```

This example shows how to use the **trust dscp** keyword:

```
Console> (enable) set port qos 3/1 autoqos trust dscp  
Port 3/1 QoS configured to trust all incoming DSCP marking.  
It is recommended to execute the "set qos autoqos" global  
command if not executed previously.  
Console> (enable)
```

Configuring Cisco AutoQoS: Native OS

```
Switch(config-if)#
```

```
auto qos voip trust
```

- The uplink interface is connected to a trusted switch or router, and the VoIP classification in the ingress packet is trusted.

```
Switch(config-if)#
```

```
auto qos voip cisco-phone
```

- Automatically enables the trusted boundary feature, which uses the CDP to detect the presence or absence of a Cisco IP Phone.
- If the interface is connected to a Cisco IP Phone, the QoS labels of incoming packets are trusted only when the Cisco IP Phone is detected.

© 2006 Cisco Systems, Inc. All rights reserved.

BCMSN v3.0-7-16

When the Cisco AutoQoS feature is enabled on the first interface, QoS is globally enabled (**mls qos** global configuration command).

When the **auto qos voip trust** interface configuration command is entered, the ingress classification on the interface is set to trust the CoS QoS label received in the packet, and the egress queues on the interface are reconfigured. QoS labels in ingress packets are trusted.

When the **auto qos voip cisco-phone** interface configuration command is entered, the trusted boundary feature is enabled. The trusted boundary feature uses the CDP to detect the presence or absence of a Cisco IP Phone.

When a Cisco IP Phone is detected, the ingress classification on the interface is set to trust the QoS label received in the packet. When a Cisco IP Phone is absent, the ingress classification is set to not trust the QoS label in the packet. The egress queues on the interface are also reconfigured. This command extends the trust boundary if an IP phone is detected.

Monitoring Cisco AutoQoS

Switch#

```
show auto qos [interface interface-id]
```

- Displays the Cisco AutoQoS configuration that was initially applied
- Does not display any user changes to the configuration that might be in effect

```
Switch#show auto qos
Initial configuration applied by AutoQoS:
wrr-queue bandwidth 20 1 80 0
no wrr-queue cos-map
wrr-queue cos 1 0 1 2 4
wrr-queue cos 3 3 6 7
wrr-queue cos 4 5
mls qos map cos-dscp 0 8 16 26 32 46 48 56
!
interface FastEthernet0/3
mls qos trust device cisco-phone
mls qos trust cos
```

© 2006 Cisco Systems, Inc. All rights reserved.

BCMSN v3.0—7-17

To display the initial Cisco AutoQoS configuration, use the **show auto qos [interface [interface-id]]** privileged EXEC command. To display any user changes to that configuration, use the **show running-config** privileged EXEC command. The **show auto qos** and the **show running-config** command output can be compared to identify the user-defined QoS settings.

Automation with Cisco AutoQoS

This subtopic describes several of the QoS technologies that are automatically implemented on the network when using Cisco AutoQoS.

Automation with Cisco AutoQoS		
DiffServ Function	Cisco IOS/Catalyst Software QoS Feature	Behavior
Classification	NBAR DSCP, Port	Classifies VoIP based on packet attributes or port trust
Marking	Class-based marking	Sets Layer 3/Layer 2 attributes to categorize packets into a class
Congestion Management	Percentage-based LLQ, WRR	Provides EF treatment to voice and best-effort treatment to data

© 2006 Cisco Systems, Inc. All rights reserved. BCM5N v3.0--7-18

Cisco AutoQoS performs these functions in a LAN:

- Enforces the trust boundary on Cisco Catalyst switch access ports, and uplinks and downlinks
- Enables Cisco Catalyst strict priority queuing (PQ) (also known as expedited queuing) with weighted round-robin (WRR) scheduling for voice and data traffic, where appropriate
- Configures queue admission criteria (maps CoS values in incoming packets to the appropriate queues)
- Modifies queue sizes and weights where required

Summary

This topic summarizes the key points discussed in this lesson.

Summary

- **QoS can reduce latency in a campus network when VoIP is configured.**
- **QoS trust boundaries allow for LAN-based classification and marking.**
- **LAN-based classification and marking can be accomplished by a Cisco Catalyst workgroup switch.**
- **Configuration is necessary to implement trust boundaries when VoIP is incorporated.**
- **Specific commands are required when configuring QoS trust boundaries on a Cisco Catalyst switch.**
- **Cisco AutoQoS is a simple way to implement a trust boundary for VoIP.**
- **Configuration of Cisco AutoQoS is simple and supported on Cisco Catalyst switches.**

© 2006 Cisco Systems, Inc. All rights reserved.

BCMSN v3.0—7-19

Module Summary

This topic summarizes the key points that were discussed in this module.

Module Summary

- **Proper planning must take into account all aspects of network engineering when configuring a switch for VoIP.**
- **Using switch-based QoS policies and procedures in a VoIP network will ensure quality and reduce congestion.**

© 2006 Cisco Systems, Inc. All rights reserved. BOMSN v3.0—7-1

When you are implementing a VoIP network into a pre-existing data network, you must address quality of service (QoS), power, and capacity planning considerations. One of the easiest ways to deal with QoS is to implement the Cisco AutoQoS features.

In addition, using auxiliary VLANs and inline power will ease the implementation of the VoIP network. This module highlighted the issues related to implementing a VoIP network, and the initial steps to take to ensure that the VoIP network works correctly.

References

For additional information, refer to these resources:

- Cisco Systems, Inc., IP Telephony/Voice over IP (VoIP): Introduction:
http://www.cisco.com/en/US/tech/tk652/tk701/tsd_technology_support_protocol_home.html
- Cisco Systems, Inc., Gateway Protocols: Troubleshooting and Debugging VoIP Call Basics:
http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a0080094045.shtml
- Cisco Systems, Inc., IP Communications/Voice Solutions: Introduction:
http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/networking_solutions_packages_list.html
- Cisco Systems, Inc., Quality of Service (QoS): Introduction:
http://www.cisco.com/en/US/tech/tk543/tsd_technology_support_category_home.html
- Cisco Systems, Inc., QOS Policing: Introduction:
http://www.cisco.com/en/US/tech/tk543/tk545/tsd_technology_support_protocol_home.html
- Cisco Systems, Inc., QoS Configuration and Monitoring: Introduction:
http://www.cisco.com/en/US/tech/tk543/tk759/tsd_technology_support_protocol_home.html
- Cisco Systems, Inc., QOS Congestion Avoidance: Introduction:
http://www.cisco.com/en/US/tech/tk543/tk760/tsd_technology_support_protocol_home.html

Module Self-Check

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

- Q1) When implementing VoIP, which design consideration is *not* an issue? (Source: Planning for Implementation of Voice in a Campus Network)
- A) Provision switches with inline power.
 - B) Ensure network bandwidth is adequate.
 - C) Determine if 800 number access is required.
 - D) Ensure that the physical plant can support VoIP.
- Q2) When you are installing a VoIP network, which method should you *not* use to improve reliability? (Source: Planning for Implementation of Voice in a Campus Network)
- A) redundant hardware
 - B) 24-hour staffing
 - C) redundant links
 - D) proactive network management
- Q3) Which transport layer protocol does VoIP use? (Source: Planning for Implementation of Voice in a Campus Network)
- A) It uses TCP.
 - B) It uses ICMP.
 - C) It uses UDP.
 - D) It does not use a transport layer protocol; traffic goes directly from IP to the application.
- Q4) What are two ways to accomplish QoS marking? (Choose two.) (Source: Accommodating Voice Traffic on Campus Switches)
- A) using the Type field in the Ethernet header
 - B) using 802.1Q ToS bits
 - C) implementing DSCP at Layer 3
 - D) implementing DSCP at Layer 2
- Q5) In which location can trust boundaries *not* be created? (Source: Accommodating Voice Traffic on Campus Switches)
- A) client's IP phone
 - B) core switch
 - C) access switch
 - D) distribution switch
- Q6) Which protocol allows creating a CoS in the 802.1Q trunking protocol? (Source: Accommodating Voice Traffic on Campus Switches)
- A) ISL
 - B) 802.1p
 - C) 802.1d
 - D) No protocol; CoS is part of 802.1Q

- Q7) What are two ways an IP header can be configured for QoS? (Choose two.) (Source: Accommodating Voice Traffic on Campus Switches)
- A) using IP precedence bits
 - B) using access lists
 - C) using resource reservation code points
 - D) using DSCPs

Module Self-Check Answer Key

- Q1) C
- Q2) B
- Q3) C
- Q4) B, C
- Q5) B
- Q6) B
- Q7) A, D

Minimizing Service Loss and Data Theft in a Campus Network

Overview

This module defines the potential vulnerabilities related to VLANs that can occur within a network. After the vulnerabilities are identified, solutions for each vulnerability are discussed, and configuration commands are defined.

The module also discusses port security for denial of MAC spoofing and MAC flooding, and using private VLANs (PVLANS) and VLAN access control lists (VACLs) to control VLAN traffic. VLAN hopping, DHCP spoofing, Address Resolution Protocol (ARP) spoofing, and Spanning Tree Protocol (STP) attacks are also explained. You will also learn about potential problems, resulting solutions, and the method to secure the switch access with use of vty access control lists (ACLs), and implementing Secure Shell Protocol (SSH) for secure Telnet access.

Objectives

Upon completing this module, you will be able to describe and implement security features in a switched network. This ability includes being able to meet these objectives:

- Explain the vulnerabilities of switches to network attacks
- Configure various features to prevent VLAN hopping and address VLAN security issues
- Explain how to defend against spoof attacks with DAI, DHCP snooping, and IP Source Guard
- Explain how to defend against Layer 2 attacks with STP security mechanisms
- Configure UDLD and loop guard to mitigate the adverse effects that unidirectional links have on spanning tree
- Identify switch security risks and list best practices when placing new switches into service

Understanding Switch Security Issues

Overview

Basic security measures should be taken to guard against a host of attacks that can be launched at a switch and its ports. Specific measures can be taken to guard against MAC flooding, which is a common Layer 2 malicious activity.

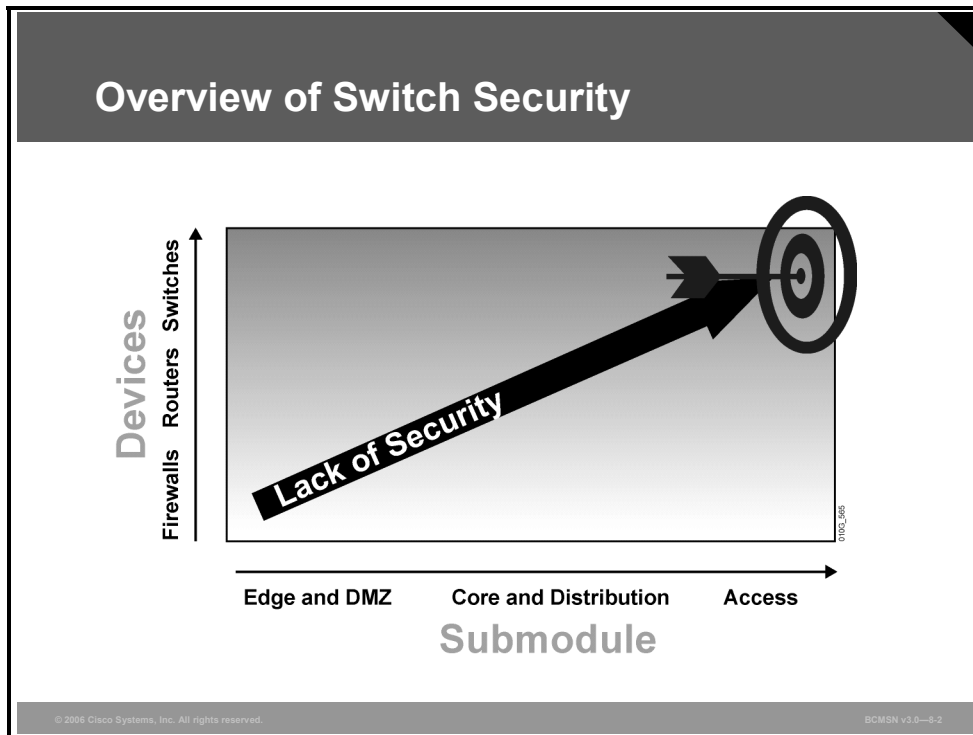
Objectives

Upon completing this lesson, you will be able to describe and implement security features in a switched network. This ability includes being able to meet these objectives:

- Describe switch and Layer 2 security as a subset of an overall network security plan
- Describe how a rogue device gains unauthorized access to a network
- Categorize switch attack types and list mitigation options
- Describe how a MAC flooding attack works to overflow a CAM Campus Backbone Layer table
- Describe how port security is used to block input from devices based upon Layer 2 restrictions
- Describe the procedure to configure port security on a switch
- Explain the sticky MAC option with port security
- Describe security in a multilayer switched network
- Describe the methods that can be used for authentication using AAA
- Describe port-based authentication using 802.1x

Overview of Switch Security Concerns

This topic describes switch and Layer 2 security as a subset of an overall network security plan.



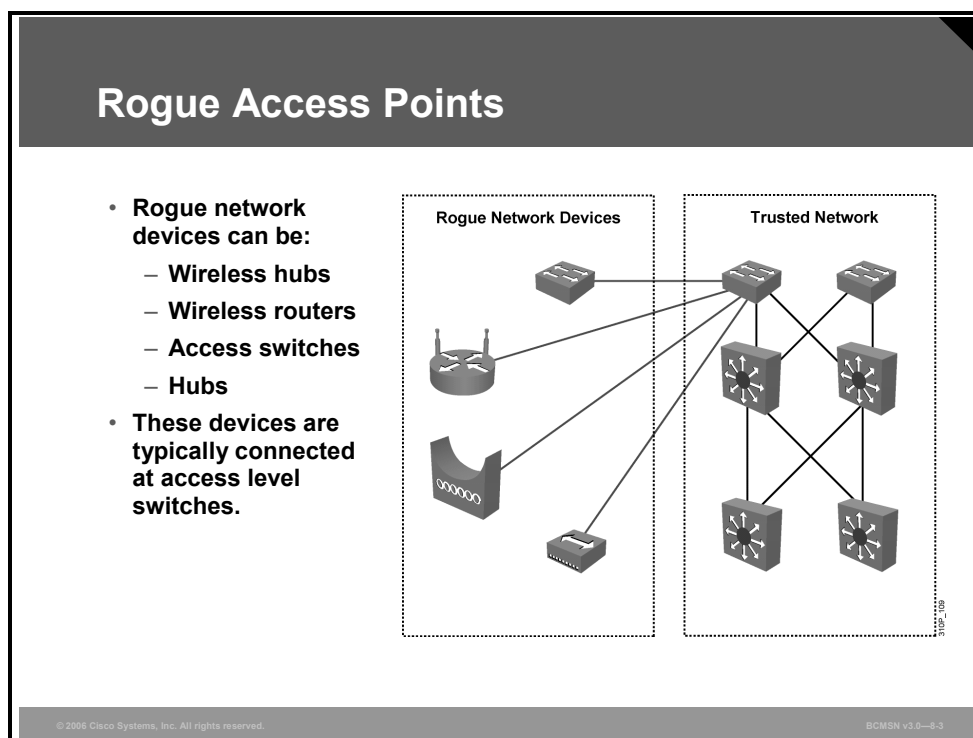
Much industry attention surrounds security attacks from outside the walls of an organization and at the upper Open Systems Interconnection (OSI) layers. Network security often focuses on edge routing devices and the filtering of packets based upon Layer 3 and Layer 4 headers, ports, stateful packet inspection, and so forth. This includes all issues surrounding Layer 3 and above, as traffic makes its way into the campus network from the Internet. Campus access devices and Layer 2 communication are left largely unconsidered in most security discussions.

The default state of networking equipment highlights this focus on external protection and internal open communication. Firewalls, placed at the organizational borders, arrive in a secure operational mode and allow no communication, until configured to do so. Routers and switches that are internal to an organization and designed to accommodate communication, delivering needful campus traffic, have a default operational mode that forwards all traffic unless configured otherwise. Their function as devices that facilitate communication often results in minimal security configuration and renders them targets for malicious attacks. If an attack is launched at Layer 2 on an internal campus device, the rest of the network can be quickly compromised, often without detection.

Many security features are available for switches and routers, but they must be enabled to be effective. As with Layer 3, where security had to be tightened on devices within the campus as malicious activity that compromised this layer increased, now security measures must be taken to guard against malicious activity at Layer 2. A new security focus centers on attacks launched by maliciously leveraging normal Layer 2 switch operations. Security features exist to protect switches and Layer 2 operations. However, as with access control lists (ACLs) for upper-layer security, a policy must be established and appropriate features configured to protect against potential malicious acts while maintaining daily network operations.

Describing Unauthorized Access by Rogue Devices

This topic describes how a rogue device gains unauthorized access to a network.



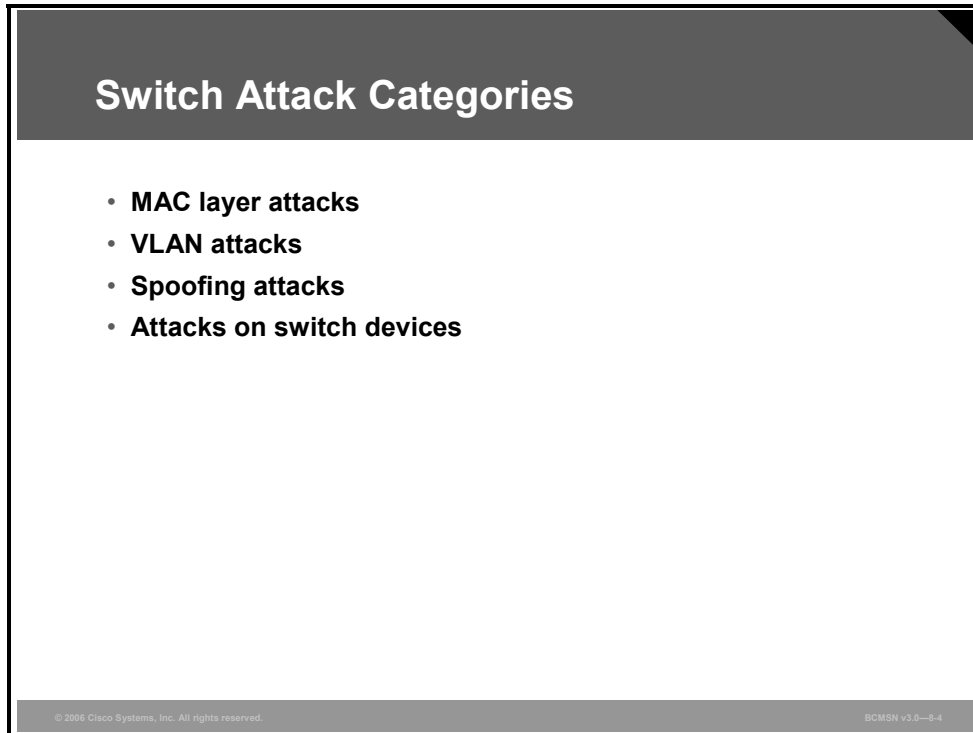
Rogue access comes in several forms. For example, because unauthorized rogue access points are inexpensive and readily available, employees sometimes plug them into existing LANs and build ad hoc wireless networks without IT department knowledge or consent. These rogue access points can be a serious breach of network security because they can be plugged into a network port behind the corporate firewall. Because employees generally do not enable any security settings on the rogue access point, it is easy for unauthorized users to use the access point to intercept network traffic and hijack client sessions.

Malicious rogue access points, although much less common than employee-installed rogue access points, are also a security concern. These rogue access points create an unsecured wireless LAN connection that puts the entire wired network at risk. Malicious rogues present an even greater risk and challenge because they are intentionally hidden from physical and network view.

To mitigate Spanning Tree Protocol (STP) manipulation, use the **root guard** and the **BPDU guard** enhancement commands to enforce the placement of the root bridge in the network and to enforce the STP domain borders. The root guard feature is designed to provide a way to enforce the root bridge placement in the network. The STP bridge protocol data unit (BPDU) guard is designed to allow network designers to keep the active network topology predictable. Although BPDU guard may seem unnecessary, given that the administrator can set the bridge priority to zero, there is still no guarantee that it will be elected as the root bridge because there might be a bridge with priority zero and a lower bridge ID. BPDU guard is best deployed toward user-facing ports to prevent rogue switch-network extensions by an attacker.

Switch Attack Categories

This topic categorizes switch attack types and lists mitigation options.



Switch Attack Categories

- **MAC layer attacks**
- **VLAN attacks**
- **Spoofing attacks**
- **Attacks on switch devices**

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0-3-4

Layer 2 malicious attacks are typically launched by a device that is connected to the campus network. This can be a physical rogue device placed on the network for malicious purposes or an external intrusion that takes control of and launches attacks from a trusted device. In either case, the network sees all traffic as originating from a legitimate connected device.

Attacks launched against switches and at Layer 2 can be grouped as follows:

- MAC layer attacks
- VLAN attacks
- Spoof attacks
- Attacks on switch devices

Significant attacks in these categories, known as of this writing, are discussed in more detail in subsequent sections of the course. Each attack method is accompanied by a standard measure for mitigating the security compromise.

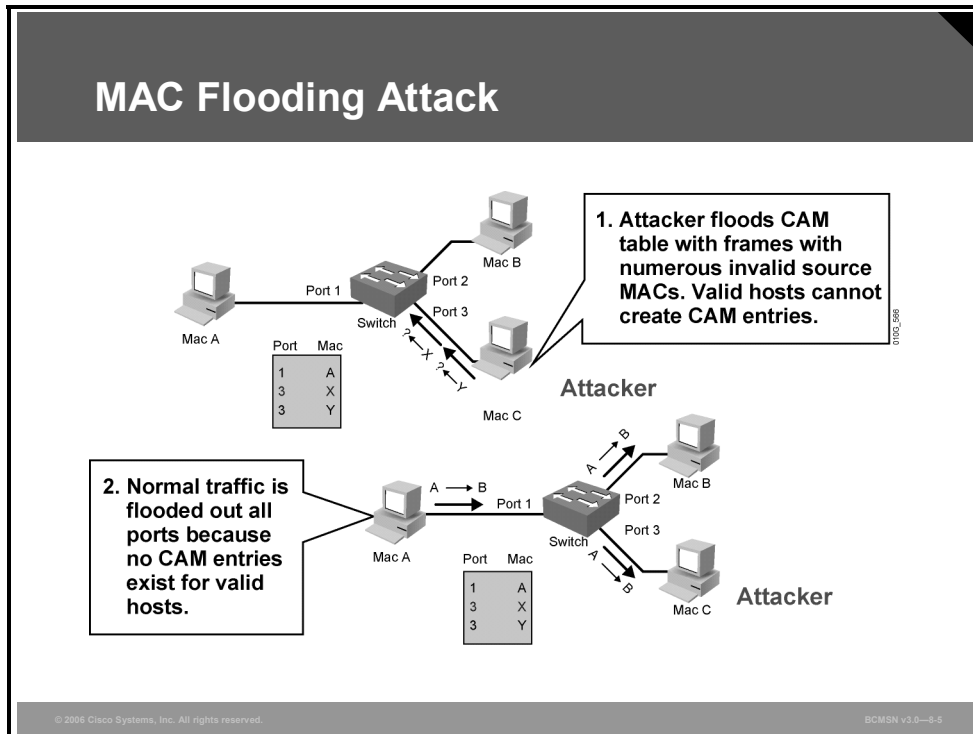
Switch Security Concerns and Mitigation Steps

The table describes attack methods and the steps to mitigation.

Attack Method	Description	Steps to Mitigation
MAC Layer Attacks		
MAC address flooding	Frames with unique, invalid source MAC addresses flood the switch, exhausting content addressable memory (CAM) table space, disallowing new entries from valid hosts. Traffic to valid hosts is subsequently flooded out all ports.	Port security. MAC address VLAN access maps.
VLAN Attacks		
VLAN hopping	By altering the VLAN ID on packets encapsulated for trunking, an attacking device can send or receive packets on various VLANs, bypassing Layer 3 security measures.	Tighten up trunk configurations and the negotiation state of unused ports. Place unused ports in a common VLAN.
Attacks between devices on a common VLAN	Devices may need protection from one another, even though they are on a common VLAN. This is especially true on service-provider segments that support devices from multiple customers.	Implement private VLANs (PVLANS).
Spoofing Attacks		
DHCP starvation and DHCP spoofing	An attacking device can exhaust the address space available to the DHCP servers for a period of time or establish itself as a DHCP server in man-in-the-middle attacks.	Use DHCP snooping.
Spanning tree compromises	Attacking device spoofs the root bridge in the STP topology. If successful, the network attacker can see a variety of frames.	Proactively configure the primary and backup root devices. Enable root guard.
MAC spoofing	Attacking device spoofs the MAC address of a valid host currently in the CAM table. Switch then forwards frames destined for the valid host to the attacking device.	Use DHCP snooping, port security.
Address Resolution Protocol (ARP) spoofing	Attacking device crafts ARP replies intended for valid hosts. The attacking device's MAC address then becomes the destination address found in the Layer 2 frames sent by the valid network device.	Use Dynamic ARP Inspection. DHCP snooping, port security.
Switch Device Attacks		
Cisco Discovery Protocol (CDP) manipulation	Information sent through CDP is transmitted in clear text and unauthenticated, allowing it to be captured and divulge network topology information.	Disable CDP on all ports where it is not intentionally used.
Secure Shell Protocol (SSH) and Telnet attacks	Telnet packets can be read in clear text. SSH is an option but has security issues in version 1.	Use SSH version 2. Use Telnet with vty ACLs.

Describing a MAC Flooding Attack

This topic describes how a MAC flooding attack works to overflow a CAM Campus Backbone Layer table.



A common Layer 2 or switch attack as of this writing is MAC flooding, resulting in a switch's CAM table overflow, which causes flooding of regular data frames out all switch ports. This attack can be launched for the malicious purpose of collecting a broad sample of traffic or as a denial of service (DoS) attack.

A switch's CAM tables are limited in size and therefore can contain only a limited number of entries at any one time. A network intruder can maliciously flood a switch with a large number of frames from a range of invalid source MAC addresses. If enough new entries are made before old ones expire, new valid entries will not be accepted. Then, when traffic arrives at the switch for a legitimate device that is located on one of the switch ports that was not able to create a CAM table entry, the switch must flood frames to that address out all ports. This has two adverse effects:

- The switch traffic forwarding is inefficient and voluminous.
- An intruding device can be connected to any switch port and capture traffic that is not normally seen on that port.

If the attack is launched before the beginning of the day, the CAM table would be full when the majority of devices are powered on. Then frames from those legitimate devices are unable to create CAM table entries as they power on. If this represents a large number of network devices, the number of MAC addresses for which traffic will be flooded will be high, and any switch port will carry flooded frames from a large number of devices.

If the initial flood of invalid CAM table entries is a one-time event, the switch will eventually age out older, invalid CAM table entries, allowing new, legitimate devices to create entries.

Traffic flooding will cease and may never be detected, even though the intruder may have captured a significant amount of data from the network.

As the figure shows, MAC flooding occurs in this progression.

MAC Flooding Attack Progression

The table describes MAC flooding attack progression.

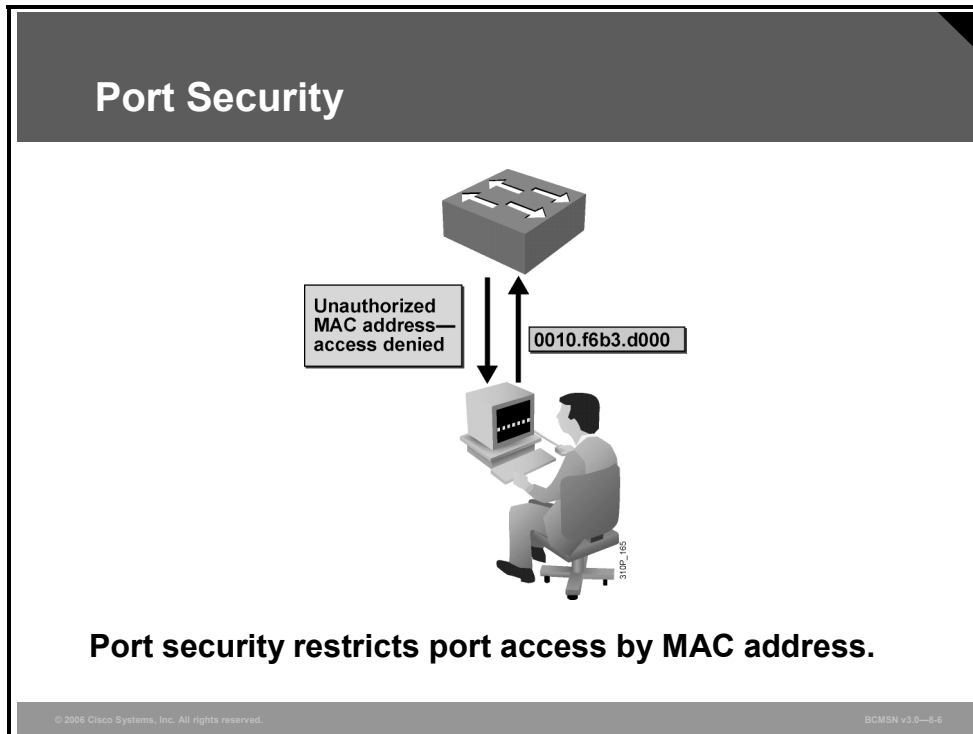
Step	Description
1.	Switch forwards traffic based on valid CAM table entries.
2.	Attacker (MAC address C) sends out multiple packets with various source MAC addresses.
3.	Over a short period of time, the CAM table in the switch fills up until it cannot accept new entries. As long as the attack is running, the CAM table on the switch will remain full.
4.	Switch begins to flood all packets that it receives out of every port so that frames sent from host A to host B are also flooded out of port 3 on the switch.

Suggested Mitigation for MAC Flooding Attacks

Configure port security to define the number of MAC addresses that are allowed on a given port. Port security can also specify what MAC address is allowed on a given port.

Describing Port Security

This topic describes how port security is used to block input from devices based upon Layer 2 restrictions.



Port security is a feature supported on Cisco Catalyst switches that restricts a switch port to a specific set or number of MAC addresses. Those addresses can be learned dynamically or configured statically. The port will then provide access to frames from only those addresses. If, however, the number of addresses is limited to four but no specific MAC addresses are configured, the port will allow any four MAC addresses to be learned dynamically, and port access will be limited to those four dynamically learned addresses.

A port security feature called “sticky learning,” available on some switch platforms, combines the features of dynamically learned and statically configured addresses. When this feature is configured on an interface, the interface converts dynamically learned addresses to “sticky secure” addresses. This adds them to the running configuration as if they were configured using the **switchport port-security mac-address** command.

Scenario

Imagine five individuals whose laptops are allowed to connect to a specific switch port when they visit an area of the building. You want to restrict switch port access to the MAC addresses of those five laptops and allow no addresses to be learned dynamically on that port.

Process

Implementing Port Security

The table describes the process that can achieve the desired results for this scenario.

Step	Action	Notes
1.	Configure port security.	Configure port security to allow only five connections on that port. Configure an entry for each of the five allowed MAC addresses. This, in effect, populates the MAC address table with five entries for that port and allows no additional entries to be learned dynamically.
2.	Allowed frames are processed.	When frames arrive on the switch port, their source MAC address is checked against the MAC address table. If the frame source MAC address matches an entry in the table for that port, the frames are forwarded to the switch to be processed like any other frames on the switch.
3.	New addresses are not allowed to create new MAC address table entries.	When frames with a nonallowed MAC address arrive on the port, the switch determines that the address is not in the current MAC address table and does not create a dynamic entry for that new MAC address because the number of allowed addresses has been limited.
4.	Switch takes action in response to nonallowed frames.	The switch will disallow access to the port and take one of these configuration-dependent actions: (a) the entire switch port can be shut down; (b) access can be denied for that MAC address only and a log error can be generated; (c) access can be denied for that MAC address but without generating a log message.

Note Port security cannot be applied to trunk ports where addresses might change frequently. Implementations of port security vary by Cisco Catalyst platform. Check documentation to see if and how particular hardware supports this feature.

Configuring Port Security on a Switch

This topic explains the procedure to configure port security on a switch.

Configuring Port Security on a Switch

- **Enable port security**
- **Set MAC address limit**
- **Specify allowable MAC addresses**
- **Define violation actions**

```
Switch(config-if)#switchport port-security [maximum value]
violation {protect | restrict | shutdown}
```

- **Enables port security and specifies the maximum number of MAC addresses that can be supported by this port.**

© 2004 Cisco Systems, Inc. All rights reserved. BCMSN v3.0-3-7

Here are the steps to set up port security that will limit switch port access to a finite number and a specific set of end-device MAC addresses.

Port Security Configuration Steps

To configure port security, follow the steps listed in the table.

Step	Description
1.	Enables port security. <pre>Switch(config-if)#switchport port-security</pre>
2.	Sets a maximum number of MAC addresses that will be allowed on this port. Default is one. <pre>Switch(config-if)#switchport port-security maximum value</pre>
3.	Specifies which MAC addresses will be allowed on this port (optional). <pre>Switch(config-if)#switchport port-security mac-address mac-address Switch(config-if)#switchport port-security mac-address mac-address</pre>
4.	Defines what action an interface will take if a nonallowed MAC address attempts access. <pre>Switch(config-if)#switchport port-security violation {shutdown restrict protect}</pre>

Caveats to Port Security Configuration Steps

- Step 1** Port security is enabled on a port-by-port basis.
- Step 2** By default, only one MAC address is allowed access through a given switch port when port security is enabled. This parameter increases that number. It implies no restriction on specific MAC addresses, just on the total number of addresses that can be learned by the port. Learned addresses are not aged out by default but can be configured to do so after a specified time using the **switchport port-security aging** command. The *value* parameter can be any number from 1 to 1024, with some restrictions having to do with the number of ports on a given switch with port security enabled.

Note Be sure to set the *value* parameter to a value of **2** when you are configuring a port to support VoIP with a phone and computer accessible on the port. If the default value is used, a port-security violation will result.

Step 3 Access to the switch port can be restricted to one or more specific MAC addresses. If the number of specific MAC addresses assigned using this command is lower than the *value* parameter set in Step 2, then the remaining allowed addresses can be learned dynamically. If you specify a set of MAC addresses that is equal to the maximum number allowed, access is limited to that set of MAC addresses.

Step 4 By default, if the maximum number of connections is achieved and a new MAC address attempts to access the port, the switch must take one of these actions:

- **Protect:** Frames from the nonallowed address are dropped, but there is no log of the violation.

Note The *protect* argument is platform or version dependent.

- **Restrict:** Frames from the nonallowed address are dropped, a log message is created, and a Simple Network Management Protocol (SNMP) trap is sent.
- **Shut down:** If any frames are seen from a nonallowed address, the interface is errdisabled, a log entry is made, an SNMP trap is sent, and manual intervention or errdisable recovery must be used to make the interface usable.

How to Verify Port Security

This subtopic describes how to verify port security.

Verifying Port Security

```
Switch#show port-security
```

- **Displays security information for all interfaces**

```
Switch#show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security
Action          (Count)        (Count)      (Count)
-----
Fa5/1            11             11           0                  Shutdown
Fa5/5            15             5            0                  Restrict
Fa5/11           5              4            0                  Protect
-----
Total Addresses in System: 21
Max Addresses limit in System: 128
```

© 2006 Cisco Systems, Inc. All rights reserved.BCMSN v3.0-5-5

Use **show** commands to verify the configuration of port security.

Verifying Network Access Security

The **show port-security** command can be used to verify the ports on which port security has been enabled. It also displays count information and security actions to be taken per interface.

The full command syntax is as follows:

```
Switch#show port-security [interface interface_id] address
```

Arguments are provided to view port security status by interface or view the addresses associated with port security on all interfaces.

Example: show port-security Command Output

The example displays output from the **show port-security** command when you enter an interface.

Verifying Port Security (Cont.)

```
Switch#show port-security interface type mod/port
```

- **Displays security information for a specific interface**

```
Switch#show port-security interface fastethernet 5/1

Port Security: Enabled
Port status: SecureUp
Violation mode: Shutdown
Maximum MAC Addresses: 11
Total MAC Addresses: 11
Configured MAC Addresses: 3
Aging time: 20 mins
Aging type: Inactivity
SecureStatic address aging: Enabled
Security Violation count: 0
```

© 2006 Cisco Systems, Inc. All rights reserved.BCMSN v3.0-8.9

Use the *interface* argument to provide output for a specific interface.

Example: show port-security Command for a Specific Interface

The example displays output from the **show port-security** command without a specified interface.

Verifying Port Security (Cont.)

```
Switch#show port-security address
```

- **Displays MAC address table security information**

```
Switch#show port-security address
Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
-----  -
1       0001.0001.0001   SecureDynamic       Fa5/1    15 (I)
1       0001.0001.0002   SecureDynamic       Fa5/1    15 (I)
1       0001.0001.1111   SecureConfigured    Fa5/1    16 (I)
1       0001.0001.1112   SecureConfigured    Fa5/1    -
1       0001.0001.1113   SecureConfigured    Fa5/1    -
1       0005.0005.0001   SecureConfigured    Fa5/5    23
1       0005.0005.0002   SecureConfigured    Fa5/5    23
1       0005.0005.0003   SecureConfigured    Fa5/5    23
1       0011.0011.0001   SecureConfigured    Fa5/11   25 (I)
1       0011.0011.0002   SecureConfigured    Fa5/11   25 (I)
-----
Total Addresses in System: 10
Max Addresses limit in System: 128
```

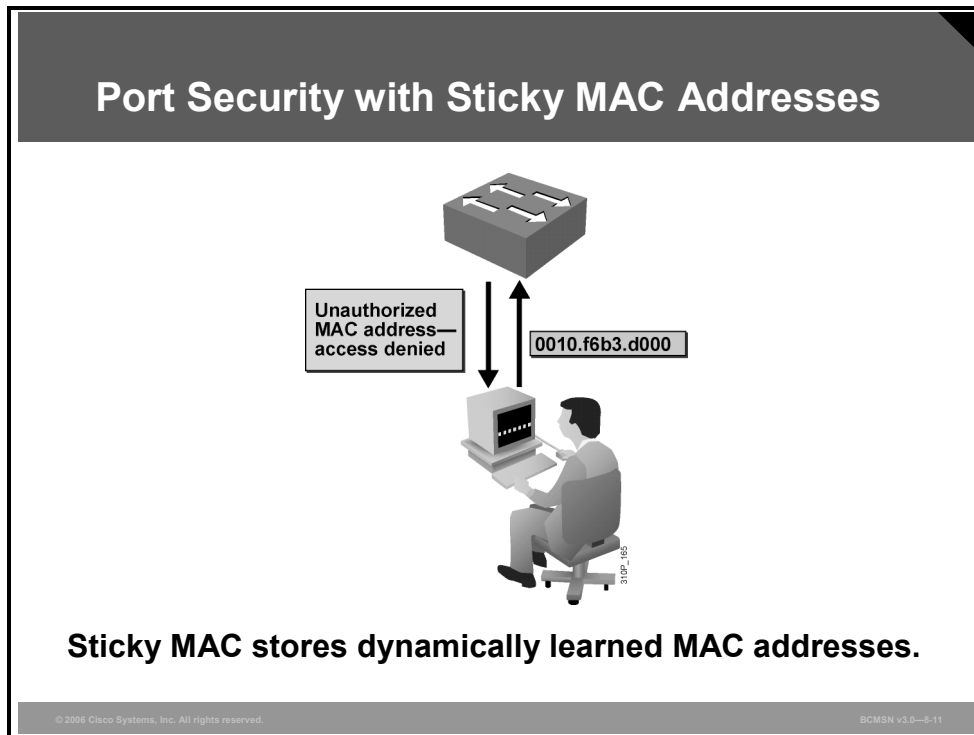
© 2006 Cisco Systems, Inc. All rights reserved.BCMSN v3.0—8-16

Use the *address* argument to display MAC address table security information. The remaining age column will only be populated if specifically configured for a given interface.

The example displays output from the **show port-security address** privileged EXEC command.

Port Security with Sticky MAC Addresses

This topic describes the sticky MAC option with port security.



Port security can be used to mitigate spoof attacks by limiting access through each switch port to a single MAC address. This prevents intruders from using multiple MAC addresses over a short period of time but does not limit port access to a specific MAC address. The most restrictive port security implementation would specify the exact MAC address of the single device that is to gain access through each port. Implementing this level of security, however, requires considerable administrative overhead.

Port security has a feature called “sticky MAC addresses” that can limit switch port access to a single, specific MAC address without the network administrator having to gather the MAC address of every legitimate device and manually associate it with a particular switch port.

When sticky MAC addresses are used, the switch port will convert dynamically learned MAC addresses to sticky MAC addresses and subsequently add them to the running configuration as if they were static entries for a single MAC address to be allowed by port security. Sticky secure MAC addresses will be added to the running configuration but will not become part of the startup configuration file unless the running configuration is copied to the startup configuration after addresses have been learned. If they are saved in the startup configuration, they will not have to be relearned upon switch reboot, and this provides a higher level of network security.

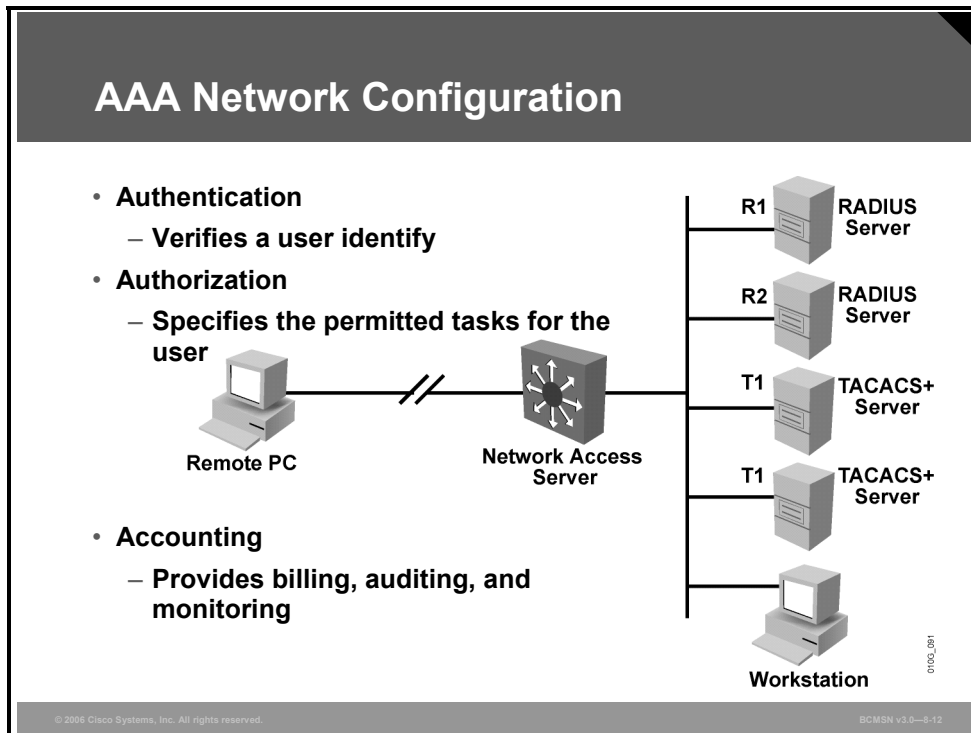
The command that follows will convert all dynamic port-security learned MAC addresses to sticky secure MAC addresses.

```
switchport port-security mac-address sticky
```

This command cannot be used on ports where voice VLANs are configured.

Authentication, Authorization, and Accounting

This topic describes security in a multilayer switched network.



Authentication, authorization, and accounting (AAA) network security services provide the primary framework through which access control is set up on a switch. AAA is an architectural framework for configuring a set of three independent security functions in a consistent manner. AAA provides a modular way of performing these services. For purposes of this course, only authentication will be discussed.

Authentication is the way a user is identified before being allowed access to the network and network services. AAA authentication is configured by defining a list of named authentication methods and then applying that list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they will be performed; it must be applied to a specific interface before any of the defined authentication methods will be performed.

The only exception is the default method list (which is named “default”). The default method list is automatically applied to all interfaces if no other method list is defined. A defined method list overrides the default method list.

In many circumstances, AAA uses protocols such as RADIUS, TACACS+, or 802.1x to administer its security functions. If the switch is acting as a network access server, AAA is the means through which the switch establishes communication between the network access server and the RADIUS, TACACS+, or 802.1x security server.

Authentication and Authorization Methods

This topic describes the methods that can be used for authentication from AAA.

Authentication Methods

```
Switch(config)#aaa authentication login {default |  
list-name} method1 [method2...]
```

- **Creates a local authentication list**

Cisco IOS AAA supports these authentication methods:

- **Enable password**
- **Kerberos 5**
- **Kerberos 5-Telnet authentication**
- **Line password**
- **Local database**
- **Local database with case sensitivity**
- **No authentication**
- **RADIUS**
- **TACACS+**

© 2006 Cisco Systems, Inc. All rights reserved. BCMN v3.0—8-19

The AAA security services facilitate a variety of login authentication methods.

The *list-name* is a character string used to name the list that is being created. The method argument refers to the actual method that the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails.

For example, to specify RADIUS as the default method for user authentication during login, enter this command:

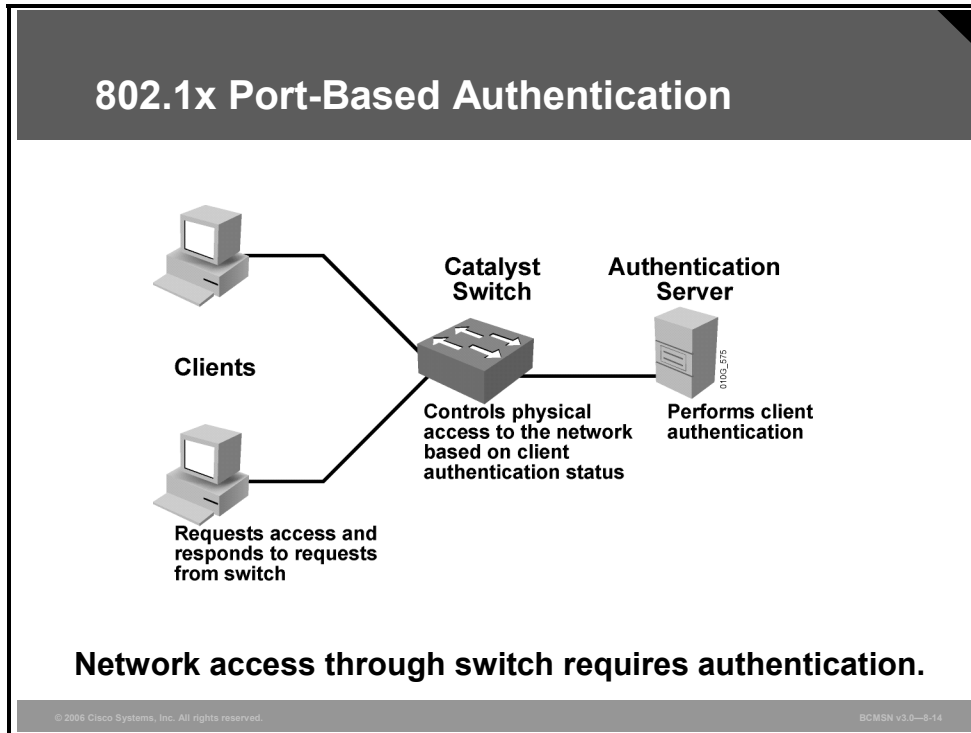
```
aaa authentication dot1x default group radius
```

Basic Process for Configuring AAA

Step	Description
1.	Enable AAA by using the aaa new-model global configuration command.
2.	If a separate security server is used, configure security protocol parameters, such as RADIUS, TACACS+, or Kerberos.
3.	Define the method lists for authentication by using an AAA authentication command.
4.	Apply the method lists to a particular interface or line, if required.

802.1x Port-Based Authentication

This topic describes 802.1x port-based authentication.



The IEEE 802.1x standard defines a port-based access control and authentication protocol that restricts unauthorized workstations from connecting to a LAN through publicly accessible switch ports. The authentication server authenticates each workstation that is connected to a switch port before making available any services offered by the switch or the LAN.

Until the workstation is authenticated, 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the workstation is connected. After authentication succeeds, normal traffic can pass through the port.

With 802.1x port-based authentication, the devices in the network have specific roles, as follows:

- **Client:** The device (workstation) that requests access to the LAN and switch services, and responds to requests from the switch. The workstation must be running 802.1x-compliant client software, such as what is offered in the Microsoft Windows XP operating system. (The port that the client is attached to is the supplicant [client] in the IEEE 802.1x specification.)
- **Authentication server:** Performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch whether or not the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the client. The RADIUS security system with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server.

- **Switch (also called the authenticator):** Controls physical access to the network based on the authentication status of the client. The switch acts as an intermediary (proxy) between the client (supplicant) and the authentication server, requesting identifying information from the client, verifying that information with the authentication server, and relaying a response to the client. The switch uses a RADIUS software agent, which is responsible for encapsulating and decapsulating the EAP frames and interacting with the authentication server.

The switch port state determines whether or not the client is granted access to the network. The port starts in the unauthorized state. While in this state, the port disallows all ingress and egress traffic except for 802.1x protocol packets. When a client is successfully authenticated, the port transitions to the authorized state, allowing all traffic for the client to flow normally.

If the switch requests the client identity (authenticator initiation) and the client does not support 802.1x, the port remains in the unauthorized state, and the client is not granted access to the network.

In contrast, when an 802.1x-enabled client connects to a port and the client initiates the authentication process (supplicant initiation) by sending the EAPOL-start frame to a switch that is not running the 802.1x protocol, no response is received, and the client begins sending frames as if the port is in the authorized state.

You control the port authorization state by using the **dot1x port-control** interface configuration command and these keywords:

- **force-authorized:** Disables 802.1x port-based authentication and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1x-based authentication of the client. This is the default setting.
- **force-unauthorized:** Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface.
- **auto:** Enables 802.1x port-based authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up (authenticator initiation) or when an EAPOL-start frame is received (supplicant initiation). The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. The switch uniquely identifies each client attempting to access the network by using the client MAC address.

If the client is successfully authenticated (receives an “accept” frame from the authentication server), the port state changes to authorized, and all frames from the authenticated client are allowed through the port.

If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the switch can retransmit the request. If no response is received from the server after the specified number of attempts, authentication fails, and network access is not granted.

When a client logs out, it sends an EAPOL-logout message, causing the switch port to transition to the unauthorized state.

Configuring 802.1x Port-Based Authentication

This subtopic describes configuring 802.1x port-based authentication.

Configuring 802.1x

```
Switch(config)#aaa new-model
```

- **Enables AAA**

```
Switch(config)#aaa authentication dot1x {default} method1 [method2...]
```

- **Creates an 802.1x port-based authentication method list**

```
Switch(config)#dot1x system-auth-control
```

- **Globally enables 802.1x port-based authentication**

```
Switch(config)#interface type slot/port
```

- **Enters interface configuration mode**

```
Switch(config-if)#dot1x port-control auto
```

- **Enables 802.1x port-based authentication on the interface**

© 2006 Cisco Systems, Inc. All rights reserved.BCMSN v3.0—6-15

Implementing 802.1x Port-Based Authentication

To implement 802.1x port-based authentication, follow these steps.

Step	Description
1.	Enable AAA. <pre>Switch(config)#aaa new-model</pre>
2.	Create an 802.1x port-based authentication method list. <pre>Switch(config)#aaa authentication dot1x {default} method1 [method2...]</pre>
3.	Globally enable 802.1x port-based authentication. <pre>Switch(config)#dot1x system-auth-control</pre>
4.	Enter interface configuration mode and specify the interface to be enabled for 802.1x port-based authentication. <pre>Switch(config)#interface type slot/port</pre>
5.	Enable 802.1x port-based authentication on the interface. <pre>Switch(config-if)#dot1x port-control auto</pre>
6.	Return to privileged EXEC mode. <pre>Switch(config)#end</pre>

Example

The example shows how to enable AAA and 802.1x on Fast Ethernet port 5/1:

```
Switch#configure terminal
Switch(config)#aaa new-model
Switch(config)#radius-server host 172.120.39.46 auth-port 1812 key rad123
Switch(config)#aaa authentication dot1x default group radius
Switch(config)#dot1x system-auth-control
Switch(config)#interface fastethernet 5/1
Switch(config-if)#dot1x port-control auto
Switch(config-if)#end
```

Summary

This topic summarizes the key points discussed in this lesson.

Summary

- **Layer 2 security measures must be taken as a subset of the overall network security plan.**
- **Rogue access to the network can undermine the security.**
- **Switch attacks fall into four main categories.**
- **MAC flooding attacks are launched against Layer 2 access switches and can overflow the CAM table.**
- **Port security can be configured at Layer 2 to block input from devices.**
- **Configuring port security on a switch is easy and recommended.**
- **Sticky MAC addresses allow port security to limit access to a specific, dynamically learned MAC address.**
- **Multilayer switches should be configured to support security.**
- **AAA can be used for authentication on a multilayer switch.**
- **802.1x port-based authentication can mitigate risk of rogue devices gaining unauthorized access.**

© 2006 Cisco Systems, Inc. All rights reserved.

BCMSN v3.0—8-16

Protecting Against VLAN Attacks

Overview

On networks using trunking protocols, there is a possibility of rogue traffic “hopping” from one VLAN to another, thereby creating security vulnerabilities. These VLAN hopping attacks are best mitigated by close control of trunk links.

Private VLANs (PVLANS) can be configured to establish security regions within a single VLAN without subnetting, and VLAN access control lists (VACLs) can be used to filter traffic within a VLAN.

Objectives

Upon completing this lesson, you will be able to configure various features to prevent VLAN hopping and to address VLAN security issues. This ability includes being able to meet these objectives:

- Describe how VLAN hopping occurs and why it is a security vulnerability
- Explain the procedure to configure a switch to mitigate VLAN hopping attacks
- Describe VACLs and their purpose as part of VLAN security
- Explain the procedure to configure VACLs
- Explain the purpose of a PVLAN
- Explain the procedure to configure PVLANS as a means of network security

Explaining VLAN Hopping

This topic describes how VLAN hopping occurs and why it is a security vulnerability.

Explaining VLAN Hopping

- **Attacking system spoofs itself as a legitimate trunk negotiating device.**
- **Trunk link is negotiated dynamically.**
- **Attacking device gains access to data on all VLANs carried by the negotiated trunk.**

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0-3-2

VLAN hopping is a network attack whereby an end system sends packets to, or collects packets from, a VLAN that should not be accessible to that end system. This is accomplished by tagging the invasive traffic with a specific VLAN ID (VID) or by negotiating a trunk link to send or receive traffic on penetrated VLANs. VLAN hopping can be accomplished by switch spoofing or double tagging.

Switch Spoofing

In a switch spoofing attack, the network attacker configures a system to spoof itself as a switch. The attack emulates Inter-Switch Link (ISL) or 802.1Q signaling along with Dynamic Trunking Protocol (DTP). This is signaling in an attempt to establish a trunk connection to the switch.

Any switch port configured as DTP auto, upon receipt of a DTP packet generated by the attacking device, may become a trunk port and thereby accept traffic destined for any VLAN supported on that trunk. The malicious device can then send packets to, or collect packets from, any VLAN carried on the negotiated trunk.

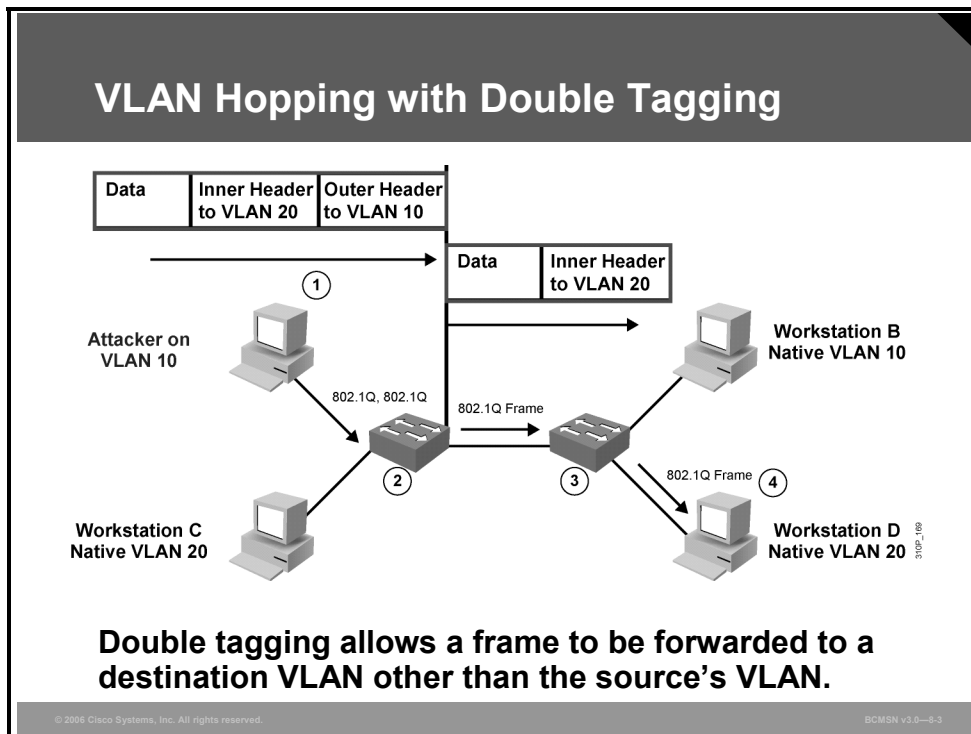
Switch Spoofing Sequence of Events

The table describes the switch spoofing sequence of events.

Step	Description
1.	Attacker gains access to a switch port and sends DTP negotiation frames toward a switch with DTP running and <i>auto</i> negotiation turned on (often, the default settings).
2.	Attacker and switch negotiate trunking over the port.
3.	Switch allows all VLANs (default) to traverse the trunk link.
4.	Attacker sends data to, or collects it from, all VLANs carried on that trunk.

Double Tagging

This subtopic describes double tagging as a means of VLAN hopping.



Another method of VLAN hopping is for any workstation to generate frames with two 802.1Q headers to cause the switch to forward the frames onto a VLAN that would be inaccessible to the attacker through legitimate means.

The first switch to encounter the double-tagged frame strips the first tag off the frame, because the first tag (VLAN 10) matches the trunk port native VLAN, and then forwards the frame out.

The result is that the frame is forwarded, with the inner 802.1Q tag, out all the switch ports, including trunk ports configured with the native VLAN of the network attacker. The second switch then forwards the packet to the destination based on the VLAN ID in the second 802.1Q header. Should the trunk not match the native VLAN of the attacker, the frame would be untagged and flooded to only the original VLAN.

Double-Tagging Method of VLAN Hopping

The table describes the double-tagging method of VLAN hopping.

Step	Description
1.	Workstation A (native VLAN 10) sends a frame with two 802.1Q headers to switch 1.
2.	Switch 1 strips the outer tag and forwards the frame to all ports within same native VLAN.
3.	Switch 2 interprets frame according to information in the inner tag marked with VLAN ID 20.
4.	Switch 2 forwards the frame out all ports associated with VLAN 20, including trunk ports.

Mitigating VLAN Hopping

This topic describes how to mitigate VLAN hopping attacks.

Mitigating VLAN Hopping

```
Switch(config)# interface-range type mod/port-port
```

- **Selects a range of interfaces to configure**

```
Switch(config-if)#switchport mode access
```

- **Configures the ports as access ports and turns off DTP**

```
Switch(config-if)#switchport access vlan vlan-id
```

- **Statically assigns the ports to specific unused VLAN**

© 2006 Cisco Systems, Inc. All rights reserved.BOMSN v3.0—3-4

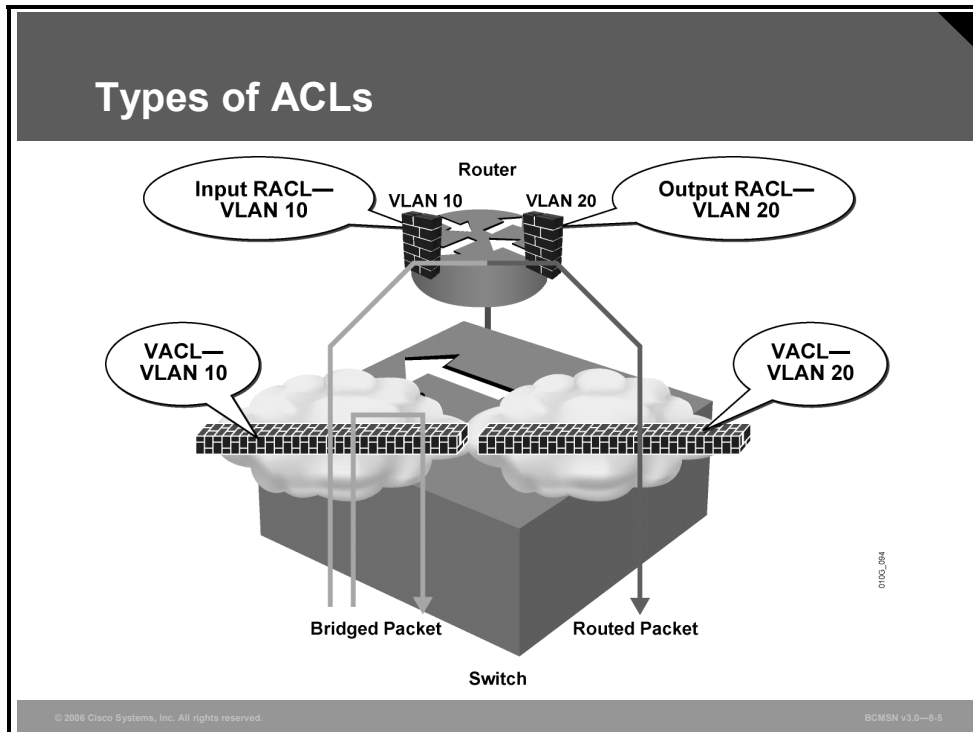
The measures to defend the network from VLAN hopping are a series of best practices for all switch ports and parameters to follow when establishing a trunk port.

- Configure all unused ports as access ports so that trunking cannot be negotiated across those links.
- Place all unused ports in the shutdown state and associate them with a VLAN designed for only unused ports, carrying no user data traffic.
- When establishing a trunk link, purposefully configure arguments so that:
 - The native VLAN will be different from any data VLANs
 - Trunking is set up as “on,” rather than as “negotiated”
 - The specific VLAN range will be carried on the trunk

Note The configuration commands in the figure will not work on access ports that support VoIP because they will be configured as trunk ports. However, on all other access ports, it is best practice to apply these commands to mitigate VLAN hopping.

VLAN Access Control Lists

Access control lists (ACLs) are useful for controlling access in a multilayer switched network. This topic describes VACLs and their purpose as part of VLAN security.



Cisco Systems multilayer switches support three types of ACLs:

- **Router access control lists (RACLs):** Supported in the TCAM hardware on Cisco multilayer switches. In Catalyst switches, RACL can be applied to any routed interface, such as a switch virtual interface (SVI) or Layer 3 routed port.
- **Port access control list (PACL):** Filters traffic at the port level. PACLs can be applied on a Layer 2 switch port, trunk port, or EtherChannel port.
- **VACLs:** Supported in software on Cisco multilayer switches.

Catalyst switches support four ACL lookups per packet: input and output security ACL and input and output quality of service (QoS) ACL.

Catalyst switches use two methods of performing a merge: order independent and order dependent. With order-independent merge, ACLs are transformed from a series of order-dependent actions to a set of order-independent masks and patterns. The resulting access control entry (ACE) can be very large. The merge is processor and memory intensive.

Order-dependent merge is a recent improvement on some Catalyst switches in which ACLs retain their order-dependent aspect. The computation is much faster and is less processor-intensive.

RACLs are supported in hardware through IP standard ACLs and IP extended ACLs, with permit and deny actions. ACL processing is an intrinsic part of the packet forwarding process. ACL entries are programmed in hardware. Lookups occur in the pipeline, whether ACLs are configured or not. With RACLs, access list statistics and logging are not supported.

Configuring VACLs

This topic describes how to configure VACLs.

Configuring VACLs

```
Switch(config)#vlan access-map map_name [seq#]
```

- **Defines a VLAN access map**

```
Switch(config-access-map)# match {ip address {1-199 | 1300-2699 | acl_name} | ipx address {800-999 | acl_name} | mac address acl_name}
```

- **Configures the match clause in a VLAN access map sequence**

```
Switch(config-access-map)#action {drop [log]} | {forward [capture]} | {redirect {type slot/port} | {port-channel channel_id}}
```

- **Configures the action clause in a VLAN access map sequence**

```
Switch(config)#vlan filter map_name vlan_list list
```

- **Applies the VLAN access map to the specified VLANs**

© 2006 Cisco Systems, Inc. All rights reserved. BOMSN v3.0—3.6

VACLs (also called VLAN access maps in Cisco IOS software) apply to all traffic on the VLAN. You can configure VACLs for IP, and MAC-layer traffic.

VACLs follow route-map conventions, in which map sequences are checked in order.

When a matching permit ACE is encountered, the switch takes the action. When a matching deny ACE is encountered, the switch checks the next ACL in the sequence or checks the next sequence.

Three VACL actions are permitted:

- **Permit** (with capture, Catalyst 6500 only)
- **Redirect** (Catalyst 6500 only)
- **Deny** (with logging, Catalyst 6500 only)

The VACL capture option copies traffic to specified capture ports. VACL ACEs installed in hardware are merged with RACLs and other features.

Two features are supported on only the Cisco Catalyst 6500:

- **VACL capture:** Forwarded packets are captured on capture ports. The capture option is on only permit ACEs. The capture port can be an IDS monitor port or any Ethernet port. The capture port must be in an output VLAN for Layer 3 switched traffic.
- **VACL redirect:** Matching packets are redirected to specified ports. You can configure up to five redirect ports. Redirect ports must be in a VLAN where a VACL is applied.

Configuring VACLs

To configure VACLs, complete these steps.

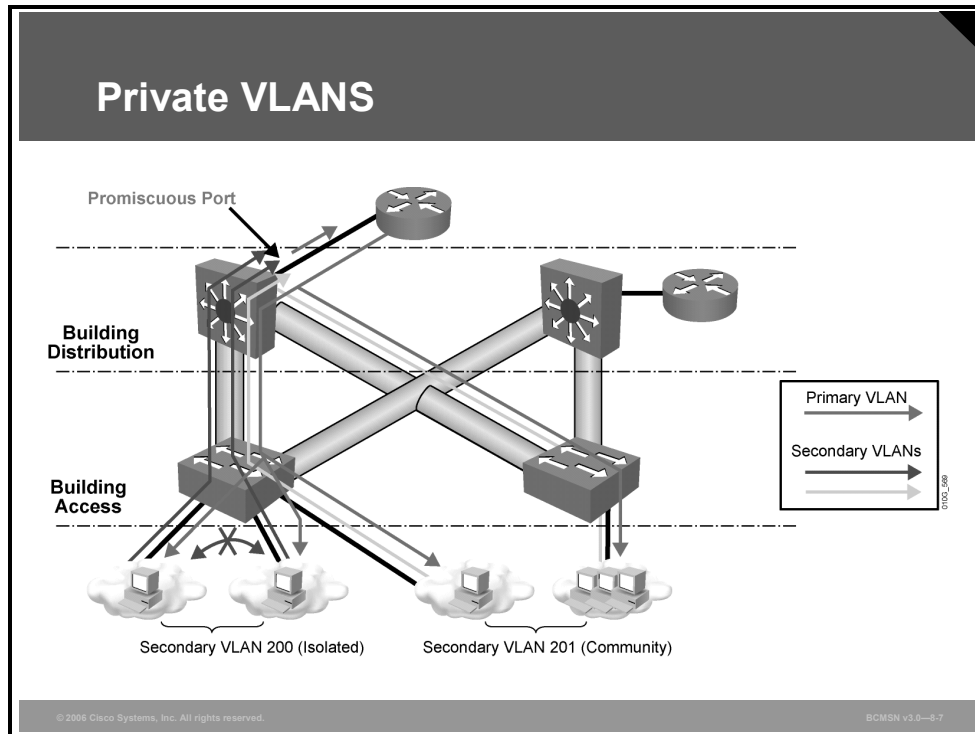
Step	Description
1.	Define a VLAN access map. <code>Switch(config)#vlan access-map map_name [seq#]</code>
2.	Configure a match clause. <code>Switch(config-access-map)#action {drop [log]} {forward [capture]} {redirect {{fastethernet gigabitethernet tengigabitethernet} slot/port} {port-channel channel_id}}</code>
3.	Configure an action clause. <code>Switch(config-access-map)#action {drop [log]} {forward [capture]} {redirect {{fastethernet gigabitethernet tengigabitethernet} slot/port} {port-channel channel_id}}</code>
4.	Apply a map to VLANs. <code>Switch(config)#vlan filter map_name vlan_list list</code>
5.	Verify the VACL configuration. <code>Switch#show vlan access-map map_name</code> <code>Switch#show vlan filter [access-map map_name vlan_id]</code>

```
Switch(config)# vlan access-map PXR1 10
Switch(config)# match ip address 1
Switch(config)# action drop
Switch(config)# vlan access-map PXR1 20
Switch(config)# action forward
Switch(config)#
Switch(config)#vlan filter PXR1vacl vlan_list 1-4094
Switch(config)#
Switch(config)# access-list 1 permit 10.1.0.0 0.0.255.255
```

```
!
vlan access-map PXR1 10
  action drop
  match ip address 1
vlan access-map PXR1 20
  action forward
vlan filter VACL vlan-list 1-4094
vlan internal allocation policy ascending
!
access-list 1 permit 10.1.0.0 0.0.255.255
!
```

Explaining PVLANS

This topic explains the purpose of a PVLAN.



Service providers often have devices from multiple clients, in addition to their own servers, on a single Demilitarized Zone (DMZ) segment or VLAN. As security issues proliferate, it becomes necessary to provide traffic isolation between devices, even though they may exist on the same Layer 3 segment and VLAN. Catalyst 6500/4500 switches implement PVLANS to keep some switch ports shared and some switch ports isolated, although all ports exist on the same VLAN. The 2950 and 3550 support “protected ports,” which are functionality similar to PVLANS on a per-switch basis.

The traditional solution to address these Internet service provider (ISP) requirements is to provide one VLAN per customer, with each VLAN having its own IP subnet. A Layer 3 device then provides interconnectivity between VLANs and Internet destinations.

Here are the challenges with this traditional solution:

- Supporting a separate VLAN per customer may require a high number of interfaces on service provider network devices.
- Spanning tree becomes more complicated with many VLAN iterations.
- Network address space must be divided into many subnets, which wastes space and increases management complexity.
- Multiple ACL applications are required to maintain security on multiple VLANs, resulting in increased management complexity.

PVLANS provide Layer 2 isolation between ports within the same VLAN. This isolation eliminates the need for a separate VLAN and IP subnet per customer.

PVLAN Port Types

This subtopic discusses PVLAN port types.

PVLAN Port Types

- **Isolated:** Communicate with only promiscuous ports
- **Promiscuous:** Communicate with all other ports
- **Community:** Communicate with other members of community and all promiscuous ports

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0—8

A port in a PVLAN can be one of three types:

- **Isolated:** An isolated port has complete Layer 2 separation from other ports within the same PVLAN, except for the promiscuous port. PVLANS block all traffic to isolated ports, except the traffic from promiscuous ports. Traffic received from an isolated port is forwarded to only promiscuous ports.
- **Promiscuous:** A promiscuous port can communicate with all ports within the PVLAN, including the community and isolated ports. The default gateway for the segment would likely be hosted on a promiscuous port, given that all devices in the PVLAN will need to communicate with that port.
- **Community:** Community ports communicate among themselves and with their promiscuous ports. These interfaces are isolated at Layer 2 from all other interfaces in other communities, or in isolated ports within their PVLAN.

Note Because trunks can support the VLANs carrying traffic between isolated, community, and promiscuous ports, isolated and community port traffic might enter or leave the switch through a trunk interface.

PVLAN ports are associated with a set of supporting VLANs that are used to create the PVLAN structure. A PVLAN uses VLANs in three ways:

- **As a primary VLAN:** Carries traffic from promiscuous ports to isolated, community, and other promiscuous ports in the same primary VLAN.
- **As an isolated VLAN:** Carries traffic from isolated ports to a promiscuous port.
- **As a community VLAN:** Carries traffic between community ports and to promiscuous ports. You can configure multiple community VLANs in a PVLAN.

Isolated and community VLANs are called secondary VLANs. You can extend PVLANS across multiple devices by trunking the primary, isolated, and community VLANs to other devices that support PVLANS.

Note A promiscuous port can service only one primary VLAN. A promiscuous port can service one isolated VLAN or many community VLANs.

With a promiscuous port, you can connect a wide range of devices as access points to a PVLAN. For example, you can connect a promiscuous port to the server port to connect an isolated VLAN or a number of community VLANs to the server.

You can use a load balancer to load balance the servers present in the isolated or community VLANs, or you can use a promiscuous port to monitor or back up all the PVLAN servers from an administration workstation.

Configuring PVLANS

This topic explains the procedure to configure PVLANS as a means of network security.

Configuring PVLANS

```
Switch(config-vlan)#private-vlan [primary | isolated | community]
```

- **Configures a VLAN as a PVLAN**

```
Switch(config-vlan)#private-vlan association {secondary_vlan_list | add svl | remove svl}
```

- **Associates secondary VLANs with the primary VLAN**

```
Switch#show vlan private-vlan type
```

- **Verifies PVLAN configuration**

© 2004 Cisco Systems, Inc. All rights reserved.BCMSN v3.0-3-9

To configure a PVLAN, follow these steps.

Step 1 Set VTP mode to transparent.

Step 2 Create the secondary VLANs.

Note Isolated and community VLANs are secondary VLANs.

Step 3 Create the primary VLAN.

Step 4 Associate the secondary VLAN with the primary VLAN. Only one isolated VLAN can be mapped to a primary VLAN, but more than one community VLAN can be mapped to a primary VLAN.

Step 5 Configure an interface as an isolated or community port.

Step 6 Associate the isolated port or community port with the primary-secondary VLAN pair.

Step 7 Configure an interface as a promiscuous port.

Step 8 Map the promiscuous port to the primary-secondary VLAN pair.

Use these commands to configure a VLAN as a PVLAN:

```
Switch(config)#vlan vlan_ID  
Switch(config-vlan)#[no] private-vlan {isolated | primary}
```

Example: PVLAN Configurations

This example shows how to configure VLAN202 as a primary VLAN and verify the configuration:

```
Switch#configure terminal
Switch(config)#vlan 202
Switch(config-vlan)#private-vlan primary
Switch(config-vlan)#end
Switch#show vlan private-vlan type
```

Primary	Secondary	Type	Interfaces
202		primary	

This example shows how to configure VLAN200 as an isolated VLAN and verify the configuration:

```
Switch#configure terminal
Switch(config)#vlan 200
Switch(config-vlan)#private-vlan isolated
Switch(config-vlan)#end
Switch#show vlan private-vlan type
```

Primary	Secondary	Type	Interfaces
202		primary	
200		isolated	

To associate secondary VLANs with a primary VLAN, perform this procedure:

```
Switch(config)#vlan primary_vlan_ID
Switch(config-vlan)#[no] private-vlan association {secondary_vlan_list
| add secondary_vlan_list | remove secondary_vlan_list}
```

When you associate secondary VLANs with a primary VLAN, attempt to use these advisable practices:

- Make sure that the *secondary_vlan_list* parameter contains only one isolated VID.
- Use the **remove** keyword with the *secondary_vlan_list* variable to clear the association between the secondary VLAN and the primary VLAN. The list can contain only one VLAN.
- Use the **no** keyword to clear all associations from the primary VLAN.
- Do not allow the command to take effect until you exit VLAN configuration submode.

Configuring PVLAN Ports

```
Switch(config-if)#switchport mode private-vlan {host |  
promiscuous}
```

- Configures an interface as a PVLAN port

```
Switch(config-if)#switchport private-vlan host-association  
{primary_vlan_ID secondary_vlan_ID}
```

- Associates an isolated or community port with a PVLAN

```
Switch(config-if)#private-vlan mapping primary_vlan_ID  
{secondary_vlan_list | add svl | remove svl}
```

- Maps a promiscuous PVLAN port to a PVLAN

```
Switch#show interfaces private-vlan mapping
```

- Verifies PVLAN port configuration

© 2006 Cisco Systems, Inc. All rights reserved.

BCMSN v3.0—8-10

To configure a Layer 2 interface as a PVLAN promiscuous port, perform this procedure:

```
Switch(config)#interface {fastethernet | gigabitethernet}  
slot/port  
Switch(config-if)#switchport mode private-vlan {host |  
promiscuous}  
Switch(config-if)#[no] switchport private-vlan mapping  
primary_vlan_ID {secondary_vlan_list | add secondary_vlan_list  
| remove secondary_vlan_list}
```

Here are best practices to consider when you configure a Layer 2 interface as a PVLAN promiscuous port:

- The *secondary_vlan_list* parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single PVLAN ID or a hyphenated range of PVLAN IDs.
- Enter a *secondary_vlan_list* or use the **add** keyword with a *secondary_vlan_list* to map the secondary VLANs to the PVLAN promiscuous port.
- Use the **remove** keyword with a *secondary_vlan_list* to clear the mapping between secondary VLANs and the PVLAN promiscuous port.
- Use the **no** keyword to clear all mapping from the PVLAN promiscuous port.

Example: Configuring PVLAN Ports

This example shows how to configure interface FastEthernet 5/2 as a PVLAN promiscuous port, map it to a PVLAN, and verify the configuration:

```
Switch#configure terminal
Switch(config)#interface fastethernet 5/2
Switch(config-if)#switchport mode private-vlan promiscuous
Switch(config-if)#switchport private-vlan mapping 202 440
Switch(config-if)#end
Switch#show interfaces fastethernet 5/2 switchport
Name: Fa5/2
Switchport: Enabled

Administrative Mode: private-vlan promiscuous
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative private-vlan host-association: none
((Inactive))

Administrative private-vlan mapping: 202 (VLAN0202) 440
(VLAN0440)

Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
```

To configure a Layer 2 interface as a PVLAN host port, perform this procedure:

```
Switch(config)#interface {fastethernet | gigabitethernet}
slot/port
Switch(config-if)#switchport mode private-vlan {host |
promiscuous}
Switch(config-if)#[no] switchport private-vlan host-
association primary_vlan_ID secondary_vlan_ID
```

This example shows how to configure interface FastEthernet 5/1 as a PVLAN host port and verify the configuration:

```
Switch#configure terminal
Switch(config)#interface fastethernet 5/1
Switch(config-if)#switchport mode private-vlan host
Switch(config-if)#switchport private-vlan host-association 202
440
Switch(config-if)#end
Switch#show interfaces fastethernet 5/1 switchport
Name: Fa5/1
Switchport: Enabled

Administrative Mode: private-vlan host
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)

Administrative private-vlan host-association: 202 (VLAN0202)
```

Administrative private-vlan mapping: none

Operational private-vlan: none

Trunking VLANs Enabled: ALL

Pruning VLANs Enabled: 2-1001

Capture Mode Disabled

To permit routing of secondary VLAN ingress traffic, perform this procedure:

```
Switch(config)#interface vlan primary_vlan_ID
Switch(config-if)#[no] private-vlan mapping primary_vlan_ID
{secondary_vlan_list | add secondary_vlan_list | remove
secondary_vlan_list}
```

When you permit routing on the secondary VLAN ingress traffic, note the following:

- Enter a value for the *secondary_vlan_list* variable or use the **add** keyword with the *secondary_vlan_list* variable to map the secondary VLANs to the primary VLAN.
- Use the **remove** keyword with the *secondary_vlan_list* variable to clear the mapping between secondary VLANs and the primary VLAN.
- Use the **no** keyword to clear all mapping from the primary VLAN.

Example: Permitting Routing of Secondary VLAN Ingress Traffic

This example shows how to permit routing of secondary VLAN ingress traffic from PVLAN440 and verify the configuration:

```
Switch#configure terminal
Switch(config)#interface vlan 202
Switch(config-if)#private-vlan mapping add 440
Switch(config-if)#end
Switch#show interfaces private-vlan mapping
Interface Secondary VLAN Type
-----
vlan202      440                isolated
```

Summary

This topic summarizes the key points discussed in this lesson.

Summary

- **VLAN hopping can allow Layer 2 unauthorized access to another VLAN.**
- **VLAN hopping can be mitigated by:**
 - **Properly configuring 802.1Q trunks**
 - **Turning off trunk negotiation**
- **Access lists can be applied to VLANs to limit Layer 2 access.**
- **VACLs can be configured on Cisco Catalyst switches.**
- **PVLANS are configured to allow traffic flows to be restricted between ports within the same VLAN.**
- **PVLAN configurations can be applied to provide Layer 2 isolation between VLANS.**

Protecting Against Spoof Attacks

Overview

DHCP, MAC, and Address Resolution Protocol (ARP) spoofing are all methods used to gain unauthorized access to a network or to redirect traffic for malicious purposes. DHCP snooping, port security, and dynamic ARP inspection (DAI) can be configured to guard against these threats.

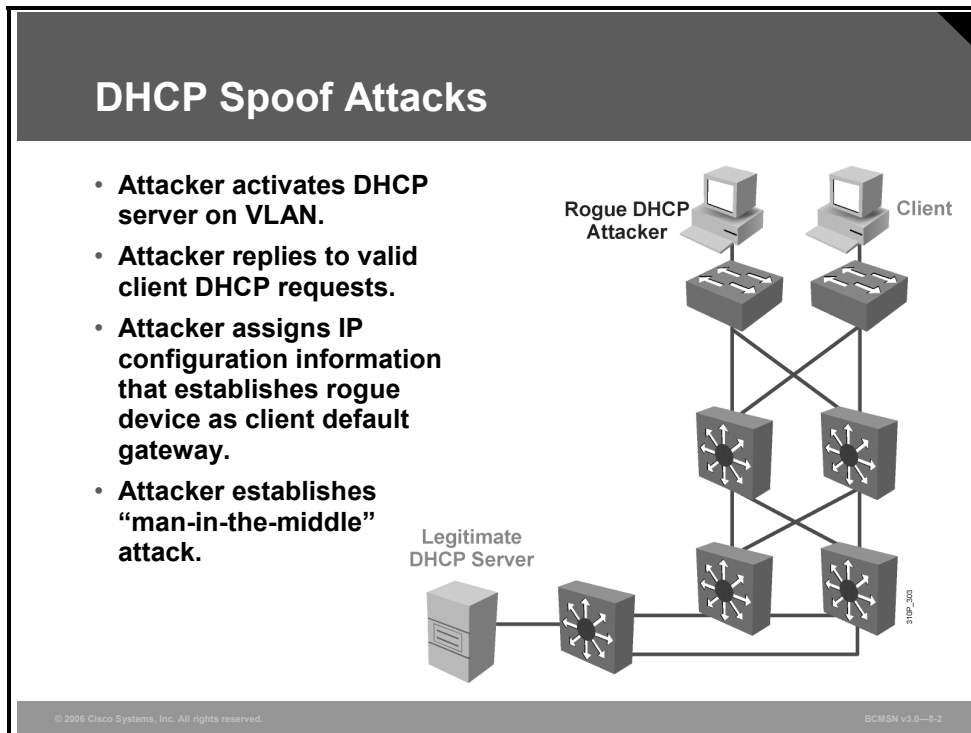
Objectives

Upon completing this lesson, you will be able to explain how to defend against spoof attacks with DAI, DHCP snooping, and IP Source Guard. This ability includes being able to meet these objectives:

- Describe what happens in a network during a DHCP spoof attack
- Describe how the DHCP snooping feature provides security by filtering trusted DHCP messages and then using these messages to build and maintain a DHCP snooping binding table
- Explain the procedure to configure DHCP snooping and IP Source Guard
- Describe what happens in a network during an attack using ARP spoofing
- Describe how DAI determines the validity of an ARP packet based on the valid MAC address to IP address bindings stored in a DHCP snooping database
- Describe the commands that can be used to configure DAI
- Explain the procedure to protect a network from ARP spoofing attacks

Describing a DHCP Spoof Attack

This topic describes what happens in a network during a DHCP spoof attack.



One of the ways that an attacker can gain access to network traffic is to spoof responses that would be sent by a valid DHCP server. The DHCP spoofing device replies to client DHCP requests. The legitimate server may reply also, but if the spoofing device is on the same segment as the client, its reply to the client may arrive first.

The intruder’s DHCP reply offers an IP address and supporting information that designates the intruder as the default gateway or Domain Name System (DNS) server. In the case of a gateway, the clients will then forward packets to the attacking device, which will in turn send them to the desired destination. This is referred to as a “man-in-the-middle” attack, and it may go entirely undetected as the intruder intercepts the data flow through the network.

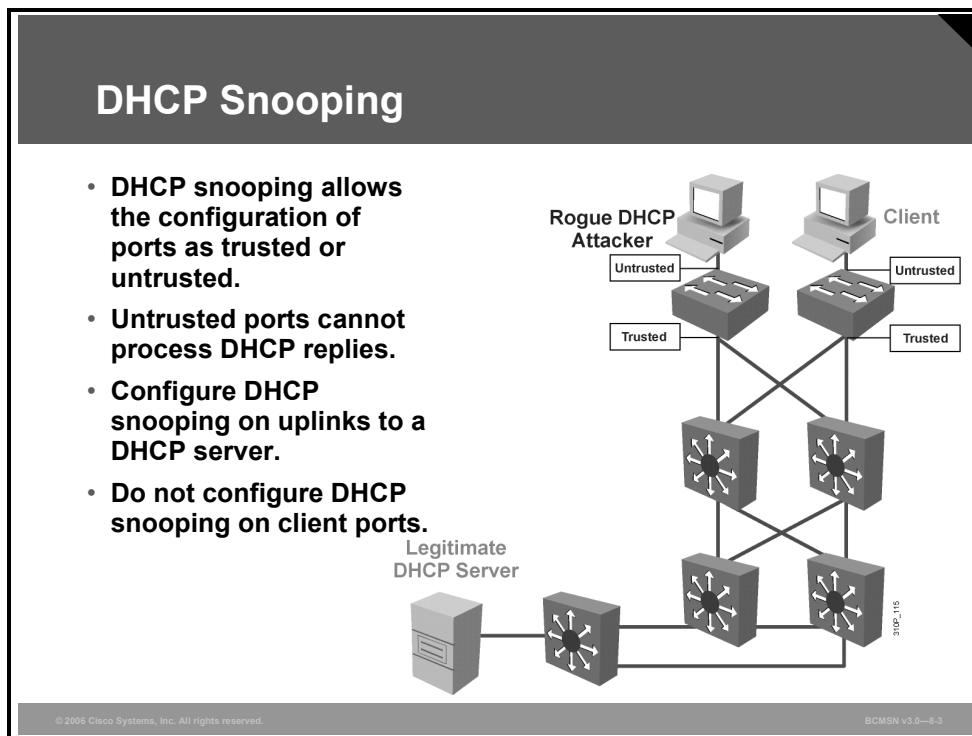
DHCP Spoof Attack Sequence

The table describes the DHCP spoof attack sequence, as shown in the figure.

Sequence of Events	Description
1.	Attacker hosts a rogue DHCP server off a switch port.
2.	Client broadcasts a request for DHCP configuration information.
3.	The rogue DHCP server responds before the legitimate DHCP server, assigning attacker-defined IP configuration information.
4.	Host packets are redirected to the attacker’s address as it emulates a default gateway for the erroneous DHCP address provided to the client.

Describing DHCP Snooping

This topic describes how the DHCP snooping feature provides security by filtering trusted DHCP messages and then using these messages to build and maintain a DHCP snooping binding table.



DHCP snooping is a Cisco Catalyst feature that determines which switch ports can respond to DHCP requests. Ports are identified as trusted and untrusted. Trusted ports can source all DHCP messages, whereas untrusted ports can source requests only. Trusted ports host a DHCP server or can be an uplink toward the DHCP server. If a rogue device on an untrusted port attempts to send a DHCP response packet into the network, the port is shut down. This feature can be coupled with DHCP Option 82, in which switch information, such as the port ID of the DHCP request, can be inserted into the DHCP request packet.

Untrusted ports are those that are not explicitly configured as trusted. A DHCP binding table is built for untrusted ports. Each entry contains the client MAC address, IP address, lease time, binding type, VLAN number, and port ID recorded as clients make DHCP requests. The table is then used to filter subsequent DHCP traffic. From a DHCP snooping perspective, untrusted access ports should not send any DHCP server responses, such as DHCPOFFER, DHCPACK, or DHCPNAK.

Sequence of Configuration	Description
1.	Configure global DHCP snooping.
2.	Configure trusted ports.
3.	Configure Option 82 insertion off (default enabled by step 2).
4.	Configure rate limiting on untrusted ports.
5.	Configure DHCP snooping for the selected VLANs.

Configuring DHCP Snooping

This topic explains the procedure to configure DHCP snooping and IP Source Guard.

Securing Against DHCP Snooping Attacks

```
Switch(config)# ip dhcp snooping
```

- Enables DHCP snooping globally

```
Switch(config)# ip dhcp snooping information option
```

- Enables DHCP Option 82 data insertion

```
Switch(config-if)# ip dhcp snooping trust
```

- Configures a trusted interface

```
Switch(config)# ip dhcp snooping limit rate [rate]
```

- Number of packets per second accepted on a port

```
Switch(config)# ip dhcp snooping vlan number [number]
```

- Enables DHCP snooping on your VLANs

© 2006 Cisco Systems, Inc. All rights reserved.
BCMSN v3.0-3-4

Steps for Enabling DHCP Snooping

To enable DHCP snooping, use these commands.

Step	Comments
1. Enable DHCP snooping globally. <pre>Switch(config)# ip dhcp snooping</pre>	By default, the feature is not enabled.
2. Enable DHCP Option 82. <pre>Switch(config)# ip dhcp snooping information option</pre>	This is optional for the forwarded DHCP request packet to contain information on the switch port where it originated.
3. Configure DHCP server interfaces or uplink ports as trusted. <pre>Switch(config-if)# ip dhcp snooping trust</pre>	At least one trusted port must be configured. Use the no keyword to revert to untrusted. By default, all ports are untrusted.
4. Configure the number of DHCP packets per second (pps) that are acceptable on the port. <pre>Switch(config-if)# ip dhcp snooping limit rate rate</pre>	Configure the number of DHCP pps that an interface can receive. Normally, the rate limit applies to untrusted interfaces. This is used to prevent DHCP starvation attacks by limiting the rate of the DHCP requests on untrusted ports.

Step	Comments
5. Enable DHCP snooping on specific VLAN(s). Switch(config)# ip dhcp snooping vlan number [number]	This is required to identify those VLANs that will be subject to DHCP snooping.
6. Verify the configuration. Switch# show ip dhcp snooping	Verify the configuration.

Verifying the DHCP Snooping Configuration

This example shows how to display the DHCP snooping configuration for a switch.

Verifying DHCP Snooping

Switch# show ip dhcp snooping

- **Verifies the DHCP snooping configuration**

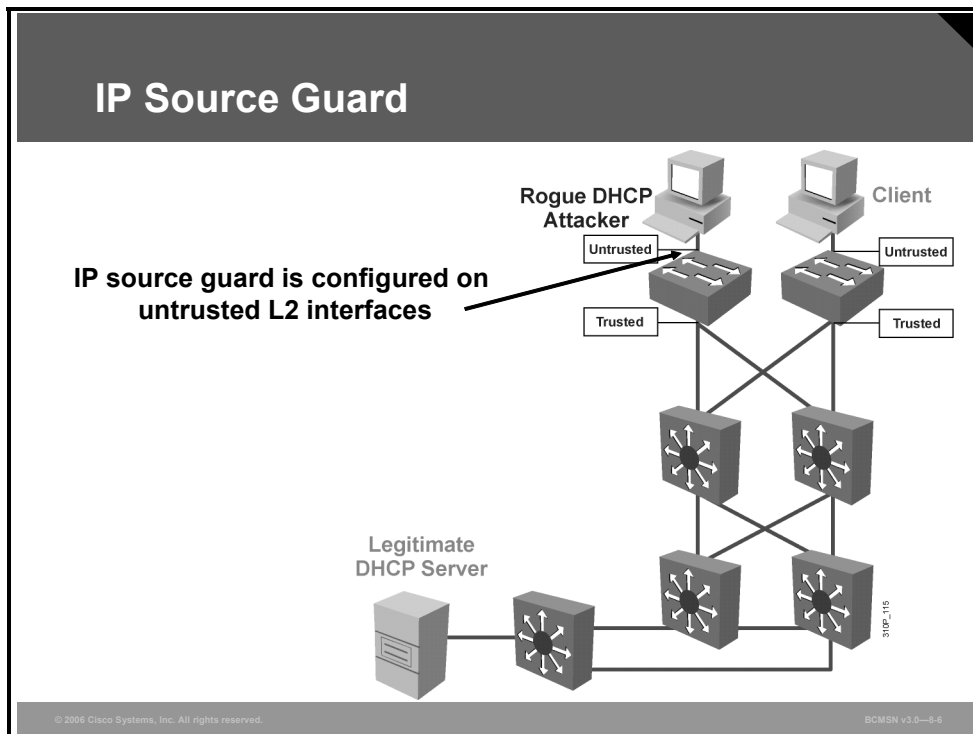
```
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP Snooping is configured on the following VLANs:
 10 30-40 100 200-220
Insertion of option 82 information is enabled.
Interface           Trusted           Rate limit (pps)
-----
FastEthernet2/1     yes              none
FastEthernet2/2     yes              none
FastEthernet3/1     no               20
Switch#
```

© 2006 Cisco Systems, Inc. All rights reserved.
BDM5N v3.0—5-5

Only ports that are trusted or that have a rate limit applied will be shown in the output. All other ports are untrusted and are not displayed.

IP Source Guard

This subtopic describes the IP source guard feature.



IP Source Guard is similar to DHCP snooping. This feature can be enabled on a DHCP snooping untrusted Layer 2 port to prevent IP address spoofing. To start, all IP traffic on the port is blocked except for DHCP packets that are captured by the DHCP snooping process.

When a client receives a valid IP address from the DHCP server, or when a static IP source binding is configured by the user, a per-port and VLAN Access Control List (PVACL) is installed on the port.

This process restricts the client IP traffic to those source IP addresses configured in the binding; any IP traffic with a source IP address other than that in the IP source binding will be filtered out. This filtering limits a host's ability to attack the network by claiming a neighbor host's IP address.

Note If IP Source Guard is enabled on a trunk port with a large number of VLANs that have DHCP snooping enabled, you might run out of access control list (ACL) hardware resources, and some packets might be switched in software.

IP Source Guard supports only the Layer 2 port, including both access and trunk. For each untrusted Layer 2 port, there are two levels of IP traffic security filtering, as follows:

- **Source IP address filter:** IP traffic is filtered based on its source IP address. Only IP traffic with a source IP address that matches the IP source binding entry is permitted.

An IP source address filter is changed when a new IP source entry binding is created or deleted on the port. The port PVACL will be recalculated and reapplied in the hardware to reflect the IP source binding change. By default, if the IP filter is enabled without any IP source binding on the port, a default PVACL that denies all IP traffic is installed on the port. Similarly, when the IP filter is disabled, any IP source filter PVACL will be removed from the interface.

- **Source IP and MAC address filter:** IP traffic is filtered based on its source IP address in addition to its MAC address; only IP traffic with source IP and MAC addresses that match the IP source binding entry are permitted.

Configuring IP Source Guard on the Switch

Use the following commands to configure the feature.

Configuring IP Source Guard on a Switch

```
Switch(config)# ip dhcp snooping
```

- Enables DHCP snooping globally

```
Switch(config)# ip dhcp snooping vlan number [number]
```

- Enables DHCP snooping on a specific VLAN

```
Switch(config-if)# ip verify source vlan  
dhcp-snooping port-security
```

- Enables IP Source Guard, source IP, and source MAC address filter on a port

© 2006 Cisco Systems, Inc. All rights reserved.
BCMSN v3.0—3-7

IP Source Guard Configuration Commands

The table describes the procedure for enabling IP Source Guard.

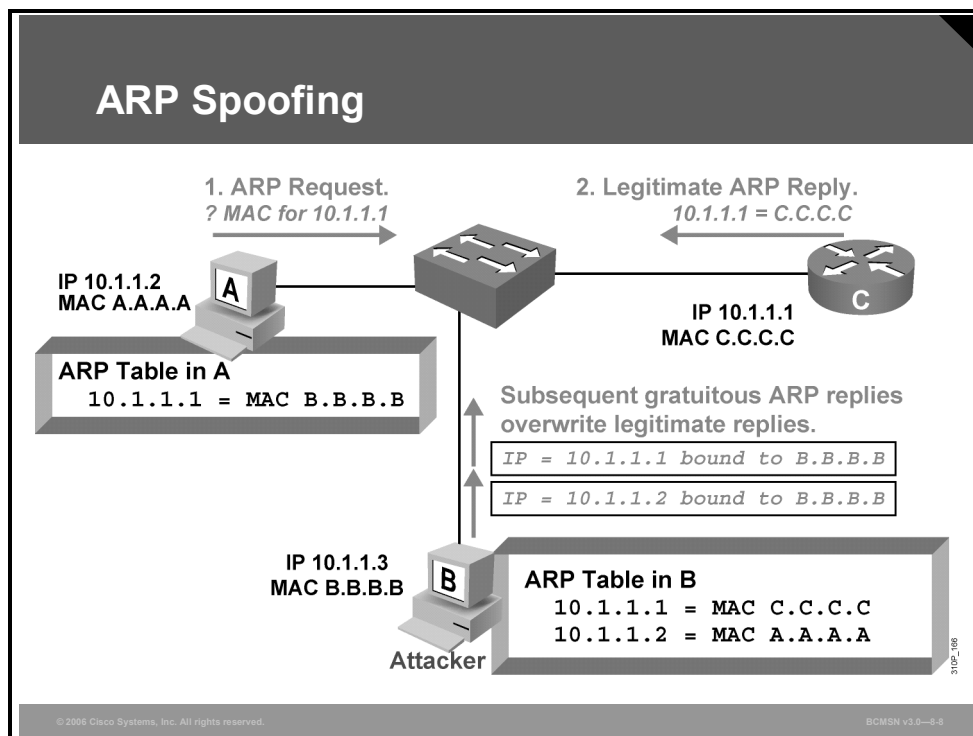
	Command	Purpose
Step 1	Switch(config)# <code>ip dhcp snooping</code>	Enables DHCP snooping globally. You can use the no keyword to disable DHCP snooping.
Step 2	Switch(config)# <code>ip dhcp snooping vlan number [number]</code>	Enables DHCP snooping on your VLANs.
Step 3	Switch(config)# <code>ip dhcp snooping vlan number [number]</code>	Configures the interface as trusted or untrusted. You can use the no keyword of to

	Command	Purpose
		configure an interface to receive only messages from within the network.
Step 4	Switch(config-if)# ip verify source vlan dhcp-snooping port-security	Enables IP Source Guard, source IP, and source MAC address filtering on the port.
Step 5	Switch(config-if)# switchport port-security limit rate invalid-source-mac N	(Optional) Sets the rate limit for bad packets. This rate limit also applies to the port where DHCP snooping security mode is enabled as filtering the IP and MAC address.
Step 6	Switch(config)# ip source binding ip-addr ip vlan number interface interface	Configures a static IP binding on the port.
Step 7	Switch(config)# end	Exits configuration mode.

Note The static IP source binding can be configured on a switch port only. If you issue the IP source binding VLAN interface command on a Layer 3 port, you will receive this error message: Static IP source binding can be configured on the switch port only.

Describing ARP Spoofing

This topic describes what happens in a network during an attack using ARP spoofing.



In normal ARP operation, a host sends a broadcast to determine the MAC address of a host with a particular IP address. The device at that IP address replies with its MAC address. The originating host caches the ARP response, using it to populate the destination Layer 2 header of packets sent to that IP address.

By spoofing an ARP reply from a legitimate device with a gratuitous ARP, an attacking device appears to be the destination host sought by the senders. The ARP reply from the attacker causes the sender to store the MAC address of the attacking system in its ARP cache. All packets destined for those IP addresses will be forwarded through the attacker system.

As illustrated in the figure, this is the sequence of events in an ARP spoofing attack.

ARP Spoofing Attack

An ARP spoofing attack follows the sequence shown in the table.

Step or Sequence Number	Description
1.	Host A sends an ARP request for C's MAC address.
2.	Router C replies with its MAC and IP addresses. C also updates its ARP cache.
3.	Host A binds C's MAC address to its IP address in its ARP cache.
4.	Host B (attacker) sends ARP binding B's MAC address to C's IP address.
5.	Host A updates ARP cache with B's MAC address bound to C's IP address.
6.	Host B sends ARP binding B's MAC address to A's IP address.
7.	Router C updates ARP cache with B's MAC address bound to A's IP address.
8.	Packets are now diverted through attacker (B).

Configure all access switch ports as untrusted and all switch ports connected to other switches as trusted. In this case, all ARP packets entering the network would be from an upstream distribution or core switch, bypassing the security check and requiring no further validation.

DAI can also be used to rate limit the ARP packets and then errdisable the interface if the rate is exceeded.

Describing Commands to Configure DAI

This topic describes the commands that can be used to configure DAI.

Configuring DAI

```
Switch(config)#ip arp inspection vlan vlan_id [,vlan_id]
```

- Enables DAI on a VLAN or range of VLANs

```
Switch(config-if)#ip arp inspection trust
```

- Enables DAI on an interface and sets the interface as a trusted interface

```
Switch(config-if)#ip arp inspection validate { [src-mac]  
[dst-mac] [ip] }
```

- Configures DAI to drop ARP packets when the IP addresses are invalid

© 2006 Cisco Systems, Inc. All rights reserved.BCMSN v3.0-8-10

DAI Commands

The table describes the commands used to configure DAI.

Command	Description
Switch(config)# ip arp inspection vlan <i>vlan_id</i> [, <i>vlan_id</i>]	Enables DAI on a VLAN or range of VLANs
Switch(config-if)# ip arp inspection trust	Enables DAI on an interface and sets the interface as a trusted interface
Switch(config)# ip arp inspection validate { [<i>src-mac</i>] [<i>dst-mac</i>] [<i>ip</i>] }	Configures DAI to drop ARP packets when the IP addresses are invalid, or when the MAC addresses in the body of the ARP packets do not match the addresses specified in the Ethernet header

It is generally advisable to configure all access switch ports as untrusted and to configure all uplink ports connected to other switches as trusted.

This example of DAI implementation illustrates the configuration required on switch 2 with port FastEthernet 3/3 as the uplink port toward the DHCP server.

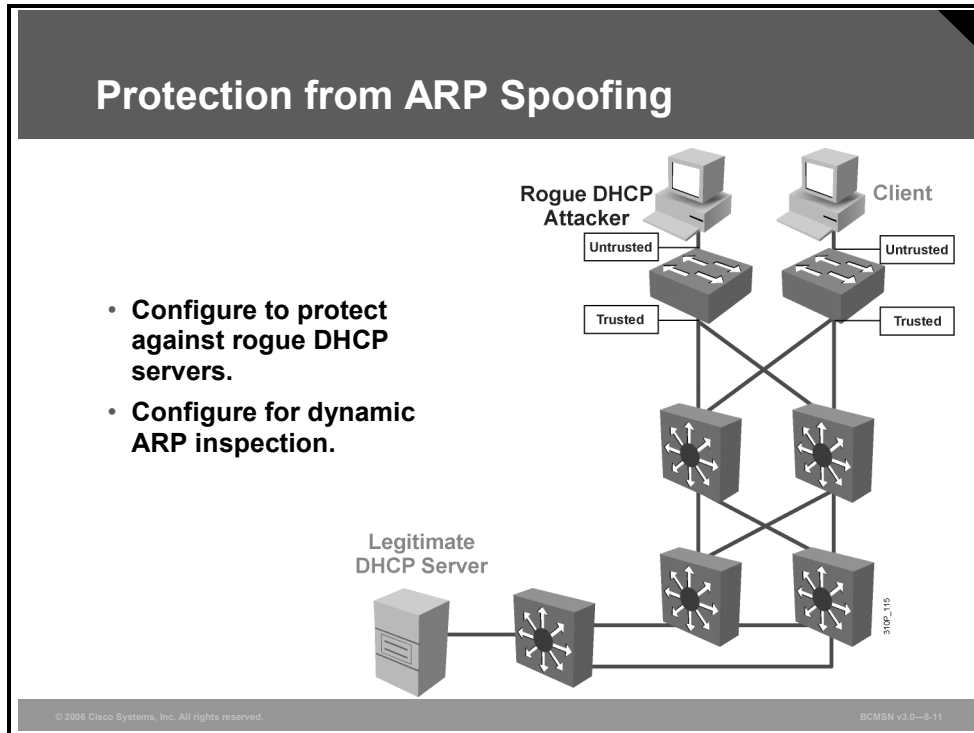
Example: DAI Implementation

This example shows how to configure DAI for hosts on VLAN1, where client devices are located for switch 2. All client ports are untrusted by default. Only port 3/3 is trusted because this is the only port where DHCP replies would be expected.

```
Switch S2(config)#ip arp inspection vlan 1
Switch S2(config)#interface fastethernet 3/3
Switch S2(config-if)#ip arp inspection trust
```

Protecting Against ARP Spoofing Attacks

This topic explains the procedure to protect a network from ARP spoofing attacks.



To mitigate the chances of ARP spoofing, these procedures are recommended:

- Step 1** Implement protection against DHCP spoofing.
- Step 2** Enable DAI.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

- **DHCP spoof attacks send unauthorized replies to DHCP queries.**
- **DHCP snooping is used to counter a DHCP spoof attack.**
- **DHCP snooping is easily implemented on a Cisco Catalyst switch.**
- **ARP spoofing can be used to redirect traffic to an unauthorized device on the network.**
- **Dynamic ARP inspection in conjunction with DHCP snooping can be used to counter ARP spoofing attacks.**
- **Configuration commands for dynamic ARP inspection are simple to understand.**
- **Dynamic APR inspection and DHCP snooping can protect against ARP spoofing attacks.**

Describing STP Security Mechanisms

Overview

After Spanning Tree Protocol (STP) operations are stable in a switched network, the administrator may want to guard against rogue switches being attached to the network because these switches may take on the role of the root or backup root bridge.

Bridge protocol data unit (BPDU) guard, BPDU filtering, and root guard are features that attempt to contain the points at which switches and root bridges can be attached to the network.

Objectives

Upon completing this lesson, you will be able to configure BPDU guard, BPDU filtering, and root guard to prevent rogue Layer 2 switches from playing a key role in STP operations when placed on specific switch ports. This ability includes being able to meet these objectives:

- Describe the methods that are available to protect the operation of STP
- Describe the commands to configure BPDU guard
- Describe the commands to configure BPDU filtering
- Describe how root guard is used to improve the stability of Layer 2 networks
- Describe the commands used to configure root guard

Protecting the Operation of STP

This topic describes the methods that are available to protect the operation of STP.

Protecting the Operation of STP

Protection against switches being added on PortFast ports.

- **BPDU guard shuts ports down.**
- **BPDU filter specifies action to be taken when BPDUs are received.**

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0-4-2

Cisco Systems provides two features to protect spanning tree from loops being created on ports where PortFast has been enabled. In a proper configuration, PortFast would be enabled on only those ports that support end devices such as servers and workstations. It is anticipated that BPDUs from a switch device should not be received on a PortFast interface. However, should this happen, BPDU guard and BPDU filtering provide protection. Both BPDU guard and BPDU filtering can be configured globally on all PortFast-configured ports or on individual ports.

BPDU Guard

BPDU guard is used to protect the switched network from the problems that may be caused by the receipt of BPDUs on ports that should not be receiving them. The receipt of unexpected BPDUs may be accidental or may be part of an unauthorized attempt to add a switch to the network.

BPDU Filtering

PortFast BPDU filtering affects how the switch acknowledges BPDUs seen on PortFast-configured ports. Its functionality differs if it is configured globally or on a per-port basis. This difference will be explained elsewhere in this course.

BPDU Root Guard

BPDU root guard protects against a switch outside the designated network attempting to become the root bridge by blocking its access until the receipt of its BPDUs ceases.

Describing BPDU Guard Configuration

This topic describes the commands to configure BPDU guard.

Enabling and Verifying BPDU Guard

```
Switch(config)#spanning-tree portfast bpduguard
```

- **Enables BPDU guard**

```
Switch#show spanning-tree summary totals
```

- **Displays BPDU guard configuration information**

```
Switch#show spanning-tree summary totals

Root bridge for: none.
PortFast BPDU Guard is enabled
Etherchannel misconfiguration guard is enabled
UplinkFast is disabled
BackboneFast is disabled
Default pathcost method used is short

Name                    Blocking Listening Learning Forwarding STP Active
-----
34 VLANs 0              0          0          36          36
```

© 2006 Cisco Systems, Inc. All rights reserved.BOMSN v3.0-3.3

BPDU guard protects the network from loops that might form if BPDUs are received on a PortFast-enabled switch port.

Note When the BPDU guard feature is enabled, spanning tree applies BPDU guard to all PortFast-configured interfaces.

BPDU Filtering Applied Globally Versus Per-Port

At the global level, you can enable BPDU guard on PortFast-enabled ports by using the **spanning-tree portfast bpduguard default** global configuration command. In a valid configuration, PortFast-enabled ports do not receive BPDUs. Receiving a BPDU on a PortFast-enabled port signals an invalid configuration, such as the connection of an unauthorized device, and the BPDU guard feature puts the port in the error-disabled state.

At the interface level, you can enable BPDU guard on any port by using the **spanning-tree bpduguard enable** interface configuration command without also enabling the PortFast feature. When the port receives a BPDU, it is put in the error-disabled state.

Configuring BPDU Guard

To enable BPDU guard globally on the switch, use this command:

```
Switch(config)# spanning-tree portfast bpduguard default
```

The **no** form of the command will disable the feature on the switch.

To enable PortFast BPDU guard on a specific switch port, enter this command:

```
Switch(config)# spanning-tree bpduguard enable
```

The **no** form of the command will disable the feature on the interface.

Verifying BPDU Guard

This example shows how to verify the BPDU configuration.

```
Switch#show spanning-tree summary totals
```

```
Root bridge for: none.
```

```
PortFast BPDU guard is enabled
```

```
Etherchannel misconfiguration guard is enabled
```

```
UplinkFast is disabled
```

```
BackboneFast is disabled
```

```
Default pathcost method used is short
```

Name	Blocking	Listening	Learning	Forwarding	STP Active
-----	-----	-----	-----	-----	-----
34 VLANs	0	0	0	36	36

Describing BPDU Filtering Configuration

This topic describes the commands to configure BPDU filtering.

Describing BPDU Filtering

```
Switch(config)#spanning-tree portfast bpdufilter default
```

- **Enables BPDU filtering**

```
Switch#show spanning-tree summary totals
```

- **Displays BPDU filtering configuration information**

```
Switch#show spanning-tree summary totals
Root bridge for:VLAN0010
EtherChannel misconfiguration guard is enabled
Extended system ID is disabled
Portfast is enabled by default
PortFast BPDU Guard is disabled by default
Portfast BPDU Filter is enabled by default
Loopguard is disabled by default
UplinkFast is disabled
BackboneFast is disabled
Pathcost method used is long

Name                Blocking Listening Learning Forwarding STP Active
-----
2 vlans              0          0          0          3          3
```

© 2006 Cisco Systems, Inc. All rights reserved.BOMS v3.0-3-4

BPDU Filtering Applied Globally Versus Per-Port

BPDU filtering can be configured globally or on individual PortFast-enabled ports. The global versus interface configuration has different effects, as follows.

When enabled globally, BPDU filtering has these attributes:

- It affects all operational PortFast ports on switches that do not have BPDU filtering configured on the individual ports.
- If BPDUs are seen, the port loses its PortFast status, BPDU filtering is disabled, and STP sends and receives BPDUs on the port as it would with any other STP port on the switch.
- Upon startup, the port transmits 10 BPDUs. If this port receives any BPDUs during that time, PortFast and PortFast BPDU filtering are disabled.

When enabled on an individual port, BPDU filtering has these attributes:

- It ignores all BPDUs received.
- It sends no BPDUs.

Caution Explicit configuration of PortFast BPDU filtering on a port that is not connected to a host station can result in bridging loops. The port ignores any incoming BPDUs and changes to the forwarding state. This does not occur when PortFast BPDU filtering is enabled globally.

BPDU Filtering Results

The table lists the possible combinations that result from configuring BPDU filtering globally and on individual ports on the same switch.

Per-Port Configuration	Global Configuration	PortFast State	PortFast BPDU Filtering State
Default	Enable	Enable	Enable
Default	Enable	Disable	Disable
Default	Disable	Not applicable	Disable
Disable	Not applicable	Not applicable	Disable
Enable	Not applicable	Not applicable	Enable

Configuring BPDU Filtering

To enable PortFast BPDU filtering globally on the switch, enter this command:

```
Switch(config)#spanning-tree portfast bpdupfilter default
```

To enable PortFast BPDU filtering on a specific switch port, enter this command:

```
Switch(config-if)# spanning-tree bpdupfilter enable
```

Verifying BPDU Filtering

To verify the configuration on the switch, enter this command:

```
Switch#show spanning-tree summary totals
PxD1#sh spanning-tree summary
Switch is in pvst mode
Root bridge for: none
Extended system ID          is enabled
Portfast Default            is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default          is disabled
EtherChannel misconfig guard is enabled
UplinkFast                  is disabled
BackboneFast                is disabled
Configured Pathcost method used is short
Name                        Blocking Listening Learning Forwarding STP Active
-----
VLAN0001                    2          0          0          6          8
-----
1 vlan                      2          0          0          6          8
PxD1#
```

To verify the configuration on a specific port, enter this command to see the associated output:

```
Switch# show spanning-tree interface fastEthernet 4/4 detail
```

```
Port 196 (FastEthernet4/4) of VLAN0010 is forwarding
```

```
Port path cost 1000, Port priority 160, Port Identifier 160.196.
```

```
Designated root has priority 32768, address 00d0.00b8.140a
```

```
Designated bridge has priority 32768, address 00d0.00b8.140a
```

```
Designated port id is 160.196, designated path cost 0
```

```
Timers:message age 0, forward delay 0, hold 0
```

```
Number of transitions to forwarding state:1
```

```
The port is in the portfast mode by portfast trunk configuration
```

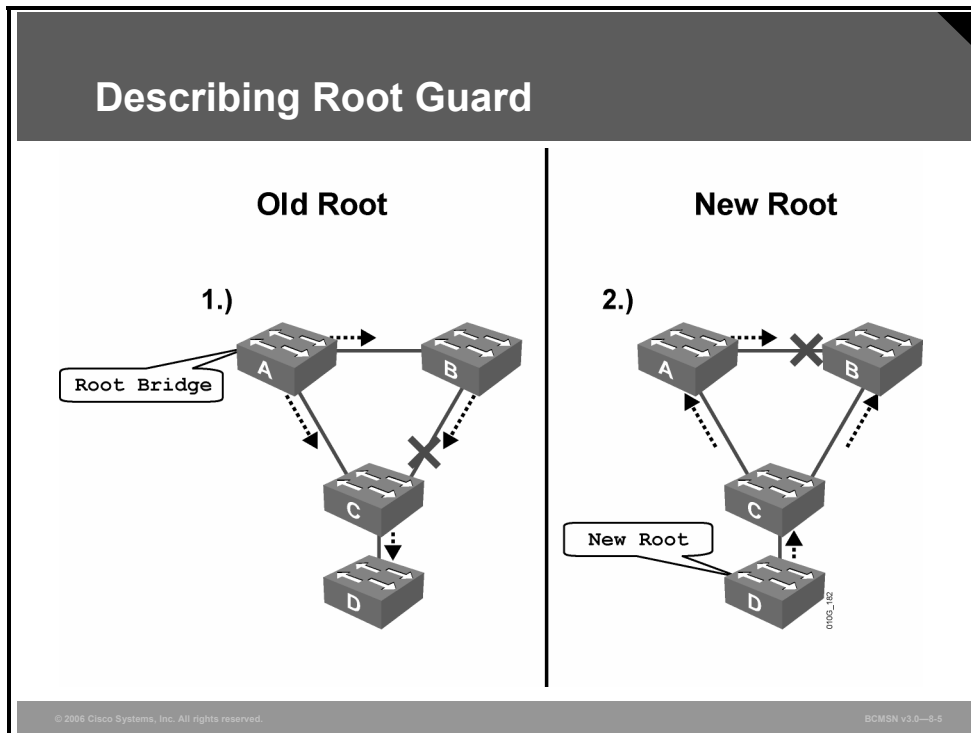
```
Link type is point-to-point by default
```

```
Bpdu filter is enabled
```

```
BPDUs:sent 0, received 0
```

Describing Root Guard

This topic describes how root guard is used to improve the stability of Layer 2 networks.



Root guard limits the switch ports out of which the root bridge may be negotiated. If a root-guard-enabled port receives BPDUs that are superior to those being sent by the current root bridge, then that port will be moved to a root-inconsistent state, which is effectively equal to an STP listening state. No data traffic will be forwarded across this port.

Example: Using Root Guard

In the example, switches A and B are the core of the network. Switch A is the root bridge for a VLAN. Switch C is an access layer switch. The link between B and C is blocking on the C side. The flow of STP BPDUs is shown with arrows.

On the left, device D begins to participate in STP. If the priority of switch D were any value lower than that of the current root bridge, it would be a superior BPDUs, and switch D would be elected the root bridge.

This would cause the link connecting switches A and B to block, thus causing all traffic from switch B to flow through switch C in the access layer, which is clearly not advantageous. If root guard were configured on the port of switch C where switch D is attached, switch D would never have been elected the root bridge.

Root guard is configured on a per-port basis. If a superior BPDUs is received on the port, root guard does not take the BPDUs into account and so puts the port into a root-inconsistent state. When switch D stops sending superior BPDUs, the port will be unblocked again and will transition through STP states like any other port.

Recovery requires no intervention. A root guard port is in an STP-designated port state. When root guard is enabled on a port, the switch does not allow that port to become an STP root port. The port remains as an STP-designated port.

Root guard should be enabled on all ports where the root bridge is not anticipated. In the example, root guard should be enabled as follows:

- Switch A: port connecting to switch C
- Switch B: port connecting to switch C
- Switch C: port connecting to switch D

This console message appears when root guard blocks a port:

```
%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-designated in  
VLAN 77. Moved to root-inconsistent state
```

Describing Root Guard Configuration Commands

This topic describes the commands used to configure root guard.

Describing Root Guard Configuration Commands

```
Switch(config-if)#spanning-tree guard root
```

- **Configures root guard**

```
Switch#show running-config interface fa 0/1  
Switch#show spanning-tree inconsistentports
```

- **Verifies root guard**

© 2006 Cisco Systems, Inc. All rights reserved.BCMSN v3.0-5-6

Root Guard Commands

These commands can be used to configure and verify root guard.

Command	Description
Switch(config-if)# spanning-tree guard root	Enables root guard on an interface
Switch(config-if)# no spanning-tree guard root	Disables root guard on an interface
Switch# show running-config interface type mod/port	Indicates if root guard has been configured on an interface
Switch# show spanning-tree inconsistentports	Indicates if any ports are in a root-inconsistent state

Here are the commands for configuring and verifying root guard.

To enable root guard on a Layer 2 access port (to force it to become a designated port) or to disable root guard, use this command preceded by the word “no.”

```
Switch(config-if)#spanning-tree guard root
```

This example demonstrates how to verify the root guard configuration.

Verifying Root Guard

```
Switch#show running-config interface interface mod/port
```

- **Displays interface configuration information**

```
Switch#show spanning-tree inconsistentports
```

- **Displays information about ports in inconsistent states**

```
Switch#show running-config interface fastethernet 5/8
Building configuration...
Current configuration: 67 bytes
!
interface FastEthernet5/8
switchport mode access
spanning-tree guard root
Switch#show spanning-tree inconsistentports
Name                Interface            Inconsistency
-----
VLAN0001            FastEthernet3/1     Port Type Inconsistent
VLAN0001            FastEthernet3/2     Port Type Inconsistent
VLAN1002            FastEthernet3/1     Port Type Inconsistent

Number of inconsistent ports (segments) in the system :3
```

© 2006 Cisco Systems, Inc. All rights reserved. BOMSN v3.0-3-7

To verify root guard, use these commands:

```
Switch#show running-config interface fastethernet 5/8
```

This example shows how to determine whether any ports are in a root-inconsistent state:

```
Switch#show spanning-tree inconsistentports
```

Name	Interface	Inconsistency
VLAN0001	FastEthernet3/1	Port Type Inconsistent
VLAN0001	FastEthernet3/2	Port Type Inconsistent
VLAN1002	FastEthernet3/1	Port Type Inconsistent
VLAN1002	FastEthernet3/2	Port Type Inconsistent
VLAN1003	FastEthernet3/1	Port Type Inconsistent
VLAN1003	FastEthernet3/2	Port Type Inconsistent
VLAN1004	FastEthernet3/1	Port Type Inconsistent
VLAN1004	FastEthernet3/2	Port Type Inconsistent
VLAN1005	FastEthernet3/1	Port Type Inconsistent
VLAN1005	FastEthernet3/2	Port Type Inconsistent

Number of inconsistent ports (segments) in the system :10

Summary

This topic summarizes the key points discussed in this lesson.

Summary

- **BPDU guard and BPDU filtering protect the operation of STP on PortFast-configured ports.**
- **When BPDU guard is configured globally, it affects all PortFast configured ports.**
- **BPDU guard can be configured per port, even on those ports not configured with PortFast.**
- **BPDU filtering can be configured globally or per port.**
- **The root switch cannot be elected via BPDUs received on a root-guard-configured port.**
- **Root guard can be configured and verified using various commands.**

Preventing STP Forwarding Loops

Overview

Spanning tree operations can be severely disrupted by links that pass traffic in one direction and not in the other direction. The Cisco Catalyst platform provides features to guard against this condition. Unidirectional Link Detection (UDLD) and loop guard protect the network from anomalous conditions that result from unidirectional link conditions.

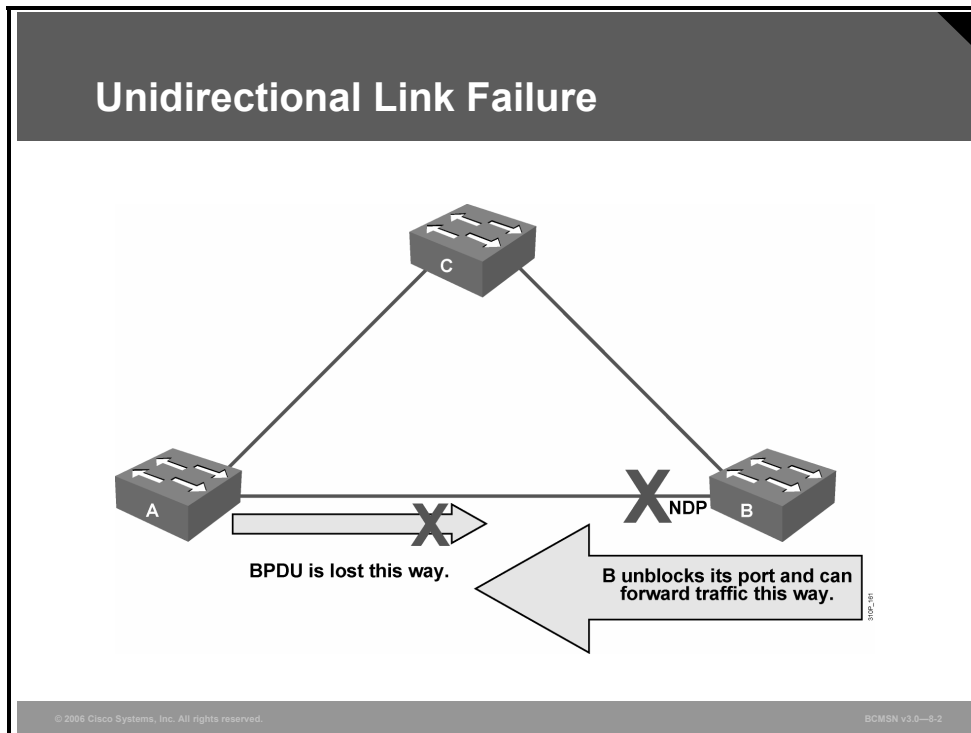
Objectives

Upon completing this lesson, you will be able to configure UDLD and loop guard to mitigate the adverse effects that unidirectional links have on spanning tree. This ability includes being able to meet these objectives:

- Describe how UDLD is used to detect and shut down unidirectional links
- Describe how loop guard is used to protect against Layer 2 forwarding loops
- Describe the commands used to configure UDLD and loop guard
- Compare the features of loop guard and UDLD as they protect against unidirectional links

Describing UDLD

This topic describes how UDLD is used to detect and shut down unidirectional links.



A unidirectional link occurs when traffic is transmitted between neighbors in one direction only. Unidirectional links can cause spanning tree topology loops. UDLD allows devices to detect when a unidirectional link exists and also to shut down the affected interface.

UDLD is a Layer 2 protocol that works with the Layer 1 mechanisms to determine the physical status of a link. If one fiber strand in a pair is disconnected, autonegotiation would not allow the link to become active or stay up. If both fiber strands are operant from a Layer 1 perspective, UDLD determines if traffic is flowing bidirectionally between the correct neighbors.

The switch periodically transmits UDLD packets on an interface with UDLD enabled. If the packets are not echoed back within a specific time frame, the link is flagged as unidirectional, and the interface is shut down. Devices on both ends of the link must support UDLD for the protocol to successfully identify and disable unidirectional links.

Although the UDLD protocol falls outside of Spanning Tree Protocol (STP), UDLD has numerous benefits that make it essential in a Layer 2 network. The function of UDLD is to prevent one-way communication between adjacent devices. When UDLD detects one-way conversation, it can do one of two things, depending on whether UDLD is configured in Normal mode or Aggressive mode.

In Normal mode, UDLD simply changes the UDLD-enabled port to undetermined state if it stops receiving UDLD messages from its directly connected neighbor. Aggressive mode was introduced in Cisco Catalyst OS 5.4(3); it makes eight attempts to re-establish the UDLD neighbor relation before error disabling the port.

Aggressive mode is the preferred method of configuring UDLD. By preventing this one-way communication, UDLD can be very useful in spanning tree networks. UDLD was first introduced in Catalyst OS 5.1(1). UDLD is a Layer 2 protocol that is enabled between adjacent switches. It uses MAC 01-00-0c-cc-cc-cc with Subnetwork Access Protocol (SNAP) High-Level Data Link Control (HDLC) protocol type 0x0111.

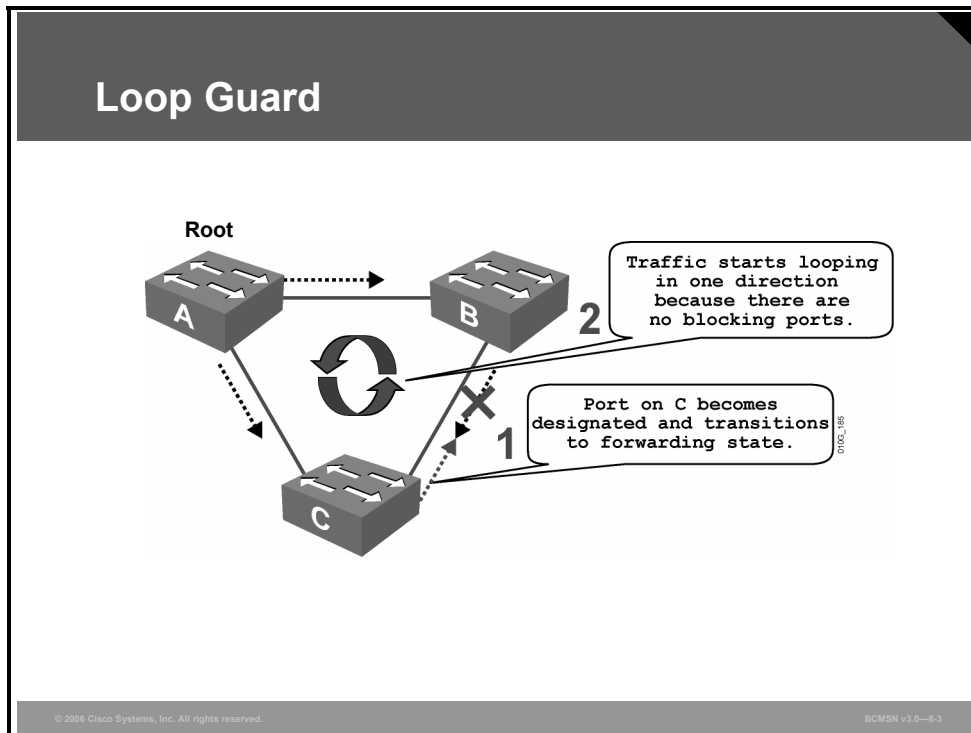
Default Status for the UDLD

The table describes the default status for the UDLD on a global and an interface basis.

Feature	Default Status
UDLD global enable state	Globally disabled
UDLD per-interface enable state for fiber-optic media	Enabled on all Ethernet fiber-optic interfaces
UDLD per-interface enable state for twisted-pair (copper) media	Disabled on all Ethernet 10/100 and 1000BASE-TX interfaces

Describing Loop Guard

This topic describes how loop guard is used to protect against Layer 2 forwarding loops.



Like UDLD, loop guard provides protection for STP when a link is unidirectional and bridge protocol data units (BPDUs) are being sent but not received on a link that is considered operational. Without loop guard, a blocking port will transition to forwarding if it stops receiving BPDUs.

If loop guard is enabled and the link is not receiving BPDUs, the interface will move into the STP loop-inconsistent blocking state. When loop guard blocks a port, this message is generated to the console or log file if allowed:

```
SPANTREE-2-LOOPGUARDBLOCK: No BPDUs were received on port 3/2 in vlan 3. Moved to loop-inconsistent state.
```

When a BPDU is received on a loop guard port that is in a loop-inconsistent state, the port will transition to the appropriate state as determined by the normal functioning of spanning tree. The recovery requires no user intervention. After the recovery, this message is logged:

```
SPANTREE-2-LOOPGUARDUNBLOCK: port 3/2 restored in vlan 3.
```

The loop guard feature protects against possible spanning tree loops by detecting a unidirectional link. With a unidirectional link, a port on one of the link partners is operationally in the up state and transmitting but is not receiving traffic. At the same time, the other link partner is operating correctly.

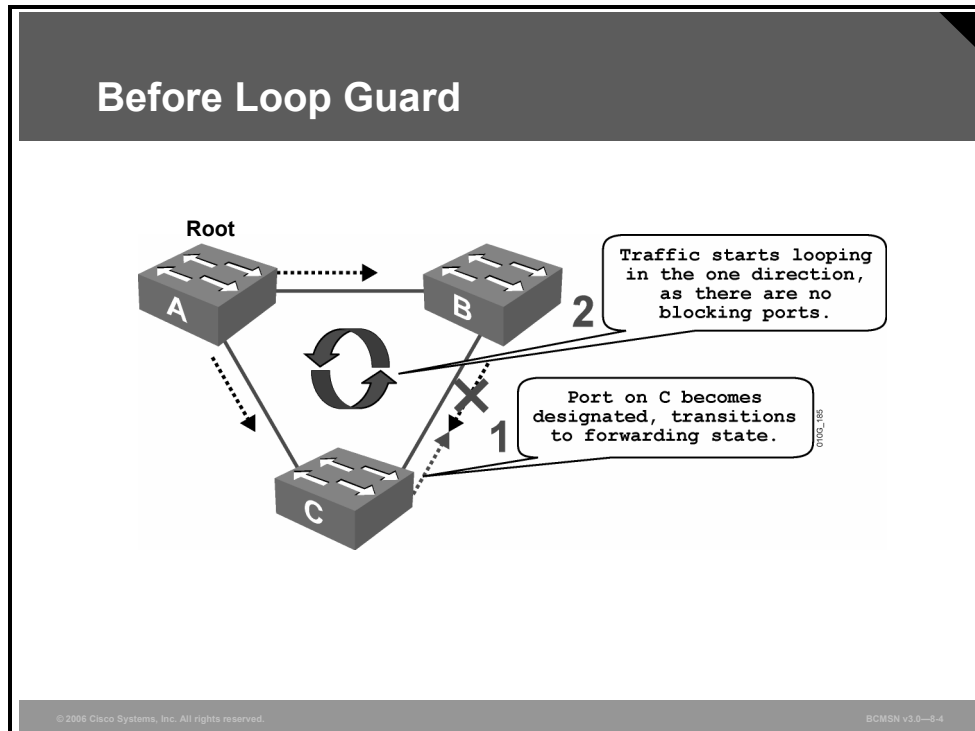
Loop guard is enabled on ports that are participating in spanning tree and are redundant at Layer 2. When the switch stops receiving BPDUs on its root or blocking port, it will transition the port to a loop-inconsistent state, which does not pass traffic.

Loop guard is configured per port on codes earlier than Catalyst OS 7.1(1). Loop guard does not work with root guard, and loop guard should not be enabled on PortFast ports.

One other caveat involving loop guard is with EtherChannel. The first operational port is used for BPDUs; if the link has a unidirectional failure, loop guard will transition all the links of the channel to a loop-inconsistent state. This is not a desirable effect because the inherent redundancy gained through channeling is lost.

Example: Before Loop Guard

This subtopic demonstrates how loops can occur as a result of unidirectional link failure.

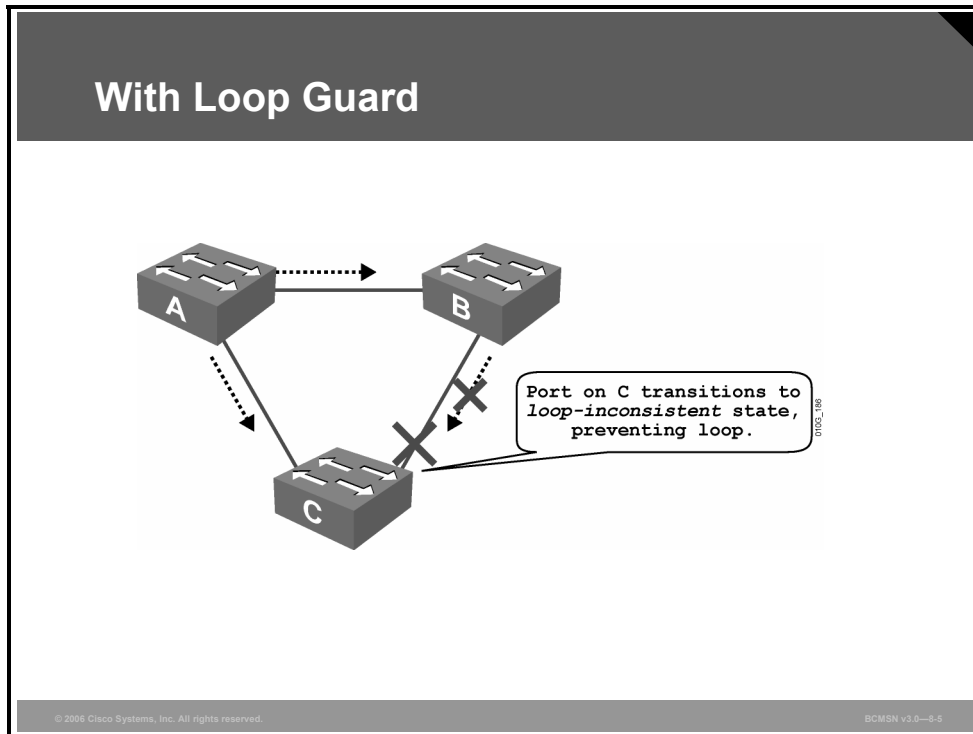


In this example, switch A is the root bridge. Because of unidirectional link failure on the link between switch B and switch C, switch C is not receiving BPDUs from B.

Without loop guard, the STP blocking port on C will transition to the STP listening state upon max age timer expiration and then to the forwarding state in two times the forward delay time. A loop will be created.

Example: With Loop Guard

This example demonstrates how loop guard works to prevent loops during a unidirectional link failure.



With loop guard enabled, the blocking port on switch C will transition into the STP loop-inconsistent state upon expiration of the max age timer. Because a port in the STP loop-inconsistent state will not pass user traffic, no loop is created. The loop-inconsistent state is effectively equal to the blocking state.

Configuring UDLD and Loop Guard

This topic describes the commands to configure UDLD and loop guard.

UDLD and Loop Guard Configuration Commands

Configuring and verifying UDLD

- `udld enable`
- `show udld interface fa0/1`

Configuring and verifying loop guard

- `spantree global-default loopguard enable`
- `show spantree guard fa0/1`

© 2006 Cisco Systems, Inc. All rights reserved. BOMSN v3.0—3-6

UDLD and Loop Guard Commands

To enable or disable UDLD and loop guard, use these commands.

Command	Description
Switch(config-if) # udld enable	Enables UDLD on fiber and nonfiber interfaces
Switch(config) # udld enable	Enables UDLD globally on all fiber-optic switch interfaces
Switch(config-if) # no udld enable	Disables UDLD on individual nonfiber-optic interfaces
Switch(config-if) # udld disable	Disables UDLD on individual fiber-optic interfaces
Switch# udld reset	Resets all interfaces that have been shut down by UDLD
Switch# show udld interface <i>type mod/port</i>	Verifies the UDLD configuration for an interface
Switch(config) # spantree global-default loopguard enable	Globally enables loop guard

Command	Description
Switch(config)# spantree global-default loopguard disable	Globally disables loop guard
Switch# show spantree guard type mod/port vlan	Verifies loop guard status

Configuring UDLD

This subtopic identifies the command options for configuring UDLD.

Configuring UDLD

`Switch(config)#udld enable`

- **Enables UDLD globally on all fiber-optic interfaces**

`Switch(config-if)#udld enable`

- **Enables UDLD on an individual interface**

`Switch(config-if)#no udld enable`

- **Disables UDLD on an individual nonfiber-optic interface**

`Switch(config-if)#udld disable`

- **Disables UDLD on an individual fiber-optic interface**

© 2006 Cisco Systems, Inc. All rights reserved.
BCMSN v3.0-3-7

UDLD is used when a link should be shut down because of a hardware failure that is causing unidirectional communication. In an EtherChannel bundle, UDLD will shut down only the physical link that has failed.

UDLD can be enabled globally for all fiber interfaces or on a per-interface basis.

Enable UDLD on an Interface

To enable UDLD on an interface use this command:

```
Switch(config-if)#udld enable
```

Enable UDLD Globally

To enable UDLD globally on all fiber-optic interfaces, use this command:

```
Switch(config)#udld enable
```

Verifying and Resetting UDLD

This subtopic identifies the command options for resetting UDLD and verifying UDLD configuration.

Resetting and Verifying UDLD

```
Switch# udld reset
```

- Resets all interfaces that have been shut down by UDLD

```
Switch#show udld interface
```

- Displays UDLD information for a specific interface

© 2006 Cisco Systems, Inc. All rights reserved.BCMSN v3.0-6.8

Interfaces will be shut down by UDLD. To reset all interfaces that have been shut down by UDLD, enter this command:

```
Switch#udld reset
```

To verify the UDLD configuration for an interface, enter this command:

```
Switch#show udld interface
```

Example: Displaying the UDLD State

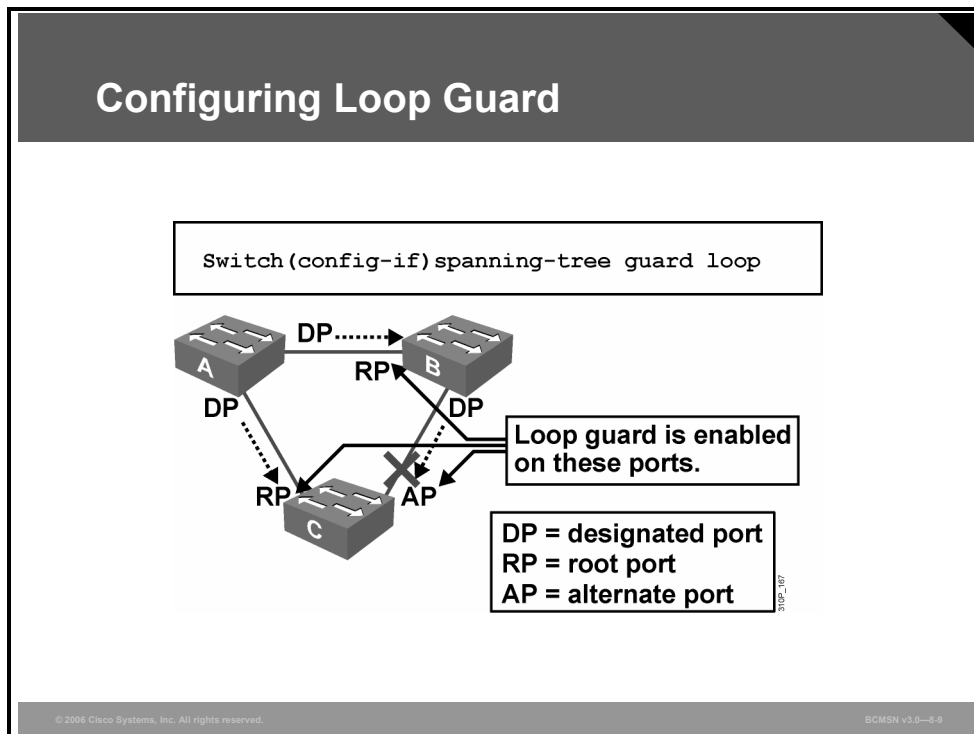
This example shows how to display the UDLD state for a single interface.

```
Switch#show udld GigabitEthernet2/2
Interface Gi2/2
---
Port enable administrative configuration setting: Follows device
default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement
Message interval: 60
Time out interval: 5
No multiple neighbors detected
  Entry 1
  ---
  Expiration time: 146
  Device ID: 1
  Current neighbor state: Bidirectional
  Device name: 0050e2826000
  Port ID: 2/1
  Neighbor echo 1 device: SAD03160954
  Neighbor echo 1 port: Gi1/1

  Message interval: 5
```

Configuring Loop Guard

This subtopic identifies how to configure loop guard.



Loop guard is enabled on a per-port basis. When loop guard is enabled, it is automatically applied to all of the active VLAN instances to which that port belongs. When you disable loop guard, it is disabled for the specified ports.

Disabling loop guard moves all loop-inconsistent ports to the listening state. If loop guard is enabled on an EtherChannel interface, the entire channel will be blocked for a particular VLAN. This is because EtherChannel is regarded as one logical port from an STP point of view.

Loop guard should be enabled on the root port and the alternative ports on access switches.

Enable Loop Guard on an Interface

To enable loop guard on a specific interface, issue this command:

```
Switch(config-if) # spanning-tree guard loop
```

To disable loop guard, issue this command:

```
Switch(config-if) # no spanning-tree guard loop
```

Enabling loop guard will disable root guard if root guard is currently enabled on the ports.

Enable Loop Guard Globally

Loop guard can be enabled globally on a switch for all point-to-point links. A full-duplex link is considered to be a point-to-point link. The status of loop guard can be changed on an interface, even if the feature has been enabled globally.

To enable loop guard globally, issue this command:

```
Switch(config)#span-tree global-default loopguard enable
```

To globally disable loop guard, issue this command:

```
Switch(config)#span-tree global-default loopguard disable
```

Verifying the Loop Guard Status

To verify the loop guard status, issue this command:

```
Switch#show span-tree guard mod/port | vlan
```

For example,

```
Switch#show span-tree guard 3/13
```

Port	VLAN	Port-State	Guard Type
3/13	2	forwarding	loop

Preventing STP Failures Caused by Unidirectional Links

This topic compares the features of loop guard and UDLD as they protect against unidirectional links.

Comparing Loop Guard and UDLD		
	Loop Guard	UDLD
Configuration	Per port	Per port
Action granularity	Per VLAN	Per Port
Autorecovery	Yes	Yes, with erddisable timeout feature
Protection against STP failures caused by unidirectional links	Yes, when enabled on all root and alternative ports in redundant topology	Yes, when enabled on all links in redundant topology
Protection against STP failures caused by problem in software, resulting in designated switch not sending BPDU	Yes	No
Protection against miswiring	No	Yes

© 2006 Cisco Systems, Inc. All rights reserved. BCM5N v3.0—8-10

The functions of UDLD and loop guard partially overlap in that both protect against STP failures caused by unidirectional links. These two features are different in their approach to the problem and also in the way they function. The figure identifies the key differences.

Depending on various design considerations, you can choose either UDLD or loop guard. UDLD provides no protection against STP failures that are caused by software and that result in the designated switch not sending BPDUs. This type of failure, however, is less common than problems caused by hardware failure.

On an EtherChannel bundle, UDLD will disable individual failed links. The channel itself remains functional if other links are available. Loop guard will put the entire channel in a loop-inconsistent state if any physical link in the bundle fails.

Loop guard does not work on shared links or a link that has been unidirectional since its initial setup. Enabling both UDLD and loop guard provides the highest level of protection.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

- **UDLD detects and disables an interface with unidirectional connectivity, protecting the network from anomalous STP conditions.**
- **Loop guard detects and disables an interface with Layer 2 unidirectional connectivity, protecting the network from anomalous STP conditions.**
- **UDLD and loop guard are configured and verified using specific commands.**
- **Implementation of UDLD and loop guard protects spanning tree operations from being disrupted due to unidirectional links.**

Securing Network Switches

Overview

The devices on any network must be secured. A number of vulnerabilities can be reduced by setting passwords on physical and virtual ports, by disabling unneeded services, by forcing the encryption of sessions, and by enabling logging at the device level.

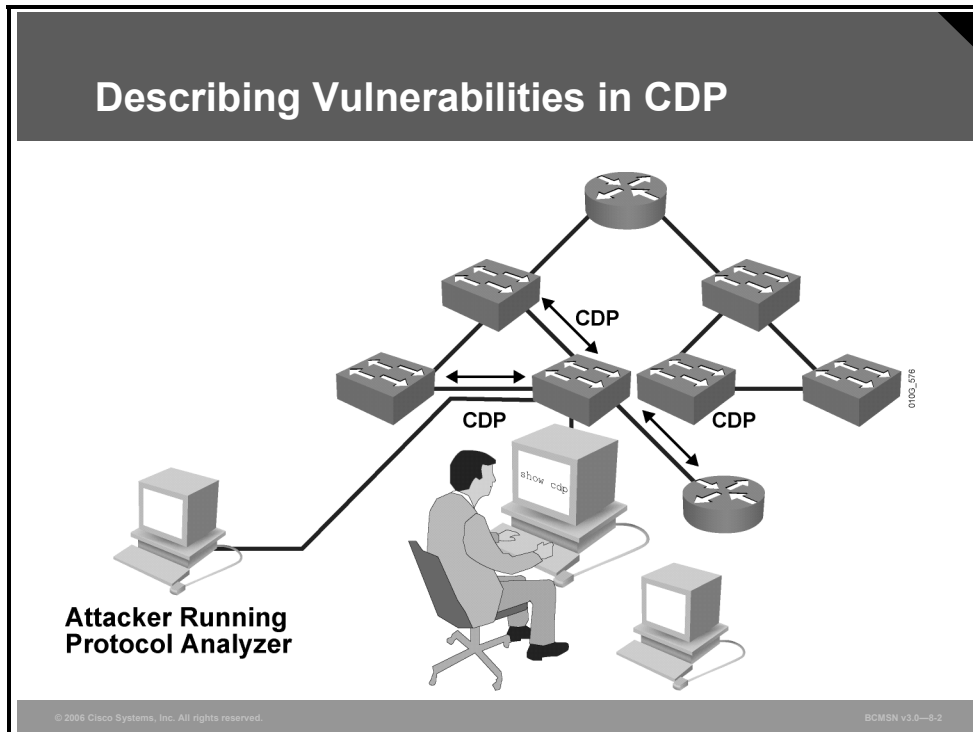
Objectives

Upon completing this lesson, you will be able to identify switch security risks and list best practices for placing new switches into service. This ability includes being able to meet these objectives:

- Describe how CDP can be used for an attack against a network
- Describe the security vulnerabilities in the Telnet option
- Describe security vulnerabilities in the SSH
- Describe vty ACLs
- Describe the commands used to apply ACLs to vty
- Describe general security considerations that should be applied in any switched network

Describing Vulnerabilities in the CDP

This topic describes how the Cisco Discovery Protocol (CDP) can be used for an attack against a network.



Attackers with knowledge of how CDP works could find ways to take advantage of the clear-text CDP packets to gain knowledge of the network. The CDP runs at Layer 2 and allows Cisco Systems devices to identify themselves to other Cisco devices. However, the information sent through CDP is transmitted in clear text and is unauthenticated. Utilizing a packet analyzer, attackers could glean information about the network device from CDP advertisements.

CDP is necessary for management applications and cannot be disabled without impairing some network-management applications. However, CDP can be selectively disabled on interfaces where management is not being performed.

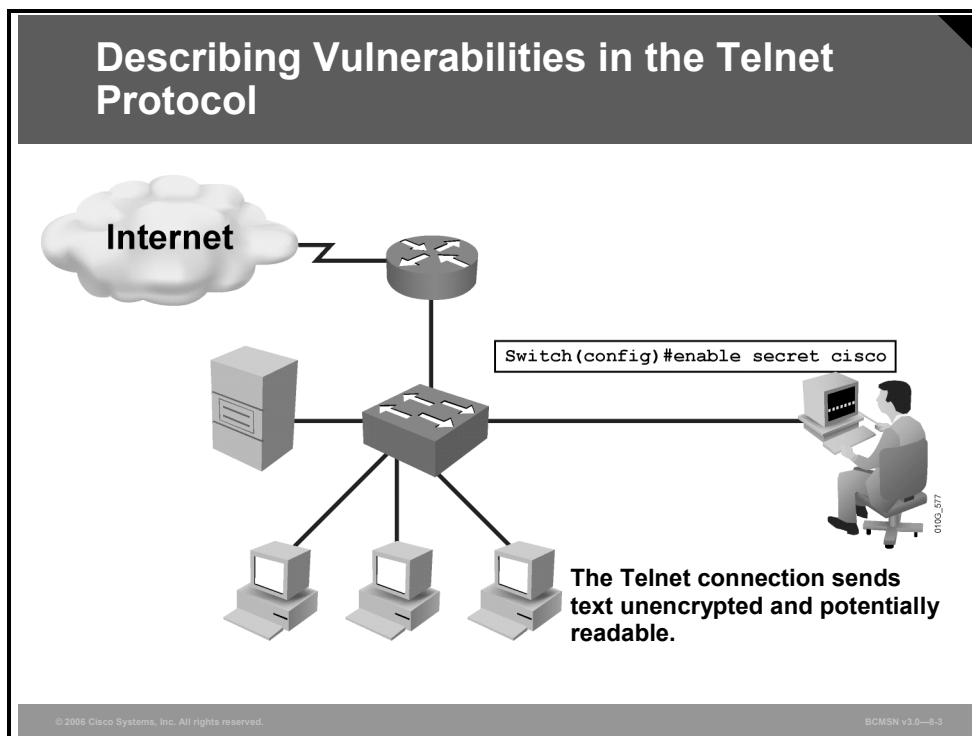
Using CDP Maliciously

The table describes how CDP can be used maliciously.

Sequence of Events	Description
1.	System administrator uses CDP to view neighbor information.
2.	Attacker uses a packet analyzer to intercept CDP traffic.
3.	Attacker analyzes information in CDP packets to gain knowledge of network address and device information.
4.	Attacker formulates attacks based on known vulnerabilities of network platforms.

Describing Vulnerabilities in the Telnet Protocol

This topic describes the security vulnerabilities in the Telnet option.

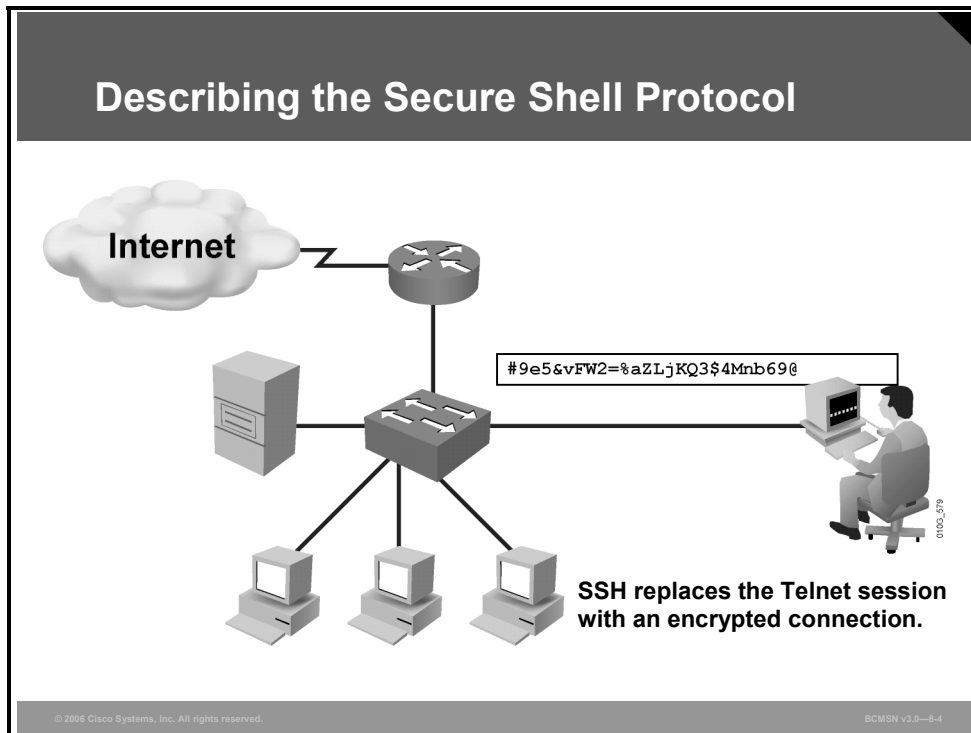


Known Telnet vulnerabilities are listed here.

- All usernames, passwords, and data that are sent over the public network in clear text are vulnerable.
- A user with an account on the system could gain elevated privileges.
- A remote attacker could crash the Telnet service, preventing legitimate use of that service.
- A remote attacker could find an enabled guest account that may be present anywhere within the trusted domains of the server.

Describing Vulnerabilities in the SSH

This topic describes security vulnerabilities in the Secure Shell Protocol (SSH).



SSH is a client and server protocol used to log in to another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. It is a replacement for rlogin, rsh, rcp, and rdist in addition to Telnet.

When using the SSH login (instead of Telnet), the entire login session, including transmission of password, is encrypted; therefore, it is almost impossible for an outsider to collect passwords.

Although SSH is secured, many vendors' implementations of SSH contain vulnerabilities that could allow a remote attacker to execute arbitrary code with the privileges of the SSH process or to cause a denial of service. Most of the SSH vulnerabilities have been addressed in the latest Cisco IOS software and in other vendors' SSH server and client software.

Caution SSH version 1 implementations are vulnerable to various security compromises. Whenever possible, use SSH version 2 instead of SSH version 1.

To activate SSH on a vty interface, use the **transport input ssh** command.

Describing vty ACLs

This topic describes the security vulnerabilities in the Telnet option.

Describing vty ACLs

- **Set up standard IP ACL.**
- **Use line configuration mode to filter access with the access-class command.**
- **Set identical restrictions on every vty line.**

The diagram illustrates a network topology for Telnet access. A PC at the top is connected to a central switch. This central switch is connected to two other switches, which are in turn connected to two more switches at the bottom. A terminal window above the PC shows the command 'C:> Telnet 10.1.1.250'. One of the switches in the network is labeled with the IP address '10.1.1.250'.

© 2006 Cisco Systems, Inc. All rights reserved. BOMSN v3.0-3-5

Cisco provides access control lists (ACLs) to permit or deny Telnet access to the vty ports of a switch. Cisco devices vary in the number of vty ports that are available by default. When configuring vty ACLs, ensure that all default ports are removed or have a specific vty ACL applied.

Telnet filtering is normally considered an extended IP ACL function because it is filtering a higher-level protocol. However, because the **access-class** command is used to filter incoming Telnet sessions by source address and to apply filtering to vty lines, standard IP ACL statements can be used to control vty access. The **access-class** command also applies standard IP ACL filtering to vty lines for outgoing Telnet sessions that originate from the switch.

vty ACLs can be applied to any combination of vty lines. The same ACL can be applied globally to all vty lines, or separately to each vty line. The most common practice is to apply the same ACL to all vty lines.

Describing Commands to Apply ACLs to vty

This topic describes the commands used to apply ACLs to vtys.

Describing Commands to Apply ACLs

```
Switch(config)#access-list access-list-number
{permit | deny | remark} source [mask]
```

- **Configures a standard IP access list**

```
Switch(config)#line vty {vty# | vty-range}
```

- **Enters configuration mode for a vty or vty range**

```
Switch(config-line)#access-class access-list-number in|out
```

- **Restricts incoming or outgoing vty connections to addresses in the ACL**

© 2006 Cisco Systems, Inc. All rights reserved.BCMSN v3.0-5-6

To configure vty ACLs on a Cisco switch, create a standard IP ACL and apply the ACL on the vty interfaces. Rather than applying the ACL to a data interface, apply it to a vty line or range of lines with the **access-class** command.

Example: vty Access

In this example, permission is granted to any device on network 192.168.1.0/24 to establish a virtual terminal (Telnet) session with the switch. Of course, the user must know the appropriate passwords to enter user mode and privileged mode.

Notice that identical restrictions have been set on every vty line because the line on which the vty user will connect cannot be controlled.

The implicit *deny any* statement at the end of the access list still applies to the ACL when it is used as an access-class entry.

```
Switch(config)# access-list 12 permit 192.168.1.0 0.0.0.255
Switch(config)# line vty 0 15
Switch (config-line)# access-class 12 in
```

Note The actual number of vty lines depends on the platform and the Cisco IOS software being run.

Best Practices: Switch Security Considerations

This topic describes general security considerations that should be applied in any switched network.

Best Practices: Switch Security

Secure switch access:

- **Set system passwords.**
- **Secure physical access to the console.**
- **Secure access via Telnet.**
- **Use SSH when possible.**
- **Configure system warning banners.**
- **Use Syslog if available.**

© 2006 Cisco Systems, Inc. All rights reserved. BCMSN v3.0-8-7

Network security vulnerabilities include loss of privacy, data theft, impersonation, and loss of integrity. Basic security measures should be taken on every network to mitigate adverse effects of user negligence or acts of malicious intent.

Best practices following these general steps are required whenever placing new equipment in service.

- Step 1** Consider or establish organizational security policies.
- Step 2** Secure switch devices.
- Step 3** Secure switch protocols.
- Step 4** Mitigate compromises launched through a switch.

Organizational Security Policies

You should consider the policies of an organization when determining what level of security and what type of security should be implemented. You must balance the goal of reasonable network security against the administrative overhead that is clearly associated with extremely restrictive security measures.

A well-established security policy has these characteristics:

- Provides a process for auditing existing network security
- Provides a general security framework for implementing network security
- Defines disallowed behaviors toward electronic data
- Determines which tools and procedures are needed for the organization
- Communicates consensus among a group of key decision makers and defines responsibilities of users and administrators
- Defines a process for handling network security incidents
- Enables an enterprise-wide, all-site security implementation and enforcement plan

Secure Switch Devices

Follow these best practices for secure switch access.

- **Set system passwords:** Use the **enable secret** command to set the password that grants enabled access to the Cisco IOS system. Because the **enable secret** command simply implements a Message Digest 5 (MD5) hash on the configured password, that password still remains vulnerable to dictionary attacks. Therefore, apply standard practices in selecting a feasible password.

Try to pick passwords that contain both letters and numbers in addition to special characters, for example, “\$pecial\$” instead of “specials,” where the “s” has been replaced with “\$,” and the “l” has been replaced with “1”(one).

- **Secure access to the console:** Console access requires a minimum level of security both physically and logically. An individual who gains console access to a system will be able to recover or reset the system-enable password, thus allowing that person to bypass all other security implemented on that system. Consequently, it is imperative to secure access to the console.
- **Secure access to vty lines:** These are the minimum recommended steps for securing Telnet access.
 - Apply the basic ACL for in-band access to all vty lines.
 - Configure a line password for all configured vty lines.
 - If the installed Cisco IOS image permits, use SSH instead of Telnet to access the device remotely.
- **Use SSH:** The SSH protocol and application provide a secure remote connection to a router. Two versions of SSH are available: SSH version 1 and SSH version 2. SSH version 1 is implemented in Cisco IOS software. It encrypts all traffic, including passwords, between a remote console and a network router across a Telnet session. Because SSH sends no traffic in clear text, network administrators can conduct remote access sessions that casual observers will not be able to view. The SSH server in Cisco IOS software will work with publicly and commercially available SSH clients.

- **Configure system-warning banners:** For both legal and administrative purposes, configuring a system-warning banner to display before login is a convenient and effective way of reinforcing security and general usage policies. By clearly stating the ownership, usage, access, and protection policies before a login, you provide more solid backing for potential future prosecution.
- **Disable unneeded services:** By default, Cisco devices implement multiple TCP and User Datagram Protocol (UDP) servers to facilitate management and integration into existing environments. For most installations, these services are typically not required, and disabling them can greatly reduce overall security exposure. These commands will disable the services not typically used:

```
no service tcp-small-servers
no service udp-small-servers
no service finger
no service config
```

- **Disable the integrated HTTP daemon if not in use:** Although Cisco IOS software provides an integrated HTTP server for management, it is highly recommended that it be disabled to minimize overall exposure. If HTTP access to the switch is absolutely required, use basic ACLs to permit access from only trusted subnets.
- **Configure basic logging:** To assist and simplify both problem troubleshooting and security investigations, monitor the switch subsystem information received from the logging facility. View the output in the on-system logging buffer memory. To render the on-system logging useful, increase the default buffer size.

Secure Switch Protocols

This subtopic continues a discussion of best practices for switch security.

Best Practices: Switch Security (Cont.)

Secure switch protocols:

- Trim CDP and use only as needed.
- Secure spanning tree.

Mitigate compromises through a switch:

- Take precautions for trunk links.
- Minimize physical port access.
- Establish standard access port configuration for both unused and used ports.

© 2006 Cisco Systems, Inc. All rights reserved.

BCMSN v3.0-3-8

Follow these best practices for switch security.

- **CDP:** CDP does not reveal security-specific information, but it is possible for an attacker to exploit this information in a reconnaissance attack, whereby an attacker learns device and IP address information for the purpose of launching other types of attacks. Two practical guidelines should be followed for CDP.
 - If CDP is not required, or if the device is located in an unsecure environment, disable CDP globally on the device.
 - If CDP is required, disable CDP on a per-interface basis on ports connected to untrusted networks. Because CDP is a link-level protocol, it is not transient across a network (unless a Layer 2 tunneling mechanism is in place). Limit it to run between trusted devices only, and disable it everywhere else. However, CDP is required on any access port when you are attaching a Cisco phone to establish a trust relationship.
- **Secure the spanning tree topology:** It is important to protect the Spanning Tree Protocol (STP) process of the switches that compose the infrastructure. Inadvertent or malicious introduction of STP bridge protocol data units (BPDUs) could potentially overwhelm a device or pose a denial of service (DoS) attack. The first step in stabilizing a spanning tree installation is to positively identify the intended root bridge in the design and to hard set the STP bridge priority of that bridge to an acceptable root value. Do the same for the designated backup root bridge. These actions will protect against inadvertent shifts in STP caused by an uncontrolled introduction of a new switch.

On some platforms, the BPDU guard feature may be available. If so, enable it on access ports in conjunction with the PortFast feature to protect the network from unwanted BPDU traffic injection. Upon receipt of a BPDU, the feature will automatically disable the port.

Mitigating Compromises Launched Through a Switch

Follow these best practices to mitigate compromises through a switch.

- **Proactively configure unused router and switch ports.**
 - Execute the **shut** command on all unused ports and interfaces.
 - Place all unused ports in a "parking-lot" VLAN used specifically to group unused ports until they are proactively placed into service.
 - Configure all unused ports as access ports, disallowing automatic trunk negotiation.
- **Considerations for trunk links:** By default, Cisco Catalyst switches running Cisco IOS software are configured to automatically negotiate trunking capabilities. This situation poses a serious hazard to the infrastructure because an unsecured third-party device can be introduced to the network as a valid infrastructure component. Potential attacks include interception of traffic, redirection of traffic, DoS, and more. To avoid this risk, disable automatic negotiation of trunking and manually enable it on links that will require it. Ensure that trunks use a native VLAN that is dedicated exclusively to trunk links.
- **Physical device access:** Physical access to the switch should be closely monitored to avoid rogue device placement in wiring closets with direct access to switch ports.
- **Access port–based security:** Specific measures should be taken on every access port of any switch placed into service. Ensure that a policy is in place outlining the configuration of unused switch ports in addition to those that are in use.

For ports enabled for end-device access, there is a macro called **switchport host**, which, when executed on a specific switch port, takes these actions: sets the switch port mode to access, enables spanning tree PortFast, and disables channel grouping.

Note The **switchport host** macro disables EtherChannel, disables trunking, and enables STP PortFast.

The command is a macro that executes several configuration commands. There is no command such as **no switchport host** to revoke the effect of the **switchport host** command. To return an interface to its default configuration, use the **default interface** *interface-id* global configuration command. This command returns all interface configurations to the default.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

- **CDP packets can expose some network information.**
- **Authentication information and data carried in Telnet sessions are vulnerable.**
- **SSH provides a more secure option for Telnet.**
- **vtY ACLs should be used to limit Telnet access to switch devices.**
- **vtY ACL configuration commands use standard IP ACL lists.**
- **Sound security measures and trimming of unused applications are the basis of best practices.**

Module Summary

This topic summarizes the key points that were discussed in this module.

Module Summary

- **Key switch security issues should be identified on a switched network and proper measures taken to mitigate known attacks.**
- **VLAN trunk links should be secured to defend against VLAN hopping attacks.**
- **DHCP snooping, port security, and dynamic ARP inspection are used to protect the network against spoofing attacks.**
- **When placed into service, switches should be configured according to best practices to secure the switch device and its protocols from attacks that can be launched through a switch.**
- **UDLD and loop guard protect the network from anomalous STP conditions that result from unidirectional links.**
- **Implement AAA services to support port authentication using 802.1x.**

© 2006 Cisco Systems, Inc. All rights reserved. BOMSN v3.0—3-1

This module covered the major vulnerabilities to unsecure VLAN topologies. MAC spoofing, Address Resolution Protocol (ARP) spoofing, and DHCP spoofing are used by hackers to disrupt the network and to gain access.

Using port security, dynamic ARP inspection (DAI), DHCP snooping, and IP source guard helps to eliminate the chances of such attacks occurring.

VLAN access control lists (VACLs) and private VLANs (PVLANS) are also used to filter and control VLAN traffic.

In addition, the use of vty ACLs and Secure Shell Protocol (SSH) helps in controlling connectivity to the network devices used in the topology.

References

For additional information, refer to these resources:

- Cisco Systems, Inc., *Configuring Port Security*:
http://cisco.com/en/US/products/hw/switches/ps4324/products_configuration_guide_chapter09186a008019d0de.html
- Cisco Systems, Inc., *SAFE Layer 2 Security In-depth Version 2*:
http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008014870f.shtml
- Cisco Systems, Inc., *Configuring 802.1X Port-Based Authentication*:
http://www.cisco.com/en/US/partner/products/hw/switches/ps628/products_configuration_guide_chapter09186a00800d84b9.html
- Cisco Systems, Inc., *VLAN Security White Paper*:
http://cisco.com/en/US/partner/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml
- Cisco Systems, Inc., *Configuring Private VLANs (4500 series)*:
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/12_1_13/config/pvlans.htm
- Cisco Systems, Inc., *Understanding and Configuring DHCP Snooping*:
http://cisco.com/en/US/partner/products/hw/switches/ps663/products_configuration_guide_chapter09186a00800dde9f.html#30724
- Cisco Systems, Inc., *Configuring DAI (4500)*:
http://cisco.com/en/US/partner/products/hw/switches/ps4324/products_configuration_guide_chapter09186a008019d0ca.html

Module Self-Check

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

- Q1) Which feature supported on Cisco Catalyst switches restricts a switch port to a specific set or number of MAC addresses? (Source: Understanding Switch Security Issues)
- A) port security
 - B) DHCP snooping
 - C) PVLAN
 - D) VACL
- Q2) What is one best practice to mitigate VLAN hopping? (Source: Protecting Against VLAN Attacks)
- A) configure all unused ports as trunks
 - B) shut down all unused ports
 - C) set trunks to “negotiate” and not “on”
 - D) set the interface speed to 10 Mbps
- Q3) What are three ways to protect against spoofing attacks? (Source: Protecting Against Spoof Attacks)
- Q4) Which two options are valid for improving STP security. (Choose two.) (Source: Describing STP Security Mechanisms)
- A) BPDU guard
 - B) MAC filtering
 - C) root guard
 - D) UDLD
- Q5) Which two features apply to loop guard? (Choose two.) (Source: Preventing STP Forwarding Loops)
- A) It allows a blocked port in a physically redundant topology to stop receiving BPDUs.
 - B) It provides additional protection against Layer 2 STP loops.
 - C) It moves ports into the STP loop-inconsistent state if BPDUs are not received on a nondesignated port.
 - D) It enables the blocking port to move to a forwarding state.
- Q6) To provide secure, strong authentication and secure communications over insecure channels, instead of Telnet use _____. (Source: Securing Network Switches)
-

Module Self-Check Answer Key

- Q1) A
- Q2) B
- Q3) DHCP snooping, port security, DAI
- Q4) A, C
- Q5) A, C
- Q6) SSH