

ONT

Optimizing Converged Cisco Networks

Volume 2

Version 1.0

Student Guide

EPGS Production Services: 07.25.06

**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

Implement Cisco AutoQoS **5-1**

Overview	5-1
Module Objectives	5-1

Introducing Cisco AutoQoS **5-3**

Overview	5-3
Objectives	5-3
Cisco AutoQoS	5-4
Automating the Delivery of Network QoS	5-5
Cisco AutoQoS Evolution	5-6
Automating the Key Elements of QoS Deployment	5-7
Protocol Discovery with NBAR	5-9
Cisco AutoQoS for the Enterprise: Router Deployment Restrictions	5-10
Router Deployment Restrictions	5-10
Router Design Considerations	5-12
Router Prerequisites	5-14
Deploying Cisco AutoQoS for the Enterprise on Routers: A Two-Step Approach	5-16
Configuring Cisco AutoQoS: Traffic Profiling on Routers with Autodiscovery	5-17
Configuring Cisco AutoQoS: Configuring QoS Policies on Routers	5-19
Example: Cisco AutoQoS for the Enterprise Router Configuration	5-20
Deploying Cisco AutoQoS VoIP on Switches	5-22
Configuring Cisco AutoQoS on Cisco Catalyst Switches	5-23
Example: Cisco AutoQoS VoIP Switch Configuration	5-24
Verifying Cisco AutoQoS	5-25
Monitoring Cisco AutoQoS on Routers	5-26
Monitoring Cisco AutoQoS on Switches	5-29
Summary	5-32
References	5-32

Mitigating Common Cisco AutoQoS Issues **5-33**

Overview	5-33
Objectives	5-33
Automation with Cisco AutoQoS	5-34
DiffServ QoS Mechanisms Enabled by Cisco AutoQoS	5-36
Automated Cisco AutoQoS DiffServ Class Provisioning	5-40
Common Cisco AutoQoS Issues	5-41
Interpreting Cisco AutoQoS Configurations	5-43
How to Interpret the show auto qos Command Output	5-44
Modifying the Active Cisco AutoQoS Configuration with MQC	5-46
Modifying the Active Cisco AutoQoS Configuration with MQC: Classification	5-47
Modifying the Active Cisco AutoQoS Configuration with MQC: Policy	5-51
Summary	5-54
References	5-54
Module Summary	5-55
Module Self-Check	5-56
Module Self-Check Answer Key	5-59

Implement Wireless Scalability **6-1**

Overview	6-1
Module Objectives	6-1

Implementing WLAN QoS **6-3**

Overview	6-3
Objectives	6-3
The Need for WLAN QoS	6-4
WLAN QoS Description	6-6
WLAN QoS RF Backoff Timing	6-8
Lightweight Access Point—Split MAC Architecture	6-9
QoS WLAN Deployment Issues	6-10

QoS Description	6-11
WLAN QoS Implementation	6-12
QoS Implementation—Ethernet to Controller	6-13
From Access Point to Wireless Client	6-15
From Client to Access Point	6-16
Traffic from Access Point to Controller	6-17
From Controller to Ethernet Switch	6-18
QoS Implementation	6-19
WLAN QoS Configuration	6-21
QoS-Configurable Profiles	6-21
Configuring WLAN IDs for QoS	6-24
Summary	6-25
Introducing 802.1x	6-27
Overview	6-27
Objectives	6-27
The Need for WLAN Security	6-28
Security Methods—Authentication and Encryption	6-29
WLAN Security Issues	6-30
WEP Attacks	6-32
Overview of WLAN Security	6-34
802.11 WEP	6-35
WLAN Authentication	6-36
802.11 Shared Key Authentication	6-37
Cisco Enhanced 802.11 WEP Security	6-38
Enhanced 802.11 Security	6-39
Encryption—TKIP and MIC	6-41
Encryption—AES	6-42
802.1x Overview	6-43
802.1x Authentication Key Benefits	6-44
802.1x and EAP Authentication Protocols	6-45
Components Required for 802.1x Authentication	6-46
LEAP	6-47
Cisco LEAP Authentication	6-48
EAP-FAST	6-49
EAP-FAST Authentication	6-50
EAP-TLS	6-51
EAP-TLS Authentication	6-52
PEAP	6-53
EAP-PEAP Authentication	6-54
Wi-Fi Protected Access	6-55
WPA Characteristics	6-55
802.11i or WPA Authentication and Key Management Overview	6-56
WPA Issues	6-58
Wireless IDSs	6-61
WPA and WPA2 Modes	6-62
WPA2 Issues	6-63
Summary	6-64
References	6-65
Configuring Encryption and Authentication on Lightweight Access Points	6-67
Overview	6-67
Objectives	6-67
Open Authentication	6-68
Static WEP Key Authentication	6-69
WPA Preshared Key	6-70
Web Authentication	6-71
802.1x Authentication	6-74
WPA with 802.1x	6-75
WPA2	6-76
Summary	6-77

Managing WLANs	6-79
Overview	6-79
Objectives	6-79
Cisco Unified Wireless Network	6-81
Business Drivers	6-81
Cisco Unified Wireless Network Components	6-83
Cisco WLAN Implementation	6-85
Describing WLAN Components	6-86
Comparison of the WLAN Solutions	6-87
CiscoWorks WLSE	6-88
CiscoWorks WLSE Key Benefits	6-89
CiscoWorks WLSE and WLSE Express	6-90
Simplified CiscoWorks WLSE Express Setup	6-92
Configuration Templates	6-93
CiscoWorks WLSE Benefits	6-95
Cisco WCS	6-96
Overview of Cisco WCS	6-96
Cisco WCS Location Tracking Options	6-97
Cisco WCS Base Software Features	6-98
Cisco WCS Location Software Features	6-100
Cisco WCS System Features	6-101
Cisco WCS Network Summary Page	6-103
Cisco WCS Controller Summary Page	6-104
Cisco Wireless Location Appliance	6-105
Cisco Wireless Location Appliance Architecture	6-106
Cisco Wireless Location Appliance Applications	6-108
Cisco WCS Configuration Example	6-110
Cisco WCS Server Login	6-110
Cisco WCS Network Summary	6-111
Adding a Cisco Wireless LAN Controller to Cisco WCS	6-112
Configuring a Cisco Access Point	6-114
Cisco WCS Maps	6-115
Adding a Campus Map to the Cisco WCS Database	6-115
Adding New Building to the Cisco WCS Database	6-117
Rogue Access Point Detection	6-119
Rogue Access Point Alarms	6-120
Rogue Access Point Location	6-121
Summary	6-122
References	6-122
Module Summary	6-123
Module Self-Check	6-124
Module Self-Check Answer Key	6-125

Implement Cisco AutoQoS

Overview

Cisco AutoQoS represents innovative technology that simplifies network administration challenges, reducing quality of service (QoS) complexity, deployment time, cost in enterprise networks, and human error. Cisco AutoQoS automates the deployment of QoS policies in a general business environment, particularly for midsize companies and branch offices of larger companies.

Module Objectives

Upon completing this module, you will be able to configure Cisco AutoQoS for enterprises. This ability includes being able to meet these objectives:

- Identify the capabilities provided by Cisco AutoQoS and explain the procedure to configure QoS on a network using Cisco AutoQoS
- Explain how to tune a Cisco AutoQoS configuration after specific issues in the configuration have been identified by reading through the **show** command output

Introducing Cisco AutoQoS

Overview

Cisco AutoQoS represents innovative technology that simplifies network administration challenges, reducing quality of service (QoS) complexity, deployment time, and overall cost in enterprise networks. Cisco AutoQoS incorporates value-added intelligence in Cisco IOS software and Cisco Catalyst software to provision and manage large-scale QoS deployments. Cisco AutoQoS provides QoS provisioning for individual routers and switches, simplifying deployment and reducing human error. This lesson explores the capabilities of Cisco AutoQoS and the requirements for configuring QoS on a network.

Objectives

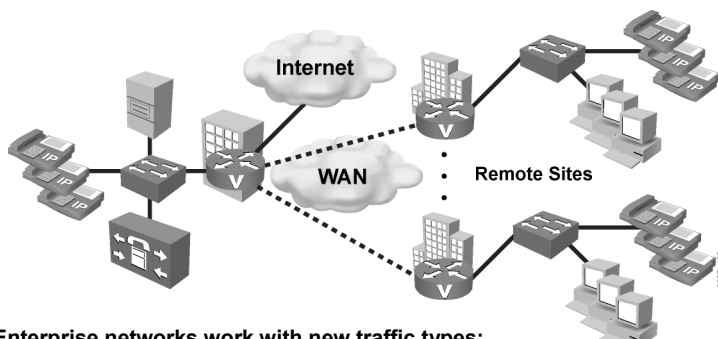
Upon completing this lesson, you will be able to identify the capabilities provided by Cisco AutoQoS and explain the procedure to configure QoS on a network using Cisco AutoQoS. This ability includes being able to meet these objectives:

- Explain how Cisco AutoQoS is used to implement QoS policy
- Describe the prerequisites for using Cisco AutoQoS and how it is configured on a network using the CLI
- Describe how to verify that Cisco AutoQoS is functioning on a network

Cisco AutoQoS

This topic describes how Cisco AutoQoS is used to implement QoS policy.

Enterprise QoS Challenges



The diagram illustrates an enterprise network topology. It features a central cloud labeled 'Internet' connected to a 'WAN' cloud. The WAN cloud is connected to two 'Remote Sites'. Each Remote Site contains a central router (marked with a 'V') and several desktop computers (marked with 'IP'). The network is also connected to a central server rack. The diagram uses various icons to represent different network components and traffic types.

- **Enterprise networks work with new traffic types:**
 - IP telephony spreads quickly and requires QoS.
 - Mission-critical applications need guaranteed bandwidth.
- **QoS implementation requires significant “challenging” knowledge:**
 - Simple networks require a simple QoS solution that works instantly.
 - QoS deployment should be cheaper and faster.

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0-6-3

Customer networks need to service application requirements and end users efficiently. The tremendous growth of the Internet and corporate intranets, the wide variety of new bandwidth-hungry applications, and convergence of data, voice, and video traffic over consolidated IP infrastructures have had a major impact on the ability of networks to provide predictable, measurable, and guaranteed services to these applications. Achieving the required quality of service (QoS) through the proper management of network delays, bandwidth requirements, and packet loss parameters while maintaining simplicity, scalability, and manageability of the network is the fundamental solution to providing an infrastructure that serves business applications from end to end.

Major enterprise QoS challenges include these:

- Voice quality for IP telephony applications
- Guaranteed bandwidth for mission-critical applications
- Simpler QoS deployments (reducing operator errors)
- Inexpensive QoS deployments (reducing costs)
- Fast QoS deployments (reducing deployment time)

Automating the Delivery of Network QoS

Cisco AutoQoS automates the deployment of QoS policies in a general business environment, particularly for midsize companies and branch offices of larger companies.

Cisco AutoQoS: Automating the Delivery of Network QoS

Cisco AutoQoS—QoS for voice, video, and data:

- **Uses Cisco IOS built-in intelligence to automate QoS delivery for most common business scenarios**
- **Protects business-critical data applications in the enterprise**
- **Simplifies QoS deployment for real-time traffic**
- **Reduces configuration errors**
- **Makes QoS deployments simpler, cheaper, and faster**
- **Follows DiffServ model and other standards in QoS**
- **Allows customers to retain complete control over their QoS configuration**

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0—5-4

There are several key benefits of Cisco AutoQoS:

- Cisco AutoQoS incorporates value-added intelligence in Cisco IOS Software and Cisco Catalyst operating system software to provision and manage QoS deployments.
- Cisco AutoQoS protects the business-critical data applications in the enterprise to maximize their availability among other applications of less priority.
- Cisco AutoQoS provides QoS provisioning for individual routers and switches, simplifying QoS deployment.
- Customers can implement the QoS features required for voice, video, and data traffic without an in-depth knowledge of the underlying technologies (PPP, Frame Relay, ATM, service policies, and link efficiency mechanisms, such as link fragmentation and interleaving [LFI]).
- Cisco AutoQoS simplifies QoS implementation and speeds up the provisioning of QoS technology over a Cisco network. It reduces the potential for human error and lowers training costs.
- Cisco AutoQoS creates class maps and policy maps on the basis of Cisco experience and best-practices methodology. AutoQoS, in creating the QoS configuration, follows industry standards such as the Differentiated Services (DiffServ) model to achieve interoperable environment.
- Customers can also use existing Cisco IOS commands to modify the configurations automatically generated by the Cisco AutoQoS, as needed to meet specific requirements.

Cisco AutoQoS Evolution

Cisco AutoQoS has evolved in two support phases: Cisco AutoQoS VoIP and Cisco AutoQoS for the Enterprise.

Cisco AutoQoS Evolution

- **Cisco AutoQoS VoIP:**
 - **First phase addressed IP telephony.**
 - **One command provisions all basic QoS required.**
 - **Support is provided across broad range of platforms (switches and routers).**
- **Cisco AutoQoS for Enterprise:**
 - **Second phase extends capabilities (routers only) for data, voice, and video.**
 - **Two QoS deployment stages:**
 - **Discovers traffic types, load, and generates policy (NBAR)**
 - **Implements the generated policy**

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0—5-5

The first phase of Cisco AutoQoS offers straightforward capabilities to automate VoIP deployments for customers who want to deploy IP telephony but who lack the expertise or staffing to plan and deploy IP QoS and IP services. Cisco AutoQoS VoIP is the first release of Cisco AutoQoS and automates QoS settings for VoIP deployments only. This feature automatically generates interface configurations, policy maps, class maps, and access control lists (ACLs). Cisco AutoQoS VoIP automatically employs Cisco Network-Based Application Recognition (NBAR) to classify voice traffic and mark it with the appropriate differentiated services code point (DSCP) value. Cisco AutoQoS VoIP can be instructed to rely on, or trust, the DSCP markings previously applied to the packets.

The second phase of Cisco AutoQoS expands its capabilities beyond VoIP and it addresses the QoS requirements of enterprise converged networks. Cisco AutoQoS for the Enterprise adds an important step—users can observe the applications that have been discovered during the observation phase (autodiscovery), and review the QoS policy that Cisco AutoQoS for the Enterprise suggests without deploying that policy. Cisco AutoQoS for the Enterprise blends the design and implementation of QoS, based on the most common enterprise scenarios, into two major steps:


- It automatically discovers which applications are used in the enterprise network and generates optimal policy. This step employs the NBAR discovery mechanism.
- It implements the generated policy.

Automating the Key Elements of QoS Deployment

Cisco AutoQoS addresses the five key elements of QoS deployment.

Cisco AutoQoS: Automating the Key Elements of QoS Deployment

1. **Application classification:**
Discovers applications and provides appropriate QoS treatment
2. **Policy generation:** Autogenerates initial and ongoing QoS policies
3. **Configuration:** Provides high-level business knobs, and automates QoS in multidevice domain
4. **Monitoring and reporting:** Generates intelligent, automatic alerts and summary reports
5. **Consistency:** Enables automatic, seamless interoperability among all QoS features and parameters



© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0-5-6

Application Classification

Cisco AutoQoS uses intelligent classification on routers, utilizing NBAR to provide deep and stateful packet inspection. Cisco AutoQoS uses Cisco Discovery Protocol (CDP) for voice packets, helping ensure that the device attached to the LAN is really a Cisco IP phone.

Policy Generation

Cisco AutoQoS evaluates the network environment and generates an initial policy. It automatically determines WAN settings for fragmentation, compression, encapsulation, and Frame Relay-ATM interworking, eliminating the need to understand QoS theory and design practices in various scenarios. Customers can meet additional or special requirements by modifying the initial policy as they normally would.

Configuration

With one command, Cisco AutoQoS configures the interface to prioritize critical traffic while still offering the flexibility to adjust QoS settings for unique network requirements.

Cisco AutoQoS not only automatically detects Cisco IP phones and enables QoS settings for the port of the phone, it will also disable those QoS settings to prevent malicious activity when a Cisco IP phone is relocated or moved.

Monitoring and Reporting

Cisco AutoQoS provides visibility into the classes of service deployed using system logging and Simple Network Management Protocol (SNMP) traps, with notification of abnormal events (for example, VoIP packet drops).

Cisco QoS Policy Manager (QPM) is the QoS monitoring platform, which uses the Cisco intelligent IP network to provide visibility into network operations. You can measure traffic throughput for top applications and service classes. You can also troubleshoot problems with real-time and historical QoS feedback. Traffic and QoS statistics can be displayed as line or bar charts, in bits or packets per second, per interface or policy. Cisco QPM enables you to view graphs before and after QoS deployment, tied to traffic filters and policies, as well as results from QoS policy actions.

Consistency

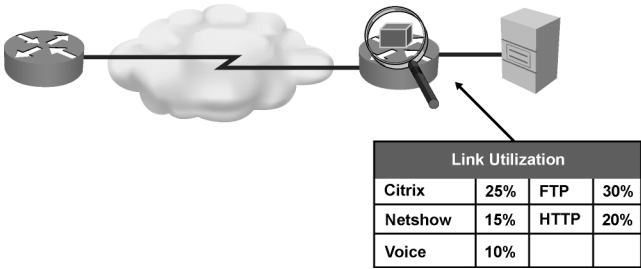
Cisco AutoQoS policies are designed to work together across Cisco devices, helping ensure consistent end-to-end QoS. Cisco QPM enables users to view the following:

- Statistics matching policies and specific filters, including NBAR application filters
- Traffic rate before any QoS policy actions, traffic transmitted after QoS policy actions, and traffic dropped (rather than transmitted) because of QoS policy drop actions
- QoS action statistics: weighted random early detection (WRED), policing, traffic shaping, and queuing

Protocol Discovery with NBAR

NBAR Protocol Discovery is a commonly used NBAR feature that collects application and protocol statistics (that is, packet counts, byte counts, and bit rates) per interface. It enables you to generate real-time statistics on the applications in the network. It also gives you an idea of the traffic distribution at key points in the enterprise network. NBAR is an important element in many Cisco initiatives, including Cisco Service-Oriented Network Architecture (SONA). Protocol Discovery has the application-specific intelligence to discover traffic types and is tightly integrated into Cisco QoS solutions.

Protocol Discovery with NBAR



Citrix	25%	FTP	30%
Netshow	15%	HTTP	20%
Voice	10%		

- Analyzes application traffic patterns in real time and discovers which traffic is running on the network
- Identifies Layer 4–7 applications and protocols using stateful and deep packet inspection
- Provides bidirectional, per-interface, and per-protocol statistics:
 - 5-minute bit rate (bps)
 - Packet counts
 - Byte counts
- Currently supports almost 100 protocols and applications

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0–5-7

The Protocol Discovery feature discovers any protocol traffic supported by NBAR. Protocol Discovery can be applied to interfaces and can be used to monitor both input and output traffic. Protocol Discovery maintains these per-protocol statistics for enabled interfaces:

- Input and output bit rates
- Total number of input and output packets and bytes

NBAR is capable of discovering and classifying these types of applications:

- Static applications that establish sessions to well-known TCP or User Datagram Protocol (UDP) destination port numbers are recognized.
- Dynamic applications that use multiple sessions using dynamic TCP or UDP port numbers are recognized. Typically, there is a control session to a well-known port number and the other sessions are established to destination port numbers negotiated through the control sessions. NBAR inspects the port number exchange through the control session.
- Some applications using non-IP protocols can also be recognized by NBAR.
- NBAR has the ability to inspect some applications for other information and to discover them based on that information; for example, HTTP sessions based on the requested URL, including Multipurpose Internet Mail Extension (MIME) type or host name.

Cisco AutoQoS for the Enterprise: Router Deployment Restrictions

This topic describes the prerequisites for using Cisco AutoQoS and how to configure it on a network using the command-line interface (CLI).

Router Deployment Restrictions

Cisco AutoQoS automates the whole QoS configuration process, but it has some restrictions.

Cisco AutoQoS on Enterprise: Router Deployment Restrictions	
	Restrictions
General restrictions	<ul style="list-style-type: none">• Supports PPP, HDLC, Frame Relay, and ATM PVC only• Interface or PVC must have an IP address
Serial interface restrictions	<ul style="list-style-type: none">• Must be configured on both ends of the link• Must have the bandwidth configured to the same value on both ends
Frame Relay DLCI restrictions	<ul style="list-style-type: none">• Cannot be configured on a DLCI if a map class or virtual template is attached to the DLCI• Cannot be configured if DLCI is already assigned to a subinterface
ATM PVC restrictions	<ul style="list-style-type: none">• Cannot be configured if a virtual template is already attached to the low-speed PVC (less than 768 kbps)

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0-5.9

General Restrictions

The feature is supported on these interfaces, data-link connection identifiers (DLCIs), and permanent virtual circuits (PVCs) only:

- Serial interfaces with PPP or High-Level Data Link Control (HDLC)
- Frame Relay point-to-point subinterfaces only
- Low-speed and high-speed ATM PVCs in point-to-point subinterfaces

Note Synchronous serial interfaces are classified as low speed if the bandwidth is less than or equal to 768 kbps. A synchronous serial interface is classified as high speed if its bandwidth is greater than 768 kbps. This classification is also true for ATM PVCs.

- Frame Relay-to-ATM interworking links

Serial Interface Restrictions

For a serial interface with a low-speed link, Multilink PPP (MLP) is configured automatically. The serial interface must have an IP address. When MLP is configured, this IP address is removed and put on the MLP bundle. To ensure that the traffic goes through the low-speed link, these conditions must be met:

- Cisco AutoQoS for the Enterprise must be configured at the both ends of the link.
- The amount of bandwidth configured must be the same on both ends of the link.

Frame Relay DLCI Restrictions

Cisco AutoQoS has the following restrictions in Frame Relay environment:

- Cisco AutoQoS cannot be configured on a Frame Relay DLCI if a map class is attached to the DLCI.
- If a Frame Relay DLCI is already assigned to one subinterface, Cisco AutoQoS VoIP cannot be configured from a different subinterface.
- For low-speed Frame Relay DLCIs configured for use on Frame Relay-to-ATM interworking, MLP over Frame Relay is configured automatically. The subinterface must have an IP address.
- When MLP over Frame Relay is configured, this IP address is removed and put on the MLP bundle. Cisco AutoQoS must also be configured on the ATM side of the network.
- For low-speed Frame Relay DLCIs with Frame Relay-to-ATM interworking, Cisco AutoQoS cannot be configured if a virtual template is already configured for the DLCI.

ATM PVC Restrictions

Cisco AutoQoS has the following restrictions in ATM environment:

- For a low-speed ATM PVC, Cisco AutoQoS cannot be configured if a virtual template is already configured for the ATM PVC.
- For low-speed ATM PVCs, MLP over ATM is configured automatically. The subinterface must have an IP address.
- When MLP over ATM is configured, this IP address is removed and put on the MLP bundle.

Router Design Considerations

When you are configuring Cisco AutoQoS, some design considerations for Cisco router platforms should be taken into account.

Cisco AutoQoS: Router Design Considerations	
	Considerations
General QoS requirements	<ul style="list-style-type: none">• Considers interface type and the bandwidth configured• Uses the bandwidth configured to determine the resulting configuration
Bandwidth implications	<ul style="list-style-type: none">• Uses the bandwidth that is allocated at the time the feature is enabled• Does not respond to later bandwidth changes
Fragmentation for Frame Relay networks	<ul style="list-style-type: none">• For Frame Relay networks, configures LFI based on G.729 using delay of 10 ms and minimum fragment size of 60 bytes— manual adjustment needed if G.711 codec with 220-byte fragment length is required

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0—5-10

General QoS Requirements

Recommended methods and values are configured to meet the QoS requirements for real-time traffic.

Cisco AutoQoS takes the interface type and bandwidth into consideration when implementing these QoS features:

- **Low latency queuing (LLQ) priority queue:** LLQ (specifically, the priority queue) is applied to the voice packets to meet the latency requirements. LLQ is used to give a priority to voice Real-Time Transport Protocol (RTP) packets over other data traffic types when they share an output link with voice.
- **Compressed Real-Time Transport Protocol (cRTP):** With cRTP, the 40-byte IP header of the voice packet is reduced to 2 or 4 bytes, reducing voice bandwidth requirements. This mechanism is used on low-speed serial links to improve link efficiency and decrease the RTP packet overhead caused by extensive voice packet headers. cRTP must be applied at both ends of a network link.
- **LFI:** LFI is used to reduce jitter for voice packets by preventing voice packets from being delayed by large data packets in a queue when real-time voice and bursty data traffic share the same low-speed output link. LFI must be applied at both ends of a network link.

Bandwidth Implications

The bandwidth of the serial interface determines the speed of the link. The speed of the link, in turn, determines the configurations generated by Cisco AutoQoS.

Note Changing the bandwidth during configuration of Cisco AutoQoS is not recommended.

Cisco AutoQoS uses the bandwidth that is allocated at the time that the feature is configured. Cisco AutoQoS does not respond to changes made to bandwidth after the feature is configured.

Fragmentation for Frame Relay Networks

For Frame Relay networks, fragmentation is configured based on G.729 using a delay of 10 ms and a minimum fragment size of 60 bytes. This configuration ensures that the VoIP packets are not fragmented. However, when the G.711 coder-decoder (codec) is used on low-speed links, the fragment size configured by Cisco AutoQoS could be smaller than the size of the G.711 VoIP packet. To solve this potential problem, choose one of these options:

- Change the fragment size to the required value.
- Replace the G.711 codec with a codec more suitable for low-bandwidth links; for instance, G.729.

For example, if Cisco AutoQoS is configured on a Frame Relay DLCI with 128 kbps, the fragment size configured by Cisco AutoQoS for the Enterprise will be 160 bytes. The size of the G.711 VoIP packet will be 160 bytes, plus the bytes in the packet headers for the layers. The workaround is to either change the fragment size from 160 bytes to 220 bytes or use G.729 or another codec that produces packets smaller than the fragment size.

Configuring Cisco AutoQoS: Router Prerequisites

- It cannot be configured if a QoS policy (service policy) is attached to the interface.
- CEF must be enabled at the interface or ATM PVC.
- It classifies an interface as low speed (less than or equal to 768 kbps) or high speed (more than 768 kbps):
 - Correct bandwidth must be configured on all interfaces
 - If low speed, an IP address must be configured on the interface

© 2006 Cisco Systems, Inc. All rights reserved.

ONT v1.0—5-11

Router Prerequisites

Before configuring Cisco AutoQoS, these prerequisites must be met:

- You must ensure that no QoS policies (service policies) are attached to the interface. Cisco AutoQoS cannot be configured if a QoS policy is attached to the interface.
- Cisco Express Forwarding (CEF) must be enabled. Cisco AutoQoS uses NBAR to identify various applications and traffic types, and CEF is a prerequisite for NBAR.
- Cisco AutoQoS classifies links as either low speed or high speed depending on the link bandwidth. Remember that on a serial interface, if the default bandwidth is not specified, it is 1.544 Mbps. Therefore, it is important that the correct bandwidth be specified on the interface or subinterface where Cisco AutoQoS is to be enabled:
 - For all interfaces or subinterfaces, be sure to properly configure the bandwidth by using the **bandwidth** command. The amount of bandwidth that is allocated should be based on the link speed of the interface.
 - If the interface or subinterface has a link speed of 768 kbps or lower, an IP address must be configured on the interface or subinterface using the **ip address** command. By default, Cisco AutoQoS enables MLP and copies the configured IP address to the multilink bundle interface.

In addition to the Cisco AutoQoS prerequisites, there are other recommendations and requirements for configuring Cisco AutoQoS (be aware that these may change with Cisco IOS software releases and should be verified before implementing Cisco AutoQoS in the environment):

- Cisco AutoQoS is supported only on these interfaces and PVCs:
 - ATM PVCs
 - Serial interfaces with PPP or HDLC
 - Frame Relay DLCIs (point-to-point subinterfaces only, because Cisco AutoQoS does not support Frame Relay multipoint interfaces)
- A configuration template generated by configuring Cisco AutoQoS on an interface or PVC can be tuned manually (via CLI configuration) if desired.
- To include SNMP traps (monitored events), SNMP support must be enabled on the router. Cisco AutoQoS SNMP traps are delivered only when an SNMP server is used in conjunction with Cisco AutoQoS and the router is familiar with how to reach the SNMP server.
- The SNMP community string “AutoQoS” should have write permission.
- If the device is reloaded with the saved configuration after configuring Cisco AutoQoS and saving the configuration to NVRAM, some warning messages may be generated by Remote Monitoring (RMON) threshold commands. These warning messages can be ignored. (To avoid further warning messages, save the configuration to NVRAM again without making any changes to the QoS configuration.)
- By default, Cisco 7200 Series Routers and earlier that support the Cisco Modular QoS CLI (MQC) reserve up to 75 percent of the interface bandwidth for user-defined classes. The remaining bandwidth is used for the default class. However, the entire remaining bandwidth is *not* guaranteed to the default class. This bandwidth is shared proportionately among the various flows in the default class and excess traffic from other bandwidth classes.

Deploying Cisco AutoQoS for the Enterprise on Routers: A Two-Step Approach

Cisco AutoQoS for the Enterprise consists of two configuration phases:

1. Autodiscovery (data collection)
2. Cisco AutoQoS template generation and installation

Deploying Cisco AutoQoS for Enterprise on Routers: A Two-Phase Approach

1. **Profile the traffic with autodiscovery:**
 - **Collects data from the offered traffic for several days (default is 3 days)**
 - **Uses NBAR for protocol discovery and statistical analysis**
2. **Generate and deploy MQC-based QoS policies:**
 - **Maps applications to their corresponding DiffServ classes**
 - **Assigns appropriate bandwidth and scheduling parameters**

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0—5-12

The autodiscovery phase uses NBAR-based Protocol Discovery to detect the applications on the network and performs statistical analysis on the network traffic.

The data collected should be a representative sampling of the volume and type of voice, video, and data on your network. Therefore, the amount of time devoted to data collection varies from network to network. Run the autodiscovery phase for as long as necessary. The length of time needed can vary, depending on the volume and nature of traffic on your network. By default, autodiscovery runs for three days.

The Cisco AutoQoS template generation and installation phase generates templates from the data collected during the autodiscovery phase, and installs the templates on the interface. These templates are then used as the basis for creating the class maps and policy maps for your network. After the class maps and policy maps are created, they are installed on the interface.

Cisco AutoQoS VoIP omits the autodiscovery phase and it goes straight to template generation and installation.

Configuring Cisco AutoQoS: Traffic Profiling on Routers with Autodiscovery

Initiate the autodiscovery phase by using the **auto discovery qos** command on the selected interface.

Configuring Cisco AutoQoS: Traffic Profiling on Routers with Autodiscovery

```
router(config-if)#  
auto discovery qos [trust]
```

- **Process begins discovering and collecting data for Cisco AutoQoS for Enterprise only.**
- **Autodiscovery is enabled on the interface of interest.**
- **Optional trust keyword is used to trust (rely on) the DSCP markings; if unspecified, NBAR will be used.**
- **Default value is untrusted.**
- **Discovery results can be seen with the show auto discovery qos command.**

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0—5-13

Before using the **auto discovery qos** command at the interface or ATM PVC, ensure that these prerequisites have been met:

- CEF must be enabled.
- If the interface or subinterface has a link speed of 768 kbps or lower, configure the primary or secondary IP address of the interface by using the **ip address** command.
- For all interfaces or subinterfaces, configure the amount of bandwidth by using the **bandwidth** command. The amount of bandwidth allocated should be based on the link speed of the interface.
- For ATM PVCs, configure the variable bit rate (VBR) by using either the **vbr-nrt** command or the **vbr-rt** command, or configure the constant bit rate (CBR) by using the **cbr** command.

When running autodiscovery, observe these restrictions:

- The **auto discovery qos** command is not supported on subinterfaces.
- Do not change the bandwidth of the interface when using the **auto discovery qos** command.
- All previously attached policies must be removed from the interface.

The optional **trust** keyword indicates that the DSCP markings of a packet are trusted (that is, relied on) for classification of voice, video, and data traffic. If the optional **trust** keyword is not specified, voice, video, and data traffic is classified using NBAR, and the packets will be marked with the appropriate DSCP value.

Note these points about the autodiscovery phase:

- If you want to stop autodiscovery, use the **no auto discovery qos** command. This command stops data collection and removes any data collection reports that have been generated.
- If you want to view the autodiscovery temporary results while discovery is in progress, use the **show auto discovery qos** command. This command displays the results of the data collected up to that point during the autodiscovery phase.

Configuring Cisco AutoQoS: Configuring QoS Policies on Routers

The **auto qos** command generates Cisco AutoQoS for the Enterprise templates on the basis of the data collected during the autodiscovery phase and then installs the templates on the interface. These templates are then used to create class maps and policy maps for use on your network. After they are created, the class maps and policy maps are also installed on the interface.

Configuring Cisco AutoQoS: Configuring QoS Policies on Routers

```
router(config-if)#  
auto qos [voip [trust] [fr-atm]]
```

- It generates and installs the QoS policy based on the autodiscovery results (AutoQoS for Enterprise).
- The optional **voip** keyword configures Cisco AutoQoS VoIP.
- Optional **trust** keyword is used to trust (rely on) the DSCP markings for VoIP classification; if unspecified, NBAR will be used.
- Default value is **untrusted**.
- Optional **fr-atm** keyword enables Cisco AutoQoS VoIP for the low-speed Frame Relay-to-ATM links.

© 2006 Cisco Systems, Inc. All rights reserved.ONT v1.0—5-14

To remove Cisco AutoQoS from the interface, use the **no** form of the **auto qos** command.

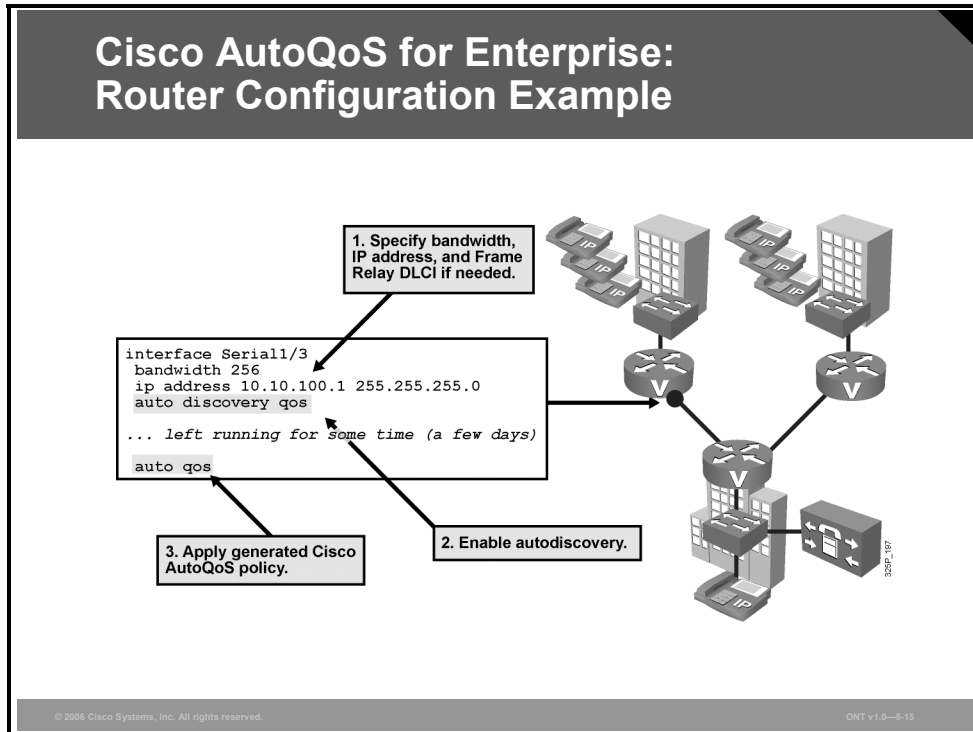
The **auto qos** command can also be used to enable Cisco AutoQoS VoIP, which does not have any prior autodiscovery. If you are using any of the earlier Cisco IOS software releases in connected routers where only Cisco AutoQoS VoIP is supported, use the **voip** keyword to generate Cisco AutoQoS VoIP templates.

For Cisco AutoQoS VoIP, the optional **trust** keyword is used to trust (that is, rely on) the DSCP markings for classification of voice traffic. If the optional **trust** keyword is not specified, voice traffic is classified using NBAR, and the packets are marked with the appropriate DSCP value.

The optional **fr-atm** keyword enables Cisco AutoQoS VoIP for the Frame Relay-to-ATM interworking links. This option is available on the Frame Relay DLCIs for Frame Relay-to-ATM interworking only.

Example: Cisco AutoQoS for the Enterprise Router Configuration

The figure shows an example of Cisco AutoQoS for the Enterprise configuration on a router interface.



The correct configuration procedure is as follows:

- Step 1** On the interface, first configure the offered bandwidth using the **bandwidth** command, configure the IP address using the **ip address** command, and configure the DLCI address using the **frame-relay interface dlci** command if you are configuring under a Frame Relay subinterface.
- Step 2** Activate the autodiscovery phase using the **auto-discovery qos** command. For the most accurate traffic analysis, leave the autodiscovery phase running for as long as possible, preferably several days. In the autodiscovery phase, the generated policy can optionally be reviewed using **show auto discovery qos**.
- Step 3** Apply the generated Cisco AutoQoS policy to the interface using the **auto qos** command.

At this point, the Cisco AutoQoS configuration is complete, but the autogenerated classification and policies can be manually tuned if necessary.

Example: Configuring Cisco AutoQoS for the Enterprise on a High-Speed Serial Interface

In this example, Cisco AutoQoS is configured on the high-speed serial 1/2 interface:

```
Router>enable
Router#configure terminal
Router(config)#interface serial1/2
Router(config-if)# ip address 10.10.100.1 255.255.255.0
Router(config-if)#bandwidth 1544
Router(config-if)#auto discovery qos
Router(config-if)#end
Router#
```

Note Leave Cisco AutoQoS discovery running, preferably for several days.

```
Router#configure terminal
Router(config)#interface serial1/2
Router(config-if)#auto qos
Router(config-if)#exit
```

Example: Configuring Cisco AutoQoS for the Enterprise on a Low-Speed Serial Interface

In this example, Cisco AutoQoS is configured on the low-speed serial 1/3 interface:

```
Router#configure terminal
Router(config)#interface serial1/3
Router(config-if)#bandwidth 256
Router(config-if)#ip address 10.10.100.2 255.255.255.0
Router(config-if)#auto discovery qos
Router(config-if)#end
Router#
```

Note Leave Cisco AutoQoS discovery running, preferably for several days.

```
Router#configure terminal
Router(config)#interface serial1/2
Router(config-if)#auto qos
Router(config-if)#exit
```

Deploying Cisco AutoQoS VoIP on Switches

There are various LAN commands, depending on the platform and operating system (Cisco IOS software versus Cisco Catalyst operating system software). For the Cisco IOS software-based Catalyst 2950 and Catalyst 3550 Series switches, there are two Cisco AutoQoS configuration commands: One command is for the IP phone connections, and the other is for trusted connections to other network devices. However, a single command is enough to enable Cisco AutoQoS VoIP.

Deploying Cisco AutoQoS VoIP on Switches

- **Commands at the interface level configure Cisco AutoQoS VoIP:**
 - Support for Cisco IP phone and Cisco SoftPhone
 - Support for Cisco SoftPhone currently only on Cisco Catalyst 6500 Series
 - Trust boundary disabled when Cisco IP phone is moved
- **Buffer allocation and egress queuing depend on interface type (Gigabit Ethernet or Fast Ethernet).**
- **It is supported on static, dynamic-access, voice VLAN access, and trunk ports.**
- **CDP must be enabled for Cisco AutoQoS VoIP to function properly.**

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0-5-16

Cisco AutoQoS VoIP in the LAN fulfils these QoS requirements:

- A single command enables Cisco AutoQoS VoIP in a LAN, and another command provides support for Cisco IP Phone and Cisco IP Communicator equipment.
- Cisco AutoQoS automatically configures QoS parameters for optimal voice performance based upon Cisco best-practice recommendations, extensive lab testing, and input from a broad base of Cisco Unified Communications customer installations.
- Cisco AutoQoS VoIP determines trust and extended trust boundary settings automatically. A user can bypass the IP phone and connect a PC directly to a switch, but trust is disabled when the IP phone is removed.
- Cisco AutoQoS VoIP configures class of service (CoS) to DSCP (to egress queue) mapping.
- Cisco AutoQoS VoIP determines optimal priority queuing (PQ) and weighted round robin (WRR) configuration settings for static, dynamic-access, voice VLAN (VLAN), and trunk ports.

To configure the QoS settings and the trusted boundary feature for Cisco IP phones, CDP version 2 or later must be enabled on the switch port, where the IP phone is connected. 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 only for the Cisco IP phone QoS configuration; CDP does not affect the other components of the automatic QoS features.

Configuring Cisco AutoQoS on Cisco Catalyst Switches

For Cisco IOS-based Catalyst switches, there are two Cisco AutoQoS VoIP configuration commands.

Configuring Cisco AutoQoS on Cisco Catalyst 2950 (EI) and 3550 Switches

```
switch(config-if)#  
auto qos voip trust
```

- Used for trusted connections.
- Used to trust the ingress VoIP packet marking.
- Use if the uplink is connected to a trusted switch or router only.

```
switch(config-if)#  
auto qos voip cisco-phone
```

- Used for Cisco IP Phone connections.
- Enables the trusted boundary feature.
- Uses CDP to detect the presence or absence of a Cisco IP Phone.
- QoS markings of incoming packets are trusted only when the Cisco IP phone is detected.

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0--5.17

One command is for trusted connections to other network devices, and the other is for Cisco IP phone connections:

- The **auto qos voip trust** interface configuration command activates Cisco AutoQoS VoIP on a Cisco IOS-based switch and sets the ingress interface to trust the ingress CoS QoS marking received in the packet. It also reconfigures the egress queues on the interface.
- The **auto qos voip cisco-phone** interface configuration command enables the trusted boundary feature. 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.

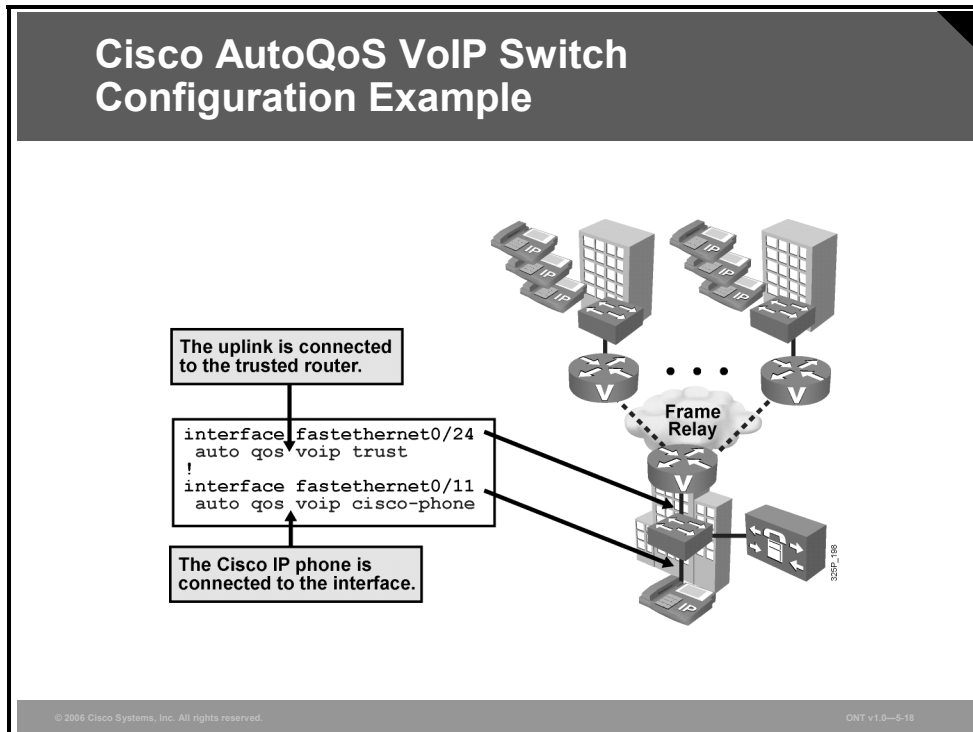
These commands should not be used if there are previous QoS configurations on the switch. However, the Cisco AutoQoS configuration parameters (Cisco AutoQoS template) generated may be tuned after using these commands.

Note Both commands, in the same format, also apply to Cisco Catalyst 4500 Series Switches. As with Cisco Catalyst 2950 (EI) and 3550 Switches, Cisco Catalyst 4500 Series Switches do not support the Cisco SoftPhone option.

When Cisco AutoQoS VoIP is enabled on the first interface, QoS is globally enabled (**mls qos** global configuration command).

Example: Cisco AutoQoS VoIP Switch Configuration

This example shows how to enable Cisco AutoQoS VoIP to trust the QoS marking received in incoming packets when the switch is connected to the trusted device (router) using the Fast Ethernet interface 0/24.



The example also shows how to enable Cisco AutoQoS VoIP to trust the QoS marking received in incoming packets when the device connected to Fast Ethernet interface 0/11 is detected and is a Cisco IP phone.

Verifying Cisco AutoQoS

This topic describes how to use Cisco IOS commands to examine and monitor a network configuration after Cisco AutoQoS has been enabled.

		Routers	Switches
P r o c e d u r e F l o w	E n t e r p r i s e	Examine autodiscovery results: <code>show auto discovery qos</code>	
		Examine Cisco AutoQoS templates and initial configuration: <code>show auto qos</code>	Examine Cisco AutoQoS templates and initial configuration: <code>show auto qos</code>
		Explore interface statistics for autogenerated policy: <code>show policy-map interface</code>	Explore interface-level autogenerated QoS parameters: <code>show policy-map interface</code>
			Examine CoS-to-DSCP maps: <code>show mls qos maps</code>

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0—5-20

The verification of Cisco AutoQoS typically follows the procedure shown in the table. The principle behind the procedure is the same for routers and switches, with the exception that there is no autodiscovery phase on switches, and therefore, there is no requirement to verify its results.

The major command used for verification on both routers and switches is **show auto qos**. The interface-specific configuration is examined afterward. Because Cisco Catalyst switches use the CoS-to-DSCP maps for egress packet queuing, you can use the **show mls qos maps** command to verify how Cisco AutoQoS defined these maps.

Monitoring Cisco AutoQoS on Routers

Use the **show auto discovery qos** command to display the data collected during the autodiscovery phase of Cisco AutoQoS for the Enterprise.

Monitoring Cisco AutoQoS on Routers

```
router#  
show auto discovery qos [interface [interface type]]
```

- **Displays the results of the data collected during the autodiscovery phase for a specific interface or all interfaces**

```
router#show auto discovery qos  
Serial2/1.1  
  
AutoQoS Discovery enabled for applications  
Discovery up time: 2 hours, 42 minutes  
AutoQoS Class information:  
Class Voice:  
Recommended Minimum Bandwidth: 517 Kbps/50% (PeakRate).  
Detected applications and data:  
Application/           AverageRate           PeakRate           Total  
Protocol              (kbps/%)             (kbps/%)           (bytes)  
-----  
rtp audio              2/<1                  517/50             703104  
  
<...rest of the output deleted...>
```

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0-5.21

The suggested policy output lets you preview class maps and policy maps before you issue the **auto qos** command on the interface. You can then continue with the autodiscovery phase to gather more data (it is recommended that you run Cisco AutoQoS discovery for several days), or you can copy the existing discovery results into a text editor and modify the autogenerated classification and policies as desired.

The optional **interface** keyword indicates that only the configurations for the specific interface type will be displayed.

Monitoring Cisco AutoQoS on Routers (Cont.)

```
router#
```

```
show auto qos [interface interface type]
```

- Displays the Cisco AutoQoS templates (policy maps, class maps, and ACLs) created for a specific interface or all interfaces

```
router#show auto qos
!
policy-map AutoQoS-Policy-Se2/1.1
 class AutoQoS-Voice-Se2/1.1
  priority percent 70
  set dscp ef
 class AutoQoS-Inter-Video-Se2/1.1
  bandwidth remaining percent 10
  set dscp af41
 class AutoQoS-Stream-Video-Se2/1.1
  bandwidth remaining percent 5
  set dscp cs4
 class AutoQoS-Transactional-Se2/1.1
  bandwidth remaining percent 5
<...rest of the output deleted...>
```

© 2006 Cisco Systems, Inc. All rights reserved.

ONT v1.0—5-22

The **show auto qos** command is used to display the Cisco AutoQoS interface templates, policy maps, class maps, and ACLs.

When the **interface** keyword is used along with the corresponding *interface type* argument, the command displays the configurations created by Cisco AutoQoS on the specified interface. When the **interface** keyword is used but an interface type is not specified, the command displays the configurations created by the AutoQoS on all the interfaces or PVCs on which the AutoQoS has been enabled.

The **show auto qos interface** command can also be used with Frame Relay DLCIs and ATM PVCs.

Monitoring Cisco AutoQoS on Routers (Cont.)

router#

```
show policy-map interface [interface type]
```

- Displays the packet statistics of all classes that are configured for all service policies on the specified interface, subinterface, or PVC

```
router#show policy-map interface FastEthernet0/0.1
FastEthernet0/0.1
Service-policy output: voice_traffic
Class-map: dscp46 (match-any)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: ip dscp 46
0 packets, 0 bytes
5 minute rate 0 bps
Traffic Shaping
Target   Byte   Sustain  Excess   Interval  Increment Adapt
Rate    Limit  bits/int bits/int (ms)      (bytes)   Active
  2500   10000  10000   10000   333       1250     -
<...rest of the output deleted...>
```

© 2006 Cisco Systems, Inc. All rights reserved.

ONT v1.0-5.23

To display the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface, use the **show policy-map interface** command.

The counters displayed after you enter the **show policy-map interface** command are updated only if there is congestion on the interface. The command will also display policy information about Frame Relay PVCs, but only if Frame Relay traffic shaping (FRTS) is also enabled on the interface (manually or by Cisco AutoQoS).

Monitoring Cisco AutoQoS on Switches

Use the **show auto qos** command to display the initial Cisco AutoQoS VoIP configuration on the switch.

Monitoring Cisco AutoQoS on Switches

```
switch#  
show auto qos [interface interface-id]
```

- Displays the Cisco AutoQoS VoIP 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. ONT v1.0--5.24

To display any user changes to that configuration, use the **show running-config** command. The **show auto qos** and the **show running-config** command output can be compared to identify the additional user-defined QoS settings.

Note From the **show** command output, you can see that the switch has four output queues available. Queue 4 is used for high-priority traffic (a value of 0 within the **wrr-queue bandwidth** command and a mapping of CoS 5 to queue 4 using the **wrr-queue cos-map** command). Queue 2 is not used at all (a value of 1 within the **wrr-queue bandwidth** command and no mapping of CoS to queue 2 using the **wrr-queue cos-map** command).

Monitoring Cisco AutoQoS on Switches (Cont.)

switch#

```
show mls qos interface [interface-id | vlan vlan-id]
[buffers | policers | queueing | statistics]
```

- Displays QoS information at the interface level

```
switch#show mls qos interface gigabitethernet0/1 statistics
Ingress
  dscp: incoming  no_change  classified  policed  dropped (in bytes)
      1 : 0         0         0           0         0
  Others: 203216935 24234242 178982693 0         0
Egress
  dscp: incoming  no_change  classified  policed  dropped (in bytes)
      1 : 0         n/a        n/a         0         0
WRED drop counts:
  qid  thresh1  thresh2  FreeQ
  1 : 0      0        1024
  2 : 0      0        1024
<...rest of the output omitted...>
```

© 2006 Cisco Systems, Inc. All rights reserved.

ONT v1.0-5.25

The **show mls qos interface** command is used to display QoS information on the Cisco Catalyst switch at the interface level, including the configuration of the egress queues and the CoS-to-egress-queue maps, the interfaces that have configured policers, and ingress and egress statistics (including the number of bytes dropped).

If no keyword is specified with the **show mls qos interface** command, the port QoS mode (DSCP trusted, CoS trusted, untrusted, and so forth), default CoS value, DSCP-to-DSCP-mutation map (if any) that is attached to the port, and policy map (if any) that is attached to the interface are displayed. If a particular interface is not specified, the information for all interfaces is displayed.

Monitoring Cisco AutoQoS on Switches (Cont.)

```
switch#
```

```
show mls qos maps [cos-dscp | dscp-cos]
```

- Displays the maps that are used to generate an internal DSCP value, to represent the priority of the traffic

```
switch#show mls qos maps dscp-cos
```

```
Dscp-cos map:  
dscp: 0 8 10 16 18 24 26 32 34 40 46 48 56  
-----  
cos:  0 1  1  2  2  3  7  4  4  5  5  7  7
```

© 2006 Cisco Systems, Inc. All rights reserved.

ONT v1.0—5-26

The **show mls qos maps** command is used to display the current DSCP and CoS mappings. All the maps are globally defined. The **cos-dscp** keyword presents the default CoS-to-DSCP map. The supported CoS values are 0–7. The **dscp-cos** keyword presents the default DSCP-to-CoS mapping. The supported DSCP values are 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48, and 56. After a default map is applied, you can define the CoS-to-DSCP or DSCP-to-CoS map by entering consecutive **mls qos map** commands.

Summary

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

Summary

- **Cisco AutoQoS significantly simplifies QoS deployments.**
- **Cisco AutoQoS allows for initial, faster, cheaper, and flawless QoS implementation.**
- **Cisco AutoQoS for the Enterprise is deployed in two steps:**
 - **Autodiscovery is used to generate policy.**
 - **Implementation of the generated policy follows.**
- **Cisco AutoQoS allows you to retain complete control over the QoS configuration:**
 - **Verification is performed with standard show commands.**
 - **Generated results are further tunable with MQC.**

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0-5-27

References

For additional information, refer to these resources:

- Cisco Systems, Inc. Quality of Service page at www.cisco.com/go/qos.
- Cisco Systems, Inc. “AutoQoS for the Enterprise” at http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a0080455a3f.html.
- Cisco Systems, Inc. CiscoWorks QoS Policy Manager page at <http://www.cisco.com/en/US/products/sw/cscowork/ps2064/index.html>.
- Cisco Systems, Inc. “Network-Based Application Recognition” at http://www.cisco.com/en/US/products/ps6616/products_case_study09186a00800ad0ca.shtml.
- Cisco Systems, Inc. *Catalyst 6500 Series Command Reference, 8.5* at http://www.cisco.com/en/US/products/hw/switches/ps708/products_command_reference_book09186a00803f54f2.html.
- Cisco Systems, Inc. “Configuring a VoIP Network” at http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a00803f58e9.html.

Mitigating Common Cisco AutoQoS Issues

Overview

Cisco AutoQoS automates the deployment of quality of service (QoS) policies in a general business environment and is especially designed for midsize companies and branch offices of larger companies. It generates templates from data collected during an autodiscovery phase and then installs the templates on the interface. The templates are used as the basis for creating the class maps and policy maps for a network. If the policy maps and class maps created do not meet the needs of your network, the policy maps and class maps can be tuned to meet specific requirements using standard Cisco IOS QoS mechanisms.

This lesson identifies situations where standard configurations generated by Cisco AutoQoS may not provide optimal QoS and explains how to manually fine-tune AutoQoS-generated configurations using the Cisco Modular QoS CLI (MQC) when required.

Objectives

Upon completing this lesson, you will be able to explain how to fine-tune a Cisco AutoQoS configuration after specific problems in the configuration have been identified by analyzing the **show** output. This ability includes being able to meet these objectives:

- Identify the QoS technologies that are automatically implemented on the network using Cisco AutoQoS
- Describe known issues with Cisco AutoQoS
- Using the **show** commands, isolate areas in the Cisco AutoQoS running configuration where the known issues typically occur
- Explain how to modify the QoS configuration created by Cisco AutoQoS

Automation with Cisco AutoQoS

This topic describes several of the QoS technologies that are automatically implemented on the network when using Cisco AutoQoS.

QoS Mechanisms Enabled Must Meet Major Enterprise QoS Requirements

- **Trust boundary definition**
- **Identification of applications, protocols of interest (number of classes), and their QoS requirements**
- **Determination of classification options**
- **Determination of traffic-marking options**
- **Determination of queue mechanisms and optimal parameters per class**
- **Definition of port- and interface-specific transport features**
- **Designation of bandwidth efficiency mechanisms for low-speed links**
- **Identification of efficient alarm and event-monitoring options**

© 2006 Cisco Systems, Inc. All rights reserved.

ONT v1.0-5.3

Cisco AutoQoS automates quality of service (QoS) deployment for the most common enterprise scenarios. Cisco AutoQoS enables several Cisco IOS QoS mechanisms to meet the QoS requirements of various applications and traffic types discovered in the enterprise network. Typical enterprise QoS requirements and tasks for Cisco AutoQoS are as follows:

- Identify trust boundary and extended trust boundary and protocols of interest
- Determine the number of Differentiated Services (DiffServ) classes that will be defined for the enterprise network
- Re-mark traffic based on local policy requirements
- Determine the queuing methods that should be enabled
- Define the individual class bandwidth needed to fulfill real-time traffic requirements and provide minimum bandwidth guarantees for other applications
- Define transport-specific QoS features (traffic shaping, Multilink PPP [MLP], and transmit ring [tx-ring] settings)
- For low-bandwidth links (less than 768 kbps), specify necessary QoS features (compressed Real-Time Transport Protocol [cRTP], MLP link fragmentation and interleaving [LFI], or Frame Relay Fragmentation [FRF.12])
- Define the alarm and event settings for monitoring purposes

In addition, in a LAN environment, Cisco AutoQoS also has these requirements:

- Determine class of service (CoS)-to-differentiated services code point (DSCP) and IP precedence-to-DSCP mappings
- Map CoS values to different egress queues (via CoS-to-DSCP maps)
- Set the queue sizes and weighted round robin (WRR) weights (that is, the appropriate WRR settings for Fast Ethernet interfaces versus Gigabit Ethernet interfaces)

DiffServ QoS Mechanisms Enabled by Cisco AutoQoS

Using Cisco best-practices recommendations, Cisco AutoQoS enables several QoS mechanisms to ensure optimal performance of autodiscovered enterprise applications.

DiffServ QoS Mechanisms Enabled by Cisco AutoQoS		
DiffServ functions are automated and simplified to expedite deployment of QoS features for voice, video, and data.		
DiffServ Function	Cisco IOS QoS Features	Behavior
Classification	<ul style="list-style-type: none">NBAR and IP precedenceDSCP and CoS	<ul style="list-style-type: none">Classify voice, video, and data traffic based on packet attributes; up to 10 classes
Marking	<ul style="list-style-type: none">Class-based marking	<ul style="list-style-type: none">Set Layer 2 and Layer 3 attributes to separate packets into classes
Congestion management	<ul style="list-style-type: none">Percentage-based LLQ and CBWFQWRR	<ul style="list-style-type: none">Provide EF treatment for voice, AF treatment for video and data, and best-effort treatment as default
Shaping	<ul style="list-style-type: none">Class-based shaping or FRTS	<ul style="list-style-type: none">Shape to CIR to prevent bursts and smooth traffic to configured rate
Congestion avoidance	<ul style="list-style-type: none">WRED	<ul style="list-style-type: none">Make intelligent packet drop decisions to prevent tail drops across multiple TCP sessions
Link efficiency	<ul style="list-style-type: none">Header compression and link fragmentation and interleaving	<ul style="list-style-type: none">Reduce VoIP bandwidth requirement and jitter experienced by voice packets

© 2006 Cisco Systems, Inc. All rights reserved. OMT v1.0-6.4

Cisco AutoQoS automatically provisions six QoS mechanisms using DiffServ technology.

Classification

Packet classification provides the ability to partition network traffic into multiple priority levels or classes of service. For example, by using the Internet Engineering Task Force (IETF)-defined DSCP specified in DiffServ standards RFC 2474 and 2475, networks can categorize application traffic into a maximum of 64 traffic classes. Cisco AutoQoS defines up to 10 classes. When packets are classified, the various QoS features in Cisco IOS software can be used to assign the appropriate traffic-handling policies for each traffic class.

Cisco AutoQoS either reuses the classification based on DSCP or IP precedence and CoS from the adjacent device (for example, the router or switch closer to the network edge) in trusted mode or activates Cisco Network-Based Application Recognition (NBAR) to classify the traffic on an ingress interface in untrusted mode. In either case, Cisco AutoQoS defines classes using the Cisco Modular QoS CLI (MQC) class maps.

Marking

Marking tools mark a packet or flow with a specific priority. This marking is performed at a trust boundary. Classification and marking should take place at the network edge, typically in the wiring closet switches, within the Cisco IP phones themselves, or at voice endpoints. Packets can be marked as important by using Layer 2 CoS settings in the user priority bits of the 802.1p portion of the 802.1Q header or the IP precedence or DSCP bits in the type of service (ToS) byte of the IP version 4 (IPv4) header. For example, all Cisco IP phone Real-Time Transport Protocol (RTP) packets should be tagged with either of these values:

- CoS value of 5 for the Layer 2 802.1p settings and a DSCP value of expedited forwarding (EF)
- IP precedence value of 5

Additionally, all control packets should be tagged with a Layer 2 CoS value of 3 and a Layer 3 DSCP value of 24–31 (or IP precedence value of 3)

Cisco AutoQoS employs class-based marking MQC mechanism for all Layer 2 frame and Layer 3 packet marking.

Congestion Management

Congestion management tools assign a packet or flow to one of several queues, based on classification, for appropriate treatment in the network. When data, voice, and video are placed in the same queue, packet loss and variable delay are more likely to occur. You can increase the predictability of network behavior and voice quality by using multiple queues on egress interfaces and placing voice packets into a strict-priority queue (low latency queuing [LLQ]) with guaranteed bandwidth, separate from data packets. Congested outbound WAN egress queues and serialization delays with low-speed WAN links (link speeds less than 768 kbps) can both result in variable delays and jitter impact on voice traffic (serialization delay is a function of both link speed and packet size). Large e-mails and data downloads can cause voice quality degradation, even in LAN environments.

To alleviate the effects of congestion and to provide enterprise applications with guaranteed bandwidth and the lowest possible latency, Cisco AutoQoS enables these Cisco IOS queuing tools:

- LLQ for real-time applications to experience the least latency in egress queues and to ensure sufficient bandwidth on the output link for optimal voice performance. LLQ processes traffic classified into the DiffServ EF class (voice) as highest priority and places that traffic into a separate, strict-priority queue. All other traffic is treated using class-based weighted fair queuing (CBWFQ).
- CBWFQ for data applications is utilized to provide sufficient bandwidth and reduce interference between high-priority and low-priority applications during periods of congestion. CBWFQ processes traffic classified into DiffServ Assured Forwarding (AF) classes (video and classified data) and the default class for unclassified traffic (best effort).
- WRR with priority queuing (PQ) on Cisco Catalyst switches processes traffic on egress switch ports using DiffServ (DSCP is mapped to CoS at the ingress automatically), ensuring priority for real-time traffic and predictable bandwidth for other traffic types.

Cisco AutoQoS uses percentage-based policies for increased scalability and manageability. The same policy map can be applied on multiple interfaces and on interfaces with varying bandwidth.

Shaping

Traffic shaping is a QoS mechanism used to send traffic in short bursts at a configured transmission rate. It is most commonly used in Frame Relay environments where the interface clock rate is not the same as the guaranteed bandwidth or committed information rate (CIR). Frame Relay traffic shaping (FRTS) is the most common traffic-shaping application in VoIP environments. Frame Relay scenarios usually have a hub-and-spoke network where the hub link speed is higher than any of the remote link speeds. In some cases, the sum of the remote link speeds is higher than the hub link speed, causing oversubscription. Without FRTS, the hub may try to send traffic at higher rates than the remote links can receive, causing the Frame Relay network to arbitrarily drop traffic. However, the remote links could all send at an aggregate rate that is higher than the hub can receive, again causing the Frame Relay network to arbitrarily drop traffic. Because the Frame Relay network has no Layer 3 or above intelligence, it can drop VoIP traffic if contracts are violated. Therefore, you need to control transmission rates into a Frame Relay cloud so that you can control which packets get dropped and which packets receive priority servicing.

Cisco AutoQoS, depending on the autodiscovered enterprise network environment, enables either class-based shaping (for non-Frame Relay environments) or FRTS mechanisms.

Congestion Avoidance

Congestion-avoidance techniques monitor network traffic loads in an effort to anticipate and avoid congestion at common network bottlenecks. Congestion avoidance is achieved through packet dropping. The router default is typically to use a crude default packet-drop mechanism called tail drop. With tail drop, packets are dropped during periods of congestion if they do not fit into the egress queue, which equally affects all traffic types, including high-priority traffic. Global synchronization is another effect of tail drop and occurs as waves of congestion crest, only to be followed by troughs during which the transmission link is not fully utilized. Global synchronization of TCP hosts, for example, can occur because packets are dropped all at once. Global synchronization is manifested when multiple TCP hosts reduce their transmission rates in response to packet dropping, then increase their transmission rates when the congestion is reduced. Cisco AutoQoS utilizes weighted random early detection (WRED) to avoid both the dropping of high-priority packets and global synchronization. WRED increases the probability that congestion will be avoided by dropping low-priority packets rather than high-priority packets.

Link Efficiency

Low-speed WAN links can tremendously degrade voice quality. Voice traffic could suffer from long delays before reaching the head of the output line, long transmission time, and insufficient bandwidth. When Cisco AutoQoS detects low-speed links during the autodiscovery phase, it minimizes these problems by enabling two link efficiency mechanisms:

Link fragmentation and interleaving (LFI) is the method used to improve serialization delay. Even when queuing is working at its best and prioritizing voice traffic, there are times when the priority queue is empty and a packet from another class is serviced. Packets from guaranteed bandwidth classes must be serviced according to their configured weight. If a priority voice packet arrives in the output queue while these packets are being serviced, the VoIP packet could wait a substantial length of time before being sent. If a VoIP packet waits behind one data packet, and the data packet is, at most, equal in size to the maximum transmission unit (MTU) (1,500 bytes for serial interfaces and 4470 bytes for high-speed serial interfaces), the wait time can be calculated based on link speed. For example, this formula calculates the wait time for a link speed of 64 kbps and MTU size of 1500 bytes:

$$\text{Serialization delay} = (1500 \text{ bytes} * 8 \text{ bits per byte}) / (64,000 \text{ bps}) = 187.5 \text{ ms}$$

Therefore, a VoIP packet may need to wait up to 187.5 ms before it can be sent if it is delayed behind a single 1500-byte packet on a 64-kbps link. VoIP packets usually are sent every 20 ms. With an end-to-end delay budget of 150 ms and strict jitter requirements, a gap of more than 180 ms is unacceptable. Some mechanism is needed that ensures that the size of one transmission unit is 10 ms or less. Any packets that have more than 10-ms serialization delay need to be fragmented into 10-ms chunks. A 10-ms chunk or fragment is the number of bytes that can be sent over the link in 10 ms. For a serialization delay of 10 ms, the corresponding size of a packet or fragment transmitted over a 64-kbps link would be 80 bytes.

Cisco AutoQoS enables one of two LFI mechanisms to fragment large packets to protect voice, when low-speed links are autodiscovered:

- Multilink PPP (MLP) with interleaving for PPP links
- Frame Relay Fragmentation (FRF.12) for Frame Relay permanent virtual circuits (PVCs)

Compressed Real-Time Transport Protocol (cRTP) reduces the 40 byte IP + User Datagram Protocol (UDP) + RTP header to 2 to 4 bytes, reducing the bandwidth required per voice call on point-to-point links. The header is compressed at one end of the link and decompressed at the other end. Cisco AutoQoS enables cRTP header compression when voice is transmitted on low-speed links.

Automated Cisco AutoQoS DiffServ Class Provisioning

Cisco AutoQoS for the Enterprise defines as many as 10 DiffServ classes, which are designed to accommodate various enterprise applications.

Automated Cisco AutoQoS DiffServ Class Provisioning		
Traffic Class	DSCP	CoS
IP routing	CS6	6
Interactive voice	EF	5
Interactive video	AF41	4
Streaming video	CS4	4
Telephony signaling	CS3	3
Transactional-interactive	AF21	2
Network management	CS2	2
Bulk data	AF11	1
Scavenger	CS1	1
Best effort	0	0

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0-5.5

The table lists the class name, the type of traffic defined for the class, and the DSCP value for the type of traffic, if applicable.

Class Name	Traffic Type	DSCP Value
IP routing	Network control traffic, such as routing protocols	CS6
Interactive voice	Interactive voice-bearer traffic	EF
Interactive video	Interactive video data traffic	AF41
Streaming video	Streaming media traffic	CS4
Telephony signaling	Telephony signaling and control traffic	CS3
Transactional-interactive	Database applications that are transactional in nature	AF21
Network management	Network management traffic	CS2
Bulk data	Bulk data transfers, web traffic, general data service	AF11
Scavenger	Casual entertainment, rogue traffic; less-than-best-effort treatment for traffic in this category	CS1
Best effort	Default class; all noncritical traffic, HTTP, all miscellaneous traffic	0

These classes are used with the MQC to define class maps after the classification criteria are determined. These classes are also chosen to meet scheduling requirements in compliance with DiffServ recommendations.

Note The actual number of classes created corresponds to the number of applications discovered during the autodiscovery phase.

Common Cisco AutoQoS Issues

This topic describes known issues with Cisco AutoQoS that users commonly encounter.

Common Cisco AutoQoS Issues	
Issue	Solution
Cisco AutoQoS generates up to 10 classes, but most enterprise networks deploy 3–6 classes today.	Manual consolidation of similar classes to meet the final number of classes actually needed
Cisco AutoQoS does not adapt to changing traffic conditions automatically.	Running Cisco AutoQoS discovery on a periodic basis followed by re-enabling of Cisco AutoQoS
Cisco AutoQoS does not handle all possible scenarios that may occur and might not fit specific classification or policies.	Manual fine-tuning of the configuration generated, adding new matching criteria to fit the specific situation

© 2006 Cisco Systems, Inc. All rights reserved. OMT v1.0—5-7

Although Cisco AutoQoS automates QoS deployment, it targets only the most common enterprise network scenarios. The QoS classes and templates that Cisco AutoQoS generates will not suit every network requirement. The following three most common issues may arise when you are using Cisco AutoQoS to generate enterprise policies:

- **Cisco AutoQoS generates too many classes and overengineers the classification:** Cisco AutoQoS generates up to 10 DiffServ classes, depending on the number and types of applications and protocols that it detected during the autodiscovery phase. The vast majority of enterprise networks today deploy only three to a maximum of six classes in order to maintain configuration manageability. There is no knob in Cisco AutoQoS to decrease the number of classes it is allowed to generate, and the only solution is to manually consolidate the classes with similarities to produce the final number of classes required.
- **Cisco AutoQoS generates QoS templates based on conditions at the time of autodiscovery:** Autodiscovery should be run for several days to maximize the probability that Cisco AutoQoS will generate policies based on conditions close to daily network reality. All of the configurations that Cisco AutoQoS generates are related solely to what was preconfigured (for example, the bandwidth configured at the interface) and what was detected at the time of autodiscovery. If network conditions change after Cisco AutoQoS has autogenerated the QoS templates, the autodiscovery phase and the QoS template deployment phase must be repeated to adapt the configuration to the new traffic conditions.

- **Cisco AutoQoS, even after repeated and extensive autodiscovery, does not generate the expected QoS templates:** Cisco AutoQoS built-in intelligence is based on Cisco best practices and the experience gained in the broad enterprise customer base. However, there may be some special exceptions in particular Cisco AutoQoS deployments that go beyond current capabilities or circumstances that are simply undetectable because they require human-like intelligence. For instance, classification may need to be based on a mix of complex, specific parameters. In these special situations, Cisco AutoQoS can be used to generate the initial class maps and policy maps, which are then manually tuned to meet the specific requirements. The autogenerated configuration is fully compliant with Cisco MQC, and practically any MQC mechanism can be used to supplement the classification or extend a policy.

Interpreting Cisco AutoQoS Configurations

This topic explains the output from a **show auto** command.

Interpreting Generated Cisco AutoQoS Configuration

Generated Cisco AutoQoS configuration is examined using show auto qos command, answering these questions:

- How many classes were identified (class maps)?
- Which traffic classification (class map) options were selected?
- Which traffic marking options were selected (policy maps)?
- Which queuing mechanisms and parameters were designated (policy maps)?
- Which other QoS mechanisms were appointed per class (policy maps)?
- Were any traffic parameters suggested?
- Where was the autogenerated policy applied (interface, DLCI, or PVC)?

© 2006 Cisco Systems, Inc. All rights reserved.

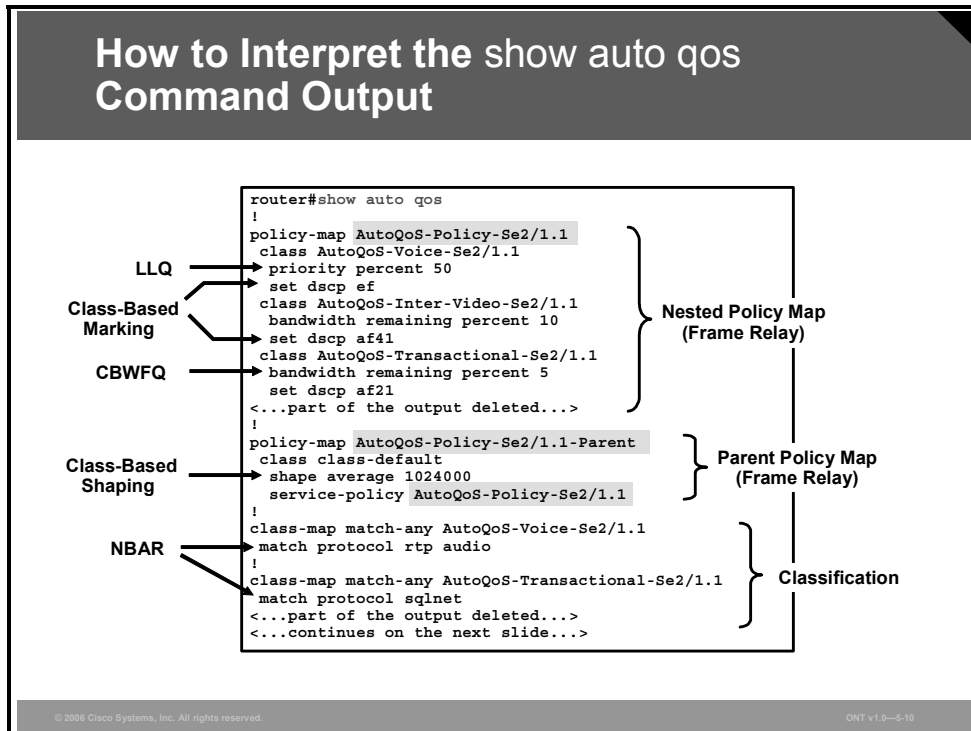
ONT v1.0-5.9

To inspect the resulting QoS templates after you apply Cisco AutoQoS, use the **show auto qos** command. This command provides the ultimate information about all QoS mechanisms and their parameters that Cisco AutoQoS enabled based on the autodiscovery results or simply generated to improve QoS. The command is specifically used to examine the following:

- How many classes were identified? This value is visible as a number of class maps.
- Which traffic classification options were selected? This parameter is visible as a **match** command option within the respective class map.
- Which traffic marking options were selected? These options can be seen in the policy maps as a **set** command option.
- Which queuing mechanisms were designated and which queuing parameters were projected? This information can be seen in the policy maps as either **bandwidth** command or **priority** command options with their individual parameter.
- Were any other QoS mechanisms appointed to serve the class? The content of policy maps can list some other mechanisms that were designated to handle the class traffic for best application performance (for example, link efficiency mechanisms or traffic shaping).
- Cisco AutoQoS can also suggest some traffic parameters such as committed bursts and CIR in Frame Relay networks, seen in the Frame Relay map class.
- How was the autogenerated policy applied to the existing router configuration? It can be applied to a serial interface, subinterface, data-link connection identifier (DLCI), or PVC. This information is also provided in the **show auto qos** command output.

How to Interpret the show auto qos Command Output

The figure shows the command output of the **show auto qos** command.



The detailed output of the **show auto qos** command varies depending on network and traffic conditions where Cisco AutoQoS was enabled, but it always has some common elements:

- The command output displays the autogenerated policy, applied in the form of the MQC policy map. In this section, the selected queuing mechanisms will be evident (LLQ or CBWFQ), but this section can also show class-based marking, class-based shaping, congestion avoidance (WRED), and link efficiency mechanisms (cRTP or LFI). Each QoS mechanism appears in the generated output in the same form that it would have if it were configured manually with the MQC.
- The other important section in the **show auto qos** command output is the classification, shown in the form of an MQC class map. The class map can use the NBAR classification option or the DSCP or IP precedence option when Cisco AutoQoS was enabled in the trusted mode. In either case, the **match** command is used within individual class maps with the appropriate parameters.
- In some special situations, such as those shown in the output for a Frame Relay PVC, Cisco AutoQoS can construct two policy maps, one nested in the other. The purpose is to use class-based shaping to fit the traffic within specific PVC traffic parameters while managing congestion using proper queuing techniques.

Individual policy maps and class maps are cross-referenced using names generated by Cisco AutoQoS.

How to Interpret the show auto qos Command Output (Cont.)

RMON Traps for Voice Packet Drops

```
rmon event 33333 log trap AutoQoS description "AutoQoS SNMP traps for Voice Drops"
owner AutoQoS

Serial2/1.1: DLCI 58 -
!
interface Serial2/1.1 point-to-point
  frame-relay interface-dlci 58
  class AutoQoS-FR-Serial2/1-58
!
map-class frame-relay AutoQoS-FR-Serial2/1-58
  frame-relay cir 1024000
  frame-relay bc 10240
  frame-relay be 0
  frame-relay mincir 1024000
  service-policy output AutoQoS-Policy-Se2/1.1-Parent
```

Applying all to the DLCI
(or Policy Map to the Serial in Non-Frame Relay)

Frame Relay Traffic Parameters

The **show auto qos** output also displays the information that Remote Monitoring (RMON) traps logging voice packet drops is enabled, which can be used for monitoring and troubleshooting.

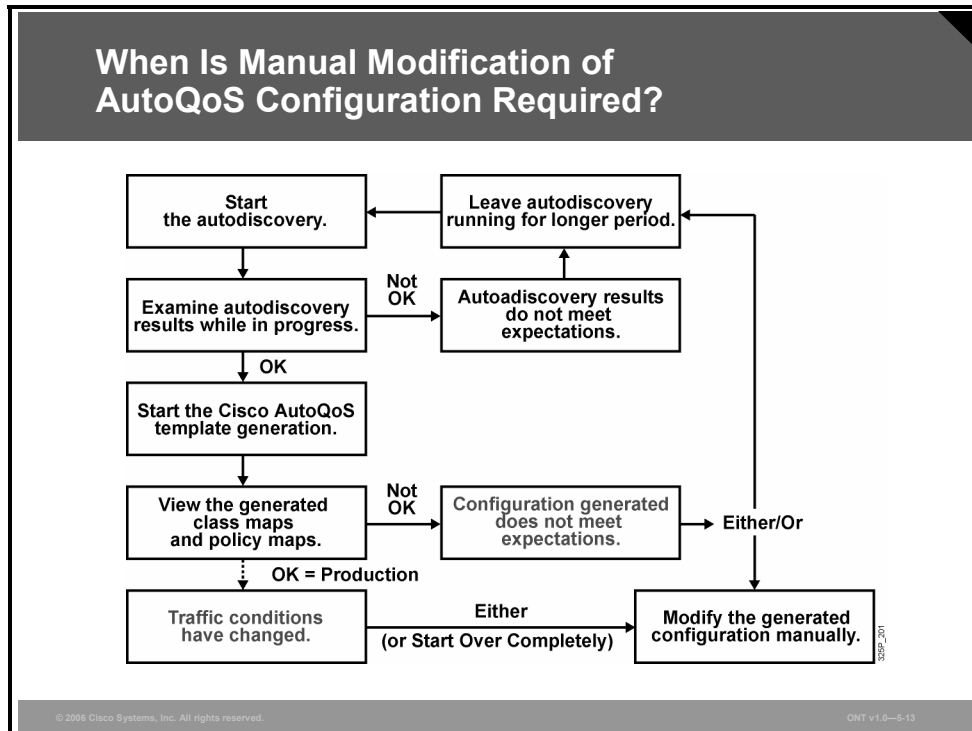
In some situations, as shown in the output for Frame Relay, Cisco AutoQoS also projects new traffic parameters. Here, Cisco AutoQoS generated the new Frame Relay map class, which is mapped to the specific DLCI using the invented map class name.

Finally, the **show auto qos** output displays how the QoS policy was applied in the configuration. In this case, the service policy was applied to the new Frame Relay map class, which in turn was mapped to the DLCI.

In addition to the contents of the interface configurations, you can also display policy maps and class maps using the **show auto qos** command. Access control lists (ACLs) are displayed if Cisco AutoQoS generated them.

Modifying the Active Cisco AutoQoS Configuration with MQC

This topic explains the procedure for modifying Cisco AutoQoS configurations with MQC.



If the policy maps and class maps created on the basis of the templates generated by the Cisco AutoQoS for the Enterprise do not meet the needs of the enterprise network, the policy maps and class maps can be modified using the appropriate Cisco IOS commands.

This issue usually occurs in two situations:

- The new configuration that was generated by Cisco AutoQoS does not meet specific enterprise expectations.
- Network or traffic conditions have changed while Cisco AutoQoS generated the configuration, and network administrators have the necessary skills to adapt the existing QoS configuration rather than running the whole Cisco AutoQoS deployment procedure again.

Caution Although you can modify the policy maps and class maps, they may not be removed properly when Cisco AutoQoS for the Enterprise is disabled using the **no auto qos** command. You may have to manually remove any modified policy maps and class maps.

Modifying the Active Cisco AutoQoS Configuration with MQC: Classification

Most commonly, Cisco AutoQoS uses NBAR and ACLs for traffic classification. But any Cisco MQC classification mechanism can supplement or replace the configuration generated by Cisco AutoQoS.

Classification

- **Generated Cisco AutoQoS classification uses NBAR and ACLs.**
- **Any MQC classification mechanism can manually tune the generated classification:**
 1. **Start the autodiscovery and review the generated results (or take the active classification if Cisco AutoQoS is already activated).**
 2. **Copy the generated classification and modify it offline.**
 3. **Apply the modified classification to a router.**

```
class-map match-any AutoQoS-Voice-Se2/1.1
match protocol rtp audio
!
class-map match-any AutoQoS-Signaling-Se2/1.1
match access-group 101
match protocol rtcp
!
class-map match-any AutoQoS-Transactional-Se2/1.1
match protocol sqlnet
match protocol citrix
!
access-list 101 permit tcp any any eq 1719
access-list 101 permit tcp any any eq 1720
access-list 101 permit udp any any eq 2427
access-list 101 permit udp any any eq 2428
```

} H.323

} MGCP

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0—5-14

Significant skills and MQC knowledge are required to perform the modification, but this procedure can adapt the classification to even the most complex classification rules. Classification can be modified either after the Cisco AutoQoS discovery but before the generated policy templates are applied or after the policy templates generated by Cisco AutoQoS are applied. There are several ways to tune and modify the existing class maps:

- Directly at the router command-line interface (CLI) using MQC
- Using Cisco QoS Policy Manager (QPM)

However, the easiest way to tune the existing class maps is to copy them into a text editor and modify the configuration offline. Add the desired new classification and remove the undesired existing classification. When the modification is complete, simply copy the new classification from the editor and paste it to a router configuration prompt to push the rules through the built-in parser of the router.

If required, the tuning procedure can be repeated in an iterative process until the optimal configuration is achieved.

Classification (Cont.)

```
router(config-cmap)#
```

```
match input-interface interface-name
match cos cos-value [cos-value cos-value cos-value]
match ip precedence ip-prec-value [ip-prec ...]
match ip dscp ip-dscp-value [ip-dscp-value ...]
match ip rtp starting-port-number port-range
```

- Besides NBAR and ACLs, these major MQC classification options can be used for tuning.
- These classification options can be used in any combination as needed to meet specific classification requirements.

© 2006 Cisco Systems, Inc. All rights reserved.

ONT v1.0-5.15

Cisco MQC offers a broad range of classification options, which can be used to add to the class map rules generated by Cisco AutoQoS. The most common classification options and their respective **match** commands are listed in the table.

match Command Syntax	Traffic Classified
<code>match input-interface interface-name</code>	All traffic coming from the specified ingress interface is matched.
<code>match cos cos-value [cos-value cos-value cos-value]</code>	Traffic with the specified Layer 2 CoS value is matched. Allowed CoS values are 0-7.
<code>match ip precedence ip-prec-value [ip-prec-value...]</code>	Traffic with the specified Layer 3 IP precedence value is matched. Allowed IP precedence values are 0-7.
<code>match ip dscp ip-dscp-value [ip-dscp-value...]</code>	Traffic with the specified Layer 3 DSCP value is matched. Generally used DSCP values are default, cs1-cs7, ef, af11-13, af21-23, af31-33, and af41-43.
<code>match ip rtp starting-port-number port-range</code>	RTP traffic with UDP port numbers falling within the defined range is matched.

Besides these classification options, any classification supported by Cisco MQC can be used in any combination to meet specific classification requirements.

The following is an example of classification tuning using the MQC:

1. Start the Cisco AutoQoS discovery process.

```
Router#configure terminal
Router(config)#interface serial0/1/0
Router(config-if)#bandwidth 384
Router(config-if)#auto discovery qos
Router(config-if)#end
```

2. Leave the Cisco AutoQoS discovery running for several days.

3. Review the Cisco AutoQoS discovery results and identify classification changes required (only the classification portion is shown).

```
Router#show auto discovery qos
Output omitted..
!
Suggested AutoQoS Policy for the current uptime:
class-map match-any AutoQoS-Voice-Se0/1/0
  match protocol rtp audio
!
class-map match-any AutoQoS-Signaling-Se0/1/0
  match protocol h323
!
class-map match-any AutoQoS-Transactional-Se0/1/0
  match protocol sqlnet
  match protocol citrix
!
class-map match-any AutoQoS-Bulk-Se0/1/0
  match protocol exchange
  match protocol ftp
!
class-map match-any AutoQoS-Scavenger-Se0/1/0
  match protocol kazaa2
!
class-map match-any AutoQoS-Management-Se0/1/0
  match protocol ldap
```

Necessary classification changes include these:

- Step 1** Also classify Session Initiation Protocol (SIP) and Media Gateway Control Protocol (MGCP) signaling.
- Step 2** Classify Telnet traffic as Transactional class.
- Step 3** Move the SQL classification from the Transactional class to the Bulk class.
- Step 4** Classify all SNMP traffic coming from the IP subnet 193.87.95.0 as Management class.

4. Apply the generated Cisco AutoQoS policy template to the interface for later modification.

```
Router#configure terminal
Router(config)#interface serial0/1/0
Router(config-if)#auto qos
Router(config-if)#end
```

5. Modify the classification generated by Cisco AutoQoS according to the requirements.

- Step 1** Also classify SIP and MGCP signaling.

```
Router#configure terminal
Router(config)#class-map AutoQoS-Signaling-Se0/1/0
Router(config-cmap)#match protocol sip
Router(config-cmap)#match protocol mgcp
Router(config-cmap)#exit
```

- Step 2** Classify Telnet traffic as Transactional.

```
Router(config)#class-map AutoQoS-Transactional-Se0/1/0
Router(config-cmap)#match protocol telnet
Router(config-cmap)#exit
```

Step 3 Move the SQL classification from the Transactional class to the Bulk class.

```
Router(config)#class-map AutoQoS-Transactional-Se0/1/0
Router(config-cmap)#no match protocol sqlnet
Router(config-cmap)#exit
Router(config)#class-map AutoQoS-Bulk-Se0/1/0
Router(config-cmap)#match protocol sqlnet
Router(config-cmap)#exit
```

Step 4 Classify all SNMP traffic coming from the IP subnet 193.87.95.0 as Management class.

```
Router(config)#access-list 101 permit udp 193.87.95.0 0.0.0.255 any eq snmp
Router(config)#class-map AutoQoS-Management-Se0/1/0
Router(config-cmap)#match access-group 101
Router(config-cmap)#end
```

6. Review the new classification policy (only the classification portion is shown).

```
Router#show auto qos
Output omitted..
!
Suggested AutoQoS Policy for the current uptime:
class-map match-any AutoQoS-Voice-Se0/1/0
  match protocol rtp audio
!
class-map match-any AutoQoS-Signaling-Se0/1/0
  match protocol h323
  match protocol sip
  match protocol mgcp
!
class-map match-any AutoQoS-Transactional-Se0/1/0
  match protocol telnet
  match protocol citrix
!
class-map match-any AutoQoS-Bulk-Se0/1/0
  match protocol exchange
  match protocol ftp
  match protocol sqlnet
!
class-map match-any AutoQoS-Scavenger-Se0/1/0
  match protocol kazaa2
!
class-map match-any AutoQoS-Management-Se0/1/0
  match protocol ldap
  match access-group 101
!
access-list 101 permit udp 193.87.95.0 0.0.0.255 any eq snmp
```


Modifying the Active Cisco AutoQoS Configuration with MQC: Policy

When you are generating QoS policy templates, Cisco AutoQoS enables several Cisco IOS QoS mechanisms.

Policy

Generated Cisco AutoQoS policy uses:

- Scheduling: LLQ and CBWFQ (both percentage based) and WRR
- Marking: Class-based Marking to re-mark the packets based on their class membership
- Shaping: Class-based Shaping and FRTS
- Link efficiency: cRTP and LFI
- Congestion avoidance: WRED

```
policy-map AutoQoS-Policy-Se4/0
class AutoQoS-Voice-Se4/0
  priority percent 70
  compress header ip
  set dscp ef
class AutoQoS-Inter-Video-Se4/0
  bandwidth remaining percent 10
  set dscp af41
class AutoQoS-Transactional-Se4/0
  bandwidth remaining percent 1
  set dscp af21
class class-default
  fair-queue
```

Any MQC policy mechanism can manually tune the generated policy with the same procedure used for classification.

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0—5-16

The Cisco IOS QoS mechanisms that Cisco AutoQoS enables include these:

- Traffic scheduling and congestion management using LLQ, CBWFQ, or WRR
- Traffic marking using class-based marking
- Traffic shaping using class-based shaping or FRTS
- Link efficiency using cRTP and LFI (MLP or FRF.12)
- Congestion avoidance using WRED

Besides these policies selected by Cisco AutoQoS, the resulting policy configuration generated can be tuned with any available Cisco IOS MQC policy option. A broad range of options is supported in Cisco IOS software to implement DiffServ per-hop behaviors (PHBs) and adapt to any enterprise policy.

The procedure for modifying an existing, active policy generated by Cisco AutoQoS is similar to the procedure for classification. The following is an example of policy modification:

1. Review the existing QoS policy, identify the new requirements, and outline the configuration modifications necessary (only the policy section is shown).

```
Router#show auto discovery qos
Output omitted..
!
Suggested AutoQoS Policy for the current uptime:
policy-map AutoQoS-Policy-Se0/1/0
  class AutoQoS-Voice-Se0/1/0
    priority percent 10
```

```

compress header ip
set dscp ef
class AutoQoS-Signaling-Se0/1/0
  bandwidth remaining percent 4
  set dscp cs3
class AutoQoS-Transactional-Se0/1/0
  bandwidth remaining percent 40
  random-detect dscp-based
  set dscp af21
class AutoQoS-Bulk-Se0/1/0
  bandwidth remaining percent 19
  random-detect dscp-based
  set dscp af11
class AutoQoS-Scavenger-Se0/1/0
  bandwidth remaining percent 1
  set dscp cs1
class AutoQoS-Management-Se0/1/0
  bandwidth remaining percent 6
  set dscp cs2
class class-default
  fair-queue

```

Necessary policy changes include these:

- Step 1** Mark the voice signaling traffic with DSCP AF31, instead of the current CS3.
- Step 2** Rate-limit the scavenger traffic to a maximum of 64 kbps.
- Step 3** Guarantee minimally 10 percent of the available interface bandwidth to the best-effort traffic.
- Step 4** Mark the management traffic with DSCP AF21, instead of the current CS2.

2. Modify the policy generated by Cisco AutoQoS according to the new requirements.

- Step 1** Mark the voice signaling traffic with DSCP AF31, instead of the current CS3.

```

Router#configure terminal
Router(config)#policy-map AutoQoS-Policy-Se0/1/0
Router(config-pmap)#class AutoQoS-Signaling-Se0/1/0
Router(config-pmap-c)#no set dscp cs3
Router(config-pmap-c)#set dscp af31
Router(config-pmap-c)#exit

```

- Step 2** Rate-limit the scavenger traffic to a maximum of 64 kbps.

```

Router(config-pmap)#class AutoQoS-Scavenger-Se0/1/0
Router(config-pmap-c)#police 64000 conform-action transmit exceed-action drop
Router(config-pmap-c)#exit

```

- Step 3** Guarantee minimally 10 percent of the available interface bandwidth to the best-effort traffic.

```

Router(config-pmap)#class class-default
Router(config-pmap-c)#bandwidth remaining percent 10
Router(config-pmap-c)#exit

```

- Step 4** Mark the management traffic with DSCP AF21, instead of the current CS2.

```

Router(config-pmap)#class AutoQoS-Management-Se0/1/0
Router(config-pmap-c)#no set dscp cs2
Router(config-pmap-c)#set dscp af21
Router(config-pmap-c)#end

```

3. Review the new service policy (only the policy portion is shown).

```
Router#show auto qos
Output omitted..
!
Suggested AutoQoS Policy for the current uptime:
policy-map AutoQoS-Policy-Se0/1/0
  class AutoQoS-Voice-Se0/1/0
    priority percent 10
    compress header ip
    set dscp ef
  class AutoQoS-Signaling-Se0/1/0
    bandwidth remaining percent 4
    set dscp af31
  class AutoQoS-Transactional-Se0/1/0
    bandwidth remaining percent 40
    random-detect dscp-based
    set dscp af21
  class AutoQoS-Bulk-Se0/1/0
    bandwidth remaining percent 19
    random-detect dscp-based
    set dscp af11
  class AutoQoS-Scavenger-Se0/1/0
    bandwidth remaining percent 1
    set dscp cs1
    police 64000 conform-action transmit exceed-action drop
  class AutoQoS-Management-Se0/1/0
    bandwidth remaining percent 6
    set dscp af21
  class class-default
    bandwidth remaining percent 10
```

Summary

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

Summary

- **Cisco AutoQoS employs the DiffServ QoS mechanisms of Cisco IOS software.**
- **DiffServ functions are automated and simplified to expedite deployment of QoS features.**
- **Cisco AutoQoS configures QoS parameters and optimal voice performance based upon Cisco best-practice recommendations.**
- **Cisco AutoQoS generates up to 10 DiffServ classes.**
- **The show auto qos command displays the Cisco AutoQoS templates.**
- **Cisco AutoQoS templates can be reviewed and fine-tuned with any MQC classification or policy mechanism.**

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0-5-17

References

For additional information, refer to this resource:

- Cisco Systems, Inc. *Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.3* at http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgr/qos_vcg.htm.

Module Summary

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

Module Summary

- **Cisco AutoQoS, supported on routers and switches, significantly simplifies QoS deployments and reduces human error.**
- **Cisco AutoQoS mitigates common problems by automating the deployment of QoS policies.**

© 2006 Cisco Systems, Inc. All rights reserved. OMT v1.0—5-1

Different implementation options are available for Quality of Service. The Cisco AutoQoS is one of them and simplifies configuration of QoS. It is supported on most of the routers and switches. The mechanism takes into account interface bandwidth, traffic pattern discovery and Cisco best practices when configuring QoS. As the system works automatically human error and some common problems are reduced.

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 two statements are true about Cisco AutoQoS? (Choose two.) (Source: Introducing Cisco AutoQoS)
- A) Cisco AutoQoS has evolved over two phases: AutoQoS for SP and AutoQoS for the Enterprise.
 - B) Cisco AutoQoS has evolved over two phases: AutoQoS VoIP and AutoQoS for the Enterprise.
 - C) Cisco AutoQoS for the Enterprise is supported on Cisco router and switch platforms.
 - D) Before you configure Cisco AutoQoS, CEF must be enabled.
 - E) Cisco AutoQoS is deployed on switches in two phases: autodiscovery and generating MQC-based policies.
- Q2) Which two DiffServ QoS mechanisms are NOT enabled by Cisco AutoQoS? (Choose two.) (Source: Mitigating Common Cisco AutoQoS Issues)
- A) traffic classification using NBAR
 - B) traffic shaping with class-based shaping
 - C) congestion management with CQ
 - D) congestion avoidance using WRED
 - E) traffic policing using CAR
- Q3) Which three statements correctly describe NBAR capabilities to discover and classify traffic types? (Choose three.) (Source: Introducing Cisco AutoQoS)
- A) NBAR can classify applications based on how much they utilize the network.
 - B) NBAR can classify static applications that establish sessions to well-known TCP or UDP destination port numbers.
 - C) NBAR is not able to discover any non-IP protocols.
 - D) NBAR can classify dynamic applications that use multiple sessions using dynamic TCP or UDP port numbers.
 - E) NBAR can also classify some applications using non-IP protocols.
 - F) NBAR cannot classify HTTP sessions based on the requested URL, MIME type, or host name.
- Q4) Which three prerequisites must be met before configuring Cisco AutoQoS on Cisco routers? (Choose three.) (Source: Introducing Cisco AutoQoS)
- A) No QoS policies (service policies) can be attached to the interface.
 - B) NBAR discovery must be enabled on router interface to support the Cisco AutoQoS discovery process.
 - C) High-speed interfaces or subinterfaces must have an IP address attached.
 - D) CEF must be enabled.
 - E) All interfaces or subinterfaces must be properly configured with the **bandwidth** command.
 - F) Router must host the SNMP server for SNMP traps support.

- Q5) Which statement correctly describes how a router distinguishes between low- and high-speed interfaces? (Source: Introducing Cisco AutoQoS)
- A) Synchronous serial interfaces are classified as low speed if the bandwidth is less than 768 kbps. A synchronous serial interface is classified as high speed if its bandwidth is greater than or equal to 768 kbps.
 - B) Synchronous serial interfaces are classified as low speed if the bandwidth is less than 768 kbps. A synchronous serial interface is classified as high speed if its bandwidth is greater than 768 kbps.
 - C) Synchronous serial interfaces are classified as low speed if the bandwidth is less than or equal to 768 kbps. A synchronous serial interface is classified as high speed if its bandwidth is greater than 768 kbps.
 - D) None of the above is correct.

- Q6) Pair the commands with their descriptions. (Source: Introducing Cisco AutoQoS)

- _____ 1. starts the Cisco AutoQoS discovery process and data collection for Cisco AutoQoS VoIP
 - _____ 2. starts the Cisco AutoQoS discovery process and data collection for Cisco AutoQoS for the Enterprise
 - _____ 3. generates and installs the QoS policy for VoIP
 - _____ 4. generates and installs the QoS policy based on the Cisco AutoQoS discovery results and uses NBAR for classification
 - _____ 5. generates and installs the QoS policy based on the Cisco AutoQoS discovery results, while trusting the ingress DSCP marking
 - _____ 6. enables the trusted boundary feature on the Cisco Catalyst switch interface and trusts all ingress marking
- A) auto qos trust
 - B) **auto qos voip**
 - C) **auto qos**
 - D) **auto qos voip cisco-phone**
 - E) **auto discovery qos**
 - F) no such command

- Q7) The _____ command is used to display the results of the Cisco AutoQoS discovery phase for all router interfaces. (Source: Introducing Cisco AutoQoS)

-
- Q8) Which command is used on Cisco Catalyst switches to display the Cisco AutoQoS configuration that was initially applied? (Source: Introducing Cisco AutoQoS)

- A) show auto qos interface all
- B) **show auto discovery qos**
- C) **show auto qos**
- D) **show auto**

- Q9) Which four DiffServ classes are automatically provisioned by Cisco AutoQoS?
(Choose four.) (Source: Mitigating Common Cisco AutoQoS Issues)
- A) IP routing
 - B) streaming voice
 - C) interactive voice
 - D) transactional
 - E) bulk data
 - F) broadcast video
 - G) LAN
- Q10) Which three statements describe the most common Cisco AutoQoS issues? (Choose three.) (Source: Mitigating Common Cisco AutoQoS Issues)
- A) Cisco AutoQoS always generates 10 classes, which does not fit all scenarios.
 - B) Cisco AutoQoS generates more classes than is currently implemented.
 - C) A router must be rebooted after the policy generated by Cisco AutoQoS is applied to its interfaces.
 - D) Cisco AutoQoS does not adapt to changing traffic conditions automatically.
 - E) Cisco AutoQoS does not handle all possible scenarios that may occur and might not fit specific classifications or policies.
 - F) The router interface where the policy generated by Cisco AutoQoS was attached must be shut down and reactivated to apply the policy properly.

Module Self-Check Answer Key

- Q1) B, D
- Q2) C, E
- Q3) B, D, E
- Q4) A, D, E
- Q5) C
- Q6) 1F, 2E, 3B, 4C, 5A, 6D
- Q7) **show auto discovery qos**
- Q8) C
- Q9) A, C, D, E
- Q10) B, D, E

Implement Wireless Scalability

Overview

This module describes wireless security standards and the importance of wireless LAN (WLAN) security. The module also defines and describes in detail the 802.1x standard and various authentication processes. The module concludes with a description of basic WLAN management.

Module Objectives

Upon completing this module, you will be able to describe and configure wireless security and basic wireless management. This ability includes being able to meet these objectives:

- Describe WLAN QoS and its current implementation
- Describe WLAN security fundamentals and various 802.1x EAP types
- Describe configuring an advanced feature set WLAN for encryption and authentication on lightweight access points
- Compare the wireless feature set and architecture of wireless networks using autonomous or lightweight access points

Implementing WLAN QoS

Overview

This lesson describes wireless LAN (WLAN) networks as the extension of wired networks. When voice and video applications are used by wireless clients, quality of service (QoS) is needed. Wired QoS designs and implementations commonly use Layer 3 differentiated services code point (DSCP) or Layer 2 802.1p to ensure priority. However, shared RF wireless does not use this technique. The Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard has many extensions; QoS defined by 802.11e is currently in draft for standardization.

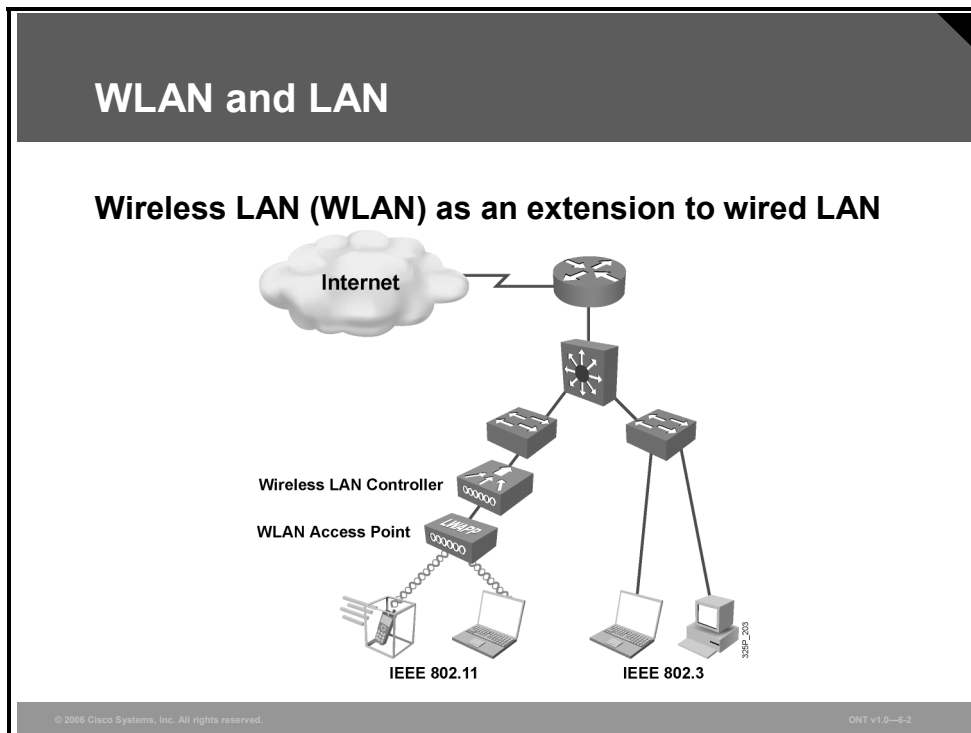
Objectives

Upon completing this lesson, you will be able to describe WLAN QoS and its current implementation. This ability includes being able to meet these objectives:

- Explain the need for WLAN QoS
- Describe WLAN QoS
- Describe the current WLAN QoS implementation
- Configure QoS features on lightweight access points through the use of WLCs

The Need for WLAN QoS

This topic describes the need for wireless QoS.



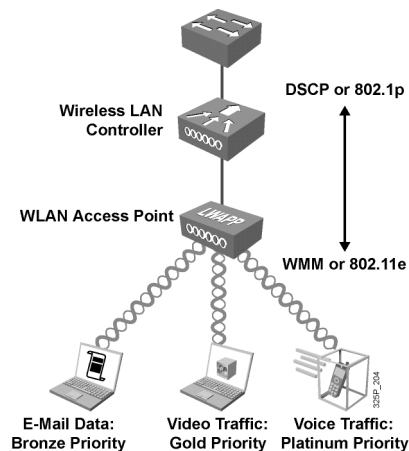
Wired LANs require that users locate in one place and stay there. Wireless LANs (WLANs) are an extension to the wired LAN network. WLANs can be an overlay to or substitute for traditional wired LAN networks. Both WLANs and wired LANs define the physical and data link layers and use MAC addresses. The same protocols and applications can be used over LANs and WLANs. Examples of such protocols are the IP and IPsec protocols for virtual private networks (VPNs). Examples of applications are web, FTP, and Simple Network Management (SNMP) management.

WLANs use carrier sense multiple access with collision avoidance (CSMA/CA) technology instead of the carrier sense multiple access with collision detection (CSMA/CD) technology that is used by Ethernet LANs. Collision detection is not possible in wireless applications because a sending station cannot receive at the same time that it is transmitting and, therefore, cannot detect a collision. Wireless 802.11 LANs try to avoid collisions instead of dealing with them after the fact as in 802.3. Wireless 802.11 deploys a Distributed Coordination Function (DCF) to avoid collisions, with the use of RF carrier sense, interframe spacing, and random wait timers to avoid collisions.

The Need for QoS Wireless

QoS extension to 802.11 to provide more consistent and quality RF transmission for:

- Voice
- Video



Quality of service (QoS) refers to the ability to allocate shared network resources in such a way that selected network traffic, such as that for voice and multimedia applications, receives enhanced service. With QoS, time-sensitive multimedia and voice traffic receives a higher priority, greater bandwidth, and less delay than best-effort data traffic. QoS provides enhanced and predictable network service:

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

Wired QoS designs and implementations commonly use Layer 3 differentiated services code point (DSCP) or Layer 2 802.1p to ensure priority. However, shared RF wireless does not use these techniques. IEEE has many extensions to 802.11 wireless, including QoS as defined by 802.11e, which is currently in draft for standardization.

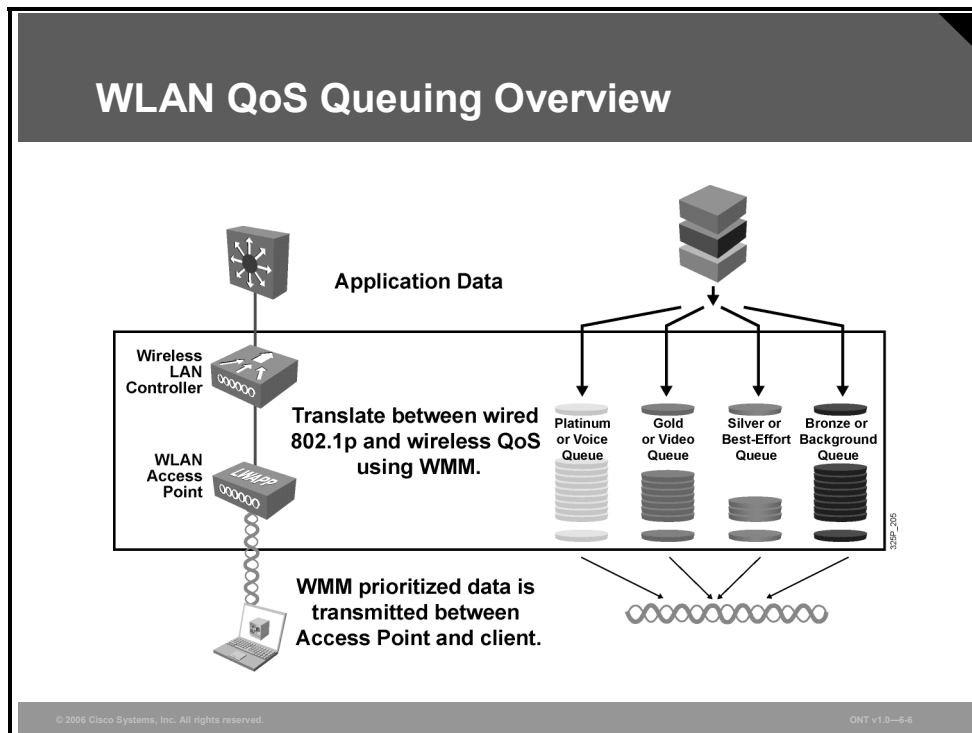
To speed the adoption of QoS in the 802.11 marketplace, the Wi-Fi Alliance has released a Wi-Fi Multimedia (WMM) standard for current implementation. WMM is a subset of the 802.11e standard that reduces the eight priority levels to four access categories.

Note The term “access category” is synonymous with priority level.

The resulting QoS allows translation from 802.1p or DSCP to appropriate RF techniques giving high-priority traffic an increased probability of RF transmission over lower-priority traffic.

WLAN QoS Description

This topic describes QoS in WLAN environment.



The WMM traffic prioritization method put forward by the Wi-Fi Alliance is used to determine the assignment of application data headed to the client. WMM is an enhancement to the MAC sublayer to add QoS functionality to Wi-Fi networks. WMM is an extension to the prior CSMA/CA-based DCF mechanism that gives all devices the same priority and that is based on a best-effort, “listen-before-talk” algorithm. Each client waits a random backoff time, and then it transmits only if no other device is transmitting at that time. This collision-avoidance method gives all the devices the opportunity to transmit, but when traffic demand is high and networks can become overloaded, the performance of all devices will be equally affected.

WMM introduces traffic-prioritization capabilities based on the four defined access categories. RF prioritization allows a higher access category the increased probability of being transmitted first. This allows the platinum level to obtain RF access for transmission before the gold, silver, or bronze levels. The access categories were designed to correspond to 802.1p or DSCP priorities to facilitate interoperability with QoS policy-management mechanisms. WMM priorities coexist with legacy devices that are not WMM-enabled. Packets not assigned to a specific access category are categorized by default as the best-effort access category. WMM prioritization maps four independent transmit queues to eight 802.1e priority levels, as listed in the table.

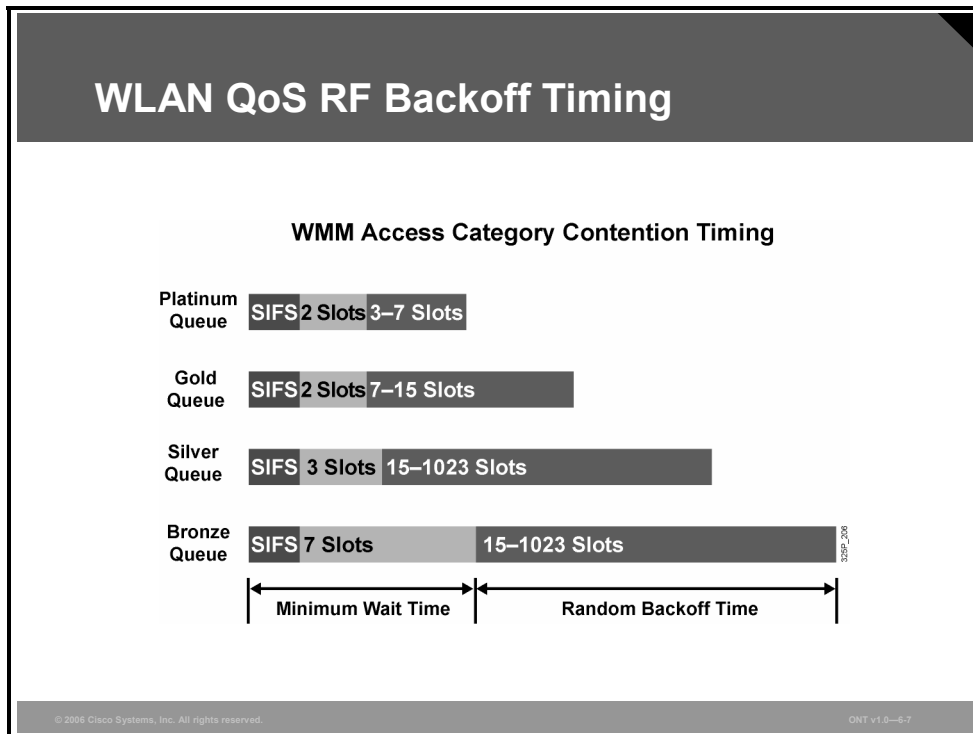
Four Access Categories Compared to Eight Priority Levels for 802.11e

WMM	802.11e
Voice	6 or 7
Video	4 or 5
Background	1 or 2
Best effort	0 or 3

Note Best effort with a value of 0 or 3 allows for prioritization above or below background.

WLAN QoS RF Backoff Timing

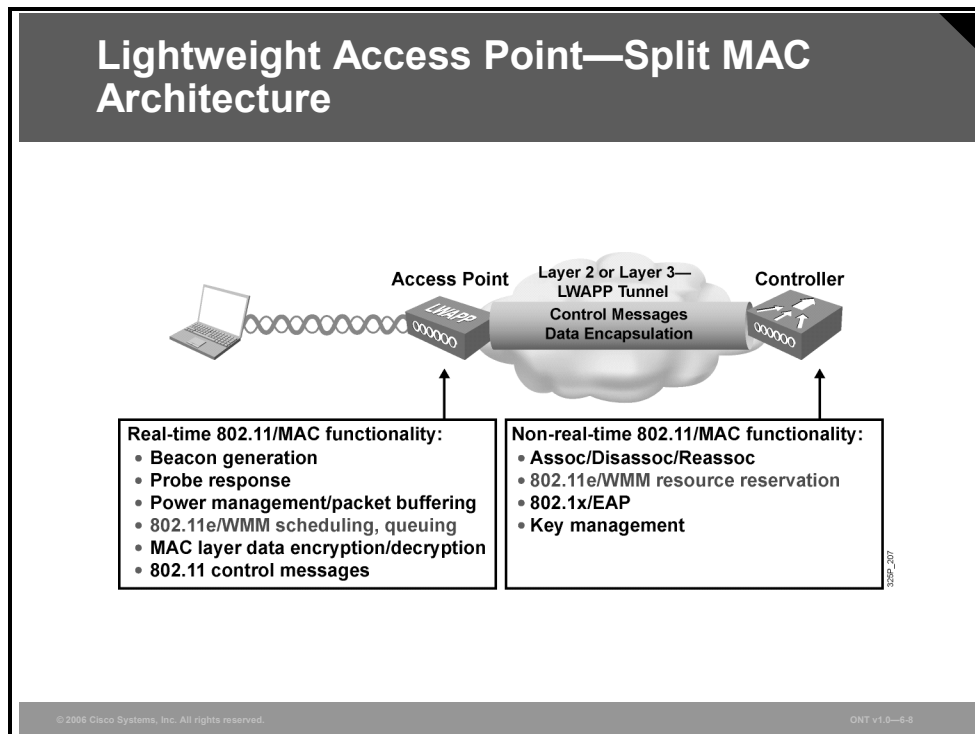
Instead of DCF, Enhanced DCF (EDCF) is used for CSMA/CA wireless QoS frame transmission.



The IEEE 802.11e supplements to 802.11, and therefore the WMM subset, replace the use of DCF with EDCF for CSMA/CA wireless frame transmission. WMM provides priority access to the RF medium in two ways. First, the wireless access point must prioritize the data into four access categories (from highest to lowest, platinum, gold, silver, and bronze). Second, the lower-priority traffic must use longer interframe wait timers allowing higher-priority traffic access to the wireless network first. The timers result from a summarization of the fixed short interframe space (SIFS), slot times (fixed-length time intervals based on priority), and a random slot timer (based on priority). The random backoff slot timers prevent media contention among traffic from within the same access category.

Lightweight Access Point—Split MAC Architecture

Lightweight Access Point Protocol (LWAPP) changed the way that WLAN deployments were managed with the concept of a “split MAC”—the ability to separate the real-time aspects of the 802.11 protocol from most of its management aspects.



Cisco has designed a centralized, lightweight access point wireless architecture to address the unique RF management needs of enterprises. A core component is its split MAC architecture, where the processing of 802.11 data and management protocols and access point capabilities is distributed between a lightweight access point and a centralized WLAN controller.

More specifically, time-sensitive activities, such as beacon handling, handshakes with clients, MAC layer encryption, and RF monitoring, are handled in the access point. All other functions are handled in the WLAN controller, where systemwide visibility is required. These functions include IEEE 802.11 management protocol, frame translation, and bridging functions, as well as systemwide policies for user mobility, security, QoS, and, perhaps most importantly, real-time RF management.

QoS WLAN Deployment Issues

End-to-end QoS implementation requires mapping between Layer 2 802.1p or Layer 3 DSCP and wireless RF using 802.11e or WMM.

QoS WLAN Deployment Issues

- **Wireless RF is a Layer 2 technology and therefore based on 802.11e or WMM, versus Layer 3 DSCP.**
- **Layer 2 marking will be lost in end-to-end transit, losing QoS information.**
- **Access points connect to switches as access ports versus trunks and lack 802.1p trunk tagging.**
- **The goal is to utilize the Layer 3 DSCP information to preserve end-to-end QoS in the absence of Layer 2 QoS information.**

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0-6.9

End-to-end QoS is based on the use of DSCP for packet marking, while wireless RF uses Layer 2 marking. It is possible that the Layer 2 header might be removed in transit and QoS information would be lost.

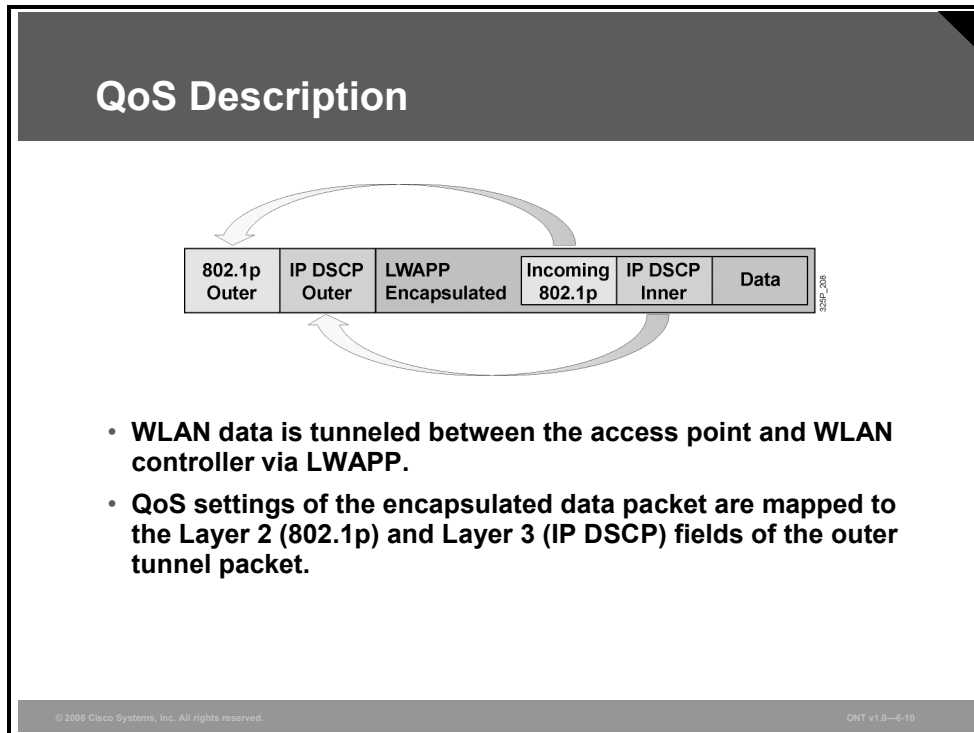
In the Cisco deployment model, traffic destined to access points will not contain 802.1p QoS tag information because the access points connect to a Cisco Catalyst switch port, which is not a trunk. As a result, packets transmitted via a WLAN will also lose Layer 2 QoS information.

It is important to utilize the Layer 3 DSCP information to provide QoS in the absence of Layer 2 QoS information.

WLAN controllers using version 3.2 or later ensure that packets receive proper QoS handling end to end. WLAN controllers ensure that the packet will maintain its QoS information as it traverses the network using RF wireless IEEE 802.1e marking and WMM mappings as appropriate.

QoS Description

The QoS of the encapsulated data packet must be appropriately mapped to the 802.1p and IP DSCP fields of the outer tunnel packet.

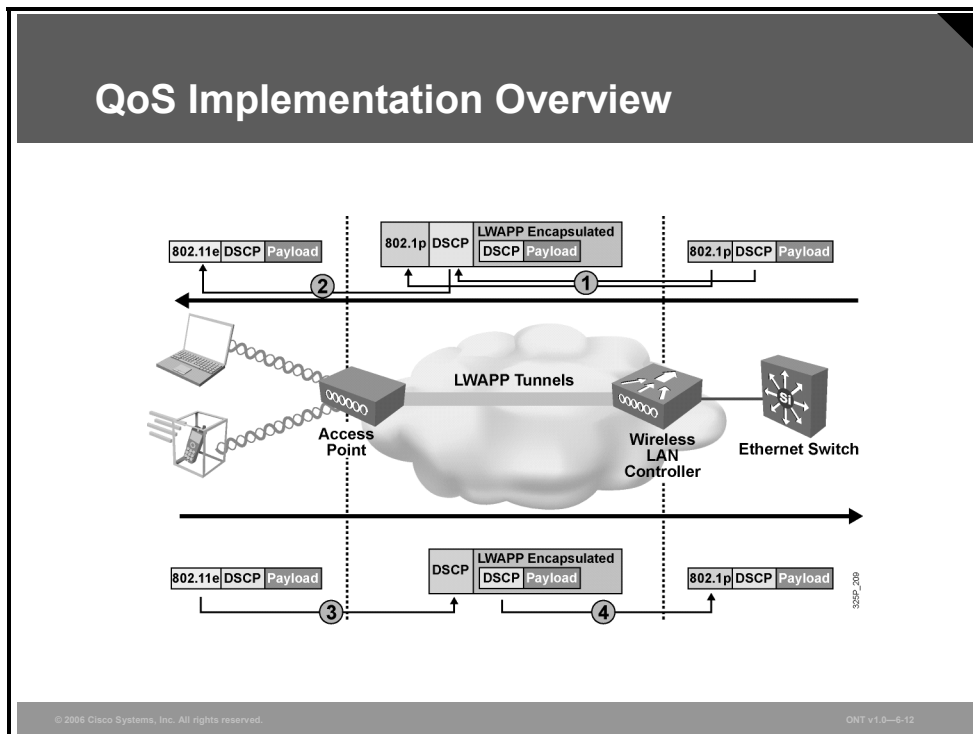


The lightweight access point WLAN solution uses the Layer 3 IP DSCP marking of packets sent by wireless LAN controllers and lightweight access points. The lightweight access point WLAN solution also enhances the way access points use Layer 3 information to ensure that packets receive the correct over-the-air prioritization when transmitted from the access point to the wireless client.

In the lightweight WLAN solution, wireless LAN data is tunneled between the access point and the wireless LAN controller via LWAPP. To maintain the original QoS classification across an LWAPP tunnel, the QoS settings of the encapsulated data packet must be appropriately mapped to the Layer 2 (802.1p) and Layer 3 (IP DSCP) fields of the outer tunnel packet.

WLAN QoS Implementation

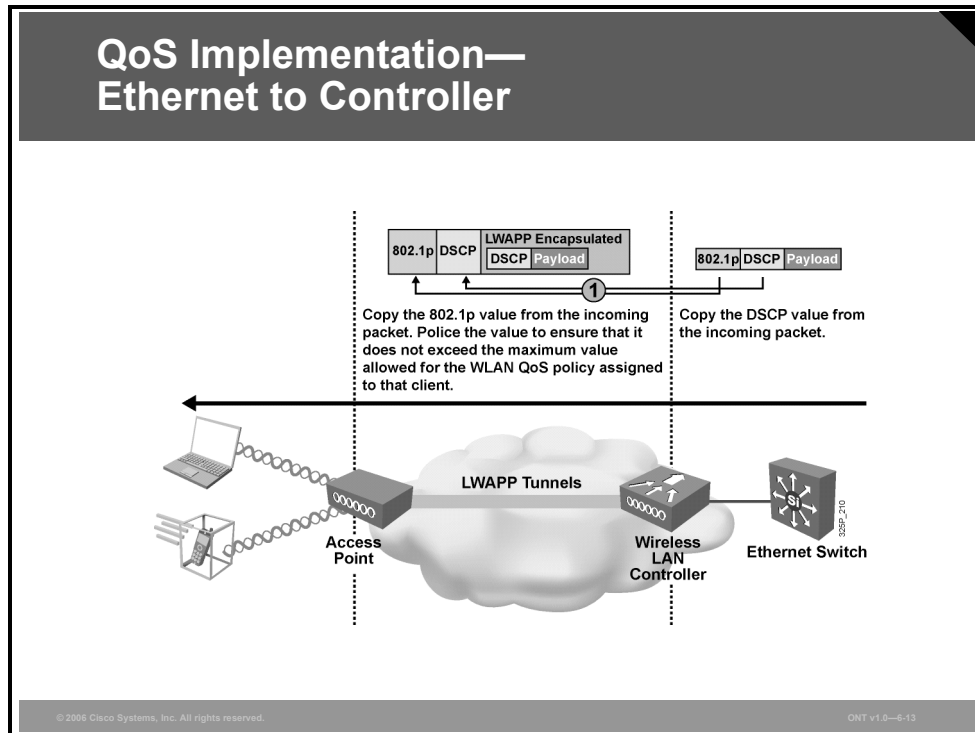
This topic describes the implementation of WLAN QoS. Packets traveling between the wired infrastructure and wireless clients through LWAPP encapsulation need to map prioritization between 802.11e (or WMM), 802.1p, and DSCP.



When WMM or 802.11e traffic is sent by a WLAN client, it has a priority classification marked in its frame. The access point needs to map this WMM or 802.11e classification into a DSCP value for the LWAPP packet carrying the frame to ensure that the packet is given the appropriate priority on its way to the wireless LAN controller. A similar process needs to occur in the opposite direction on the wireless LAN controller for LWAPP packets going to the access point. A mechanism is also needed to classify traffic on both the access point and the wireless LAN controller for non-802.11e clients, so that their LWAPP packets can also be assigned the appropriate default priority.

QoS Implementation—Ethernet to Controller

The outer header in LWAPP packet must contain the QoS information when the packet is forwarded from the Ethernet switch toward an access point via a controller.



This series of subtopics gives the steps of QoS implementation:

- Step 1** The controller copies the DSCP value from the incoming packet. It then translates the DSCP value of the incoming packet to the appropriate 802.1p priority value. These values are placed in the outer header of the LWAPP frame. LWAPP control packets are always tagged with 802.1p of 7, while the LWAPP data packets derive the DSCP and 802.1p value from the original packet.

Feature: QoS Packet Marking Translations

Default mapping between DSCP, 802.1p, and 802.11e exist.

Feature: QoS Packet-Marking Translations			
Cisco 802.1p Priority-Based Traffic Type	DSCP Priority	802.1p Priority	IEEE 802.11e Priority
Reserved	56–62	7	7
IP routing	48	6	7
Voice	46 (EF)	5	6
Video	34 (AF41)	4	5
Voice control	26 (AF 31)	3	4
Background gold	18 AF21)	2	2
Background silver	10 (AF11)	1	1
Best effort	0 (BE)	0	0 or 3

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0–6-14

The following are notes on Layer 3 QoS packet marking enhancements:

- Layer 3 QoS is not supported when you are using Layer 2 LWAPP encapsulation. You must use 802.1p tagging for QoS marking to ensure that packets receive the proper level of QoS.
- The Layer 3 QoS packet marking translations are not configurable.

The benefits of Layer 3 QoS packet marking enhancements include these:

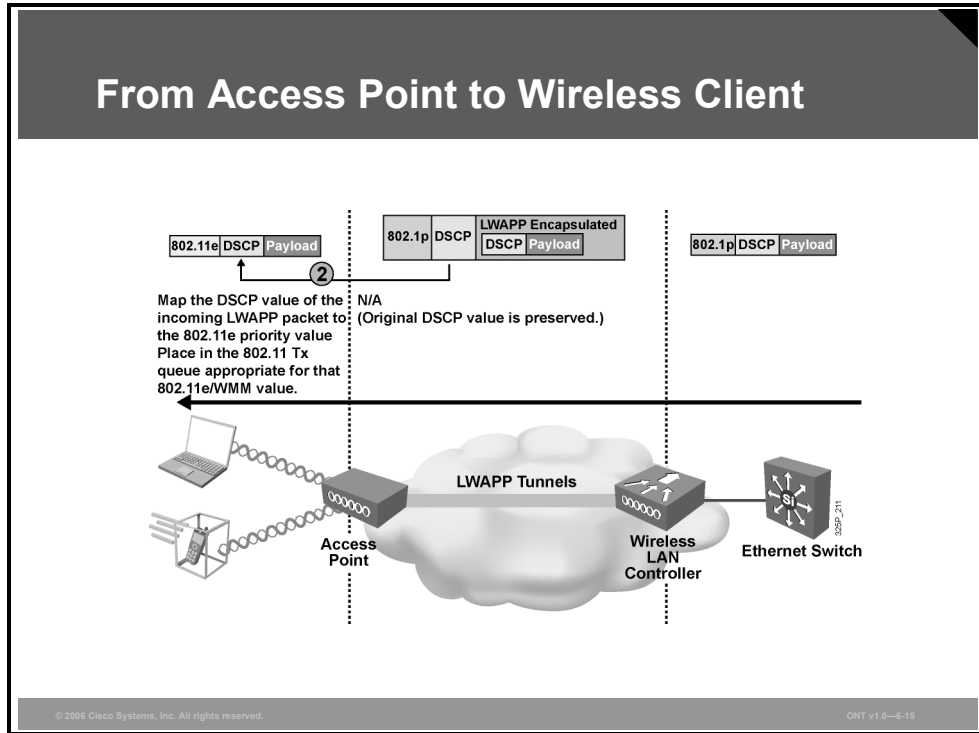
- They ensure that packets receive the proper QoS handling from end to end.
- Policing of 802.11e priority (or WMM), 802.1p, and IP DSCP values ensures that wireless endpoints conform to network QoS policies.

The following are notes on network control (IP DSCP 56, Cisco Unified Communications 802.1p 7, and IEEE 802.1e 7):

- The 802.1p priority level 7 requires special handling because it is reserved for LWAPP control.
- Data packets with a priority of 7 are always degraded to priority 6 or DSCP 46.
- An LWAPP control priority of 7 also translates to DSCP 46 because there are no other logical options.

From Access Point to Wireless Client

When packet is sent from an access point to the client, the DSCP value from the incoming LWAPP packet is mapped to the 802.11e priority value.

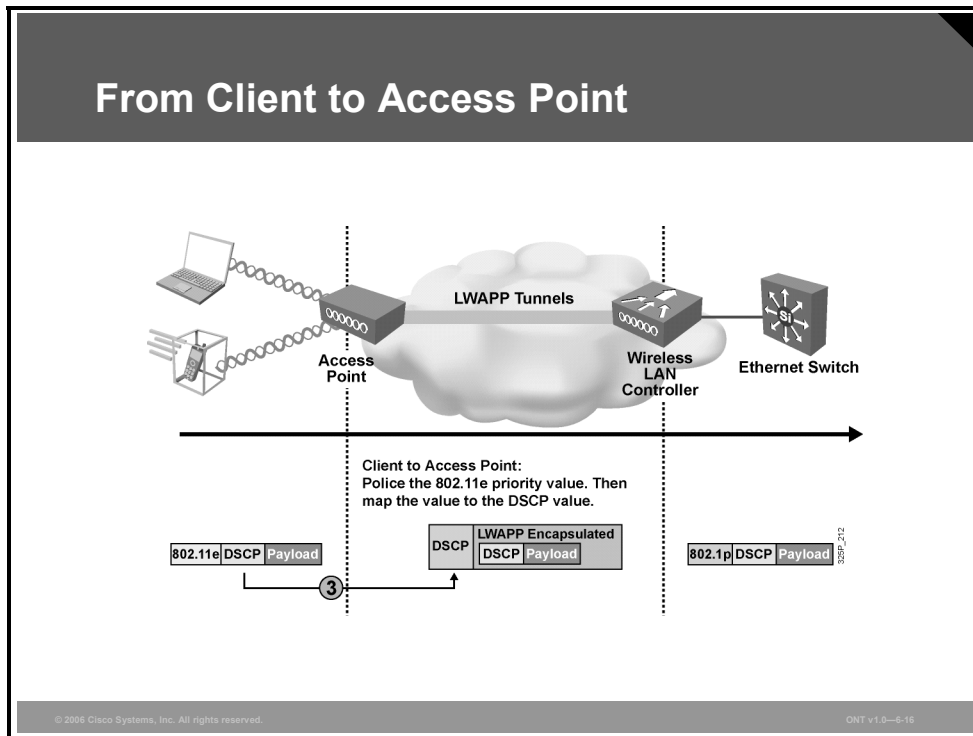


Step 2 For a WMM client, the access point translates the DSCP value of the incoming LWAPP packet to the 802.11e priority value. Police the value to ensure that it does not exceed the maximum value allowed based on the WLAN QoS policy assigned to that client. Then the access point places the packet in the 802.11e transmit queue appropriate for that WMM access category or 802.11e priority level.

For a regular (non-WMM) client, the access point places the packet in the default 802.11e or WMM transmit queue based on the WLAN QoS policy assigned to that client.

From Client to Access Point

When packet is sent from the client to the access point, the 802.11e priority value is mapped to the DSCP value on the access point.



Step 3 When the access point receives an 802.11 frame from a WMM client, it polices the 802.11e priority value to ensure that it does not exceed the maximum value allowed for the QoS policy assigned to that client and then maps the 802.11e priority value to the DSCP value.

When the access point receives a frame from a regular (non-WMM) client, it uses the default 802.11e priority or WMM value for the QoS policy assigned to that client or WLAN ID and translates the value to the DSCP value.

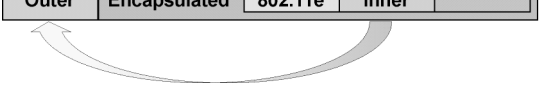
Traffic from Access Point to Controller

When packets from an access point are sent to the controller, the DSCP value is mapped to the outer LWAPP frame.

Traffic from Access Point to Controller

The access point will not send tagged packets on a nontrunk port destined for the controller; therefore, the access point will not copy the 802.11e client incoming priority value to the 802.1p (outer) destined for the switch.

IP DSCP Outer	LWAPP Encapsulated	Incoming 802.11e	IP DSCP Inner	Data
------------------	-----------------------	---------------------	------------------	------



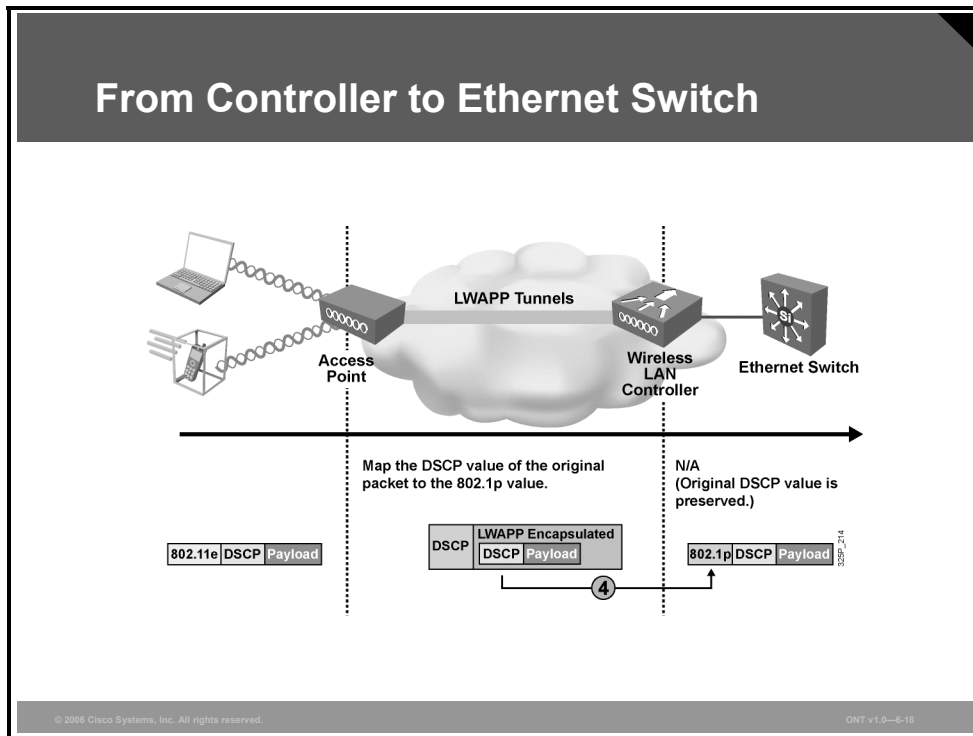
© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0-6-17

The access point does not send tagged packets because doing so causes a problem with Cisco switches not configured for trunking from the access point.

The access point does not copy the 802.11e incoming value to a 802.1p (outer) packet because trunking is not enabled. The DSCP is mapped to the outer frame.

From Controller to Ethernet Switch

The incoming outer DSCP value from an LWAPP packet is used to generate an 802.1p priority value in the packets, which are sent to the Ethernet switch by the controllers.



Step 4 When the controller receives an LWAPP packet, it generates the IEEE 802.1p priority value for the wired side, using the incoming DSCP (outer).

The outer 802.1p value from the access point does not exist anymore because the access point will no longer be sending null VLAN ID frames.

QoS Implementation

This topic describes the process of the QoS implementation.

QoS Implementation

- **802.1p or DSCP-tagged packets received from LAN:**
 - Tag is propagated to LWAPP frame.
 - **WLAN ID-configured QoS takes priority for assigned access category; if tag is lower than configured QoS, access point will queue packet at lower access category.**
 - **AAA override can be applied to Cisco IBNS WLAN clients.**
- **Untagged packets received from LAN:**
 - **WLAN ID-configured QoS will be applied for access category.**
 - **AAA override can be applied to Cisco IBNS WLAN clients.**

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0—6-19

The 802.1p- or DSCP-tagged packets are received from the LAN:

- The tag is propagated to the LWAPP frame.
- The WLAN ID-configured QoS takes priority for the assigned access category; if the tag is lower than the configured QoS, the access point queues the packet at a lower access category.
- An authentication, authorization, and accounting (AAA) override can be applied to Cisco Identity Based Networking Services (IBNS) WLAN clients.

Untagged packets received from the LAN receive the following treatment:

- The WLAN ID-configured QoS is applied for the access category.
- An AAA override can be applied to Cisco IBNS WLAN clients.

QoS Implementation (Cont.)

- **802.11e QoS packets received from WLAN:**
 - Tag is propagated to LWAPP frame.
 - WLAN ID-configured QoS takes priority for assigned 802.1p tag; if 802.11e access category is lower than configured QoS, lower 802.1p tag will be applied.
 - 802.11e QoS packets received from WLAN will be 802.1p-tagged when transmitted on the LAN by the controller.
- **Non-QoS packets received from WLAN will be best effort (default silver) when transmitted on the LAN by the controller.**

© 2006 Cisco Systems, Inc. All rights reserved.

ONT v1.0-6-20

The 802.11e QoS packets received from the WLAN receive this treatment:

- The tag is propagated to the LWAPP frame.
- The WLAN ID-configured QoS takes priority for the assigned 802.1p tag; if the 802.11e access category is lower than the configured QoS, a lower 802.1p tag will be applied.
- The 802.11e QoS packets received from the WLAN are 802.1p-tagged when they are transmitted on the LAN by the controller.

Non-QoS packets received from WLAN will be given best-effort priority (default silver) when they are transmitted on the LAN by the controller.

WLAN QoS Configuration

This topic describes how QoS configurable profiles can be configured on a controller.

QoS-Configurable Profiles

Each level has a configurable per-bandwidth contract rate:

- **Per-user data bandwidth contract**—Configurable peak and average data rate enforcement for non-UDP traffic
- **Per-user real-time bandwidth contract**—Configurable peak and average data rate enforcement for UDP traffic

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0—6-22

QoS-Configurable Profiles

By default, the WLAN priority is set by the slot timers used by EDCF. In addition, a bandwidth contract rate can be configured for each of the four access categories. Each bandwidth contract rate is further divided into average and peak rates of User Datagram Protocol (UDP) or non-UDP traffic. It is recommended that the bandwidth rate be left at the default parameters unless Cisco guideline documents state otherwise.

On the same web page, the “Over the Air QoS” settings control the maximum RF usage from each WMM access category, which by default are all set at 100 percent. The queue depth controls the internal queue depth for each respective access category. The defaults for both parameters are listed in the table.

QoS-Configurable Profiles (Cont.)

Each level has configurable “over the air” QoS rates:

- **Maximum RF usage per access point (%)**—Defined maximum percentage of air bandwidth given to an access category
- **Queue depth**—Defined depth of queue for a particular user level that will cause packets in excess of the defined value to be dropped

The screenshot shows the 'Edit QoS Profile' interface for a profile named 'bronze'. The 'Description' is 'For Background'. Under 'Per-User Bandwidth Contracts (k) *', the values for Average Data Rate, Burst Data Rate, Average Real-Time Rate, and Burst Real-Time Rate are all set to 0. The 'Over the Air QoS' section, which is circled in red, shows 'Maximum RF usage per AP (%)' set to 100 and 'Queue Depth' set to 25. The 'Wired QoS Protocol' section shows 'Protocol Type' as 'None' and '802.1P Tag' as 1. A footnote at the bottom states: '* The value zero (0) indicates the feature is disabled'.

© 2006 Cisco Systems, Inc. All rights reserved.

ONT v1.0-6-23

Access Category	RF Usage	Queue Depth
Platinum	100 percent	100
Gold	100 percent	75
Silver	100 percent	50
Bronze	100 percent	25

QoS-Configurable Profiles (Cont.)

The 802.1p tag is applied to the wired side to allow proper precedence to be applied to traffic across the entire network infrastructure.

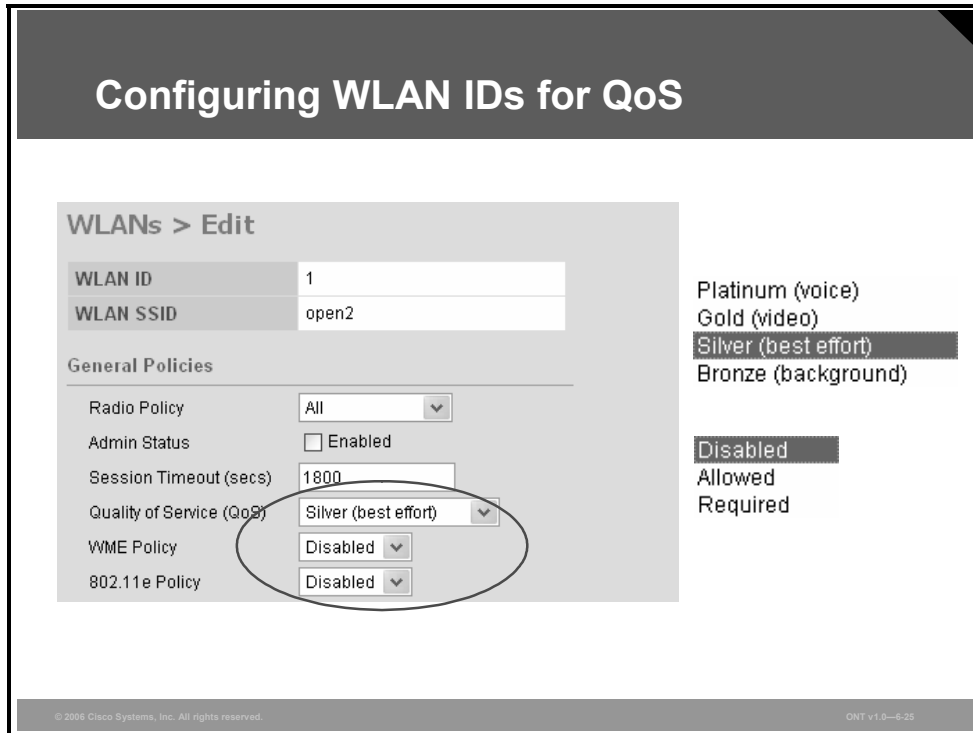
The image shows two side-by-side screenshots of the 'Edit QoS Profile' configuration page. The left screenshot is for the 'bronze' profile, and the right is for the 'platinum' profile. Both screenshots have a circle drawn around the '802.1P Tag' field. In the bronze profile, the tag is set to '1'. In the platinum profile, the tag is set to '6'. The 'Protocol Type' is set to 'None' in both. A note at the bottom of each screenshot states: '* The value zero (0) indicates the feature is disabled'.

The mapping from 802.1p to WMM access categories can also be specified at a broad controller-wide level. The only option for the “Protocol Type” drop-down field is 802.1p. Current (version 3.2) controller codes have the default mappings as listed in the table.

Access Category	802.1p Priority
Platinum	6
Gold	5
Silver	3
Bronze	1

Configuring WLAN IDs for QoS

This section describes how WLAN IDs can be configured individually for QoS on a controller.



The general WMM or 802.11e policy for wireless client interaction to the access point can be controlled at the WLAN ID of the wireless controller. The three possible values are listed and described in the table.

Parameter Value	Description
Disabled	The Disabled parameter simply ignores the WMM or 802.11e QoS request.
Allowed	The Allowed parameter offers QoS to WMM- or 802.11e-capable wireless clients and default QoS for non-WMM/802.11e wireless clients.
Required	The Required parameter requires all wireless clients to be WMM or 802.11e compliant to use any WLAN ID defined by this parameter.

Note The WLAN ID is the association from the WLAN service set identifier (SSID) to a unique internal number, which in turn associates to security policies and the existing Ethernet interface of the controller.

Summary

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

Summary

- **Video and voice applications are used with wireless clients as well as data applications, and QoS is required for them.**
- **802.11e or WMM scheduling and queuing is implemented on access points.**
- **DCSP and 802.1p tagging is used to tag different types of traffic inside LWAPP tunnels.**
- **QoS policies and types of traffic are defined for each WLAN ID in the Wireless LAN Controller.**

Introducing 802.1x

Overview

This lesson describes the evolution of wireless security standards and the 802.1x standard with various 802.1x Extensible Authentication Protocol (EAP) types. The lesson describes basic security issues and their solutions in the evolution of wireless security. The lesson continues with a description of Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2). EAP, defined in the 802.1x standard, and the various types of EAP authentication processes are explained, including Lightweight EAP (LEAP), EAP with Flexible Authentication via Secure Tunneling (EAP-FAST), Protected EAP (PEAP), and EAP with Transport Layer Security (EAP-TLS).

Objectives

Upon completing this lesson, you will be able to describe WLAN security fundamentals and various 802.1x EAP types. This ability includes being able to meet these objectives:

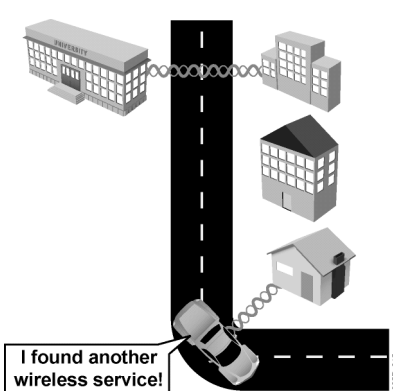
- Explain the need for WLAN security standards and why WLAN security is so important
- Describe the difference between authentication and encryption
- Describe how enhanced 802.11 security improves on basic 802.11 security
- Describe the basic concepts of 802.1x authentication
- Describe LEAP, or EAP Cisco Wireless
- Describe EAP-FAST
- Describe EAP-TLS
- Describe PEAP
- Explain the WPA authentication process

The Need for WLAN Security

This topic describes the need for wireless LAN (WLAN) security and the reasons for WLAN security.

The Need for WLAN Security

- **IEEE 802.11 equipment is widely available and inexpensive.**
- **The 802.11 standard is designed for ease of use and deployment.**
- **Many sniffers are available.**
- **Statistics on WLAN security are not encouraging.**
- **Media reports about hot spots, WLAN hacking, and war driving are frequent.**
- **Encryption is not optimally implemented in standard WEP.**
- **Authentication is vulnerable.**



The illustration shows a car driving on a road that turns a corner. On the left side of the road, there is a building labeled 'SECURITY'. On the right side, there are several houses of varying sizes. A speech bubble from the car says 'I found another wireless service!'. The road is marked with a dashed white line down the center. The image is credited to '© 2006 Cisco Systems, Inc. All rights reserved.' and 'ONT v1.0-6.3'.

With the lower costs of IEEE 802.11b systems, it is inevitable that hackers will have many more unsecured WLANs from which to choose.

Incidents have been reported of people using numerous open source applications to collect and exploit vulnerabilities in the IEEE 802.11 standard security mechanism, Wired Equivalent Privacy (WEP).

Wireless sniffers enable network engineers to passively capture data packets so that they can be examined to correct system problems. These same sniffers can be used by hackers to exploit known security weaknesses.

“War driving” is a phrase that originally referred to someone using a cellular scanning device looking for cell phone numbers to exploit. War driving also refers to someone driving around with a laptop and an 802.11b client card looking for an 802.11b system to exploit.

Most wireless devices sold today are wireless network-ready. End users often do not change the default settings, or they implement only standard WEP security, which is not an optimal solution for secure wireless networks.

With only basic WEP encryption enabled (or, obviously, with no encryption enabled), it is possible to collect data and obtain sensitive network information, such as user login information, account numbers, and personal records.

Security Methods—Authentication and Encryption

This topic describes the difference between authentication and encryption.

Security Methods—Authentication and Encryption

- **Authentication: Proves that you belong on the network**
- **Encryption: Protects the data traversing the network**

Both authentication and encryption are needed and mandated by standards.

© 2006 Cisco Systems, Inc. All rights reserved. OWT v1.0—6-5

The two primary facilities for securing the WLAN are authentication and encryption. Authentication is a process that requires a user to present some form of identifying credentials to be permitted access to a resource.

Encryption is the mechanism that is used to protect the data flowing over the actual data pathway. A common example of encryption is Triple-Data Encryption Standard (3DES), used in many Cisco wired network environments. Typically, a data connection between two devices is encrypted after the user is authenticated and authorized to use the resource.

Current security standards require that both authentication and encryption be used to protect client devices from having their data intercepted and to protect the network from unauthorized clients attempting to access internal data files.

WLAN Security Issues

In the past, security on WLANs was not a major concern. This lack of concern was, in large part, because WLANs were restrictive. Some of these restrictions involved bandwidth, proprietary systems, and the inability to manage the WLAN as part of the LAN. The most common methods of securing the WLAN were service set identifiers (SSIDs) and the authentication process.

WLAN Security Issues

- **Rogue access points**
- **Weakness of older forms of security:**
 - **Service set identifier (SSID)**
 - **Authentication controlled by MAC**
 - **Static WEP keys**
 - **Nonmutual authentication—one way only**

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0-6.6

A rogue access point is an access point that has been placed on a WLAN and that might be used to interfere with normal network operations (for denial-of-service [DoS] attacks, for example). If a rogue access point is programmed with the correct WEP key, client data may be captured. The access point may also be configured to provide unauthorized users with information about the network, such as MAC addresses of clients (both wireless and wired), the ability to capture and spoof data packets, and at worst, access to servers and files.

The SSID is a network-naming scheme and configurable parameter that both the client and the access point must share. If the client does not have the proper SSID, it is unable to associate with the access point and would have no access to the network. The SSID feature serves to logically segment the users and access points that form part of a wireless subsystem. Under 802.11 specifications, an access point may advertise, or broadcast, its SSID. During the association process, any 802.11 wireless client with a null string (no value entered in the SSID field) requests that the access point broadcast its SSID. If the access point is so configured, it sends the SSID to the client. The client then uses this SSID to associate with the access point. For these reasons, the SSID should not be considered a security feature of WLAN products.

A client connecting to an access point must go through the process of authenticating and associating. Some WLANs support filtering using a MAC address. Tables are manually constructed on the access point to allow or disallow clients based on their physical hardware address. However, MAC addresses may be relatively easily spoofed, and MAC address filtering is not considered a security feature either.

Basic 802.11 WEP security is designed to guard against the threat to network security from unauthorized 802.11 devices outside the LAN. Any device with a valid WEP key is considered a legitimate and authorized user. If the WEP key was obtained through hardware loss, theft, or a wireless security exploit, the network and wireless users are rendered vulnerable, and keys must be changed. Note that persistent WEP keys may be assigned to a client adapter (keys stored in nonvolatile memory on the card itself) via most WLAN client utilities.

Basic 802.11 WEP security provides only one-way authentication. The client is authenticated with the access point (the WEP key is checked), but not vice versa. The client has no way of knowing whether the access point is a legitimate part of the WLAN or a rogue device (that uses same WEP key).

WEP Attacks

In 2000 and 2001, several documented weaknesses in the 802.11 authentication method were made public, as were weaknesses in the data frame encryption method (WEP).

WEP Attacks

- **Weak, static WEP key**
- **Passive or weak initialization vector (IV) attack details**
- **Active or “bit flipping” and replay attack**
- **Authentication dictionary attacks**

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0-6.7

The main problem identified with WLAN security was that very few WLANs were implementing any form of security at all. Any user with an 802.11 client card could potentially attach to one of these WLANs, and, as a result, attach to the LAN.

A hacker using shared key authentication could capture the challenge text packet that was sent to the client and then capture the encrypted response, thus allowing the hacker to derive the WEP key being used. And, using a WLAN sniffer, a hacker could capture enough packets to crack the security and derive the WEP keys, no matter which method of authentication was being used.

A passive or weak initialization vector (IV) is another reason for attacks. The purpose of the IV is to ensure that the same plaintext data frame will never generate the same WEP-encrypted data frame. The method of changing the IV depends on the vendor implementation. (Cisco Aironet wireless products change the IV on a per-packet basis.)

The IV is transmitted as plaintext, and a user “sniffing” the WLAN could see it. Using the same IV over and over with the same WEP key, a hacker could capture the frames and derive information about the data in the frame and data about the network.

Static WEP keys have proven to be highly vulnerable to this type of attack, and that is why it is recommended that WLANs not use static WEP but instead use the more advanced security features implementing 802.1x.

Cisco Aironet access point firmware includes features to improve RC4 and WEP security by hashing WEP keys, thus protecting against weak IVs.

Care must be taken when configuring WLAN security to protect against this type of attack. Configuring the WEP key timeout on the authentication server provides protection. This practice forces wireless clients to reauthenticate, resulting in the generation of a new WEP key.

The result of the shorter timeout period is that wireless clients do not use the same WEP key long enough for a hacker to capture the number of frames needed to deduce the WEP key.

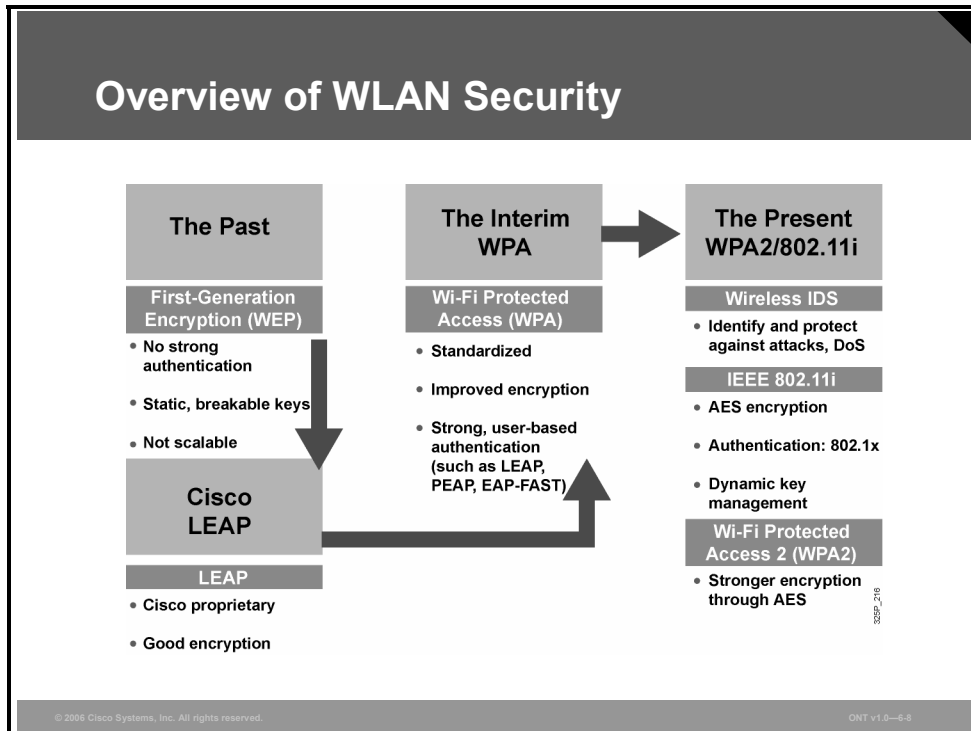
Most password-based authentication algorithms are susceptible to online (active) and offline (passive) dictionary attacks. During a dictionary attack, an attacker tries to guess a password and gain network access by using every “word” in a dictionary of common passwords or possible combinations of passwords. A dictionary attack relies on the fact that a password is often a common word, name, or concatenation of words or names with a minor modification such as a trailing digit or two. Longer passwords with a variety of characters (such as 4yosc10cP!) offer the greatest protection against dictionary attacks.

During an online dictionary attack, an attacker tries to actively gain network access by trying possible combinations of passwords for a specific user. Online dictionary attacks can be prevented using lockout mechanisms available on RADIUS servers to lock the user out after a certain number of invalid login attempts. Online attacks also provide some evidence that a breach or compromise is being attempted, allowing you to take corrective measures.

An offline dictionary attack is carried out in two phases to uncover a password. In the first phase, the attacker captures the challenge and response messages between the user and the network. In the second phase, the attacker looks for a password match by computing a list of possible challenge response messages (using a precomputed dictionary, usually with the aid of a password-cracking program) and comparing these messages against the captured challenge and response messages. The attacker uses known authentication protocol vulnerabilities to reduce the size of the user password dictionary. A strong password policy and requirement that users periodically change their passwords significantly reduce the potential for a successful offline attack using these tools. Unlike online attacks, offline attacks are not easily detected.

Overview of WLAN Security

The figure shows the evolution of wireless LAN security.



In the past, devices supported WEP encryption only. This nonscalable solution used static breakable keys using weak authentication.

Responding to customer requests, Cisco enhanced wireless security by introducing LEAP. LEAP is a Cisco proprietary wireless encryption technique offering dynamic WEP keys and mutual authentication (between a wireless client and a RADIUS server). LEAP allows for clients to reauthenticate frequently.

LEAP made WLANs more secure, but the encryption was not strong enough. New attacks were shown that improvements were required. An interim solution called Wi-Fi Protected Access (WPA) provides standardized improved encryption and stronger user-based authentication (PEAP, EAP, and EAP-FAST).

The interim solution WPA evolved into WPA2, which provides stronger encryption through Advanced Encryption Standard (AES). It includes 802.1x authentication as well as dynamic key management.

WPA2 additionally includes wireless an intrusion detection system (IDS), which identifies and protects against attacks, including DoS attacks. Cisco delivers intrusion prevention system (IPS) capability for Cisco access points to serve as sensors that provide rich RF data to an IPS server.

802.11 WEP

The 802.11 WEP standard uses the RC4 algorithm and has known vulnerabilities.

802.11 WEP

- **IEEE standard for encryption**
- **Uses RC4 algorithm—known vulnerabilities**
- **Keys can be static and shared among many clients**
- **Or keys can be dynamic and unique for each client (as with 802.1x) per session**

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0—4-8

The 802.11 standard defines a type of security: WEP using 40-bit keys. This method uses a wireless client and access point sharing static WEP keys. This key is checked during the authentication process. If the client WEP key does not match that of the access point, the client is not allowed to associate and is unable to connect to the network.

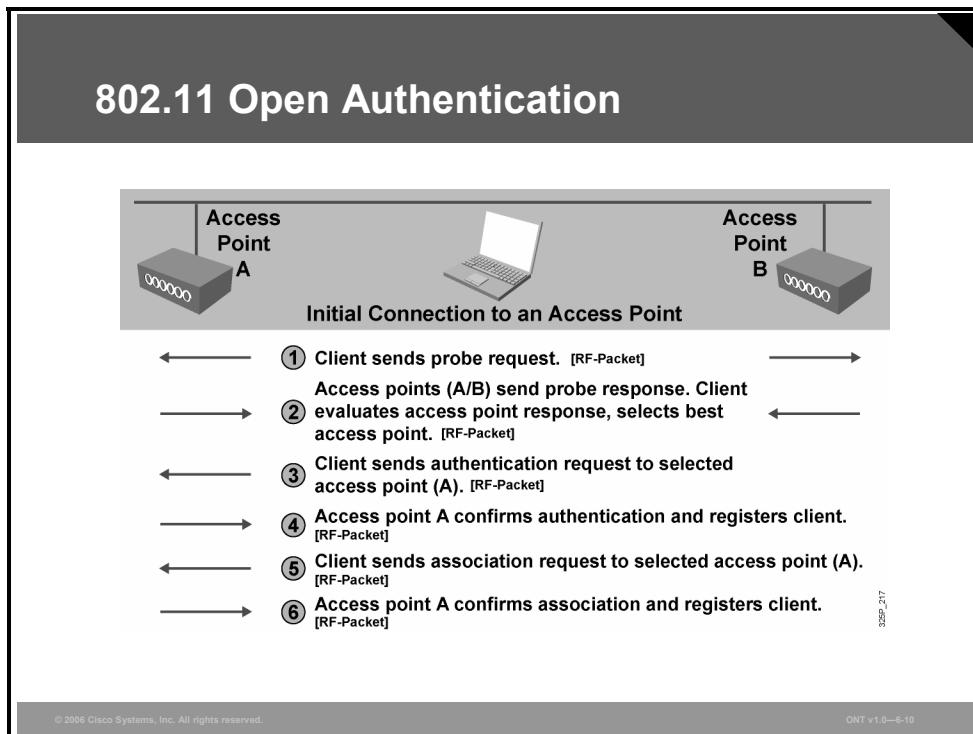
WEP is based upon a familiar encryption type, RC4, a stream cipher. This method allows encryption up to 128 bits. IEEE 802.11 has chosen to use 40-bit keys. Several vendors, such as Proxim and Cisco Systems, support 128-bit WEP encryption with their WLAN solutions for improved security. Cisco Aironet 128-bit devices support both 40-bit and 128-bit encryption. Both the encrypting and decrypting endpoints must share the key. Neither key distribution nor key negotiation is mentioned in the standard.

Note that WEP keys can be referenced as 40- or 64-bit and 104- or 128-bit, depending on whether the IV of 24 bits is included.

Using Cisco Aironet security features means that each wireless client can be granted a new, dynamic WEP key each time it accesses the network. Because these keys are dynamic and session-based, an intruder cannot learn the system WEP keys and then use them to access the WLAN. WEP keys administered in this fashion are referred to as *session keys*. Each user has a unique WEP key. The access point has all the WEP keys for each associated client, allowing it to communicate with each client. Other users who receive information are unable to decrypt the information.

WLAN Authentication

Two types of authentication are defined by 802.11: open and shared key. This section examines both of these types and the process that the client undergoes during the authentication and association process.



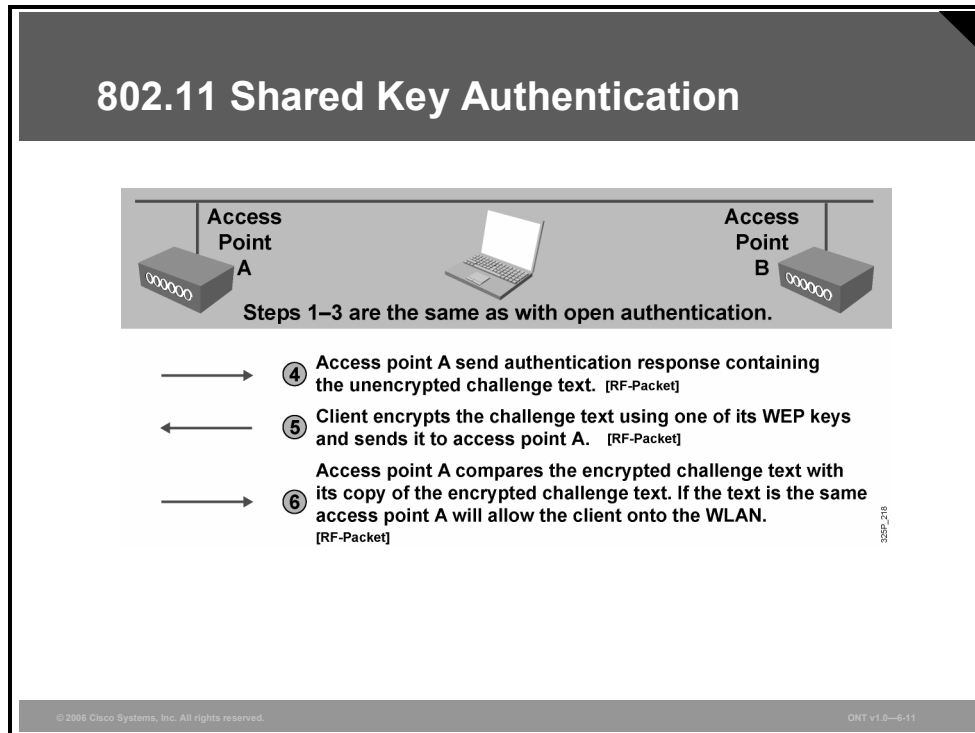
802.11 Open Authentication

The open authentication method allows authorization and associations with or without a WEP key. If the client does not use a WEP key, the client undergoes the normal authentication without any kind of key or password, followed by association with the access point. The user is then granted access to the network. This is normal for public hot spot areas offering Internet access.

If a WEP key is used, the client goes through the normal authentication and association process. When the client is associated and data transmission begins, a client using a WEP key encrypts the data. If the WEP key on the access point does not match, then the access point is unable to decrypt the data, so it is impossible to send the data via the WLAN. Note that the header is not encrypted; only the payload (or data) is encrypted.

802.11 Shared Key Authentication

This example shows the wireless client using shared key authentication to attempt to associate with an access point.



Steps 1 through 3 are the same as those for the open authentication process shown in the previous figure. The next steps are as follows:

- Step 4** Access point A sends an authentication response. The authentication response from the access point to the client is sent containing challenge text. This packet is unencrypted.
- Step 5** The client then uses the text from the authentication response to form another authentication packet, which is encrypted using one of the client WEP keys, and sends this as a response to the access point.
- Step 6** Access point A then compares the encrypted challenge text against the access point copy of the encrypted challenge text. If the encrypted text is the same, then the access point allows the client on the WLAN.

Shared key authentication is considered less secure than open authentication because of the challenge text packet. Because this packet is sent unencrypted and then returned as an encrypted packet, it may be possible to capture both packets and determine the stream cipher.

Cisco Enhanced 802.11 WEP Security

This topic describes how enhanced 802.11 security improves on basic 802.11 security.

Cisco Enhanced 802.11 WEP Security

- **Cisco Prestandard enhancements**
- **Implemented in 2001 and 2002**
- **Authentication:**
 - **802.1x and Extensible Authentication Protocol (EAP) protocols**
 - **User, token, machine credentials**
 - **Dynamic encryption key generation**
- **Encryption:**
 - **Cisco Key Integrity Protocol (CKIP)**
 - **Cisco Message Integrity Check (CMIC)**

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0-4-13

Starting in 2001 and continuing into 2002, Cisco introduced a prestandard form of enhanced 802.11 security that incorporates two elements to improve upon standard or basic 802.11 security. Improved authentication and encryption enhance security to both check user credentials before granting access and increase the security integrity of the user session after association to the network.

Authentication in 802.11 leverages the 802.1x standard to authenticate users and to permit policy assignment to those users as a result of the authentication transaction. Basing the authentication transaction on user credentials rather than machine credentials reduces the risk of security compromise from lost or stolen equipment. Using 802.1x authentication also permits flexible credentials to be used for client authentication. Passwords, one-time tokens, public-key infrastructure (PKI) certificates, or device IDs may be used for authentication. Using 802.1x for wireless client authentication also has the advantage that dynamic encryption keys may be distributed to each user each time that the user authenticates to the network.

Encryption for 802.11 is enhanced with multiple mechanisms to aid in protecting the system from malicious exploits against the WEP key as well as to protect the investment in the system by facilitating encryption improvements in existing hardware.

Cisco Key Integrity Protocol (CKIP) protects the WEP key from exploits that seek to derive the key using packet comparison. Cisco Message Integrity Check (CMIC) is a mechanism for protecting the wireless system from “inductive attacks,” which seek to induce the system to send either key data or a predictable response that can be analyzed (compared to known data) to derive the WEP key.

Cisco clients and compatible clients can use CKIP and CMIC with 802.1x authentication or with static WEP keys when communicating to Cisco autonomous access points.

Enhanced 802.11 Security

Enhanced 802.11 security through either WPA or WPA2 (802.11i) incorporates two elements to improve standard or basic 802.11 security. Authentication and encryption are used with enhanced security to check user credentials before granting access and to increase the security integrity of the user session after association to the network.

Enhanced 802.11 Security

- **Encryption:**
 - **Temporal Key Integrity Protocol and Message Integrity Check**
 - **Wi-Fi Protected Access (WPA)—TKIP encryption**
 - **WPA2—Advanced Encryption Standard (AES)**
- **Authentication:**
 - **802.1x and Extensible Authentication Protocol (EAP) protocols**
 - **User, token, machine credentials**
 - **Dynamic encryption key generation**
 - **IEEE 802.11i**

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0—6-14

Authentication in 802.11 leverages the IEEE 802.1x standard to authenticate users and to permit policy assignment to those users as a result of the authentication transaction. Basing the authentication transaction on user rather than machine credentials reduces the risk of security compromise from lost or stolen equipment. The 802.1x authentication also permits flexible credentials to be used for client authentication. Either passwords, one-time tokens, PKI certificates, or device IDs may be used for authentication. Using 802.1x for wireless client authentication also has the advantage of allowing dynamic encryption keys to be distributed to each user each time that the user authenticates to the network.

Encryption for 802.11 is enhanced with multiple mechanisms to aid in protecting the system from malicious exploits against the WEP key as well as in protecting the investment in the system by facilitating encryption improvements in existing hardware.

Temporal Key Integrity Protocol (TKIP) protects the WEP key from exploits that seek to derive the key using packet comparison. Message integrity check (MIC) is a mechanism for protecting the wireless system from inductive attacks, which seek to induce the system to send either key data or a predictable response that can be analyzed to derive the WEP key.

TKIP and MIC are both elements of the WPA standard, which is intended to secure a system against all known WEP key vulnerabilities. Note that Cisco implemented a prestandard version of TKIP and MIC in late 2001, known as CKIP and CMIC, before WPA was available for customers. Current Cisco equipment supports prior CKIP and CMIC and the Wi-Fi WPA and WPA2 standards as well. Different algorithms are used in CKIP and TKIP, making them incompatible between wireless client and access point. Both the access point and the client must use the same protocol. Although access points can be configured to support both security protocols in a mixed environment, it is always recommended that you use TKIP.

Wi-Fi WPA2, or IEEE 802.11i, is a security standard that was ratified in June 2004. This standard encompasses the prior WPA features plus a number of security improvements. 802.11i standardized on a new form of encryption for 802.11 wireless—AES, called “WPA2.” AES is recognized as a stronger security algorithm than the RC4 stream cipher used with WEP, although AES is undeniably more processor-intensive. Hardware updates will be required to move to AES encryption while maintaining comparable throughput.

Encryption—TKIP and MIC

The first enhancements to the 802.11b WEP standard fall under the umbrella of TKIP.

Encryption—TKIP and MIC

- **Enhancements to RC4-based WEP:**
 - **Key hashing for unique seed values per packet**
 - **MIC from Michael algorithm**
 - **Broadcast key rotation**
- **Key hashing protects against WEP initialization vector vulnerabilities, whereas MIC protects against man-in-the-middle or replay attacks.**

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0—6-15

TKIP contains several key enhancements to RC4-based WEP: key hashing or per-packet keying, MIC, and broadcast key rotation.

WPA is a standard developed in 2003 by the Wi-Fi Alliance, formerly known as the Wireless Ethernet Compatibility Alliance (WECA).

WPA provides a standard for authentication and encryption of WLANs that is intended to solve known security problems up to and including 2003. These problems include the well-publicized AirSnort and man-in-the-middle WLAN attacks.

The WPA mechanisms were designed to be implemented by vendors in current hardware, meaning that users should be able to implement WPA on their current systems with only a firmware or software modification.

WPA has these elements:

- A mechanism for authenticated key management, where the user is first authenticated, and then a master key is derived at server and client. This master key is used to generate the actual keys used in encrypting the user session. The master key is not directly used.
- Key validation mechanisms are in place for both unicast and broadcast keys.
- TKIP is used, which for WPA includes both per-packet keying and MIC.
- The IV is expanded from 24 to 48 bits, which prevents “collisions” or reuse of the same vector, which can be used in exploits to attempt to derive an encryption key. IV collisions are one of the primary mechanisms used by tools such as AirSnort.

Broadcast key rotation is usually used with server-based authentication, and the result is the key, which is changed quickly enough that attackers cannot accept enough packets to get it.

Encryption—AES

AES replaces RC4 as the encryption mechanism in the IEEE 802.11i specification (or WPA2). The protocol is officially called “Advanced Encryption Standard-Cipher Block Chaining Message Authentication Code Protocol” (AES-CCMP).

Encryption—AES

- **Specified in 802.11i**
- **128-bit block cipher—cryptographically more robust than RC4**
- **Part of WPA2**
- **Requires new radio cards on clients and access points because more CPU power is required**

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0—6-16

AES is the next-generation encryption function approved by the U.S. National Institute of Standards and Technology (NIST). NIST solicited the cryptography community for new encryption algorithms. The algorithms had to be fully disclosed and available royalty-free. NIST judged candidates on cryptographic strength as well as practical implementation. The finalist, and the adopted method, is known as the Rijndael algorithm.

AES uses a 128-bit block cipher and requires newer or current radio cards on both access points and clients to eliminate throughput reduction stemming from an increase in computational load for encryption and decryption. If you are planning to implement AES on existing equipment, check Cisco.com documentation to verify whether your current hardware supports AES or whether upgrades are required.

AES-CCMP uses IVs to augment the key stream. The IV increases by one after encrypting each block. This technique provides a unique key stream for each block. AES-CCMP also uses a message authentication check to verify packet integrity using frame length, destination and source addresses, and data in input values.

802.1x Overview

This topic discusses the basic concepts of 802.1x authentication.

802.1x Authentication Overview

- **Extensible and Interoperable supports:**
 - Different EAP authentication methods or types
 - May be used with multiple encryption algorithms
 - Depends on client capability
- **Supported by Cisco since December 2000.**

```
graph LR; Client[Client] --- EAP --- AP[Access Point]; AP --- RADIUS --- RS[RADIUS Server]; RS --- UD[(User Database)];
```

The diagram illustrates the 802.1x authentication process. A Client (laptop) connects to an Access Point (AP) via EAP. The AP then connects to a RADIUS Server, which in turn connects to a User Database. The RADIUS Server and User Database are connected via RADIUS.

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0—6-16

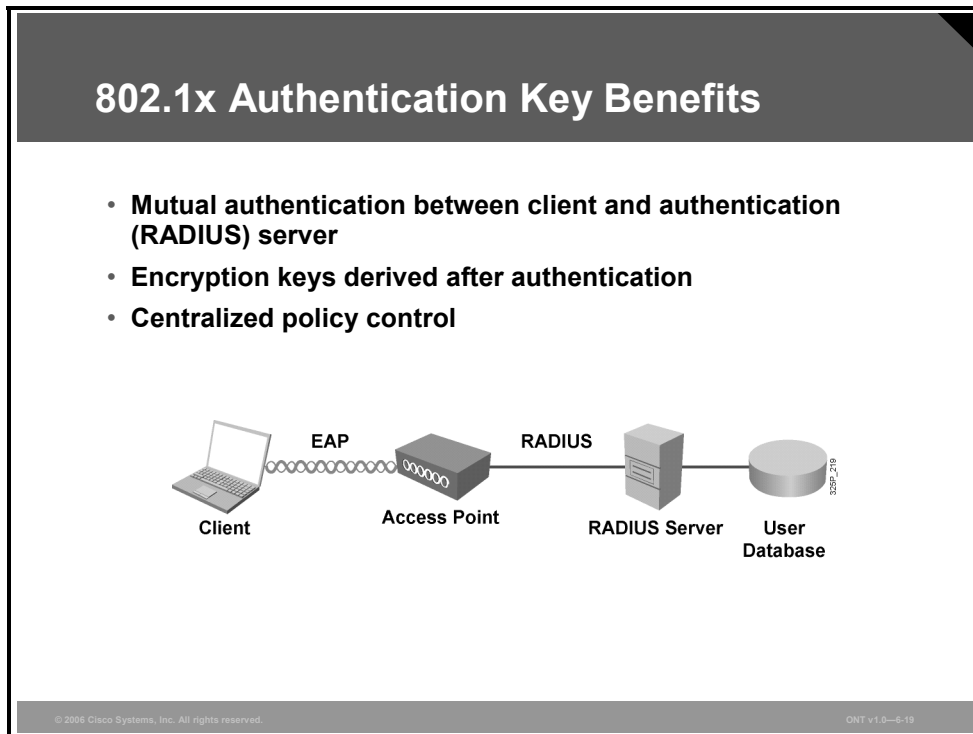
The IEEE developed a supplement to the IEEE 802.1d standard that defines the changes necessary to the operation of a MAC-layer bridge to provide port-based network access control capability. This is the 802.1x standard.

WLAN 802.1x has the following features:

- RADIUS and EAP are used for encapsulation of EAP packets within RADIUS.
- Multiple EAP types are supported.
- Identification is based on the network access identifier (NAI).
- The standard supports roaming access in public spaces.
- RADIUS is supported for centralized AAA.
- It may be used with multiple encryption algorithms:
 - AES
 - WPA TKIP
 - WEP
- WEP keys are dynamic instead of static and do not require user intervention-based management.
- It is compatible with existing roaming technologies, enabling use in hotels and public places.

802.1x Authentication Key Benefits

A major advantage of EAP and the 802.1x standard is that they are designed to leverage existing standards.



With support for EAP, WLANs can now offer these features:

- **Support for RFC 2284, with password authentication:** Users are authenticated based upon username and password that is typically already stored in an active directory on the network. This directory is then connected to a certificate server, such as a RADIUS server or the Cisco Secure Access Control Server (ACS).
- **One-time password (OTP):** OTP encrypts a plaintext password. Thus, plaintext passwords never have to be typed on an insecure connection (Telnet and FTP use no encryption and therefore are not considered secure protocols).

EAP support is designed to allow additional authentication methods to be deployed with no changes to the access point or client network interface card (NIC). Nothing beyond the latest versions of firmware and drivers are required for Cisco Aironet equipment to take advantage of the benefits offered by EAP.

The wireless authentication protocols do require client software to participate in the authentication process. This software is commonly referred to as a “supplicant.”

With all 802.1x authentication types, dynamic encryption key distribution may be supported. Dynamic keying, and the ability to centrally manage the user database, is a major advantage of 802.1x and EAP.

802.1x and EAP Authentication Protocols

The 802.1x specification requires mutual authentication of client and server device.

802.1x and EAP Authentication Protocols

- **Lightweight Extensible Authentication Protocol (LEAP)—EAP Cisco Wireless**
- **EAP-Flexible Authentication via Secure Tunneling (EAP-FAST)**
- **EAP-Transport Layer Security (EAP-TLS)**
- **Protected EAP (PEAP):**
 - **PEAP-GTC**
 - **PEAP-MSCHAPv2**

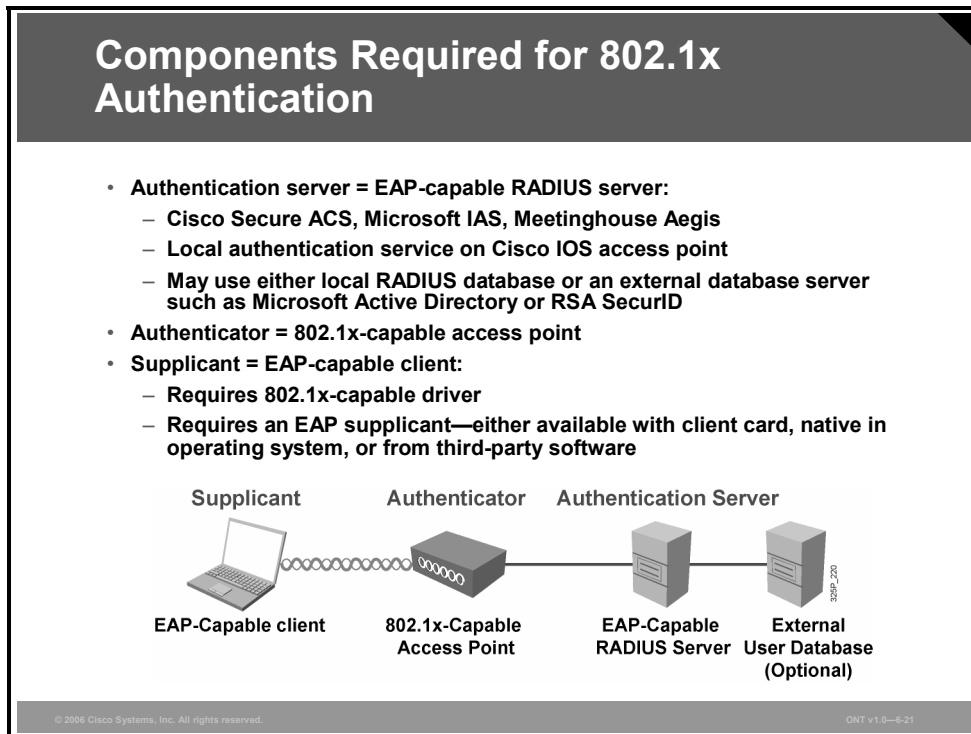
© 2006 Cisco Systems, Inc. All rights reserved.ONT v1.0—6-20

This process may be accomplished through various mechanisms:

- Lightweight Extensible Authentication Protocol (LEAP) is an 802.1x-compliant authentication mechanism developed by Cisco and made available on Cisco NICs and NICs from other vendors.
- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) is a client-server security architecture that encrypts EAP transactions with a TLS tunnel. Although it is similar to Protected Extensible Authentication Protocol (PEAP) in this respect, it differs significantly in that EAP-FAST tunnel establishment is based on strong secrets called the “protected access credential” (PAC) that are unique to users.
- Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) uses certificates to authenticate both the server (network) and client.
- PEAP is a “protected” authentication mechanism that uses a certificate to encrypt the authentication exchange between the client and the EAP server. The authentication exchange may be either Generic Token Card (GTC) or Microsoft Challenge Handshake Authentication Protocol version 2 (MSCHAPv2).

Components Required for 802.1x Authentication

An authentication server is required for 802.1x. 802.1x uses a RADIUS server to authenticate clients to the network.



An authenticator could be a device such as a switch or an access point. This device operates on the enterprise edge, meaning that it is the interface between the enterprise network and the public or semipublic network, where security is most needed.

The client device contains a supplicant. The supplicant sends authentication credentials to the authenticator, which, in turn, sends the information to the authentication server. There, the logon request is compared against a user database to determine whether, and at what level, the user may be granted access to network resources.

LEAP

This topic discusses Lightweight EAP (LEAP, sometimes referred to as EAP Cisco Wireless).

Cisco LEAP

- **Client support:**
 - **Windows 98-XP, Windows CE, Macintosh OS 9.X or 10.X, and Linux Kernel 2.2 or 2.4**
 - **Cisco Compatible Extensions Clients (CCXv1)**
- **RADIUS server:**
 - **Cisco Secure ACS and Cisco Access Registrar**
 - **Meetinghouse Aegis**
 - **Interlink Merit**
- **Microsoft domain or Active Directory (optional) for back-end authentication (must be Microsoft format database)**
- **Device support:**
 - **Cisco autonomous access points and bridges**
 - **Cisco lightweight access points and WLAN controllers**
 - **Cisco Unified Wireless IP Phone 7920 (VoIP) handset**

© 2006 Cisco Systems, Inc. All rights reserved. OWT v1.0—6-23

LEAP provides some unique capabilities that may be difficult to duplicate with other authentication schemes. A few of them are as follows:

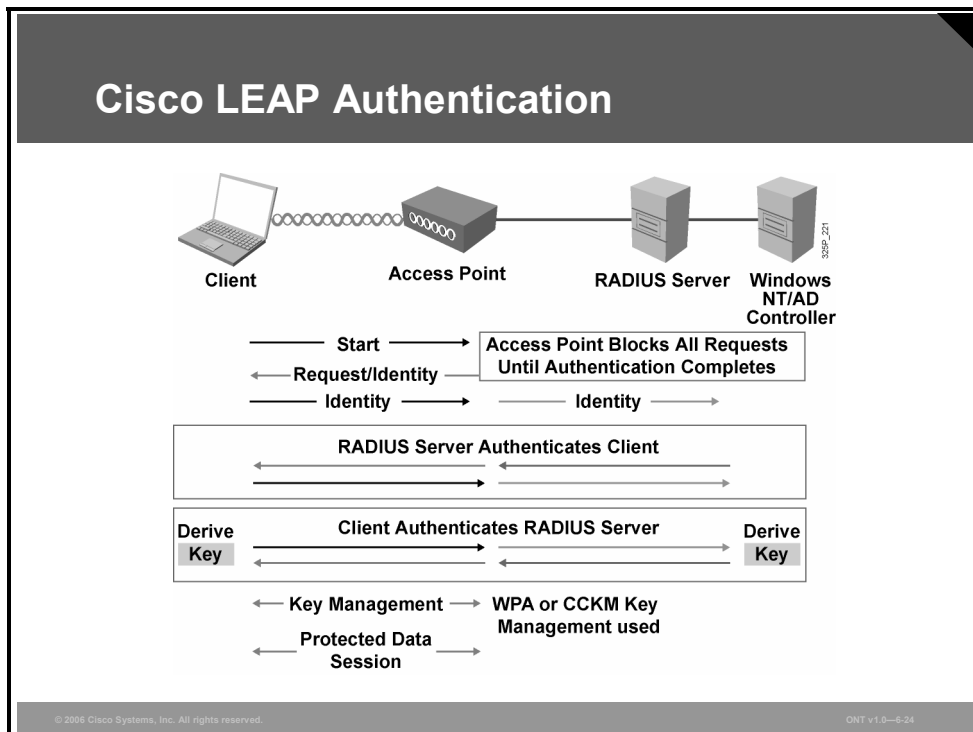
- Fast, secure roaming with Cisco clients or compatible clients
- A broad range of operating systems and devices, including Macintosh, Linux, and DOS
- Single login to a Microsoft Active Directory or Windows NT domain using Microsoft credentials

If a Microsoft database is used, and if it is desirable to use native operating system authentication support, it may be possible to use Microsoft PEAP (PEAP [EAP-MSCHAPv2]) or EAP-TLS. Single login is supported with these solutions also.

Several RADIUS servers support Cisco LEAP, including Cisco Secure Access Control Server (ACS) and Cisco Access Registrar, Meetinghouse Aegis, and Interlink Merit.

Cisco LEAP Authentication

As you can see from this figure, the authentication process requires three components, shown at the top: the client, or supplicant; the access point, or authenticator; and the RADIUS server (in 802.1x terminology, the authentication server).



The authentication can start in one of two ways: by client initiation with the Start message or by access point initiation with the Request/Identity message. In either case, the client responds to the access point with a user name. The access point encapsulates that response in a RADIUS Access-Request message and forwards it to the RADIUS server. The RADIUS server then begins the challenge response process with the client. After the challenges are met with correct authentication, a Success message is sent to the access point, indicating that the client has been authenticated.

The client needs to validate that the access point and RADIUS server are truly what they say they are. This process is the LEAP mutual authentication function. The client sends a challenge message to the access point to forward to the RADIUS server. The RADIUS server must then correctly respond to the challenge for the client to validate the network and then associate. Upon successful authentication, a pairwise master key (PMK) is generated on both the client and the RADIUS server. The RADIUS server forwards the PMK for installation in the access point for that specific client. The access point and the client perform the four-way handshake.

EAP-FAST

This topic discusses EAP-Flexible Authentication via Secure Tunneling (EAP-FAST).

EAP-FAST: Flexible Authentication via Secure Tunneling

Considered in three phases:

- **Protected access credential is generated in phase 0 (Dynamic PAC provisioning)**
 - Unique shared credential used to mutually authenticate client and server
 - Associated with a specific user ID and an authority ID
 - Removes the need for PKI
- **A secure tunnel is established in phase 1**
- **Client is authenticated via the secure tunnel in phase 2**

EAP-FAST consists of an optional phase 0, followed by phases 1 and 2:

- **Phase 0:** Unique to EAP-FAST, phase 0 is a tunnel-secured means of providing an EAP-FAST end-user client with a PAC for the user requesting network access. Phase 0 is optional, and PACs can be manually provided to end-user clients.

A PAC is a digital credential distributed to users for network authentication. A PAC always consists of a secret part and an opaque part. The secret part is secret key material that can be used in future transactions. The opaque part is presented when the client wishes to obtain access to network resources. It aids the server in determining that the client possesses the secret part. Each PAC has a specific user ID and an authority ID associated with it.

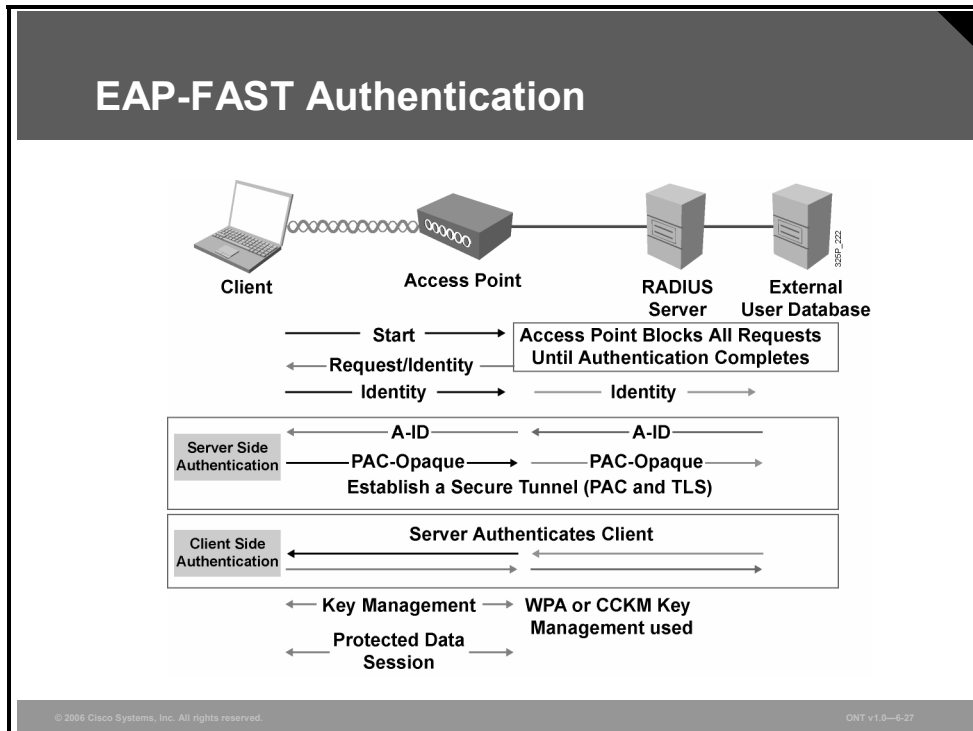
- **Phase 1:** In phase 1, the AAA server and the end user-client use the PAC to authenticate each other and establish a secure tunnel.

Like PEAP, EAP-FAST uses TLS to verify the identity of the AAA server and establish a secure tunnel between the client and the AAA server. The PAC replaces the digital certificate used in PEAP and eliminates the need for a PKI to manage the certificates.

- **Phase 2:** In phase 2, the RADIUS server authenticates the user credentials with EAP-GTC, which is protected by the TLS tunnel created in phase 1.

EAP-FAST Authentication

The wireless client associates with access point using open authentication.



The access point restricts all traffic from the client until the client has authenticated to the RADIUS server.

The client sends an EAP over LAN (EAPOL)-start frame to the access point.

The access point returns a Request/Identity to the client.

The client sends an NAI (e-mail format) address to the access point, which passes it on to the RADIUS server.

The server and the client mutually authenticate each other using phase 1 and phase 2 of the EAP-FAST process.

The RADIUS server sends the session key to the access point in a Success packet. The RADIUS server and client negotiate and derive the session encryption key. This process varies based on whether the client is using WEP or IEEE 802.11i.

The client and the access point use the keys during the session.

At the end of the session, the client sends an EAPOL-logoff packet, and the access point returns to the preauthentication state (filtering all but EAPOL traffic).

EAP-TLS

This topic discusses EAP-Transport Layer Security (EAP-TLS).

EAP-TLS

- **Client support:**
 - **Windows 2000, XP, and Windows CE (natively supported)**
 - **Non-Windows platforms: Third-party supplicants (Meetinghouse)**
 - **User certificate required for each client**
- **Infrastructure requirements:**
 - **EAP-TLS supported RADIUS server**
 - **Cisco Secure ACS, Cisco Access Registrar, Microsoft IAS, Aegis, Interlink**
 - **RADIUS server requires a server certificate**
 - **Certificate authority server (PKI)**
- **Certificate management:**
 - **Both client and RADIUS server certificates to be managed**

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0—6-29

EAP-TLS is one of the original authentication methods specified by the IEEE when 802.1x and EAP were initially proposed and established as a standard. TLS is used in many environments, and is intended to be an alternative, standardized version of the widely deployed Secure Sockets Layer (SSL) encryption mechanism.

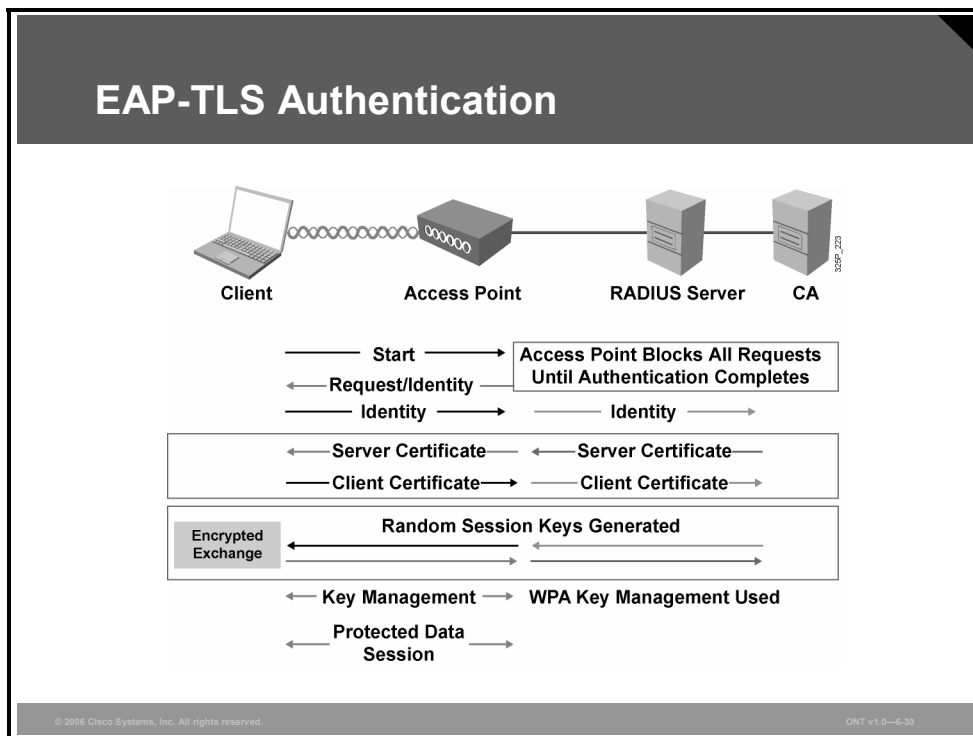
EAP-TLS uses a message authentication code that is derived from a certificate to authenticate a user. Certificates are issued to users and computers by a certificate authority (CA) and are used to validate identity. The maintenance of the CA (which is part of a PKI) may be a barrier to EAP-TLS deployment for some customers. All clients (users) must have their own certificates personally issued and installed on their machines to do TLS authentication. Each AAA server must also have its own certificates.

EAP-TLS has native support on Microsoft Windows 2000, Windows XP, and Windows CE. Third-party supplicants can be used for non-Windows support. Meetinghouse has supplicant software that will support EAP-TLS.

With the Cisco (and Microsoft) implementation of EAP-TLS, it is possible to tie the Microsoft credentials of the user with the certificate of that user in a Microsoft database, which permits single sign-on to a Microsoft domain.

EAP-TLS Authentication

The figure illustrates the 802.1x EAP authentication process with EAP-TLS as the authentication protocol.



The EAP-TLS exchange is as follows:

- The wireless client associates with the access point using open authentication.
- The access point restricts all traffic from the client until the client has authenticated to the RADIUS server.
- The client sends an EAPOL-start frame to the access point.
- The access point returns a Request/Identity to the client.
- The client sends an NAI (e-mail format) address to the access point, which passes it on to the radius server.
- The server and the client mutually authenticate each other using an exchange of digital certificates.
- The RADIUS server sends the session key to the access point in a Success packet. The RADIUS server and client negotiate and derive the session encryption key. This process varies based on whether the client is using WEP or 802.11i.
- The client and the access point use the keys during the session.
- At the end of the session, the client sends an EAPOL-logoff packet, and the access point returns to the preauthentication state (filtering all but EAPOL traffic).

PEAP

This topic discusses Protected EAP (PEAP).

EAP-PEAP

- **Hybrid authentication method:**
 - Server-side authentication with TLS
 - Client-side authentication with EAP authentication types
 - EAP-GTC
 - EAP-MSCHAPv2
- Clients do not require certificates.
- RADIUS server requires a server certificate:
 - RADIUS server has self-issuing certificate capability.
 - Purchase a server certificate per server from PKI entity.
 - Set up a simple PKI server to issue server certificates.
- Allows for one-way authentication types to be used:
 - One-time passwords
 - Proxy to LDAP, Unix, Microsoft Windows NT and Active Directory, Kerberos

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0—6-32

PEAP is an authentication protocol that was jointly proposed and developed by Cisco, Microsoft, and RSA Security. The purpose of PEAP is to *protect* the authentication transaction with a TLS-secured connection, much as you might secure a connection to an e-commerce website when performing an online transaction.

Note that there are two implementations of PEAP:

- PEAP-Generic Token Card (GTC)
- PEAP-Microsoft Challenge Handshake Authentication Protocol version 2 (MSCHAPv2)

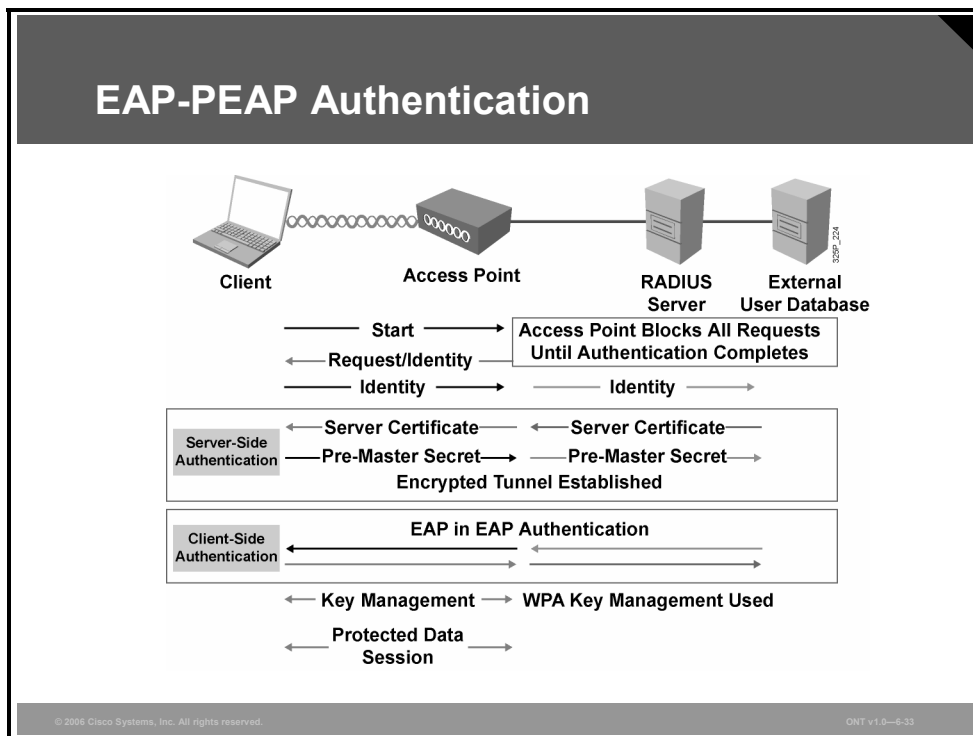
The PEAP-GTC authentication mechanism allows *generic* authentication to a number of databases—Novell Directory Service (NDS), Lightweight Directory Access Protocol (LDAP), OTP, and so on. The PEAP-MSCHAPv2 authentication mechanism allows authentication to databases supporting the MSCHAPv2 format, including Microsoft NT and Microsoft Active Directory.

As with other 802.1x and EAP types, dynamic encryption may be used with PEAP.

A CA certificate must be used at each client to authenticate the server to each client before the client submits its authentication credentials.

EAP-PEAP Authentication

The figure illustrates the 802.1x EAP authentication process with EAP-PEAP as the authentication protocol.



The EAP-PEAP exchange is as follows:

- The wireless client associates with the access point using open authentication.
- The access point restricts all traffic from the client until the client has authenticated to the RADIUS server.
- The initial handshake between the client and the access point is a TLS handshake, as seen earlier.
- The client authenticates the server using a CA to verify the digital certificate of the server. Then the client and the server establish an encrypted tunnel. The client submits its credentials inside the tunnel using either MSCHAPv2 or GTC.
- The RADIUS server sends the session key to the access point in a Success packet. The RADIUS server and client negotiate and derive the session encryption key. This process varies based on whether the client is using WEP or 802.11i.
- The client and the access point use the keys during the session.

At the end of the session, the client sends an EAPOL-logoff packet, and the access point returns to the preauthentication state (filtering all but EAPOL traffic).

Wi-Fi Protected Access

This topic describes WPA and how the authentication process works.

Wi-Fi Protected Access

- **WPA introduced in late 2003**
- **Prestandard implementation of IEEE 802.11i WLAN security**
- **Addresses currently known security problems with WEP**
- **Allows software upgrade on deployed 802.11 equipment to improve security**
- **Components of WPA:**
 - **Authenticated key management using 802.1x: EAP authentication and preshared key authentication**
 - **Unicast and broadcast key management**
 - **Standardized Temporal Key Integrity Protocol (TKIP) per-packet keying and message integrity check (MIC) protocol**
 - **Initialization vector space expansion: 48-bit initialization vectors**
 - **Migration mode—coexistence of WPA and non-WPA devices (optional implementation that is not required for WPA certification)**

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0—6-35

WPA Characteristics

WPA is the Wi-Fi Alliance standards-based mechanism to create secure and interoperable WLAN networks. WPA provides a mechanism to authenticate keys for use in 802.11 environments as well as providing enhancements to WEP encryption to increase the robustness of the security protocol.

WPA was an interim solution proposed by the wireless industry consortium to create a WLAN standard in advance of the IEEE standard for security, IEEE 802.11i, which was ratified in June 2004.

WPA addressed vulnerabilities of standard 802.11 WEP security and permitted a path for migration of users to this new security mechanism through a software upgrade; that is, with no hardware changes required.

Components of WPA

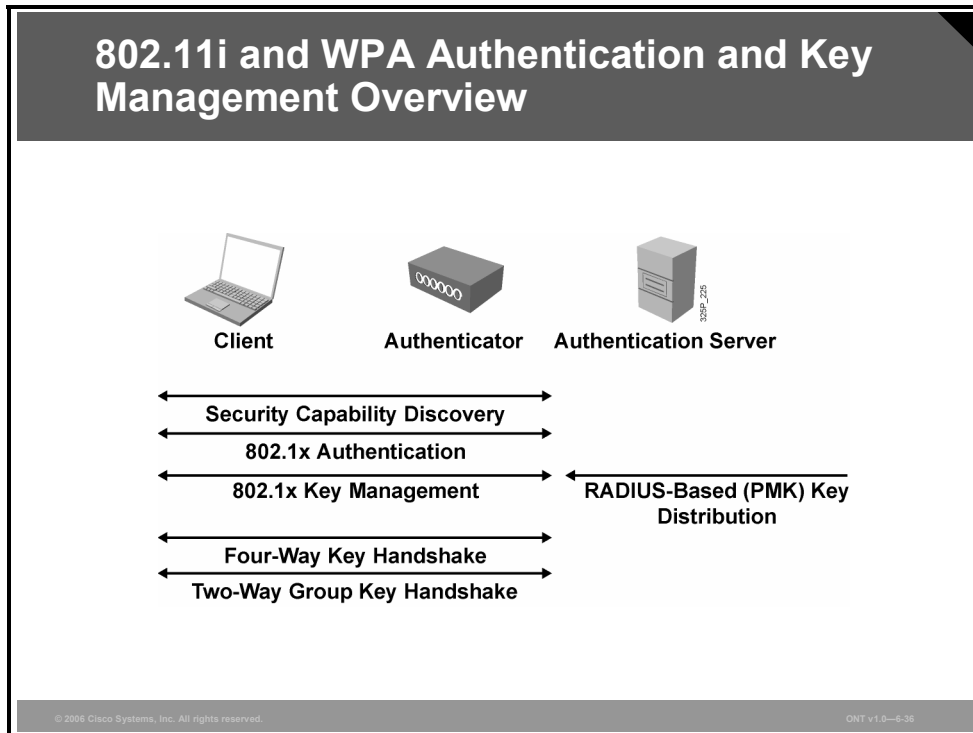
WPA is a standard describing a combination of security capabilities. These capabilities were available before WPA became an industry standard (note that WPA was not an IEEE standard as of late 2003), but WPA pulls the capabilities into one definition.

The following are the most important aspects of WPA:

- **Authenticated key management:** Either using 802.1x authentication or a preshared key, the user is authenticated prior to authentication of the keys used.
- **Unicast and broadcast key management:** The keys derived after user authentication are authenticated through a handshake process between the access point and client.
- **TKIP (per-packet keying) and MIC**
- **IV space expansion:** The IV space is expanded from 24 bits, as in 802.11 WEP, to 48 bits in WPA.

802.11i or WPA Authentication and Key Management Overview

Initial authentication using WPA is essentially identical to standard 802.11 authentication and association.



The primary difference in WPA is in the initial association request (probe request) that the client and access point send. The client and access point must agree to a security capability during association.

After initial association and exchange of security capabilities, the client and authentication servers proceed with standard 802.1x authentication.

After successful authentication, the server derives and distributes a master key to the access point. The same master key is derived at the client.

With these master keys, the access point and the client perform a four-way handshake to validate the access point, and the client validates the group or broadcast key using a two-way handshake.

Unicast Keys: Four-Way Handshake

Before the WPA handshake can occur, the pairwise master key (PMK, a 256-bit key) is generated as a result of the 802.1x authentication process between the client and the authentication server, or the process uses the 64-hexadecimal character preshared key (or a key stream derived from the preshared key phrase).

- Step 1** The access point sends a nonce or random number to the client.
- Step 2** The client responds to the access point with its own nonce or random number, along with the WPA information element, pairwise transient key (PTK), and MIC key information.
- Step 3** The access point sends the nonce again, along with the information element, PTK, MIC key information, and install message. The re-sending of this information validates that the client and access point share common authentication information.

Step 4 The client sends MIC key information and the PTK to the access point for acknowledgment.

Note A pseudorandom function (PRF) is used to compute the PTK as a function of client and access point random numbers and the MAC addresses of the access point and client.

Group Key Handshake

The group master key (GMK) is either generated using a random number function or is initialized by the first PTK that the access point uses.

When the access point has the GMK, a group random number is generated. This random number is used to derive a group transient key (GTK). Inputs are a PRF that uses the random number and the access point address.

The GTK is used to provide a group key as well as MIC keys, which may be used to verify the integrity of the key data.

WPA Key Management Phases

As part of WPA compliance, an access point must be capable of advertising security capabilities in its 802.11 beacons. This process describes the unicast, multicast, and authentication types supported. From the capabilities advertised by the access point, the client selects the “best” supported security type for its authentication.

After the client has determined its authentication type, it proceeds with open authentication, using either 802.1x to a RADIUS server or using a preshared key between the access point and the client. This process has the advantage of mutual authentication of client and server, as well as providing a centralized resource for client admission control.

Upon completion of standard 802.1x or EAP messaging between the client and server, a master key is independently generated at the server and client. This master key is then used to derive a PTK that is used in the authentication of the encryption key components used between the access point and the client.

WPA Issues

WPA is an updated security option that was intended to address attacks on static WEP keys, but the WPA solution also has some issues.

WPA Issues

- **WPA uses TKIP, which uses the same base encryption algorithm—RC4—as WEP.**
- **WPA cannot avoid the design flaws of WEP entirely.**
- **WPA, in the end, a compromise solution.**
- **Software upgrade is required for clients and access points, which gives no guarantee that all vendors will support the solution.**
- **Operating system support or a supplicant client is required.**
- **WPA is susceptible to a new type of DoS attack.**
- **WPA is susceptible to a recently discovered weakness when preshared keys are used.**

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0—6-57

The Temporal Key Integrity Protocol (TKIP) used with WPA is an enhancement to the basic security mechanism defined by 802.11 WEP (RC4 encryption). Note that TKIP is a “wrapper” around the WEP and RC4 encryption mechanism. WPA relies on RC4 instead of 3DES, AES, or another encryption algorithm.

WPA requires access point firmware support—it is not guaranteed that all wireless access point manufacturers will release firmware upgrades for older models so that they can support WPA.

WPA requires software driver support for wireless cards—it is not guaranteed that all wireless card manufacturers will release software driver upgrades for older models so that they can support WPA.

WPA requires operating system support or a supplicant client—the WPA security mechanisms rely on 802.1x or EAP support directly in the operating system or via a supplicant client such as the Funk Software Odyssey Client.

Moving to WPA is sometimes an all-or-nothing proposition. Some vendors may not allow mixing WEP and WPA devices; the Wi-Fi Alliance does not recommend mixing WEP and WPA. Of course, mixing may not actually be possible, given that some vendors have no intention of releasing WPA software upgrade patches for older wireless hardware—they would simply prefer to sell newer wireless gear with WPA support. This means that some organizations that want to deploy WPA may have to replace a significant amount of their wireless infrastructure.

EAP deployment can be a significant undertaking, given that there are more than a half-dozen variants (EAP-Message Digest 5 [EAP-MD5], EAP-TLS, EAP-Tunneled TLS [EAP-TTLS], PEAP, LEAP, EAP-Subscriber Identity Module [EAP-SIM], and so on), each with its own shortcomings and installation issues. It also requires the use of an external RADIUS server to authenticate the incoming wireless user connection attempts. Because each manufacturer may offer different EAP methods in its firmware and driver software, customers may not be able to use existing wireless equipment and will be forced to purchase new equipment that supports the chosen EAP method.

To maintain backward hardware compatibility, MIC was designed to incur very little computational overhead. As a result, it offers only 20 bits of effective security.

WPA is susceptible to a new type of DoS attack based on countermeasure techniques employed by MIC. If an access point running WPA receives two packets in quick succession with bad MICs, it shuts down the entire basic service set (BSS) for one minute.

WPA is susceptible to a recently discovered weakness when preshared keys are used instead of 802.11i or EAP; the use of a small, noncomplex passphrase can allow an attacker to perform a dictionary attack on captured traffic and recover the passphrase.

IEEE 802.11i—WPA2

- **802.11i:**
 - **Ratified in June 2004**
 - **Standardizes:**
 - **802.1x for authentication**
 - **AES encryption—Facilitates U.S. government FIPS 140-2 compliance**
 - **Key management**
- **WPA2:**
 - **Supplement to WPA “version 1”—Wi-Fi Alliance interoperable implementation of 802.11i**
 - **Provides for AES encryption to be used**
 - **Proactive Key Caching**
 - **Third-party testing and certification for WLAN device compatibility**

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0—6-38

The 802.11i standard, which was ratified in June 2004, added the following:

- 802.1x for authentication
- AES for encryption
- Key management

The Wi-Fi Alliance WPA2 standard provides third-party testing and certification that WLAN devices meet the standard.

WPA2 Overview

WPA2 is a new security standard developed by the IEEE 802.11i task group. The Robust Security Network (RSN) specification is the IEEE equivalent of WPA2. WPA2 generally uses AES block ciphers with Cipher Block Chaining Message Authentication Code Protocol (CCMP) for encryption and supports TKIP:

- Generally uses 802.1x authentication methods—supports preshared keys
- Comparable to WPA—the same authentication architecture, key distribution, and key renewal
- Supports Proactive Key Caching (PKC) and preauthentication
- IDS added to identify and protect against attacks

Wireless IDSs

Traditional wired IDSs focus on Layer 3 and higher, but the nature of the RF medium and wireless standards mandate IDS at the physical and data link layers.

Wireless Intrusion Detection Systems

- **Address RF-related vulnerabilities:**
 - Detect, locate, mitigate rogue devices
 - Detect and manage RF interference
 - Detect reconnaissance if possible
- **Address standards-based vulnerabilities:**
 - Detect management frame and hijacking style attacks
 - Enforce security configuration policies
- **Complementary functionality:**
 - Forensic analysis
 - Compliance reporting

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0-6.39

The RF medium has several vulnerabilities, such as the unlicensed spectrum, which is subject to interference and is not contained by physical security boundaries. Standard vulnerabilities include unauthenticated management frames, session hijacking, and replay-type attacks.

IDS protection includes rogue detection and location mapping, IDS attack signatures, client exclusion and containment, and high-resolution location tracking.

Cisco offers wireless intrusion prevention system (IPS) options based on the architecture selection:

- WLAN controller-based
- Autonomous access point
- Autonomous access point with partner integration

WPA and WPA2 Modes

WPA has two modes: Enterprise and Personal. Both modes provide encryption support and user authentication.

	WPA	WPA2
Enterprise mode (business, education, government)	Authentication: IEEE 802.1x/EAP Encryption: TKIP/MIC	Authentication: IEEE 802.1x/EAP Encryption: AES-CCMP
Personal mode (SOHO, home/personal)	Authentication: PSK Encryption: TKIP/MIC	Authentication: PSK Encryption: AES-CCMP

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0-4-40

WPA provides authentication support using IEEE 802.1x and preshared keys (IEEE 802.1x is recommended for enterprise deployments). WPA also provides encryption support using TKIP. TKIP includes MIC and per-packet keying via IV hashing and broadcast key rotation.

In comparison to WPA, WPA2 authentication is identical except that the encryption used is AES-CCMP.

Enterprise Mode

“Enterprise mode” is a term given to products that are tested to be interoperable in both the preshared key and IEEE 802.1x or EAP modes of operation for authentication. When IEEE 802.1x is used, an AAA server (the RADIUS protocol for authentication and key management and centralized management of user credentials) is required. Enterprise mode is targeted to enterprise environments.

Personal Mode

“Personal mode” is a term given to products tested to be interoperable in the preshared key-only mode of operation for authentication. It requires manual configuration of a preshared key on the access point and clients. A preshared key authenticates users via a password, or identifying code, on both the client station and the access point. No authentication server is needed. Personal mode is targeted to small office-home office (SOHO) environments.

WPA2 Issues

WPA2 solved the remaining security issues of WPA. Because AES is used for encryption, more computing power is required, and the hardware must be changed to support WPA2.

WPA2 Issues

- **Client (supplicant) must have a WPA2 driver that supports EAP.**
- **RADIUS server must understand EAP.**
- **PEAP carries EAP types within a channel secured by TLS and so requires a server certificate.**
- **WPA2 is more compute-intensive with optional AES encryption.**
- **WPA2 may require new WLAN hardware to support AES encryption.**

© 2006 Cisco Systems, Inc. All rights reserved. OMT v1.0--6-61

The client (supplicant) must have a WPA2 driver that supports EAP. This standard is not prevalent, and it can be a limitation. The RADIUS server must also understand EAP. Although many RADIUS servers support EAP, not all of them do.

PEAP carries EAP types within a channel secured by TLS. When TLS is used, a server certificate is used. This feature allows dynamic keys.

Compared to WPA, WPA2 is CPU-intensive. More computing power is required for AES encryption support, and this requires hardware upgrades rather than a firmware upgrade only. Some older access points will never support WPA2 because hardware upgrades are not available. New equipment is WPA-ready, and only a software upgrade is required.

Summary

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

Summary

- **Authentication and encryption are the two primary facilities for securing the WLAN.**
- **Encryption is the method of ensuring that data remains uncorrupted throughout the sending and receiving process.**
- **Encryption using static WEP keys is very vulnerable.**
- **EAP and the 802.1x standards are designed to leverage existing standards.**
- **The LEAP authentication process is mutual because the client needs to authenticate the server and the server needs to authenticate the client.**

© 2006 Cisco Systems, Inc. All rights reserved.

ONT v1.0—6-42

Summary (Cont.)

- **With EAP-FAST, the wireless client associates with access point using open authentication.**
- **EAP-TLS uses authentication derived from digital certificates for user and server authentication.**
- **PEAP uses user authentication with OTP or static password.**
- **WPA has two different modes: Enterprise and Personal. Both modes provide encryption support and user authentication.**
- **WPA2 is similar to WPA but supports AES encryption.**

© 2006 Cisco Systems, Inc. All rights reserved.

ONT v1.0—6-43

References

For additional information, refer to this resource:

- Cisco Systems, Inc. “Cisco Aironet Response to Press—Flaws in 802.11 Security” at http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a0080088832.html.

Configuring Encryption and Authentication on Lightweight Access Points

Overview

This lesson describes configuring an advanced feature set wireless LAN (WLAN) for encryption and authentication on lightweight access points. The general steps required for configuration are shown. The lesson describes configuring authentication using open authentication, static Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) preshared keys, web authentication, and WPA and WPA version 2 (WPA2) with 802.1x.

Objectives

Upon completing this lesson, you will be able to describe configuring an advanced feature set WLAN for encryption and authentication on lightweight access points. This ability includes being able to meet these objectives:

- Describe configuring open authentication on the controller
- Describe configuring preshared key authentication on the controller
- Describe configuring web authentication on the controller
- Describe configuring 802.1x on the controller

Open Authentication

This topic describes configuring open authentication on the Cisco Wireless LAN Controller.

WLANs > Edit

WLAN ID: 1
WLAN SSID: Open2

General Policies

Radio Policy: All
Admin Status: Enabled
Session Timeout (secs): 0
Quality of Service (QoS): Silver (best effort)
WME Policy: Disabled
Broadcast SSID: Enabled
Allow AAA Override: Enabled
External Policy Validation: Enabled
Client Exclusion: Enabled ** 60
DHCP Server: Override
DHCP Addr. Assignment: Required
Interface Name: management

Security Policies

IPv6 Enable:
Layer 2 Security: None
MAC Filtering:
Layer 3 Security: None
Web Authentication *:

*Web Authentication cannot be used in combination with IPsec and L2TP.
**When client exclusion is enabled, a timeout value of zero means infinity(will require administrative override to reset excluded clients)

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0-6-3

Open authentication is used when no authentication or encryption is desired. This is normal for a “guest” implementation for visitors or hot-spot applications.

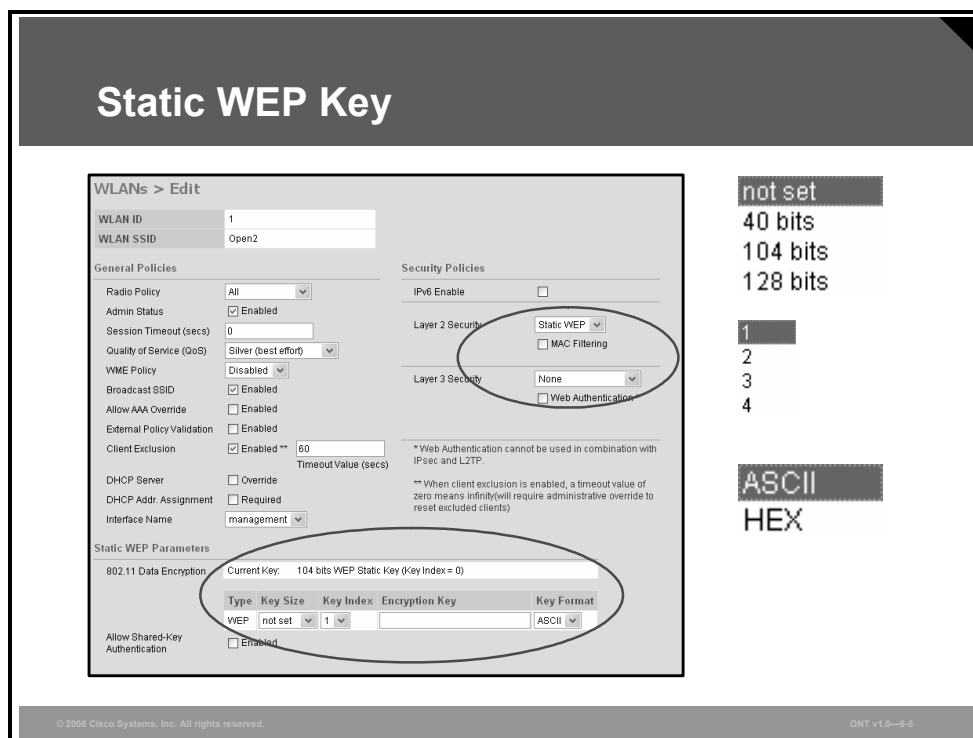
For existing wireless LANs (WLANs), choose **WLANs** and then **Edit** to navigate to this page. For new WLANs, create a new WLAN by choosing **WLANs > New**, then click **Apply** to navigate to this page. This page allows you to edit the configurable parameters for a WLAN.

The default authentication method for a new WLAN is 802.1x, which will be displayed. The reason for setting this parameter as the default is to protect against accidental open authentication. The next step is to change the value in the Layer 2 Security drop-down list under the Security Policies heading from 802.1x to **None**. Ensure that both the Layer 2 and Layer 3 Security fields are set to **None**.

Note Depending on the security policy options selected, the bottom of the page will change to reflect the appropriate security parameters.

Static WEP Key Authentication

This topic describes configuring preshared key authentication on the controller.



For existing WLANs, choose **WLANs** and then **Edit** to navigate to this page. For new WLANs, create a new WLAN by choosing **WLANs > New**, then click **Apply** to navigate to this page. This page allows you to edit the configurable parameters for a WLAN.

Choose **Static WEP** from the Layer 2 Security drop-down list under the Security Policies heading. The bottom of the screen will update to show the static Wired Equivalency Protocol (WEP) options with the appropriate parameters listed.

The static WEP encryption parameters are as follows:

- Key sizes are 40/64, 104/128, and 128/152 bits.
- Key index is from 1 to 4.
- Enter the encryption key.
- Choose ASCII or HEX as the encryption key format.

Note One unique WEP key index can be applied to each WLAN. Because there are only four WEP key indexes, only four WLANs can be configured for static WEP Layer 2 encryption.

WPA Preshared Key

For existing WLANs, choose **WLANs** and then **Edit** to navigate to this page.

WPA Preshared Key

WLANs > Edit

WLAN ID: 2
WLAN SSID: WPAPSK2

General Policies

Radio Policy: All
Admin Status: Enabled
Session Timeout (secs): 0
Quality of Service (QoS): Silver (best effort)
WME Policy: Disabled
Broadcast SSID: Enabled
Allow AAA Override: Enabled
External Policy Validation: Enabled
Client Exclusion: Enabled ** 60
Timeout Value (secs)

Security Policies

IPv6 Enable:

Layer 2 Security: WPA
 MAC Filtering

Layer 3 Security: None
 Web Authentication *

* Web Authentication cannot be used in combination with IPsec and LZTP.
** When client exclusion is enabled, a timeout value of zero means infinity (will require administrative override to reset excluded clients)

WPA Parameters

802.11 Data Encryption: TKIP-MIC

Pre-Shared Key: Enabled
 Set Passphrase

© 2004 Cisco Systems, Inc. All rights reserved. ONT v1.0—6-6

For new WLANs, create a new WLAN by choosing **WLANs > New**, and click **Apply** to navigate to this page. This page allows you to edit the configurable parameters for a WLAN:

- Choose **WPA** from the Layer 2 Security drop-down list under the Security Policies heading. The bottom of the page will change to reflect appropriate parameters for Wi-Fi Protected Access (WPA).
- Check the **Enabled** check box at the bottom of page for a preshared key. The bottom of the page will again change to reflect this option, and the Set Passphrase field will appear.
- Enter the WPA preshared key passphrase in the field.

Web Authentication

This topic describes configuring web authentication on the controller.

Web Authentication

- **Users authenticate via a web browser interface.**
- **Clients using HTTP are automatically directed to a login page:**
 - **Customizable for logos and text**
 - **Maximum simultaneous authentication requests—21**
 - **Maximum local web authentication users—2500**
- **Generally used for guest access:**
 - **Data is not secure between the access point and the client.**

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0—6-8

Web authentication allows users to authenticate through a web browser interface.

Clients who attempt to access the WLAN using HTTP are automatically redirected to a login page. The login page is customizable for both logos and text.

The maximum simultaneous authentication requests using web authentication is 21.

The maximum number of local web authentication users is 2500.

Web authentication is generally used for “guest” access, and you should bear in mind that client data is not secured between client and access point. Because there is no encryption, per-packet authentication, or message integrity check (MIC), users should use some other security mechanism after authentication. This authentication method does not protect against interception, hijacking, or packet modification.

Note Web authentication is a feature of Cisco 4400 Series Wireless LAN Controllers and Cisco Catalyst 6500 Series Wireless Services Module (WiSM). It is not a feature of Cisco 2000 Series Wireless LAN Controllers or Cisco Integrated Services Routers Wireless LAN Controller Modules.

Web Authentication (Cont.)

Security Policies

IPv6 Enable

Layer 2 Security MAC Filtering

Layer 3 Security Web Policy *
 Authentication Passthrough

Preauthentication ACL Email Input

* Web Policy cannot be used in combination with IPsec and L2TP.

For existing WLANs, choose **WLANs** and then choose **Edit** to navigate to this page. For new WLANs, create a new WLAN by choosing **WLANs > New**, and click **Apply** to navigate to this page. This page allows you to edit the configurable parameters for a WLAN.

In the Layer 3 Security area, check the Web Policy check box to enable the web policy. The bottom of the page will change to reflect this choice and offer the following parameters for web authentication:

- **Authentication:** If you choose this option, you will be prompted for username and password while the client is connecting to the wireless network. The authentication credentials will be verified against the controller internal user database. If no username is matched, then an external RADIUS server will be used if it is configured.
- **Passthrough:** If you choose this option, you can access the network directly without entering a username and password. This option might be used to simply present a legal notice before allowing access.
 - **Email Input:** This option is available for the Passthrough option only. If you choose this option, you will be prompted for an e-mail address when connecting to the network.
- **Preauthentication ACL:** Choose the access control list (ACL) to be used for traffic between the client and the controller.

Note The controller will have to reboot to load and enable the web authentication feature.

Web Authentication (Cont.)

Web Login Page Preview...

Use External Web Authentication

This page allows you to customize the content and appearance of the Login page. The Login page is presented to web users the first time they access the WLAN if 'Web Authentication' is turned on (under WLAN Security Policies).

Cisco Logo Show Hide

Redirect URL after login

Headline

Message

Web Login Page Preview...

Use External Web Authentication

URL

External Web Servers

Web Server IP Address

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0-8-10

Choose **Management > Web Login Page** to navigate to this page. You can customize the content and appearance of the web login page that appears the first time a user accesses the client. The Web Login page parameters are as follows:

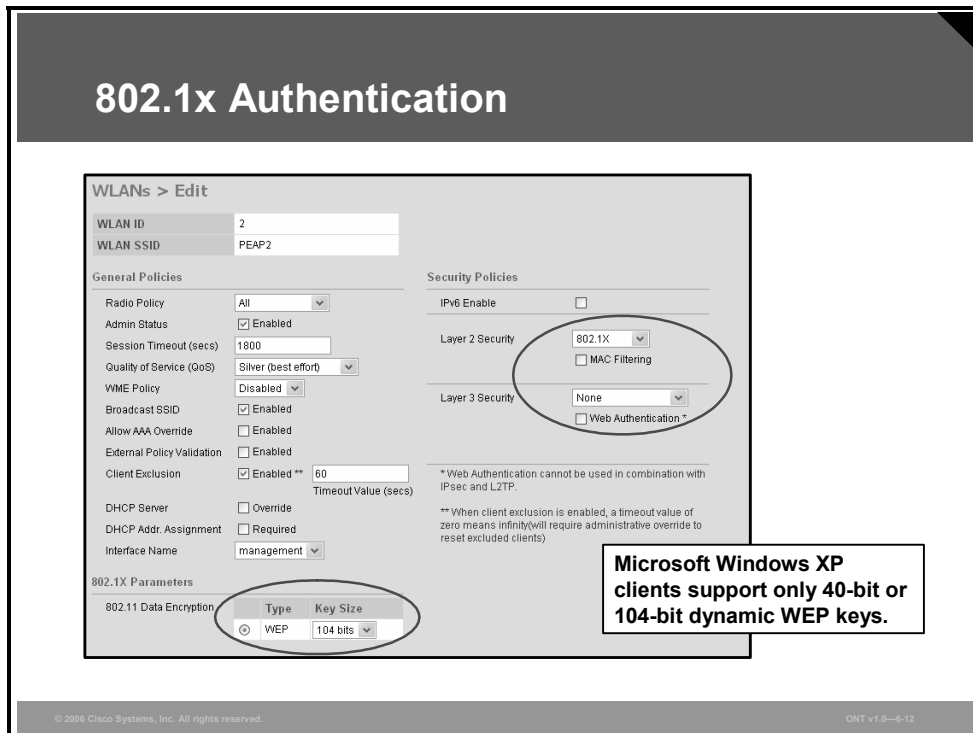
- **Use External Web Authentication:** Enable this option and enter the URL if you want to use a customized login page configured on your web server for web authentication instead of the default web authentication page provided by the Cisco 4000 Series Wireless LAN Controllers. The maximum length is 254 characters.

Note The following parameters will be displayed only if the Use External Web Authentication option is disabled.

- **Redirect URL after Login:** Enter the URL to which you want the user to be redirected after login. For example, you may enter your company URL here, and users will be directed to that URL after login. The maximum length is 254 characters. By default, the user is redirected to the URL that was entered in the user's browser before the login page appeared.
- **Headline:** Specify the login page headline; for example, "Welcome to the Cisco Wireless Network." The maximum length is 127 characters.
- **Message:** Specify the login page message; for example, "Please enter your username and password." or "This page will not be available from 1:00 to 2:00 p.m. today because of maintenance." The maximum length is 2047 characters.

802.1x Authentication

This topic describes configuring 802.1x authentication on the controller.



For existing WLANs, choose **WLANs** and then **Edit** to navigate to this page. For new WLANs, create a new WLAN by choosing **WLANs > New**, then click **Apply** to navigate to this page. This page allows you to edit the configurable parameters for a WLAN.

Choose **802.1x** from the Layer 2 Security drop-down list under the Security Policies heading. If this is a new WLAN ID, 802.1x will be the default authentication policy. The bottom of the screen will update to show the 802.1x options with the appropriate parameters.

802.1x uses dynamic 802.11 WEP keys. The options are these:

- 40/64 bits
- 104/128 bits
- 128/152 bits

Note 802.11 standards support 40/64- and 104/128-bit keys. 128/152-bit keys are supported by 802.11i, WPA, and WPA2.

WPA with 802.1x

For existing WLANs, choose **WLANs** and then **Edit** to navigate to this page.

WPA with 802.1x

WLANs > Edit

WLAN ID: 2
WLAN SSID: WFAPEAP2

General Policies

Radio Policy: All
Admin Status: Enabled
Session Timeout (secs): 0
Quality of Service (QoS): Silver (best effort)
WME Policy: Disabled
Broadcast SSID: Enabled
Allow AAA Override: Enabled
External Policy Validation: Enabled
Client Exclusion: Enabled ** 60
Timeout Value (secs)

Security Policies

IPv6 Enable:

Layer 2 Security: WPA
 MAC Filtering

Layer 3 Security: None
 Web Authentication *

* Web Authentication cannot be used in combination with IPsec and L2TP.
** When client exclusion is enabled, a timeout value of zero means infinity (will require administrative override to reset excluded clients)

WPA Parameters

802.11 Data Encryption: TKIP-MIC
Pre-Shared Key: Enabled

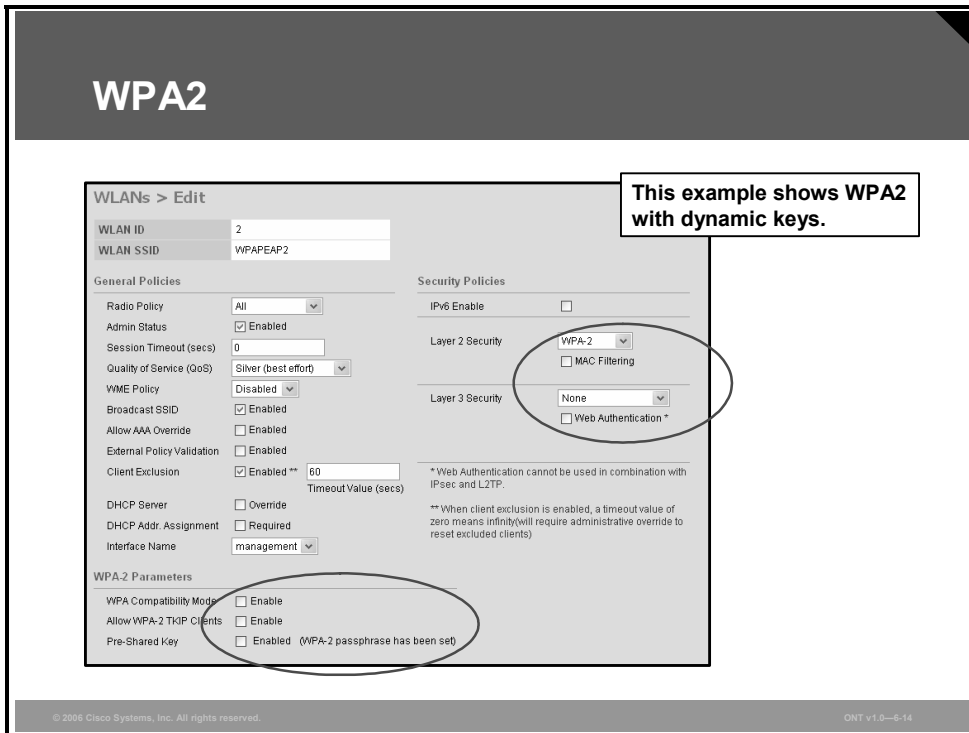
© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0—6-13

For new WLANs, create a new WLAN by choosing **WLANs > New**, then click **Apply** to navigate to this page. This page allows you to edit the configurable parameters for a WLAN.

Choose **WPA** from the Layer 2 Security drop-down list under the Security Policies heading. Leave the Pre-Shared Key Enabled check box unchecked, because no static keys are defined. The authentication process will use dynamic Extensible Authentication Protocol (EAP) 802.1x authentication to a RADIUS server.

WPA2

For existing WLANs, choose **WLANs** and then **Edit** to navigate to this page.



For new WLANs, create a new WLAN by choosing **WLANs > New**, then click **Apply** to navigate to this page. This page allows you to edit the configurable parameters for a WLAN.

Choose **WPA-2** from the Layer 2 Security drop-down list under the Security Policies heading. The security policy options and parameters at the bottom of the page are as follows:

- **WPA Compatibility Mode:** This option allows support for both WPA and WPA2 clients on the same service set identifier (SSID) to support legacy systems during migration to WPA.
- **Allow WPA-2 TKIP Clients:** This option allows support of legacy hardware that cannot run Advanced Encryption Standard-Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP) but can run WPA2.
- **Pre-Shared Key:** When this option is checked, you can choose to enable a preshared key with or without an 8- to 63-character Record Sequence Number (RSN) passphrase.

Summary

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

Summary

- **Configuration is done using a GUI.**
- **Guest or hot-spot access can deploy open or web authentication.**
- **Basic security can be implemented with static WEP.**
- **Improved security results when you use WPA or WPA2 using preshared keys or dynamic 802.1x.**

Managing WLANs

Overview

This lesson describes elements of the Cisco wireless LAN (WLAN) network. The five elements of the Cisco Unified Wireless Network are fundamental to building secure, successful enterprise-class WLANs. Customers can select the Cisco Unified Wireless Network elements and products that best meet their wireless networking needs. They can begin with client devices and a mobility platform of autonomous or lightweight access points and then add additional elements as their wireless networking requirements grow. All Cisco Aironet lightweight access points connect to Cisco Wireless LAN Controllers and support advanced services such as Fast Secure Roaming for voice and location services for real-time network visibility. Location and management services are supported by the optional Cisco Wireless Location Appliance and the Cisco Wireless Control System (WCS). Cisco Aironet access points operating autonomously are individually managed through the Cisco IOS command-line interface (CLI) or a web interface. Each autonomous access point is independent and does not require a wireless LAN controller or additional hardware for normal operation. Autonomous access points can be managed through CiscoWorks Wireless LAN Solution Engine (WLSE) or CiscoWorks WLSE Express. However, to receive all the advanced features and benefits of the Cisco Unified Wireless Network, customers must upgrade their existing Cisco Aironet autonomous access points to run Lightweight Access Point Protocol (LWAPP) and operate with a Cisco Wireless LAN Controller. CiscoWorks WLSE, Cisco WCS, and Cisco Wireless Location Appliance are part of WLAN management and are described in this lesson as well.

Objectives

Upon completing this lesson, you will be able to compare the wireless feature set and architecture of wireless networks using autonomous or lightweight access points. This ability includes being able to meet these objectives:

- Compare wireless solutions using autonomous access points to wireless solutions using lightweight access points, identifying how the two solutions together produce a complete unified wireless network
- Describe how Cisco implements WLANs
- Explain the hierarchy of components that are required to build a WLAN
- Describe basic features of CiscoWorks WLSE for the wireless feature set using autonomous access points and related products

- Describe the basic features of Cisco WCS for the wireless feature set using lightweight access points and related products
- Describe the Cisco WCS tracking options that are available
- Describe the use of the Cisco WCS Monitor tab functions to manage the WLAN
- Explain the function of the Cisco 2700 Series Wireless Location Appliance
- Describe basic Cisco WCS configuration
- Describe how to add, change, and use maps in the Cisco WCS database
- Describe the Cisco WCS rogue access point methodology

Cisco Unified Wireless Network

This topic describes the Cisco Unified Wireless Network.

Business Drivers

- **Wi-Fi-enabled notebook computers driving adoption of enterprise WLANs**
- **Anywhere, anytime connectivity**
- **Deployment wizard for access points**
- **Secure WLAN access required**
- **WLAN management scale of access point deployment**

© 2006 Cisco Systems, Inc. All rights reserved. OWT v1.0-4-2

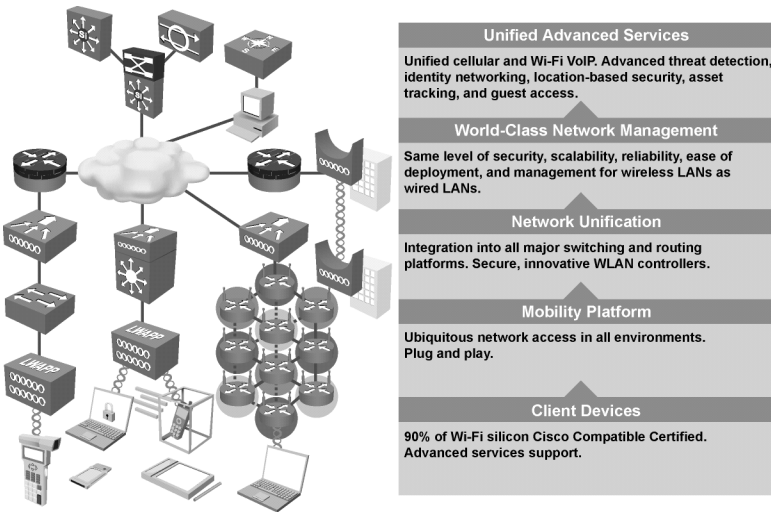
Business Drivers

A worldwide revolution is occurring in business. WLAN adoption is being driven by mobile users, traveling executives, wireless applications, and advanced services such as VoIP over Wi-Fi.

The modern business climate requires anywhere, anytime connectivity. Mobility changes the way that organizations do business.

Network managers need to protect their networks and deliver secure WLAN access for their organizations. They need a wireless infrastructure that embraces the unique attributes of RF technology and effectively supports today's business applications. They need to keep their wired network secure while laying a foundation for the smooth integration of new applications that embrace wireless technology. Network managers need a WLAN solution that takes full advantage of existing tools, knowledge, and network resources to cost-effectively address critical WLAN security, deployment, and control issues. The Cisco WLAN solution consists of Cisco Wireless LAN Controllers and their associated lightweight access points controlled by the operating system, all concurrently managed by any or all of the operating system user interfaces. All these elements are described in this lesson.

Cisco Unified Wireless Network



© 2006 Cisco Systems, Inc. All rights reserved.

ONT v1.0-6.4

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. Cisco's unique 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.

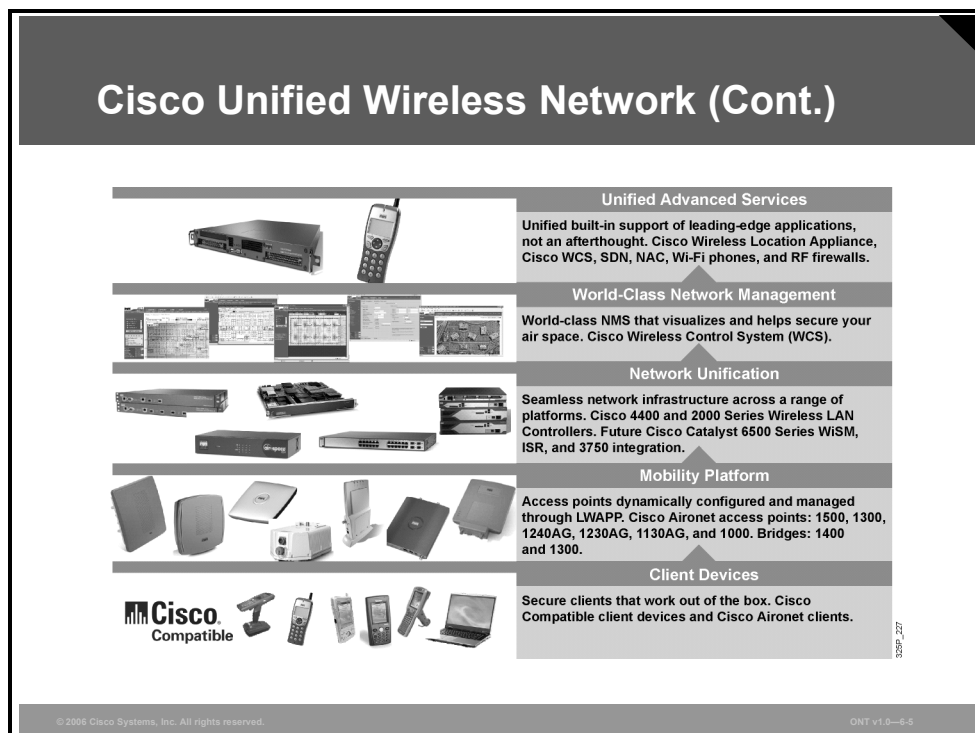
The Cisco Unified Wireless Network is composed of five interconnected elements that work together as building blocks to deliver a unified enterprise-class wireless solution.

- **Client devices:** Cisco is leading the development of interoperable, standards-based client devices through its Cisco Compatible Extensions program. This 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 Extensions client devices deliver “out of the box” wireless mobility, quality of service (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 through Cisco Wireless LAN Controllers. Cisco Wireless LAN Controllers are responsible for systemwide WLAN functions, such as an integrated intrusion prevention 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. Cisco's world-class WLAN management interface is the industry-leading Cisco WCS. 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 other wireless point product vendors. Cisco's 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 (NAC), Self-Defending Network, Cisco Identity Based Networking Services (IBNS), intrusion detection systems (IDSs), and guest access for end-to-end network security

Cisco Unified Wireless Network Components

This subtopic describes the components of the Cisco Unified Wireless Network.



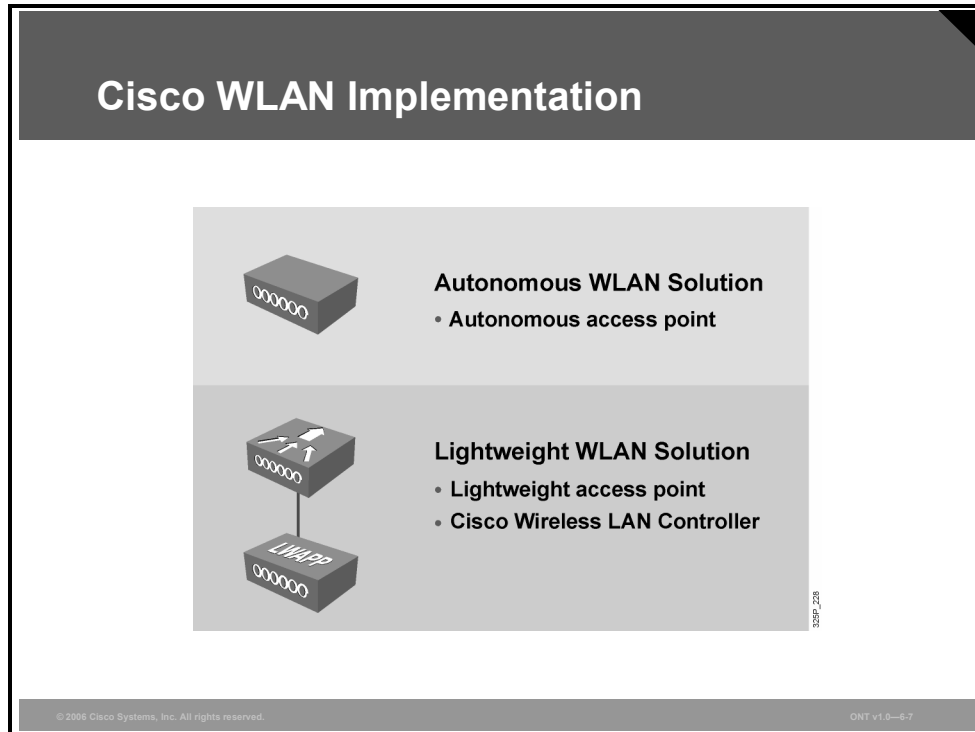
The following Cisco WLAN products support the five interconnecting elements of the Cisco Unified Wireless Network and business-class WLANs:

- **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 is likely to be 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 LWAPP are supported.

- **Network unification:** The Cisco Unified Wireless Network leverages existing wired networks and the investment in Cisco products. It supports a seamless network infrastructure across a range of platforms. Wired and wireless unification occurs with the Cisco 4400 and 2000 Series Wireless LAN 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, IPS, and 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's advanced services are industry-leading, innovative, and comprehensive. The Cisco Unified Wireless Network advanced services are delivered by wireless lightweight access points, Cisco Wireless Location Appliance, and wireless IP phones.

Cisco WLAN Implementation

This topic describes how Cisco implements WLANs.

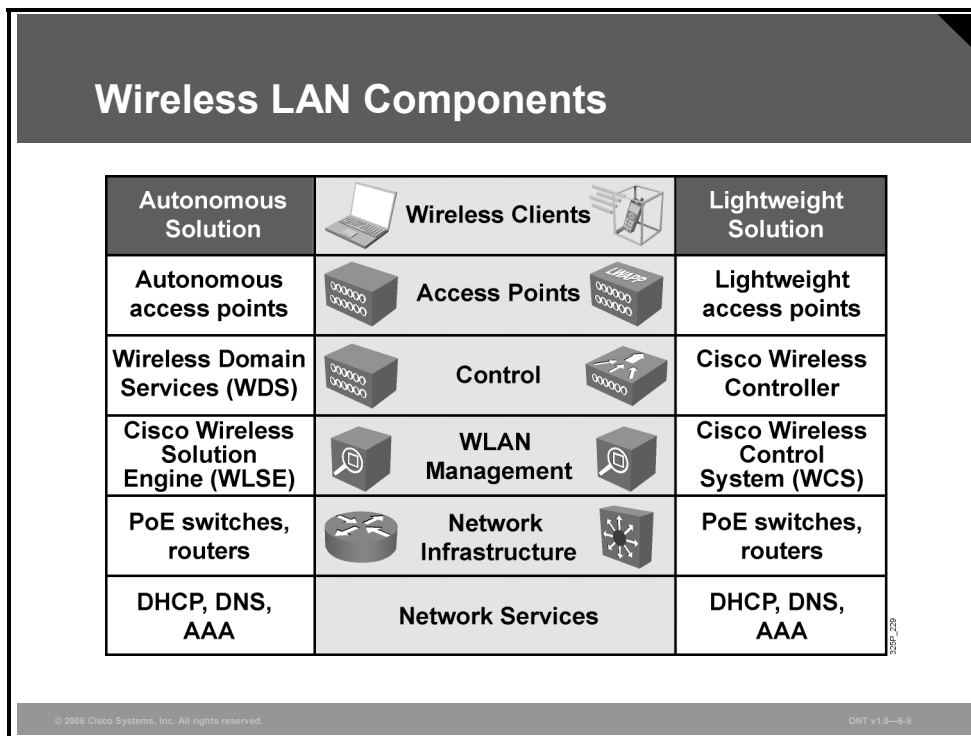


Cisco offers two WLAN implementations:

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

Describing WLAN Components

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



A WLAN consists of the following components:

- Wireless clients are connected to the network (for example, notebooks or IP phones).
- Access points build the WLAN infrastructure.
 - Autonomous access points are configured independently.
 - Lightweight access points are configured through LAN controllers.
- Radio monitoring and control is provided.
 - Autonomous access points aggregate information through Wireless Domain Services (WDS) which in turn forwards to a CiscoWorks WLSE.
 - Lightweight access points use LWAPP encapsulation to forward information independently to their respective LAN controllers.
- WLAN management is used to administer and monitor large deployments of WLANs.
 - Autonomous access points use CiscoWorks WLSE management.
 - Lightweight access points use Cisco WCS management.
- The network infrastructure is provided by switches and routers to connect access points, controllers, management, and servers.
- Network services such as DHCP, Domain Name System (DNS), and authorization, authentication, and accounting (AAA) are required both for the wireless network and the user.
- Cisco Aironet bridges operate at the MAC address layer (data link layer).

Comparison of the WLAN Solutions

This subtopic compares the autonomous and lightweight WLAN solutions.

Comparison of the WLAN Solutions	
Autonomous WLAN solution	Lightweight WLAN solution
<ul style="list-style-type: none">• Autonomous access point• Configuration of each access point• Independent operation• Management via CiscoWorks WLSE and WDS• Access point redundancy	<ul style="list-style-type: none">• Lightweight access point• Configuration via Cisco Wireless LAN Controller• Dependent on Cisco Wireless LAN Controller• Management via Cisco Wireless LAN Controller• Cisco Wireless LAN Controller redundancy

© 2006 Cisco Systems, Inc. All rights reserved. OMT v1.0—6-10

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 through CiscoWorks WLSE. Radio monitoring and management communication is facilitated between the autonomous access points and CiscoWorks WLSE through use of WDS. WDS is a feature enabled in any access point that forwards aggregated RF information from a grouping of access points to CiscoWorks WLSE.

Lightweight access points are configured via the Cisco Wireless LAN Controller. They depend on the controller for control and data transmission. Only in Remote-Edge Access Point (REAP) mode does a lightweight access point not depend on the Cisco Wireless LAN Controller for data transmission. Monitoring and security are implemented by the controller. Centralized configuration, monitoring, and management can be done through Cisco WCS. Cisco Wireless LAN Controllers can be installed with redundancy within wireless LAN controller groups.

CiscoWorks WLSE

This topic describes CiscoWorks WLSE, which supports basic centralized configuration, firmware, and radio management of autonomous access points.

CiscoWorks WLSE Software Features

CiscoWorks WLSE is a solution for managing the Cisco autonomous access point infrastructure:

- **Configuration of access points**
- **Fault and policy monitoring**
- **Reporting**
- **Firmware upgrade on access points and bridges**
- **Radio management**
- **CiscoWorks WLSE administration**
- **Deployment wizard for access points**

© 2006 Cisco Systems, Inc. All rights reserved.

ONT v1.0-4-12

CiscoWorks WLSE is a systems-level solution for managing the entire Cisco Aironet WLAN infrastructure based on autonomous access points. The RF and device-management features of CiscoWorks WLSE simplify the everyday operation of WLANs, helping to ensure smooth deployment of security and network availability while reducing deployment and operating expense. CiscoWorks WLSE operates by gathering fault, performance, and configuration information about Cisco devices that it discovers in the network. The access points, WDS, switches, and routers must be properly configured with Cisco Discovery Protocol (CDP) and Simple Network Management Protocol (SNMP) to provide information to CiscoWorks WLSE for the access point discovery process. After devices are discovered, you decide which devices to manage with CiscoWorks WLSE. CiscoWorks WLSE is a core component of the WLAN autonomous access-point solution.

CiscoWorks WLSE has these major features:


- **Configuration:** Allows you to apply configuration changes to access points. Up to 2500 access points can be supported from a single CiscoWorks WLSE console. All Cisco Aironet access points are supported.
- **Fault and policy monitoring:** Monitors device fault and performance conditions, Lightweight Extensible Authentication Protocol (LEAP) server responses, and policy misconfigurations.
- **Reporting:** Allows you to track device, client, and security information. You can e-mail, print, and export reports.
- **Firmware:** Allows you to upgrade the firmware on access points and bridges.
- **Radio management:** Helps you manage your WLAN radio environment.

- **CiscoWorks WLSE administration:** Manages CiscoWorks WLSE software, including software upgrades, monitoring CiscoWorks WLSE, backing up data, and using two CiscoWorks WLSE devices as a redundant, highly available WLAN management solution. CiscoWorks WLSE supports warm-standby redundancy. A backup server can be configured to take over wireless management if there is a primary CiscoWorks WLSE failure.
- **Deployment wizard:** Configures and discovers access points used in a Cisco Unified Wireless Network.

CiscoWorks WLSE Key Benefits

Autonomous access points can be managed through CiscoWorks WLSE, which provides many benefits.

CiscoWorks WLSE Key Benefits



- **Improved WLAN security**
- **Simplified access point deployment**
- **RF visibility**
- **Dynamic RF management**
- **Simplified operations**

© 2006 Cisco Systems, Inc. All rights reserved.
ONT v1.0—6-13


CiscoWorks WLSE provides centralized management and RF visibility for Cisco Aironet autonomous access points and bridges. This solution gives users many benefits:

- **Improved WLAN security:** Wireless IDS for rogue access points, ad hoc networks, excess 802.11 management frames that signal denial-of-service (DoS) attacks, and man-in-the-middle attacks
- **Simplified access point deployment:** Configuration policies created using Deployment Wizard that are automatically applied to new access points
- **RF visibility:** RF coverage and received signal strength indicator (RSSI) displays, rogue access point location, and roaming boundaries
- **Dynamic RF management:** Self-healing, assisted site survey, automatic re-site survey, interference detection, and associated access point tracking for clients
- **Simplified operations:** Template-based configuration and image updates, reporting, and threshold-based monitoring

CiscoWorks WLSE and WLSE Express

Two versions of CiscoWorks WLSE exist. CiscoWorks WLSE Express is focused on small and medium-sized businesses (SMBs) and supports fewer access points.

CiscoWorks WLSE and CiscoWorks WLSE Express



CiscoWorks WLSE **CiscoWorks WLSE Express**

- **Centralized management appliance for autonomous access point solution**
- **CiscoWorks WLSE:**
 - Used for medium-to-large enterprises (up to 2500)
 - Requires external AAA server
- **CiscoWorks WLSE Express:**
 - Used for SMB, commercial, and branch offices (up to 100)
 - AAA server included

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0-6-14

CiscoWorks WLSE is used for centralized management of wireless networks using autonomous access points. CiscoWorks WLSE supports the following WLAN devices:

- Cisco Aironet autonomous access points and bridges
- Access point- and Cisco Catalyst 6500 Series Wireless LAN Services Module (WLSM)-based WDS

CiscoWorks WLSE supports Secure Shell (SSH), HTTP, CDP, and SNMP host resources MIB.

CiscoWorks WLSE integrates with CiscoWorks wired management tools and third-party network management systems (NMSs):

- Simple Object Access Protocol (SOAP) Extensible Markup Language (XML) application programming interface (API) for data export
- SNMP trap and syslog forwarding for faults

The two versions of CiscoWorks WLSE available scale to different network sizes. CiscoWorks WLSE is used for medium to large enterprise and wireless verticals (up to 2500 WLAN devices). CiscoWorks WLSE Express is used for SMBs (250 to 1500 employees) and commercial and branch offices (up to 100 WLAN devices) looking for a cost-effective solution with integrated WLAN management and security services. Enterprise branch office deployments usually want to localize WLAN security and management services to provide WLAN access survivability during WAN failures. They do not want to use WAN bandwidth for WLAN and RF management traffic. Some service providers can use CiscoWorks WLSE Express, because public WLAN (PWLAN) hot-spot management requires fewer WLAN devices. CiscoWorks WLSE requires an external AAA server, which is already included with CiscoWorks WLSE Express. CiscoWorks WLSE Express has integrated WLAN security and management services supporting 802.1x LEAP, Protected Extensible Authentication Protocol (PEAP), Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), and Extensible Authentication Protocol-Transport Layer Security (EAP-TLS). The user directory supports Lightweight Directory Access Protocol (LDAP), Microsoft Active Directory, and a local user database. Both wired and wireless user authentication are supported. WLAN IDS features are supported, too.

Simplified CiscoWorks WLSE Express Setup

CiscoWorks WLSE Express setup can be simplified by using automatic setup, or you can use manual setup commands.

Simplified CiscoWorks WLSE Express Setup

Setup options:

- **Automatic configuration download from DHCP server:**
 - DHCP enabled by default
 - Options 66, 67 provide TFTP IP address and filename
- **Use setup command to configure CiscoWorks WLSE Express**

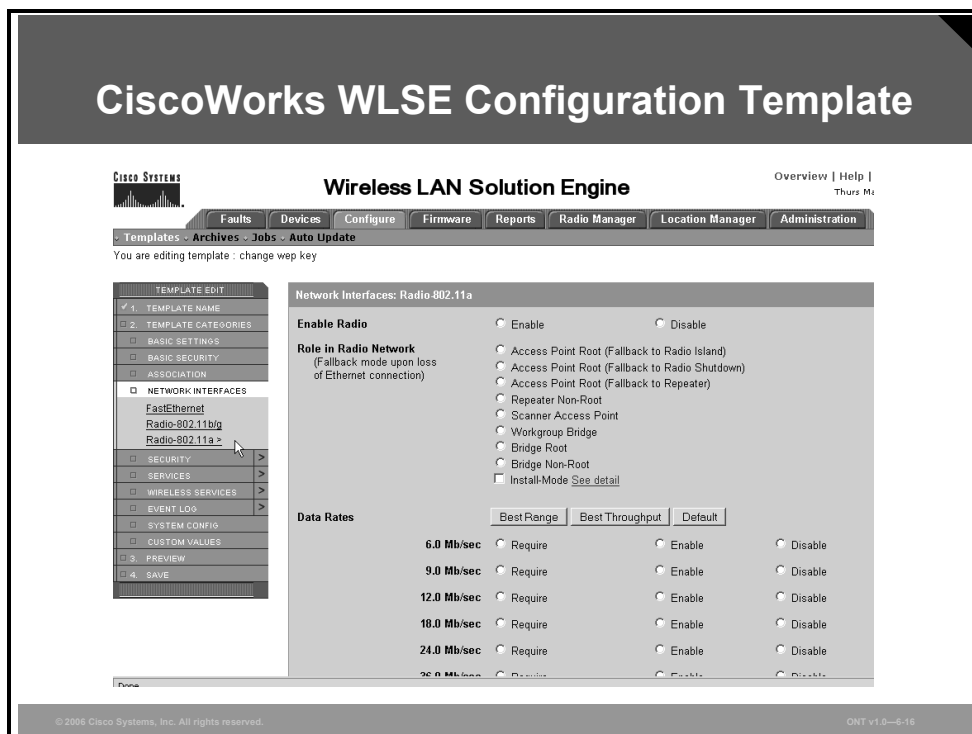
© 2006 Cisco Systems, Inc. All rights reserved.ONT v1.0-6-15

CiscoWorks WLSE Express supports two modes of setup options:

- **Automatic:** After you have installed CiscoWorks WLSE Express, you can arrange for it to be autoconfigured. As each CiscoWorks WLSE is started for the first-time, a special configuration file is automatically downloaded, and CiscoWorks WLSE is ready for use. The configuration is downloaded from a DHCP server. The DHCP option is enabled by default. A TFTP IP address and filename are provided with options 66 and 67. CiscoWorks WLSE Express downloads its configuration, including host name, default gateway, and so on.
- **Manual:** By default, the CiscoWorks WLSE Express Ethernet interface is set to DHCP mode. When it is powered on, a CiscoWorks WLSE attempts to obtain its network configuration from a DHCP server. If you do not want to configure a DHCP server with this information, you can log in and configure the network parameters manually after CiscoWorks WLSE starts. You can manually configure CiscoWorks WLSE Express using the setup script and entering CLI commands.

Configuration Templates

CiscoWorks WLSE configuration is done through a web-based GUI using templates. Besides configuration and monitoring, CiscoWorks WLSE supports performance optimization and high availability.



CiscoWorks WLSE supports centralized configuration and image management. Easy deployment uses several templates:

- Plug-and-play deployment
- Automatic configuration of access points added to CiscoWorks WLSE
- Automatic RF configuration of access points
- Calculation of optimal RF configurations by access points

CiscoWorks WLSE includes WLAN intrusion detection with the following features:

- Detection of location and automatic shutdown of rogue access points via disabled switch ports
- Ad hoc network detection
- Man-in-middle detection by monitoring message integrity check (MIC) failures
- Access point configuration monitor to ensure that security policies are always enforced
- Sensor mode access points that can augment WLAN deployments for enhanced features

CiscoWorks WLSE is designed for all day-to-day operations as well as for performance optimization and high availability using Auto Re-Site Survey and Self Healing.

Using Auto Re-Site Survey, CiscoWorks WLSE can provide optimal channel and power-level settings based on the access point air and RF monitoring phase of Assisted Site Survey only. Client walkabout is not needed, but performing client walkabouts during the Assisted Site Survey is recommended. It increases the coverage for RF management and makes the survey more effective.

CiscoWorks WLSE can detect that an access point has failed. It compensates for the loss by automatically increasing the power and cell coverage of nearby access points. The Self Healing feature minimizes the outage impact to wireless client devices and maximizes the availability of wireless applications. Self Healing also recalculates power coverage when the radio comes back up.

CiscoWorks WLSE Benefits

CiscoWorks WLSE reduces total cost of ownership, minimizes security vulnerabilities, and improves WLAN uptime.

CiscoWorks WLSE Benefits	
Feature	Benefits
Centralized configuration, firmware, and radio management	Reduces WLAN total cost of ownership by saving time and resources required to manage large numbers of access points
Autoconfiguration of new access points	Simplifies large-scale deployments
Security policy misconfiguration alerts and rogue access point detection	Minimizes security vulnerabilities
Access point utilization and client association reports	Helps in capacity planning and troubleshooting
Proactive monitoring of access points, bridges, and 802.1x EAP servers	Improves WLAN uptime

© 2006 Cisco Systems, Inc. All rights reserved. OMT v1.0--6.17

CiscoWorks WLSE supports centralized configuration, firmware, and radio management, which reduces WLAN total cost of ownership by saving the time and resources required to manage large numbers of access points. CiscoWorks WLSE aggregates all configurations, images, and management information in one place.

Templates, one of the features of CiscoWorks WLSE, allow autoconfiguration of new access points for simplified large-scale deployment of access points. When a new access point is added to the system, you can use the template to configure it.

Access points added to the system require correct configuration. CiscoWorks WLSE detects misconfiguration and follows with an alert, the process used to detect a rogue access point and to minimize security vulnerabilities.

CiscoWorks WLSE is capable of monitoring access point utilization and client association. A report that includes the number of access points and clients can be used for capacity planning and troubleshooting.

The CiscoWorks WLSE configuration templates are not only used for new access points. The system allows you to proactively monitor access points, bridges, and 802.1x EAP servers. The system is able to push down to an access point configuration changes or any other changes required, which improves WLAN uptime.

Cisco WCS

This topic describes Cisco Wireless Control System (WCS), which supports advanced centralized configuration, firmware, radio management, and IDS of lightweight access points and their associated controllers.

Cisco WCS Overview

- **Cisco WCS is a solution for managing Cisco lightweight access point infrastructure**
- **Flexible and secure network management tool:**
 - Intuitive GUI
 - Browser accessible via HTTPS
 - Device management via SNMP (supports SNMPv1, SNMPv2, and SNMPv3)
- **Ease of system maintenance**
- **Three versions of Cisco WCS:**
 - Cisco WCS Base
 - Cisco WCS Location
 - Cisco WCS Location + Cisco 2700 Series Wireless Location Appliance

© 2006 Cisco Systems, Inc. All rights reserved.ONT v1.0—6-18

Overview of Cisco WCS

Cisco WCS is a Cisco WLAN solution network-management tool that adds to the capabilities of the web user interface and CLI, moving from individual controllers to a network of controllers. Cisco WCS includes the same configuration, performance monitoring, security, fault management, and accounting options used at the controller level and adds a graphical view of multiple controllers and managed access points.

Cisco WCS runs on the Microsoft Windows and Linux platforms. It can run as a normal application or as a service, which runs continuously and resumes running after a reboot.

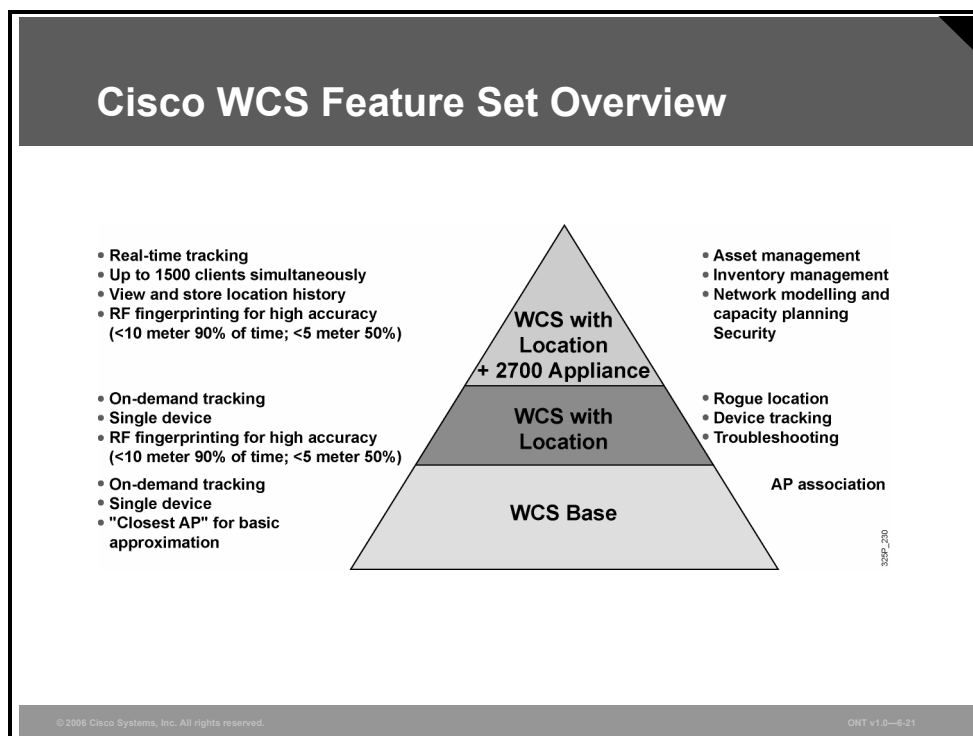
The Cisco WCS user interface enables operators to control all permitted Cisco WLAN solution configuration, monitoring, and control functions through Microsoft Internet Explorer 6.0 or later. Operator permissions are defined by the administrator using the Cisco WCS user interface Administration menu, which enables the administrator to manage user accounts and schedule periodic maintenance tasks.

Cisco WCS simplifies controller configuration and monitoring while reducing data-entry errors with the Cisco Wireless LAN Controller autodiscovery algorithm. Cisco WCS uses SNMP to communicate with the controllers.

Cisco WCS software is the industry-leading platform for WLAN planning, configuration, and management. It provides a powerful foundation that IT managers can use to design, control, and monitor enterprise wireless networks from a centralized location, simplifying operations and reducing the total cost of ownership. Flexible and secure NMSs are made possible by an intuitive GUI with a browser accessible via HTTPS. Cisco WCS supports SNMP version 1 (SNMPv1), SNMPv2, and SNMPv3.

Cisco WCS Location Tracking Options

This topic describes three Cisco WCS tracking options.



Cisco provides a variety of options for efficiently tracking wireless devices, including Wi-Fi-enabled laptops, PDAs, voice handsets, and mobile assets equipped with 802.11 transceivers.

The base version of Cisco WCS can determine which access point a wireless device is associated with, giving IT managers a general approximation of where wireless devices are situated.

Environments that require more granular location services can implement an optional version of Cisco WCS, called Cisco WCS Location, that uses Cisco's patent-pending RF fingerprinting technology. This technology compares real-time client RSSI information to known RF building characteristics, making Cisco the only WLAN infrastructure with the ability to accurately locate a wireless device to within a few meters.

In addition, Cisco WCS Location can be deployed in conjunction with Cisco Wireless Location Appliance to simultaneously track thousands of wireless clients in real time.

With these advanced location-tracking capabilities, the Cisco Unified Wireless Network is an ideal platform for helping to enable key business applications that take advantage of wireless mobility, such as asset tracking, inventory management, and enhanced 911 (e911) services for voice. By incorporating indoor location tracking into the wireless LAN infrastructure itself, Cisco reduces the complexities of wireless LAN deployment and minimizes total cost of ownership.

Cisco WCS Base Software Features

Cisco WCS Base supports wireless client data access, rogue access point detection and containment functions (such as real-time location of rogue access points to the nearest Cisco access point and real-time and historical location of clients to the nearest Cisco access point), and Cisco WLAN solution monitoring and control.

Cisco WCS Base Software Features

- **Autodiscovery of access points**
- **Autodiscovery of rogue access points**
- **Map-based organization of access point coverage areas**
- **User-supplied campus, building, and floor plan graphics**
- **Systemwide control of streamlined network, controller, and managed APs:**
 - **Configuration, channel, and power level assignment**
 - **Status and alarm monitoring**
 - **Monitoring of rogue access points and security violations**
 - **Full event logs**

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0-4.22

Cisco WCS software features include graphical views of the following:

- Autodiscovery of access points as they associate with controllers
- Autodiscovery and containment or notification of rogue access points
- Map-based organization of access point coverage areas, which is helpful when the enterprise spans more than one geographical area
- User-supplied campus, building, and floor plan graphics, which show this information:
 - Locations and status of managed access points.
 - Locations of rogue access points based on the signal strength received by the nearest managed Cisco access points.
 - Coverage hole alarm information for access points based on the received signal strength from clients. This information appears in tabular rather than map format.
 - RF coverage maps.

Cisco WCS Base also provides systemwide control of the following:

- Configuration using customer-defined templates for controllers and managed access points
- Status and alarm monitoring of network, controllers, and managed access points
- Automated and manual data client monitoring and control functions
- Automated monitoring of rogue access points, coverage holes, security violations, controllers, and access points

- Full event logs for data clients, rogue access points, coverage holes, security violations, controllers, and access points
- Automatic channel and power level assignment by radio resource management (RRM)
- User-defined automatic controller status audits, missed trap polling, configuration backups, and policy cleanups

Cisco WCS Location Software Features

Cisco WCS Location includes all the features of Cisco WCS Base plus some enhancements.

Cisco WCS Location Software Features

- **All Cisco WCS Base software features**
- **On-demand location of rogue access points to within 33 feet (10 meters)**
- **On-demand location of clients to within 33 feet**
- **Ability to use Cisco Wireless Location Appliances**

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0—6-23

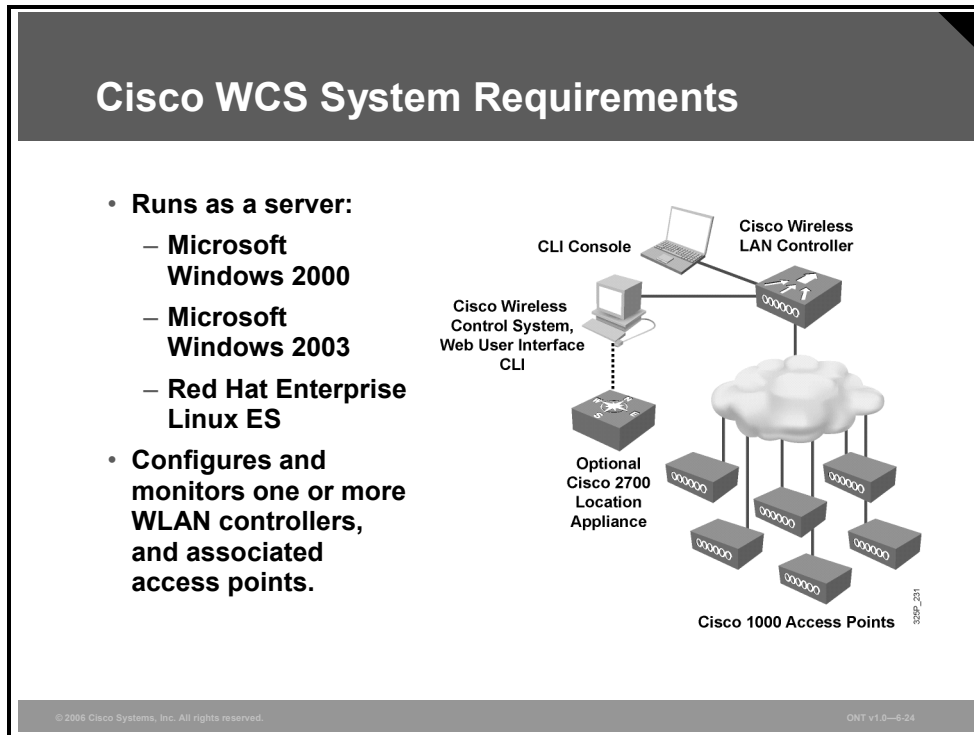
Cisco WCS Location includes all the features of the Cisco WCS Base as well as these enhancements:

- On-demand location of rogue access points to within 33 feet (10 meters)
- On-demand location of clients to within 33 feet
- The ability to use location appliances to collect and return historical location data viewable in the Cisco WCS Location user interface

Cisco Wireless Location Appliance can be used to improve the functionality of Cisco WCS Location. Cisco Wireless Location Appliance performs location computations based on the RSSI information received from Cisco Wireless LAN Controllers. The Cisco Wireless LAN Controllers that gather the RSSI information must be associated with the Cisco Wireless Location Appliance. The Cisco 2700 Series Location Appliance is a Cisco Wireless Location Appliance that can be used (its use is explained later in the lesson).

Cisco WCS System Features

The Cisco WCS operating system manages all data client, communications, and system administration functions, performs RRM functions, manages systemwide mobility policies using the operating system security solution, and coordinates all security functions using the operating system security framework.



Cisco WCS is supported under Microsoft Windows 2000, Windows 2003, and Red Hat Enterprise Linux ES v.3 servers as either a normal application or a service.

The Cisco WLAN solution consists of Cisco Wireless LAN Controllers and their associated lightweight access points controlled by the operating system, all concurrently managed by any or all of the operating system user interfaces. One of them is Cisco WCS. The following user interfaces exist:

- An HTTPS full-featured web user interface hosted by Cisco controllers can be used to configure and monitor individual controllers.
- A full-featured CLI can be used to configure and monitor individual controllers.
- Cisco WCS can be used to configure and monitor one or more controllers and associated access points. Cisco WCS has tools to facilitate large-system monitoring and control.
- An industry-standard SNMPv1, SNMP 2c, and SNMPv3 interface can be used with any SNMP-compliant third-party network management system.

Cisco WCS User Interface

The Cisco WCS user interface enables the network operator to create and configure Cisco WLAN solution coverage area layouts, configure system operating parameters, monitor real-time Cisco WLAN solution operation, and perform troubleshooting tasks using an HTTPS web browser window. The Cisco WCS user interface also enables the WCS administrator to create, modify, and delete user accounts; change passwords; assign permissions; and schedule periodic maintenance tasks. The administrator creates new usernames and passwords and assigns them to predefined permissions groups.

Note It is recommended that you use Microsoft Internet Explorer 6.0 or later on a Windows workstation for full access to Cisco WCS functionality.

System Requirements for Cisco WCS

Minimum server requirements are as follows:

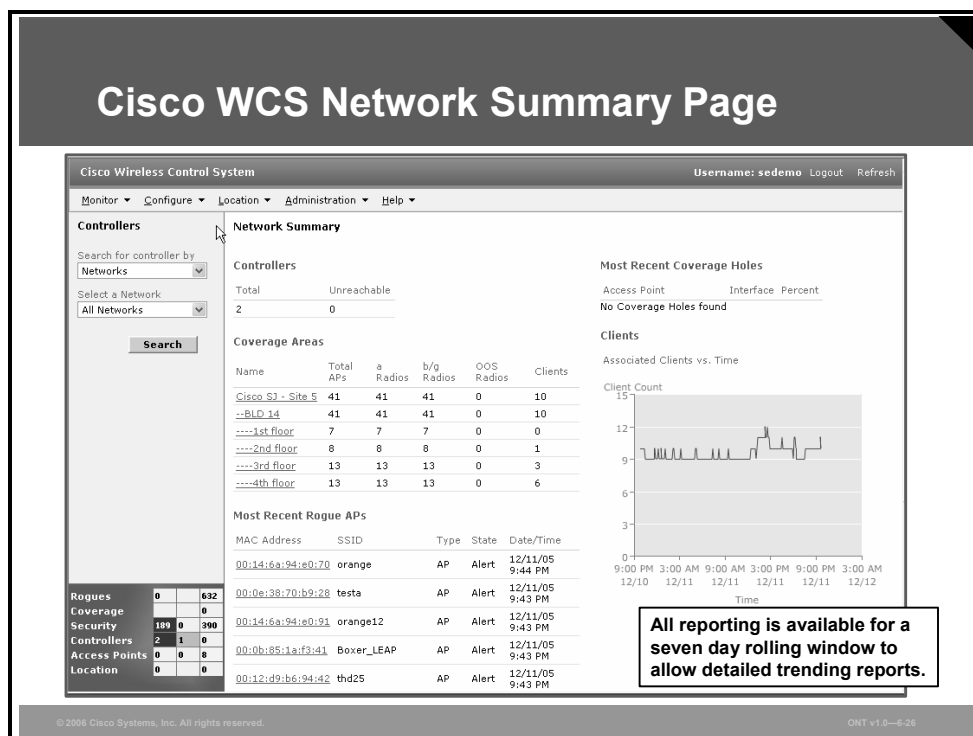
- Windows 2000 Service Pack 4 (SP4) or greater, Windows 2003 SP1 or greater, or Red Hat Enterprise Linux ES v.3
- Up to 500 access points: 2.4-GHz Pentium with 1-GB RAM
- More than 500 access points: dual processors (At least 2.4 GHz each) with minimum 2-GB RAM
- 20-GB hard drive

The minimum client requirement is as follows:

- Internet Explorer 6.0 with SP1 or later

Cisco WCS Network Summary Page

This topic discusses the use of the Monitor tab functions to manage the WLAN.



Choose **Monitor** > **Network Summary** to access the Network Summary page. This page provides a top-level description of your network and includes information about controllers, coverage areas, access points, clients, and so on.

Menu Bar

There are four menus on each screen. When you move the mouse over any of the menu items, a drop-down menu appears:

- **Monitor:** The Monitor menu provides you with a top-level description of the devices on your network.
- **Configure:** The Configure menu allows you to configure templates, controllers, and access points on your network.
- **Administration:** The Administration menu allows you to schedule tasks such as making a backup, checking device status, auditing your network, synchronizing the location server, and so on.
- **Location:** The Location menu allows you to configure Cisco Wireless Location Appliances.

Note The Location menu is displayed only with Cisco WCS Location.

Cisco WCS Controller Summary Page

Cisco WCS is designed to support 50 Cisco Wireless LAN Controllers and 1500 access points.

Cisco WCS Controller Summary Page

Controllers > 171.71.128.75 > Summary

General

IP Address	171.71.128.75
Name	SJC 14 LWAPP1
Type	4400
UP Time	10 days 3 hrs 19 mins 53 secs
System Time	Sun Dec 11 23:00:27 2005
Internal Temperature	5000 C
Location	SJC Bld 14
Total Client Count	1
Current LWAPP Transport Mode	Layer3
Power Supply One	Absent , Not Operational
Power Supply Two	Present , Operational

Inventory

Software Version	3.2.78.0
Description	Cisco Controller
Model No.	WLC4404-100
Serial No.	FLS0923003U
Burned-in MAC Address	00:0b:85:32:ad:a0
Number of APs Supported	100

Total APs 15

Utilization (%)

Cisco WCS is designed to support 50 Cisco Wireless Controllers and 1500 access points.

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0-4-27

This section provides access to the controller summary details. Use the selector area to access details for the respective controllers.

Choose **Monitor > Devices > Controllers** to access this section. By default, the Monitor Controllers > Search Results page is displayed.

The data area of this screen contains a table with the following information:

- **IP address:** Local network IP address of the controller management interface. Select the title to toggle from ascending to descending order. Select an IP address in the list to display Controllers > <IP address> > Summary.
- **Controller name:** Select the title to toggle from ascending to descending order.
- **Location:** The geographical location (such as a campus or building). Select the title to toggle from ascending to descending order.
- **Mobility group name:** Name of the controller mobility or Microsoft Wireless Provisioning Services (WPS) group.
- **Reachability status:** Reachable or unreachable. Select the title to toggle from ascending to descending order.

Cisco Wireless Location Appliance

This topic describes the functions of the Cisco 2700 Series Wireless Location Appliance, which enhances the high-accuracy location abilities built into Cisco WCS by computing, collecting, and storing historical location data.

Cisco Wireless Location Appliance Overview

- **Cisco 2700 Series Wireless Location Appliances are servers that enhance the high-accuracy built-in Cisco WCS:**
 - **Computing historical location data**
 - **Collecting historical location data**
 - **Storing historical location data**
- **Configuration and operation uses Cisco WCS, which has an easy-to-use GUI.**
- **Initial configuration using a CLI console session is required before you use the GUI.**

© 2006 Cisco Systems, Inc. All rights reserved.

ONT v1.0—6-23

Product Overview

The Cisco Wireless Location Appliance is an innovative, easy-to-deploy solution that uses advanced RF fingerprinting technology to simultaneously track thousands of 802.11 wireless devices from directly within a WLAN infrastructure, increasing asset visibility and control of the airspace.

Cisco 2700 Series Wireless Location Appliances are servers that enhance the high-accuracy built-in Cisco WCS location abilities by computing, collecting, and storing historical location data for up to 1500 laptop clients, palmtop clients, VoIP telephone clients, radio frequency identifier (RFID) asset tags, rogue access points, and rogue access point clients.

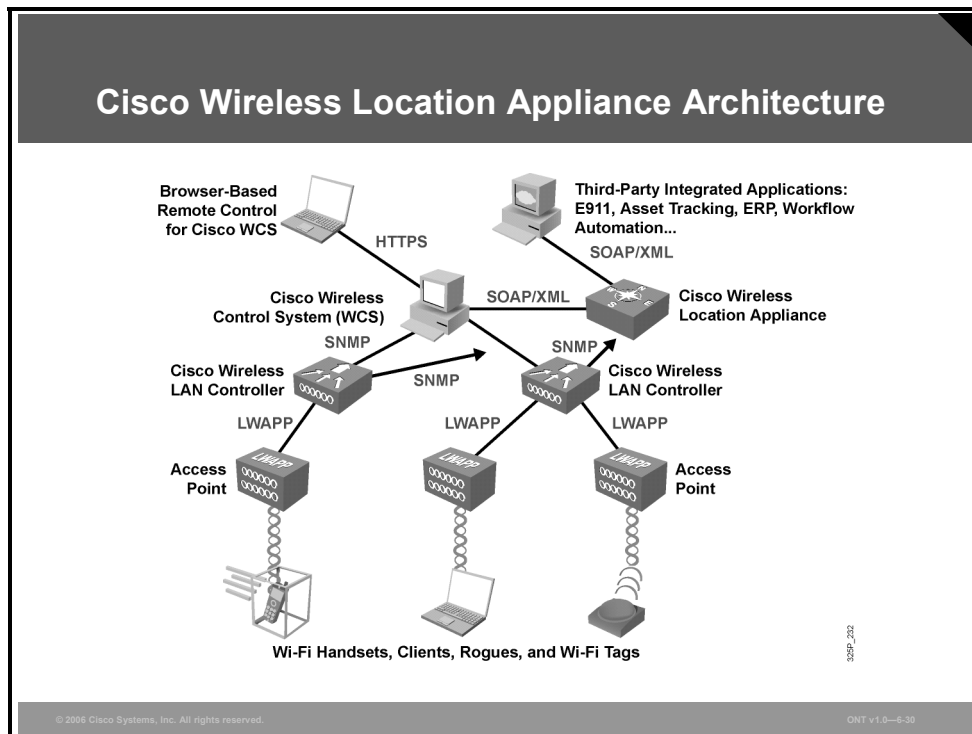
A Cisco 2700 Series Wireless Location Appliance acts as a server to one or more Cisco WCS devices, collecting, storing, and passing on data from its associated Cisco Wireless LAN Controllers.

Additionally, the appliance provides location-based alerts for business policy enforcement and records rich historical location information that can be used for location trending, rapid problem resolution and RF capacity management.

By design, the Cisco 2700 Series Wireless Location Appliance is directly integrated into the WLAN infrastructure to lower total cost of ownership and extend the value and security of the existing WLAN infrastructure by making it “location aware.” As a component of the Cisco Unified Wireless Network, the Cisco Wireless Location Appliance uses Cisco Wireless LAN Controllers and Cisco Aironet lightweight access points to track the physical location of wireless devices to within a few meters. Moreover, the centralized WLAN management capabilities and intuitive GUI of Cisco WCS are extended for managing and configuring the Cisco Wireless Location Appliance, making setup fast and intuitive.

Cisco Wireless Location Appliance Architecture

The Cisco Wireless Location Appliance serves as a client to Cisco WCS. Cisco WCS provides control and visualization of Cisco Wireless Location Appliance capabilities. A single Cisco WCS can manage multiple Cisco Wireless Location Appliances.



The Cisco Wireless Location Appliance uses the same Cisco lightweight access points that deliver traffic as location “readers” for 802.11 wireless clients and Wi-Fi tags. These access points collect RSSI information from all Wi-Fi devices, including Wi-Fi-enabled laptops, voice handsets, Wi-Fi tags, rogue (unauthorized) devices and rogue access points. The collected RSSI information is then sent through Lightweight Access Point Protocol (LWAPP) to the Cisco Wireless LAN Controllers or certain wireless integrated switches or routers.

Note Wi-Fi tags, which transmit wireless signals, are tags added to equipment to make it easy to track. Access points can collect RSSI information that can be later used for processing.

The Cisco Wireless LAN Controllers then aggregate the RSSI information and send it to the Cisco Wireless Location Appliance through SNMP.

The Cisco Wireless Location Appliance performs location computations based on the RSSI information received from the Cisco Wireless LAN Controllers. The Cisco Wireless LAN Controllers that gather the RSSI information must be associated with the Cisco Wireless Location Appliance.

After network maps and access points are added to the appliance, RF predictions and heat maps can be generated to graphically display the location of thousands of devices on the site floor plans. Cisco WCS displays location information visually, providing an immediate location application for customers that want to enhance their RF capacity management, use location-based security, and maintain asset visibility for WLAN devices. This location information is also available to third-party applications through a SOAP XML API on the appliance, creating an extensible foundation for a host of rich location-based applications.

Cisco WCS manages the Cisco Wireless Location Appliance through an intuitive and visually rich GUI providing centralized management and configuration. For greater scalability, Cisco WCS can manage one or more Cisco Wireless Location Appliances. The Cisco WCS view filters and flexible search criteria make targeted viewing of location data easy and adaptive to user needs.

Cisco Wireless Location Appliance Applications

After it is configured, each location server communicates directly with the Cisco Wireless LAN Controllers to which it was assigned to collect operator-defined location data. You can then use the associated Cisco WCS server to communicate with each location server to transfer and display selected data.

Cisco Wireless Location Appliance Applications

- **Visibility and tracking of 1500 mobile devices for 30 days**
- **Work-flow automation and people tracking**
- **Telemetry**
- **WLAN security and network control**
- **RF capacity management and visibility**



© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0—4-31

After the Cisco Wireless Location Appliance is configured, you can configure appliances to collect data for Cisco WLAN solution clients, access points, mobile stations, and RFID asset Wi-Fi tags at intervals that you define. The collected information is used for tracking. Tracking of up to 1500 devices for a 30-day period is enabled.

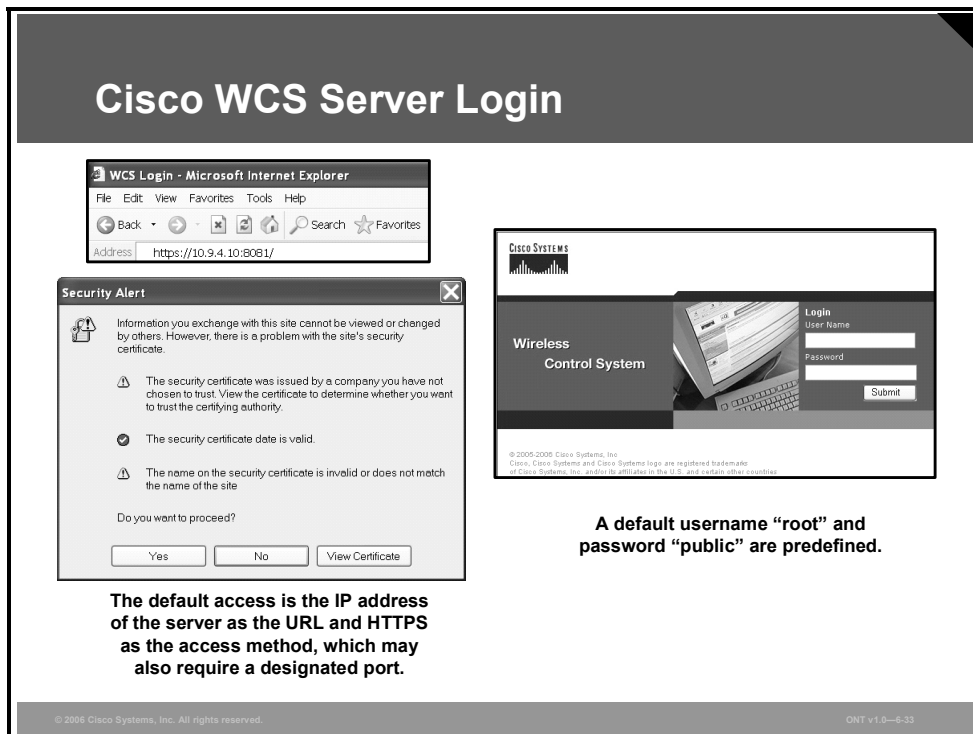
The Cisco Wireless Location Appliance can be deployed in a wide variety of environments and situations across multiple industries. Some of the primary usage scenarios include these:

- **Visibility and tracking of mobile devices by using Wi-Fi tags:** Operating and capital expenses can be reduced by preventing loss or theft of valuable mobile assets such as wheelchairs and infusion pumps in a healthcare environment and overhead projectors, laptops, and voice handsets in an enterprise. Individuals and assets can be quickly located anywhere within a wireless environment.
- **Work-flow automation and people tracking:** Inventory use and electronic work-flow and dispatch processes are optimized. In a retail environment, store layout and queue management can be optimized based on tracking customer shopping patterns. In amusement parks, children can be tracked, allowing parents to know where they are at all times, and security personnel can be tracked in any relevant facility.
- **Telemetry:** Wi-Fi tags with serial interfaces can be attached to a piece of equipment to relay important information about the device directly to business applications. For instance, car rental businesses often want telemetric information relating to mileage and fuel level of returned cars.

- **WLAN security and network control:** IT staff can rapidly locate security threats, such as rogue access points and rogue client devices. IT managers also can use the location appliance to establish a framework for location-based security, where the physical security in a building is used to control WLAN access, enhancing WLAN security.
- **RF capacity management and visibility:** Integrating location tracking into the WLAN allows IT staff to do more than just track users. With the Cisco Wireless Location Appliance, they can generate location-based trend reports and analyze the changes in traffic patterns, helping enable better real-time RF capacity management.

Cisco WCS Configuration Example

This topic describes basic Cisco WCS configuration. Authorized login is required to start the application, followed by several configuration steps, including adding devices to the system, adding maps of locations, and others.



The screenshot illustrates the Cisco WCS Server Login process. It shows a Microsoft Internet Explorer browser window with the address bar set to `https://10.9.4.10:8081/`. A security alert dialog box is displayed, warning that the site's security certificate is not trusted. The alert includes the following information:

- Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
- The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
- The security certificate date is valid.
- The name on the security certificate is invalid or does not match the name of the site.

The alert asks "Do you want to proceed?" with "Yes", "No", and "View Certificate" buttons. Below the alert, text states: "The default access is the IP address of the server as the URL and HTTPS as the access method, which may also require a designated port." To the right, the Cisco WCS Login page is shown, featuring a "Wireless Control System" header, a "Login" form with "User Name" and "Password" fields, and a "Submit" button. A note below the login page states: "A default username 'root' and password 'public' are predefined." The footer of the screenshot includes "© 2006 Cisco Systems, Inc. All rights reserved." and "ONT v1.0-6-33".

Cisco WCS Server Login

Complete these steps to log in to the Cisco WCS server:

Step 1 Launch Microsoft Internet Explorer version 6.0 or later.

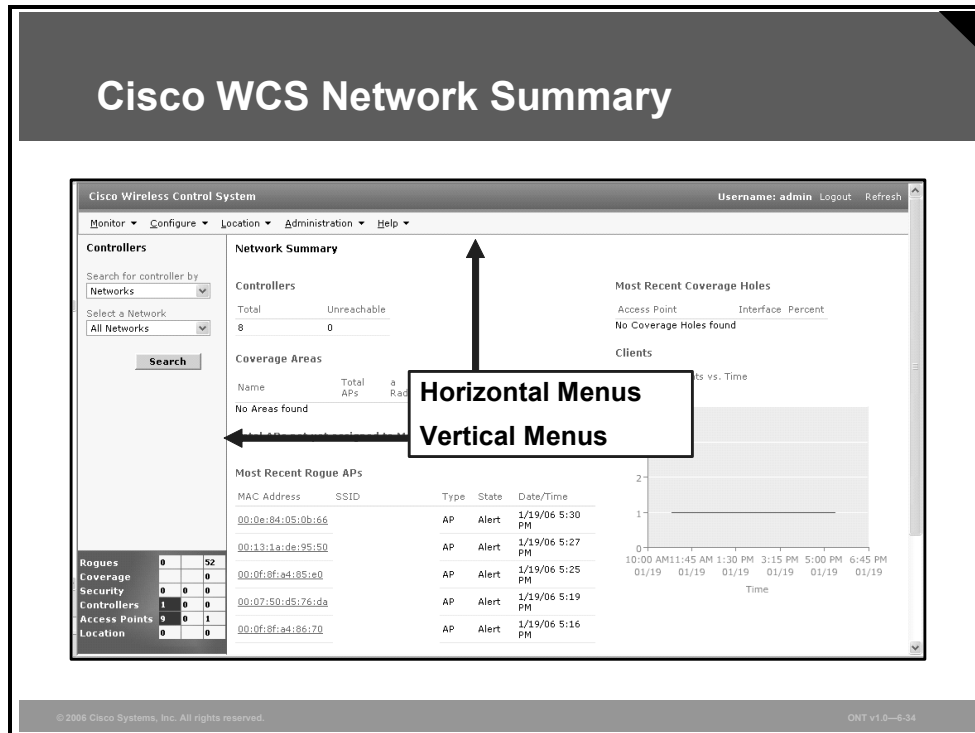
Note Some Cisco WCS features might not function properly if you use a web browser other than Internet Explorer 6.0 on a Windows workstation.

Step 2 In the browser address line, enter `https://localhost` when the Cisco WCS user interface is on a Cisco WCS server. Enter `https://wcs-ip-address` when the Cisco WCS interface is on any other workstation.

Step 3 The Cisco WCS user interface displays the Cisco WCS Login page. On the login page, enter your username and password. The default username is **root** and the default password is **public**.

Cisco WCS Network Summary

After successful login, Cisco WCS is ready to use. The Network Summary page is shown in the figure, from which the operator can start adding the devices and configuring the system.



The Cisco WCS user interface becomes active and available for use after login and displays the Network Summary (Network Dashboard) page, which provides a summary of the Cisco WLAN solution, including reported coverage holes, access point operational data, the most recently detected rogue access points, and client distribution over time.

There are both horizontal and vertical main menus and submenus. The figure displays the Network Summary page. The display is very similar to that of the Controller page.

When Cisco WCS receives alarm messages from the controller, the Cisco WCS user interface displays an alarm in an indicator in the lower-left corner area known as the Alarm Monitor. Alarms indicate the current fault or state of an element that needs attention. They are usually generated by one or more events. The alarms can be cleared, but the event remains. Alarm color codes are given in the table.

Alarm Color Codes

Color Code	Type of Alarm
Clear	No alarm
Red	Critical alarm
Orange	Major alarm
Yellow	Minor alarm

Adding a Cisco Wireless LAN Controller to Cisco WCS

This topic describes how to add and change Cisco Wireless LAN Controllers in the Cisco WCS database.

Adding a Controller

Cisco Wireless Control SystemUsername: admin Logout Refresh

Monitor > Configure > Location > Administration > Help >

Controllers

Search for controller by
Networks

Select a Network
All Networks

Search

Regues	0	50
Coverage		0
Security	0	0
Controllers	1	0
Access Points	0	0
Location	0	0

All Controllers

<input type="checkbox"/>	IP Address	Controller Name	Type	Location	Software Version		
<input type="checkbox"/>	10.9.4.20	C2	4400		3.2.78.0		
<input type="checkbox"/>	10.9.4.30	C3	4400		3.2.78.0		
<input type="checkbox"/>	10.9.4.40	C4	4400		3.2.78.0		
<input type="checkbox"/>	10.9.4.50	C5	4400		3.2.78.0		
<input type="checkbox"/>	10.9.4.60	C6	4400		3.2.78.0		
<input type="checkbox"/>	10.9.4.70	C7	4400		3.2.78.0	training7	Reachable
<input type="checkbox"/>	10.9.4.80	C8	4400		3.2.78.0	default	Reachable
<input type="checkbox"/>	10.9.4.90	Cisco_43:4c:03	4400		3.2.78.0	default	Reachable

Select a command -- GO

- Select a command --
- Add Controller...
- Remove Controllers
- Reboot Controllers
- Download Software..
- Download IDS Signatures
- Save Config to Flash
- Refresh Config from Controller
- View Audit Reports..

The Cisco WCS instance is initially empty and needs to be populated using the Select a command drop-down menu.

Cisco WCS has search criteria, such as networks, controller name, or IP address.

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0-4-35

When you know the IP address of controller service port or the controller name, follow these steps to add the controller to the Cisco WCS database:

Note It is recommended that you manage controllers through the controller dedicated service port for improved security. However, when you manage controllers on which the service port is disabled or when you manage a controller that does not have a service port (such as a Cisco 2000 Series Wireless LAN Controller), you must use the controller management interface.

- Step 1** Log in to the Cisco WCS user interface.
- Step 2** Choose **Configure > Controllers** to display the All Controllers page.
- Step 3** From the Select a Command drop-down menu, choose **Add Controller** and click **Go** to display the Add Controller page.
- Step 4** Enter the controller IP address, network mask, and required SNMP settings in the Add Controller fields.

6-112 Optimizing Converged Cisco Networks (ONT) v1.0

© 2006 Cisco Systems, Inc.

The PDF files and any printed representation for this material are the property of Cisco Systems, Inc., for the sole use by Cisco employees for personal study. The files or printed representations may not be used in commercial training, and may not be distributed for purposes other than individual study.

Configure > Controller > Add Controller > Go

Cisco Wireless Control System

Monitor > Configure > Location > Administration > Help >

Controllers

Search for controller by
Networks
Select a Network
All Networks
Search

Add Controller

IP Address: 10.9.4.90
Network Mask: 255.255.255.0

SNMP Parameters*

Version: v2c
Retries: 3
Timeout (seconds): 4
Community: private

OK Cancel

* Please enter SNMP parameters for the write access if you have one. If you enter read-only access parameters then controller will be added but WCS will be unable to modify configuration.

IP Address	Type	Status
10.9.4.90	Controller	Added successfully to WCS

Add Controller

© 2006 Cisco Systems, Inc. All rights reserved. OMT v1.0—8-36

Step 5 Click **OK**. Cisco WCS displays the Please Wait dialog box while it contacts the controller, adds the current controller configuration to the Cisco WCS database, and then displays the Add Controller page again.

If Cisco WCS does not find a controller at the IP address that you entered for the controller, the Discovery Status dialog displays this message: “No response from device, check SNMP.” Check these settings to correct the problem:

- The controller service port IP address might be set incorrectly. Check the service port setting on the controller.
- Cisco WCS might not have been able to contact the controller. Make sure that you can ping the controller from the Cisco WCS server.
- The SNMP settings on the controller might not match the SNMP settings that you entered in Cisco WCS. Make sure that the SNMP settings configured on the controller match the settings that you enter in Cisco WCS.

Add additional controllers using the Add Controller page, or choose the Configure tab to display the All Controllers page.

Configuring a Cisco Access Point

Access points that are associated to Cisco Wireless LAN Controllers are automatically added to Cisco WCS.

Configure > Access Points

Cisco Wireless Control SystemUsername: admin Logout Refresh

Monitor Configure Location Administration Help

Access Points

Search for APs by
Unassigned APs

Select Radio Type
All Radios

Search

Rogues	0	50
Coverage	0	0
Security	0	0
Controllers	0	0
Access Points	9	1
Location	0	0

All Access Points

-- Select a command --

<input type="checkbox"/>	AP Name ▲	Ethernet MAC	Radio	Map Location	Controller	Oper Status	Alarm Status
<input type="checkbox"/>	ap:Sf-4b:b0	00:0b:85:5f:4b:b0	802.11a	Unassigned	10.9.4.20	Up	●
<input type="checkbox"/>	ap:Sf-4b:b0	00:0b:85:5f:4b:b0	802.11b/g	Unassigned	10.9.4.20	Up	●
<input type="checkbox"/>	ap:Sf-50:20	00:0b:85:5f:50:20	802.11a	Unassigned	10.9.4.50	Up	●
<input type="checkbox"/>	ap:Sf-50:20	00:0b:85:5f:50:20	802.11b/g	Unassigned	10.9.4.50	Up	●
<input type="checkbox"/>	ap:Sf-50:e0	00:0b:85:5f:50:e0	802.11a	Unassigned	10.9.4.80	Up	●
<input type="checkbox"/>	ap:Sf-50:e0	00:0b:85:5f:50:e0	802.11b/g	Unassigned	10.9.4.80	Up	●
<input type="checkbox"/>	ap:Sf-51:00	00:0b:85:5f:51:00	802.11a	Unassigned	10.9.4.60	Up	●
<input type="checkbox"/>	ap:Sf-51:00	00:0b:85:5f:51:00	802.11b/g	Unassigned	10.9.4.60	Up	●

After adding a controller, associated access points are automatically added.

© 2006 Cisco Systems, Inc. All rights reserved.ONT v1.0-4-37

To view all access points, choose **Configure > Access Points**.

This page allows you to view a summary of all Cisco lightweight access points in the Cisco WCS database. It also allows you to add third-party access points, and remove selected Cisco lightweight access points.

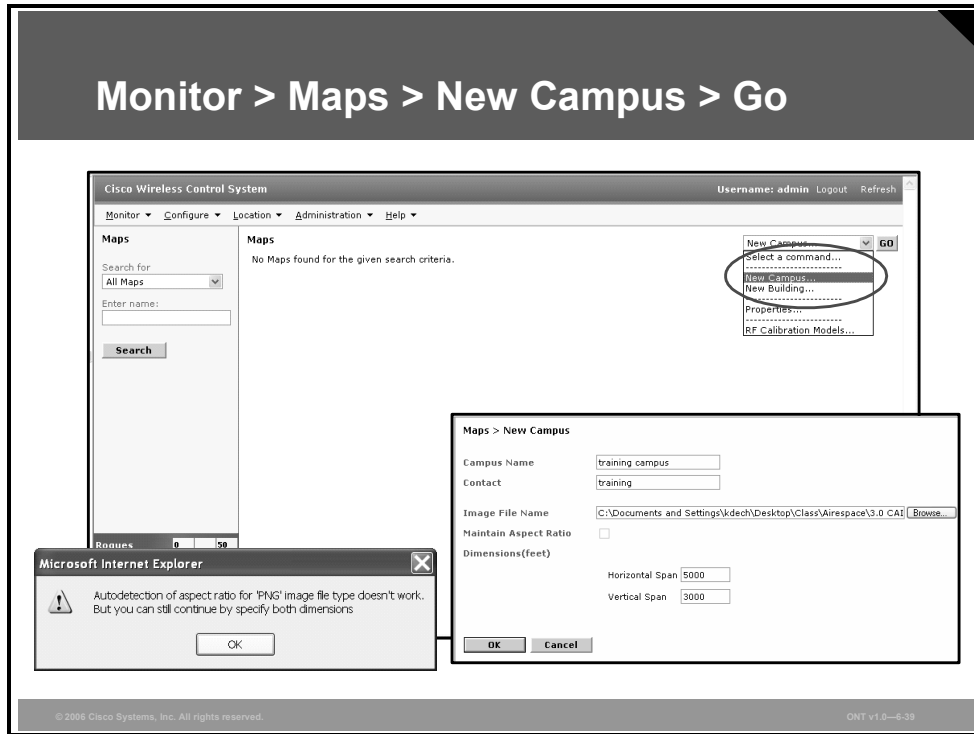
Note There is no need to add Cisco lightweight access points to the Cisco WCS database. The operating system software automatically adds Cisco lightweight access points as they associate with existing Cisco Wireless LAN Controllers in the Cisco WCS database.

The following information is displayed:

- Access point name
- Radio type
- Map location
- Controller
- Port
- Operational status
- Alarm status

Cisco WCS Maps

This topic describes how to add, change, and use maps in the Cisco WCS database.



Adding a Campus Map to the Cisco WCS Database

When you add maps to Cisco WCS, you can view your managed system on realistic campus, building, and floor plan maps. Complete these steps to add a single campus map to the Cisco WCS database:

- Step 1** Save the map in .png, .jpg, .jpeg, or .gif format. The map can be any size because Cisco WCS automatically resizes the map to fit its working areas.
- Step 2** Browse to the map and import it from anywhere in your file system.
- Step 3** Choose the **Monitor** tab.
- Step 4** Choose **Maps** to display the Maps page.
- Step 5** From the Select a Command drop-down menu, choose **New Campus** and click **Go** to display the New Campus page.

Monitor > Maps > New Campus > Go (Cont.)

Maps

Name	Type	Status
training	Campus	●
training1	Building	●

- **Maps can start at either a campus or building, but only a campus will provide an outdoor coverage area.**
- **A building can be added as a single entity or as part of a campus.**

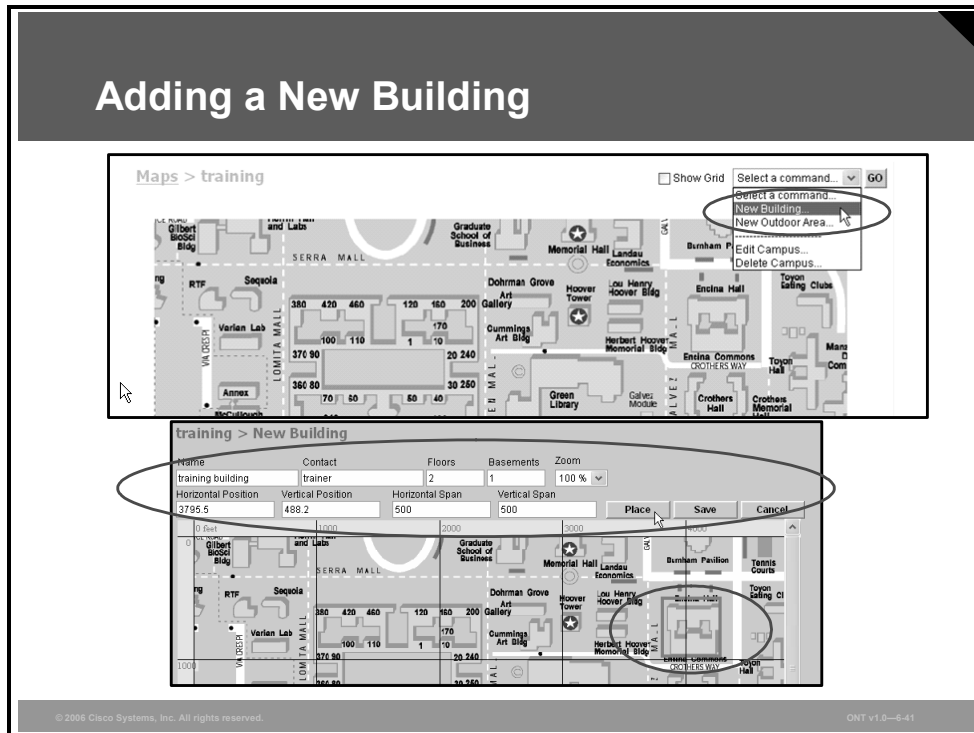
© 2006 Cisco Systems, Inc. All rights reserved.

ONT v1.0-6-40

- Step 6** On the New Campus page, enter the campus name and campus contact information.
- Step 7** Choose **Browse** to search for and select the campus graphic name.
- Step 8** Choose **Maintain Aspect Ratio** to prevent length and width distortion when Cisco WCS resizes the map.
- Step 9** Enter the horizontal span and the vertical span of the map in feet. The campus horizontal span and vertical span should be larger than any building or floor plan to be added to the campus.
- Step 10** Click **OK** to add the campus map to the Cisco WCS database. Cisco WCS displays the Maps page, which lists maps in the database, map types, and campus status.

Adding New Building to the Cisco WCS Database

You can add buildings to the Cisco WCS database whether or not you have added maps or campuses to the database.



Follow these steps to add a building to a campus in the Cisco WCS database:

- Step 1** Choose the **Monitor** tab.
- Step 2** Choose **Maps** to display the Maps page.
- Step 3** Choose the desired campus. Cisco WCS displays the Campus page.
- Step 4** From the Select a Command drop-down menu, choose **New Building** and click **Go** to display the New Building page.
- Step 5** On the New Building page, follow these steps to create a virtual building to organize related floor plan maps:
 1. Enter the building name.
 2. Enter the building contact name.
 3. Enter the number of floors and basements.
 4. Enter an approximate building horizontal span and vertical span (width and depth on the map) in feet. These numbers should be as large as or larger than any floors that you might add later.

Tip You can also press Ctrl-Left-Select to resize the bounding area in the upper left corner of the campus map. As you change the size of the bounding area, the Building Horizontal Span and Vertical Span parameters vary to match your changes.

- Step 6** Choose **Place** to put the building on the campus map. Cisco WCS creates a building rectangle scaled to the size of the campus map.

- Step 7** Select the building rectangle and drag it to the desired position on the campus map.
- Step 8** Choose **Save** to save the building definition and its campus location in the database. Cisco WCS saves the building name in the building rectangle on the campus map. Note that there will be a hyperlink associated with the building that takes you to the corresponding Maps page.

Rogue Access Point Detection

This topic describes Cisco WCS rogue access point methodology.

Detecting and Locating Rogue Access Points

- An alarm indicator appears in Cisco WCS showing 51 rogue access points detected.
- Select the alarm for more information.

Rogues	0		51
Coverage			0
Security	0	0	0
Controllers	0	0	0
Access Points	9	0	0
Location	0		0

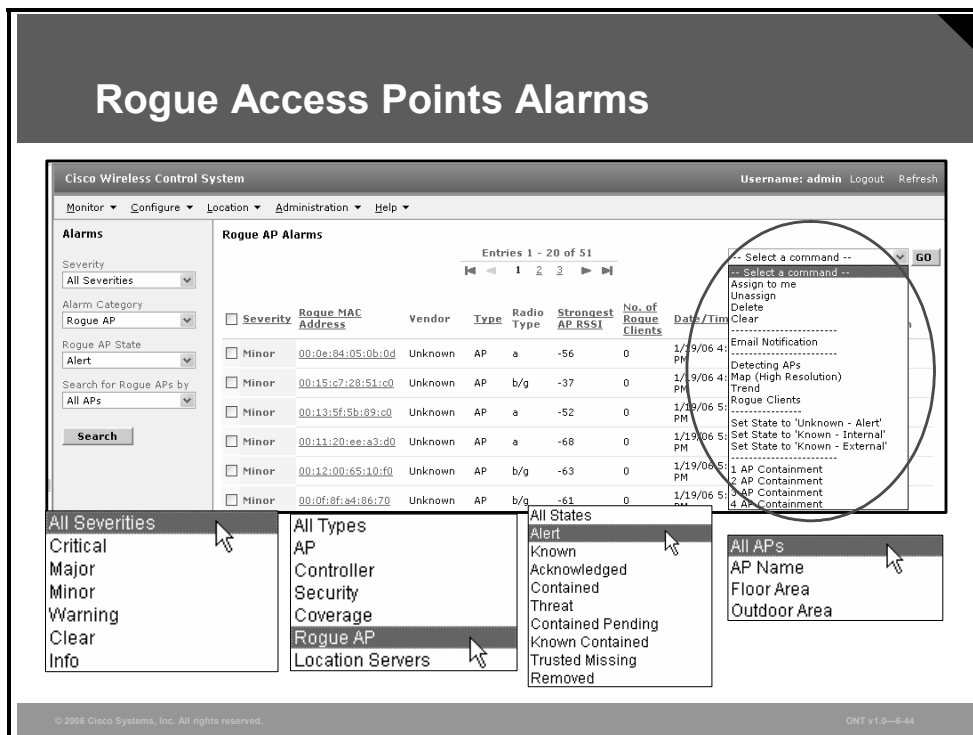
© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0—6-43

When the lightweight access points on your WLAN are powered up and associated with controllers, Cisco WCS immediately starts listening for rogue access points. When Cisco Wireless LAN Controller detects a rogue access point, it immediately notifies Cisco WCS, which creates a rogue access point alarm. When Cisco WCS receives a rogue access point message from Cisco Wireless LAN Controller, an alarm indicator appears in the lower-left corner of all Cisco WCS user interface pages.

Select the indicator to display the Rogue AP Alarms page.

Rogue Access Point Alarms

The Rogue AP Alarms page lists the severity of the alarms, the rogue access point MAC addresses, the rogue access point types, the owners (Cisco WCS operators), the date and time when the rogue access points were first detected, the channel numbers they are broadcasting on, and their service set identifiers (SSIDs).

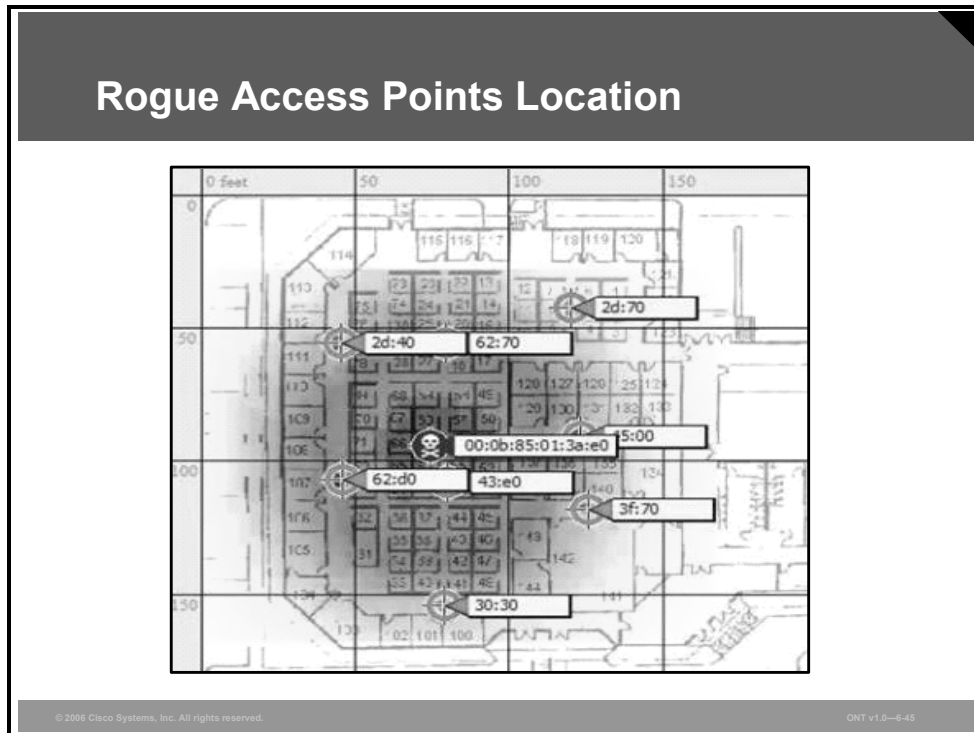


On this page, you can highlight one or more entries by checking the desired check boxes and choosing one of the following commands from the Select a Command drop-down menu to apply it all selected rogue access point alarms: Assign to Me, Unassign, Delete, Clear, or Email Notification.

To see more rogue access point information, click any link in the Rogue MAC Address column to display the associated Alarms > Rogue AP MAC Address page.

Rogue Access Point Location

On the Rogue AP MAC Address page, choose **Map** to display the currently calculated rogue access point location on the Maps > Building Name > Floor Name page.



If you are using Cisco WCS Location, Cisco WCS compares the RSSI signal strength from two or more access points to find the most probable location of the rogue access point and places a small skull-and-crossbones indicator at the most likely location. Cisco WCS Base (without the Location option) relies on RSSI signal strength from the rogue access point and places a small skull-and-crossbones indicator next to the access point receiving the strongest RSSI signal from the rogue unit.

Acknowledging Rogue Access Points

To acknowledge known rogue access points, navigate to the Rogue AP Alarms page. Right-click the rogue access point (red, unknown) to be acknowledged, and choose **Set State to 'Known Internal'** or **Set State to 'Known External.'** In either case, Cisco WCS removes the red rogue access point entry from the Alarms page.

Summary

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

Summary

- **The main components of the Cisco Unified Wireless Network are client devices, the mobility platform, network unification, network management, and unified advanced services.**
- **Cisco offers two WLAN implementations: an autonomous and a lightweight WLAN solution.**
- **Autonomous access points are configured per access point, while lightweight access points are configured via the WLAN controller.**
- **CiscoWorks WLSE is a server that supports centralized configuration, firmware, and radio management.**
- **Cisco WCS is a Cisco WLAN solution network management tool used for WLAN planning, configuration, and management.**
- **Three Cisco WCS tracking options are available: WCS Base, WCS Location, and WCS Location and Cisco 2700 Series Wireless Location Appliance.**

© 2006 Cisco Systems, Inc. All rights reserved. ONT v1.0-4-46

References

For additional information, refer to these resources:

- Cisco Systems, Inc. *User Guide for the CiscoWorks WLSE and WLSE Express, 2.12*, at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_12/index.htm.
- Cisco Systems, Inc. CiscoWorks Wireless LAN Solution Engine (WLSE) Express page at <http://www.cisco.com/en/US/products/ps6379/index.html>.
- Cisco Systems, Inc. *Cisco 2700 Series Location Appliance Installation and Configuration Guide* at http://www.cisco.com/en/US/products/ps6386/prod_installation_guides_list.html.

Module Summary

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

Module Summary

- **Video and voice applications are used with wireless clients as well as wired clients and QoS is required for them.**
- **EAP support to 802.1x is designed to allow additional authentication methods to be deployed with no changes to the access point or client NIC.**
- **Improved security can use WPA or WPA2 using preshared keys or dynamic 802.1x.**
- **The Cisco Unified Wireless Network is composed of five interconnected elements: client devices, the mobility platform, network unification, world-class network management, and unified advanced services.**

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) Can the best-effort WMM access category be prioritized above or below background WMM access category? (Source: Implementing WLAN QoS)
- A) above
 - B) below
 - C) both
- Q2) Which encryption method is supported in WPA2? (Source: Introducing 802.1x)
- A) TKIP
 - B) WEP
 - C) AES
 - D) WEP2
- Q3) What is authentication used for? (Source: Introducing 802.1x)
- A) Authentication proves that you belong on the network.
 - B) Authentication provides encryption keys after encryption.
 - C) Authentication is used to dynamically generate keys.
 - D) Authentication is using the RC4 or 128-bit block cipher algorithm.
- Q4) Which is not an advantage of 802.11? (Source: Introducing 802.1x)
- A) mutual authentication
 - B) dynamically derived keys
 - C) session-based keys
 - D) centralized user and key management
 - E) device-based authentication
- Q5) Which two formats can the static WEP encryption key be specified in? (Choose two.) (Source: Configuring Encryption and Authentication on Lightweight Access Points)
- F) ASCII
 - G) BIN
 - H) DEC
 - I) HEX
 - J) text
- Q6) Which statement about CiscoWorks WLSE is false? (Source: Managing WLANs)
- A) CiscoWorks WLSE is a solution for managing the entire Cisco Aironet WLAN infrastructure.
 - B) CiscoWorks WLSE allows you to apply configuration changes to access points.
 - C) CiscoWorks WLSE configuration is done via the CLI.
 - D) CiscoWorks WLSE includes WLAN intrusion detection.
- Q7) Which two are versions of Cisco WCS? (Choose two.) (Source: Managing WLANs)
- A) Base
 - B) Extended
 - C) Location
 - D) Advanced
 - E) Lightweight

Module Self-Check Answer Key

- Q1) C
- Q2) C
- Q3) A
- Q4) E
- Q5) A, D
- Q6) C
- Q7) A, C

