

CIPT2

Cisco IP Telephony Part 2

Volumes 1 & 2

Version 4.1

Student Guide

CLS Production Services: 09.20.05

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco 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



Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCSP, 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, ASIST, 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, Empowering the Internet Generation, 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, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO 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. (0501R)

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 1

<i>Course Introduction</i>	1
Overview	1
Learner Skills and Knowledge	1
Course Goal and Objectives	2
Course Flow	3
Additional References	4
Cisco Glossary of Terms	5
Your Training Curriculum	6
<i>Securing IP Telephony</i>	1-1
Overview	1-1
Module Objectives	1-1
<i>Securing the Windows Operating System</i>	1-3
Overview	1-3
Objectives	1-3
Threats Targeting the Operating System	1-4
Security and Hotfix Policy	1-9
Operating System Hardening	1-11
Antivirus Protection	1-17
Cisco Security Agent	1-19
Administrator Password Policy	1-27
Common Windows Exploits	1-32
Security Taboos	1-35
Summary	1-40
<i>Securing Cisco CallManager Administration</i>	1-41
Overview	1-41
Objectives	1-41
Threats Targeting Remote Administration	1-42
HTTPS Overview	1-43
HTTPS Certificate Operations	1-45
MLA Overview	1-50
Enabling MLA	1-53
MLA Functional Groups	1-55
MLA User Groups	1-57
Creating a New Functional Group and User Group	1-62
Summary	1-69
<i>Preventing Toll Fraud</i>	1-71
Overview	1-71
Objectives	1-71
Toll-Fraud Exploits	1-72
Restricting Call Forward All and Voice Mail Using Calling Search Spaces	1-74
Blocking Commonly Exploited Area Codes	1-81
Example	1-82
Using Time-of-Day Routing	1-83
Examples	1-88
Example	1-91
Using FAC	1-93
Restricting External Transfers	1-103
Gateways and Trunks	1-105
Route Patterns	1-106
Example 1	1-111
Example 2	1-111
Example 3	1-111

Dropping Conference Calls	1-114
Summary	1-117
Hardening the IP Phone	1-119
Overview	1-119
Objectives	1-119
Threats Targeting Endpoints	1-120
Stopping Rogue Images from Infiltrating Phones	1-123
Disabling Phone Settings in Cisco CallManager Administration	1-125
Disabling the PC Port, the Settings Button, and Web Access to the IP Phone	1-126
Ignoring Gratuitous ARP	1-128
Blocking PC Access to the Voice VLAN	1-130
Authentication and Encryption in Cisco CallManager Administration and IP Phones	1-132
Summary	1-133
Understanding Cryptographic Fundamentals	1-135
Overview	1-135
Objectives	1-135
What Is Cryptography?	1-136
Symmetric Encryption	1-141
AES History	1-143
AES versus 3DES	1-143
AES in IP Telephony	1-144
Asymmetric Encryption	1-145
RSA History	1-147
RSA Applications	1-147
RSA in IP Telephony	1-147
Hash Functions	1-148
The SHA-1 Algorithm	1-149
Digital Signatures	1-152
Summary	1-155
Understanding PKI	1-157
Overview	1-157
Objectives	1-157
The Need for a PKI	1-158
Manual Key Exchange	1-159
Automated Key Exchange	1-159
PKI as a Trusted Third-Party Protocol	1-162
PKI Entities	1-169
CA Examples	1-170
End Entities and Self-Signed Certificates	1-172
PKI Enrollment	1-173
PKI Revocation and Key Storage	1-177
Example	1-180
PKI Examples	1-181
Summary	1-188
Understanding Cisco IP Telephony Authentication and Encryption Fundamentals	1-189
Overview	1-189
Objectives	1-189
Threats Targeting the IP Telephony System	1-190
How a Cisco IP Telephony Network Protects Against Threats	1-192
PKI Topologies in Cisco IP Telephony	1-200
PKI Enrollment in Cisco IP Telephony	1-211
Keys and Certificate Storage in Cisco IP Telephony	1-214
Authentication and Integrity	1-215
Encryption	1-221
Summary	1-228

Configuring Cisco IP Telephony Authentication and Encryption	1-229
Overview	1-229
Objectives	1-229
Authentication and Encryption Configuration Overview	1-230
Enabling Services Required for Security	1-233
Installing the Cisco CTL Client	1-234
Using the Cisco CTL Client	1-236
Working with LSCs	1-238
Configuring the Device Security Mode	1-245
Generating a CAPF Report	1-247
Finding IP Phones with Security Features	1-249
Summary	1-251
Module Summary	1-253
References	1-254
Module 1 Self-Check	1-256
Module 1 Self-Check Answer Key	1-267

Volume 2

<i>Enabling IP Video Telephony</i>	2-1
Overview	2-1
Module Objectives	2-1
<i>Introducing IP Video Telephony</i>	2-3
Overview	2-3
Objectives	2-3
IP Video Telephony Solution Components	2-4
Video Calls	2-8
Example	2-10
Video Protocols Supported in Cisco CallManager	2-13
Bandwidth Management	2-21
The Media Channels of a Video Call	2-22
Example	2-23
Actual Bandwidth Used Per Video Call	2-24
Call Admission Control Within a Cluster	2-27
Call Admission Control Between Clusters	2-34
Summary	2-39
<i>Configuring Cisco VT Advantage</i>	2-41
Overview	2-41
Objectives	2-41
Cisco VT Advantage Overview	2-42
How Calls Work with Cisco VT Advantage	2-48
Configuring Cisco CallManager for Video	2-51
Configuring Cisco IP Phones for Cisco VT Advantage	2-59
Installing Cisco VT Advantage	2-65
Cisco IP Phone	2-67
PC Hardware Requirements	2-67
Cisco VT Camera	2-68
PC Feature Requirements	2-69
Cisco VT Advantage Software	2-69
Low Frame Rate Example	2-75
Summary	2-76
Module Summary	2-77
References	2-77
Module 2 Self-Check	2-79
Module 2 Self-Check Answer Key	2-81

Monitoring and Managing IP Telephony	3-1
Overview	3-1
Module Objectives	3-1
Introducing Database Tools and Cisco CallManager Serviceability	3-3
Overview	3-3
Objectives	3-3
Database Management Tools	3-4
Cisco CallManager Serviceability Overview	3-11
Alarm	3-12
Trace	3-13
Tools	3-13
Application	3-13
Help	3-14
Control Center	3-15
Service Activation	3-18
Tools Overview	3-22
Summary	3-25
Monitoring Performance	3-27
Overview	3-27
Objectives	3-27
Performance Counters and Objects	3-28
Microsoft Event Viewer	3-30
Log Types	3-31
Event Types	3-31
Microsoft Performance Monitor	3-32
Graphs	3-34
Histograms	3-34
Real-Time Monitoring Tool Overview	3-36
Menu Bar	3-37
Controlling Center Pane	3-37
Viewing Pane	3-38
Tab Bar	3-38
Real-Time Monitoring Configuration Profiles	3-39
Real-Time Monitoring Tool Window	3-41
Summary	3-45
Configuring Alarms and Traces	3-47
Overview	3-47
Objectives	3-47
Alarm Overview	3-48
Alarm Configuration	3-51
Trace Configuration	3-55
SDI Trace	3-56
SDL Trace	3-56
Trace Analysis	3-61
Trace Collection	3-65
Downloading and Compressing Trace Files	3-67
Bulk Trace Analysis	3-69
Trace Tools	3-72
Q.931 Translator	3-73
Voice Log Translator	3-73
Dick Tracy	3-73
Ethereal	3-73
Summary	3-74
Configuring CAR	3-75
Overview	3-75
Objectives	3-75

CAR Overview	3-76
CDRs and CMRs	3-77
CAR Users	3-79
CAR Report Types and User Levels	3-80
CAR System Parameter Configuration	3-82
Report Scheduling	3-87
System Database Configuration	3-90
User Report Configuration	3-93
Summary	3-96
Using Additional Management and Monitoring Tools	3-97
Overview	3-97
Objectives	3-97
Remote Management Tools	3-98
SNMP Basics	3-102
Dependency Records	3-110
Example	3-110
Dependency Records Buttons	3-113
Password Changer Tool	3-114
Cisco Dialed Number Analyzer	3-118
Quality Report Tool	3-127
Summary	3-133
Module Summary	3-134
References	3-134
Module 3 Self-Check	3-135
Module 3 Self-Check Answer Key	3-141

Course Introduction

Overview

Cisco IP Telephony Part 2 (CIPT2) v4.1 is designed to provide learners with the necessary knowledge and skills to enable video calls and to secure, monitor, and manage a Cisco IP telephony solution based on Cisco CallManager, the call-routing and signaling component of the Cisco IP telephony solution.

Learner Skills and Knowledge

This subtopic lists the skills and knowledge that learners must possess to benefit fully from the course. The subtopic also includes recommended Cisco learning offerings that learners should complete in order to benefit fully from this course.

Learner Skills and Knowledge

Cisco.com

- *Cisco IP Telephony Part 1 (CIPT1)*:
 - Working knowledge of Cisco CallManager functions; role Cisco CallManager plays in Cisco AVVID strategy; SQL publisher and subscriber relationship
 - Ability to configure Cisco CallManager to add and configure users, devices (phones, gateways, trunks), media resources, and applications
 - Ability to configure dial plans and features in Cisco CallManager
- *Interconnecting Cisco Network Devices (ICND)*; Cisco CCNA® certification recommended prerequisite; *Building Cisco Multilayer Switched Networks (BCMSN)*:
 - Working knowledge of fundamental terms and concepts of computer networking to include LANs, WANs, and IP switching and routing
 - Ability to configure and operate Cisco routers and switches and to enable VLANs and DHCP
- *Cisco Voice over IP (CVOICE)*:
 - Fundamental knowledge of converged voice and data networks
 - Ability to configure voice interfaces on Cisco voice-enabled equipment for connection to traditional, nonpacketized telephony equipment and to configure the call flows for POTS and VoIP dial peers

© 2005 Cisco Systems, Inc. All rights reserved. CIPT2 v4.1-3

Course Goal and Objectives

This topic describes the course goal and objectives.

Course Goal

Cisco.com

“To provide learners with the necessary knowledge and skills to enable video calls and to secure, monitor, and manage a Cisco IP telephony solution based on Cisco CallManager, the call-routing and signaling component of the Cisco IP telephony solution”

Cisco IP Telephony Part 2

© 2005 Cisco Systems, Inc. All rights reserved. CIPT2 v4.1—4

Upon completing this course, you will be able to meet these objectives:

- Harden Cisco IP telephony devices, prevent toll fraud, understand cryptographic concepts, and apply cryptography to your Cisco IP telephony system
- Make IP video telephony calls with Cisco VT Advantage and describe the basic components and characteristics of video calls and Cisco CallManager configuration parameters that enable video
- Classify and use system maintenance tools that can be used in a Cisco CallManager environment

Course Flow

This topic presents the suggested flow of the course materials.

Course Flow			
<small>Cisco.com</small>			
	Day 1	Day 2	Day 3
A M	Course Introduction	Securing IP Telephony	Monitoring and Managing IP Telephony
	Securing IP Telephony		
Lunch			
P M	Securing IP Telephony	Securing IP Telephony	Monitoring and Managing IP Telephony
		Enabling IP Video Telephony	Wrap-Up
<small>© 2005 Cisco Systems, Inc. All rights reserved. CPT2 v4.1-3</small>			















The schedule reflects the recommended structure for this course. This structure allows enough time for the instructor to present the course information and for you to work through the lab activities. The exact timing of the subject materials and labs depends on the pace of your specific class.

Additional References

This topic presents the Cisco icons and symbols used in this course, as well as information on where to find additional technical references.

Cisco Icons and Symbols


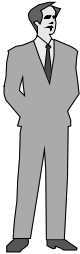




Cisco.com

	Router		Cisco CallManager		File Server
	Voice Router		Camera PC/Video		Network Cloud
	SRST-Enabled Router		Phone		PC
	Switch Router		IP Phone		Laptop
	Switch		Gateway		

© 2005 Cisco Systems, Inc. All rights reserved.
CIPT2 v4.1—6

Cisco Icons and Symbols (Cont.)

Cisco.com

	Government		IP Telephony and PKI User		IP Telephony and PKI User
	Building				
	End User				
			Key		

© 2005 Cisco Systems, Inc. All rights reserved.
CIPT2 v4.1—7

Cisco Glossary of Terms

For additional information on Cisco terminology, refer to the *Cisco Internetworking Terms and Acronyms* glossary of terms at <http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm>.

Your Training Curriculum

This topic presents the training curriculum for this course.

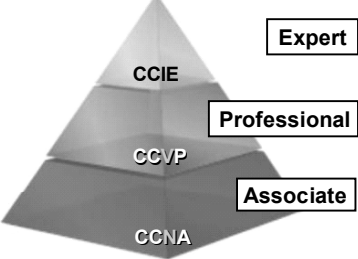
Cisco Voice Career Certifications

Cisco.com

**Expand Your Professional Options
and Advance Your Career**

Cisco Voice Career Certifications

Professional-level recognition in Cisco Voice Career Certifications



Required Exam	Recommended Training Through Cisco Learning Partners
<Insert exam number(s)>	<Insert course title(s)>
<Insert exam number(s)>	<Insert course title(s)>
<Insert exam number(s)>	<Insert course title(s)>
<Insert exam number(s)>	<Insert course title(s)>

<http://www.cisco.com/go/certifications>

© 2005 Cisco Systems, Inc. All rights reserved.
CIPT2 v4.1-8

You are encouraged to join the Cisco Certification Community, a discussion forum open to anyone holding a valid Cisco Career Certification (such as Cisco CCIE[®], CCNA[®], CCDA[®], CCNP[®], CCDP[®], CCIP[™], or CCSP[®]). It provides a gathering place for Cisco-certified professionals to share questions, suggestions, and information about Cisco Career Certification programs and other certification-related topics. For more information, visit http://www.cisco.com/en/US/learning/le3/le2/le41/learning_certification_level_home.html.

Module 1

Securing IP Telephony

Overview

This module deals with various aspects of secure telephony, including the telephony servers, the phones, and the communication among all of them.

Module Objectives

Upon completing this module, you will be able to harden Cisco IP telephony devices, prevent toll fraud, understand cryptographic concepts, and apply cryptography to your Cisco IP telephony system. This ability includes being able to meet these objectives:

- Identify best practices to further harden the Cisco IP telephony operating system on which Cisco CallManager runs
- Secure Cisco CallManager Administration
- Prevent toll fraud
- Harden the Cisco IP Phone
- Define fundamentals of cryptography and describe how they are applied to provide various services
- Describe the concept of PKI, describe what certificates are and how they are issued, and explain how PKI can secure applications
- Explain what cryptographic services are available in a Cisco IP telephony environment and how a PKI is used to provide these services
- Configure a Cisco CallManager cluster for secure operation

Lesson 1-1

Securing the Windows Operating System

Overview

The telephony system is a business-critical, system, 24 hours a day, seven days a week, to all companies. Such critical environments must be as secure as possible to avoid breakdowns related to failures in the system or attacks involving the network. The Microsoft Windows 2000 Server Operating System is the base of Cisco CallManager. This lesson discusses options for hardening and securing the Cisco CallManager operating system and gives students an overview of possible vulnerabilities and of practices for tightening security in the Cisco IP Telephony Operating System.

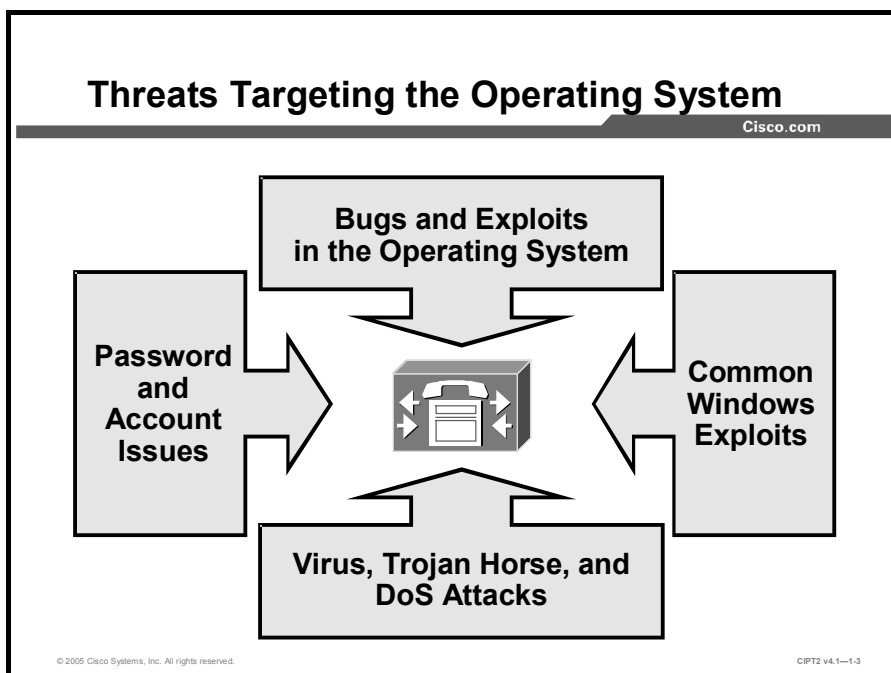
Objectives

Upon completing this lesson, you will be able to identify best practices to further harden the Cisco IP Telephony Operating System on which Cisco CallManager runs. This ability includes being able to meet these objectives:

- Identify security threats to the Windows operating system
- Explain the Cisco security and hotfix policy for keeping the operating system up to date
- Explain how the optional operating system security script and manual security settings provide more stringent security controls to the hardened Windows operating system
- Identify the anti-virus protection software that is approved for use on a Cisco CallManager server
- Explain the features and functions of Cisco Security Agent as they relate to securing Cisco CallManager
- Define and administer a password policy for the administrator password
- Explain how to protect Windows against the most common exploits
- Explain common security practices and settings that are not recommended on Cisco CallManager

Threats Targeting the Operating System

This topic describes security threats targeting the Windows operating system.



When you are securing an operating system, several threats should be considered.

Bugs in the operating system, as well as in the services and applications that come with the operating system, can pose severe security threats. Because the operating system serves as a basis for applications, even well-written and secure applications can be affected by vulnerabilities in the underlying operating system. Built-in networking services and applications are especially sensitive because they are exposed to remote attacks. That vulnerability also applies to the IP stack in the Windows operating system. The IP stack has a strategic importance and unfortunately also a long tradition of more and less severe security issues that result not only from the particular implementation of the IP protocol, but also from the protocol itself, which lacks any security mechanisms.

Insecure settings are another problem of operating systems. Attacks can target both of the following:

- Password and account policies
- Insecure Windows configuration settings

Microsoft Windows, as the most popular operating system, is well known to the public. As a result, there are many known issues related to its password policies as well as vulnerabilities in the operating system default settings. An attacker may just try to log in to the operating system using the Administrator account and commonly used passwords. In Microsoft networking, for instance, "simple file shares" can be used (and had been turned on by default in some versions of Windows), allowing access to file shares without any security checking.

Another threat to the system is malicious code execution by viruses, worms, or Trojan horses. Protection against these threats consists of blocking the threats from the system and detecting and eliminating attacks that were not blocked.

Finally and extremely important for servers—operating systems are vulnerable to denial of service (DoS) attacks. If the server operating system cannot resist DoS attacks, an attacker can tear down the whole IP telephony infrastructure with a single, focused attack against key servers, such as Cisco CallManager nodes. Besides other methods (separating the server network from other parts of the network and establishing access control), the server itself should be hardened to resist at least simple and common DoS attacks.

Lowering the Threats in Windows Operating System

Cisco.com

Reduce or eliminate vulnerabilities by:

- **Hardening the Windows operating system with Cisco operating system upgrades**
- **Apply Cisco security and hotfix policies**
- **Securing Windows password policies**
- **Deploying secure Windows password policies**
- **Using protection against attacks from the network:**
 - **Antivirus software**
 - **Cisco Security Agent**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1.4

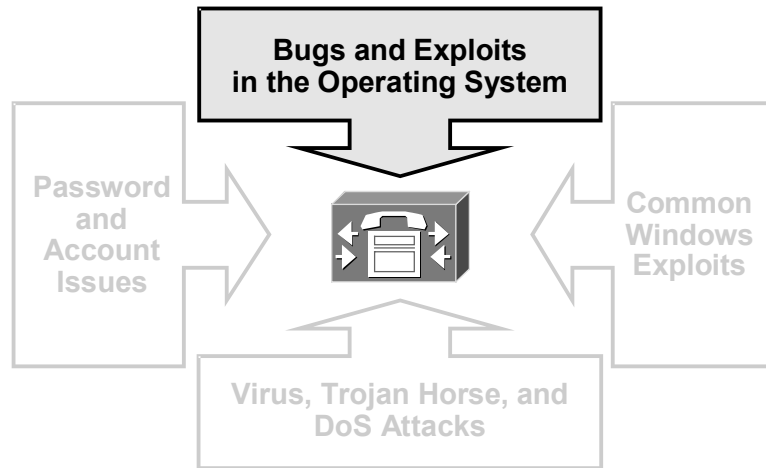
The possible countermeasures against attacks to the operating system itself can be divided into measures that eliminate vulnerabilities to certain threats and methods to protect the system against attacks exploiting the remaining vulnerabilities.

The following are practices to reduce possible vulnerabilities:

- Harden the Windows operating system with Cisco operating system upgrades.
- Deploy the Cisco security and hotfix policy.
- Implement a secure Windows password policy.
- Protect against common exploits involving Windows.
- Protect against attacks from the network by using the following:
 - Antivirus software
 - Cisco Security Agent

Cisco IP Telephony Operating System

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-1-6

To protect against bugs and exploits involving Microsoft Windows, Cisco provides an already hardened version of the Windows operating system called Cisco IP Telephony Operating System. Windows 2000 Server has to be kept up to date to secure the operating system against new security holes. For that reason, Cisco provides operating system upgrades and hotfixes. Cisco CallManager and other Cisco IP telephony applications require these upgrades to function properly.

Cisco IP Telephony Operating System Upgrades

Cisco.com

- **Cisco IP Telephony Operating System is a hardened version of Windows 2000 Server used by several Cisco IP Telephony server components.**
- **Cisco increases security by deploying operating system upgrades.**
- **Upgrades and security patches make every operating system version incrementally more secure.**
- **Cisco IP Telephony Operating System upgrades are available for download at Cisco.com.**
- **Do not download any patches directly from Microsoft.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1.6

The Cisco IP Telephony Operating System is used by several Cisco IP Telephony Application Server components, such as Cisco CallManager, Cisco Emergency Responder (ER), Cisco IP Contact Center (IPCC), and Cisco Interactive Voice Response (IVR).

Cisco IP Telephony Operating System upgrades are built on top of each other and are incrementally more secure. The upgrades provide changes to, for example, the IP stack, file system, registry, access control lists (ACLs), and dynamic link library (DLL) engines.

Note Before you run an operating system upgrade provided by Cisco, read the release notes for that upgrade carefully. The operating system upgrade may not apply to your installation and could harm the running applications. Before upgrading the Cisco IP Telephony Operating System, consider making a backup.

Cisco IP Telephony Operating System upgrades can be downloaded from Cisco.com, <http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des>.

Verify that you are using the proper operating system upgrade for your Cisco CallManager version.

Note The compatibility matrix is available on Cisco.com at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm and should be consulted before you run an operating system upgrade.

Caution The operating system upgrades provided by Cisco are not the same as upgrades provided by Microsoft. The operating system upgrades and patches provided by Cisco are tailored for IP telephony applications. If a Microsoft service pack (SP) is installed for the Cisco IP Telephony Operating System, the applications running on the Cisco IP Telephony Operating System may be adversely affected.

Security and Hotfix Policy

This topic describes the Cisco security and hotfix policy for keeping the operating system up to date.

Cisco IP Telephony Security and Hotfix Policy

Cisco.com

- **Cisco monitors several sites for new Microsoft vulnerabilities.**
- **Critical patches are tested and posted at Cisco.com within 24 hours.**
- **Applicable patches are consolidated into a monthly posted service release.**
- **Automatic notification tools are available at Cisco.com:**
 - **Cisco CallManager Notification Tool—updates related to Cisco CallManager**
 - **Cisco PSIRT Advisory—security-related updates**

© 2005 Cisco Systems, Inc. All rights reserved.CPT2 v4.1—1-7

Cisco closely monitors security bulletins from Microsoft and evaluates them based on the impact to Cisco CallManager and other IP telephony applications with the respective operating system installation.

When Microsoft posts a security patch, Cisco determines whether the patch affects applications and operating system components in Cisco CallManager and applications that share the same operating system installation process. This is a list of applications and operating system components that might be affected by a patch:

- Microsoft Windows 2000 Server (including any Windows component or subcomponent installed by Cisco)
- Microsoft Internet Information Server (IIS)
- Microsoft Internet Explorer
- Microsoft Structured Query Language (SQL) Server

Relevant patches are tested to verify correct operation with Cisco applications.

The security patch and hotfix policy for Cisco CallManager specifies that any applicable patch deemed Severity 1 or Critical must be tested and posted to Cisco.com within 24 hours as a hotfix. All other applicable patches are consolidated and posted once a month as incremental service releases.

Note Patches and security hotfixes can be downloaded from <http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des>.

There is also a document that provides information on tracking Cisco-supported operating system files, SQL server, and security file documents. This document is available at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/osbios.htm.

Notification tools (e-mail service) for providing automatic notification of new fixes, operating system updates, and patches for Cisco CallManager and associated products are also available:

- **Cisco CallManager Notification Tool:** This e-mail service provides automatic notification of new fixes, operating system updates, and service releases that are available for Cisco CallManager and related products, including Cisco CallManager Attendant Console, Cisco IP Manager Assistant (IPMA), and Bulk Administration Tool (BAT). To subscribe, go to http://www.cisco.com/warp/public/779/largeent/software_patch.html and follow the instructions on the web page.
- **Cisco Product Security Incident Response Team (PSIRT) Advisory Notification Tool:** This e-mail service provides automatic notification of all Cisco security advisories released by Cisco PSIRT. Advisories that describe security issues that directly impact Cisco products provide a set of actions required to repair these products. To subscribe, go to http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html and follow the instructions on the web page.

Note The Cisco IP Telephony Operating System configuration and patch process does not currently allow an automated patch-management process.

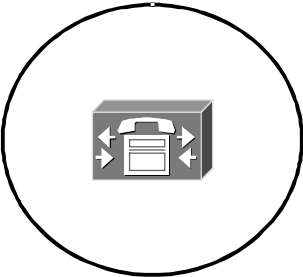
Operating System Hardening

This topic describes how the optional operating system security script and manual security settings provide more stringent security controls to the hardened Windows operating system.

Operating System Hardening

Cisco.com

- Use the latest operating system upgrade available for your Cisco CallManager release.
- Do not use IP Telephony Operating System as a file server, print server, or user workstation.
- Select the Cisco CallManager roles and appropriate services carefully.
- Consider using additional Cisco IP Telephony Operating System security scripts.
- Do not install additional applications not approved by Cisco.



© 2005 Cisco Systems, Inc. All rights reserved. CPT2 v4.1--1-8

One of the most important steps in securing an IP telephony server is installing all the applicable product or component security updates and then making sure that they are kept up to date. Cisco provides three types of updates for the Cisco IP Telephony Operating System:

- **Operating system upgrade:** Comprehensive upgrade to all components of the operating system that is released two to three times a year, including: Microsoft Windows 2000 SPs, Internet Explorer SPs, BIOS, firmware, drivers, Microsoft hotfixes, security configuration changes, third-party software that is installed in the base operating system, and configuration changes to match the currently shipping operating system version.
- **Operating system service releases:** Primarily a comprehensive roll-up of security hotfixes that are released the third Tuesday of each month when needed to deliver new security hotfixes. The operating system service release occasionally contains nonsecurity hotfixes or configuration changes that are needed to resolve a defect in the operating system.
- **Critical hotfixes:** When Microsoft releases a hotfix that is critical for Cisco IP telephony products, Cisco tests the hotfix for one day and posts it to Cisco.com within one business day of the release by Microsoft.

An IP telephony server must be used for IP telephony purposes only. The server should not be used as a common file server that stores user data or has user applications, such as office products, installed on it. File-share access has to be limited to the absolute minimum needed (for instance, to access log files and generate reports). Strict file access control has to be deployed, and auditing of network file access should be enabled. This practice will also eliminate the need to add user accounts to the server; only administrator and auditor accounts should exist. If network file access is not needed at all, it should be disabled to enhance the security of the server.

The more services that are running on a server, the more likely it is that vulnerabilities can be exploited by an attacker. To minimize this risk, only the services that are needed should be activated. Many services that are not needed have already been disabled in the Cisco hardened version of the Microsoft Windows 2000 Server operating system

To make Cisco CallManager even more secure, Cisco provides additional security scripts and information on how to protect the Cisco IP Telephony Operating System against common threats.

Do not install any other application on the servers unless it is approved software, such as Cisco Security Agent or antivirus products. A hardened IP telephony server has to be stripped down to run only the services and applications that are needed for its operation.

Additional IP Telephony Operating System Security Scripts

Cisco.com

- **Cisco IP Telephony Operating System 2.6 and later include scripts and information on additional security settings**
- **Can be run on Cisco CallManager Release 3.3(2) or later**
- **Not supported when colocated applications are used**
- **May cause problems with supported third-party applications**
- **Limited amount of testing**
- **Should be applied only by experienced Microsoft administrators**

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1—1-9

The security guide and script provide additional security settings beyond those that are installed by default in the Cisco IP Telephony Operating System. The settings in the optional security script have not been included by default and are not intended for all customers to use. When planning to use the optional security script, consider these points:

- The optional security script settings are supported only for Windows 2000 servers that are running Cisco CallManager Release 3.3(2) and later.

Caution The optional security script settings may have an adverse impact on some of the other Cisco IP telephony applications that use this operating system, on the interaction between Cisco CallManager servers and some other Cisco IP telephony applications, and on some supported third-party software.

- Because these settings are not installed by default, they receive only a limited amount of testing.
- Only experienced Windows administrators should apply the optional security script or manual settings.

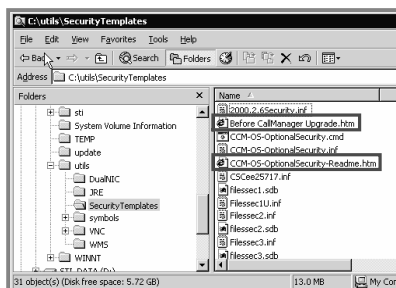
Caution Applying the optional security script can destroy colocated installations, such as Cisco IPCC Express, Cisco IP IVR, and Cisco IP Queue Manager (IP QM).

Additional IP Telephony Operating System Security Scripts (Cont.)

Cisco.com

The C:\utils\SecurityTemplates folder contains:

- **CCM-OS-OptionalSecurity-Readme.htm** file with optional security settings
- **Before CallManager Upgrade.htm** file describes necessary steps before upgrading the system



The optional security script and some additional information are available in the C:\utils\SecurityTemplates folder.

The script file is a batch job that can be started by clicking the CCM-OS-OptionalSecurity.cmd file. Before doing so, read the CCM-OS-OptionalSecurity-Readme.htm file to identify possible issues with applications running on the operating system:

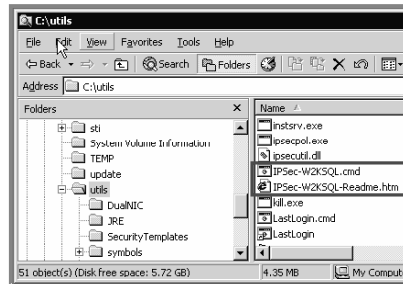
- The CCM-OS-OptionalSecurity-Readme.htm file contains information on what the CCM-OS-OptionalSecurity script is changing in the operating system and provides additional security settings that can be configured manually.
- Some of the optional security settings cause upgrades to fail. Therefore, if the Cisco IP Telephony Operating System optional security settings have been installed on the server and you want to upgrade the server, read the “Before CallManager Upgrade” guide. It includes a checklist of all settings to which you must revert for the upgrade to work.

Additional IP Telephony Operating System Security Scripts (Cont.)

Cisco.com

The C:\utils folder contains:

- IPsec-W2KSQL.cmd file—the IPsec filter will block the fixed Windows 2000 and SQL ports.
- Follow the instructions in the IPsec-W2KSQL-Readme.htm to install the IPsec filter.



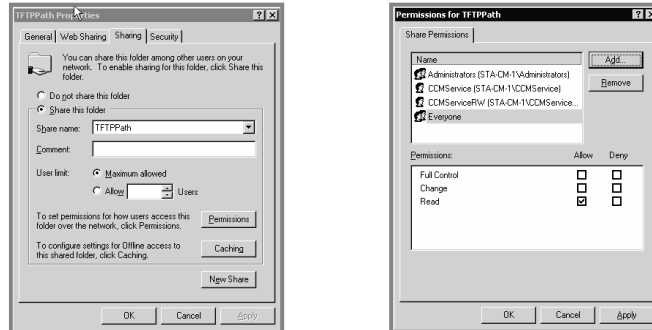
An additional security script is provided in the C:\utils directory. This script is called the IP security filter and will block the fixed Windows 2000 and SQL ports. Read the IPsec-W2KSQL-Readme.htm file for instructions on how to use the IP security filter:

- Blocking the fixed Windows 2000 and SQL ports adds an extra layer of protection from viruses, worms, and hackers. A provided script eases the creation of the IP security filter. The script needs to be customized with the IP addresses that the organization wants to allow through the filter. For example, the Cisco CallManager uses SQL ports allowing every IP address to connect to these port numbers. The IPsec-W2KSQL script would allow SQL connections only from the IP addresses defined in the script. These consist mostly of the other Cisco CallManager servers in the cluster and applications that need direct access to the database, for example, to the Call Detail Record (CDR) tables.
- Using this IP security filter increases the management overhead of the servers. If the IP infrastructure changes or additional servers are added to the Cisco IP telephony solution, the permit lists on all the servers will need to be updated.

Note The name of the IPsec-W2kSQL file has nothing to do with the IPsec virtual private network (VPN) umbrella standard.

File Sharing Considerations

Cisco.com



- **Consider removing the Everyone group from share permissions:**
 - CDR folder
 - TFTPPath folder
- **Detailed information is available in the OptionalSecurity readme file.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-12

To secure the access to file shares, limit access to the absolute minimum number of users who need it.

Check the share permissions on all shared folders, for example, the CDR and TFTPPath folders, and consider removing share permissions for the Everyone group. Get detailed information on how to secure file shares in the CCM-OS-OptionalSecurity-Readme guide, located in the folder C:/Utils/SecurityTemplates.

Antivirus Protection

This topic describes the antivirus software that is approved for use on a Cisco CallManager server.

Antivirus Protection

Cisco.com

- To protect the Cisco IP Telephony Operating System against attacks by viruses, Trojan horses, and worms, consider implementing antivirus protection software

```
graph TD; A[Password and Account Issues] --> C[Attacks by Viruses, Trojan Horses, and Worms]; B[Bugs and Exploits in the Operating System] --> C; D[Common Windows Exploits] --> C;
```

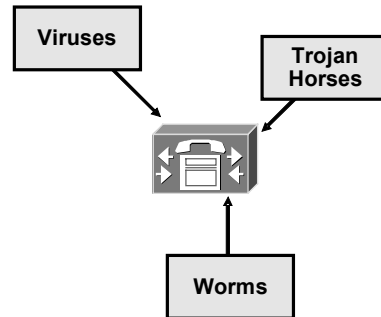
© 2005 Cisco Systems, Inc. All rights reserved. CIP12 v4.1-1-13

In addition to hardening the Cisco IP Telephony Operating System by using built-in tools, the system should also be protected by antivirus software. This practice will defend against attacks by viruses, Trojan horses, and worms.

Antivirus Protection (Cont.)

Cisco.com

- **Antivirus software supported by Cisco CallManager 4.1:**
 - McAfee VirusScan Enterprise 4.5, 7.0, and 7.1
 - Symantec AntiVirus Corporate Edition 7.61, 8.0, and 8.1
 - Trend Micro ServerProtect 5—all versions
- **Disable heuristic scanning**



© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-1-14

For the detection of viruses, it is recommended that you have antivirus software installed on your servers. Make sure that the software itself as well as the virus definition files are kept up to date so that the newest viruses can be detected. Do not enable heuristic scanning because it can block Cisco CallManager web pages from operating. Currently these antivirus products are supported on the Cisco IP Telephony Operating System:

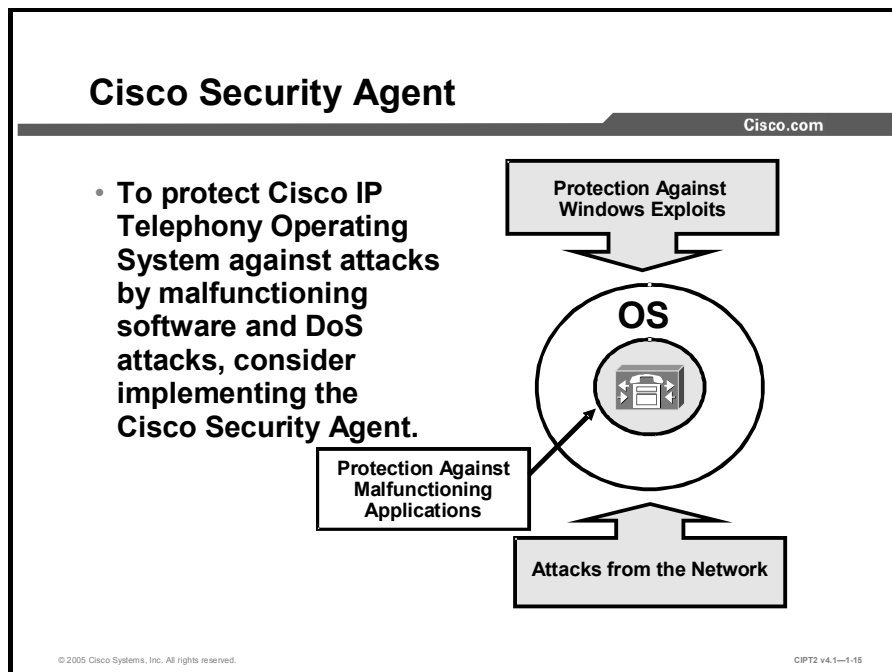
- McAfee VirusScan Enterprise 4.5, 7.0, and 7.1
- Symantec AntiVirus Corporate Edition 7.61, 8.0, and 8.1
- Trend Micro ServerProtect v5

The list of the latest supported antivirus software is available at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_bulletin0900aecd800f8572.html.

Tip Heuristic scanning refers to the ability of the software to flag suspicious files or attachments because they resemble known viruses. Heuristic scanning uses behavior-based rules to identify and block new viruses without requiring you to first download a patch.

Cisco Security Agent

This topic describes the features and functions of Cisco Security Agent and how Cisco Security Agent can secure Cisco CallManager.



In addition to antivirus protection, the operating system has to be protected against other threats from the network, such as DoS attacks. For these issues, Cisco provides Cisco Security Agent software that should be installed on every Cisco CallManager system.

Cisco Security Agent (Cont.)

Cisco.com

- **HIPS, among other functions, provides operating system protection:**
 - **Operating system integrity hardening**
 - **Application misbehavior prevention/restriction**
 - **Endpoint firewalls**
- **Independent of host operating system security**
- **Protects the Cisco IP Telephony Operating System against known and yet-unknown attacks**
- **Available for IP telephony servers as headless and managed versions**

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-1-16

For additional server operating system protection, host-based intrusion prevention systems (HIPSs) can provide an additional layer of protection against known and yet-unknown attacks and at the same time provide security services not offered by the host operating system. Examples are personal firewalls or software keylogger detection, based on application behavior.

Cisco Security Agent is designed to protect the endpoint from network-borne attacks, and it enforces its protection rules on several levels. One of them is the protection of the underlying operating system from potentially hostile applications. Cisco Security Agent provides three basic areas of operating system protection:

- Protection of operating system integrity, where Cisco Security Agent policy rules always prohibit access to sensitive system files and registry settings. For example, no application can change files in the Windows system folder.
- Prevention or restriction of application misbehavior resulting from injection of hostile code or other network attacks. Several policy rules are dynamic and allow or disallow local resource access based on the behavior of the application and hence its potential “hostility.” For example, if a client application accesses the network, it is automatically considered less trusted and its access to local resources is further restricted.
- Endpoint, or personal, firewalls, where Cisco Security Agent can allow or deny network access to any local application, and hence minimize access to and from the system, enforcing the least-privilege rule.

Cisco Security Agent operates independently of native operating system functions, providing an independent layer of protection that prevents attacks even when the native operating system access control methods are breached. Cisco Security Agent should never be deployed instead of strong host security but as an additional protective layer and to provide protection methods not available in the host operating system.

The rationale behind the behavioral approach is that although the number of methods and exploits to attack a system is extremely large, the number of possible consequences of these attacks is relatively small. For example, a web server can be persuaded by the attacker to

execute a local file or an executable attachment in an e-mail attempting to access the Windows registry. Cisco Security Agent can recognize application behavior leading to or following an attack and prevent the malicious actions. This ability is also why Cisco Security Agent does not require constant updates; its policies need to be updated only if a completely different class of attacks is created, which is relatively rare.

Cisco Security Agent for IP telephony servers is available in two versions:

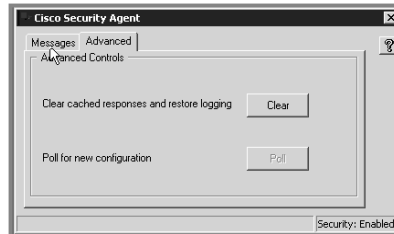
- **Headless agent:** This version comes with a set of rules for a specific server platform, such as Cisco CallManager; no further configuration is necessary.
- **Managed agent:** This version has to be configured with rules for the appropriate IP telephony servers. Predefined rules can be downloaded from Cisco.com.

Caution Do not use the headless agent when running Cisco CallManager with colocated applications, such as Cisco IPCC Express, Cisco IP IVR, or Cisco IP QM, because the fixed policy of the headless agent will not support these applications (and as a consequence they will not work properly).

Cisco Security Agent Headless Agent

Cisco.com

- **Prebuilt application-specific kit freely downloadable from Cisco.com**
- **Used for simple and static server configuration**
- **Fixed security policy**
- **No centralized event-reporting capabilities**



© 2005 Cisco Systems, Inc. All rights reserved.

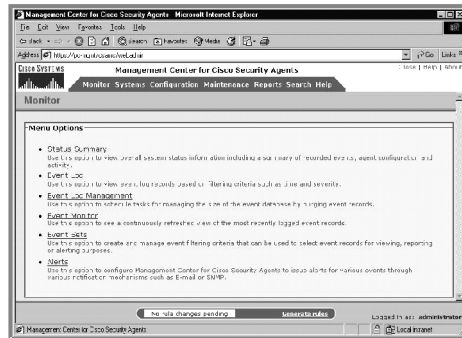
CIPT2 v4.1-1-17

The free headless agent has a fixed security policy and no centralized reporting capabilities. For each type of IP telephony server, a different (predefined) agent kit is available for the headless agent. The headless agent is configured with appropriate policies and exceptions for a typical supported configuration of that server. The headless agent should be used in environments where centralized reporting is not required or practical and the IP telephony servers are aligned with Cisco specifications for installed software and system and application configuration and where they feature no add-ons that might conflict with the security rules of the headless agent.

Cisco Security Agent Managed Agent

Cisco.com

- Requires CiscoWorks VMS and Cisco Security Agent MC to centralize policy management
- Allows centralized event correlation and reporting
- IP telephony server-specific policies for agents
- Enables the use of Cisco Security Agent Profiler tool
- Use with complex server environments



© 2005 Cisco Systems, Inc. All rights reserved.

CIP72 v4.1-1-18

The managed version of Cisco Security Agent uses CiscoWorks VPN/Security Management Solution (VMS) and Cisco Security Agent Management Center (MC) for centralized policy distribution and allows event correlation and reporting. As with the headless agent, which comes in different configurations for different types of IP telephony servers, Cisco Security Agent MC also allows the administrator to load predefined, application-specific policies for each IP telephony server type.

The managed agent should be used in environments where centralized reporting is required, where servers do not use a typical configuration (for example, with nondefault TCP or UDP ports) or have special application requirements (for example, custom systems management software), or where the default policies need to be augmented with site-specific protection requirements.

Deployment of the managed agent also allows the use of Cisco Security Agent Profiler, an expert add-on tool that can, to a large extent, automate generation of custom application policies. This add-on would allow an expert Cisco Security Agent administrator to further enhance the built-in policies and confine every IP telephony application to a sandbox, similar to the functions that the built-in Restrictive MS IIS Module and Restrictive MS SQL Server Module provide for those two applications.

The Cisco Security Agent Profiler must be purchased separately, but it does not require any other software to be installed on the profiled servers.

Cisco Security Agent Supported Applications

Cisco.com

- **Cisco IP telephony application:**
 - **Cisco CallManager Release 3.2(3) and later**
- **Some of the add-on applications:**
 - **HP OpenView Operations Agent 7.1**
 - **McAfee VirusScan 7.0**
 - **Trend Micro AntiVirus**
 - **Real VNC**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-19

Cisco Security Agent is available for Cisco CallManager Release 3.2(3), 3.3, and later. To use Cisco Security Agent for another Cisco IP telephony application, check the Cisco Security Agent administration manual to determine whether Cisco Security Agent is supported for that particular application.

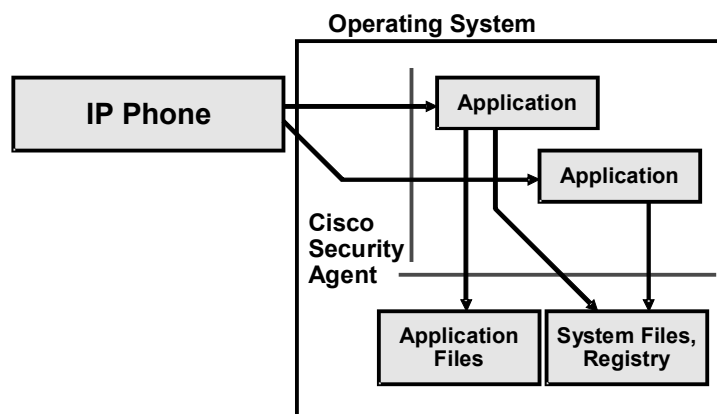
This is a list of software add-ons that are supported with Cisco Security Agent on the same server:

- BMC PATROL
- Concord eHealth Monitor
- Diskeeper Server Standard Edition 8.0.478.0
- HP OpenView Operations Agent 7.1
- HP OpenView Performance Manager 3.3
- Integrated Research PROGNOSIS
- McAfee VirusScan 7.0
- Micromuse Netcool
- NAI ePolicy Agent
- NetIQ Vivinet Manager
- RealVNC VNC
- Symantec AntiVirus Corporate Edition 8.0
- Trend Micro AntiVirus
- Windows Terminal Services

Note The Cisco Security Agent headless agent and the Cisco Security Agent policies for the Cisco Security Agent MC are both available at <http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des>.

Cisco Security Agent Operating System Protection

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

CIP72 v4.1-1-20

The Cisco Security Agent default operating system protection rules for IP telephony servers provide basic operating system hardening and integrity protection and contain rule exceptions for supported add-on applications. In regard to local resource access control, these policies can be summarized as follows:

- Allow specific actions required by basic operating system processes
- Protect the integrity of the system binaries and other sensitive files from local applications
- Protect the integrity of the system registry from local applications
- Allow all other actions (including network access and access to local files as dictated by the native security of the local host, for example, file ACLs in Windows)

In addition to these basic rules, many other rule modules constitute the total Cisco Security Agent protection policy of a system.

Cisco Security Agent Guidelines

Cisco.com

- **Use at least the headless agent**
- **Use default policies for operating system protection**
- **Use Cisco Security Agent only with Cisco approved software**
- **Cisco Security Agent personal firewall allows all inbound connections by default**
- **Disallow manual stop of Cisco Security Agent service**

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-1-21

At the minimum, for each server, deploy the headless Cisco Security Agent. The built-in operating system protection policies are sound and generally do not require tuning for enhanced protection, except where dictated by the site policy.

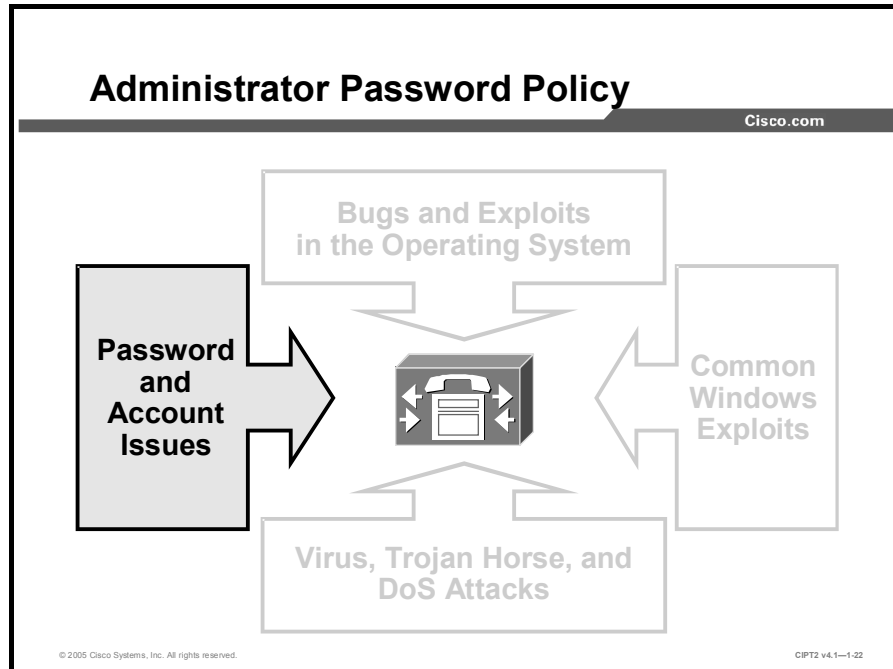
So-called “false positives,” events that are erroneously classified as attacks, are very likely when using unsupported server add-ons, such as system management and unsupported antivirus software. To eliminate this erroneous behavior, deploy the managed agent and add the requested permissions for these applications so that Cisco Security Agent will not consider them to be malicious.

Cisco Security Agent also provides personal firewall functions by restricting network connections to the server. The headless agent has a fixed policy that allows all inbound connections to the server, and this cannot be changed. If you want to use Cisco Security Agent to control network connectivity to the server, you have to use the managed agent. Alternatively, you could use native Windows IP security filtering or rely solely on packet filtering by network devices, such as routers or firewalls.

Cisco Security Agent by default allows the agent service to be stopped by the local administrator (using the **net stop csagent** command). When using the managed version of Cisco Security Agent, you can applying an agent policy that blocks the local administrator from stopping the agent.

Administrator Password Policy

This topic describes the password policy for administrative accounts.

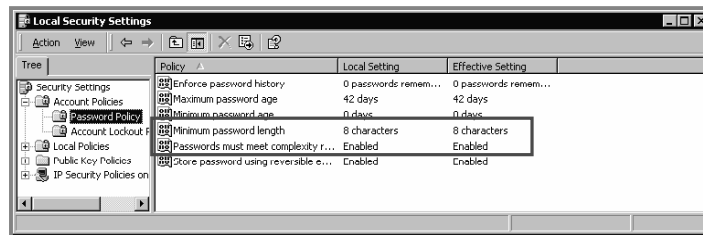


One of the easiest and most frequently used attacks against Microsoft operating systems is to try to log in to the Administrator account, using various well-known passwords. To block that security hole, consider using strong password policies, renaming the Administrator account, and other mechanisms to protect the Administrator account.

Administrator Password Policy (Cont.)

Cisco.com

- Use local security settings very carefully.
- Do not change anything on the password policy except:
 - Minimum Password Length
 - Password Must Meet Complexity Requirements
- Do not change any account lockout policies



© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-1-23

The Windows operating system gives administrators the ability to assign restrictions to password and account policies. A general rule is not to create any user accounts on an IP telephony server. Only administrators and operators should have access to the server. Make sure that these accounts have complex passwords. If a password is too simple, not kept secret, or not changed for a long period, it can be discovered and misused by unauthorized people. The account policy settings should not be modified, because setting the lockout policies can adversely affect the system during the next upgrade (requiring a new installation from scratch). Consider these issues:

- Setting the account policy is more important for servers with user accounts because otherwise the administrator has no control over the frequency of password changes by the users.
- The Minimum Password Length parameter determines how short passwords can be. If it is set to zero, blank passwords are allowed. It is recommended that you set this value to at least eight characters.
- The Passwords Must Meet Complexity Requirements parameter determines whether password complexity is enforced. If this setting is enabled, passwords must meet these requirements:
 - The password is at least six characters long
 - The password contains characters from at least three of these categories:
 - English uppercase characters (A through Z)
 - English lowercase characters (a through z)
 - Base-10 digits (0 through 9)
 - Nonalphanumeric characters (For example: \$, !, %, #, &)
 - The password does not contain three or more characters from the username

To configure the password policy for an account, complete these steps:

- Step 1** From the Cisco CallManager server, click **Start**.
- Step 2** Choose **Settings**.
- Step 3** From the Settings menu, choose **Control Panel**.
- Step 4** When the Control Panel window opens, click **Administrative Tools**.
- Step 5** In the Administrative Tools window, click **Local Security Policy**.
- Step 6** When the Local Security Settings window opens, click **Account Policy**.
- Step 7** Click **Password Policy**.

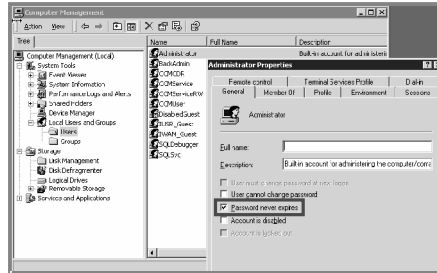
You can configure the password policies to meet complexity requirements and set the minimum length of the password.

Tip The password complexity settings should be applied before you install the Cisco CallManager application. If the passwords applied in the installation process do not fit the complexity requirements, the Cisco CallManager services will no longer be able to start.

Account and Password Considerations

Cisco.com

- Consider creating individual users placed in Administrators group
- Consider renaming Administrator account
- Consider creating a decoy Administrator account
- Verify that “Password never expires” is set on service accounts
- Add passwords on screen saver, CMOS, and HP iLO



© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-24

When giving individual users the ability to log in to the Cisco IP Telephony Operating System as administrators, you should create a separate account for each user and put each into the Administrators group. Doing so enables tracking of changes made to the Cisco IP Telephony Operating System.

In addition, the administrator name could be changed and a decoy Administrator account could be created that has no rights but is strictly monitored (by enabling auditing of login attempts or usage of that account).

Note Cisco CallManager installations and upgrades currently require the Administrator account to be used. Before installing or upgrading Cisco CallManager, rename the decoy Administrator account and change the name of the real Administrator account back to “Administrator” on all Cisco CallManager servers in the cluster.

Follow general security guidelines for accounts and passwords, such as removing unnecessary accounts and requiring complex passwords, but also harden the server by applying password protection to complementary metal oxide semiconductor (CMOS) access, screen savers, and Hewlett-Packard Integrated Lights-Out (iLO) access (used for out-of-band server management).

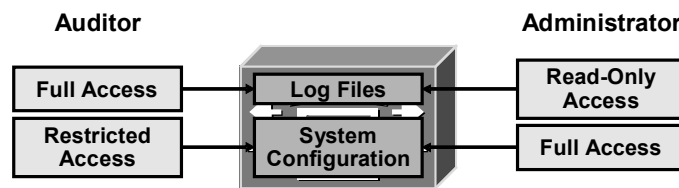
Note More information on iLO can be found at <http://h71028.www7.hp.com/enterprise/cache/98327-0-0-225-121.aspx>.

Note Information on CMOS is provided in server hardware manuals. The CMOS information for the MCS-XXA can be found at www.hp.com, and information on the MCS-XXI hardware can be found at www.ibm.com.

Administrator Account Considerations

Cisco.com

- Consider creating separate auditor accounts.
- Auditors should have very limited privileges on the system itself, but full access to logs.
- Administrators should have read-only access to logs.



© 2005 Cisco Systems, Inc. All rights reserved.

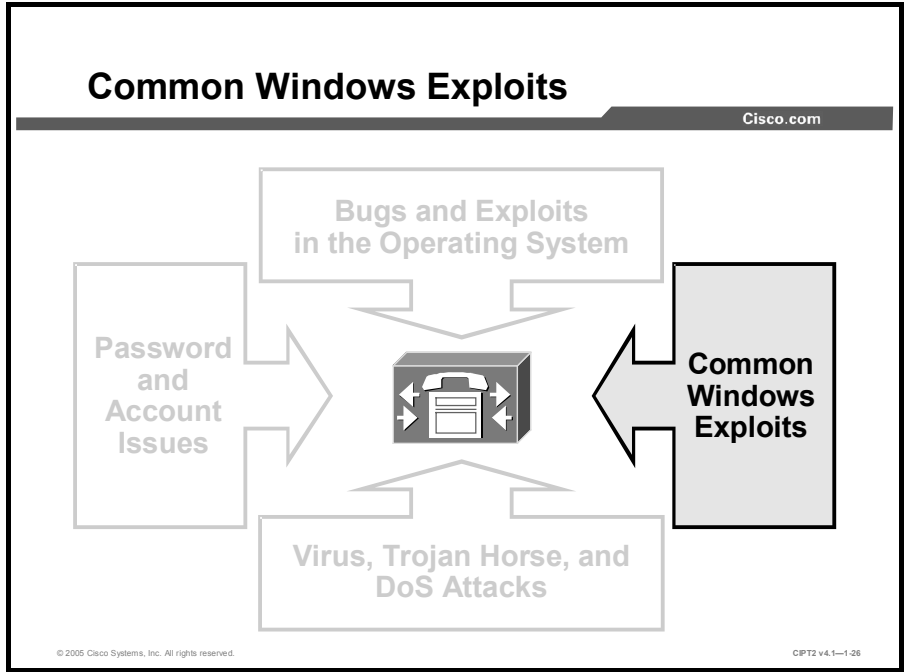
CIPT2 v4.1-1-25

Some corporate security policies require separating the system auditors from the system administrators.

To enable more accurate auditing information regarding the identity of an administrator, it is a good practice to create individual accounts for each administrator and make them members of the Administrator group. In addition, separate administration from auditing by creating separate auditor accounts. Auditor accounts should have full rights to logs but should not have any other administrative permission, while administrator accounts should have only read access to log files.

Common Windows Exploits

This topic describes how to protect Microsoft Windows against the most common exploits.

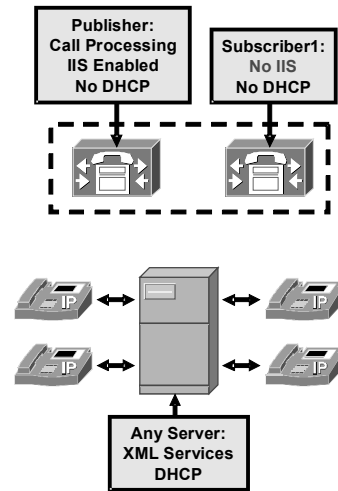


A hardened Cisco IP Telephony Operating System can successfully defend against many common Windows exploits. There are some active services that cannot be disabled because Cisco CallManager uses them. To secure these areas, you must design the IP telephony-ready network properly and choose the proper roles for the Cisco CallManager nodes in the cluster.

Common Windows Exploits (Cont.)

Cisco.com

- **Most XML applications retrieve data from the Internet—offload XML to a dedicated server.**
- **80 percent of attacks against Windows are targeted at IIS—disable IIS on Cisco CallManager subscribers.**
- **Deploy DHCP server close to the endpoints.**



© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-27

You need to protect Windows against some of the most common exploits. One common exploit involves Extensible Markup Language (XML) applications running on HTTP (TCP port 80), and most XML applications go to the Internet to get their data. It is recommended that you offload XML services to a dedicated server. The Cisco CallManager server that is providing TFTP services, for instance, must not be the Cisco CallManager that is doing active call processing.

The most important task for Microsoft IIS issues is to turn off IIS on all subscribers. IIS is the parent process for HTTP, Simple Mail Transfer Protocol (SMTP), and FTP. Eighty percent of the attacks against Windows are against the IIS parent process. Turn off IIS on the subscribers, where all of the active call processing is taking place, and run it only on the publisher for administration purposes. This practice will minimize the threats against Windows by 80 percent and actually bring it closer to parity with what is considered to be the normal security settings of UNIX or Linux operating systems.

In a Cisco CallManager cluster, different servers can have different roles and hence do not need the same active services. One server could act as a pure management server by providing access only to Cisco CallManager Administration web pages, while other servers are providing call-routing functions and others are being used for applications such as phone services. Because IIS is a common target, run it only where needed—at the publisher. During upgrades, IIS will also be needed on subscribers but will automatically be started when needed as long as the service is set to manual rather than disabled. Therefore, set IIS to manual on all subscribers and keep the setting automatic only at the publisher.

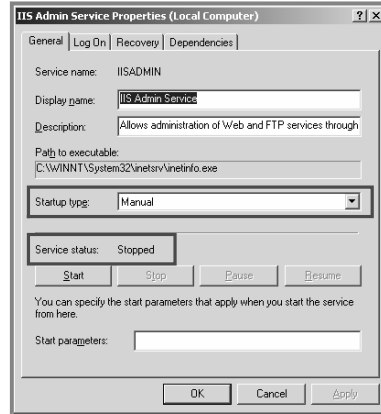
To avoid attacks against the Dynamic Host Configuration Protocol (DHCP) server, which in most installations is used to provide IP settings (such as option 150—Cisco CallManager TFTP server), push DHCP as close to the endpoints as possible.

Hardening IIS

Cisco.com

Turn off IIS on the subscriber Cisco CallManager nodes:

- IIS service set to Manual and Stopped
- Cisco CallManager installer script can activate IIS when set to Manual and Stopped



© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-28

It is important to set the IIS Startup Type option to Manual and Stopped rather than setting it to Disabled.

IIS needs to be available during upgrades. If you have set the IIS Startup Type option to Disabled, the upgrade will fail.

When IIS is set to Manual and Stopped, a pop-up window will remind you that IIS needs to be active to perform the upgrade. The installer automatically activates IIS, performs the upgrade, and turns IIS off when the upgrade is finished.

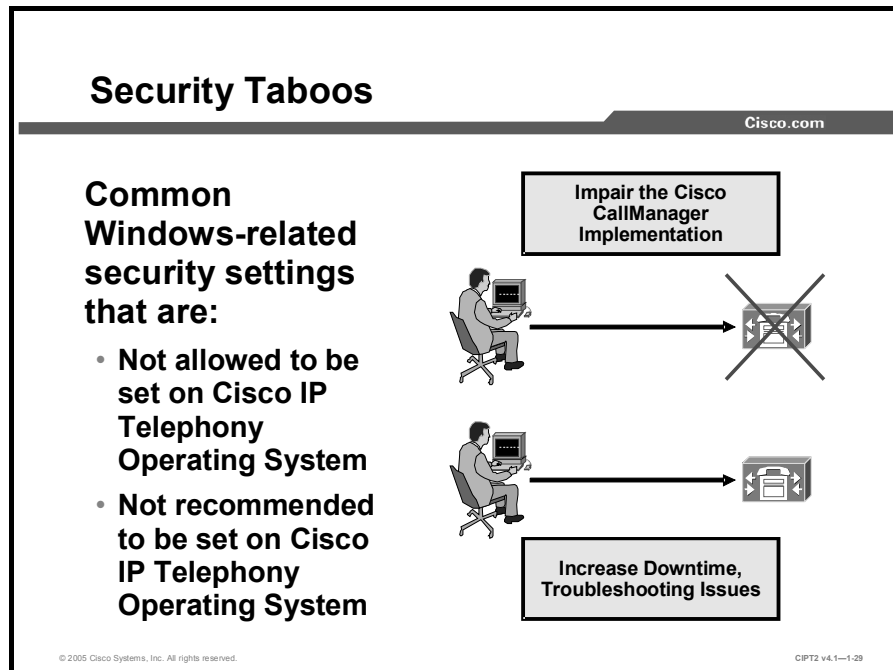
This table shows what will happen during a Cisco CallManager upgrade when the IIS is set to different options.

Behavior of Cisco CallManager During an Upgrade

IIS Service Parameter	Resulting Upgrade Behavior
Enabled	The upgrade will work with no interference.
Disabled	The upgrade will fail; no message is displayed.
Manual and Stopped	The upgrade will stop, a message that the IIS is not running will pop up, the IIS service will start, and the upgrade will continue. On the next reboot, the IIS service will be in the Manual and Stopped state again.
Manual and Running	The upgrade will work with no interference.

Security Taboos

This topic describes common security practices and settings that are not recommended or that are strictly forbidden on Cisco CallManager.



After you have protected Cisco CallManager against common Windows exploits such as attacks on IIS, there are additional security settings that, from the point of view of a Windows administrator, are nice to have but that are not recommended in a Cisco CallManager environment.

Some of the settings that a Windows administrator would normally implement on the servers could cause the Cisco CallManager installation to fail, increase the system downtime of the Cisco CallManager server, and delay troubleshooting efforts.

Security Taboos (Cont.)

Cisco.com

Not to Be Done in Any Circumstance	Reason Why It Is Not Allowed
Do not delete, disable, or rename any service accounts.	Services like Cisco CallManager or SQL might not function.
Do not change "password never expires" on service accounts created by Cisco.	Services might not start.
Do not change any file, folder, or registry key permissions unless documented.	A high probability exists that Cisco CallManager will not function.
Do not set the CMOS power-on password.	The server will not boot after power failure until password is entered.

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-1-30

Some actions should never, under any circumstances, be applied on a Cisco CallManager system. The Cisco Technical Assistance Center (TAC) will not support any Cisco CallManager system where one of these settings has been applied:

- Do not delete, disable, or rename any accounts created in Cisco CallManager or SQL. Any of these actions will adversely affect Cisco CallManager, because these accounts are required for proper operation of Cisco CallManager.

Note Cisco CallManager Release 4.1 uses the following service accounts: CCMCDR, CCMSvc, CCMSvcRW, CCMUser, and SQLSvc.

- It is strictly forbidden to change the setting for expiration of the passwords of the Cisco CallManager service accounts. Doing so affects the ability of these services to function properly.
- Do not change the security permissions (ACL) for any folder, file, or registry key installed by Windows 2000 or Cisco, other than those that are set by Cisco installs or security templates or that are listed in the CCM-OS-OptionalSecurity-Readme.htm document as a manual step.
- Do not set the CMOS power-on password. The Cisco CallManager server is considered a mission-critical, 24x7 system. If the server is rebooted remotely or if it automatically reboots as corrective measure, it should not stop with the Power-On Password window waiting for an administrator to enter a password.

Note Do not confuse the CMOS access password with the CMOS power-on password. Although the system requests the CMOS power-on password to boot, the CMOS access password is checked when you try to enter CMOS configuration. You should always protect CMOS access by requiring a password, but you should never enable the CMOS power-on password.

Security Taboos (Cont.)

Cisco.com

Not to Be Done in Any Circumstance	Reason Why It Is Not Allowed
Do not delete, disable, or rename the IUSR_Guest or IWAM_Guest accounts.	Some IIS virtual directories require them.
Do not disable parent paths in IIS.	Some Cisco CallManager web pages will no longer work.
Do not remove the IIS application mappings for .asp, .cer, .cdx, and .asa.	Some Cisco CallManager web pages will no longer work.
Do not install unapproved third-party software, utilities, or agents.	Issues with Cisco support arise.

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-31

The figure presents other practices that you should not implement on Cisco CallManager:

- Do not delete, disable, or rename the IUSR_Guest or IWAM_Guest accounts. Some IIS virtual directories require them.
- Do not disable parent paths in IIS, or some Cisco CallManager pages will no longer work.
- Do not remove the IIS application mappings for .asp, .cer, .cdx, or .asa extensions, or IIS will not work properly.
- Do not install any third-party software, utilities, or agents that have not been approved for use with the version of the Cisco CallManager on the server. These applications may cause problems with system operation, and Cisco will not be able to support these applications or resolve issues they may cause.

Not Recommended Security Settings

Cisco.com

Not Recommended Setting	Reason Why It Is Not Recommended
Join an Active Directory domain	Role-based administrator not supported Complexity of Active Directory group policies (too many possible permutations)
Shutdown if Unable to Write Security Log	Not ideal for a strategic application
Disable crash control	Disabling Dr. Watson crash dumps adds complexity to forensic troubleshooting
Convert disk D from FAT to NTFS	Same server recovery will not work
Clear page file at reboot	Reboots can take 30 minutes or longer
Account lockout after N failed login attempts	Disables low-level service accounts

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-32

The security settings listed previously should never be used because they prevent Cisco CallManager from working properly, but there are also settings that could be used with Cisco CallManager but that are not recommended, unless they are really needed. It will depend on the security policy of the organization whether or not the disadvantages of such settings are acceptable for the sake of a slightly higher security level. If your security policy does not list any of these settings as mandatory, the recommendation is that you not use them:

- Do not integrate Cisco CallManager into Microsoft Active Directory. The main reason to join an Active Directory domain would be to use role-based administration, but this configuration is not supported by the current version of Cisco CallManager. If Active Directory group policies are used, Cisco TAC cannot support the configuration because of the extremely high number of possible permutations of settings (at the moment, there are $9.3 * 10^{157}$ possibilities). Incorrect Active Directory group policies can easily impair Cisco CallManager operation. As an example, customized account and password policies can adversely affect services accounts that are necessary for Cisco CallManager to function properly.

Caution If the Cisco CallManager is integrated into the Microsoft Active Directory, the installation will lose its Cisco TAC support.

- Cisco CallManager is considered a mission-critical, 24x7 system. In most cases, it is better to maintain phone service and lose auditing information than to halt the server. With the Shutdown if Unable to Write Security Log setting enabled, the Cisco CallManager server could, and is even likely to, halt, and phone service will not be provided until the system auditor clears the log files.
- If you disable Dr. Watson crash dumps, the time required to solve a problem that causes a process to crash increases. After a process crashes, the crash control settings have to be returned to the standard settings in the operating system provided by Cisco so that the next time the process crashes, the information file needed to troubleshoot the crash will be created.

- If you convert disk D from File Allocation Table (FAT) to Windows NT File System (NTFS), same server recovery does not work. In addition to server recovery issues, same server recovery can also be needed for Cisco CallManager upgrades. This was the case for migration from Cisco CallManager Release 3.1 or 3.2 to Cisco CallManager Release 3.3 or later. If you decide to convert disk D from FAT to NTFS, whenever you need to use same server recovery, you will either have to manually change the partition back to FAT format or reinstall the server from scratch.
- If the Clear Page File at Shutdown option is enabled, shutdowns and reboots will take substantially longer because the page file is being cleared. During shutdowns and reboots, a blank blue screen appears while the page file is being cleared. This setting will increase the down time of the server.
- If the account lockout policy is enabled, locking out the user account that is used by Cisco CallManager services can create a DoS attack against Cisco CallManager. With the account locked out, the service will eventually stop and cannot restart until the system administrator unlocks the user account and restarts the service.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **There are many security threats targeting Microsoft Windows operating systems.**
- **Harden the Cisco IP Telephony Operating System and keep it updated.**
- **Consider using the optional security scripts.**
- **Install approved antivirus protection software.**
- **Install the Cisco Security Agent to protect against DoS attacks.**
- **Use complex password and account policies.**
- **Do not rename accounts and passwords of services related to Cisco CallManager.**
- **Avoid security taboos on Cisco CallManager, or Cisco TAC support will not be available.**

© 2005 Cisco Systems, Inc. All rights reserved. CPT2 v4.1—1-33

Securing Cisco CallManager Administration

Overview

Security is not important for network devices such as switches and routers only. This lesson describes how communication with Cisco CallManager is secured by using Secure HTTP (HTTPS), so that a hacker cannot listen to this data stream during HTTP sessions. For large voice environments, it is important to distribute the various administration tasks. Cisco CallManager multilevel administration access (MLA) allows you to assign different authorization levels to administrators.

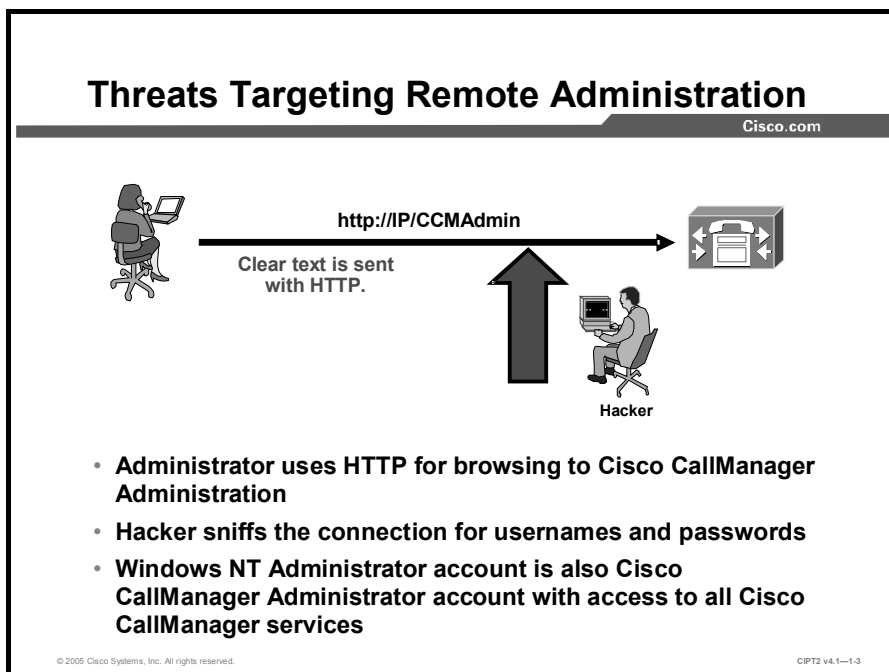
Objectives

Upon completing this lesson, you will be able to secure Cisco CallManager Administration. This ability includes being able to meet these objectives:

- Explain the threats targeting remotely accessing Cisco CallManager Administration and other applications
- Explain how HTTPS provides secure remote communication and login to Cisco CallManager Administration
- Describe HTTPS certificate details, use Microsoft IIS to save a certificate to a trusted folder, and copy the certificate to a file
- Describe how MLA provides multiple levels of security to Cisco CallManager Administration
- Enable MLA and assign a password to the superuser
- Define a functional group and identify the two types of functional groups
- Define a user group and identify how its privileges are mapped to functional groups
- Create a new functional group and a new user group and assign an access privilege level to the members of the user group

Threats Targeting Remote Administration

This topic describes the impact of insecure communication with the Cisco CallManager Administration.



In releases earlier than Cisco CallManager Release 4.1, HTTP is the standard protocol for accessing the Cisco CallManager Administration web pages. If an attacker intercepts the connection and looks for the username and password of the administrator, the attacker can find the relevant information easily because the connection is not secured. Beginning with Cisco CallManager Release 4.1, HTTPS (RFC 2818) is the standard protocol for accessing the Cisco CallManager Administration pages, without installing or configuring any additional security parameters.

Without MLA, the Cisco CallManager Administrator account is the Microsoft Windows Administrator account. If a hacker learned this login information, he or she could not only access the Cisco CallManager Administration pages but could also log in to the operating system of the Cisco CallManager server with full access to all information.

HTTPS Overview

This topic describes the HTTPS protocol, how it works, and the advantages of using it.

HTTPS Overview

Cisco.com

Secures communication between browser and web server:

- **Provides web server authentication**
- **Provides integrity of data by using packet signatures**
- **Provides privacy of data by packet encryption**
- **Supports most Cisco CallManager applications**

© 2005 Cisco Systems, Inc. All rights reserved.CPT2 v4.1-14

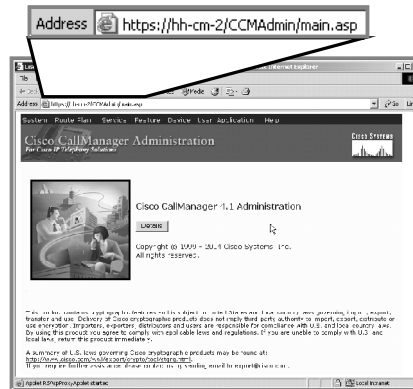
HTTPS secures communication between the browser on the client PC and a web server such as Microsoft Internet Information Server (IIS). It allows authentication of the web server and protects communication between the client and the web server. All packets are signed to provide integrity, so the receiver has a guarantee that the packets are authentic and have not been modified during transit. In addition, all packets are encrypted to provide privacy, so that sensitive information can be sent over untrusted networks. These Cisco CallManager applications support HTTPS:

- Cisco CallManager Administration
- Cisco CallManager Serviceability
- Cisco IP Phone User Options web pages
- Bulk Administration Tool (BAT)
- Tool for Auto-Registered Phones Support (TAPS)
- Cisco Call Detail Record (CDR) Analysis and Reporting (CAR)
- Trace Collection Tool
- Real-Time Monitoring Tool (RTMT)

Secure Administration over HTTPS

Cisco.com

- **Username and passwords**
- **Configuration changes**
- **Serviceability and other tools**
- **Speed dials and call forwarding on user pages**



© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1.5

When you are using HTTPS for browsing to Cisco CallManager Administration and user options web pages, communication is secure. A hacker who sniffs the communication will find it very difficult to recreate any information from the sniffed packets.

HTTPS secures not only the username and passwords in the communication but also configuration changes in Cisco CallManager Administration and other applications, such as Cisco CallManager Serviceability. If a user configures parameters such as call forwarding or speed dials on the user options web pages, the client and IIS communicate in a secure way.

HTTPS Certificate Operations

This topic describes why a certificate is needed, how Cisco CallManager gets a certificate, and how to prevent security alerts when browsing to the Cisco CallManager Administration pages.

HTTPS Certificate Operations

Cisco.com

- **HTTPS uses certificates for web server authentication.**
- **Certificates provide information about a device and are signed by an issuer (CA).**
- **Cisco CallManager uses a self-signed certificate by default.**
- **Cisco CallManager can optionally use a certificate issued by a company CA or an external CA, such as VeriSign.**

© 2005 Cisco Systems, Inc. All rights reserved.CPT2 v4.1-1-6

HTTPS uses certificates for web server authentication. Certificates provide information about a device and are signed by an issuer, the Certificate Authority (CA). By default, Cisco CallManager uses a self-signed certificate, but it also allows you to use a certificate issued by a company CA or even an external CA such as VeriSign. The file where the Cisco CallManager HTTPS certificate is stored is C:\Program Files\Cisco\Certificates\httpscert.cer.

The certificate will be used on the IIS default web site that hosts the Cisco CallManager virtual directories, which include the following:

- CCMAAdmin and CCMUser
- CCMSERVICE
- Administration Serviceability Tool (AST)
- BAT and TAPS
- RTMTReports
- CCMTraceAnalysis
- PktCap
- Administrator Reporting Tool (ART)
- CCMSERVICETraceCollectionTool

To use a certificate issued by a CA after a Cisco CallManager installation or upgrade, delete the self-signed certificate and install the CA signed certificate instead, as described in *Cisco CallManager Security Guide, Release 4.1(3)* at:

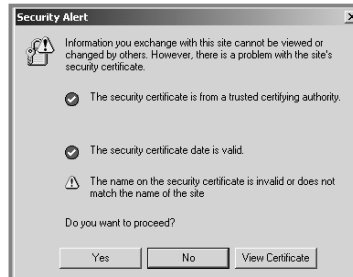
http://www.cisco.com/en/US/partner/products/sw/voicesw/ps556/products_administration_guide_chapter09186a00803fe674.html#wp1064578.

Note For more information on how to obtain a certificate from an external CA, contact a vendor of Internet certificates such as VeriSign or consult with the administrator of your company CA (if using your own CA).

Verify Authenticity When Browsing to Cisco CallManager

Cisco.com

- **Yes—Trust the certificate one time**
- **No—No access to the Cisco CallManager Administration pages**
- **View Certificate—Start installing the certificate on the client; Security Alert dialog box will not be displayed anymore**



© 2005 Cisco Systems, Inc. All rights reserved.

C IPT2 v4.1—1.7

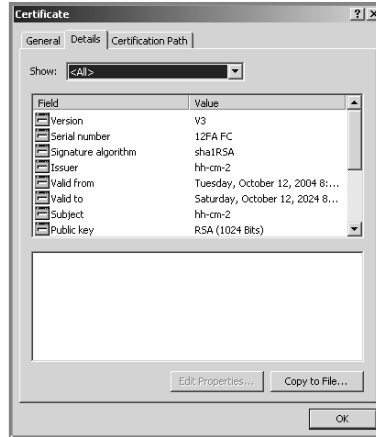
The first time that a user accesses Cisco CallManager Administration or other Cisco CallManager applications after the Cisco CallManager Release 4.1 installation or upgrade from a browser client, a Security Alert dialog box asks whether the user trusts the server. When the dialog box appears, clicking the buttons results in these actions:

- **Yes:** Trust the certificate for the current web session only. The Security Alert dialog box will display each time you access the application.
- **No:** Cancel the action. No authentication occurs, and the user cannot access the Cisco CallManager Administration pages.
- **View Certificate:** Start certificate installation tasks, so that the certificate is always trusted. After you install the certificate, the Security Alert dialog box no longer appears when you access the Cisco CallManager Administration pages.

View the Certificate in Detail

Cisco.com

- **General certificate tab shows:**
 - Issued to and by whom
 - Duration of validity
- **In the Details tab, the information can be grouped:**
 - All
 - Version 1 fields only
 - Extensions only
 - Properties only



© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-8

Click the **View Certificate** button. The Security Alert dialog box appears and the Certificate window opens. The General tab shows brief information about the certificate, such as the issuer and the validation. For more detailed information, click the **Details** tab.

Another way to get information about the certificate is to check the certificate directly on the Cisco CallManager. On the Cisco CallManager publisher, right-click the certificate name in C:\Program Files\Cisco\Certificates\httpscert.cer and choose **Open**. It is not possible to change any data in the certificate.

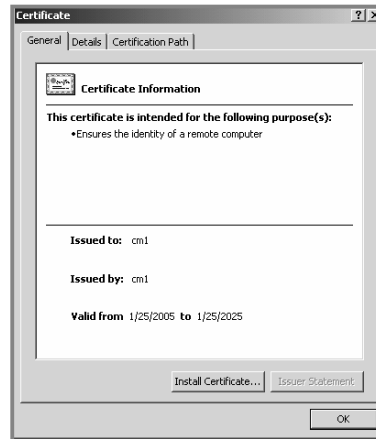
This table lists the certificate settings displayed when different options are chosen in the Show drop-down list.

All	Version 1 Fields Only	Extensions Only	Critical Extensions Only	Properties Only
<ul style="list-style-type: none"> ■ Version ■ Serial number ■ Signature algorithm ■ Issuer ■ Valid from ■ Valid to ■ Subject ■ Public key ■ Subject key installer ■ Key usage ■ Enhanced key usage ■ Thumbprint algorithm ■ Thumbprint 	<ul style="list-style-type: none"> ■ Version ■ Serial number ■ Signature algorithm ■ Issuer ■ Valid from ■ Valid to ■ Subject ■ Public key 	<ul style="list-style-type: none"> ■ Subject key installer ■ Key usage ■ Enhanced key usage 	<ul style="list-style-type: none"> ■ Critical extensions, if any 	<ul style="list-style-type: none"> ■ Thumbprint algorithm ■ Thumbprint

Install the Certificate

Cisco.com

- **Verify the certificate information.**
- **Click Install Certificate.**
- **A Certificate Import window guides the user.**
- **Select a certificate store.**



© 2005 Cisco Systems, Inc. All rights reserved.

C:PT2 v4.1—1-9

When you browse to the Cisco CallManager Administration page, the Security Alert dialog box appears. Click **View Certificate**, and the certificate window opens. Then click **Install Certificate**, and the Certificate Import Wizard opens. The wizard guides you through the installation of this certificate and asks you where to store the certificate. Choose the preselected option **Automatically Select the Certificate Store** and click **Next**. The wizard displays an overview with the selected certificate store and the content. Click **Finish**, and the wizard closes and a message shows that the import was successful.

Click **OK** in the certificate window to close it. Click **Yes** in the Security Alert dialog box, and the Cisco CallManager Administration page opens. To test the certificate installation, close the browser and access the Cisco CallManager Administration page again. If no Security Alert dialog box opens, the installation was successful.

After you have installed the certificate with the hostname of the local Cisco CallManager on your PC, the Security Alert dialog box will not appear again when you browse to Cisco CallManager Administration—although there is an exception. If you are browsing to Cisco CallManager Administration using the IP address and not the hostname, the Security Alert dialog box appears again, because the installed certificate is based on the hostname and not on the IP address.

MLA Overview

This topic describes MLA and explains compatibility and migration for MLA and Cisco CallManager.

MLA Overview

Cisco.com

- **Without MLA, there is one login for everything.**
- **Multiple levels of security are available with MLA:**
 - **Functional groups for administrative tasks**
 - **User groups for administrator hierarchy**
- **Access levels can be configured for functional groups and can vary for every user group:**
 - **No access**
 - **Read-only access**
 - **Full access**

© 2005 Cisco Systems, Inc. All rights reserved.CPT2 v4.1-1-10

Prior to the availability of MLA, there was only one administrator login. Administrators had full read and write access to Cisco CallManager configuration. An administrator could change any parameter in the database or directory that is accessible through the Cisco CallManager Administration and Cisco CallManager Serviceability pages. The entire system could be disabled with a few mouse clicks that accidentally modified data to which the user did not need access.

MLA provides multiple levels of security to Cisco CallManager Administration. Cisco CallManager menus are grouped in functional groups. Users are grouped in user groups. MLA permits you to grant only the privileges required to a selected group of users and to limit access to the configuration menu for a particular user group.

Different access levels can be assigned to each functional group, such as no access, read-only access, and full access. And of course, the access rights can be set for every configured user group. MLA also provides audit logs of user logins and of access to and modifications to Cisco CallManager configuration data.

MLA Login Authentication

Cisco.com

- **Without MLA, Cisco CallManager administrator uses local Windows NT Administrator account**
- **With MLA, usernames and passwords stored in the LDAP directory**
- **Predefined CCMAAdministrator account:**
 - **Stored in Windows registry**
 - **Encrypted password**
 - **The only user that can log in when LDAP directory is not available**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-11

Prior to the availability of MLA, Cisco CallManager administrators logged in using a local Windows NT Administrator account.

With MLA, usernames and passwords are stored in Lightweight Directory Access Protocol (LDAP) directory and provide the basis for login authentication.

During enabling, MLA creates a predefined user called CCMAAdministrator. The Windows registry stores the user ID and the encrypted password of the CCMAAdministrator user. Thus, even when the LDAP directory is unavailable, the CCMAAdministrator user can log in to Cisco CallManager Administration, because the CCMAAdministrator ID and password are the only ones that are not stored in the LDAP directory.

MLA Compatibility and Migration

Cisco.com

- **First introduction in Cisco CallManager Release 3.2(2c) and MLA 1.1(1)**
- **Included in Cisco CallManager installation with release 4.0:**
 - **Choose User > Access Rights**
 - **Disabled by default**
- **When MLA was installed separately from Cisco CallManager before release 4.0:**
 - **The configuration is migrated when updating to Cisco CallManager Release 4.0 or later.**
 - **The CCMAAdministrator password is reset.**

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-1-12

MLA was introduced with the Cisco CallManager Release 3.2(2c) and had to be separately installed. For interoperability with Cisco CallManager releases earlier than release 4.0, check the Cisco CallManager Compatibility Matrix at:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm.

With Cisco CallManager Release 4.0 and later, MLA is integrated in Cisco CallManager but disabled by default.

When you are updating Cisco CallManager to release 4.0 or later, the existing MLA version is migrated and MLA will be enabled.

Note After an upgrade to Cisco CallManager Release 4.0 or later from either Cisco CallManager Release 3.3 or 3.2 with MLA enabled, the password for the CCMAAdministrator is reset to a random password. At the end of the upgrade, a message window displays the new CCMAAdministrator password. Use this password for the next login to Cisco CallManager Administration and then change the password.

When you browse to Cisco CallManager Administration, you will find the Access Rights option in the User menu. Choose **User > Access Rights > Configure MLA Parameters** to verify whether MLA is disabled or enabled.

Enabling MLA

This topic describes how to enable MLA on Cisco CallManager.

Enabling MLA

Cisco.com

- **Choose** User > Access Rights > Configure MLA Parameters.
- **Set Enable MultiLevelAdmin to True.**
- **The Administrator account has no access rights anymore.**
- **CCMAdministrator is the only user that can log in the first time after installation.**
- **After enabling MLA:**
 - **Restart the WWW Publishing Service.**
 - **Reopen the browser.**

© 2005 Cisco Systems, Inc. All rights reserved.CIP12 v4.1-1-13

The Enable MultiLevelAdmin enterprise parameter designates whether MLA is enabled or not. This enterprise parameter can be found in the Cisco CallManager menu User > Access Rights > Configure MLA Parameters. You can set the Enable MultiLevelAdmin parameter to True (enabled) or False (disabled); False is the default value.

When you choose True, enter a new password at the New Password for CCMAdministrator prompt and re-enter the password at the Confirm Password for CCMAdministrator prompt. Only the CCMAdministrator user can now log in to Cisco CallManager; the Windows NT Administrator account no longer has access rights to Cisco CallManager Administration.

When the Enable MultiLevelAdmin enterprise parameter value is modified, the World Wide Web Publishing Service has to be restarted. Then, reopen the browser and reauthenticate with Cisco CallManager by using the new CCMAdministrator account.

MLA Enterprise Parameter

Cisco.com

Configure the MLA parameters:

- **Enable MultiLevelAdmin.**
- **Enter the password.**
- **Specify the user base directory.**
- **Set the debug level.**
- **Configure correct access privileges for overlapping user groups and functional groups.**

Parameter Name	Parameter Value
User Group Base	ou=MultiLevelAdmin,ou=Admins,ou=cisco.com
Administrative User Base	ou=Users,ou=cisco.com
Debug Level	None
Effective Access Privileges For Overlapping User Groups	Maximum
Effective Access Privileges For Overlapping Functional Groups	Maximum
Enable MultiLevelAdmin	True
New Password for CCMAdministrator	*****
Confirm password for CCMAdministrator	*****

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-14

Browse to the MLA Enterprise Parameter Configuration window to enable MLA.

The User Group Base parameter designates the user group base that MLA uses and includes the default values to connect to DC-Directory. Also, a Netscape directory or Microsoft Active Directory can be included.

You can change the Administrative User Base parameter to make use of the Windows groups that are created in Active Directory. The Administrative User Base parameter designates the administrative user base that MLA uses and is set, by default, to the enterprise user base found in the system profile.

The Debug Level enterprise parameter designates a value that is used to set the debug level for MLA debug logs. Set this parameter as follows:

- **None:** To turn off debugging
- **Trace:** To generate trace information
- **Debug:** To generate debug information

The Debug Level enterprise parameter specifies a default value for trace. The debug log files are stored in the C:\Program Files\Cisco\Trace\MLA folder, in a file named DirAndUI???.log.

The Effective Access Privileges for Overlapping User Groups and Effective Access Privileges for Overlapping Functional Groups parameters determine the level of user access for users that belong to multiple user groups or functional groups and that have conflicting privileges. For both groups, the options are Minimum or Maximum; Maximum is the default value.

When you set the Enable MultiLevelAdmin parameter to True, the New Password for CCMAdministrator and Confirm Password for CCMAdministrator fields appear. Enter the password and click **Update** to set the parameter and refresh the window.

MLA Functional Groups

This topic describes functional groups and contrasts the default and custom-based functional group.

MLA Functional Groups

Cisco.com

- **Consist of groups of Cisco CallManager Administration pages in a functional group**
- **Two types of functional groups:**
 - **Standard groups (default), cannot be modified or deleted**
 - **Custom-based groups**
- **Each Cisco CallManager menu makes up a standard functional group**

© 2005 Cisco Systems, Inc. All rights reserved.CIP12 v4.1-1-15

A functional group consists of a collection of Cisco CallManager system administration submenus. All the web pages that compose each functional group belong to a common administrative menu. Two types of functional groups exist:

- Standard functional groups, which are the default functional groups
- Custom-based functional groups

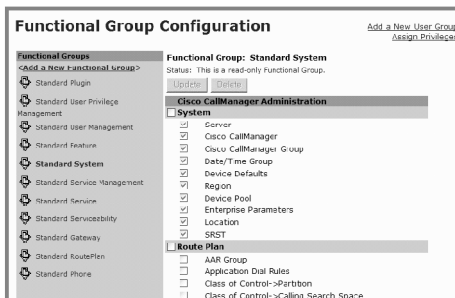
Standard functional groups are created as a part of MLA during Cisco CallManager installation and cannot be modified or deleted. Users may define their own custom-based functional groups to allow a group of administrators to access to specific Cisco CallManager Administration menus.

Functional Group Configuration

Cisco.com

Standard System functional group:

- Comprises all submenus of the Cisco CallManager System menu
- All other menus and submenu check boxes are unchecked



© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-16

When you enable Cisco CallManager MLA, a complete set of standard functional groups becomes available:

- Standard Plugin
- Standard User Privilege Management
- Standard User Management
- Standard Feature
- Standard System
- Standard Service Management
- Standard Service
- Standard Serviceability
- Standard Gateway
- Standard RoutePlan
- Standard Phone

Caution In the Standard System functional group, all submenus of the Cisco CallManager System menu, such as Server, Cisco CallManager, Cisco CallManager Group, and so on, are enabled. A user with full access rights in the Standard System functional group could, for example, change the IP address of the server. Be careful when you assign access rights to the fundamental Cisco CallManager menus.

MLA User Groups

This topic describes what an MLA user group is and how to assign privileges to different users.

MLA User Groups

Cisco.com

- **List of grouped directory users**
- **User may belong to multiple user groups:**
 - **Groups with different access rights**
 - **For overlapping access rights, determine effective privilege level in the MLA enterprise parameter configuration**
- **Assign privileges to user group**

© 2005 Cisco Systems, Inc. All rights reserved. CIP12 v4.1-1-17

A user group is a list of directory users. A user may belong to multiple user groups. With the standard installation, no users are assigned to any user group. Add users from the LDAP directory to the relevant user group in the Cisco CallManager Administration by first selecting the relevant user group and then clicking **Add a User to Group**.

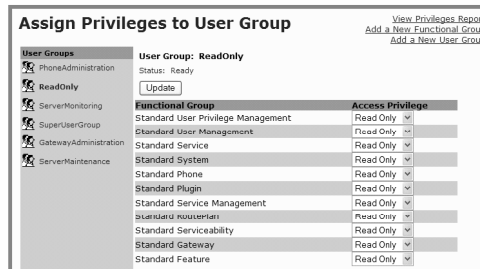
Next, proceed with assigning privileges to the user group. A user could have overlapping access rights for a functional group. The MLA Effective Access Privileges enterprise parameter determines the privilege level of a user with overlapping access rights.

Assign Privileges to User Group

Cisco.com

The privilege levels are:

- No access
- Read only
- Full access



© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-18

For each user group, one of the three privilege levels applies for access to each of the functional groups:

- **No access:** Specifies that users in a user group with this privilege level defined for a particular functional group can neither view nor change any pages that belong to that functional group.
- **Read only:** Specifies that users in a user group with this privilege level defined for a particular functional group can only view the pages that belong to that functional group; they cannot modify them. Buttons such as Insert, Delete, Update, and Reset appear dimmed to prevent modifications to database and directory data.
- **Full access:** Specifies that users in a user group with this privilege level defined for a particular functional group can view and change any page that belongs to that functional group. Users with full access privileges can perform operations such as insert, delete, update, and reset, as well as executive functions that can start or stop a process or service from Cisco CallManager Administration and Cisco CallManager Serviceability.

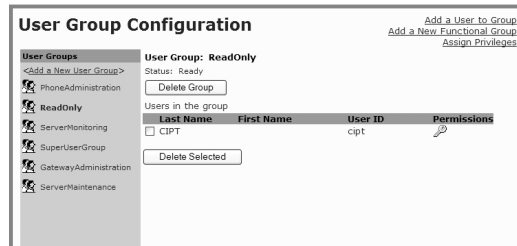
Default access privileges are assigned to each user group and for each functional group during the Cisco CallManager installation. For example, the access privileges of the ReadOnly user group are all set to Read Only.

User Group Configuration

Cisco.com

Configure user groups:

- Six standard groups are predefined.
- No users are assigned to the standard user groups.
- Create new user groups.
- Add users to the groups.



© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-19

Various user groups are predefined and have no members assigned when you enable MLA. The CCMAAdministrator user can add users to these groups, set the access rights for the user groups, and configure additional named user groups as needed. To add users, select the relevant user group and click **Add a User to Group**.

These user groups are created at the time of installation:

- PhoneAdministration
- ReadOnly
- ServerMonitoring
- SuperUserGroup
- GatewayAdministration
- ServerMaintenance

Verifying the Privileges

Cisco.com

Privileges Report [Back to Assign Privileges](#)

Functional Groups

User Groups	Standard Plugin	Standard User Privilege Management	Standard User Management	Standard Feature	Standard System
PhoneAdministration	Read Only	Read Only	Full Access	Read Only	Read Only
ReadOnly	Read Only	Read Only	Read Only	Read Only	Read Only
ServerMonitoring	Read Only	Read Only	Read Only	Read Only	Read Only
SuperUserGroup	Full Access	Full Access	Full Access	Full Access	Full Access
GatewayAdministration	Read Only	Read Only	Read Only	Read Only	Read Only
ServerMaintenance	Full Access	Read Only	Read Only	Full Access	Full Access

Functional Groups

User Groups	Standard Service Management	Standard Service	Standard Serviceability	Standard Gateway	Standard RoutePlan
PhoneAdministration	Read Only	Read Only	Read Only	Read Only	Read Only
ReadOnly	Read Only	Read Only	Read Only	Read Only	Read Only
ServerMonitoring	Read Only	Read Only	Full Access	Read Only	Read Only
SuperUserGroup	Full Access	Full Access	Full Access	Full Access	Full Access
GatewayAdministration	Read Only	Read Only	Read Only	Full Access	Full Access
ServerMaintenance	Full Access	Full Access	Read Only	Full Access	Read Only

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-1-20

After assigning access privileges, verify the configuration with the privileges report. The privileges report shows the privilege levels that are assigned to all user and functional groups in a matrix. The report displays user groups in the left column. In the other columns are the functional groups with the related access privileges for the user group.

Use this procedure to view the privileges report:

- Step 1** Choose **User > Access Rights > Assigning Privileges to User Group**. The Assign Privileges to User Group window is displayed.
- Step 2** Click **View Privileges Report**, and the Privileges Report window is displayed.

User Group Interaction

Cisco.com

User PhoneAdministration

User Group: PhoneAdministration
 Status: Ready

Functional Group	Access Privilege
Standard Service	Read Only
Standard RoutePlan	Read Only
Standard System	Read Only
Standard Plugin	Read Only
Standard Feature	Read Only
Standard Phone	Full Access
Standard User Privilege Management	Read Only
Standard Serviceability	Read Only
Standard Service Management	Read Only
Standard Gateway	Read Only
Standard User Management	Full Access

Standard Phone Functional Group Device Section

Device	Enabled
<input checked="" type="checkbox"/> CTI Route Point	
<input type="checkbox"/> Gatekeeper	
<input type="checkbox"/> Gateway	
<input checked="" type="checkbox"/> Phone	
<input type="checkbox"/> Trunk	
<input checked="" type="checkbox"/> Device Settings->Device Profile Default	
<input checked="" type="checkbox"/> Device Settings->Device Profile	
<input checked="" type="checkbox"/> Device Settings->Firmware Load Information	
<input checked="" type="checkbox"/> Device Settings->Phone Button Template	
<input checked="" type="checkbox"/> Device Settings->Softkey Template	
<input checked="" type="checkbox"/> Device Settings->CAPF Report	

User PhoneAdministration has full access to the Standard Phone functional group.
In detail: CTI Route Point, Phone, and all Device Settings submenus.

© 2005 Cisco Systems, Inc. All rights reserved. CIP72 v4.1-1-21

Users are added to a user group. In a user group, access privileges are set for each functional group. The functional group defines the Cisco CallManager menus that can be used by the relevant user group.

This example shows the items in the Device menu that are enabled for the Standard Phone functional group. The PhoneAdministration user group has full access rights to the Standard Phone functional group. This means that a user assigned to the PhoneAdministration user group can add, change, or delete the configuration of the computer telephony integration (CTI) points and phones. A user in the PhoneAdministration user group can also access all Device Settings submenus.

Creating a New Functional Group and User Group

This topic describes, with an example, how to configure a level of security so that a user can configure a Cisco Survivable Remote Site Telephony (SRST) reference and nothing else.

Creating a New Functional Group and User Group

Cisco.com

For example, create a level of security so that a user can configure only SRST references:

- 1. Create a new functional group.**
- 2. Create a new user group.**
- 3. Assign privileges.**
- 4. Verify the administration access configuration.**

© 2005 Cisco Systems, Inc. All rights reserved. CPT2 v4.1—1-22

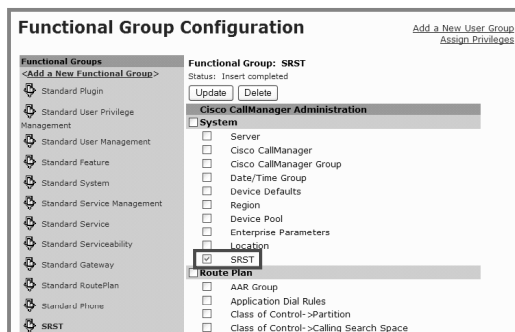
This example shows a level of security being configured. The goal in this example is to give this user access privileges that allow configuration of a Cisco SRST reference in Cisco CallManager Administration, but no other privileges:

- Step 1** Create a new functional group.
- Step 2** Create a new user group.
- Step 3** Assign the relevant privileges to the newly created user group.
- Step 4** Verify proper operation.

Adding a SRST Functional Group

Cisco.com

1. Add a new functional group.
2. Name it "SRST".
3. Select the submenu called SRST.



Follow this procedure to add a new functional group:

- Step 1** Choose **User > Access Rights > Functional Group**, and click **Add a New Functional Group**.
- Step 2** In the Functional Group Name field, enter the name of a new functional group (in this example, SRST).
- Step 3** Check the check box next to the menu that you want to include in the new functional group. In this example, check only the **SRST** check box under System, and click **Insert**.

Adding SRSTAdmin to User Group

Cisco.com

1. Add a new user group.
2. Name it SRSTAdmin.
3. Add the user called CIPT.

User Group Configuration

Add a User to Group
Add a New Functional Group
Assign Privileges

User Groups

- <Add a New User Group>
- PhoneAdministration
- ReadOnly
- ServerMonitoring
- SRSTAdmin**
- SuperUserGroup
- GatewayAdministration
- ServerMaintenance

User Group: SRSTAdmin

Status: Ready

Delete Group

Users in the group

Last Name	First Name	User ID	Permissions
		cipt	

CIPT

Delete Selected

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-24

This procedure explains how to add a new user group:

- Step 1** Choose **User > Access Rights > User Group**, and click **Add a New User Group**.
- Step 2** In the User Group Name field, enter the name of the new user group (in this example, SRSTAdmin), and click **Insert**.
- Step 3** Click **Add a User to Group**, and enter the username (which must already have been configured in Cisco CallManager Administration). In this example, the user CIPT was chosen from the directory.

Assigning Privileges to SRSTAdmin

Cisco.com

Configure the privileges of the user:

- By default, all access privileges for a new user group are “no access.”
- Set the access privilege for the SRSTAdmin user group to full access for the SRST functional group.

Assign Privileges to User Group

User Group: SRSTAdmin
status: ready

[View Privileges Report](#)
[Add a New Functional Group](#)
[Add a New User Group](#)

Functional Group	Access Privilege
Standard RoutePlan	No Access
Standard User Privilege Management	No Access
Standard Gateway	No Access
Standard Service	No Access
Standard Plugin	No Access
SRST	Full Access
Standard Serviceability	No Access
Standard Service Management	No Access
Standard System	No Access
Standard Feature	No Access
Standard User Management	No Access
Standard Phone	No Access

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-25

To assign privileges to the user group, follow this procedure:

- Step 1** Choose **User > Access Rights > Assigning Privileges to User Group**.
- Step 2** Click the name of the user group to which you want to assign privileges. In this case, the SRSTAdmin user group is chosen.
- Step 3** Choose the privilege level for each functional group within the user group. Three privilege levels are available from the drop-down list: No Access, Read Only, and Full Access. Choose **Full Access** for the functional group SRST, and click **Update**.

Verification with Privileges Report

Cisco.com

Privileges Report [Back to User Group Configuration](#)

Permissions for User: CIPT

Functional Groups					
User Groups	Standard Plugin	Standard User Privilege Management	Standard User Management	Standard Feature	Standard System
SRSTAdmin	No Access	No Access	No Access	No Access	No Access
Net Permissions	No Access	No Access	No Access	No Access	No Access

Functional Groups					
User Groups	Standard Service Management	Standard Service	Standard Serviceability	Standard Gateway	Standard RoutePlan
SRSTAdmin	No Access	No Access	No Access	No Access	No Access
Net Permissions	No Access	No Access	No Access	No Access	No Access

Functional Groups		
User Groups	Standard Phone	SRST
SRSTAdmin	No Access	Full Access
Net Permissions	No Access	Full Access

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-26

To verify whether a specific user has the correct access rights, click the **Key** symbol in the Permission column in the User Group Configuration window. In this figure, the user CIPT was chosen, and therefore the SRSTAdmin user group is displayed with the configured access rights. The privileges report shows that CIPT has no access to any functional group except the SRST group, to which it has full access.

Note Be sure to verify the values for the Effective Access Privileges for Overlapping User Groups parameter and the Effective Access Privileges for Overlapping Functional Groups parameter in the MLA parameters configuration window; access privileges do not function properly when those values conflict.

Verification with Login Testing

Cisco.com

The screenshot displays two overlapping windows from the Cisco CallManager 4.1 Administration interface. The top window, titled "Access Denied", shows a message: "Cisco CallManager 4.1 Administration. You do not have access to this page." A callout box points to this window with the text: "User attempts to open SRST menu with no access rights". The bottom window, titled "SRST Reference Configuration", shows a form for adding a new SRST reference. The form includes fields for "SRST Reference Name*", "IP Address*", "Port*" (set to 2000), "Is SRST Secure?" (checkbox), and "SRST Certificate Provider Port*" (set to 2445). The "Insert" and "Cancel" buttons are dimmed. A callout box points to these buttons with the text: "User opens SRST menu with read-only rights; Insert and Cancel buttons are dimmed".

Access Denied

Cisco CallManager 4.1 Administration
You do not have access to this page

SRST Reference Configuration

[Add New SRST Reference](#)
[Back to Find/List SRST References](#)

SRST Reference: New

Status: Ready

SRST Reference Name*

IP Address*

Port*

Is SRST Secure?

SRST Certificate Provider Port*

* indicates required item

© 2005 Cisco Systems, Inc. All rights reserved. CIPT2 v4.1-1-27

When you are testing a login and check any menu with the access privileges set to deny access, an Access Denied message is displayed by Cisco CallManager. If the user has read-only access privileges, the Insert and Cancel buttons are dimmed. In the example of user CIPT, CIPT has full access rights, so all functionalities will be available.

Verification with Login Testing (Cont.)

Cisco.com

- The user opens the SRST menu with full access rights.
- This is the expected result for the CIPT user when accessing the SRST menu.

SRST Reference Configuration

[Add New SRST Reference](#)
[Back to Find/List SRST References](#)
[Dependency Records](#)

SRST Reference: NewOne
Status: Update completed

SRST Reference Name*

IP Address*

Port*

Is SRST Secure?

SRST Certificate Provider Port*

* indicates required item

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-28

The newly configured user CIPT should have the right to configure the SRST reference only. When you browse to the SRST Reference Configuration window to verify that the user has full access rights, you see no difference from the familiar Cisco CallManager Administration window. If the Access Denied message appears or the Insert and Cancel buttons are dimmed, access privileges are not assigned properly.

The CIPT user in the example is able to insert, modify, or delete only SRST references. In this example, the SRST reference is called NewOne. The CIPT user will see an Access Denied message when browsing to any other menu in Cisco CallManager Administration.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **With HTTP, communication to Cisco CallManager is not secure; with a sniffed administrator password, a hacker has full access to the Cisco CallManager operating system.**
- **HTTPS secures the connection between the browser and IIS.**
- **With a Cisco CallManager Release 4.1 installation, Cisco CallManager creates a self-signed certificate.**
- **MLA allows you to give users different access rights for Cisco CallManager Administration.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-29

Summary (Cont.)

Cisco.com

- **MLA has to be enabled in the MLA enterprise parameters. The old administrator account will be disabled.**
- **Standard functional groups are created with the installation and can be supplemented by custom functional groups.**
- **User groups unite access privileges, functional groups, and users.**
- **The privilege report is a powerful tool to verify the access rights of a user.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-30

Preventing Toll Fraud

Overview

Business consumers have more control over their telecommunications services than ever before. New technologies provide more information and more flexibility in how businesses use their telecommunications services. Unfortunately, the shift in control has made businesses and telephone companies more susceptible to toll fraud and led to an increase in fraud. This lesson discusses ways to prevent toll fraud in a company.

Objectives

Upon completing this lesson, you will be able to take measures to prevent toll fraud. This ability includes being able to meet these objectives:

- Explain how legitimate devices can be exploited for fraudulent use of the IP PBX system to make toll calls
- Using partitions and calling search spaces, restrict call forwarding based on user classes and restrict voice-mail transfers to internal destinations
- Explain the usage of blocking commonly exploited area codes
- Configure Cisco CallManager to route calls to different locations based on the time of day when a call is made
- Design and implement FAC to require user authorization for different classes of calls
- Provide external call transfer blocking by setting service parameters and configuring gateways, trunks, and route patterns as OffNet devices
- Configure Cisco CallManager administration to drop a conference call when the conference creator leaves the call or when the last OnNet party leaves

Toll-Fraud Exploits

This topic describes toll-fraud exploits.

Exploits of Toll Fraud

Cisco.com

- **Toll fraud can occur either from inside or from outside.**
- **Misuse of company phone system is done by:**
 - **Employees placing private calls—no differentiation of business calls versus private calls is possible based on the dialed number**
 - **External attackers gaining unauthorized access to the system to exploit it**
 - **Using telephone features for private calls**
- **It is difficult to block all possibilities of toll fraud in most companies.**

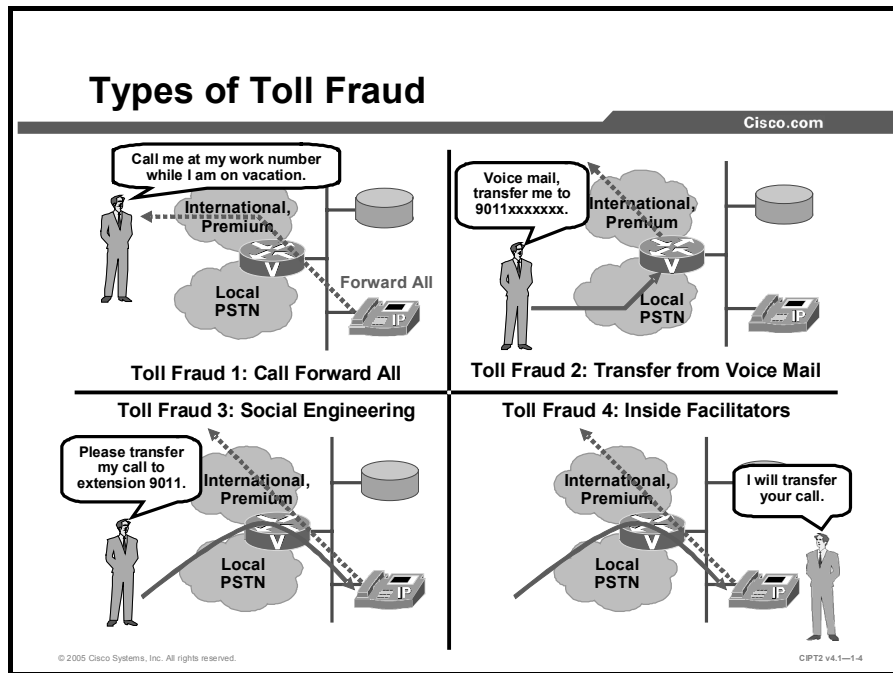
© 2005 Cisco Systems, Inc. All rights reserved. CIPT2 v4.1-1.3

A company telephony system can be subject to toll fraud by company employees or by external people who try to find vulnerabilities in the system. The first group, employees, simply ignores policies, hoping that their activities will not be detected because it is difficult to differentiate between business calls and private calls based on the dialed number. The other group of people, the external callers, is more technically oriented. They try to find vulnerabilities in network devices, including IP telephony systems. Sometimes they do not even specifically look for voice systems, they just exploit whatever system they can get control of.

The main difference between these two groups is the way in which you can mitigate the “attack.” In case of external attackers, the key is to prevent unauthorized access to the system and its devices. For authorized users of the system, the administrator has to very carefully limit the technical abilities and features of the system without compromising the flexibility and efficiency of its users.

There are also some features in a telephony system that can be misused. These include call forward and call transfer settings and voice-mail transfer options. If the features that are commonly used for toll fraud are well-protected, users may try to exploit the system using other features. As an example, if a user is not allowed to transfer an external call to another external destination, the user could try to set up a conference call for these two parties and then leave the conference.

Usually an administrator has to accept the fact that toll fraud cannot be eliminated completely. The only way to achieve complete elimination would be to block all external calls and disable all features that would allow employees to place calls to the outside the company. This technique might be feasible for single-function telephones, such as public telephones located in a lobby, but is not desirable for telephones used by standard employees. Therefore, only those calls that can be clearly identified as nonbusiness calls will be blocked. However, in many cases, you cannot judge in advance whether the call being placed is business-related or private.



This figure shows different types of toll fraud.

- **Call Forward All (CFA):** The first example describes a scenario where an employee forwards his or her office number to, for example, an international or mobile number. This employee then tells friends to call the office number. The call is forwarded to the number that the employee specified, making the company pay the costs of the calls.
- **Transfer from voice mail:** The second toll fraud example shows an attacker making an external call to the voice-mail system, which forwards the call to an international premium destination. The attacker is billed only for a local call, while the company, from which the call is forwarded, pays for the international call.
- **Social engineering:** The third example shows a scenario where an attacker calls from outside the company and uses social engineering tricks (for instance, pretending to be an employee working from home) to be transferred to an external number, such as 9011. The 9011 prefix is used in the United States to place international calls. This attacker is also charged only for a local call, while the company again pays for the connection to an international telephone number.
- **Inside facilitators:** The fourth example is very similar to the third one. But in this case, an employee inside the company transfers the external call to another external number. In this case the toll fraud has an internal source.

Restricting Call Forward All and Voice Mail Using Calling Search Spaces

This topic describes how to restrict forwarding with calling search spaces.

Call Forward All Exploits

Cisco.com

- Forward the office phone number to the home phone number and have others call toll-free number for the office.
- Forward the office phone number to a hotel phone number in foreign country while on vacation there.
- Forward the office phone number to an international phone number to make an international call.
- Exploits can be avoided by CFA restrictions.

© 2005 Cisco Systems, Inc. All rights reserved. CIPT2 v4.1-1-6

Call Forward All (CFA) is a feature in Cisco CallManager that allows an internal number (for example, an employee office number) to be forwarded to an external number (for example, an international number, mobile number, or premium number).

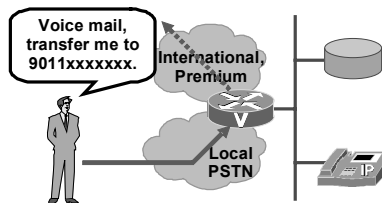
An employee can, for example, call his or her own office number, which is then forwarded to the number specified in the forwarding field. This number can be an international or premium number. The setting can be configured using the web interface, so the forwarding configuration can be set up and removed very easily from home or elsewhere.

CFA exploits can be avoided by applying a calling search space to the CFA feature.

Voice Mail Forwarding Exploits

Cisco.com

- The voice-mail system can allow a caller to be transferred to an extension.
- If callers can enter the number to which they want to be transferred, they could try dialing external numbers, such as international or premium.
- Exploits can be avoided by voice-mail port restrictions.



© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-1-6

Voice-mail systems, which can transfer a call to an extension, can be misused in a similar way, if they are configured to allow transfer of calls when the called party is not available and redirection of the call to the voice-mail system. If such transfers are not limited, a caller could connect to the voice-mail system by a local call and then transfer to the public telephony network (for example, a long-distance number). Voice-mail forwarding exploits can be avoided by applying a calling search space to the voice-mail port in the Cisco CallManager configuration.

Steps to Restrict Forwarding

Cisco.com

- **Steps to restrict Call Forward All:**
 1. **Create partitions.**
 2. **Create calling search spaces.**
 3. **Assign calling search spaces to the IP Phone Forward All field.**
- **Steps to restrict Voice-Mail Forward:**
 1. **Create a partition for voice mail ports.**
 2. **Create a calling search space.**
 3. **Assign the calling search space to the IP Phone Voicemail Forward field.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1.7

When you are restricting call forwarding with Cisco CallManager, you must configure partitions and calling search spaces if you have not already done so.

These are the steps to restrict CFA:

- Step 1** Create separate partitions for different types of calls (such as internal numbers, local numbers, and long-distance numbers) and attach the corresponding route patterns.
- Step 2** Create calling search spaces and put the partitions into the calling search spaces.
- Step 3** Assign the calling search spaces to the Cisco IP Phone Forward All field to restrict or allow call forwarding to different numbers.

The steps to configure voice-mail forwarding restrictions are very similar to configuring the Forward All field of the Cisco IP Phone:

- Step 1** Create a partition and place all voice-mail ports in it.
- Step 2** Create a calling search space and put the partition with the voice-mail ports in this calling search space.
- Step 3** Assign the calling search space to the Voice-Mail Forward field so that the voice-mail ports can call only other voice-mail ports.

Call Forward All Restriction Example

Cisco.com

calling search space	Partition	Allowed Destinations
Executives_and_Manager	Internal	Internal DNs
	Local	Local DNs
	Long-Distance	Long-distance DNs
General	Internal	Internal DNs

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-1-0

Partitions facilitate call routing by dividing the route plan into logical subsets that are based on organization, location, and call type.

This figure shows three partitions:

- The Internal partitions contain all directory numbers (DNs) within the company.
- The Local partition contains a route pattern that allows only local calls.
- The Long-Distance partition contains route patterns that allow long-distance calls.

A phone that has the Executives_and_Manager calling search space applied for CFA has more possibilities to forward calls than a phone where the General calling search space is configured.

To protect against toll fraud, partitions and calling search spaces are used to block or allow calls for different users (for example, general employees and managers) in different scenarios. These scenarios include these:

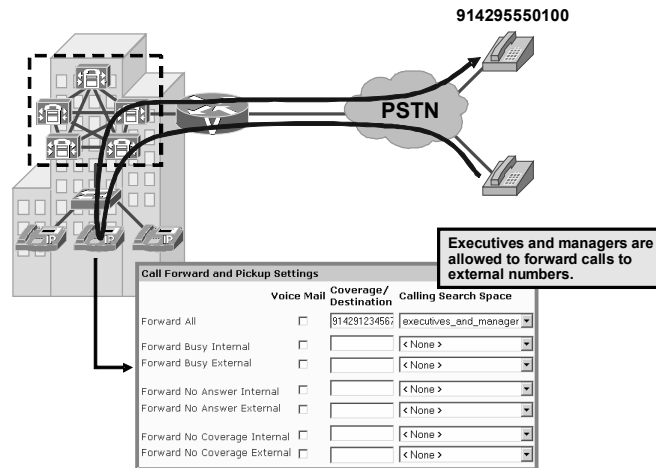
- Normal calls
- Call Forward All
- Voice-mail ports

Example

The administrator has configured a calling search space called “General” for the Forward All field on phone A. This calling search space allows calls made to the DN of phone A to be forwarded only to internal destinations. An attempt to forward a call to phone A to an external destination will give the caller a busy signal because forwarding to the external destination is restricted through the General calling search space.

Call Forward All Restriction Example—Permitted Call

Cisco.com



The Forward All field can be found in the line configuration options for either a telephone or a device profile. The telephone number to which the calls are forwarded can be configured using the CFwdAll softkey on the Cisco IP Phone or the Cisco CallManager User Options web interface.

Note The user website can be found at <https://<CCM Publisher Server name or IP address>/CCMUser>.

When the Executives_and_Manager calling search space is assigned to the Forward All field of an IP Phone, this phone is allowed to forward a call to an internal or external destination. In this example, a call is forwarded to telephone number 914295550100.

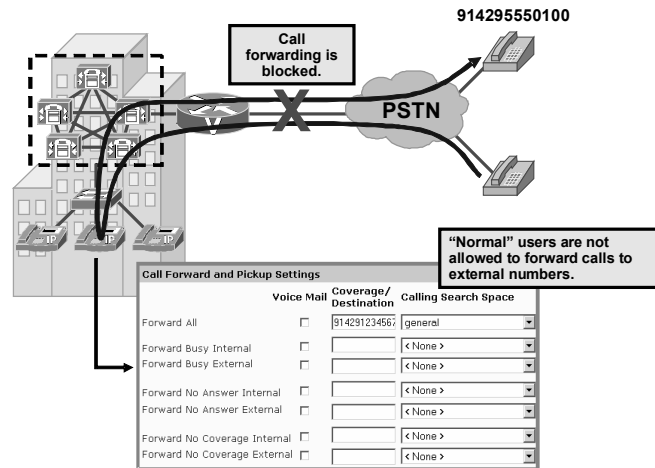
If a call is routed to 914295550100, the route pattern in the Long-Distance partition matches, and the call is routed through the gateway to the public switched telephone network (PSTN) destination.

Example

Phone B has the Executives_and_Manager calling search space configured in the Forward All field. This calling search space allows the user to forward calls to either internal or external destinations but not to international numbers. When an attempt is made to forward a call made to the DN of phone B to a national destination, the call will be forwarded. But when an attempt is made to forward a call made to the DN of phone B to an international number, forwarding is restricted.

Call Forward All Restriction Example—Denied Call

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1—1-10

In this example, the General calling search space is used. Call forwarding to the external number 914295550100 is restricted. Someone calling the number receives a busy tone. The call is not forwarded to the external destination because the General calling search space contains only the Internal partition, which points to all internal numbers but not to any external number.

Voice-Mail Port Restrictions—Example

Cisco.com

Use partitions and calling search spaces to restrict calls to and from voice-mail ports:

- Partition “voicemail_ports” allows calls to the voice-mail system only from devices that have this partition in their calling search space.
- Calling search space “voicemail” defines permitted targets for calls coming from the voice-mail system.

Cisco Voice Mail Port Configuration

Cisco Voice Mail Port: CiscoUM1-V12 (Voicemail)
Registration: Unknown
IP Address:
Status: Ready
Copy Update Delete Reset Port

Device Information

Port Name*	CiscoUM1-V12
Description	Voicemail
Device Pool*	Default
Calling Search Space	voicemail
AAR Calling Search Space	voicemail
Location	< None >

Directory Number Information

Directory Number*	501
Partition	voicemail_ports
Calling Search Space	voicemail
AAR Group	< None >
Display (Internal Caller ID)	Voicemail
External Number Mask	

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1—1-11

Restricting voice-mail forwarding is very similar to the Forward All field configuration for IP Phones. In this case, all voice-mail ports are placed in the voicemail_ports partition. The calling search space named “voicemail” will include only partitions with internal DNs. Therefore, if the voice-mail system routes a call back to Cisco CallManager, the calling search space of the voice-mail port will define where the call is allowed to be routed. In the example shown, the calling search space voicemail allows calls to be routed to internal numbers only.

Blocking Commonly Exploited Area Codes

This topic describes calls to area codes commonly exploited in toll fraud.

[Cisco.com](#)

Block Commonly Exploited Area Codes

Create a unique route pattern or general route pattern with a route filter for each area code to block.

Use partitions and calling search spaces to create different restriction levels.

Block all numbers that are not needed according to company policies or that simply are not used.

[Add a New Route P.](#)
[Back to Find/List Route Pa](#)

Route Pattern Configuration

Route Pattern:
Status: Ready
Note: Any update to this Route Pattern automatically resets the associated gateway or Route List
[Copy](#) [Update](#) [Delete](#)

Pattern Definition

Route Pattern*	91242XXXXXX	
Partition	Internal	
Description	Block Calls to Bahamas	
Numbering Plan*	North American Numbering Plan	
Route Filter	<None>	
MLPP Precedence	Default	
Gateway or Route List*	[S]/DS1-9@SDA000E3879D34F (Edit)	
Route Option	<input type="checkbox"/> Route this pattern <input checked="" type="checkbox"/> Block this pattern <input type="checkbox"/> Call Rejected	
Call Classification*	Other	
<input checked="" type="checkbox"/> Provide Outside Dial Tone	<input type="checkbox"/> Allow Overlap Sending	<input type="checkbox"/> Allow Device Override
<input type="checkbox"/> Require Forced Authorization Code		<input type="checkbox"/> Urgent Priority
Authorization Level	0	
<input type="checkbox"/> Require Client Matter Code		

When blocking commonly exploited area codes, create a unique route pattern for each area code that you want to block. You can create different restriction levels; for example, general employees are not allowed to call these numbers, but executives and managers are allowed to. Use different route filters, partitions, and calling search spaces to generate restriction levels. As a general recommendation to prevent toll fraud, you should block as many numbers as possible. In this example, all calls to the Bahamas are blocked. For each number that you want to block, create a route pattern that explicitly blocks the number. Often the decision as to whether a number should be blocked or allowed depends on company policies or simply on whether it is necessary to call the number.

Note The ability to block frequently exploited area codes applies to the United States and Canada only as it requires a dial plan, such as the North American Numbering Plan (NANP).

Examples of Commonly Exploited Area Codes

Cisco.com

Country	Area Code	Blocked Cisco CallManager Pattern	Country	Area Code	Blocked Cisco CallManager Pattern
Anguilla	264	9.1264xxxxxx	Jamaica	876	9.1876xxxxxx
Antigua/ Barbuda	268	9.1268xxxxxx	Montserrat	664	9.1664xxxxxx
Bahamas	242	9.1242xxxxxx	Puerto Rico	787	9.1787xxxxxx
Barbados	246	9.1246xxxxxx	St. Kitts & Nevis	869	9.1869xxxxxx
Bermuda	441	9.1441xxxxxx	St. Lucia	758	9.1758xxxxxx
British Virgin Islands	284	9.1284xxxxxx	St. Vincent & the Grenadines	784	9.1784xxxxxx
Cayman Islands	345	9.1345xxxxxx	Toll Charge	900 976	9.1900xxxxxx 9.1976xxxxxx
Dominica	767	9.1767xxxxxx	Trinidad & Tobago	868	9.1868xxxxxx
Dominican Republic	809	9.1809xxxxxx	Turks & Caicos Islands	649	9.1649xxxxxx
Grenada	473	9.1473xxxxxx	U.S. Virgin Islands	340	9.1242xxxxxx

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-1-13

The figure shows some of the most commonly exploited area codes that you might want to block. It is not an exhaustive list, and some of these area codes may not apply to your organization.

In the worldwide country code numbering scheme, there are several countries that do not use their own country codes.

These numbers have the same format as the NANP—[access code] [area code] [number] (for example, 9.142xxxxxx)—but a call to one of these destinations results in an international toll charge.

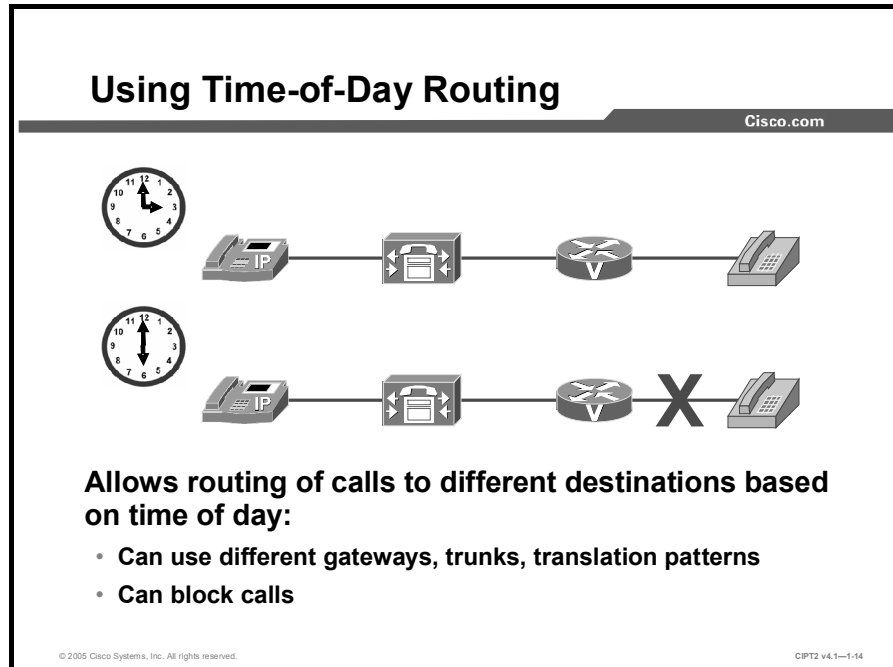
Administrators should make sure that all of the devices in the IP telephony network can reach only the destinations that they should be able to reach. For example, a lobby phone should not be able to call international numbers. In situations where individuals in your organization have legitimate business in one of these countries, the recommendation is to explicitly configure route patterns that will match those businesses, while still blocking the area code as a whole.

Example

In a company, customers can use a lobby phone to make internal and local calls. A customer calls the number 917675550100. It seems to be a long-distance call within the country, but it is actually an international call to Dominica, and the company will be charged for an international call. To prevent these frauds, create a route pattern that blocks calls to 91767xxxxxx.

Using Time-of-Day Routing

This topic describes configuring time-of-day routing to allow or restrict calls for a specific time of day.



With the 4.1 release of Cisco CallManager, time-of-day routing routes calls to different locations based on the time of day when a call is made. For example, during business hours, the calls can be routed to an office, while after business hours the calls can go directly to a voice-messaging system or to a home number.

Time-of-day routing can be used for other purposes as well. With time-of-day routing, a least-cost routing system can be designed to choose the cheapest provider for a specific time of day. For example, assume that there are two telephony providers, ABC and XYZ. Between 8 a.m. and 1 p.m., provider ABC is the cheaper provider, so Cisco CallManager routes calls over this provider during that period. After 1 p.m., provider XYZ becomes the cheaper, so the Cisco CallManager uses this provider then.

Time-of-Day Routing

Cisco.com

Partitions are extended by a time-configuration attribute:

- **Route patterns and translation patterns are applied to partitions (as before).**
- **The partitions in the calling search space are available based on time-of-day settings.**

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1—1-15

Time-of-day routing comprises individual time periods that the administrator defines and groups into time schedules. The administrator associates time schedules with a partition. In the Partition Configuration window, the administrator chooses either the time zone of the originating device or any specific time zone for a time schedule. Route or translation patterns are applied to partitions as before, when route or translation patterns configured without time-of-day routing. The system checks the chosen time zone against the time schedule when the call is placed to DN's in this partition. The Time Period and Time Schedule menu items are located in the Route Plan menu under the Class of Control submenu in Cisco CallManager.

Steps to Configure Time-of-Day Routing

Cisco.com

1. **Configure a time period.**
2. **Configure a time schedule.**
3. **Assign the time schedule to a partition.**
4. **Assign the partition to a calling search space.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1—1-16

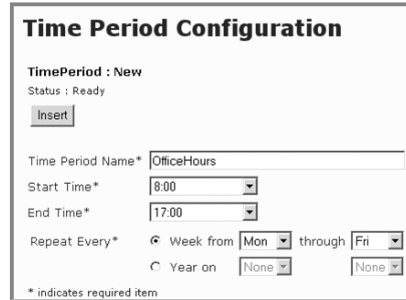
When configuring time of day routing, complete these steps:

- Step 1** Define a time period when time-of-day routing should be used.
- Step 2** Combine several time periods into the time schedule configuration.
- Step 3** Assign the time schedule to a partition that should be used for time-of-day routing.
- Step 4** After preparing the partitions, assign them to a calling search space, if you have not already done so.

Time Period Configuration

Cisco.com

- Can be configured at **Route Plan > Class of Control** on Cisco CallManager
- Specific time ranges:
 - Time period name
 - Time interval
 - Repetition interval
- Will be assigned to partitions



© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-1-17

Choose **Route Plan > Class of Control** to configure time-of-day routing on Cisco CallManager. The time period configuration contains the following:

- Time Period Name field
 - The name of the time period. The name can contain up to 50 alphanumeric characters and any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each time period name is unique to the plan.

Note Use concise and descriptive names for time periods. The hours_or_days format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a time period. For example, "office_M_to_F" identifies a time period for the business hours of an office from Monday to Friday.

- Time interval
 - Start Time field
 - From the drop-down list, choose the time when this time period starts. The available start times consist of 15-minute intervals throughout a 24-hour period.
 - The default value is No Office Hours.

Note To start a time period at midnight, choose the value 0:00.

- End Time field
 - From the drop-down list, choose the time when this time period ends. The available end times consist of 15-minute intervals throughout a 24-hour period.
 - The default value is No Office Hours.

Note The end time must be later than the start time. To end a time period at midnight, choose the value 24:00.

- No Office Hours is an option in the Start Time and End Time fields; this value means that the selected partition will not be active for the defined days of the week or year.
- Repetition interval
 - Week From: Use the Week From and Through drop-down lists to choose the days of the week when the time period applies. The following are examples:
 - Choose a Week From value of Mon(day) and a Through value of Fri(day) to define a time period that applies from Monday to Friday.
 - Choose a Week From value of Sat(urday) and a Through value of Sat(urday) to define a time period that applies only on Saturdays.
 - Year On: Use the drop-down lists to choose the month and day of the year when the time period applies. The following is an example:
 - Choose the month Jan(uary) and the day 1 to define a time period that applies yearly on New Year's Day.

The time period (in this example, OfficeHours) is assigned to all route patterns that should use it.

The table lists some examples of time period configuration.

Examples of Time Period Configuration

Time Period Name	Start Time	End Time	Repeat Every
weekdayofficehours	8:00	17:00	Monday through Friday
newyearsday	0:00	24:00	January 1
noofficehours	No Office Hours	No Office Hours	Wednesday

Adding a Time Period

When adding a time period, complete these steps:

- Step 1** From the menu bar, choose **Route Plan > Class of Control > Time Period**.
- Step 2** Click **Add a New Time Period**.
- Step 3** Enter the appropriate settings as described in the table. All settings in the table are examples and should be changed according to your needs.
- Step 4** Click **Insert** to add the new time period.

Repeat Steps 2 to 4 to add more time periods.

Time Schedule Configuration

Cisco.com

- The time schedule is a list of one or more time periods.
- All selected time period configurations are combined to calculate the active time interval.
- The same time period can be associated with multiple time schedules.

Time Schedule Configuration

Time Schedule: TimeSchedule_SanJose
Status: Insert completed
Copy Update Delete

Time Schedule Information

Time Schedule Name* TimeSchedule_SanJose

Time Periods for this Time Schedule

Available Time Periods
ThanksGivingDay

Selected Time Periods*
OfficeHours
Holiday

* indicates required item

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-1-18

A time schedule consists of a group of defined time periods. Enter a name in the Time Schedule Name field. The name can contain up to 50 alphanumeric characters and any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each time schedule name is unique to the plan. After you have configured a time period, the time period is displayed in the Available Time Periods pane in the Time Schedule Configuration window. You can select a time period and add it to the Selected Time Periods pane by clicking the Down arrow. To remove a time period, select the time period in the Selected Time Periods pane and click the Up arrow.

Note After you select a time period for association with a time schedule, the time period remains available for association with other time schedules.

Examples

This example presents a procedure for configuring a time schedule for the United States.

Define the time schedule TimeSchedule_SanJose as a group of these time periods: newyearsday, presidentsday, memorialday, independenceday, laborday, thanksgivingday, and christmasday. You must first configure the applicable time periods. Next, add a time period for office hours, for example, from Monday to Friday.

Adding a Time Schedule

To add a time schedule, complete these steps:

Step 1 From the menu bar, choose **Route Plan > Class of Control > Time Schedule**.

Step 2 Click **Add a New Time Schedule**.

Step 3 Click **Insert** to add the new time schedule.

Repeat Steps 2 and 3 to add more time schedules.

Partition Configuration

Cisco.com

- A partition can be associated with a time schedule.
- By default, the partition is not associated with any time schedule.
- The administrator can specify the time zone to be used.
- The time schedule ensures that partitions are active or visible only at certain times.

Partition Configuration

Partition: working_hours_sj
Status: Ready
Update Delete Restart Devices

Partition Name* working_hours_sj
Description working hours in SanJose
Time Schedule TimeSchedule_SanJose

Time Zone Originating Device Specific Time Zone
(GMT) Monrovia, Casablanca
(GMT) Monrovia, Casablanca
(GMT+01:00) Amsterdam, Berlin, Stockholm, Rome, Bern, Vienna
(GMT+02:00) Athens, Helsinki, Istanbul
(GMT+02:00) Cairo
(GMT+02:00) Eastern Europe
(GMT+01:00) Brussels, Paris, Madrid, Copenhagen
(GMT+01:00) Prague, Warsaw, Budapest
(GMT+02:00) Harare, Pretoria
(GMT+02:00) Israel
(GMT+03:00) Baghdad, Kuwait, Nairobi, Djibouti
(GMT+03:00) Moscow, St. Petersburg, Kazan, Volgograd

* indicates required item

After you have configured a time schedule, you can use the Partition Configuration window to select either the time zone of the originating device or any specific time zone for a defined time schedule. The selected time zone is checked against the time schedule when the user places the call.

The time-of-day feature filters the calling search space string through time-of-day settings that are defined for each partition in the calling search space.

When time-of-day routing is configured, if the time of an incoming call is within one of the time periods in the time schedule, the partition is included in the filtered partition list search for the call.

When you activate time-of-day routing for a partition, the specified time ranges in the time schedule make partitions active or visible only at certain times.

Time Schedule

From the drop-down list in the Partition Configuration window, choose a time schedule to associate with this partition. The associated time schedule specifies when the partition is available.

The default value is None, which implies that time-of-day routing is not in effect and the partition remains active at all times.

In combination with the Time Zone value, association of a partition with a time schedule configures the partition for time-of-day routing. The system checks incoming calls to this partition against the specified time schedule.

Time Zone

Choose one of these options to associate a partition with a time zone:

- **Originating Device:** If this radio button is selected, the system checks the partition against the associated time schedule with the time zone of the calling device.
- **Specific Time Zone:** If this radio button is selected, choose a time zone from the drop-down list.

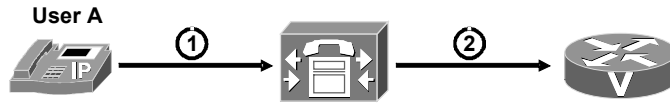
The system checks the partition against the associated time schedule at the time that is specified in the specified time zone.

The options shown in the figure all specify the time zone. When there is an incoming call, the current time on Cisco CallManager is converted to the specific time zone set when one of the options was chosen. This specific time is validated against the value in the Time Schedule field.

Note For time-of-day routing, a special timer can be configured. The Time Of Day Initialization Timer parameter specifies the time in seconds to allow the TODManager to initialize. If initialization does not complete within the specified time, Cisco CallManager restarts. The Time Of Day Initialization Timer parameter is a required field. The default value for the timer is 900 seconds. The value range for the timer is from 10 to 1200 seconds. To change the Time Of Day Initialization Timer parameter on Cisco CallManager, choose Service > Service Parameters > Cisco CallManager.

Time-of-Day Routing Example

Cisco.com



1. Phone A dials 9011442088248000.
2. Cisco CallManager extends call to VoIP gateway.

Partition CiscoGW → US Hours
Time Schedule: US Hours → Time Period: Office Hours and Holiday
Time Period: Office Hours → 8:00 a.m. – 5:00 p.m. Monday through Friday
Time Period: Holiday → No Office Hours Dec 25th



Friday
3:00 pm

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-20

If time-of-day routing is enforced, users cannot set certain CFA numbers at certain times, place calls, and so on.

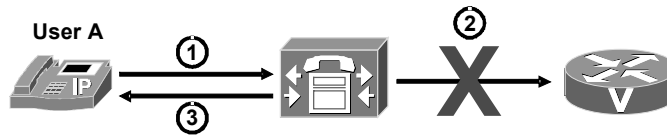
Example

Calling search space forwarding from user A includes a time-of-day configured partition that allows international calls from 8:00 a.m. to 5:00 p.m. User A wants to configure the CFA number to an international number. User A can set this number only during the 8:00 a.m.-to-5:00 p.m. time period because outside these hours the system does not find the international number in the partition that is used to validate the CFA number.

If user A sets the CFA during office hours, when it is allowed, and receives a call outside office hours, the caller hears a fast busy tone.

Time-of-Day Routing Example (Cont.)

Cisco.com



1. Phone A dials 9011442088248000.
2. Cisco CallManager rejects the call because it is made after 5:00 p.m.
3. Cisco CallManager plays a fast busy tone.

Partition CiscoGW → US Hours
Time Schedule: US Hours → Time Period: Office Hours and Holiday
Time Period: Office Hours → 8:00 a.m. – 5:00 p.m. Monday through Friday
Time Period: Holiday → No Office Hours Dec 25th



Friday
6:00 pm

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-1-21

In the second example, the call is placed at 6 p.m. The call is rejected because it is outside office hours, which are specified as between 8:00 a.m. and 5:00 p.m., Monday through Friday. The user will hear a fast busy tone that indicates that the call is rejected.

Using FAC

This topic describes using Forced Authorization Codes (FAC) and Client Matter Codes (CMC) to regulate types of calls.

Using FAC

Cisco.com

- **Prevents users from making unauthorized calls**
- **Sensitive destinations can be “secured” with a FAC**
- **Route patterns configured with FAC play a tone and request a FAC to be entered:**
 - **Route pattern configuration specifies minimum level of accepted codes**
- **Usage of FAC is written to CDR**

© 2005 Cisco Systems, Inc. All rights reserved. CIP12 v4.1-1.22

FAC became available in Cisco CallManager Release 3.3(4). It is not included in Cisco CallManager Release 4.0 but has been included since Cisco CallManager Release 4.1. In Cisco CallManager Administration, various levels of authorization can be configured. With FAC, sensitive destinations can be “secured” by requiring use of authorization codes for such destinations. When a call is routed through a FAC-enabled route pattern Cisco CallManager plays a tone and requests an authorization code. If the authorization code entered by the user does not meet or exceed the level of authorization that is specified to route the dialed number, the user receives a reorder tone. If the authorization is accepted, the call is routed. The authorization is logged to Call Detail Records (CDRs) so that the information can be used by CDR Analysis and Reporting (CAR) to generate reports for accounting and billing.

FAC is useful for colleges and universities or any business or organization for which limiting access to specific classes of calls proves beneficial. An additional benefit is that when you assign unique authorization codes, the users who can place calls can be determined. For example, for each user, a unique authorization code can be specified.

Enable FAC for relevant route patterns by checking the appropriate check box and specifying the minimum authorization level for calls through that route pattern. After updating the route patterns in Cisco CallManager Administration, the dial-plan documents have to be updated to define the FAC-enabled route patterns and configured authorization level.

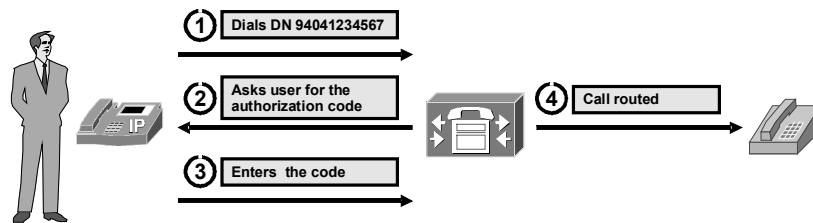
To implement FAC, devise a list of authorization levels and corresponding descriptions to define the levels. Authorization levels must be specified in the range of 0 to 255. Cisco allows authorization levels to be arbitrary, so define what the numbers mean for your organization. Before defining the levels, review the following examples of levels that can be configured for a system:

- Configure an authorization level of 10 for intrastate long-distance calls in North America.
- Because interstate calls often cost more than intrastate calls, configure an authorization level of 20 for interstate long-distance calls in North America.
- Configure an authorization level of 30 for international calls.

Tip Incrementing authorization levels by 10 establishes a structure that provides scalability when more authorization codes need to be added. The range for authorization codes is from 0 to 255.

Example of FAC

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-23

The FAC feature allows regulation of the types of calls that certain users can place. It forces the user to enter a valid authorization code on the IP Phone before the call can be completed.

The FAC feature requires making changes to route patterns and updating dial-plan documents to reflect whether FAC is enabled or disabled for each route pattern.

Configure FAC

Cisco.com

1. **Design and document the system:**
 - **Current dial-plan design**
 - **Client matter codes**
 - **Authorization levels**
 - **Update dial-plan documentation**
2. **Create authorization codes and assign a level to them.**
3. **Apply FAC to the desired route patterns.**
4. **Provide the user with all the necessary information.**

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-1-24

These steps should be used as a configuration checklist when you are configuring FAC:

Step 1 Design and document the system (for example, document a list of destinations that need to be tracked). Update the dial-plan documents or keep a printout of the Cisco Bulk Administration Tool (BAT) comma-separated values (CSV) file with them.

Step 2 Insert the codes using Cisco CallManager Administration or BAT.

Tip Consider using BAT for small or large batches of codes; the CSV file in BAT can serve as a blueprint for the codes, corresponding names, corresponding levels, and so on.

Step 3 To enable FAC, add or update route patterns in Cisco CallManager Administration.

Step 4 Provide all necessary information (for example, the codes) to users and explain how the features work.

FAC Configuration

Cisco.com

- Go to FAC configuration window in Cisco CallManager Administration: **Feature > Forced Authorization Code**.
- Authorization code name is displayed in the CDRs.

Forced Authorization Code: 600

Status :Ready

Update Delete

Forced Authorization Code Information

Authorization Code Name* International

Authorization Code* 600

Authorization Level* 30

* indicates required item

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-25

In Cisco CallManager Administration, choose **Feature > Forced Authorization Code**. In the newly opened window there are three parameters, as described in the table.

Configuration Settings for FAC

Parameter	Description
Authorization Code Name	Enter a unique name that is no more than 50 characters. This name ties the authorization code to a specific user or group of users; this name is displayed in the CDRs for calls that use this code.
Authorization Code	Enter a unique authorization code that is no more than 16 digits. The user enters this code when placing a call through a FAC-enabled route pattern.
Authorization Level	Enter a three-digit authorization level in the range of 0 to 255; the default is 0. The level that is assigned to the authorization code determines whether the user can route calls through FAC-enabled route patterns.

In the figure, the code created must be entered for all international calls. The authorization code, 600, must be entered by any user who calls an international destination. If the code entered by the user matches the configured authorization code, the authorization level is checked. To route a call, the user authorization level must be equal to or greater than the authorization level that is specified for the route pattern for the call.

When user X places an international call that matches route pattern A (which requests an authorization level of 20 or higher), user X enters the authorization code 600 and the call is placed, because the route pattern has a lower authorization level than the authorization level configured (in this example, 30). If user X places a long-distance call that matches route pattern B (authorization level of 10), user X can enter the authorization code 600 once more and the call is routed because the authorization code of the route pattern is again lower.

Client Matter Codes

Cisco.com

- **CMC allows you to distinguish between private and business calls and can be applied on sensitive route patterns:**
 - **Forces the user to flag call with a client matter code**
 - **Code is then written into CDR**
- **CMC allows reports about private calls.**
- **CMC does not prevent users from marking private calls as business calls.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-26

Client Matter Codes (CMC) can also be used by companies to keep track of private calls placed by their employees. For example, a company could allow employees to place private calls using the company telephony infrastructure but require the employee to pay the cost. External route patterns (for example, those for long distance and international calls and those for the 900 area code) can be configured to request a client matter code to be entered and, therefore, to be logged accordingly.

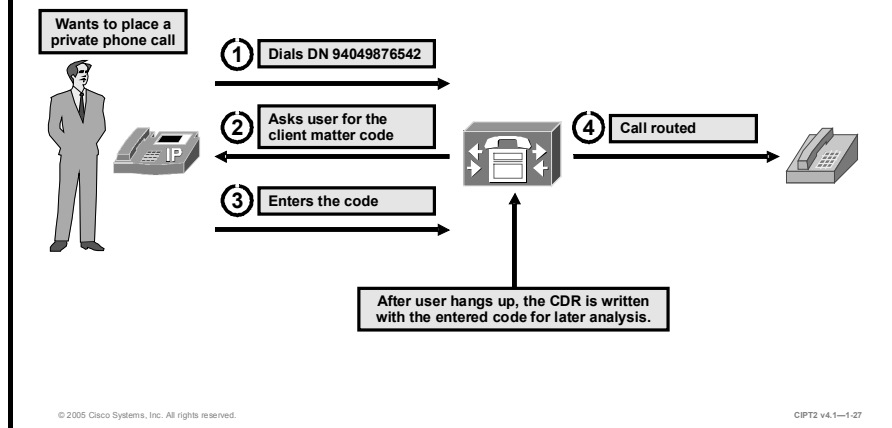
This feature does not prevent users from making private calls using business telephones, but it allows a company to have a policy that does not deny private calls in general but requests that users identify them as such and pay for them. In both situations (denying private calls in general or permitting them if properly flagged) additional tools (logging, reporting) are needed to detect improper usage.

When CMC is configured, users hear a tone prompting them to enter any valid client matter code. The CDR will include the code that is entered for later processing.

CMC was first available in Cisco CallManager Release 3.3(4). It is not included in Cisco CallManager Release 4.0 but has been included since Cisco CallManager Release 4.1.

Client Matter Codes (Cont.)

Cisco.com



When the CMC feature is enabled, users must enter a client matter code to reach certain dialed numbers. CMC is enabled and disabled through route patterns, and multiple codes can be configured. When a user dials a number that is routed through a CMC-enabled route pattern, a tone prompts the user for the client matter code. If the user enters a valid code, the call is routed; if the user enters an invalid code, reorder occurs. The code is written to the CDR, so the information can be collected by using CAR, and you can generate reports for client accounting and billing.

Configure Route Patterns to Use FAC and CMC

Cisco.com

- Choose Route Plan > Route/Hunt > Route Pattern in Cisco CallManager.
- Check the Required Forced Authorization Code box and insert a FAC level.
- Check the Require Client Matter Code box to use client matter codes.

Route Pattern Configuration

Route Pattern: 904.XXXXX

Status: Insert completed
Note: Any update to this Route Pattern automatically resets the associated gateway or Route List

Copy Update Delete

Pattern Definition

Route Pattern* 904.XXXXX

Partition <None>

Description Site2 with CMC/FAC

Numbering Plan* North American Numbering Plan

Route Filter <None>

MLPP Precedence Default

Gateway or Route List* ICT_u_CM22 (Edit)

Route Option

Route this pattern

Block this pattern --NotSelected--

Call Classification* OffNet

Provide Outside Dial Tone Allow Overlap Sending Allow Device Override Urgent Priority

Require Forced Authorization Code

Authorization Level 20

Require Client Matter Code

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-28

To configure FAC in route patterns, complete these steps:

- Step 1** In Cisco CallManager Administration, choose **Route Plan > Route/Hunt > Route Pattern**.
- Step 2** In the Route Pattern Configuration window, check the **Require Forced Authorization Code** check box.
- Step 3** In the Authorization Level field, enter the authorization level for the route pattern. The number that is specified in this field determines the minimum authorization level that is needed to successfully route a call through this route pattern.

Tip Even if the Require Forced Authorization Code check box is not checked, the authorization level can still be specified because the database stores the level even if the feature itself is currently deactivated.

After the features are configured, communicate the necessary information to users:

- Inform users about restrictions.
- Provide users with all information needed to use the features (for example, authorization code, authorization level, and client matter codes). Inform users that dialing a number produces a tone that prompts for the codes.
- Advise users of the types of calls that they can place; before users notify the phone administrator about a problem, users should hang up and retry the dialed number and code.
- Inform users that they can start entering the code before the tone completes.
- To immediately route the call after the user enters the code, the user can press # on the phone. Otherwise the call is routed after the interdigit timer (T302) expires, which equals 15 seconds by default.

- The phone plays a reorder tone when a user enters an invalid code. If a user misdials the code, the user must hang up and try the call again. If the reorder tone persists, the user should notify the phone or system administrator that a problem may exist with the code.

Note When FAC and CMC are enabled in a route pattern, the user is first asked for the FAC code and then for the CMC code.

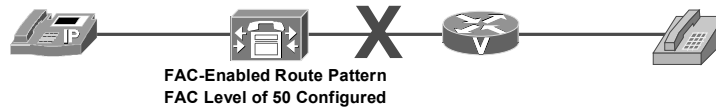
FAC Example

Cisco.com

Dials DN 94045550100
FAC Code 11155
FAC Level 100



Dials DN 94045550100
FAC Code 65319
FAC Level 20



© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-1-23

As shown in the figure, when the number 94045550100 is dialed, a FAC-enabled route pattern matches. Cisco CallManager plays a tone to prompt the user to enter a FAC code. If the FAC level of the code entered is equal to or higher than the FAC level configured in the route pattern, the call is routed. If the FAC level of the code entered is lower than the FAC level in the route pattern, the call is rejected.

In the Cisco CallManager configuration shown, only those using the FAC code 11155 (or another FAC code with an authorization level of 50 or higher) are able to call 94045550100. Those who use the FAC code 65319 are not able to complete the call. Their authorization level is too low, and the call is rejected.

Restricting External Transfers

This topic describes how to restrict transfers to external numbers.

Restricting External Transfers

Cisco.com

- **Operator or employee can transfer the call to an international or a premium number:**
 - From the inside for destinations that the user cannot call
 - From the outside
- **Friends or family members can be transferred to international or premium number:**
 - After they place a local call to the user's number
 - After the user called them

© 2005 Cisco Systems, Inc. All rights reserved. CPT2 v4.1-1-30

When calls are transferred to an external destination, very often the reason is that the caller whose call is transferred does not have permission to dial that external destination.

The operator or an employee, for instance, could be asked to transfer a call of a colleague who is home on vacation to an international destination. Or an employee who is not allowed to call international numbers could ask a colleague who is allowed to call international numbers to transfer the call to that international number. An employee could also save money by having family members call the employee in the office when they need to place costly calls. All that the employee has to do is to transfer the call for them. To eliminate the cost of their call to the office of the employee, the employee could even hang up and call them back before transferring the call.

Restricting External Transfers (Cont.)

Cisco.com

- **Cisco CallManager allows blocking external-to-external transfers.**
- **Uses OffNet and OnNet classification of gateways, trunks, and route patterns:**
 - **For incoming calls, trunk or gateway configuration determines OffNet versus OnNet classification**
 - **For outgoing calls, route pattern classification is used**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-31

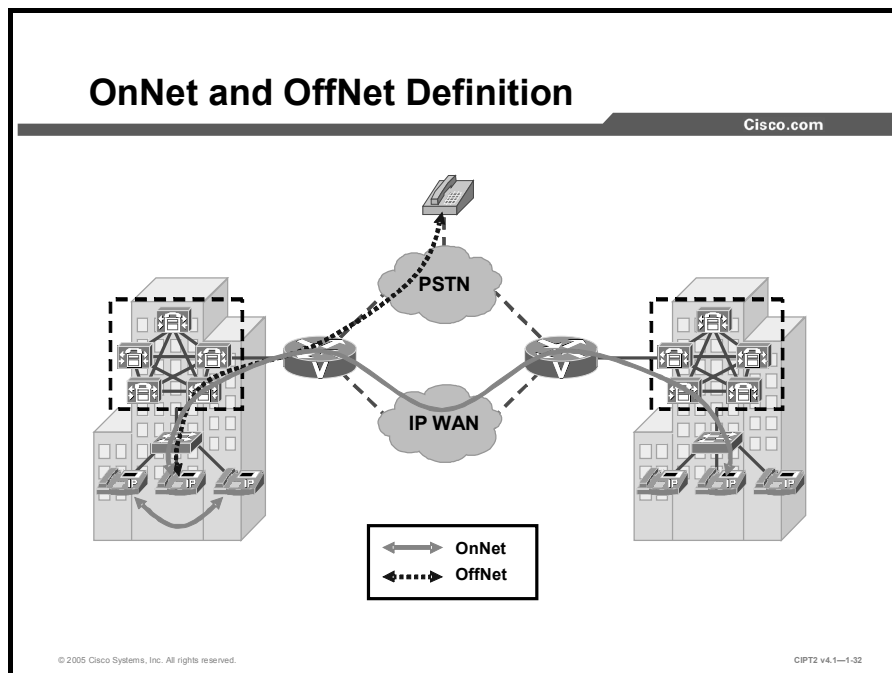
Cisco CallManager can be configured to block external-to-external call transfers. When you set the service parameter and configure gateways, trunks, and route patterns as OffNet (external) devices, external-to-external call transfers will not be allowed. This feature provides an OnNet or OffNet alerting tone to the terminating end of the call (determined by the configuration of the device as either OnNet or OffNet). For incoming calls, trunks or gateways determine OffNet versus OnNet classification. For outgoing calls, the route pattern classification is used.

The external call-transfer restriction requires the Cisco CallManager Release 4.1 or later software component.

Note Call transfer restrictions are implemented in Cisco CallManager 3.3(4) but there are defaults for OnNet and OffNet based on the gateway type and trunk and so on. Cisco CallManager Release 4.1 and later offer more flexibility because of the classification features.

OnNet and OffNet Definition

Cisco.com



Cisco CallManager classifies internal and external calls as OnNet and OffNet. A call coming from an external PSTN is classified as an OffNet call. A call that is placed internally (from one telephone to another, or between two Cisco CallManager clusters, where the call is routed over the WAN) is classified as an OnNet call, as illustrated in the figure. When you are using automated alternate routing (AAR) in OnNet or OffNet implementations, it is important to know from where the call is coming. With AAR, the source can be either the WAN connection or the PSTN connection. When the call is routed over the WAN connection, it is classified as an OnNet call at the called site. If AAR reroutes the call over the PSTN, the call is classified as an OffNet call at the called site.

Gateways and Trunks

Gateways and trunks can be configured as OnNet (internal) or OffNet (external) by using gateway configuration, using trunk configuration, or setting a cluster-wide service parameter to classify devices automatically. This parameter can be set in the service parameter configuration window. When the feature is used in conjunction with the cluster-wide service parameter Block OffNet to OffNet Transfer, the configuration determines whether calls can transfer over a gateway or trunk.

These devices can be configured as internal and external to Cisco CallManager:

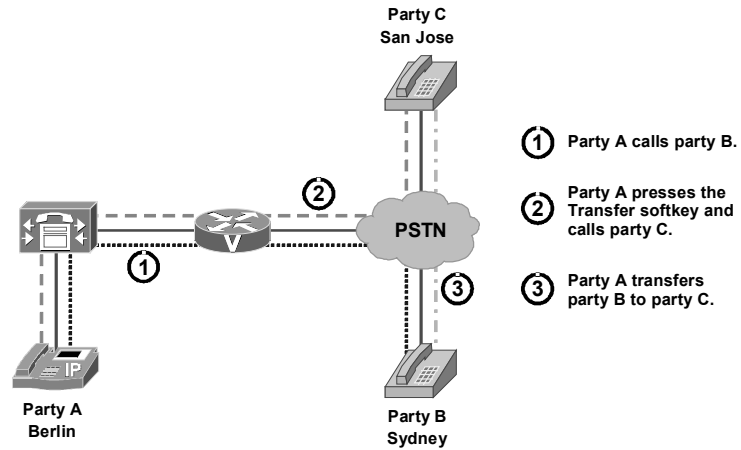
- H.323 gateway
- Media Gateway Control Protocol (MGCP) Foreign Exchange Office (FXO) trunk
- MGCP T1/E1 trunk
- Intercluster trunk
- Session Initiation Protocol (SIP) trunk

Route Patterns

To classify a call as OnNet or OffNet, you can set the Call Classification field in the Route Pattern Configuration window to OnNet or OffNet. You can override the route pattern setting and use the trunk or gateway setting by checking the Allow Device Override check box in the Route Pattern Configuration window.

Call Transfer Example Without Call-Transfer Restrictions

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-33

This example illustrates how callers use transfer to avoid paying for long-distance calls.

Party A in Berlin calls party B in Sydney. After the call is connected, party A presses the Transfer softkey (the second step) and transfers the call to party C in San Jose (the third step). When the transfer completes, party B and party C are connected and party A hangs up. As a result, the company where party A initiated the call from is billed for the call between Sydney and San Jose.

Configuring Call Transfer Restrictions

Cisco.com

- **Configure OnNet and OffNet devices:**
 - **Route patterns**
 - **Intercluster trunks**
 - **Gateways**
- **Enable “Block OffNet to OffNet Transfer” service parameter**

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1—1-34

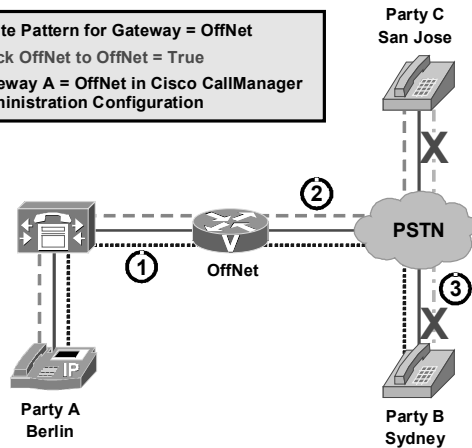
Complete these steps to block external calls from being transferred to external devices:

- Step 1** You can specify the OnNet or OffNet classification on the following:
- Route patterns
 - Intercluster trunks
 - Gateways
- Step 2** For incoming calls, configure individual gateways or trunks as **OffNet**.
- Step 3** For outgoing calls, configure the route pattern Call Classification field as **OffNet**.
- Step 4** Set the Block OffNet to OffNet Transfer cluster-wide service parameter to **True**.

Call Transfer Example with Call-Transfer Restrictions

Cisco.com

Route Pattern for Gateway = OffNet
Block OffNet to OffNet = True
Gateway A = OffNet in Cisco CallManager Administration Configuration



- ① Party A calls party B.
- ② Party A presses the Transfer softkey and calls party C.
- ③ Party A cannot transfer party B to party C because party A calls go through the OffNet route pattern.

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-35

In the Cisco CallManager configuration shown, the route pattern that is used to reach the external destinations is classified as an OffNet pattern. The gateway is also classified as OffNet. The service parameter Block OffNet to OffNet Transfer in the Cisco CallManager Service Parameter Settings window is set to True. Thus, the attempt by party A to call party B and transfer the call to party C will not work because OffNet-to-OffNet call transfers are restricted.

OnNet and OffNet Classification

Cisco.com

- **Route pattern classification applies to outgoing calls, while intercluster trunk or gateway classification applies to incoming calls.**
- **Route patterns can be configured to use the intercluster trunk or gateway classification for outgoing calls by checking the Allow Device Override check box.**

Route Pattern Configuration

Route Pattern: New
Status: Ready
Note: Any update to this Route Pattern automatically resets the associated gateway or Route List

Insert

Pattern Definition

Route Pattern* 01
Partition <None>
Description
Numbering Plan* North American Numbering Plan
Route Filter <None>
MLPP Precedence Default
Gateway or Route List* Not Selected
Route Option
 Route this pattern
 Block this pattern

Call Classification*
 Provide Outside Dial Tone
 Require Forced Authorization

OffNet
OnNet
Gateway

Allow Device Override
 Urgent Priority

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-36

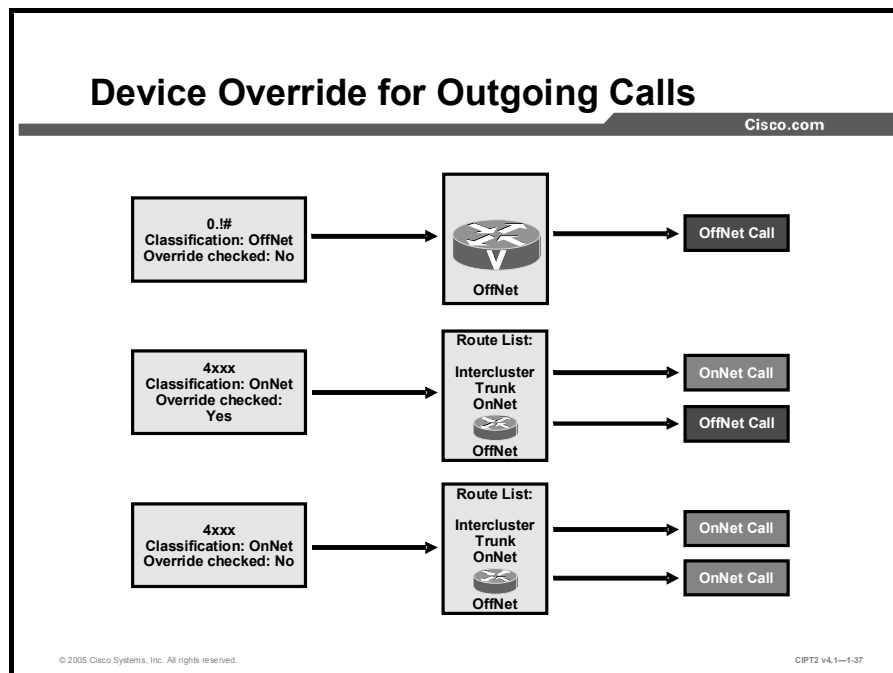
To classify calls in a route pattern, choose **Route Plan > Route/Hunt > Route Pattern** in Cisco CallManager. In the Call Classification field, choose whether the route pattern is an OffNet or OnNet pattern. The Allow Device Override check box is not checked by default.

The OnNet or OffNet classification can be configured on the following:

- **Route patterns:** If Allow Device Override is checked, the Call Classification setting of the associated device is taken into account. This feature is useful when a route list is associated with a route pattern because then the device setting (OnNet or OffNet) is used to classify the outgoing call.
- **Intercluster trunks:** In the Trunk Configuration window, when the Use System Default option is selected for the Call Classification service parameter, the Call Classification service parameter value is taken into account. By default, intercluster trunks are classified as OnNet (internal).
- **Gateways:** In the Gateway Configuration window, when the Use System Default option is selected for the Call Classification parameter, the Call Classification service parameter value is taken into account. The default value of the Call Classification service parameter is OffNet, which classifies the gateways as external.

Device Override for Outgoing Calls

Cisco.com



When you are configuring route patterns, you can configure the Allow Device Override parameter. This check box is unchecked by default. When it is checked, the system uses the Call Classification setting that is configured on the associated gateway or trunk to classify the outgoing call as OffNet or OnNet. The figure shows three examples.

Example 1

The route pattern (classified as OffNet) points to a gateway. The Allow Device Override check box is not checked. The associated gateway is classified as an OffNet device.

This configuration means that when a user calls a number that matches the route pattern `0.!#`, the call is classified as an OffNet call. If the Allow Device Override check box were checked, the call would be also classified as an OffNet call because the gateway is an OffNet device.

Example 2

The route pattern (classified as OnNet) points to a route list. The Allow Device Override check box is checked. The associated route list includes an intercluster trunk, which is an OnNet device, and a gateway, which is an OffNet device.

This configuration means that when a user calls a number that matches the route pattern `4xxx`, the call is classified as a OnNet call (as defined in the route pattern). Because the Allow Device Override check box is checked, the call is classified as an OnNet call when it is routed over the intercluster trunk and as an OffNet call when it is routed over the gateway. The classification that is configured at the route pattern level is overridden by the settings configured at the intercluster trunk or on the gateway.

Example 3

The route pattern (classified as OnNet) points to a route list. The Allow Device Override check box is not checked. The associated route list includes an intercluster trunk, which is an OnNet device, and a gateway, which is an OffNet device.

This configuration means that when a user calls a number that matches the route pattern 4xxx, the call is classified as an OnNet call (as defined in the route pattern). Because the Allow Device Override check box is not checked, the call is classified as an OnNet call when it is routed over the intercluster trunk and as an OnNet call when it is routed over the gateway. The classification that is configured at the route-pattern level is not overridden by the settings configured at the intercluster trunk or on the gateway.

Configure Cisco CallManager to Block OffNet-to-Offnet Transfers

Cisco.com

- Can be set in Cisco CallManager Administration: Service > Service Parameters
- By default, Block OffNet To OffNet Transfer parameter set to False
- When parameter is set to True, no OffNet-to-OffNet call transfers possible

Block OffNet To OffNet Transfer*	False	False
Drop Ad Hoc	Never	Never

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-38

To block OffNet-to-OffNet transfers, choose **Cisco CallManager Administration > Service > Service Parameters**; the Service Parameters Configuration window opens. In the Service drop-down list, choose Cisco CallManager. The Cisco CallManager Service Parameter configuration window opens. Locate the Block OffNet To OffNet Transfer parameter in the Cisco CallManager Service Parameter configuration window.

When the Block OffNet To OffNet Transfer service parameter is set to False, the transfer is not restricted. When this parameter is set to True and an OffNet party attempts to transfer a call to another OffNet party, the transfer is restricted.

Dropping Conference Calls

This topic describes how to enable conference call restrictions in Cisco CallManager.

Types of Ad Hoc Conference Restrictions

Cisco.com

- **Ad hoc conferences can be configured to be dropped in certain situations:**
 - **When Conference Creator Drops Out—Available since Cisco CallManager Release 3.3(4)**
 - **When No OnNet Parties Remain in the Conference—Available since Cisco CallManager Release 4.1**
- **Ad hoc conferences use OnNet and OffNet classification.**

© 2005 Cisco Systems, Inc. All rights reserved. CPT2 v4.1-1-39

The Drop Conference feature determines how an existing ad hoc conference should be dropped. Beginning in Cisco CallManager Release 3.3(4), the conference call can be configured to be dropped when its creator leaves the conference. Beginning in Cisco CallManager Release 4.1, the value When No OnNet Parties Remain in the Conference can also be configured. Determine the OnNet status for each party by checking the device or route pattern that the party is using, as with call-transfer restrictions.

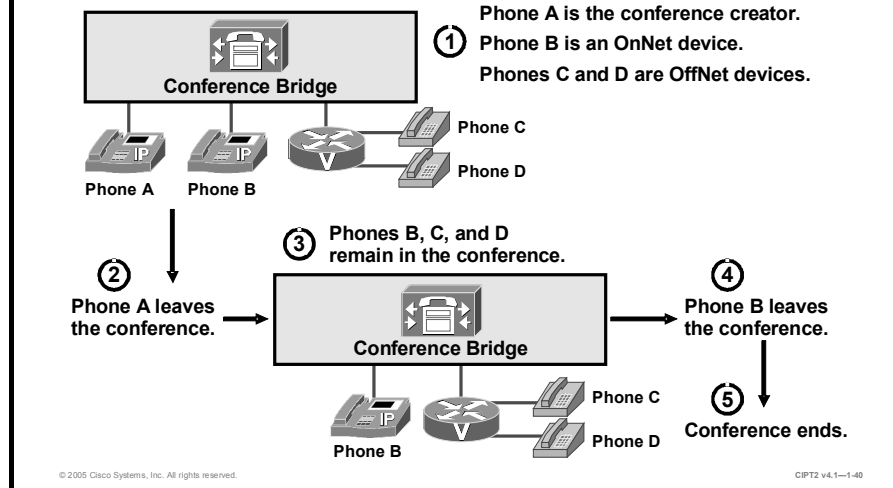
Note IP Phones are always classified as OnNet devices. Gateways, trunks, and route patterns can be classified either as OnNet or as OffNet.

Valid values for the Drop Ad Hoc Conference service parameter are as follows:

- **Never:** The conference call stays active even when the conference creator hangs up. This behavior retains the original behavior of the conference feature. This is the default value.
- **When Conference Creator Drops Out:** When the conference creator hangs up, the conference call is dropped. When the conference creator transfers, redirects, or parks the call and the retrieving party hangs up, the conference is also dropped.
- **When No OnNet Parties Remain in the Conference:** When the last OnNet party in the conference hangs up, the conference is dropped.

Service Parameter Set to When No OnNet Parties Remain in the Conference Example

Cisco.com



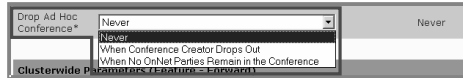
The figure illustrates an example with four phones: phone A, phone B, phone C, and phone D. Phone A is the conference creator or primary controller of the conference. Phone A and phone B are OnNet devices, and phone C and phone D are OffNet devices. (Phone C and phone D are external callers.)

If the Drop Ad Hoc Conference service parameter is set to When No OnNet Parties Remain in the Conference and phone A leaves the conference, the conference remains active. When the last OnNet device, in this case, phone B, leaves the conference, the conference ends immediately.

Configuration of the Drop Ad Hoc Conference Parameter

Cisco.com

- In the Cisco CallManager Administration window: Service > Service Parameters > Cisco CallManager to change the parameter
- Parameter can be changed to three different values



© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-141

Configuring ad hoc conference restrictions is very similar to configuring call-transfer restrictions. A service parameter has to be modified for ad hoc conferences.

To configure the service parameter for ad hoc conference restrictions in Cisco CallManager Administration, choose **Service > Service Parameters > Cisco CallManager**. The Cisco CallManager Service Parameter Configuration window opens. Locate the Drop Ad Hoc Conference service parameter.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- Sources of toll fraud can be external or internal.
- Call forwarding can be restricted through partitions and calling search spaces.
- Block commonly exploited area codes to prevent toll fraud.
- FAC is used to authorize users to make calls.
- Time-of-day routing is used to change permissions to place calls at special hours or days.
- Classify devices, route patterns, and trunks as OnNet or OffNet to restrict external call transfers.
- Cisco CallManager can be configured to drop ad hoc conferences when no OnNet parties remain on the call or when the conference creator drops out.

© 2005 Cisco Systems, Inc. All rights reserved.

CIP12 v4.1-1-42

Hardening the IP Phone

Overview

The IP Phone is a target for attacks just like all other components of the network. Very often endpoints, such as IP Phones, are not protected—only servers and network infrastructure devices are hardened. This is not a good practice because IP Phones have default settings that make them vulnerable to certain attacks. However, there are several options available to harden IP Phones and thus protect them against various attack and infiltration methods.

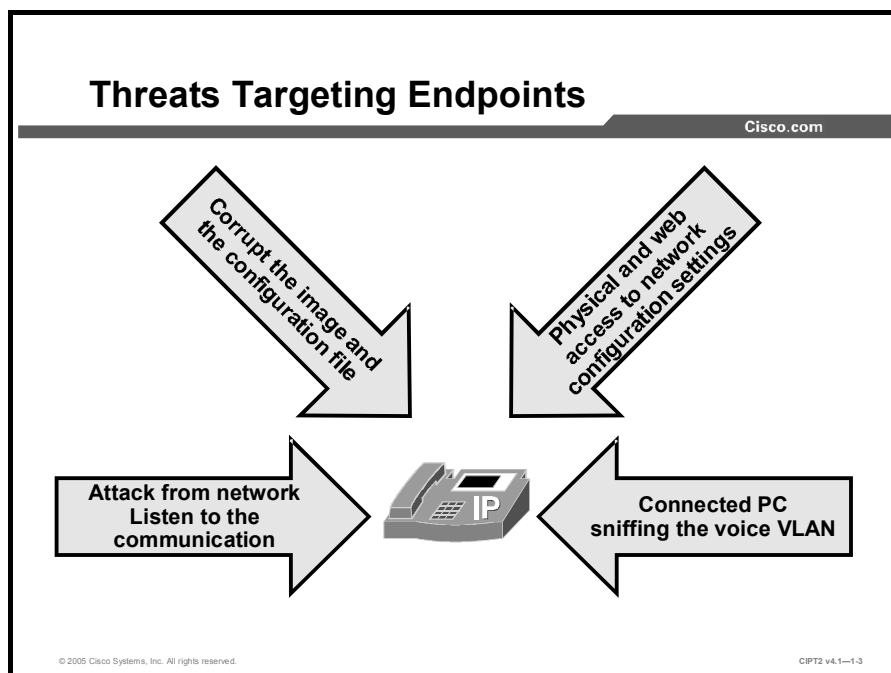
Objectives

Upon completing this lesson, you will be able to harden the Cisco IP Phone. This ability includes being able to meet these objectives:

- Identify potential threats against IP Phones and the attack tool or method
- Explain how signed firmware images prevent rogue or incorrect images from being placed on the IP Phone
- Configure parameters in the Phone Configuration window of Cisco CallManager Administration to harden the IP Phone
- Explain how disabling the PC port, the Settings button, and web access help secure the IP Phone
- Explain how, by ignoring gratuitous ARP, the IP Phone can help prevent a man-in-the-middle attack
- Explain how blocking the PC from accessing the voice VLAN through the IP Phone prevents eavesdropping on the voice conversation
- Explain how authentication and encryption on Cisco CallManager and the IP Phones prevent identity theft of the phone or Cisco CallManager server, data tampering, and call-signaling and media-stream tampering

Threats Targeting Endpoints

This topic describes different ways to attack an IP Phone.



There are many attack paths against an IP Phone, including a connection through the network or through the integrated switch port to which a PC is attached. Corrupt images and altered configuration files can sabotage the IP telephony environment. Further attacks can be started from an infiltrated IP Phone that is generally trusted and has access to the network. The physical access to the IP Phone can be misused for violations of the IP Phone integrity and the privacy of the user. Information can be gathered by browsing to the IP Phone as well. In addition, IP Phone conversations are vulnerable to various attacks when the network has been infiltrated, so the privacy of calls must be protected.

Endpoint Infiltration and Attack

Cisco.com

- **Endpoints can be infiltrated by modifying the image and configuration file.**
- **Endpoints can be wire-tapped:**
 - **Behind the switch of the IP Phone**
 - **Man-in-the-middle attack with gratuitous ARP**
- **Information about network infrastructure can be uncovered:**
 - **DHCP, DNS, default router, Cisco CallManager, TFTP**
 - **These could be next targets of the attacks**

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-14

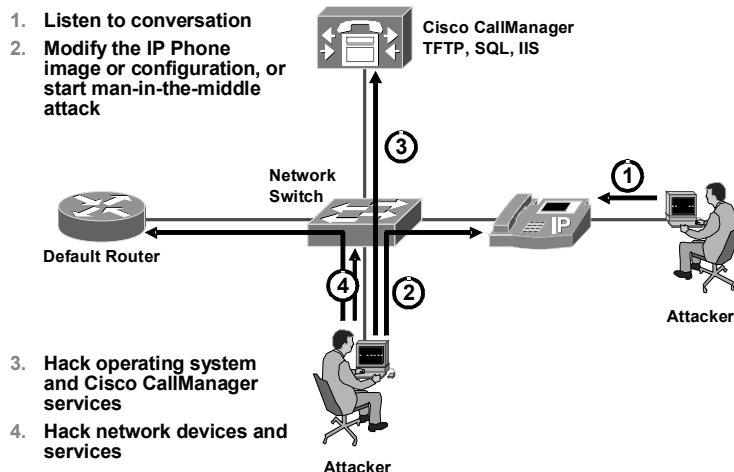
Endpoints are a common target of attacks because they are usually less protected than strategic devices, such as servers or network infrastructure devices. If an attacker gets control of an endpoint, such as an IP Phone, the attacker could use that device as a jumping-off point for further attacks. Because the endpoints are trusted devices and have certain permissions in the network, an attacker can use them to target devices that he or she would not be able to reach directly. To get control of an IP Phone, an attacker could try to modify the image and configuration file (for example, by spoofing the TFTP server or by replacing the file on the TFTP server itself or while in transit).

Another major threat is eavesdropping on conversations. If an attacker has physical access to the IP Phone, he or she could “tap the wire,” either by connecting between the IP Phone and the switch or by connecting to the PC port of the IP Phone. If the attacker does not have physical access to the IP Phone or its network connection, the attacker could launch a man-in-the-middle attack from any network between two communicating endpoints. In a man-in-the-middle attack, the attacker pretends to be a neighboring system (such as the default gateway when the communication is between two IP networks or a peer on the same IP network) and hence receive all packets. A common type of man-in-the-middle attack is to use gratuitous Address Resolution Protocol (ARP) for redirection of packets at the MAC address layer.

A lot about the IP Phone and the telephony infrastructure can be learned just by looking into the network settings or browsing to the HTTP server of the IP Phone. This information contains Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), default router, TFTP, and Cisco CallManager addresses. With this information, a hacker can direct an attack at the TFTP or Cisco CallManager server, because Windows hosts are generally more vulnerable than network components.

Where to Start an Attack?

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1.5

The simplest way to eavesdrop on the conversations of a user, depicted as the first method in the figure, is to tap the wire between the IP Phone and the PC attached to it. A variety of tools exist, such as ettercap—a suite for man-in-the-middle attacks that allows sniffing and on-the-fly manipulation of data, voice over misconfigured Internet telephones (vomit)—a tool that can create .wav files from captured G.711 conversations, and Ethereal—a sniffer and network protocol analyzer that allows both capturing conversations and converting them to playable files.

An attacker could try to get control of an IP Phone by modifying the IP Phone image or configuration file, depicted as the second method in the figure. This attack is carried out either at the TFTP server by manipulating the files themselves or by replacing the content while it is in transit. For the first method, the attacker needs access to the directory of the TFTP server; for the second, the attacker has to launch a man-in-the-middle attack.

The hacker may want to direct the attack at the most critical telephony components—the servers—as depicted in the third method. An easy way to gather information about the IP addresses of critical components (such as the Cisco CallManager addresses, default gateway address, TFTP server address, DNS server address, and voice VLAN ID) is to retrieve them from the IP phone. This retrieval can be done locally at an IP Phone by using the Settings button or by connecting to the IP address of the IP Phone with a web browser. From the retrieved information, the hacker can build a topology map, associate it with services, and use the topology map to attack relevant devices.

If the attacker manages to get access to network devices, such as routers and switches, he or she could redirect traffic to any destination using various kinds of tunnels. These include Generic Route Encapsulation (GRE), IPsec, Layer 2 Protocol Tunneling (L2TP), or Switched Port Analyzer (SPAN). These techniques allow either redirection or duplication of packets and enable an attacker to receive the packets at a remote location.

Stopping Rogue Images from Infiltrating Phones

This topic describes how the IP Phone can be protected against infiltration by using phone image and configuration file authentication.

Phone Security Overview

Cisco.com

- **Phone image authentication was introduced with Cisco CallManager Release 3.3(3):**
 - Image signed by Cisco manufacturing
 - Also includes information about phone model
 - Current image verifies signature of new image
 - Only if new image is properly signed is the new image accepted
- **Phone configuration file authentication was introduced with Cisco CallManager Release 4.0 for Cisco IP Phone 7940, 7960, and 7970 models:**
 - Configuration file signed by Cisco CallManager
 - Signature verified before new configuration is applied

© 2005 Cisco Systems, Inc. All rights reserved.CPT2 v4.1-1-6

Cisco IP Phone image authentication was introduced with Cisco CallManager Release 3.3(3). In this and later releases, phone images are signed by Cisco manufacturing. Such a signature proves the authenticity of the origin, and the Cisco IP Phone will not accept images that are not published by Cisco manufacturing. The image also contains information about the IP Phone model, so an IP Phone will not accept an image for a different model. Since the introduction of image authentication, the current image verifies the signature of a new image. Only if the new image is properly signed by Cisco manufacturing is the new image accepted.

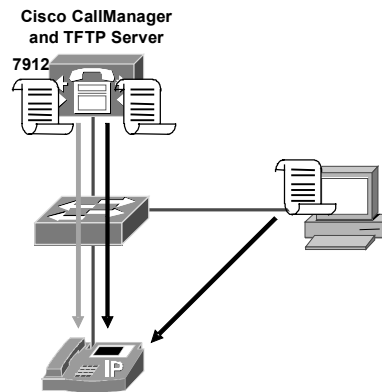
Cisco IP Phone configuration file authentication was introduced with Cisco CallManager Release 4.0 for Cisco IP Phone 7940, 7960, and 7970 models. The configuration files are signed by Cisco CallManager. The phone now verifies the signature and accepts the new configuration file only if it is properly signed by Cisco CallManager. Cisco IP Phone configuration file authentication requires additional configuration and hardware (Universal Serial Bus [USB] security tokens) and is not on by default.

IP Phones Validate Signed Firmware

Cisco.com

IP Phone rejects image because of:

- Modified image from a hacker or TFTP server
- Incorrect IP Phone model image



© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1.7

IP Phones will reject images with invalid signatures. They verify that the signature really validates the corresponding file whether it was obtained from an attacker or from the legitimate TFTP server.

Since the introduction of this feature, the actual (current) image used in the phone includes the code to accept new images only if they have a valid signature. The actual image also includes the public key that is needed to verify the signature of new images. This way, only images that have been signed with the correct private key (owned by Cisco engineering) can be loaded. This also means that after you load the first image that features signature verification, you cannot load an older image that does not include a valid signature. This limitation guarantees that no image that has been tampered with can be loaded to your phone.

With image signature information about the IP Phone model having been added to the image as well, the IP Phone can verify that the image that is loaded is not for a different phone model. Before the introduction of this feature, a phone stopped responding if an image for another model was loaded, while today, such a wrong image is simply not accepted.

Disabling Phone Settings in Cisco CallManager Administration

This topic describes the options to secure an IP Phone.

Disabling Phone Settings in Cisco CallManager Administration

Cisco.com

Protect the IP Phone by disabling security settings:

- **Speakerphone**
- **PC port**
- **Settings access**
- **Gratuitous ARP**
- **PC voice VLAN access**
- **Web access**

Product Specific Configuration

Disable Speakerphone	<input type="checkbox"/>
Disable Speakerphone and Headset	<input type="checkbox"/>
Forwarding Delay**	Disabled
PC Port**	Enabled
Settings Access**	Enabled
Gratuitous ARP**	Enabled
PC Voice VLAN Access**	Enabled
Video Capabilities**	Disabled
Auto Line Select**	Disabled
Web Access**	Enabled

** Indicates a required item.
** Indicates time on Publisher.

© 2005 Cisco Systems, Inc. All rights reserved. C IPT2 v4.1-1-8

The product-specific configuration parameters of Cisco IP Phones are set by default to achieve the greatest functionality but are considered insecure. To secure Cisco IP Phones, these settings can be modified:

- **Disable Speakerphone and Disable Speakerphone and Headset:** Disable these features to prevent eavesdropping on conversations in the office by a hacker gaining remote control of the IP Phone and listening to the sound near it.
- **PC Port:** Disable the PC port to prevent a PC from connecting to the network via the IP Phone switch.
- **Settings Access:** Disable or restrict access to the IP Phone settings to avoid the risk that details about the network infrastructure could be exposed.
- **Gratuitous ARP:** Disable this feature to prevent gratuitous ARP-based man-in-the-middle attacks.
- **PC Voice VLAN Access:** Disable this feature to stop the IP Phone from forwarding voice VLAN traffic to the PC.
- **Web Access:** Disable access to the IP Phone from a web browser to avoid the risk that details about the network infrastructure could be exposed.

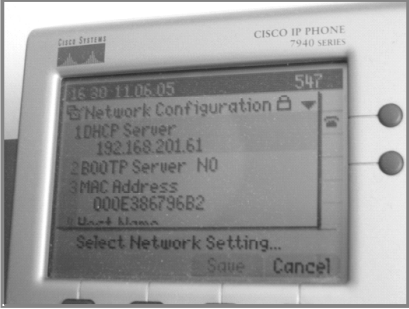
Disabling the PC Port, the Settings Button, and Web Access to the IP Phone

This topic describes the parameters that control access to the phone settings and the integrated switch port.

Hardening the IP Phone with Product-Specific Parameters

Cisco.com

- **Disable the PC port:**
 - For example, for lobby phones
 - Attackers do not get access to the network
- **Disable settings access:**
 - Disabled option deactivates the Settings button
 - Restricted option grants access to contrast and ringer menu only



© 2005 Cisco Systems, Inc. All rights reserved. CIPT2 v4.1-1-8

The PC port is typically disabled in special areas like a lobby or areas where no additional PC access is allowed. It is not a common setting, though, because it entails a major functionality constraint.

Disabling the settings access prevents users from gathering information about, for example, DHCP server, TFTP server, default router, and Cisco CallManager IP addresses. Cisco CallManager Release 4.1 and later releases offer the Restricted option for settings access. With restricted access, the user can modify the contrast and ringer settings but cannot see any other information.

IP Phone Web Service

Cisco.com

- Displays similar information as the Settings button on the IP Phone
- Discloses information about network infrastructure
- Disable web access for a phone to stop the web service

Device Information	MAC Address	000F24A978A7
Network Configuration	Host Name	SEP000F24A978A7
Network Statistics	Phone DN	2017
Ethernet	App Load ID	P00307000200
Port 1 (Network)	Boot Load ID	PC0303010001
Port 2 (Access)	Version	7.0(2.0)
Port 3 (Phone)	Expansion Module 1	
Device Logs	Expansion Module 2	
Debug Display	Hardware Revision	4.2
Stack Statistics	Serial Number	INM08061F9J
Status Messages	Model Number	CP-7940G
Streaming Statistics	Codec	ADLCodec
Stream 1	Amps	5V Amp
	C3PO Revision	2
	Message Waiting	NO

© 2005 Cisco Systems, Inc. All rights reserved.

CIP72 v4.1—1-10

You can use a web browser to connect to the HTTP server of the IP Phone by simply browsing to the IP address of the phone. The HTTP server displays similar information that can be viewed directly on the IP Phone using the Settings button, enhanced by some additional statistics. A hacker can use the intelligence gained by discovering the network configuration to direct attacks at the most critical telephony components, such as Cisco CallManager and the TFTP server. Therefore, from a security perspective, it is recommended that you disable web access to the phone.

When web access is disabled, the IP Phone will not accept incoming web connections and hence does not provide access to sensitive information.

Note Disabling web access at the IP Phone stops Extensible Markup Language (XML) push applications from working. If you want to use XML push applications on some IP Phones (for instance, for an emergency notification application) you cannot disable web access to the IP Phone.

Ignoring Gratuitous ARP

This topic describes how to prevent a man-in-the-middle attack based on gratuitous ARP.

Gratuitous ARP

Cisco.com

- **Usually ARP operates in request-response fashion.**
- **Learned MAC addresses are added to a local ARP cache.**
- **Gratuitous ARP packets are ARP packets that have not been requested:**
 - **Are sent by a station that announces its own MAC address**
 - **Allows update of ARP caches in receiving devices**
 - **Usually sent after MAC address changes**
 - **Can be misused for packet redirection in a man-in-the-middle attack**

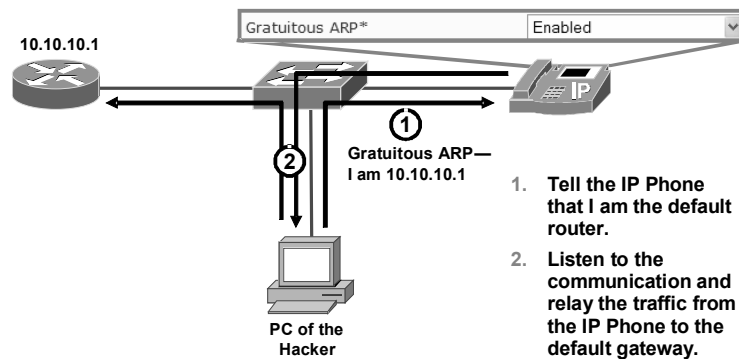
© 2005 Cisco Systems, Inc. All rights reserved.CIPT2 v4.1-1-11

Usually ARP operates in a request-and-response fashion. When a station needs to know the MAC address of a given IP address, it sends an ARP request. The device with the corresponding IP address replies and thus provides its MAC address. All receiving devices update their ARP cache by adding the IP and MAC address pair. Gratuitous ARP packets are packets that announce the MAC address of the sender even though this information has not been requested. This technique allows receiving devices to update their ARP caches with the information. Usually such gratuitous ARP messages are sent after the MAC address of a device has changed to avoid packets being sent to the old MAC address until the related entry has timed out in the ARP caches of the other devices.

Gratuitous ARP, however, can also be used by an attacker to redirect packets in a man-in-the-middle attack.

Gratuitous ARP Attack

Cisco.com



Stop gratuitous ARP attacks by disabling gratuitous ARP at the IP Phones.

© 2005 Cisco Systems, Inc. All rights reserved.

CIP72 v4.1—1-12

The figure illustrates a gratuitous ARP attack against an IP Phone. Cisco IP Phones by default do accept gratuitous ARP messages and update their ARP cache whenever they receive a gratuitous ARP packet.

The attacker located in the VLAN of the IP Phone repeatedly sends out gratuitous ARP packets announcing its MAC address to be the MAC address of the default gateway of the IP Phone. The IP Phone accepts the information, updates its ARP cache, and forwards all packets meant for the default gateway to the attacker. With tools such as ettercap, the hacker can copy or modify the information and then relay it to the real default gateway. The user does not notice that someone is listening to the data stream as long as the hacker does not significantly increase the delay and does not drop packets.

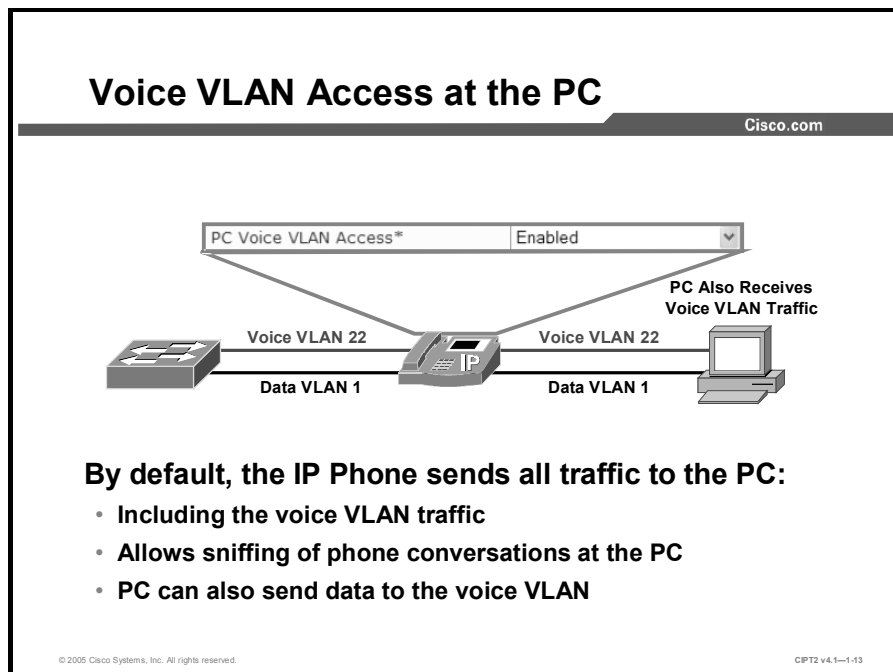
In this example, only traffic from the IP Phone toward the default gateway is sent to the attacker, but if the attacker also impersonates the IP Phone toward the router, the attacker could control bidirectional traffic. In this case, the router would also have to listen to gratuitous ARP packets.

To prevent gratuitous ARP-based attacks against an IP Phone, the gratuitous ARP feature of the IP Phone should be disabled.

Note There are several methods to prevent gratuitous ARP attacks. You can disable it on end devices or you can use features such as Dynamic ARP Inspection (DAI) and IP Source Guard at switches. You can find more information about DAI and IP Source Guard in your Cisco IOS or Cisco Catalyst operating system switch configuration guide.

Blocking PC Access to the Voice VLAN

This topic describes how to prevent the PC connected to the IP Phone from accessing the voice VLAN.



By default, an IP Phone sends all traffic that it receives from the switch out its PC port. This enables the PC to see not only the traffic of the native VLAN, the data VLAN, but also to see the traffic of the voice VLAN. When the PC receives voice VLAN traffic, the traffic can be captured and hence the conversation can be sniffed.

Further, the PC can also send packets to the voice VLAN if they are tagged accordingly. This breaks the separation of voice VLANs and data VLANs, because the PC that is supposed to have access to the data VLAN only is now able to send packets to the voice VLAN, bypassing all access-control rules (access control lists [ACLs] in routers or firewalls) that might be enforced between the two VLANs.

Usually the PC does not need access to the voice VLAN, and therefore you should block PC access to the voice VLAN.

Note Some applications, such as call recording or supervisory monitoring in call centers, require access to the voice VLAN. In such situations, you should not disable the PC Voice VLAN Access setting.

Disable PC Voice VLAN Access

Cisco.com

- The IP Phone will not forward voice VLAN-tagged traffic to the PC when received from the switch.
- The IP Phone will not forward voice VLAN-tagged traffic to the switch when received from the PC.
- Sniffing voice VLAN traffic at the PC is impossible.
- For troubleshooting, sniff the network devices.
- Different behavior with different IP Phone models:
 - Cisco IP Phone 7970 blocks all packets with 802.1q header.
 - Cisco IP Phone 7960 and 7940 block access to the voice VLAN only.
 - Cisco IP Phone 7960 and 7940 allow PC to send and receive frames tagged with VLAN IDs other than the voice VLAN.
 - Cisco IP Phone 7912 does not support disabling PC voice VLAN access.

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1—1-14

To block the PC from accessing the voice VLAN, set the PC Voice VLAN Access configuration parameter to Disabled. When a phone is configured this way, it will not forward voice VLAN-tagged traffic to the PC when it receives such frames from the switch. In addition, the phone will not forward voice VLAN-tagged traffic to the switch if it receives such frames from the PC. Although this setting is recommended from a security perspective, it makes troubleshooting more difficult because you cannot analyze voice VLAN traffic from a PC connected to the PC port of the IP Phone. Whenever you need to capture voice VLAN traffic to analyze network problems, you will have to sniff the traffic on the network devices. On Cisco Catalyst switches, you can configure SPAN ports to duplicate traffic from certain ports or VLANs to another port where you attach the PC that is running your protocol analyzer. Remote SPAN (RSPAN) even allows you to send the selected traffic to another switch for remote analysis.

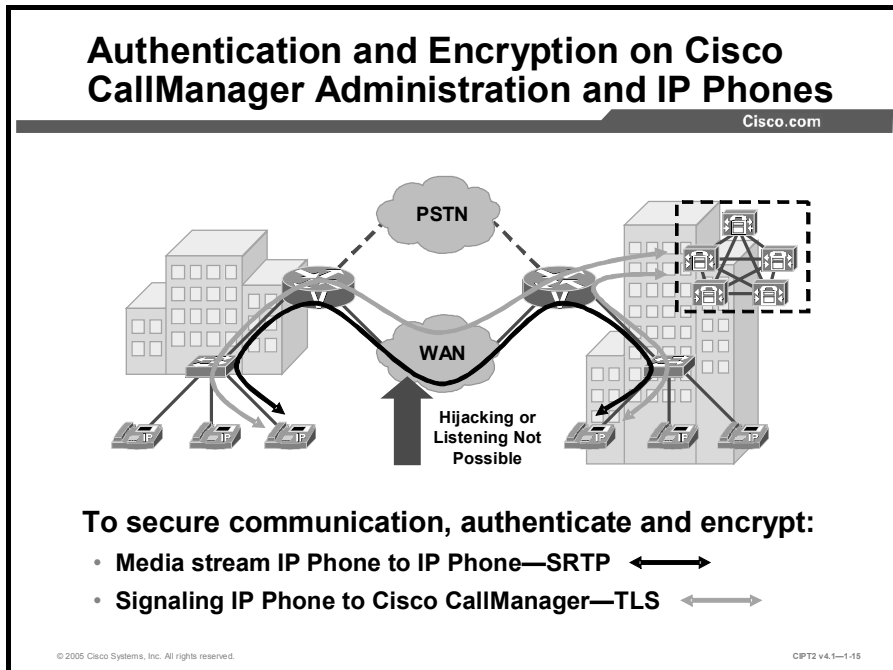
Note You can find more information about SPAN and RSPAN in your Cisco IOS or Cisco Catalyst operating system switch configuration guide.

Disabling PC voice VLAN access on a Cisco IP Phone results in different behavior, depending on the IP Phone model:

- The Cisco IP Phone 7970 blocks all frames with 802.1q headers. This means that the PC can send and receive only untagged frames.
- The Cisco IP Phone 7960 and 7940 models block only frames tagged with the voice VLAN ID. This means that the PC can send and receive untagged frames and frames that are tagged with a different VLAN ID than the voice VLAN ID.
- The Cisco IP Phone 7912 does not support disabling PC voice VLAN access.

Authentication and Encryption in Cisco CallManager Administration and IP Phones

This topic describes the technology to protect the signaling and the audio stream from and to a Cisco IP Phone.



Cisco CallManager Release 4.0 introduced certificate-based authentication and encryption of signaling and media. Skinny Call Control Protocol (SCCP), used between the IP Phone and Cisco CallManager for call signaling, can be secured by Transport Layer Security (TLS), formerly known as Secure Socket Layer (SSL). This protects the signaling channels from most types of attacks. The media stream between two IP Phones is protected with Secure Real-Time Transfer Protocol (SRTP), which encrypts and authenticates the voice data. A hacker cannot modify the packets and is not able to listen to the audio stream, because it is now encrypted.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Hackers typically begin with the weakest points in the network, such as IP Phones.**
- **IP Phones can validate images and configuration updates.**
- **Every IP Phone has specific product configuration menus.**
- **Disable settings access and web access to prevent hackers from viewing the network configuration.**
- **Disable gratuitous ARP to prevent man-in-the-middle attacks.**
- **Block the PC port if no PC is attached to it, and generally block access to the voice VLAN to avoid unauthorized network access.**
- **TLS secures SCCP and SRTP secures the audio stream.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIP12 v4.1-1-16

Understanding Cryptographic Fundamentals

Overview

Configuring Cisco CallManager for security is relatively straightforward; however, the underlying security services, algorithms, and operations are often not well-known to the Cisco CallManager administrators who must secure the Cisco CallManager installation. This lesson provides information about cryptographic fundamentals. It helps you understand the elements that are the basis of cryptography in the data world.

Objectives

Upon completing this lesson, you will be able to define the fundamentals of cryptography and understand how they are applied to provide various services. This ability includes being able to meet these objectives:

- Define cryptography and explain the four cryptographic services: confidentiality, integrity, authentication, and nonrepudiation
- Explain the basic operation and uses of symmetric encryption algorithms and identify the common algorithms in use today
- Explain the basic operation and uses of asymmetric encryption algorithms and identify the common algorithms in use today
- Explain how hash functions provide data integrity and list common hash functions in use today
- Define digital signatures and explain how they provide identity and integrity

What Is Cryptography?

This topic defines cryptography and describes the services that cryptography provides. It gives an overview of the application of encryption and authentication techniques for each of these services.

What Is Cryptography?

Cisco.com

- **The science of transforming readable messages into an unintelligible form and the later reversal of that process**
- **Provides four services:**
 - **Data authenticity (proof of source)**
 - **Data confidentiality (privacy and secrecy)**
 - **Data integrity (detection of unauthorized change)**
 - **Data nonrepudiation (nondeniability)**
- **Uses encryption and authentication methods**

© 2005 Cisco Systems, Inc. All rights reserved.CIPT2 v4.1-1.3

Cryptography is the science of transforming readable messages into an unintelligible form and the later reversal of that process. The application is to send the transformed, unreadable message over an untrusted channel. In the data world, this untrusted channel very often is a public network, such as the Internet.

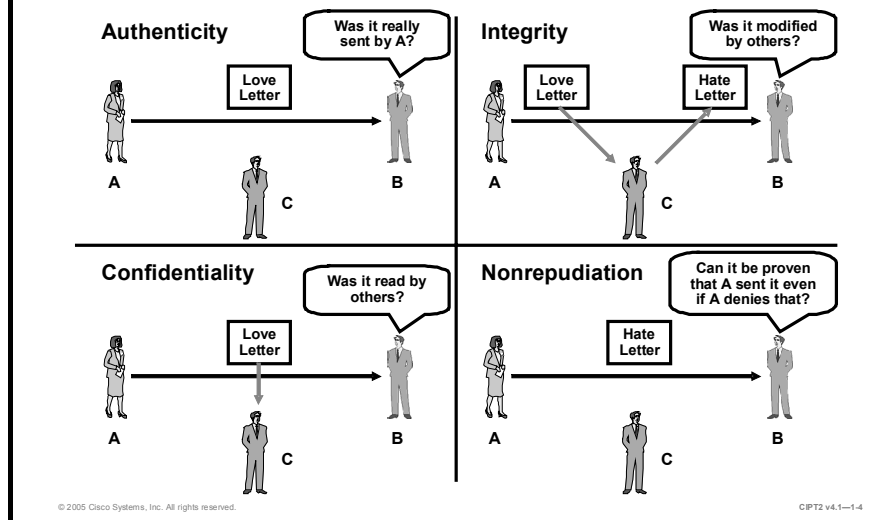
Cryptography provides four services:

- **Data authenticity:** This service should guarantee that the message comes from the source that it claims to come from. When an application such as e-mail or protocols such as IP do not have any built-in mechanisms that prevent spoofing of the source, cryptographic methods can be used for proof of sources.
- **Data confidentiality:** This service provides privacy by ensuring that messages can be read only by the receiver.
- **Data integrity:** This service ensures that the messages are not altered in transit. With data integrity, the receiver can verify that the received message is identical to the sent message and that no manipulation was done.
- **Data nonrepudiation:** This service allows the sender of a message to be uniquely identified. With nonrepudiation services in place, a sender cannot deny having been the source of that message.

All these services are based on encryption and authentication methods. However, for different applications, different kind of encryption and authentication techniques are used.

Services of Cryptography

Cisco.com



The figure illustrates examples of the four services. These scenarios are possible:

- **Authenticity:** If B receives a love letter that says it is coming from A, how can B be sure that it was really sent by A and not someone else? Without any reliable service that ensures authenticity of the source, user B will never know.
- **Confidentiality:** On the other hand, if there are means of guaranteeing the authenticity of the source, B might be afraid that somebody else read the love letter while it was in transit, resulting in a loss of privacy. This problem could be solved by a service providing confidentiality.
- **Integrity:** If B were to receive a hate letter, formed in a way that it proved the authenticity of the source, how can B know that the content has not been modified in transit? A service that ensures integrity of the message is needed to eliminate this kind of threat.
- **Nonrepudiation:** However, if B receives a hate letter from A that seems to be authentic, can B prove to others that it must have been sent by A? A nonrepudiation service is needed in this case.

It might appear that the authenticity service and the nonrepudiation service are fulfilling the same function. Although both address the question of the proven identity of the sender, there is a small difference in the two, which is sometimes quite important:

- When the receiver needs to be sure about the authenticity of the source, the method and the means that are used to achieve the proof of authenticity can be available to both the sender and the receiver. Because the receiver knows that he or she was not the source, it does not matter that sender and receiver both know how to treat a message to provide authenticity of the source.
- If, however, the receiver has to prove the source of the sender to others, it is not acceptable that the receiver know how the sender treated this message to prove authenticity, because the receiver could then have pretended to be the sender.

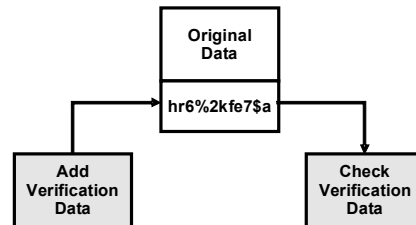
An example for authenticity versus nonrepudiation would be data exchange between two computers of the same company versus data exchange between a customer and a web shop.

When the two computers do not have to prove to others which of them sent a message, but just need to make sure that whatever was received by one was sent by the other, the two computers can *share* the same way of transforming their messages. This practice would not be acceptable in business applications such as a web shop. If the web shop would know how a customer transforms messages to prove authenticity of the source, the web shop could easily fake “authentic” orders. Therefore, in such a scenario, the sender must be the only party having the knowledge how to transform messages. Then the web shop can prove to others that the order must have been sent by the customer. The customer could not argue that the order was faked by the web shop when the web shop does not know how to transform the messages from the customer to make them authentic.

Authentication Overview

Cisco.com

- Provides **authenticity, integrity, and nonrepudiation**
- **Sender adds verification data to the actual data**
- **Receiver checks verification data**
- **Uses HMACs or digital signatures**



© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1—1-6

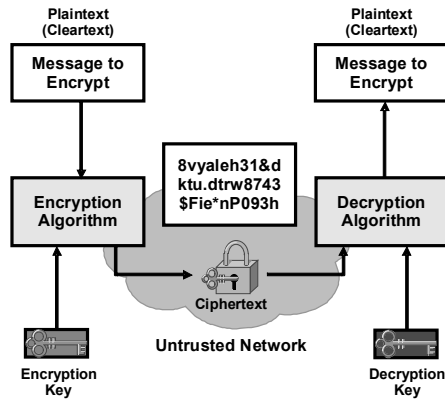
Authentication functions are used to provide authenticity, integrity, and nonrepudiation. To achieve this, the sender adds (appends) verification data to the actual data. The authenticated data can be information about the sender (such as its identity) or the information that should be passed from the sender to the receiver itself. The receiver checks the verification data added by the sender and if successful, can confirm authenticity.

There are various ways to create the verification data, the most common being Hash-Based Message Authentication Code (HMAC) or digital signatures.

Encryption Overview

Cisco.com

- Provides confidentiality
- Transforms cleartext into ciphertext (encryption)
- Only authorized peers can transform ciphertext back to cleartext (decryption)
- Uses symmetric or asymmetric encryption algorithms and keys



© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1.6

Confidentiality is provided by encryption. More precisely, the transformation of cleartext to ciphertext is called encryption, while the transformation of the ciphertext back to the original cleartext is called decryption.

Encryption utilizes an encryption algorithm and keys. If the key that is used to encrypt the data and the key that is used to decrypt the data is the same, the encryption algorithm is symmetric (with symmetric keys). If the encryption and decryption keys are different, the encryption algorithm is asymmetric (with asymmetric keys).

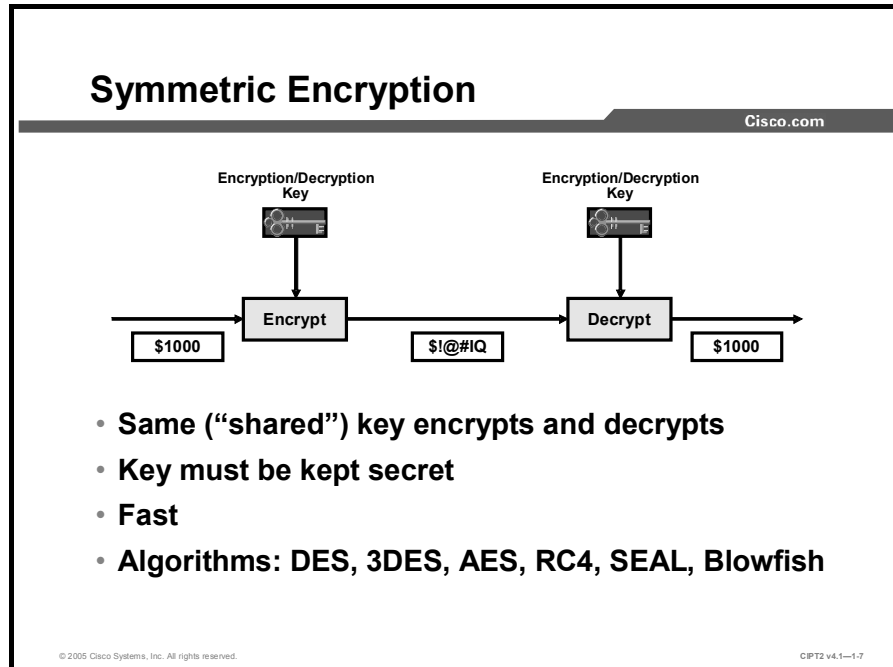
Although the encryption algorithms are usually well-known, the keys that are used for the encryption have to be secret. Symmetric keys have to be known by both endpoints that want to use a symmetric encryption algorithm for their data exchange. With asymmetric encryption, the sender needs to know only the encryption key, while the receiver needs to know only the decryption key.

Desirable features of an encryption algorithm are as follows:

- **Resistance to cryptographic attacks:** The algorithm itself must be trusted by the cryptographic community and there must be no shortcut to decipher data other than knowing or guessing the decryption key.
- **Variable key lengths and scalability:** The longer the encryption key, the longer it will take attackers to break it if they try all the possible keys (for example, a 16-bit key = $2^{16} = 65,536$ possible keys, while a 56-bit key = $7.2 * 10^{16}$ possible keys). Scalability provides flexible key length, and the strength or speed of encryption can be selected as needed.
- **Avalanche effect:** When only a small part of the plaintext message is changed (a few bits), and that small change causes its ciphertext to change completely, the algorithm has an avalanche effect. The avalanche effect is a desired feature because it allows very similar messages to be sent over an untrusted medium, with their encrypted (ciphertext) messages being completely different.

Symmetric Encryption

This topic describes how symmetric encryption works, when it is used, and which symmetric algorithms are commonly used for data security today.



Symmetric encryption has two main characteristics: It is very fast (compared to asymmetric encryption) and uses the same key for encryption and decryption. As a consequence, the *same* key has to be known by the sender and the receiver. To ensure confidentiality, nobody else is allowed to know the key. Such keys are also called *shared secrets*.

Symmetric encryption has been used for decades, and there are several algorithms that are commonly used. Among the best-known and most widely trusted symmetric encryption algorithms are Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA), the RC series (RC2, RC4, RC5, RC6), Software Encryption Algorithm (SEAL), and Blowfish.

They are all based on the same concept: They have two types of input (the cleartext and the key) and produce unreadable output (the ciphertext). For decryption, the ciphertext and the key are the input data and the original cleartext is the output.

Symmetric Encryption Considerations

Cisco.com

- **Used for bulk data encryption (e-mail, IPSec packets, SRTP, HTTPS)**
- **Key management difficult:**
 - **Same secret key must be available to both parties**
 - **Different key per pair of devices**
 - **Keys should be changed frequently**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-8

Symmetric algorithms are usually very simple in their structure, therefore quite fast, and as a consequence, they are often used for wire-speed real-time encryption in data networks. They are, in their essence, based on simple mathematical operations and can be easily hardware-accelerated using specialized encryption application-specific integrated circuits (ASICs). Typical applications are e-mail, IPsec, Secure Real-Time Transfer Protocol (SRTP), or Secure HTTP (HTTPS).

Keys should be changed frequently because they could be discovered otherwise, and loss of privacy would be the consequence. The “safe” lifetime of keys depends on the algorithm, the volume of data for which they are used, the key length, and the time period for which the keys are used. The key length is usually 128 to 256 bits.

Because of the limited lifetime (usually hours to days) and the fact that each pair of devices should use a different key, key management is rather difficult.

Symmetric Encryption Example: AES

Cisco.com

- **Algorithm developed by Joan Daemen and Vincent Rijmen**
- **Publicly announced by NIST in 2000**
- **128-, 192-, or 256-bit key length**
- **Much faster and more efficient than 3DES**
- **Used in IP telephony for SRTP (media) and signaling encryption**

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-1.0

AES History

For a number of years, it had been recognized that Data Encryption Standard (DES) would eventually reach the end of its useful life. In 1997, the AES initiative was announced, and the public was invited to propose encryption schemes, one of which could be chosen as the encryption standard to replace DES.

On October 2, 2000, the U.S. National Institute of Standards and Technology (NIST) announced the selection of the Rijndael cipher as the AES algorithm. The Rijndael cipher, developed by Joan Daemen and Vincent Rijmen, has a variable block length and key length. The algorithm currently specifies how to use keys with lengths of 128, 192, or 256 bits to encrypt blocks with lengths of 128, 192, or 256 bits (all nine combinations of key length and block length are possible). Both block length and key length can be extended very easily to multiples of 32 bits, allowing the algorithm to scale with security requirements of the future.

The U.S. Department of Commerce approved the adoption of AES as an official U.S. government standard, effective May 26, 2002.

AES versus 3DES

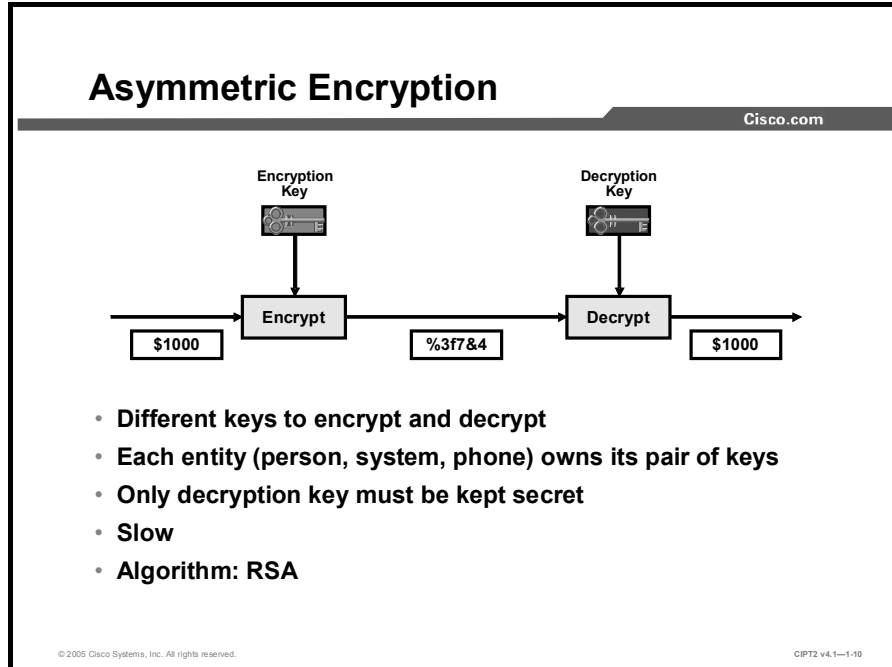
AES was chosen to replace DES and 3DES, because they are either too weak (DES, in terms of key length) or too slow (3DES) to run on modern, efficient hardware. AES is therefore more efficient on the same hardware (much faster, usually by a factor of around five compared to 3DES), and is more suitable for high-throughput, low-latency environments, especially if pure software encryption is used. However, AES is a relatively young algorithm, and, as the golden rule of cryptography states, a more mature algorithm is always more trusted. 3DES is therefore a more conservative and more trusted choice in terms of strength, because it has been analyzed for around 30 years. AES has also been thoroughly analyzed during the selection process, and is considered mature enough for most applications.

AES in IP Telephony

AES is the algorithm for encrypting both IP Phone-to-Cisco CallManager communication (signaling with Transport Layer Security [TLS] protection) and phone-to-phone and phone-to-gateway (media with SRTP protection) channels in Cisco IP telephony.

Asymmetric Encryption

This topic describes how asymmetric encryption works, when it is used, and which asymmetric algorithm is commonly used for data security today.



Asymmetric algorithms (also sometimes called public-key algorithms) are designed in such a way that the key used for encryption is different from the key used for decryption. The decryption key cannot (at least in any reasonable amount of time) be calculated from the encryption key and vice versa.

The main feature of asymmetric encryption algorithms is that the encryption key (often called the *public key*) does not have to be secret—it can be published freely and anyone can use this key to encrypt data. The corresponding decryption key (often called the *private key*), however, is known only to a single entity that can decrypt data encrypted with the encryption key. Therefore, when you need to send an encrypted message to someone else, you first obtain the public (encryption) key of the other person and transform the message with it. Only the recipient knows the private (decryption) key and can therefore decrypt the message.

Asymmetric algorithms are relatively slow (up to 1000 times slower than symmetric algorithms). Their design is based on computational problems, such as factoring extremely large numbers or computing discrete logarithms of extremely large numbers.

The best-known asymmetric cryptographic algorithms are the Rivest, Shamir, and Adleman (RSA), ElGamal, and elliptic curve algorithms. RSA is recommended because it is widely trusted for its resistance against attacks and well-known internals.

Asymmetric Encryption Considerations

Cisco.com

- **Used for encrypting small amounts of data (for example, to encrypt symmetric keys)**
- **Key management simpler than with symmetric encryption keys:**
 - **One of the keys can be publicly available.**
 - **Each device has one key pair.**
 - **Keys can be used for longer periods.**

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-1-11

Because of their lack of speed, asymmetric encryption algorithms are usually used to protect small quantities of data (digital signatures, key exchange).

Key management tends to be simpler compared to symmetric (secret key) algorithms. As stated before, with asymmetric encryption, each device has a pair of keys (public and private). The public key of each device has to be publicly available (known by all other devices) to allow a full mesh of encrypted communication, while with symmetric encryption different symmetric keys have to be safely distributed for each combination of two peers.

Asymmetric keys are usually used for longer time (months to years).

Asymmetric Encryption Example: RSA

Cisco.com

- **Algorithm developed by Ron Rivest, Adi Shamir, and Len Adleman in 1977**
- **Public domain since patent expired in 2000**
- **Key length is usually from 1024 to 2048 bits**
- **RSA can be used for:**
 - **Confidentiality—Data is encrypted with public key of the receiver**
 - **Digital signatures—Data is encrypted with private key of the sender**

© 2005 Cisco Systems, Inc. All rights reserved.

CIP72 v4.1—1-12

RSA History

Ronald L. Rivest, Adi Shamir, and Leonard M Adleman invented the RSA algorithm in 1977. It was a patented public-key algorithm, and its patent expired in September 2000, putting the algorithm in the public domain. Of all the public-key algorithms proposed over the years, RSA is still the most strongly preferred.

RSA has withstood years of extensive cryptanalysis, and although analysis has neither proven nor disproven the security of the RSA algorithm, it does suggest a justifiable confidence. The security of RSA is based on the difficulty of factoring very large numbers, that is, breaking them into multiplicative factors. If an easy method of factoring these large numbers were discovered, the effectiveness of RSA would be destroyed (and, as a side effect, mathematics might take a huge leap).

RSA keys are usually 1024 to 2048 bits long.

RSA Applications

RSA, like all asymmetric encryption algorithms, can be used in two different ways:

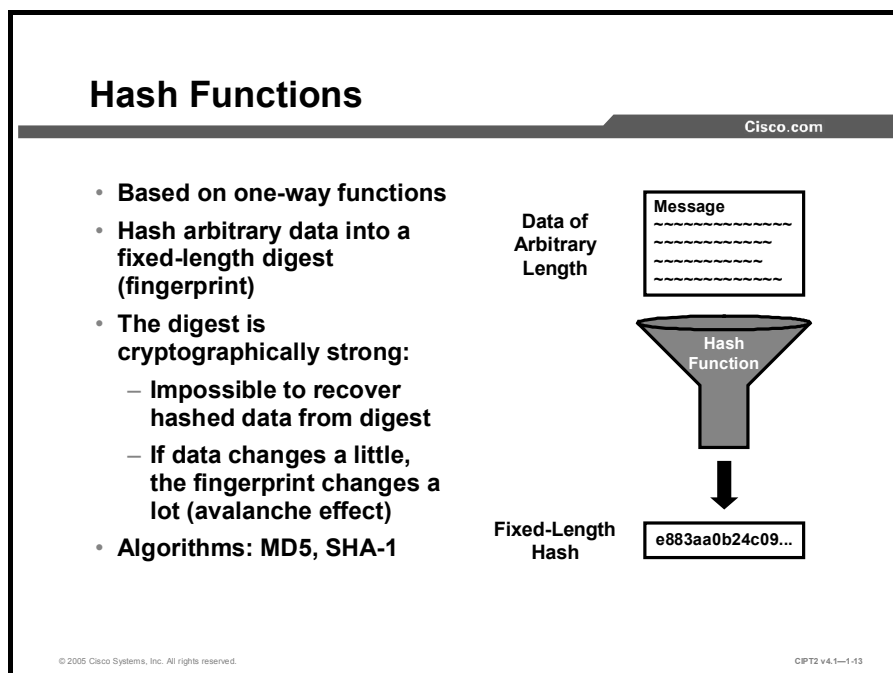
- **Confidentiality:** The sender encrypts the data with the public key of the receiver. This guarantees that only the receiver can decrypt the data.
- **Authenticity of digital signatures:** The sender uses its private key to sign (encrypt) the data. Such a signature can be verified by everybody because only the public key is needed to verify (decrypt) the signature.

RSA in IP Telephony

RSA is used for device authentication (IP Phone to Cisco CallManager and vice versa) in Cisco IP telephony.

Hash Functions

This topic describes what hash functions are and how they can be used for authentication.



Hash functions are used for several cryptographic applications. They can be used for secure password verification or storage and are also a base component for data authentication.

Hashing is a one-way function of input data, which produces fixed-length output data, the digest. The digest uniquely identifies the input data and is cryptographically very strong, that is, it is impossible to recover input data from its digest, and if the input data changes just a little, the digest (fingerprint) changes substantially (avalanche effect). Therefore, high-volume data can be identified by its (shorter) digest. For this reason, the digest is called a fingerprint of the data. Given only a digest, it is not computationally feasible to generate data that would result in such a digest.

The figure illustrates how hashing is performed. Data of arbitrary length is input to the hash function, and the result of the hash function is the fixed-length hash (digest, fingerprint). Hashing is similar to the calculation of cyclic redundancy check (CRC) checksums, except that it is much stronger from cryptographic point of view. With CRC, given a CRC value, it is easy to generate data with the same CRC. However, with hash functions, this is not computationally feasible for an attacker.

The two best-known hashing functions are these:

- Message Digest 5 (MD5), with 128-bit digests
- Secure Hash Algorithm 1 (SHA-1), with 160-bit digests

There is considerable evidence that MD5 may not be as strong as originally envisioned and that collisions (different inputs resulting in the same fingerprint) are more likely to occur than designed for. Therefore, MD5 should be avoided as an algorithm of choice and SHA-1 used instead.

The SHA-1 Algorithm

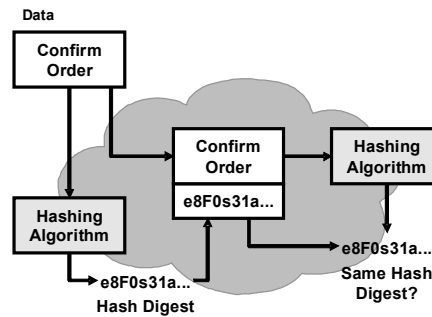
NIST developed SHA, the algorithm specified in the Secure Hash Standard. SHA-1 is a revision to SHA that was published in 1994; the revision corrected an unpublished flaw in SHA. Its design is very similar to the MD4 family of hash functions developed by Rivest.

The algorithm takes a message of no less than 264 bits in length and produces a 160-bit message digest. The algorithm is slightly slower than MD5, but the larger message digest makes it more secure against brute-force collision and inversion attacks.

Lack of Security in Pure Hashing

Cisco.com

- Only the algorithm has to be known to create a valid hash—algorithms are well-known
- Attacker changing the data can easily create a new hash
- Receiver cannot detect the manipulation
- For security, a secret element has to be added to the computation



© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-1-14

The figure illustrates hashing in action. The sender wants to ensure that the message will not be altered on its way to the receiver. The sender uses the message as the input to a hashing algorithm and computes its fixed length digest or fingerprint. This fingerprint is then attached to the message (the message and the hash are cleartext) and sent to the receiver. The receiver removes the fingerprint from the message and uses the message as input to the same hashing algorithm. If the hash computed by the receiver is equal to the one attached to the message, the message has not been altered during transit.

Be aware that there is no security added to the message in this example. Why? When the message traverses the network, a potential attacker could intercept the message, change it, recalculate the hash, and append the newly recalculated fingerprint to the message (a man-in-the-middle interception attack). Hashing only prevents the message from being changed accidentally (that is, by a communication error). There is nothing unique to the sender in the hashing procedure; therefore, anyone can compute a hash for any data, as long as they know the correct hash algorithm.

Thus, hash functions are helpful to ensure that data was not changed accidentally but cannot ensure that data was not deliberately changed. For the latter, you need to employ hash functions in the context of HMAC. They will extend hashes by adding a secure component.

Hash-Based Message Authentication Code

Cisco.com

- **A secret key is added to the data as input to the hash function.**
- **The secret key is known to the sender and to the receiver:**
 - **Symmetric nature**
 - **Provides authentication and integrity assurance**
- **It does not provide nonrepudiation because the receiver could pretend to be the sender.**
- **Fast**
- **Based on existing hash functions:**
 - **Keyed MD5—128-bit key and hash**
 - **Keyed SHA-1—160-bit key and hash**
- **Keyed SHA-1 HMAC used in IP telephony for signaling and media protection**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1—1-15

HMAC uses existing hash functions, but with the significant difference of adding an additional secret key as the input to the hash function when calculating the digest (fingerprint). Only the sender and the receiver share the secret key, and the output of the hash function now depends on the input data and the secret key. Therefore, only parties who have access to that secret key can compute or verify the digest of a HMAC function. This defeats man-in-the-middle attacks and also provides authentication of data origin. If only two parties share a secret HMAC key and use HMAC functions for authentication, the receiver of a properly constructed HMAC digest with a message can be sure that the other party was the originator of the message, because that other party is the only other entity possessing the secret key. However, because both parties know the key, HMAC does not provide nonrepudiation. For the latter, every entity would need its own secret key instead of having a secret key shared between two parties.

HMAC functions are generally fast and are often applied in these situations:

- To provide a fast proof of message authenticity and integrity among parties sharing the secret key, such as with IPsec packets or routing protocol authentication
- To generate one-time (and one-way) responses to challenges in authentication protocols (such as PPP Challenge Handshake Authentication Protocol [CHAP], Microsoft NT Domain, and Extensible Authentication Protocol-MD5 [EAP-MD5])
- To provide proof of integrity of bulk data, such as with file-integrity checkers (for example, Tripwire), or with document signing (digitally signed contracts, public-key infrastructure [PKI] certificates)

Some well-known HMAC functions are:

- Keyed MD5, based on the MD5 hashing algorithm, which should be avoided
- Keyed SHA-1, based on the SHA-1 hashing algorithm, which is recommended

Cisco IP telephony uses SHA-1 HMAC for protecting signaling traffic and media exchange.

Digital Signatures

This topic describes what digital signatures are, how they work, and how they can be used for authentication.

Digital Signatures

Cisco.com

- **Provide three key security services:**
 - Data authenticity
 - Data integrity
 - Nonrepudiation of data
- **Are based on asymmetric cryptographic methods:**
 - Signature-generating key
 - Signature-verification key
- **Are slower than HMAC:**
 - Not used for real-time traffic
 - Used for device authentication and exchange of symmetric keys

© 2005 Cisco Systems, Inc. All rights reserved. CPT2 v4.1-1-16

Digital signatures are verification data appended to the data that is to be signed. They provide three basic security services in secure communications:

- **Authenticity of digitally signed data:** Authentication of source, proving that a certain party has signed the data in question.
- **Integrity of digitally signed data:** Guarantee that the data has not changed since being signed by the signer.
- **Nonrepudiation of the transaction:** The recipient can take the data to a third party, which will accept the digital signature as a proof that this data exchange really did take place. The signing party cannot repudiate (that is, deny) that it has signed the data.

Digital signatures are usually based on asymmetric encryption algorithms to generate and verify digital signatures. Compared to using asymmetric encryption for confidentiality, the usage of the keys is reversed when creating digital signatures: The private key is used to create the signature, and the public key is used to verify the signature.

Because digital signatures are based on asymmetric (slow) algorithms, they are not used today to provide real-time authenticity and integrity guarantees to network traffic. In network protocols, they are usually used as a proof of endpoint (client, server, and phone) identity when two entities initially connect (for example, an IP Phone authenticating to Cisco CallManager, or a Cisco VPN Client authenticating to a Cisco VPN Concentrator). For real-time protection of authenticity and integrity, which do not require nonrepudiation (for example, signaling messages between IP Phones and a Cisco CallManager, or IPsec packet protection), HMAC methods are used instead.

Digital Signatures and RSA

Cisco.com

- **Digital signatures require a key pair per entity:**
 - One key for creating a signature
 - The other key to verify the signature
- **RSA can be used for that purpose**
- **Application of RSA is reversed compared to RSA data encryption:**
 - **Private key used to create the signature (encrypt the data)**
 - **Public key used to verify the signature (decrypt the data)**

© 2005 Cisco Systems, Inc. All rights reserved.

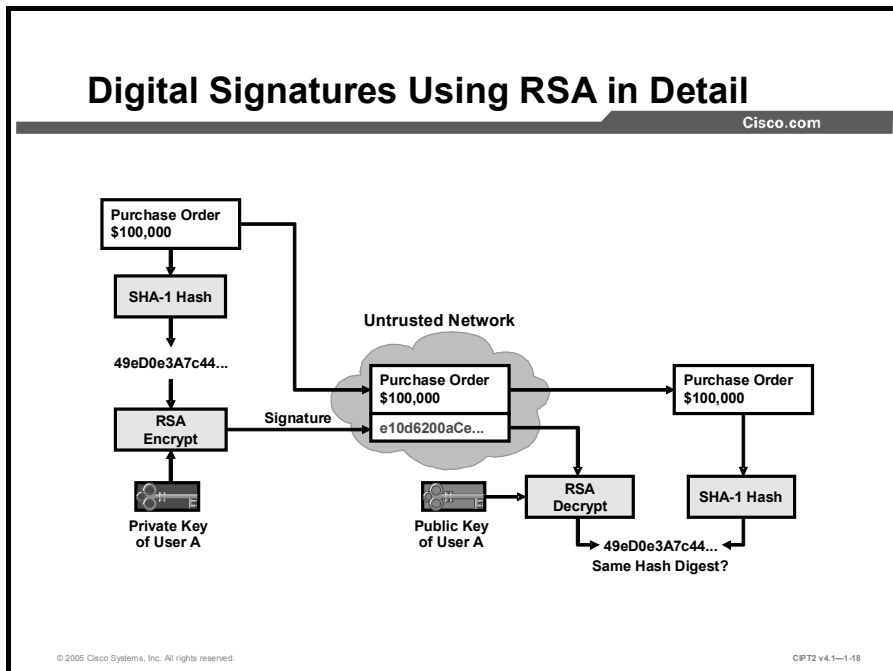
CIPT2 v4.1-1-17

Digital signatures require a key pair for each device that wants to create signatures. One key is used to create signatures and the other is used to verify signatures. RSA can be used for that purpose. The usage of the RSA keys for digital signatures is opposite to their usage for encryption:

- **Digital signatures:** The signer uses its private key to sign (encrypt) data. The signature is checked by a recipient that is using the public key of the signer to verify (decrypt) the signature.
- **Encryption:** The sender encrypts the data with the public key of the receiver. This guarantees that only the receiver can decrypt the data, because the encrypted data can only be decrypted by the holder of the private key.

Digital Signatures Using RSA in Detail

Cisco.com



RSA is extremely slow and not designed for real-time encryption of a large volume of data. Therefore, when it is used to create signatures, the data that are to be signed is first hashed, and only the hash digest is signed by RSA (encrypted with the private key). This practice significantly improves performance, because RSA transforms only the fingerprint of the data (not all of the data). The signature process, illustrated in the figure, is as follows:

Step 1 The signer makes a hash (fingerprint) of the document, which uniquely identifies the document and all its contents.

Note There are two reasons why a hash of the data is created: First, RSA is extremely slow, and it is more efficient to sign only the (shorter) fingerprint than to sign the whole of the data. Next, if the transferred information should be out-of-band verified, it is simpler to compare the shorter fingerprint than to compare all the transferred information.

Step 2 The signer encrypts the hash only with its private key.

Step 3 The encrypted hash (the signature) is appended to the document.

The verification process works as follows:

Step 1 The verifier obtains the public key of the signer.

Step 2 The verifier decrypts the signature with the public key of the signer. This process unveils the assumed hash value of the signer.

Step 3 The verifier makes a hash of the received document (without its signature) and compares this hash to the decrypted signature hash. If the hashes match, the document is authentic (that is, it has been signed by the assumed signer) and has not been changed since the signer signed it.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Cryptography is the science of transforming cleartext into ciphertext and transforming the ciphertext back into cleartext.**
- **Symmetric encryption uses the same key for encryption and decryption.**
- **With symmetric encryption, a different key is needed per pair of devices.**
- **Asymmetric encryption uses a different key for encryption and decryption.**
- **With asymmetric encryption, each device needs a pair of keys.**
- **Hashes are one-way functions that can be used to authenticate data if a secret value, shared between the two peers, is added to the input data.**
- **Digital signatures sign data by using asymmetric encryption to encrypt fingerprints (hashes) of the data.**

© 2005 Cisco Systems, Inc. All rights reserved. CIP12 v4.1-1-19

Understanding PKI

Overview

Cisco CallManager Release 4.0 and later supports many security features that are based on a public-key infrastructure (PKI) solution. In earlier releases, Cisco CallManager did not use PKI-like features, and many Cisco CallManager administrators are not familiar with PKI. This lesson discusses the concept of a PKI, its components, and its applications.

Objectives

Upon completing this lesson, you will be able to describe the concept of PKI, describe the function of certificates and how they are issued, and explain how PKI can secure applications. This ability includes being able to meet these objectives:

- Describe the problem of secure, scalable distribution of public keys and present PKI as a solution
- Explain the concept of a trusted introducer
- Explain certificates, CAs, certification paths, certificate trust, and revocation lists
- Explain the certificate enrollment procedure
- Explain PKI certificate revocation
- Explain the use of PKI in existing applications

The Need for a PKI

This topic describes when a PKI is helpful and what problems it solves.

Key Distribution Issues

Cisco.com

Secure and scalable key exchange is the main issue when deploying cryptography:

- **Symmetric cryptography:**
 - **Keys should be changed frequently.**
 - **Distribution of the keys to the peers is needed.**
 - **Confidentiality of key exchange is needed.**
- **Asymmetric cryptography:**
 - **Public keys need to be known at all devices.**
 - **Distribution of public keys is needed.**
 - **Authenticity of key exchange is needed.**

© 2005 Cisco Systems, Inc. All rights reserved.CIPT2 v4.1-1.3

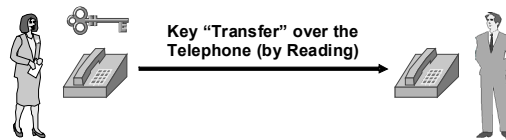
Scalable and secure key exchange is the main issue when deploying cryptography. Depending on the cryptographic algorithm that is used, there are different needs.

In symmetric encryption, the keys should be changed frequently. They are shared between two peers. But how can you get the keys safely to the peers? Symmetric keys should be known only by the two peers using them, and therefore *confidentiality* must be ensured for the key exchange.

In asymmetric encryption, the public key of a device has to be known by all other devices (made public). But how can you distribute the public keys safely to your devices? You have to ensure that the public keys that are exchanged over the network are authentic, and hence *authenticity* must be ensured for that key exchange.

Key Exchange in Symmetric Cryptography

Cisco.com



- **Out-of-band manual exchange:**
 - Over the phone, by mail, or on media, such as CDs
 - Does not scale
- **Two options for automated exchange:**
 - Diffie-Hellman algorithm
 - Exchange of keys protected by asymmetric encryption algorithm

© 2005 Cisco Systems, Inc. All rights reserved.

C IPT2 v4.1-1-4

When exchanging keys in symmetric cryptography, there are two possible options: You can use out-of-band manual key exchange or you can use in-band automated key exchange.

Manual Key Exchange

Manual key exchange is the simplest method of exchanging secret keying material. However, it does not scale and often relies on the human operator to perform the procedure securely. Every peer with which the entity wants to exchange encrypted traffic must go through a one-time manual key exchange. After the keys are generated, the two parties exchange the keys manually, through a secure channel (for example, by telephone, or in person). This process should include an out-of-band method of authentication to ensure that the keys were exchanged unaltered with the right party. This concept is often applied when using authenticated routing protocol updates, where the symmetric key that is used for the authentication has to be entered on all participating routers. If multiple router administrators are involved, they can exchange the symmetric key in person or use some other protected channel (such as encrypted e-mail and Secure Shell [SSH Protocol]).

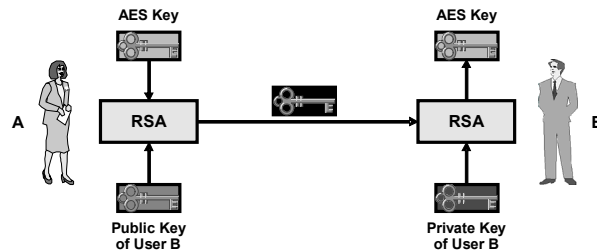
Automated Key Exchange

Most key exchanges are automated and do not require any human intervention. A couple of good methods for automatic key exchange are heavily used in modern cryptosystems. One of them is the Diffie-Hellman algorithm, which allows two peers to compute the same value (key) without exchanging all information that is needed for that computation. Another method is to send the actual symmetric keys but encrypt them using an asymmetric encryption algorithm first.

In Cisco IP telephony, asymmetric encryption algorithms are used to exchange symmetric keys securely.

Key Exchange Protected by Asymmetric Encryption

Cisco.com



1. **Symmetric key is generated by one peer**
2. **Key is encrypted with the public key of the receiver and sent over the network**
3. **Only receiver can decrypt the message by using its private key**
4. **Relies on knowledge of public keys of all possible peers**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1.5

When using asymmetric encryption to secure the automated exchange of symmetric keys, the keys are encrypted with the public key of the receiver and then sent over the untrusted network. Only the receiver can decrypt the message (the keys) because only the receiver knows the corresponding private key. This solution relies on the knowledge of public keys of all possible peers at all the participating devices.

At the end, both methods that can be used to secure automated symmetric key exchange have their problems or limitations.

In the example, user A wants to use symmetric encryption with user B. For secure key exchange, asymmetric encryption will be used in this way:

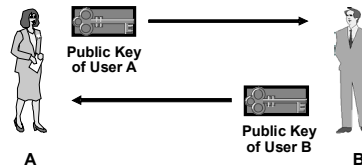
- Step 1** User A generates the symmetric key.
- Step 2** User A encrypts the symmetric key with the public key of user B and sends the encrypted key over the untrusted network to user B.
- Step 3** User B decrypts the key using his private key.
- Step 4** Now both of them know the symmetric key and can start using it for encrypting their communication channel.

As mentioned before, this solution assumes that user A securely (authenticated) knows the public key of user B.

Key Exchange in Asymmetric Cryptography

Cisco.com

- All entities have to know public keys of all other entities.
- Although the key is not secret, exchange of public keys has to be secured:
 - Authenticity is needed.
 - Otherwise a man-in-the-middle attack can replace a public key in transit with its own.
 - This problem is addressed by PKI.



© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-1-6

Asymmetric algorithms offer the advantage of one of the keys being public, which simplifies key exchange and distribution. The pitfall of this approach is not obvious at first glance. Obtaining the public key from another person can be very tricky. Although it is true that public keys are public information and can be published in a well-known directory, an extremely important issue remains: When I receive public key from someone, how do I really know it belongs to that person?

When a public key is requested or is sent over an untrusted network, an attacker could intercept that key and substitute another public key for it. This man-in-the-middle attack would cause the message sender to encrypt all messages with the public key of the attacker. A mechanism is therefore needed that allows verification of the relationship between a name of an entity and its public key. The PKI is the solution to this problem and allows such systems to scale, although, on a smaller scale, alternative, manual solutions can be devised.

PKI as a Trusted Third-Party Protocol

This topic describes how PKI uses the concept of trusted “introducing” to provide scalability for public key exchange.

PKI as a Trusted Third-Party Protocol

Cisco.com

- **Does not eliminate the need for authenticity of public keys**
- **Solves scalability issues:**
 - **Uses a single trusted introducer**
 - **Only public key of the introducer has to be initially known and verified (for instance, out of band) by all other entities**
 - **Introducer will then guarantee authenticity of public keys of other entities**
 - **Uses certificates for each entity, signed by the introducer**

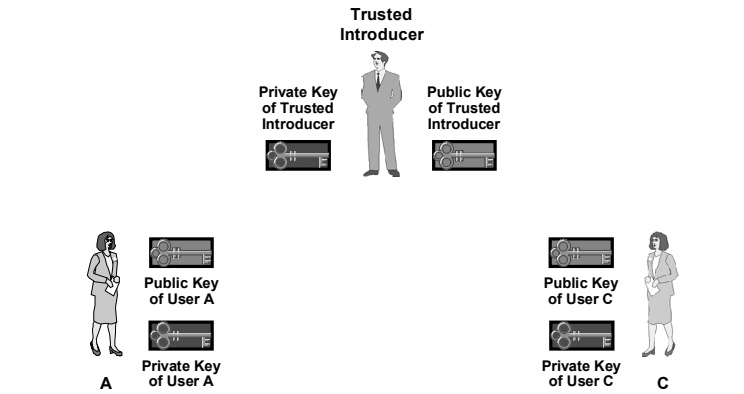
© 2005 Cisco Systems, Inc. All rights reserved. CIPT2 v4.1-1.7

PKI does not eliminate the need for authenticity when exchanging public keys in an asymmetric encryption environment, but PKI solves the scalability issues associated with that process. It uses the concept of a single, trusted introducer. Instead of securely exchanging all public keys among all devices, only the public key of the trusted introducer has to be securely distributed to all devices. This is usually done by downloading the public key and then verifying it out of band.

When all devices know the authentic key of the introducer, the introducer can guarantee the authenticity of the public keys of all devices by using a certificate for each device in the topology. The certificate includes information about the identity of a device and its public key. The (publicly trusted) introducer then signs the certificates of the individual devices, and the devices can directly distribute their public keys by sending their certificates. A device receiving such a certificate can verify it by checking the signature of the issuer (the introducer).

Trusted Introducing in PKI— Locally Generated Key Pairs

Cisco.com



Every entity, including the trusted introducer, has its own public and private key pair.

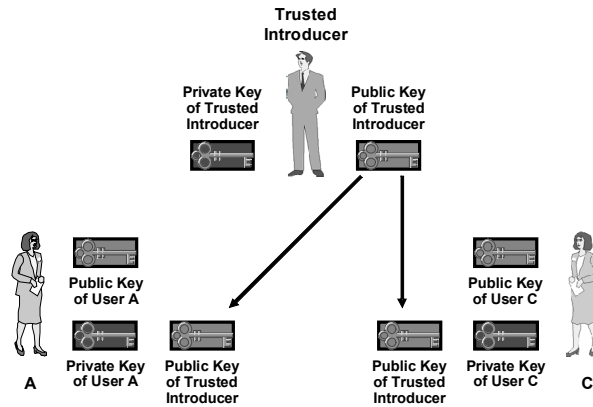
© 2005 Cisco Systems, Inc. All rights reserved.

C/PT2 v4.1—1-6

The concept of trusted introduction is shown in the figure. It illustrates a network where each entity has a pair of asymmetric keys—a public and a private key. User A and user C wish to communicate securely, and the trusted introducer is the trusted third party, who is unconditionally trusted by all other users.

Distribution of the Public Key of the Trusted Introducer

Cisco.com



Every entity gets the public key of the trusted introducer and verifies its authenticity (usually out of band).

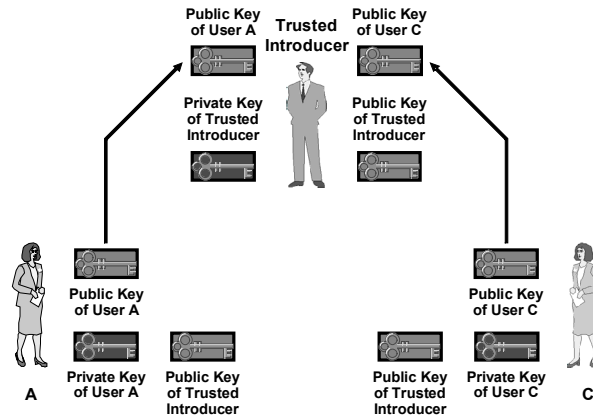
© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1.0

Every user in the system trusts information provided by the introducer. In practice, this is accomplished by digital signatures. Anything that the introducer signs is considered to be trusted. To verify the signatures of the trusted introducer, each user of this system must first obtain the public key of the trusted introducer, as shown in the figure.

Request for Signature of Public Keys of Entities

Cisco.com



Every entity submits its public key to the trusted introducer.

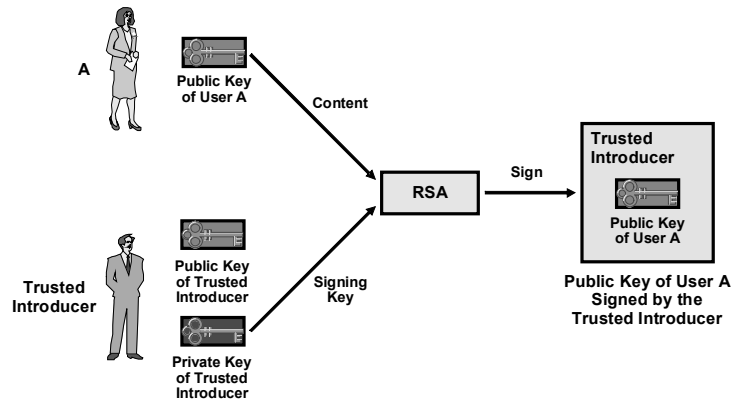
© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-10

To become a part of the trust system, all end users enroll with the introducer; that is, they submit their identity and their public key to the introducer.

Signing of Public Keys

Cisco.com



The trusted introducer digitally signs the submitted public keys.

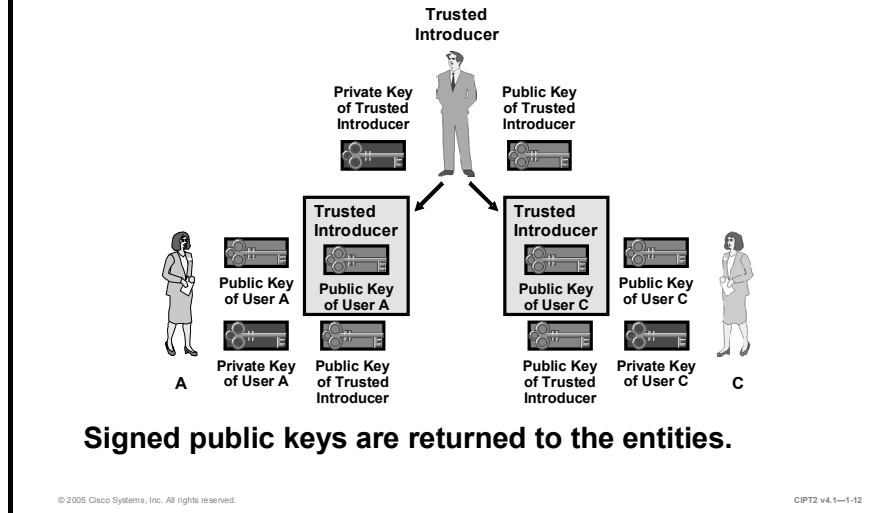
© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-1-11

As shown in the figure, the trusted introducer verifies the identity and public key of each enrolling user and, if they are correct, the trusted introducer digitally signs the submitted public key with the private key of the introducer. The result is a kind of “document” for each user that includes the identity (name) of the user and the public key of the user.

Providing Entities with Their Signed Public Keys

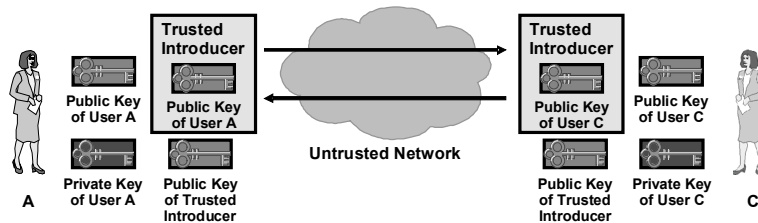
Cisco.com



The trusted introducer provides each user with his or her signed document, containing the name and public key of the user, bound together by the signature of the trusted introducer. As shown in the figure, each user now possesses his or her public and private key pair, the public key of the trusted introducer, and a document with the identity and public key of the user. This document is signed by the trusted introducer.

Public Key Exchange Between Entities Using Their Signed Public Keys

Cisco.com



- **Entities can now exchange their signed public keys with each other over an untrusted network.**
- **A received public key is verified with the public key of the trusted introducer, which each entity has available locally.**

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-1-13

Because every all users now have their own documents containing the correct name and public key, signed by the trusted introducer, and the public key of the trusted introducer, they can verify all data signed by the trusted introducer. The entities can now (independently of the trusted introducer) establish point-to-point trusted relationships by exchanging information about themselves in the form of that document.

In practice, this means that at this stage the end users can mutually exchange signed public keys over an insecure medium and use the digital signature of the trusted introducer as the protection mechanism for the exchange. Again, the signature of the trusted introducer is trusted because it can be verified (the entities have the public key of the trusted introducer), and the trusted introducer and its operations are considered to be secure.

PKI Entities

This topic describes components of PKI systems, their names, and their functions.

PKI Entities	
Term	Function
CA	The central authority (acting as the trusted introducer) Signs public keys of associated entities (PKI users)
PKI Users	Devices, users, or applications that want to safely distribute their public keys
Certificates	Include the identity of a PKI entity, its public key, and a signature (created by the CA) Use standard format (X.509v3)
CRL	A list of certificates that should not be trusted anymore

© 2005 Cisco Systems, Inc. All rights reserved. CIP12 v4.1-1.14

A PKI is the service framework needed to support large-scale public key-based technologies. The PKI is a set of all the technical, organizational, and legal components needed to establish a system that enables large-scale use of public key cryptography to provide authenticity, confidentiality, integrity, and nonrepudiation services.

Two very important terms need to be defined when talking about a PKI:

- A *Certificate Authority* (CA) is the trusted third party (trusted introducer) that signs the public keys of all end-entities (PKI users).
- A *certificate* is a document that, in essence, binds the name of the entity and its public key that has been signed by the CA, so that every other entity will be able to trust it.

Note Certificates are not secret information and do not need to be encrypted in any way. The idea is not to hide anything but to ensure the authenticity and integrity of the information contained in the certificate.

Another term that is often used with a PKI is *certificate revocation list* (CRL). The CRL is a list of certificates that should not be trusted anymore. Examples of when a certificate is added to the CRL (“revoked”) include exposure or loss of the private key. A PKI user who receives a certificate should verify the CRL to ensure that the received certificate is not on the list of revoked certificates.

CA Examples

Many vendors offer CA servers as a managed service or as an end-user product:

- Microsoft Windows 2000 Certificate Services (www.microsoft.com) is a Windows Server add-on that allows an organization to set up its own CA server.
- VeriSign (www.verisign.com) offers outsourced PKI services.
- Entrust Technologies (www.entrust.com) offers both PKI products and outsourcing services.
- The CA Proxy Function (CAPF) in Cisco CallManager can act as a stand-alone CA.

X.509v3 Certificates

Cisco.com

Certificate Format Version	Version 3
Certificate Serial Number	12457801
Signature Algorithm Identifier for CA	RSA with SHA-1
Issuer X.500 Name	C=US O=Cisco CN=CA
Validity Period	Start=04/01/04 Expire=04/01/09
Subject X.500 Name	C=US O=Cisco CN=CCMCluster001
Subject Public Key Information	756ECE0C9ADC7140...
Extension(s) (v3)	
CA Signature	2C086C7FE0B6E90DA396AB...

© 2005 Cisco Systems, Inc. All rights reserved.

CIP72 v4.1-1-15

X.509 is the ubiquitous and well-known standard that defines basic PKI data formats, such as certificate and CRL format, to enable basic interoperability. This format is already extensively used in the infrastructure of the Internet. X.509 is used for these applications:

- With secure web servers for website authentication in the Secure Socket Layer (SSL) protocol
- With web browsers for services that implement client certificates in the SSL protocol
- With user mail agents that support mail protection using the Secure/Multipurpose Internet Mail Extensions (S/MIME) protocol
- In IPsec virtual private networks (VPNs) where certificates can be used as a public key distribution mechanism for Internet Key Exchange (IKE) Rivest, Shamir, and Adleman (RSA)-based authentication

The figure shows an example certificate format, following X.509 Version 3 (X.509v3). The most important pieces of information contained in the certificate are these:

- Name of the holder
- Public key
- Signature of the CA

Other fields include these:

- Certificate serial number
- Certificate validity period
- Algorithms used to generate the signature of the CA

Self-Signed Certificates

Cisco.com

- **CA, as the root of a PKI, signs its own certificate (self-signed “CA certificate”).**
- **Sometimes entities issue self-signed certificates:**
 - **If they are not part of a PKI (not associated with a CA) but use PKI-enabled applications**
 - **Cannot be verified automatically**
 - **Need additional methods of verification (such as manual verification)**

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-1-16

In a PKI system, all public keys are distributed in a form of a certificate, including the certificate of the trusted introducer, the CA. The obvious question is: Who signs the certificate of the CA, if it is itself the signer of all other certificates? In reality, the CA also issues a certificate to itself, just to have a consistent format for distributing its public key. This process is how the end entities obtain the public key of the CA—by obtaining its self-signed certificate. The signature of a self-signed certificate of the CA cannot be verified using the standard method (verification by using the public key of the signer) because that public key should actually be protected by the signature. Therefore, other methods (such as manual verification) are needed to ensure the authenticity of a CA certificate.

End Entities and Self-Signed Certificates

Sometimes end entities also sign their own certificates. This happens if that particular end entity is not a part of a PKI but uses a PKI-enabled application. For example, a web server could generate a private and public RSA key and sign its public key with its private key to create a self-signed certificate. This certificate could then be used in Secure HTTP (HTTPS), where the web server would present a self-signed certificate to the connecting web browser. However, how does the web browser verify the presented certificate, if it was not issued (signed) by a known CA for which the web browser has a locally available certificate? This web server certificate therefore cannot be accepted automatically, but needs to be verified using some other method (such as the manual, out-of-band verification that is also used in pre-PKI protocols).

PKI Enrollment

This topic describes how PKI users are added to a PKI system securely.

PKI Enrollment

Cisco.com

- **Enrollment is the procedure of adding a new user to the PKI:**
 - **The PKI user has to receive the CA certificate.**
 - **The CA needs to receive the identity and public key of the user, sign them, and return a signed certificate to the user.**
- **Procedure is vulnerable to man-in-the-middle attacks—needs to be secured**

© 2005 Cisco Systems, Inc. All rights reserved.CIP12 v4.1-1-17

PKI enrollment is the process of adding a PKI user (such as a person, a device, or an application) to the PKI. The enrollment is done in the following way:

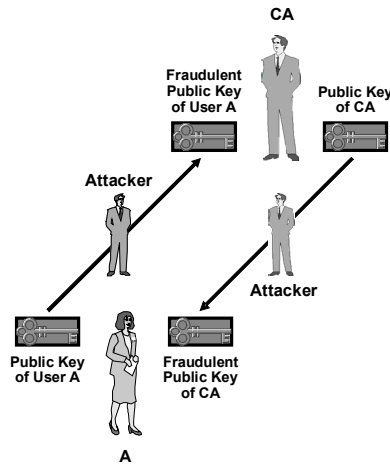
- An enrolling user obtains the CA certificate (self-signed) in which the public key of the CA is embedded. This public key will be used to verify the digital signature on certificates of the other entities.
- The enrolling user sends its identity information and public key to the CA.
- The CA verifies (authenticates) the user, signs the submitted information, and returns the signed data in the form of a certificate.
- The user verifies the returned certificate using the public key of the CA from the previously obtained CA certificate.

The enrollment procedure is the initial step of establishing trust between a user and the CA. If the process is executed over an untrusted network, it would be vulnerable to man-in-the-middle attacks. Therefore it has to be secured in such cases.

Man-in-the-Middle Attack During PKI Enrollment

Cisco.com

- Attacker can replace public key of the user by its own public key when asking real CA for a certificate (pretends to be the user to the CA)
- Attacker can replace CA certificate by a self-generated certificate (pretends to be the CA to the user)



© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-1-18

Without any additional protection for the enrollment process, a man-in-the-middle attack can be used to spoof identities:

- The attacker could replace the submitted public key of the user with the public key of the attacker, causing the CA to possibly issue a certificate to the attacker instead of to the legitimate user.
- The attacker could replace the real CA certificate with the false CA certificate of the attacker when the end user requests the certificate of the CA. The end user would then trust the CA of the attacker instead of the real CA.

Note The attacker would replace only the public key of the user, not the identity (name) of the user. When the CA issues the certificate, the attacker can pretend to be the user by presenting the certificate with the name of the user but the public key of the attacker.

Secure PKI Enrollment

Cisco.com

- **Authentication is needed for secure PKI enrollment:**
 - **User needs to verify certificate of the CA**
 - **CA needs to verify certificate of the user**
 - **Enrollment cannot be automated**
 - **Sent and received fingerprints of messages (certificates) have to be compared**
- **Authentication is not needed if enrollment is done over a secure network channel (physically separated network or network protected by IPSec).**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-19

To mitigate the risk of interception and key substitution during enrollment, the enrollment procedure needs to incorporate two out-of-band authentication procedures:

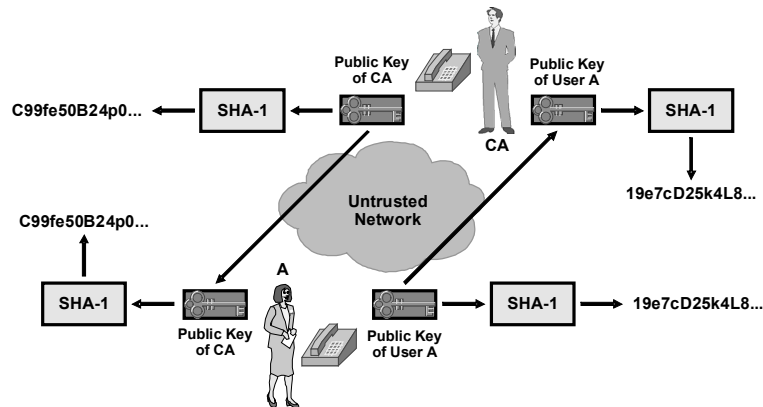
- Verification by the enrolling PKI user that the correct CA certificate has been received
- Verification by the CA that it has received the correct enrollment information from the enrolling PKI user

This can be done by out-of-band exchange of fingerprints of the messages (certificates). If the out-of-band received fingerprint matches the fingerprint of the received message, the message is authentic.

If the enrollment is completed over a secure network, where interception is not possible, those security procedures may be relaxed or omitted completely.

Authentication of PKI Enrollment

Cisco.com



Out-of-band verification (for example, over the telephone) of local fingerprint (hash) and remote fingerprint is needed.

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-20

The figure illustrates an out-of-band verification.

To verify that the correct CA certificate has been received, a local hash (fingerprint) of the received information is calculated. This fingerprint is compared to the true CA certificate fingerprint, obtained over the telephone or another secure channel. If they match, the true CA certificate has been received.

When the user submits identity and public key information, a local hash (fingerprint) of the submitted information is calculated again. The CA also performs a hashing procedure of the received information. The CA then compares its hash of the received information to the hash of the user of the submitted information over the telephone or any other secure channel. If the two hashes match, the CA has received an unmodified enrollment request.

PKI Revocation and Key Storage

This topic describes how to deal with compromised keys and how and where to store keys to prevent keys from being compromised.

PKI Revocation

Cisco.com

- **Certificates (and, hence, associated public and private keys) have a lifetime, which is usually relatively long (up to one year or more).**
- **Sometimes keys become invalid before expiration:**
 - **If the private key is compromised or lost**
 - **If the contract with the PKI user is terminated**
- **Certificate revocation is used in such cases—an announcement that a private key is no longer trusted.**

© 2005 Cisco Systems, Inc. All rights reserved. CIP12 v4.1-1.21

A certificate and the public key included in the certificate and its associated private key have a lifetime. When a certificate is issued, the CA sets the lifetime of the certificate. The lifetime of certificates is usually relatively long (months to years). But how do you handle a situation where a key becomes compromised before its expiration? This would happen if, for instance, a private key is stolen. In such a case, all other entities have to know not to trust that private key (and its corresponding public key).

Possible reasons why a certificate should not be trusted anymore include these:

- Private key compromise
- Contract termination for that PKI user
- Loss of private keys (for instance, because of device replacement)

A PKI can offer such a solution by revoking a certificate. Certificate revocation is the announcement that a private key is not trustworthy anymore. There are different methods for revoking a certificate.

PKI Revocation Methods

Cisco.com

- **Manual revocation:**
 - **Deleting the compromised certificates or keys on affected systems**
 - **Does not scale**
- **Automatic revocation:**
 - **Publishing a list of revoked certificates using a CRL, downloaded by PKI users**
 - **Providing an online service answering certificate status queries in real time using the OCSP**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-22

Keys that are not trusted anymore could be manually revoked by deleting the certificates and the corresponding keys on all affected systems. This process does not scale, so automatic revocation is needed.

Automatic revocation can be achieved by different methods:

- **CRLs:** These lists contain all certificates that are no longer valid. The CRL is signed by the CA and has a lifetime. It is stored in a Lightweight Directory Access Protocol (LDAP)-accessible directory or on a web server and made publicly available. It is the duty of the end user to download a fresh CRL after the lifetime of the current CRL has expired. Whenever an end user wants to use a certificate, it should be checked against the downloaded CRL.
- **Online Certificate Status Protocol (OCSP):** OCSP is a protocol designed for real-time verification of certificates against a database of revoked certificates. Upon receipt of a certificate of another user, the end user or device queries the OCSP server in real time to verify whether the received certificate has been revoked. OCSP is not yet widely used in the network infrastructure.

The main advantage of OCSP over CRLs is that it ensures up-to-date information because of the real-time verification of the certificate. CRLs may contain stale information, because they are issued periodically, usually every couple of hours. If a key is compromised, there is a window of vulnerability until the end user downloads a new CRL listing the certificate of the compromised system. To at least limit this window of vulnerability, the CRL lifetime is used.

Key Storage

Cisco.com

- **Private or shared secret keys should be considered at least as sensitive as the messages protected with the keys:**
 - **Ideally, keys are never stored anywhere in cleartext form or in user-accessible storage.**
- **Keys with long lifetimes, such as asymmetric keys, should be protected especially well:**
 - **Ideally, they are stored on smart cards or tokens.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1—1-23

Secret (for symmetric algorithms) and private (for asymmetric algorithms) keys must be stored securely, because forgery and loss of privacy could result if their secrecy is compromised. The measures taken to protect a secret or private key must be at least equal to the required security of the messages encrypted with that key. Ideally, keys are never stored in cleartext form or in user-accessible storage.

Keys, especially long-term keys (such as RSA) should be protected especially well. They are very often stored on nonvolatile storage media:

- **Hard drives:** For example, storing private RSA keys on a PC
- **Flash memory:** Sometimes, in the form of a Personal Computer Memory Card International Association (PCMCIA) card
- **Read-only memory (ROM):** For example, encryption keys that are hard-coded in hardware

Ideally, RSA keys are stored on smart cards or tokens where all key-related operations are done so that the key itself does not even have to leave that device.

Smart Cards and Smart Tokens

Cisco.com

Small “computers”:

- Providing tamper-resistant storage for protecting cryptographic keys and other information
- Allowing portability of private information between devices
- Isolating security-related functions involving authentication, digital signatures, and key exchange from other parts of the system
- Actual signing happens inside the smart device with the private key never leaving it



© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-24

A smart card or smart token is essentially a small computer, capable of performing basic cryptographic operations and containing the protected secret keys within its internal memory. The host computer, to which the smart-card reader is attached, simply passes challenges to the card, which, for example, computes an authentication response. This technique ensures that the private key never leaves the card and provides one of the strongest key-protection methods available today.

Any PKI-based application that uses certificates to distribute public keys can store the relevant private key on a smart card instead in some less well-protected memory (such as the hard disk of the end user). The application software then offloads all public key operations to the smart card.

Example

In Cisco IP telephony, the private RSA key used to sign the Certificate Trust List (CTL) is stored on a smart token and never leaves it. The smart token is a small computer that can sign data fed to it over the Universal Serial Bus (USB) interface.

Note More information on smart card and smart token technology can be found at www.opencard.org, www.chipcard.ibm.com, and www.gemplus.com.

PKI Examples

This topic describes some examples of PKI-enabled applications that are used frequently on the Internet.

PKI Examples

Cisco.com

- **SSL:**
 - **Designed for secured HTTP browsing**
 - **Used by sensitive web servers (for example, e-banking and e-commerce)**
- **TLS:**
 - **Successor of SSL**
 - **Application-independent**
- **S/MIME for secure messaging**

© 2005 Cisco Systems, Inc. All rights reserved. CIP12 v4.1-1-25

Among the first applications of a PKI were Internet browsers and web servers using SSL. With these applications, the web server authenticates to the browser using a PKI system. HTTPS is widely used on the Internet today and whenever secure web communication is needed (for example, online banking and e-commerce).

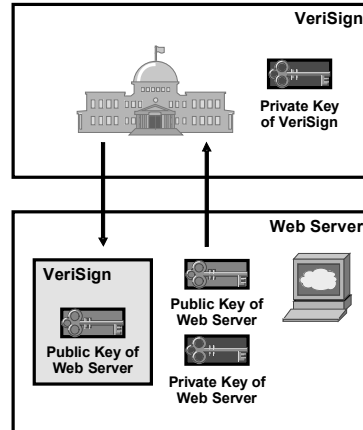
Transaction Layer Security (TLS) is the successor of SSL and is application-independent, hence not limited to HTTP traffic. TLS is very similar to SSL and also uses a PKI system to provide secure communication.

S/MIME, used for secure messaging, is another example of an application that relies on a PKI.

PKI and SSL/TLS

Cisco.com

- **Used for sensitive web applications**
- **The web server has a private and public key**
- **The web server has a certificate, usually issued by a public Internet CA (such as VeriSign)**



© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-26

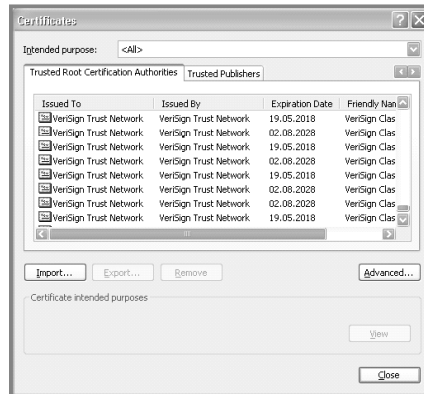
If a web server runs sensitive applications, SSL or TLS is used to secure the communication channel between the client and the server.

A company that needs to run a secure web server (a server supporting authenticated and encrypted HTTP sessions) first generates a public and private key on the web server. The public key is then sent to one of the Internet CAs, which, after verifying the identity of the submitter, issues a certificate to the server by signing the public key of the web server with the private key of the CA.

Internet CAs are mainly run by either specialized private companies (such as VeriSign), telecommunications companies, or governments. The certificates of those CAs are embedded at installation into client operating systems (such as Microsoft Windows) or inside browsers (such as Mozilla). The collection of embedded CA certificates serves as the trust anchor for the user. The user can then verify the validity of signatures of any other certificate signed using the public keys contained in those CA certificates.

Browser-Embedded CA Certificates

Cisco.com



A client operating systems or browser has more than 100 Internet CA certificates already embedded.

© 2005 Cisco Systems, Inc. All rights reserved.

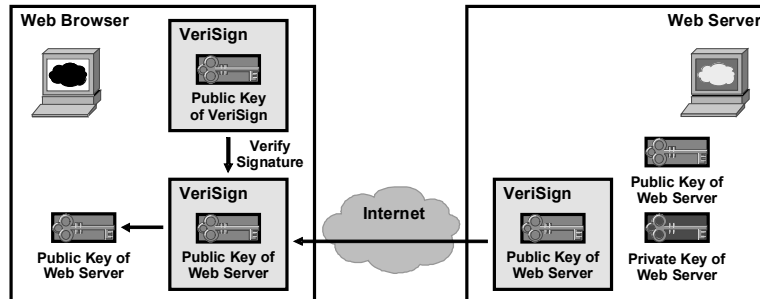
CIPT2 v4.1-1-27

The figure shows part of the list of the CA certificates embedded in the Microsoft Windows XP operating system.

To see the CA certificates installed in your computer, open Internet Explorer, choose **Tools > Internet Options**, choose the **Content** tab, click **Publishers**, and choose the **Trusted Root Certification Authorities** tab.

Web Server Certificate Verification

Cisco.com



- The server passes its certificate to the client at connection startup.
- The client verifies the certificate using the embedded certificate of the CA that has issued the certificate of the web server.
- The client extracts the public key of the web server from the certificate.

© 2005 Cisco Systems, Inc. All rights reserved.

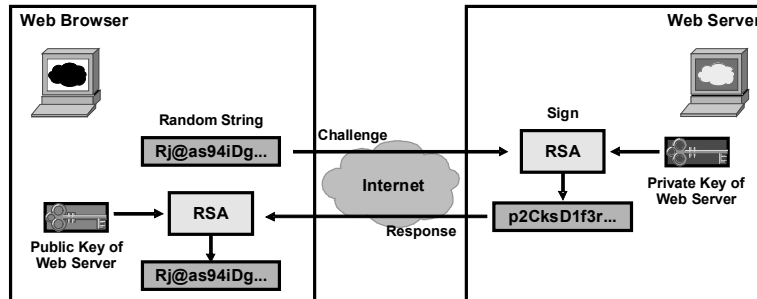
CIPT2 v4.1-1-28

When a browser contacts a secure web server using HTTPS, the first step of the protocol is to authenticate the web server—to verify that the browser indeed has connected to the correct web server, as desired by the user. Here is an example where a user connects to <https://www.amazon.com>:

- Authentication of the web server uses a challenge-response method, with which the server will prove that it possesses the private key of the desired server (www.amazon.com). However, to prove possession of the private key of the server, the browser needs the public key of the server first. Here is the sequence of events:
 1. When the client connects to the www.amazon.com web server, the web server first sends its certificate, signed by a well-known Internet CA to the client.
 2. The client uses one of the local CA certificates (the certificate of the issuer of the certificate of the server) to verify its validity, and optionally downloads the CRL to verify that the server certificate has not been revoked.
 3. If verification is successful, the client now knows that it has an authentic public key of the www.amazon.com server in its possession.

Web Server Authentication

Cisco.com



- The client sends random data to the web server.
- The web server uses its private key to sign the data and sends it back.
- The client verifies the returned data using the public key of the web server retrieved from the certificate.
- If returned data matches the sent data, the web server has the correct private key and therefore it is authentic.

© 2005 Cisco Systems, Inc. All rights reserved.

CIP72 v4.1-1-29

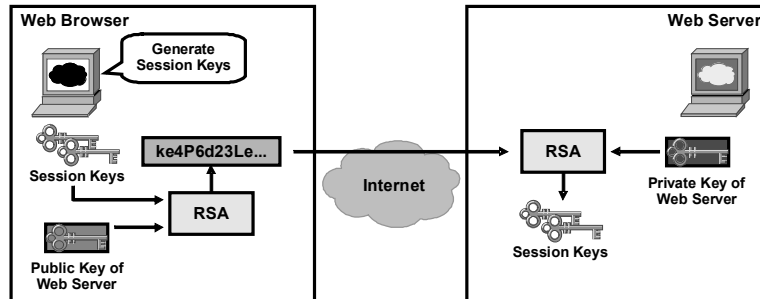
Next, the client challenges the web server to verify that the web server has the private key that belongs to the public key that the client received in the certificate of the web server. This private key should be known only to the www.amazon.com web server:

- The client generates random data, and sends it to the web server to be encrypted with the private key of the web server (challenge).
- The web server signs (RSA-encrypts) the random data using its private key and returns the signed random data to the client (response).
- The client verifies (RSA-decrypts) the signed random data using the public key of the server from the verified certificate and compares it against the random data that the client generated previously.
- If the signature is authentic, the web server really possesses the private key, corresponding to the public key in the certificate of the web server (www.amazon.com), and is therefore authentic.

Note In this example the web server was authenticated by the client; the web server, however, has no idea about the identity of the client. Authentication of the client is optional in SSL and TLS and, if used, would use exactly the reverse procedure to authenticate the client, provided that the client also possesses a private and public RSA key pair and a certificate recognized by the web server. However, most servers choose to authenticate the client using a simple username/password mechanism over the secure SSL/TLS session, because this method is easier to deploy than client-side certificates.

Exchange of Session Keys

Cisco.com



- The client generates symmetric session keys for encryption and HMAC algorithms to provide session protection.
- The client encrypts the keys using the public key of the web server and sends them to the web server.
- The web server (only) can decrypt the session keys using its private key.

© 2005 Cisco Systems, Inc. All rights reserved.

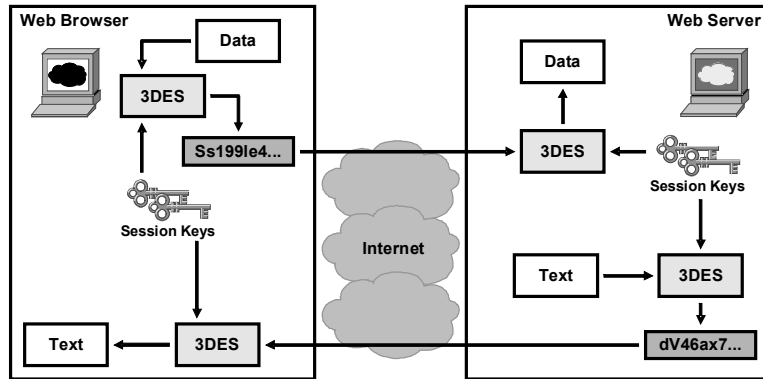
CIPT2 v4.1-1-30

Using the authentic certificate of the web server, the client can now send session keys, which are used by the symmetric encryption algorithm of SSL or TLS to communicate securely with the web server. As shown in the figure, the exchange of session keys is done in the following way:

- The client generates symmetric session keys for SSL or TLS Hash-Based Message Authentication Code (HMAC) and encryption algorithms.
- The client encrypts these keys using the `www.amazon.com` public key of the web server and sends them to the server.
- The `www.amazon.com` web server (only) can decrypt the such-encrypted session keys using its private key.

Session Encryption

Cisco.com



Packets between web server and client can now be signed (using HMAC, such as keyed MD5 or keyed SHA-1) and encrypted (using encryption algorithms, such as 3DES or RC4).

© 2005 Cisco Systems, Inc. All rights reserved.

CIP72 v4.1-1-31

Now, when the client and the server share the secret session keys, they can use them to exchange authenticated (signed using the HMAC algorithm) and encrypted (using a symmetric encryption algorithm, such as Triple Data Encryption Standard [3DES], Advanced Encryption Standard [AES], or RC4) messages, as shown in the figure.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **PKI is needed for secure, scalable key exchange.**
- **PKI uses the concept of a single trusted introducer to eliminate the need for any-to-any authentication.**
- **PKI entities, such as the CA and its associated users, have certificates issued by the CA.**
- **PKI enrollment is the process of adding new users to the system.**
- **PKI enrollment always needs separate authentication.**
- **PKI revocation allows certificates to be announced as invalid before the lifetime has expired.**
- **PKI revocation is needed when private keys become compromised and therefore cannot be trusted anymore.**
- **SSL, TLS, and S/MIME are common examples of PKI-enabled protocols.**

© 2005 Cisco Systems, Inc. All rights reserved.CPT2 v4.1—1-32

Understanding Cisco IP Telephony Authentication and Encryption Fundamentals

Overview

Cisco IP telephony systems are subject to several threats, including eavesdropping, identity spoofing, and denial of service (DoS) attacks. In Cisco CallManager Release 4.0 and later, the Cisco IP telephony solution can be secured against these threats by enabling authentication and encryption features. This lesson explains how authentication and encryption can be applied in a Cisco IP telephony environment.

Objectives

Upon completing this lesson, you will be able to explain what cryptographic services are available in a Cisco IP telephony environment and how a PKI is used to provide these services. This ability includes being able to meet these objectives:

- Explain how file manipulation, tampering with call-processing signaling, man-in-the-middle attacks, eavesdropping, and IP Phone and server identity theft can compromise a Cisco CallManager system
- Explain how the authentication and encryption mechanisms in a Cisco CallManager system protect against security threats
- Explain the role of CAPF, external CAs, MIC and LSC, CTLs, and Cisco CTL client
- Explain the PKI enrollment process in a Cisco IP telephony environment
- Explain where keys and certificates are stored in a Cisco IP telephony environment
- Describe the processes of image authentication, device authentication, file authentication, and signaling authentication
- Describe the processes and protocols used for signaling encryption and media encryption

Threats Targeting the IP Telephony System

This topic provides an overview about the threats that are targeting an IP telephony system.

Threats Targeting the IP Telephony System

Cisco.com

- **Loss of privacy—because of sniffed calls**
- **Loss of integrity—because of intercepted and altered calls**
- **Impersonation—because of identity spoofing**
- **Loss of functionality from DoS attacks:**
 - **Against IP telephony components (such as tampering with IP Phone images or IP Phone configuration files)**
 - **Against the underlying infrastructure**

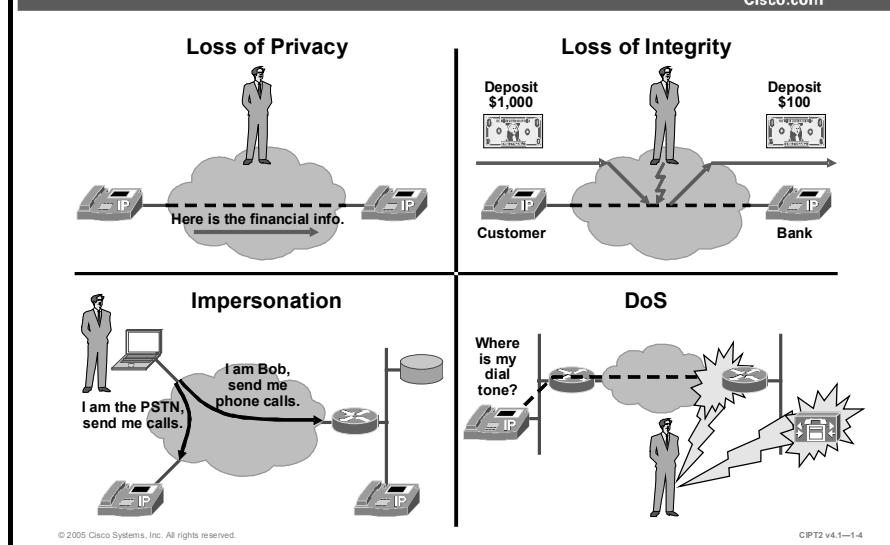
© 2005 Cisco Systems, Inc. All rights reserved. CIPT2 v4.1-1.3

The main threats targeting the IP telephony system are:

- **Loss of privacy:** If calls can be sniffed, conversations can be replayed or eavesdropped. Because of the open nature of IP networks and, especially, the low trust level in the Internet, privacy is a commonly raised concern when comparing IP telephony solutions against traditional telephony solutions.
- **Loss of integrity:** If voice call signaling or media messages can be intercepted, they can be modified. Although this issue might not arise for human conversations very often, do not forget that calls such as telebanking, e-mail or voice-mail access over a telephone, and similar applications using interactive voice response (IVR) may require secure communication.
- **Impersonation:** Identity spoofing is not limited to humans (for instance, the person behind a telephone) but can also extend to devices, such as Cisco CallManager, a voice gateway, or an IP Phone.
- **DoS:** These attacks cause loss of functionality. They can be directed against IP telephony components, such as voice gateways, Cisco CallManager nodes, or IP Phones, or against the underlying infrastructure. An example would be replacing IP Phone configuration files or images stored on a TFTP server with invalid files that cause the IP Phone to malfunction.

Examples of Threats Targeting the IP Telephony System

Cisco.com



This figure illustrates four examples of threats targeting the IP telephony system:

- **Loss of privacy:** The example shows an attacker intercepting the session between two IP telephony users and capturing voice media packets, which enables him to listen to the conversation either in real time or after the call. During the call, sensitive (company financial) information is discussed. Confidentiality is desired by the IP telephony users but is compromised by the attacker.
- **Loss of integrity:** The example shows an attacker again intercepting the session between two IP telephony users and modifying the exchanged packets. In the example, a customer calls into a telebanking application to make a money transfers using an IVR application. The attacker can modify dual-tone multifrequency (DTMF) tones (either in-band by replacing media packets or out-of-band by replacing signaling messages).
- **Impersonation:** The example shows an attacker impersonating the public switched telephone network (PSTN) gateway to users so that all their external calls are directed to the attacker instead of to the real gateway. The attacker also spoofs the identity of one or more users toward the gateway and can intercept the conversation in both directions. This allows the attacker either to capture the traffic without being in the normal path or to modify it.
- **DoS:** The example shows an attacker launching a DoS attack against the Cisco CallManager and a gateway. Because these devices are not able to fulfill their functions, users experience loss of functionality (no dial tone).

How a Cisco IP Telephony Network Protects Against Threats

This topic describes how an IP telephony network can be secured to resist common threats.

How a Cisco IP Telephony Network Protects Against Threats

Cisco.com

- **Secure signaling:**
 - Provides authentication of devices and signaling messages
 - Provides encryption of messages
 - Stops all kind of signaling attacks
- **Secure media transfer:**
 - Provides authentication and encryption of media transfer
 - Stops capturing of IP Phone conversations
- **Authentication of IP Phone images and IP Phone configuration files:**
 - Provides authentication of IP Phone images and configuration files
 - Stops attacks against IP Phone images and configuration files

© 2005 Cisco Systems, Inc. All rights reserved. CIPT2 v4.1-1-6

A Cisco IP telephony network can be protected by using cryptographic services. These services are used to provide the following:

- **Secure signaling:** For authentication of devices and authentication and encryption of signaling messages. This precaution will stop all kind of signaling attacks.
- **Secure media transfer:** For authentication and encryption of media streams, preventing eavesdropping on conversations.
- **Authentication of phone images:** To stop attacks against phone images by ensuring the integrity of the image file.
- **Authentication of phone configuration files:** To stop attacks against phone configuration files, again by ensuring the integrity of the file.

Secure Signaling

Cisco.com

- **Provides authentication and authorization of devices (IP Phone and Cisco CallManager)**
- **Provides authentication and encryption of signaling messages exchanged between the devices**
- **Is a prerequisite for secure media transfer because of media key exchange inside Skinny messages**
- **Uses TLS**
- **Based on Cisco IP telephony PKI solution**

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1—1-6

Secure signaling in Cisco IP telephony provides authentication and authorization of communicating devices (Cisco IP Phones and Cisco CallManager) and authentication of the signaling messages exchanged between them. It can also provide encryption of the signaling messages.

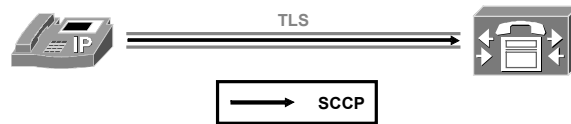
Secure signaling is mandatory (in an authenticated and encrypted fashion) when media transfer is to be secured as well. The reason for this precaution is that the keys used for securing the media channels are exchanged inside signaling messages.

Secure signaling is achieved by using Transport Layer Security (TLS) and is based on the Cisco IP telephony public-key infrastructure (PKI) solution.

Note For all features that are based on the Cisco IP telephony PKI solution, you must globally configure your Cisco CallManager cluster for security. This process involves extra hardware (security tokens) and considerable configuration change.

Secure Signaling Using TLS

Cisco.com



- **Skinny messages sent inside a protected TLS session**
- **Transport-layer protection**
- **Similar to SSL used for web server access**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1.7

The figure illustrates secure signaling encapsulating Skinny Client Control Protocol (SCCP, or Skinny) messages in TLS. TLS provides transport-layer protection and is similar to Secure Socket Layer (SSL), used for secure web browsing.

Secure Media Transfer

Cisco.com

- **Provides confidentiality—sniffed packets cannot be interpreted (conversation cannot be played back)**
- **Provides integrity and authenticity—conversation cannot be altered during transit (modified, injected, or removed packets are detected as such)**
- **Requires encrypted signaling**
- **Uses Secure RTP (SRTP)**
- **Based on Cisco IP telephony PKI solution**

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1—1-6

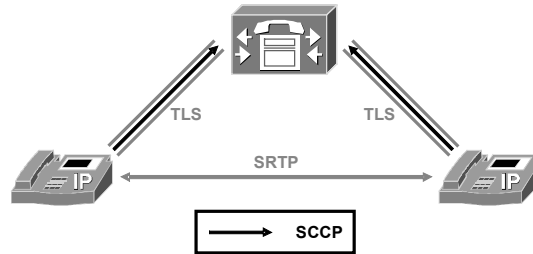
Secure media transfer in Cisco IP telephony provides confidentiality by encrypting the media stream. If media streams are captured, they cannot be interpreted and the conversation cannot be played back. Secure media transfer also provides integrity and authenticity so that the packets cannot be altered while in transit. If an attacker modifies, removes, or adds Real-Time Transport Protocol (RTP) packets, the receiver detects this manipulation because of the missing or incorrect authentication data.

Secure media transfer requires encrypted signaling because media encryption keys are exchanged over signaling channels.

Secure RTP (SRTP) is used for secure media transfer and is based on the Cisco IP telephony PKI solution.

Secure Media Transfer Using SRTP

Cisco.com



- **RTP packets sent encrypted**
- **Standard-based—uses RFC 3711 (Secure RTP)**
- **Application-layer (inside-payload) protection; the protocol headers stay the same**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1.0

The figure illustrates that for secure media transfer, SRTP is used instead of the insecure RTP to exchange voice packets between IP Phones. SRTP is standard-based (RFC 3711, *The Secure Real-Time Transport Protocol*) and is an application-layer encryption that performs inside-payload encryption where the protocol headers do not change. Because the headers in RTP and SRTP are the same, an attacker who sniffs the conversation does not know whether the RTP stream has been encrypted when examining the packet header only. Only when further analyzing the sniffed packets and trying to play them back can the attacker recognize that the audio has been encrypted.

Authentication of IP Phone Images

Cisco.com

- **Totally independent from the Cisco IP telephony PKI solution**
- **Supported on all IP Phones**
- **Images are signed by Cisco development (using a private key)**
- **Cisco CallManager Release 3.3(3) and later IP Phone images contain the corresponding public key**
- **Allows new images to be verified without any additional configuration**
- **Also checks image device type (prevents loading the incorrect image to a certain IP Phone model)**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1—1-10

To ensure the integrity of Cisco IP Phone images that are loaded from a TFTP server, authenticated images are used. IP Phone image authentication is supported on all Cisco IP Phone models. With image authentication, the images are signed by Cisco manufacturing (using a private key) and the signature is appended to the actual firmware.

IP Phone image authentication was introduced with Cisco CallManager Release 3.3(3). In this and later versions, phone images include the public key that corresponds to the private key used by Cisco manufacturing to sign phone images. In addition, the firmware accepts new images only if their signature is authentic.

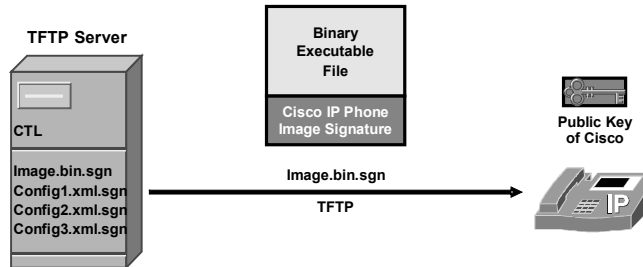
IP Phone image authentication does not need any additional configuration and it is totally independent of the Cisco IP telephony PKI that is used for other features.

The phone also checks the image device type so that incorrect images (those for other phone models) are not loaded.

Note If you need to downgrade to an IP Phone image that does not yet support IP Phone image authentication (earlier than Cisco CallManager Release 3.3(3)) a special “breakout” image can be obtained from the Cisco Technical Assistance Center (TAC). Simply trying to load an older image does not work because the current image will accept only signed images.

Phone Image Verification

Cisco.com



- The administrator installs a new Cisco-signed IP Phone image on the TFTP server.
- The IP Phone verifies the signature using the corresponding public key already embedded in the existing IP Phone image.

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-1-11

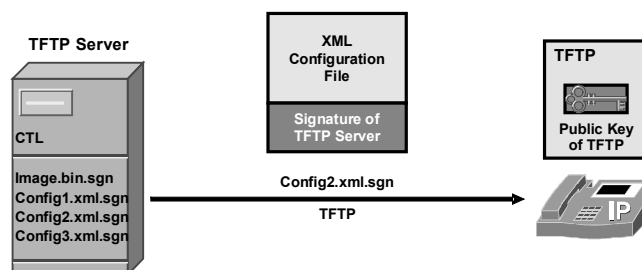
The figure shows an IP Phone that has an image supporting the IP Phone image authentication feature.

The administrator installs a new IP Phone image on the TFTP server that was signed by Cisco development.

An IP Phone loading that image verifies the signature of the image using the public key that is embedded in the existing image.

Authentication of IP Phone Configuration Files

Cisco.com



- Configuration files signed by the TFTP server
- Phone verifies signature before applying configuration
- Uses Cisco IP telephony PKI solution
- Stops tampering with configuration files on the TFTP server or in transit

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-12

In addition to IP Phone images, IP Phone configuration files can be signed as well. Signed IP Phone configuration files are implemented differently from signed images.

The configuration files are signed by the Cisco TFTP server (with its private key).

An IP Phone loading a new configuration verifies the configuration file before applying it. The IP Phone needs the public key of the TFTP server to do so. Except for the Cisco development public key, the public key of the TFTP server is different for every installation and therefore cannot be embedded in the firmware of the IP Phone. Therefore, verification must use the Cisco IP telephony PKI. Authenticated IP Phone configuration files prevent tampering with the files on the TFTP server or in transit.

Note Because authenticated IP Phone configuration files depend on the existence of a Cisco IP telephony PKI, the deployment of this feature is far more complex than signed IP Phone images. On the other hand, when you enable your cluster for security, authentication of phone configuration files is automatic for all IP Phones that are configured for secure operation.

PKI Topologies in Cisco IP Telephony

This topic describes all possible PKI topologies in Cisco IP telephony.

PKI Topologies in Cisco IP Telephony

Cisco.com

Cisco IP telephony PKI is not a single PKI system:

- **Cisco CallManager servers certificates are self-signed.**
- **MICs on Cisco IP Phone 7970 models are signed by Cisco manufacturing CA.**
- **LSCs on Cisco IP Phone 7940, 7960, or 7970 models are signed by Cisco CallManager CAPF or by an external CA.**

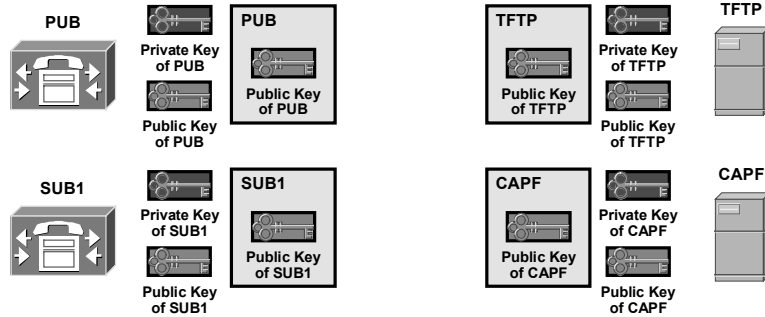
© 2005 Cisco Systems, Inc. All rights reserved. CPT2 v4.1-1-13

Unlike classic enterprise PKI deployments, the PKI topology in Cisco IP telephony is not a single PKI system. Instead of having a single Certificate Authority (CA) that issues all certificates, there are several instances issuing certificates:

- **Self-signed certificates:** Cisco CallManager and other servers issue their certificates on their own.
- **Certificates signed by the Cisco manufacturing CA:** Cisco IP Phone 7970 models have manufacturing installed certificates (MICs).
- **Certificates signed by Cisco CallManager Certificate Authority Proxy Function (CAPF) or by an external CA:** One of these two options is used to issue locally significant certificates (LSCs) to Cisco IP Phone 7940, 7960, or 7970 models.

Cisco IP Telephony Self-Signed Certificate PKI Topologies

Cisco.com



- Each Cisco CallManager has a self-signed certificate.
- Cisco CallManager TFTP servers also have self-signed certificates.
- If the CAPF is used (needed for LSC), it also has a self-signed certificate.
- All of them act as their own PKI root.

© 2005 Cisco Systems, Inc. All rights reserved.

CIP72 v4.1-1-14

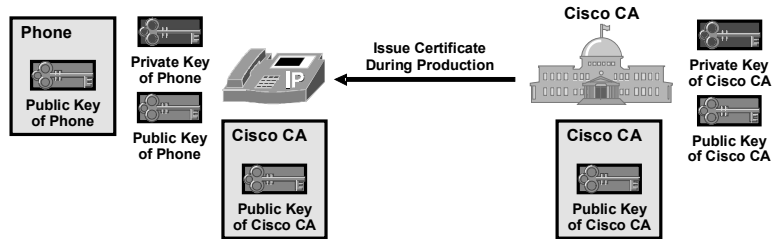
The figure illustrates several IP telephony services with self-signed certificates:

- Each Cisco CallManager has a self-signed certificate.
- Cisco CallManager TFTP servers have self-signed certificates.
- If the CAPF is used (needed for LSC), it will have a self-signed certificate.

All of them act as their own PKI root.

Cisco IP Telephony MIC PKI Topology

Cisco.com



- Cisco IP Phone 7970 models have a public and a private key pair, a MIC for the phone, and a Cisco manufacturing CA certificate installed.
- The certificate of the IP Phone is signed by the Cisco manufacturing CA.
- Cisco manufacturing CA is the PKI root for all MICs.

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-1-15

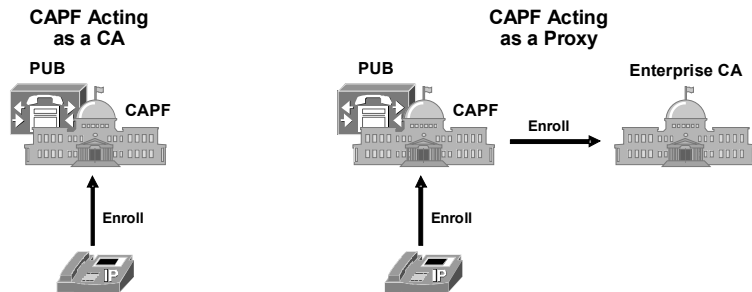
This figure shows the PKI used for MICs:

- Cisco IP Phone 7970 models have a public and private key pair, a MIC for their own public key, and a Cisco manufacturing CA certificate, all installed during production.
- The IP Phone certificate (MIC) is signed by the Cisco manufacturing CA.

The Cisco manufacturing CA is the PKI root for all MICs.

Cisco IP Telephony LSC PKI Topology

Cisco.com



- The Cisco IP Phone 7940 and 7960 do not have a MIC installed.
- They use LSCs issued either by the CAPF or by an external CA.
- The CAPF or external CA is the root for all LSCs.

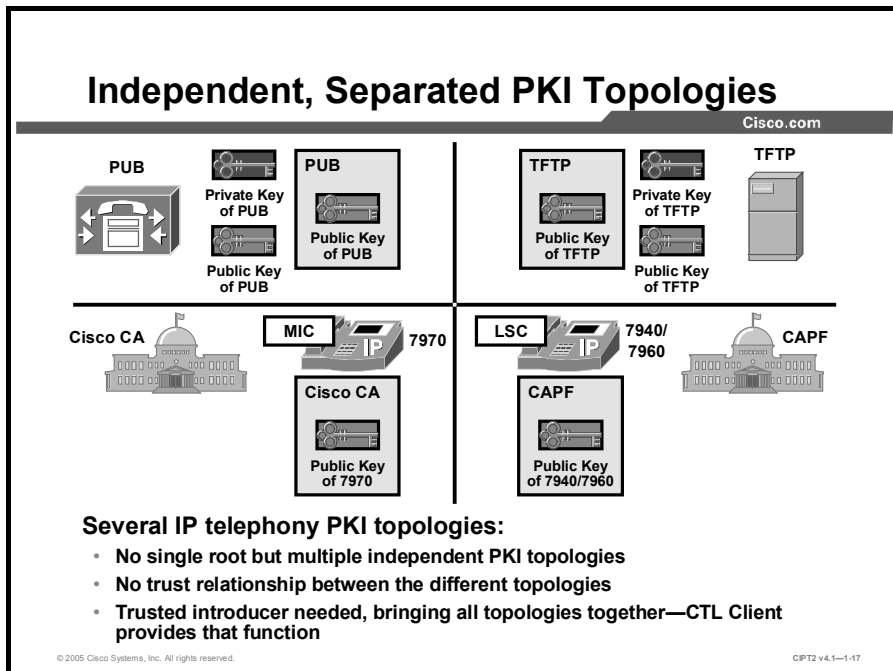
© 2005 Cisco Systems, Inc. All rights reserved.

CIP72 v4.1-1-16

Cisco IP Phone 7940 and 7960 models do not have a MIC installed. They have to request an LSC from the CAPF, which is signed in one of two possible ways:

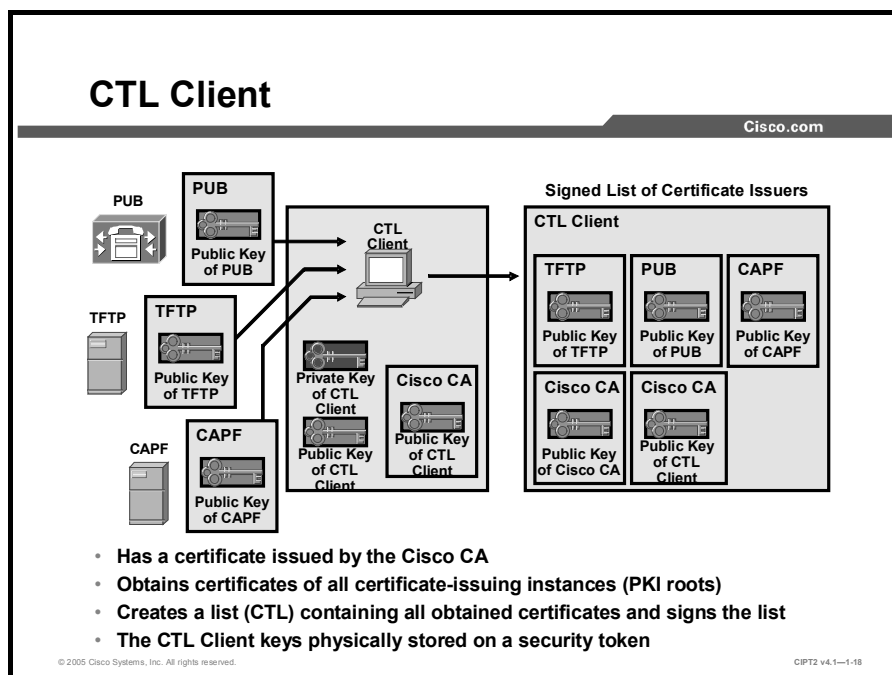
- The CAPF can issue the certificate on its own (acting as a CA).
- The CAPF can issue proxy enrollment requests to an external CA, and the external CA issues the certificate.

The CAPF or an external CA is the root for all LSCs.



As illustrated in the figure, several PKI topologies coexist in an IP telephony network.

There is no single root; instead there are multiple independent PKI topologies. So far, there is no trust relationship among these different PKIs. A trusted introducer is needed, bringing all the PKI topologies together. The Certificate Trust List (CTL) client provides that function.



The Cisco CTL client itself has a certificate issued by the Cisco manufacturing CA. The Cisco CTL client obtains the certificates of all entities that issue certificates (self-signed certificates only or certificates for other devices). Then the Cisco CTL client signs the list of these certificates, the CTL, using its private key. The public and private keys of the Cisco CTL client are stored on a smart token called a security token.

Now there is a single, trusted introducer in the system again: The Cisco CTL client “introduces” trusted devices—not by signing their certificates but by signing a list of trusted certificates signed by several PKI roots.

Note The CTL can be compared to the root certificate store of Microsoft Internet Explorer. Both are a list of trusted certificate-issuing entities.

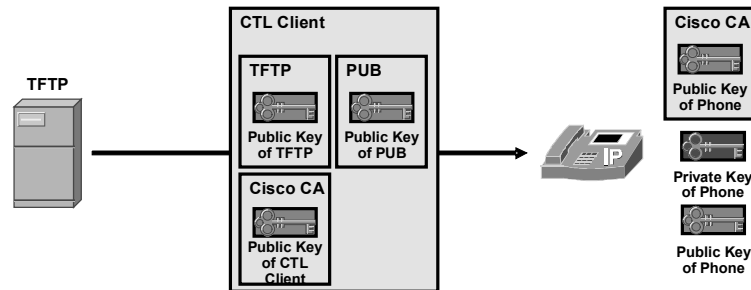
The CTL usually includes these certificates:

- **Cisco CallManager certificates:** Each Cisco CallManager has a self-signed certificate. It allows the Cisco CallManager to authenticate to a device (IP Phone) during device registration.
- **TFTP server certificate:** The TFTP server that provides the IP Phone with files, such as the IP Phone image or the IP Phone configuration file, is trusted by the IP Phone only if the TFTP server is listed in the CTL of the IP Phone.
- **CAPF certificate:** When you are using LSC, the CAPF issues certificates to the IP Phones. The certificate of the CAPF allows the CAPF to authenticate to an IP Phone during the enrollment.

- **Cisco certificate:** MICs and the certificate of the security tokens (storing the keys used by the Cisco CTL client) are issued by Cisco manufacturing CA. To allow the phone to verify certificates issued by this Cisco CA, the phone needs the certificate of the Cisco manufacturing CA.
- **Cisco CTL client certificate:** The Cisco CTL client signs the CTL using one of the security tokens. The certificates of the Cisco CTL client (one per security token) have to be known to the IP Phone to allow verification of the signature of the CTL.

CTL Download

Cisco.com



- The CTL is sent to the IP Phones over TFTP at boot.
- The CTL contains all entities that issue certificates.
- The IP Phone now knows which issuers are trusted.

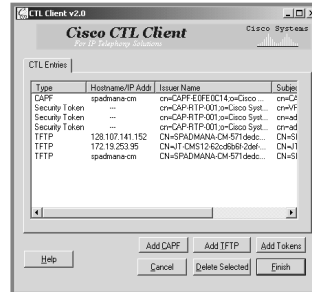
© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-19

When an IP Phone boots, the CTL is downloaded from the TFTP server. It contains all certificates of the entities that issued certificates. By having this list, the IP Phone knows which PKI roots to trust and can trust all certificates that have been issued by any PKI root contained in the CTL.

CTL Client Application

- CTL client software is used to create or update the CTL.
- The CTL is signed by CTL client keys that are one of the administrator security tokens, which are all signed by the Cisco CA.
- The CTL file must be updated only when new IP telephony servers or new security tokens are added to the system.
- CTL also acts as an authorization list specifying which certificates belong to which IP telephony function (such as Cisco CallManager and TFTP).



Security Token

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-20

The Cisco CTL client software, available as a plug-in application on Cisco CallManager Administration, is used to create or update the CTL. When the list is accurate, the Cisco CTL client will ensure that the CTL is signed by the keys of the Cisco CTL client. These keys are stored on an external Universal Serial Bus (USB) device—the security token. When the CTL needs to be signed, the Cisco CTL client passes the CTL to the security token, and the security token signs it and then returns the signed CTL to the Cisco CTL client application. The Cisco CTL client itself does not have access to the private key stored on the security token. Therefore it is not the CTL client application that actually signs the CTL; the CTL client only interacts with the security token requesting the security token to create the signature.

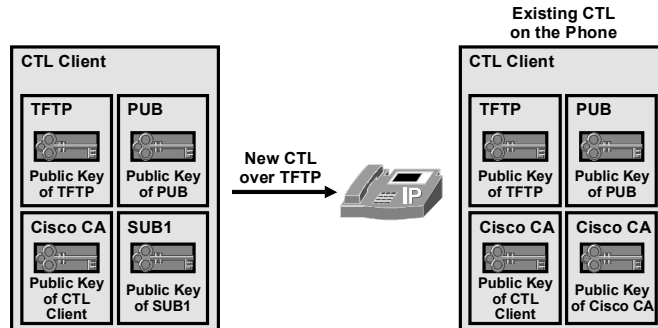
The public key of a security token is signed by the Cisco manufacturing CA during production, and the appropriate certificate is also stored on the security token itself.

The CTL file needs to be updated after configuration changes, such as changing or adding IP telephony servers or security tokens to the system.

The CTL also acts as an authorization list because it also specifies which certificates belong to which IP telephony function. A TFTP server, for instance, is not allowed to sign a CTL, only IP Phone configuration files. The CAPF, as another example, is allowed to sign the LSCs of other IP Phones only but not the CTL or any TFTP files.

CTL Verification on the IP Phone

Cisco.com



Every time the IP Phone receives a new CTL, it is verified:

- CTL must be signed by one of the authorized security tokens (public key for signature verification is taken from the existing CTL on the IP Phone).
- Security token certificate is verified using the public key of the Cisco manufacturing CA (also taken from the existing CTL on the IP Phone).

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-21

Every time that an IP Phone receives a new CTL, the new CTL is verified. It is accepted by the IP Phone only if it was signed by the Cisco CTL client using one of the administrator tokens. The phone can verify the signature using the public key (the certificate) of the Cisco CTL client (in fact, the certificate of the appropriate administrator token), which must be included in the currently installed ("old") CTL.

This certificate of the administrator token is signed by the Cisco manufacturing CA. This signature is also validated by using the certificate of the Cisco manufacturing CA, which also must be included in the currently installed CTL.

This concept works well as long as the phone already has a CTL.

Initial Deployment Issue

Cisco.com

How does a IP Phone know which security token is trusted without already having the CTL?

- **Problem only occurs at initial deployment when the IP Phone does not yet have a local CTL.**
- **Any security token could pretend to be a valid token in this IP Telephony system.**
- **The problem can be solved by downloading the initial CTL over a trusted network.**
- **If the CTL is erased in the IP Phone, the same problem occurs.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-22

For the first download of a CTL to an IP phone, there is an issue: How does an IP Phone know which administrator tokens are trusted without already having a CTL?

This problem occurs only at initial deployment, when the phone does not yet have a local CTL. In this case, any administrator token could pretend to be a valid token for the IP telephony system in question. An attacker could either replace the CTL file on the TFTP server with a falsified file or change the CTL file in the path between the IP Phone and the TFTP server.

The problem can be solved by downloading the initial CTL over a trusted network to ensure that no falsified initial CTL is loaded to the phone. When the phone has a valid CTL, it will trust new CTLs only if they are signed using a security token that is already known to the IP Phone.

If the CTL file in the IP Phone is erased, the same problem occurs. Again, you must ensure that the next CTL download is done over a trusted network path because the IP Phone will blindly accept any CTL.

After the IP Phone is deployed, it is usually difficult to trust the network path between the phone and Cisco CallManager. Therefore, a user should not be able to erase the initially installed CTL. There are two ways to remove a CTL from an IP Phone: a factory reset or the IP Phone Settings menu. A factory reset is not simple, but using the Settings menu is rather easy. To prevent users from using the Settings menu to remove the CTL, you should disable settings access at the phone.

Note When using authentication strings as the authentication method during CAPF phone certificate operations, you have to enable settings access during the enrollment. After successful enrollment, you should then disable settings access again.

PKI Enrollment in Cisco IP Telephony

This topic describes how IP Phones enroll with the CAPF or an external CA.

PKI Enrollment in Cisco IP Telephony

Cisco.com

- **With MIC, enrollment is done by Cisco manufacturing CA:**
 - The IP Phone has the private and public RSA keys, a certificate issued by the Cisco manufacturing CA, and the certificate of the Cisco manufacturing CA installed.
 - No other IP Phone PKI provisioning tasks are required.
- **With LSC, enrollment has to be done by the customer:**
 - The MIC (if available) remains on the IP Phone, even when LSC is used.
- **MICs are supported on the Cisco IP Phone 7970 only, while LSCs are supported on Cisco IP Phone 7940, 7960, and 7970 models:**
 - If both a MIC and an LSC exist in a IP Phone, the LSC has priority (only possible with 7970).

© 2005 Cisco Systems, Inc. All rights reserved. CIP12 v4.1-1-23

To obtain a signed certificate, an IP Phone needs to enroll with the entity that will issue (sign) the certificate. During enrollment, the phone will get the certificate of the issuer and then send its data to the issuer asking for a (signed) certificate. IP Phone enrollment depends on the type of certificate.

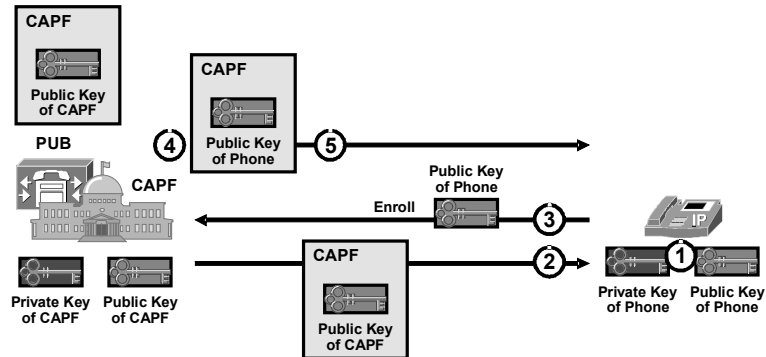
With MICs, enrollment was already done by Cisco manufacturing during production. When the IP Phone is shipped to the customer, it already has its public and private keys, a certificate issued by the Cisco manufacturing CA, and the certificate of the Cisco manufacturing CA installed. No other PKI provisioning tasks are required.

With LSCs, enrollment has to be done by the customer. MICs always remain on the phone, even if an LSC is added.

MICs are supported on Cisco IP Phone 7970 models only, while LSCs are supported on Cisco IP Phone 7940, 7960, and 7970 models. If the IP Phone has both a MIC and an LSC, the LSC has priority.

CAPF Acting as a CA

Cisco.com



1. The phone generates its public and private key pairs.
2. The phone downloads certificate of CAPF and establishes a TLS session with the CAPF with it.
3. The phone enrolls with the CAPF, sending its identity, its public key, and an optional authentication string.
4. The CAPF issues a certificate for the phone signed with its private key.
5. The CAPF sends the signed certificate to the phone.

© 2005 Cisco Systems, Inc. All rights reserved.

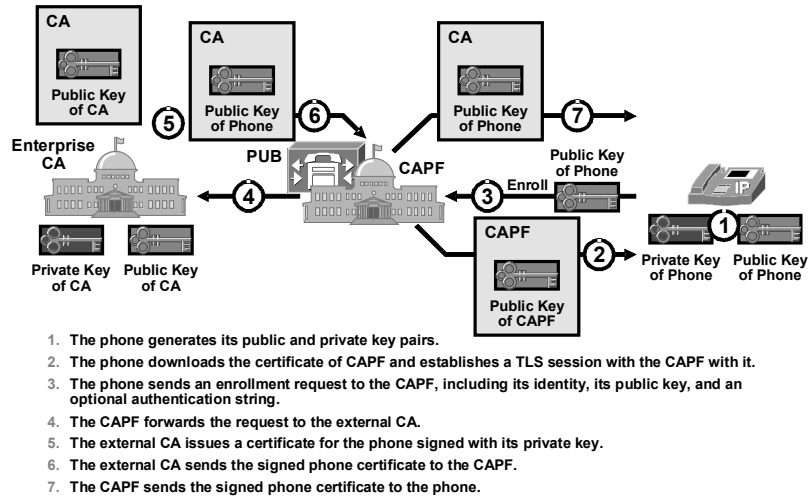
CPT2 v4.1-1-24

To obtain an LSC from the CAPF acting as a CA, an IP Phone has to enroll with the CAPF, as shown in the figure:

- Step 1** The IP Phone generates its public and private key pairs.
- Step 2** The IP Phone downloads the certificate of the CAPF and uses it to establish a TLS session with the CAPF.
- Step 3** The IP Phone enrolls with the CAPF, sending its identity, its public key, and an optional authentication string.
- Step 4** The CAPF issues a certificate for the IP Phone signed with its private key.
- Step 5** The CAPF sends the signed certificate to the IP Phone.

CAPF Acting as a Proxy to an External CA

Cisco.com



If an IP Phone should obtain an LSC from an external CA using the CAPF as a proxy, the IP Phone has to enroll with the external CA, as shown in the figure:

- Step 1** The IP Phone generates its public and private key pairs.
- Step 2** The IP Phone downloads the certificate of the CAPF and uses it to establish a TLS session with the CAPF.
- Step 3** The IP Phone sends an enrollment request to the CAPF including its identity, its public key, and an optional authentication string.
- Step 4** The CAPF forwards the request to the external CA.
- Step 5** The external CA issues a certificate for the IP Phone signed with private key of the CA.
- Step 6** The external CA sends the signed IP Phone certificate to the CAPF.
- Step 7** The CAPF sends the signed IP Phone certificate to the phone.

Keys and Certificate Storage in Cisco IP Telephony

This topic describes where various devices store their keys and certificates.

Key and Certificate Storage in Cisco IP Telephony

Cisco.com

- **IP Phones: Keys and certificate are stored in IP Phone nonvolatile memory**
- **IP telephony servers (Cisco CallManager, CAPF, TFTP): Keys and certificate are stored in the Microsoft certificate store of the servers**
- **CTL client (trusted introducer): Keys and certificate are stored on security tokens**

© 2005 Cisco Systems, Inc. All rights reserved.CPT2 v4.1—1-26

Key storage is a major part of key management, because an improperly stored key may enable an attacker to compromise parts of the PKI or the whole PKI.

The IP Phone stores its public and private RSA keys and its certificate in its nonvolatile memory. This information is preserved across phone reboots and resets. The keys cannot be extracted from the IP Phone unless the phone is taken apart and the nonvolatile memory is then physically analyzed.

The IP telephony servers (Cisco CallManager, CAPF, and TFTP server) store certificates on the local hard disk, in a special area called the Microsoft certificate store. The private key of the server is stored in the private-key storage. The private-key storage is protected by the periodically changed master key. The master key itself is encrypted with Triple Data Encryption Standard (3DES) using a key derived from the password of the user.

Microsoft Windows XP stores a certificate locally on the computer or device that requested it or, in the case of a user, on the computer or device that the user used to request it. The storage location is called the certificate store.

The Cisco CTL client stores its public and private RSA keys on the security tokens supplied by Cisco. The keys are embedded on the token during production, and the token is designed never to leak these keys from its memory.

Authentication and Integrity

This topic describes how to secure calls to provide authentication and integrity for signaling messages and media transfers.

Authentication and Integrity

Cisco.com

Cisco CallManager allows authentication of calls:

- **Device authentication for the IP Phone and the server is provided using device certificates and digital signatures.**
- **Authentication and integrity of signaling messages are provided using TLS SHA-1 HMAC.**

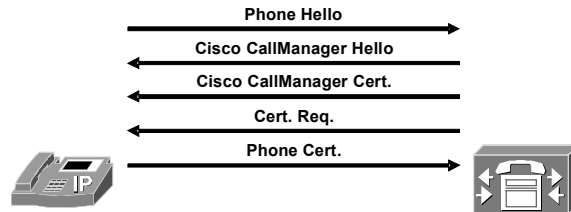
© 2005 Cisco Systems, Inc. All rights reserved.CIP12 v4.1-1-27

Cisco CallManager allows authentication of calls. When you are configuring devices for authenticated calls, two services are provided:

- **Device authentication for the IP Phone and the server:** Achieved by using device certificates and digital signatures
- **Authentication and integrity of signaling messages:** Achieved by using TLS Secure Hash Algorithm 1 (SHA-1) Hash-Based Message Authentication Code (HMAC) (with symmetric keys)

Certificate Exchange in TLS

Cisco.com



- **At the beginning of a TLS session, the server and the IP Phone exchange certificates in a TLS handshake.**
- **The certificates are then validated.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-28

At the beginning of a TLS session, the Cisco CallManager server and the IP Phone exchange certificates using the messages shown in the figure:

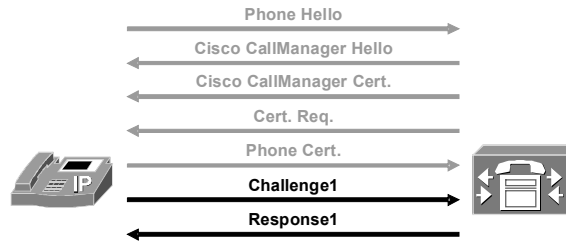
- Step 1** The IP Phone and the Cisco CallManager server negotiate the cryptographic algorithms in the IP Phone Hello and Cisco CallManager Hello messages.
- Step 2** The server sends its (self-signed) certificate to the IP Phone.
- Step 3** The server requests a certificate from the IP Phone.
- Step 4** The IP Phone sends its certificate to the server.

At this point, both the IP Phone and the server validate the certificates they just received over the network:

- The IP Phone simply looks up the certificate of the server in its local certificate store. The received certificate must be found locally because it must have been sent in the CTL. If it is not included in the CTL, the session is dropped. If it is found, the public key of the server is extracted from the certificate.
- The server looks up the IP Phone in the local device database to see if this IP Phone is known and authorized to connect via TLS. Then the certificate of the IP Phone is validated using the locally available CAPF public key (from the CAPF certificate), and if valid, the public key of the IP Phone is extracted from the IP Phone certificate.

Server to Phone Authentication

Cisco.com



- The IP Phone sends a random challenge to the server and requests that the server sign it.
- The server signs the random challenge with its RSA private key and returns it to the IP Phone.
- The IP Phone verifies the signature using the RSA public key of the server (available locally in the CTL).

© 2005 Cisco Systems, Inc. All rights reserved.

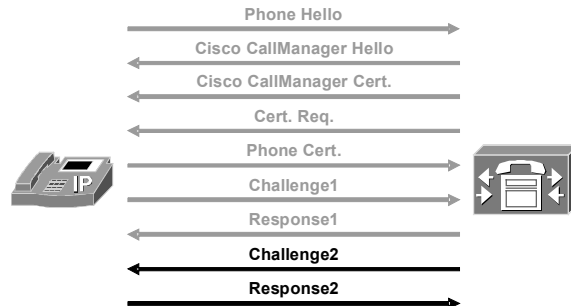
CIPT2 v4.1-1-29

The next stage of the TLS handshake is authentication of the server by the IP Phone. A simplified version of the authentication steps is shown in the figure.

- Step 1** The IP Phone generates a random challenge string and sends it to the server, requesting that the server sign it with the private RSA key of the server.
- Step 2** The server signs the message with its private RSA key and returns the result (response) to the IP Phone.
- Step 3** The IP Phone verifies the signature using the public key of the server.

Phone to Server Authentication

Cisco.com



- The server sends a random challenge to the IP Phone and requests that the phone sign it.
- The IP Phone signs the random challenge with its RSA private key and returns it to the server.
- The server verifies the signature using the RSA public key of the IP Phone just received over the network (in the certificate).

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-1-30

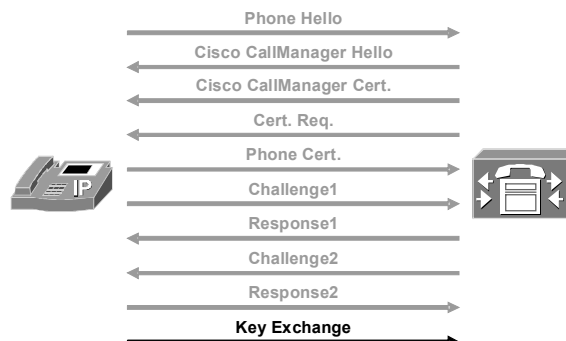
After the server has authenticated to the IP Phone, the IP Phone needs to authenticate to the server. A simplified version of the authentication steps is shown in the figure.

- Step 1** The server generates a random challenge string and sends it to the IP Phone, requesting that the IP Phone sign it with the private RSA key of the IP Phone.
- Step 2** The IP Phone signs the message with its private RSA key and returns the result (response) to the server.
- Step 3** The server verifies the signature with the public key of the IP Phone.

Note In the certificate of the IP Phone, the public key of the IP Phone is tied to the identity of the IP Phone. Because Cisco CallManager identifies an IP Phone by MAC address and not by IP address or name, the MAC address of the phone is used as the identifier in the certificate of the IP Phone.

TLS SHA-1 Session Key Exchange

Cisco.com



- The IP Phone generates a session key for SHA-1 hashing, encrypts it using the public RSA key of the server, and sends it to the server.
- The server decrypts the message, and now the IP Phone and the server can start signing signaling messages (signaling channel integrity).

© 2005 Cisco Systems, Inc. All rights reserved.

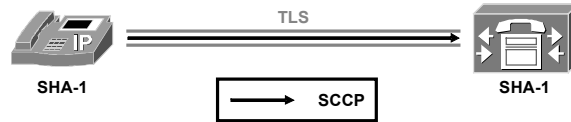
CIPT2 v4.1—1-31

After the bidirectional authentication, a SHA-1 session key is exchanged using these steps:

- Step 1** The IP Phone generates a session key for SHA-1 hashing.
- Step 2** The IP Phone encrypts it using the public RSA key of the server and sends it to the server.
- Step 3** The server decrypts the message and thus also knows which key to use for SHA-1 hashing of the TLS packets.

Authenticated Signaling Using TLS

Cisco.com



Each signaling (SCCP) message is carried over authenticated (signed) TLS packets.

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-1-32

The IP Phone and the server can now exchange signaling messages over authenticated TLS packets, ensuring the integrity and authenticity of each signaling message exchanged between the two.

Encryption

This topic describes how to secure calls to provide confidentiality for signaling messages and media transfers.

Encryption

Cisco.com

Cisco CallManager also allows encryption of calls:

- **For signaling messages using TLS encryption with AES 128-bit encryption**
- **For media transfer using SRTP AES 128-bit encryption**
- **To ensure the authenticity of encrypted packets, encryption is supported only if combined with authentication (applies to both TLS and SRTP)**

© 2005 Cisco Systems, Inc. All rights reserved.C IPT2 v4.1-1-33

In addition to authentication and integrity, Cisco CallManager also provides confidentiality of calls by using encryption. When configuring devices for encrypted calls, signaling messages and media streams are encrypted as follows:

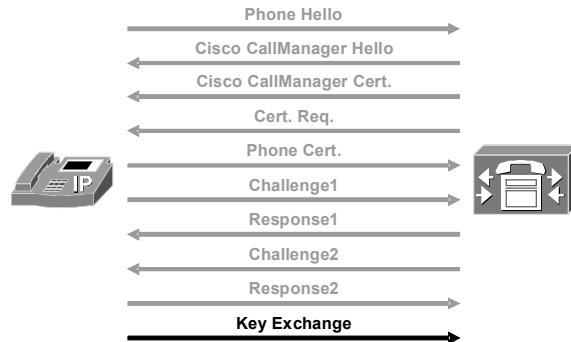
- Signaling messages are encrypted using TLS encryption with Advanced Encryption Standard (AES) 128-bit encryption.
- Media streams are encrypted using SRTP with AES 128-bit encryption.

To ensure the authenticity of encrypted packets, in Cisco CallManager, encryption is supported only if combined with authentication. This limitation applies to both protocols, TLS and SRTP.

Note It is a general rule in cryptography to always complement packet encryption with packet authentication. If encryption is used without authentication, the receiver of an encrypted packet has no guarantee that the packet comes from the expected source. Assuming that an attacker does not know the key to be used for the encryption, the attacker might not be able to send valid data but could send arbitrary data to keep the receiver busy with decrypting the packets. Because this decryption performed at the receiver can cause considerable processing overhead, an attacker could launch a DoS attack just by flooding a system with packets that will be decrypted by the receiver. In some situations the attacker could even inject incorrect data into the application. This is possible when the sent data does not have any special format but when any bit patterns are considered to be valid data and are accepted by the receiver. An example would be encrypted digitized voice samples. An example where the receiver can detect invalid data is the transfer of an encrypted Microsoft Word file. In this case, after decrypting the received arbitrary data (or a valid file that has been encrypted with an incorrect key) the receiver would not recognize the file as a valid Word document.

TLS AES Encryption

Cisco.com



- If configured for encryption, the IP Phone will not only create a SHA-1 key but also an AES key after the two-way authentication.
- The IP Phone encrypts both keys using the public RSA key of the server and sends them to the server.
- The server decrypts the message, and now the IP Phone and the server can start signing and encrypting signaling messages.

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-1-34

If an IP Phone is configured for encryption, it will not only create a SHA-1 key but also an AES key after the two-way authentication in TLS. The IP Phone encrypts both keys using the public RSA key of the server and then sends them to the server. The server decrypts the message so that the IP Phone and the server can exchange signaling messages over authenticated and encrypted TLS packets.

In Cisco IP telephony, TLS encryption requires TLS authentication so that the authenticity of the encrypted TLS packets is always guaranteed.

SRTP Media Encryption

Cisco.com

- **SRTP session keys (for media authentication and media encryption) are generated by Cisco CallManager.**
- **Keys are sent from Cisco CallManager to the IP Phones inside signaling messages.**
- **To ensure protection of media key distribution, encrypted signaling is mandatory.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-35

Media streams are encrypted by using SRTP. Cisco CallManager generates the SRTP session keys (for media authentication and media encryption) and sends them to the IP Phones inside signaling messages. If the signaling messages are not protected, an attacker could easily learn the SRTP keys just by sniffing the signaling messages. To ensure protection of the key distribution, encrypted signaling is mandatory in Cisco CallManager when media streams are encrypted.

As stated before, in Cisco CallManager, encrypted packets always have to be signed to ensure the authenticity of the source and the content of the packet.

To summarize, for security reasons, these rules apply to Cisco CallManager authentication and encryption:

- Signaling encryption requires signaling authentication.
- Media encryption requires media authentication and signaling encryption (hence also signaling authentication).

In addition, for no security-related reasons, Cisco CallManager security is implemented as follows:

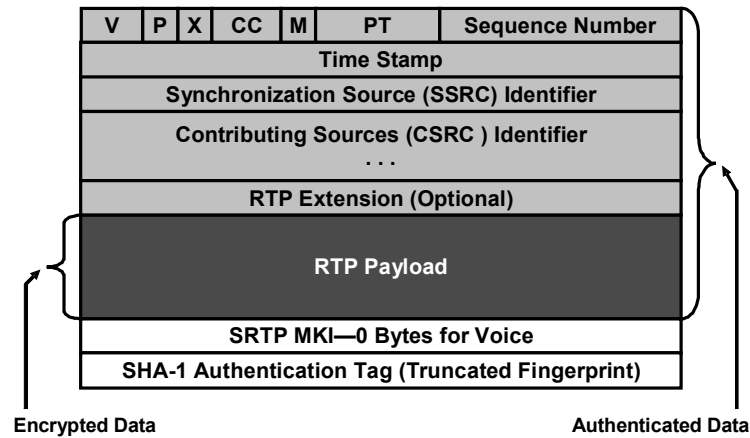
- Media authentication requires media encryption.
- Signaling encryption requires media encryption.

As a consequence of these rules, you can configure one of the following secure operation modes in Cisco CallManager:

- **Authenticated:** This mode provides authenticated signaling only (TLS SHA-1).
- **Encrypted:** This mode provides authenticated and encrypted signaling (TLS SHA-1 and TLS AES) and authenticated and encrypted media transfer (SRTP SHA-1 and SRTP AES).

SRTP Packet Format

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1—1-36

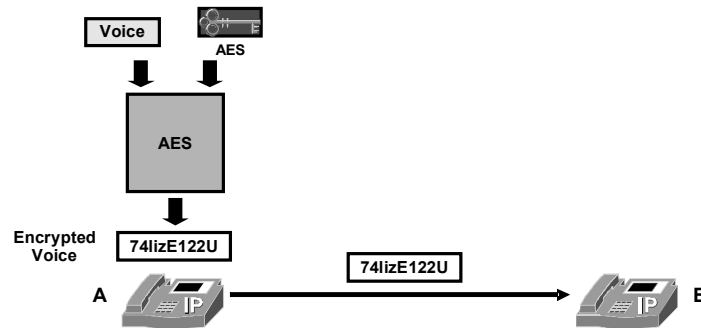
The SRTP packet header does not differ from an RTP packet header. The RTP payload differs only in the sense that it is not cleartext voice but encrypted voice. In addition to the encrypted payload, a 32-bit SHA-1 authentication tag is added to the packet. The authentication tag holds the first 32 bits of the 160-bit SHA-1 hash digest computed from the RTP header and the encrypted voice payload (“truncated fingerprint”).

As you can see from the figure, the RTP packet header and the RTP payload (encrypted voice) are authenticated. Therefore, RTP encryption is performed before RTP authentication.

Note The SRTP Master Key Index (MKI) shown in the figure is optional and not used in secure IP telephony.

SRTP Encryption

Cisco.com



- The sender encrypts the RTP payload using the AES algorithm and the AES key received from the Cisco CallManager.
- The receiver uses the same AES key (also received from Cisco CallManager) to decrypt the RTP payload.

© 2005 Cisco Systems, Inc. All rights reserved.

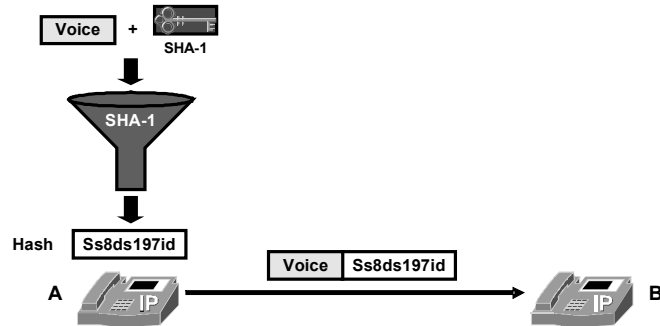
CIPT2 v4.1-1-38

When phones exchange voice over SRTP, the SRTP encryption works as shown in the figure:

- The sender encrypts the RTP payload using the AES algorithm and the AES key that it received from the Cisco CallManager when the call was set up.
- The receiver uses the same AES key (also received from the Cisco CallManager) to decrypt the RTP payload.

SRTP Authentication

Cisco.com



- The sender hashes the RTP payload together with the SHA-1 key received from Cisco CallManager.
- The hash digest is added to the RTP packet, and the combined packet is sent to the receiver.
- The receiver uses the same SHA-1 key (also received from the Cisco CallManager) to verify the hash digest.

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-37

When IP Phones exchange voice over SRTP, the SRTP authentication works as shown in the figure:

- The sender hashes the RTP header and the RTP payload together with the SHA-1 key that it received from Cisco CallManager when the call was set up.
- The first 32 bits of the hash digest are added to the RTP packet, and the packet is then sent to the receiver.
- The receiver uses the same SHA-1 key (also received from the Cisco CallManager) to verify the hash digest.

Secure Call Flow Summary

Cisco.com

1. IP Phones and Cisco CallManager exchange certificates
2. IP Phones and Cisco CallManager authenticate each other
3. IP Phones create TLS session keys for SHA-1 authentication and AES encryption
4. IP Phones encrypt session keys with Cisco CallManager public key and send the keys to Cisco CallManager
5. Cisco CallManager shares TLS keys with each IP Phone and starts secure exchange of signaling messages
6. Cisco CallManager creates session keys for SRTP SHA-1 authentication and SRTP AES encryption
7. Cisco CallManager distributes the session keys to both IP Phones
8. IP Phones share SRTP keys and start secure media exchange

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-39

When a call is placed between two IP Phones when encryption is enabled, the following sequence occurs:

- Step 1** The IP Phones and Cisco CallManager exchange certificates.
- Step 2** The IP Phones and Cisco CallManager authenticate each other by requesting some random data to be signed. When this process is finished, Cisco CallManager and the IP Phones know that the other devices are authentic.
- Step 3** Each IP Phone creates TLS session keys. One key will be used for TLS SHA-1 authentication; the other key will be used for TLS AES encryption.
- Step 4** Each IP Phone encrypts the generated keys with the public key of the Cisco CallManager and sends the encrypted keys to Cisco CallManager.
- Step 5** Now each IP Phone shares its session keys with Cisco CallManager. At this stage, each phone can exchange signaling messages with Cisco CallManager over an authenticated and encrypted TLS session.
- Step 6** When the call is established between the two IP Phones, Cisco CallManager creates SRTP session keys. One key is used for SRTP SHA-1 authentication; the other key is used for SRTP AES encryption.
- Step 7** Cisco CallManager sends the generated SRTP session keys to both IP Phones over the secured TLS session.
- Step 8** The IP Phones now share the session keys for authenticating and encrypting their RTP packets. At this stage, the two IP Phones can start secure media exchange.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Threats targeting Cisco IP telephony include eavesdropping, IP Phone image and configuration file tampering, and DoS attacks.**
- **Cisco IP telephony uses authentication and encryption techniques to protect against such threats.**
- **There is no single PKI topology in Cisco IP telephony.**
- **CTL client acts as a trusted introducer for the different PKI systems.**
- **IP Phones can use preinstalled certificates (MICs) or use LSCs issued by CAPF or a company CA.**

© 2005 Cisco Systems, Inc. All rights reserved. CPT2 v4.1—140

Summary (Cont.)

Cisco.com

- **Cisco CallManager stores self-signed certificates in the operating system private key storage, the keys used by the CTL client are stored on security tokens, and IP Phones store keys in protected nonvolatile memory.**
- **Cisco CallManager supports device authentication, authenticated signaling using TLS SHA-1, and authenticated media using SRTP SHA-1.**
- **Cisco CallManager supports encryption of signaling messages using TLS AES and encryption of media using SRTP AES.**

© 2005 Cisco Systems, Inc. All rights reserved. CPT2 v4.1—141

Configuring Cisco IP Telephony Authentication and Encryption

Overview

This lesson explains how to configure Cisco IP telephony authentication and encryption.

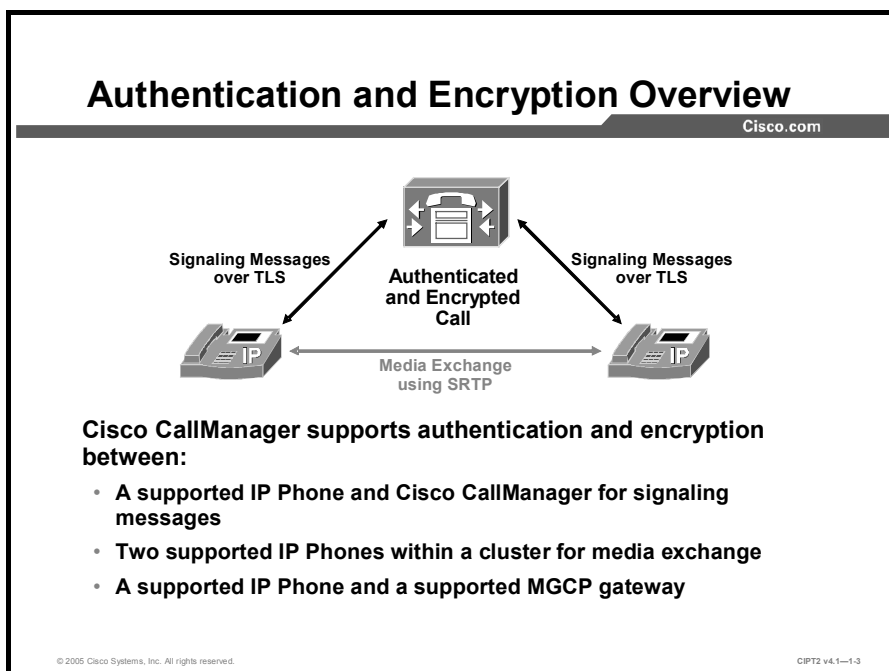
Objectives

Upon completing this lesson, you will be able to configure a Cisco CallManager cluster for secure operation. This ability includes being able to meet these objectives:

- Identify the steps to configure a Cisco CallManager system for authentication and encryption
- Activate the Cisco CTL Provider service and the CAPF service in Cisco CallManager Serviceability
- Install the Cisco CTL client on a Windows 2000 server or workstation with a USB port
- Configure the Cisco CTL client to create a CTL file and set the cluster security mode
- Use the CAPF settings in the Phone Configuration window to install, upgrade, delete, and troubleshoot LSCs
- Configure the default security mode for supported IP Phone models and the device security mode for a single device
- Generate a CAPF report in Cisco CallManager Administration to view authentication strings and authentication modes
- Find IP Phones in the network that support authentication, support encryption, or use CAPF for LSC operations

Authentication and Encryption Configuration Overview

This topic provides an overview of what you have to configure when enabling your Cisco CallManager cluster for secure calls.



Cisco CallManager Release 4.0 and later releases support authentication and encryption in a Cisco CallManager cluster. By using this feature you can secure these communications:

- **Signaling messages between a supported Cisco IP Phone and Cisco CallManager:** Cisco IP Phone 7970, 7960, and 7940 models can be configured to use Transport Layer Security (TLS) for authenticated and encrypted signaling.
- **Media exchange between two supported IP Phones within a Cisco CallManager cluster:** Cisco IP Phone 7970, 7960, and 7940 models can be configured to use Secure Real-Time Transport Protocol (SRTP) for authenticated and encrypted media exchange.

Note Cisco CallManager-to-Cisco CallManager intracluster communication is not secured. If two Cisco IP Phones are configured to use SRTP and are registered to different Cisco CallManager servers within the cluster, there is a security risk because the SRTP session keys need to be exchanged between the Cisco CallManager nodes (in cleartext). Therefore, if the communication paths between Cisco CallManager nodes within a cluster are not trusted, the recommendation is to use IPSec between the Cisco CallManager nodes.

- **Media exchange between a supported Cisco IP Phone and a supported Media Gateway Control Protocol (MGCP) gateway:** Cisco IP Phone 7970, 7960, and 7940 models and Cisco IOS MGCP gateways (running Cisco IOS Software Release 12.3(11)T2 or later) can be configured to use SRTP for authenticated and encrypted media exchange.

Note When using SRTP with an MGCP gateway, the SRTP session keys by default are exchanged in cleartext between Cisco CallManager and the MGCP gateway. Therefore, if the communication path between Cisco CallManager and the MGCP gateway is not trusted, the recommendation is to use IPSec between Cisco CallManager and the MGCP gateway.

- **Signaling messages between a supported IP Phone and a supported Cisco Survivable Remote Site Telephony (SRST) device:** Cisco IP Phone 7970, 7960, and 7940 models and Cisco IOS SRST Version 3.3 or later devices (running Cisco IOS Software Release 12.3(14)T or later) can be configured to use TLS for authenticated and encrypted signaling.
-

Note The Cisco SRST device can also provide SRTP session keys to the Cisco IP Phones so that the IP Phones that are in fallback mode can still use both signaling message and media exchange protection.

With the current release of Cisco CallManager, authenticated and encrypted calls are not possible in any other situation than listed, including these:

- **Calls to other Cisco CallManager clusters using intercluster trunks:** Secure signaling and media exchange are supported only for calls within a Cisco CallManager cluster; intercluster trunk calls are not supported.
- **Calls that are connected to any media resources, such as conferences, transcoders, or music on hold (MOH):** Secure media exchange is supported only between supported endpoints (Cisco IP Phones and Cisco IOS MGCP gateways); conference bridges, transcoders, or MOH servers are not supported endpoints.

Authentication and Encryption Configuration Checklist

Cisco.com

- **Enable security services:**
 - Cisco CTL Provider
 - CAPF
- **Use the Cisco CTL client to activate security options:**
 - Activate mixed mode
 - Create a signed CTL
- **Configure devices for security:**
 - Select MICs versus LSCs
 - Set device security mode (authenticated or encrypted)
 - Set CAPF parameters if LSCs are used

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1.4

To enable authentication and encryption support in your Cisco CallManager cluster, you need to complete these tasks:

- **Enable security services:** You need to enable the Cisco Certificate Trust List (CTL) Provider service and the Cisco Certificate Authority Proxy Function (CAPF) service.
- **Use the Cisco CTL client to activate security options:** You need to configure mixed mode and create a signed CTL.
- **Configure devices for security:** IP Phones need to have certificates (either manufacturing installed certificates [MICs] or locally significant certificates [LSCs]), they have to be configured for a security mode (authenticated or encrypted), and the CAPF parameters have to be set if LSCs are used.

Enabling Services Required for Security

This topic describes the services that have to be activated and started when enabling security in your Cisco CallManager cluster.

Enabling Services Required for Security

Cisco.com

Activate these services for security using Cisco CallManager Serviceability:

- **Cisco CTL Provider on all Cisco CallManager nodes and Cisco TFTP servers in the cluster**
- **Cisco CAPF on the publisher server only**

Service Activation Control Center

Servers: Server: 10.1.1.1
Status: Ready

[Update](#) | [Go Default](#)

Service Name	Activation Status
NT Service	
<input checked="" type="checkbox"/> Cisco CallManager	Activated
<input checked="" type="checkbox"/> Cisco Tftp	Activated
<input type="checkbox"/> Cisco Messaging Interface	Deactivated
<input type="checkbox"/> Cisco IP Voice Media Streaming App	Deactivated
<input type="checkbox"/> Cisco CallManager	Unactivated
<input type="checkbox"/> Cisco Telephony Call Dispatcher	Deactivated
<input type="checkbox"/> Cisco SIP Status Transceiver	Deactivated
<input checked="" type="checkbox"/> Cisco RPS Data Collector	Activated
<input checked="" type="checkbox"/> Cisco Database Layer Monitor	Activated
<input type="checkbox"/> Cisco CDR Insert	Deactivated
<input type="checkbox"/> Cisco Extended Functions	Deactivated
<input checked="" type="checkbox"/> Cisco Serviceability Reporter	Activated
<input checked="" type="checkbox"/> Cisco CTL Provider	Activated
<input checked="" type="checkbox"/> Cisco Certificate Authority Proxy Function	Activated
Remote Web Service	
<input type="checkbox"/> Cisco Enterprise Mobility	Deactivated
<input type="checkbox"/> Cisco IP Manager Assistant	Deactivated
<input type="checkbox"/> Cisco WebDialer	Deactivated

Note: While deactivating a service, make sure to deactivate all of the services that are dependent on this service. Please refer to online help for service dependencies for single- or multi-server configurations.

© 2005 Cisco Systems, Inc. All rights reserved. CPT2 v4.1-1-6

When enabling security in your Cisco CallManager cluster, you have to activate these services:

- **Cisco CTL Provider:** This service has to be activated on all Cisco CallManager servers and Cisco TFTP servers of your cluster.
- **Cisco Certificate Authority Proxy Function:** This service has to be activated on the publisher server.

Activate Cisco CallManager services from the Cisco CallManager Serviceability Service Activation window.


Installing the Cisco CTL Client

This topic describes how to install the Cisco CTL client application.

Installing the Cisco CTL Client

Cisco.com

- Cisco CTL client is installed from Cisco CallManager Install Plugins window
- Cisco CTL client can be installed on any Windows 2000 workstation or server with a USB port:
 - Cisco CallManager server itself
 - Any client PC
- Smart Card service has to be activated



© 2005 Cisco Systems, Inc. All rights reserved. CIPT2 v4.1-1-6

The Cisco CTL client application is installed from the Cisco CallManager Administration Install Plugins window. During installation, you are prompted for the destination folder; you can set any directory of your choice or simply accept the default.

The Cisco CTL client application can be installed on any PC running Microsoft Windows 2000 Workstation or Microsoft Windows 2000 Server, as long as that the PC has at least one Universal Serial Bus (USB) port. This device can be any Cisco CallManager server in your cluster or any client PC.

The Smart Card service has to be activated on the PC. To activate the Smart Card service under Microsoft Windows 2000, choose **Start > Settings > Control Panel > Administrative Tools > Services** to launch the Microsoft services administration tool. Then use the tool to verify the status of the Smart Card service. The startup type should be set to Automatic and the current Status should be Running.

When to Use the Cisco CTL Client

Cisco.com

- For the initial activation of secure calls
- When changing the cluster security mode
- After modifying Cisco CallManager or Cisco TFTP server configuration (adding, removing, renaming, or changing the IP address)
- After adding or removing a security token
- After replacing or restoring a Cisco CallManager or Cisco TFTP server

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1—1.7

The Cisco CTL client is needed in these situations:

- For the initial activation of security in your cluster
- For the deactivation or reactivation of security in your cluster
- After modifying Cisco CallManager or Cisco TFTP server configuration (which includes adding, removing, renaming, or restoring a server or changing the IP address or hostname of a server)
- After adding or removing a security token

Note Reasons to remove a security token include loss or theft of the security token.

- After replacing or restoring a Cisco CallManager or Cisco TFTP server

In all the situations listed, the Cisco CTL client creates a new CTL and signs it by using a security token. The Cisco IP Phones load the new CTL and are then aware of the changes to the IP telephony system. Any changes that are not reflected in the CTL (for instance, if you change the IP address of a server but do not create a new CTL using the Cisco CTL client application) cause the Cisco IP Phones to treat the corresponding device as untrusted. From this perspective, the CTL can be seen as the certificate root store of your browser (listing all trusted certificate-issuing entities). If any device that was previously trusted is not trustworthy anymore (for instance, when a security token is lost), there is no need for a certificate revocation list (CRL). Instead, you will use the Cisco CTL client and update the CRL by removing the untrusted entry (for instance, a lost security token) from the list.

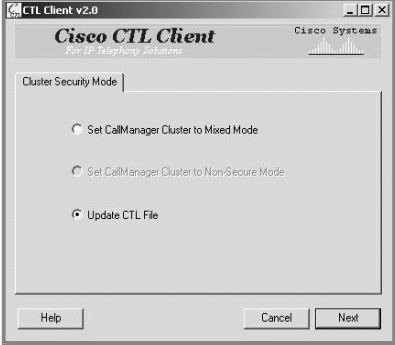
Using the Cisco CTL Client

This topic describes how to use the Cisco CTL client application.

Setting the Cluster Security Mode

Cisco.com

- There are only two modes:
 - **Mixed mode**—allows secure calls between compatible phones
 - **Nonsecure mode**—default configuration without any authenticated and encrypted calls
- There is no secure-only mode



© 2005 Cisco Systems, Inc. All rights reserved. CIPT2 v4.1-1-8

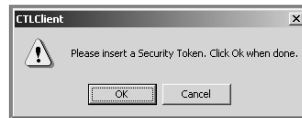
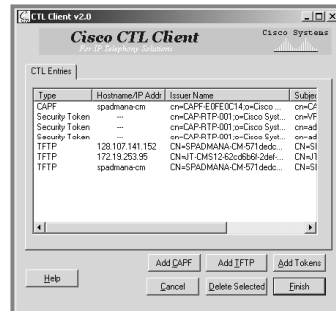
When starting the Cisco CTL client for the first time, you can either set the cluster security mode or update the CTL file. A Cisco CallManager cluster supports two security modes:

- **Mixed mode:** This mode allows secure calls between two security-enabled devices and allows nonsecure calls between devices where at least one of the devices is not security-enabled.
- **Nonsecure mode:** This is the default configuration, in which all calls are nonsecure.

Note There is no secure-only mode that would prevent Cisco IP Phones without security enabled from placing calls.

Updating the CTL

- Allows changing the CTL (necessary after adding or removing components)
- New CTL has to be signed by a security token



In addition to setting the cluster security mode, you use the Cisco CTL client to update the CTL file. This update is needed after adding or removing components, such as servers or security tokens. After changing the list of CTL entries, you need to sign the new CTL using a security token, as illustrated in the figure.

Working with LSCs

This topic describes how to create LSCs using Cisco CAPF.

Working with LSCs

Cisco.com

- **Cisco IP Phone 7940 and 7960 models do not have MICs; those IP Phones work only with LSC.**
- **The Cisco IP Phone 7970 can use either MICs or LSCs (if an LSC is installed, it has higher priority than a MIC).**
- **CAPF is used to sign IP Phone LSCs:**
 - **CAPF can act as a CA itself, signing the LSCs.**
 - **CAPF can act as a proxy to an external CA.**

© 2005 Cisco Systems, Inc. All rights reserved.CPT2 v4.1-1-10

Cisco IP Phone 7940 and 7960 models do not have MICs; they only work with LSCs. The Cisco IP Phone 7970 can use either MICs or LSCs. If an LSC is installed in a Cisco IP Phone 7970, the LSC has higher priority than the MIC.

CAPF is used to issue LSCs. CAPF can act as a Certificate Authority (CA) itself, signing the LSCs, or it can act as a proxy to an external CA, having the external CA signing the LSCs.

CAPF Service Configuration Parameter

Cisco.com

Current Service: Cisco Certificate Authority Proxy Function ?

Status: Ready

All parameters apply to the current server except those in the Clusterwide group(s)

General Parameters		
Parameter Name	Parameter Value	Suggested Value
Certificate Issuer*	Cisco Certificate Authority Proxy Function	Cisco Certificate Authority Proxy Function
Duration Of Certificate Validity (years)	15	15
Key Size (bits)*	1024	1024
Maximum Allowable Time For Key Generation (minutes)*	30	30
Maximum Allowable Attempts for Key Generation*	3	3
KEON Jurisdiction ID		
SCEP Port Number	446	446
Certificate Authority Address		

* indicates required item

- Used to set the certificate issuer (CAPF itself or external CA) and address of external CA (if used)
- Allows modification of default values, such as the key size or certificate lifetime

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-11

CAPF is configured at the CAPF service parameter web page: choose **Cisco CallManager Administration > Service > Service Parameter > Cisco Certificate Authority Proxy Function**.

You can set the certificate issuer (CAPF itself or external CA) and IP address of the external CA (if used). You can also modify some default values, such as the Rivest, Shamir, and Adleman (RSA) key size or the certificate lifetime.

CAPF—Phone Configuration Window

Cisco.com

- **Used to load LSCs into IP Phones**
- **Four possible operations:**
 - **Install/Upgrade**
 - **Delete**
 - **Troubleshoot**
 - **No Pending Operation**
- **Four possible authentication modes:**
 - **Authentication String**
 - **Null String**
 - **Existing LSC**
 - **Existing MIC**

Phone Configuration (Model = Cisco 7960)
Certification Authority Proxy Function (CAPF) Information

Certificate Operation	Install/Upgrade
Authentication Mode	By Authentication String
Authentication String	<input type="text"/> <input type="button" value="Generate String"/>
Key Size (bits)	1024
Operation Completes By**	2004 : 10 : 9 : 12 (YYYY : MM : DD : HH)
Certificate Operation Status :	

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-12

When you want to install or upgrade LSCs for Cisco IP Phones that you are configuring, use the relevant CAPF settings at the Phone Configuration window by choosing **Cisco CallManager Administration > Device > Phone**. All possible settings are found in the Certificate Authority Proxy Function (CAPF) Information area.

There are four operations options in the Certificate Operation field (as shown in the figure):

- **Install/Upgrade:** This operation allows the installation of an LSC (if the IP Phone does not already have an LSC) and the upgrade (replacement) of an existing LSC (if the IP Phone already has an LSC).
- **Delete:** This operation allows the removal of an existing LSC from a Cisco IP Phone.
- **Troubleshoot:** This operation retrieves all existing IP Phone certificates from the IP Phone and stores them in CAPF trace files. There are separate CAPF trace files for MICs and for LSCs. The CAPF trace files are located in C:\Program Files\Cisco\Trace\CAPF.
- **No Pending Operation:** This is the default value. You can also change back to this value when you want to cancel a previously configured operation that has not yet been executed.

In the Authentication Mode field (as shown in the figure), you can choose one of four possible authentication modes:

- **By Authentication String:** This authentication mode is the default and requires the Cisco IP Phone user to manually initiate the installation of an LSC. The user must authenticate to Cisco CallManager by the authentication string that has been set by the administrator in the Authentication string field. To enable the user to enter the correct authentication string, the administrator has to communicate the configured authentication string to the user.
- **By Null String:** This authentication mode disables Cisco IP Phone authentication for the download of the IP Phone certificate (enrollment). The enrollment of the IP Phone should be done over a trusted network only when this setting is used. Because no user intervention is needed, the enrollment is done automatically the next time the that the Cisco IP Phone boots or is reset.

- **By Existing Certificate (Precedence to LSC):** This authentication mode uses an existing certificate (with precedence to the LSC if both a MIC and an LSC are present in the IP Phone) for IP Phone authentication. Because no user intervention is needed, the enrollment is done automatically the next time that the IP Phone boots or is reset.
- **By Existing Certificate (Precedence to MIC):** This authentication mode uses an existing certificate (with precedence to MIC if both a MIC and an LSC are present in the IP Phone) for IP Phone authentication. Because no user intervention is needed, the enrollment is done automatically the next time that the IP Phone boots or is reset.

Example: First-Time Installation of a Certificate with Manually Entered Authentication String

Cisco.com

Certification Authority Proxy Function (CAPF) Information	
Certificate Operation	Install/Upgrade
Authentication Mode	By Authentication String
Authentication String	6420184262 <input type="button" value="Generate String"/>
Key Size (bits)	1024
Operation Completes By**	2004 : 6 : 19 : 15 (YYYY : MM : DD : HH)
Certificate Operation Status : Operation Pending	

- **Set Certificate Operation to Install/Upgrade.**
- **Set Authentication Mode to By Authentication String.**
- **Click Update and reset the phone.**
- **The user initiates install of certificate from IP Phone Settings menu.**
- **The user has to enter the authentication string (after a prompt).**
- **If successful, the certificate is issued.**

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-1-13

The figure illustrates an example for a first-time installation of a certificate with a manually entered authentication string.

For such a scenario, set the Certificate Operation field to Install/Upgrade and the Authentication Mode to By Authentication String.

You can manually enter a string of four to ten digits, or click the Generate String button to create an authentication string (and populate the Authentication String field). After you click Update and reset the IP Phone, the IP Phone is ready for enrollment. However, enrollment is not automatically triggered; it has to be initiated by the user (from the Settings menu of the Cisco IP Phone).

Note The Settings menu can also be used to gain information about the IP telephony system or remove the CTL. Usually you do not want IP Phone users to have access to such options, and therefore access to the settings on the IP Phone is often restricted or disabled. LSC enrollment with authentication by authentication string is not possible if settings access is not (fully) enabled. If access to settings is restricted or disabled, you have to enable it for the enrollment and then return it to its previous value.

When a user starts the enrollment procedure, he or she has to enter the authentication string configured, and if the process is successful, the certificate is issued to the IP Phone.

On a Cisco IP Phone 7940, the user would complete these steps:

- Step 1** Press the **Settings** button to access the Settings menu.
- Step 2** Scroll to the Security Configuration option and press the **Select** softkey to display the Security Configuration menu.
- Step 3** Press ****#** to unlock the IP Phone configuration.

- Step 4** Scroll to LSC and press the **Update** softkey to start the enrollment.
- Step 5** Enter the authentication string and press the **Submit** softkey to authenticate the IP Phone to the CAPF when prompted to do so.
- Step 6** The IP Phone generates its RSA keys and requests a certificate signed by the CAPF. When the signed certificate is installed, the message “Success” appears at the lower left corner of the Cisco IP Phone display.

Example: Certificate Upgrade Using an Existing LSC

Cisco.com

Certification Authority Proxy Function (CAPF) Information	
Certificate Operation	Install/Upgrade
Authentication Mode	By Existing Certificate (precedence to LSC)
Authentication String	By Authentication String
Key Size (bits)	By Existing Certificate (precedence to LSC)
Operation Completes By**	2004 : 6 : 19 : 15 (YYYY : MM : DD : HH)
Certificate Operation Status : Operation Pending	

- **Set Certificate Operation to Install/Upgrade.**
- **Set Authentication Mode to By Existing Certificate (Precedence to LSC).**
- **Click Update and reset the IP Phone.**
- **The IP Phone will automatically contact CAPF for update.**
- **The existing certificate will be used to authenticate the new enrollment.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIP72 v4.1-1-14

This figure illustrates an example of a certificate upgrade using an existing LSC. A reason for such an upgrade could be that an LSC that will soon reach its expiration date. By issuing a new LSC shortly before the expiration of the existing LSC, the existing LSC can still be used for the upgrade.

For such a scenario, set the Certificate Operation field to Install/Upgrade and the Authentication Mode to By Existing Certificate (Precedence to LSC).

After you click Update and reset the Cisco IP Phone, the IP Phone automatically contacts the CAPF for the download of the new certificate. The existing certificate is used to authenticate the new enrollment, and there is no need for a manually entered authentication string.

Configuring the Device Security Mode

This topic describes how to configure Cisco IP Phones to support authenticated or encrypted calls.

Configuring the Device Security Mode

Cisco.com

Cisco CallManager Defaults

Parameter Name	Parameter Value	Suggested Value
Device Security Mode*	Non Secure	Non Secure
Cluster Security Mode*	Non Secure Authenticated Encrypted	0
CAPF Phone Port*		3804

Individual Phone Settings

Location	< None >
User Locale	< None >
Network Locale	< None >
Device Security Mode	Use System Default Non Secure Authenticated Encrypted
Signal Packet Capture Mode	Encrypted

- **Default device security mode is set under Cisco CallManager Administration > System > Enterprise Parameters.**
- **Security mode of individual phone is set at Phone Configuration window under Cisco CallManager Administration > Device > Phone.**

© 2005 Cisco Systems, Inc. All rights reserved. CPT2 v4.1-1-15

After Cisco CallManager is configured for mixed mode and the Cisco IP Phones have certificates, the IP Phones have to be configured to support authenticated or encrypted calls. The device security mode is used to configure a Cisco IP Phone for one of three security modes:

- **Non Secure:** The IP Phone will not support authenticated or encrypted calls.
- **Authenticated:** The IP Phone will support authenticated calls.
- **Encrypted:** The IP Phone will support encrypted calls.

The default device security mode is configured in the Cisco CallManager Enterprise Parameters window; choose **Cisco CallManager Administration > System > Enterprise Parameters**. The possible values are: Non Secure, Authenticated, and Encrypted. The default is Non Secure.

In addition to setting the default value, you can configure each individual IP Phone with the device security mode. Choose **Cisco CallManager Administration > Device > Phone** to display the Phone Configuration window. The possible values are: Use System Default, Non Secure, Authenticated, and Encrypted. The default is Use System Default.

Caution There are several situations in which you should not use cryptographic services for Cisco IP Phones at all. With some Cisco IP Contact Center (IPCC) applications, for instance, cleartext signaling messages or media packets have to be seen by other devices (for instance, attached PCs). Another example is the use of Network Address Translation (NAT) or Port Address Translation (PAT). Because the translating device has to see cleartext signaling messages to be able to dynamically allow the negotiated UDP ports that will be used for Real-Time Transport Protocol (RTP), encryption cannot be used.

Actual Security Mode Depends on Configuration of Both Phones

Cisco.com

		Phone 2		
		Non Secure	Authenticated	Encrypted
Phone 1	Non Secure	Non Secure	Non Secure	Non Secure
	Authenticated	Non Secure	Authenticated	Authenticated
	Encrypted	Non Secure	Authenticated	Encrypted

- If any of the devices is set to Non Secure, a nonsecure call is placed.
- If both devices are set to Encrypted, an encrypted call is placed (the call is authenticated and encrypted).
- In all other situations, an authenticated call is placed.

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-16

The actual security mode used for a call depends on the configuration of both IP Phones participating in the call. As shown in the table, these rules apply:

- If one device is set to Non Secure, a nonsecure call (that is, a call without authentication and without encryption) is placed.
- If both devices are set to Encrypted, an encrypted call (that is, a call with authentication and encryption) is placed.
- In all other situations (either both IP Phones are set to Authenticated or one is set to Authenticated and the other one is set to Encrypted), an authenticated call (that is, a call with authentication only) is placed.
- If one phone is set to authenticated and the other set to non secure the (end to end) call is not considered to be authenticated because only one phone will use authenticated signaling to Cisco Call Manager.

Generating a CAPF Report

This topic describes how to generate CAPF reports from Cisco CallManager Administration.

Generating a CAPF Report

Cisco.com

- **CAPF reports can be created from Cisco CallManager Administration.**
- **Allows searching for IP Phones matching selected CAPF criteria:**
 - **Certificate Operation Status**
 - **Device Security Mode**
 - **Authentication Mode**
 - **Authentication String**
- **Entries from the results list can be clicked to directly access the configuration page of the corresponding IP Phone.**
- **The results list can be saved in CSV format.**

© 2005 Cisco Systems, Inc. All rights reserved. CPT2 v4.1-1-17

CAPF reports can be created from Cisco CallManager Administration.

To generate a CAPF report, you can search for IP Phones matching selected CAPF criteria:

- **Certificate Operation Status**

Note The Certificate Operation Status displays the result of the last CAPF activity for each IP Phone. Possible values include None (typically shown on IP Phones with device security mode Non Secure), Operation Pending (when CAPF waits for a user to manually retrieve a [new] certificate) and result information (success, failure) after upgrade, delete, or troubleshooting operations.

- **Device Security Mode**
- **Authentication Mode**
- **Authentication String**

Entries from the results list can be clicked to directly display the configuration window of the corresponding IP Phone.

The results list of a search can be saved to a file in comma-separated value (CSV) format.

CAPF Report Example

Cisco.com

The screenshot shows the Cisco CallManager Administration interface. At the top, there is a navigation menu with items: System, Route Plan, Service, Feature, Device, User, Application, and Help. Below the menu is the page title "Cisco CallManager Administration" and the Cisco Systems logo. The main heading is "CAPF Report". The content area displays the message: "No matches were found for Certificate Operation Status begins with """. Below this message is a search form with the following fields: "Find phones where" followed by a dropdown menu set to "Certificate Operation Status", "begins with" followed by a dropdown menu set to "Upgrade Failed", and a "Find" button. Below the search form, it says "and show 20 items per page." and "Upgrade Failed". At the bottom of the search form, there is a small note: "To list all items, click Find without entering any search text, or use 'Device Name is not empty' as the search."

- **Open the CAPF window from Cisco CallManager Administration > Device > Device Settings > CAPF Report.**
- **The CAPF report user interface is similar to the Find and List Phones window.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIP72 v4.1—1-18

The example shows a CAPF report where the administrator accessed the CAPF Report window by choosing Cisco CallManager Administration > Device > Device Settings > CAPF Report and started a report for all IP Phones where the certificate operation status is Upgrade Failed. No such entries were found.

The CAPF report user interface is similar to the Find and List Phones window.

Finding IP Phones with Security Features

This topic describes how you can find IP Phones with security features from Cisco CallManager Administration.

Finding Phones with Security Features

Cisco.com

Two different tools can be used to find phones with security features:

- **CAPF report, which allows you to search for CAPF related criteria only**
- **The standard Find and List Phones window, which allows to you search for fewer CAPF criteria but offers other search criteria:**
 - **LSC status**
 - **Device security mode**
 - **Device name**
 - **Description**
 - **Directory number**

© 2005 Cisco Systems, Inc. All rights reserved. CPT2 v4.1-1-19

To find IP Phones with security features, you have two options:

- **Use CAPF reports:** These reports allow searching for CAPF-related criteria only but allow saving the result in a CSV file.
- **Use the standard Find and List Phones window:** This window allows searching for CAPF criteria and other criteria that are not available in the CAPF reports. Search results are displayed on the screen but cannot be saved to a file.

When using the Find and List Phones window, you can search for these criteria that are not available in the CAPF report tool:

- Device name
- Description
- Directory number
- Others (for example, device pool and device type)

Example: Finding Phones Using the Find and List Phones Window

Cisco.com

The screenshot shows the Cisco CallManager Administration interface. The 'Find and List Phones' window is open, displaying search results for IP phones where the device security mode begins with 'Authenticated'. The search criteria are: 'Find phones where Device Security Mode begins with Authenticated'. The results show two entries:

Device Security Mode	Device Name	Description	Directory Number	Owner User ID	Copy
Authenticated	SEP000F24497661	Auto 1001	1001		
Authenticated	SEP0012D9421EB2	Auto 1002	1002		

- The Find and List Phones window is used to search for phones where device security mode begins with “Authenticated.”
- Two entries have been found.

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-1-20

The figure shows an example of using the Find and List Phones window (accessible by choosing Cisco CallManager Administration > Device > Phone) to search for IP Phones where the device security mode is Authenticated. Two IP Phones have been found matching the search criteria.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Cisco IP telephony features authentication and encryption.**
- **The Cisco CTL Provider service and the Cisco CAPF service need to be enabled for secure telephony.**
- **The CTL client, software that is used to sign the CTL by utilizing a security token, needs to be installed manually.**
- **The CTL client needs to be executed whenever CTL entries change.**

© 2005 Cisco Systems, Inc. All rights reserved. CPT2 v4.1—1-21

Summary (Cont.)

Cisco.com

- **Cisco IP telephony allows the use of LSCs on all security-enabled IP Phones.**
- **Devices can be configured for nonsecure calls, authenticated calls only, or authenticated and encrypted calls.**
- **CAPF reports allow searching for IP Phones that match selected CAPF criteria.**
- **Security-enabled phones can be found by using CAPF reports or by using the Find and Select Phones window.**

© 2005 Cisco Systems, Inc. All rights reserved. CPT2 v4.1—1-22

Module Summary

This topic summarizes the key points discussed in this module.

Module Summary

Cisco.com

- **The Cisco CallManager operating systems need to be secured to resist attacks.**
- **HTTPS and MLA allow secure administration of Cisco CallManager.**
- **Cisco CallManager provides several features to prevent toll fraud.**
- **The Cisco IP Phone needs to be hardened to resist attacks.**

© 2005 Cisco Systems, Inc. All rights reserved. CPT2 v4.1-1-1

Module Summary (Cont.)

Cisco.com

- **There are four cryptographic services: confidentiality, integrity, authentication, and nonrepudiation.**
- **A PKI allows scalable and secure deployment of cryptographic services.**
- **Authentication and encryption can be configured in a Cisco IP telephony system to provide secure IP telephony.**
- **The configuration of authentication and encryption in an IP telephony system includes cluster-wide settings and device-specific parameters.**

© 2005 Cisco Systems, Inc. All rights reserved. CPT2 v4.1-1-2

This module described how to secure a Cisco IP telephony system. It also provided information about cryptographic fundamentals and how they are applied to the Cisco IP telephony system. It first described how to secure Cisco CallManager operating systems and then explained how HTTPS and MLA allow secure administration of the system. It covered features that help to prevent toll fraud and described how to harden Cisco IP Phones. The module provided information about cryptographic services and the role of a PKI in a secure environment. Then the module explained how a Cisco IP telephony system can be secured with authentication and encryption and ended with information on how to configure authentication and encryption in a Cisco IP telephony system.

References

For additional information, refer to these resources:

- Cisco Systems Inc. *Cisco CallManager Administration Guide, Release 4.1(3)*.
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_book09186a00803be4ec.html.
- Cisco Systems Inc. *Cisco CallManager System Guide, Release 4.1(3)*.
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_book09186a00803be4ee.html.
- Cisco Systems Inc. *Cisco CallManager Security Guide, Release 4.1(3)*.
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_book09186a00803c8c67.html.
- Cisco Systems Inc. Cisco CallManager Compatibility Matrix.
http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm.
- Federal Information Processing Standards Publications. *Secure Hash Standard*.
<http://www.itl.nist.gov/fipspubs/fip180-1.htm>.
- Internet Engineering Task Force. *The Secure Real-time Transport Protocol (SRTP), RFC 3711*.
<http://www.ietf.org/rfc/rfc3711.txt>.
- Microsoft Corporation (Microsoft Windows 2000 Certificate Services).
www.microsoft.com.
- VeriSign, Inc (outsourced PKI services).
www.verisign.com.
- Entrust Technologies (PKI products and outsourced PKI services).
www.entrust.com.
- OpenCard and GemPlus S.A. (smart card and smart token technologies).
www.opencard.org.
www.gemplus.com.
- Cisco Systems Inc. *Cisco IOS SRST Version 3.3 System Administrator Guide, Setting Up Secure SRST*.
http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5207/products_administration_guide_chapter09186a008022c969.html.
- Cisco Systems Inc. *Cisco CallManager Security Guide, Release 4.1(3), Configuring a Secure MGCP Gateway*.
http://www.cisco.com/en/US/partner/products/sw/voicesw/ps556/products_administration_guide_chapter09186a00803fe67b.html.

Module 1 Self-Check

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module 1 Self-Check Answer Key.

- Q1) When are critical hotfixes and patches to the Cisco IP Telephony Operating System posted on Cisco.com for download? (Source: Securing the Windows Operating System)
- A) 24 hours after the announcement from Microsoft
 - B) monthly in a consolidated security release
 - C) with the next operating system upgrade
 - D) should be downloaded from Microsoft as soon as they appear
- Q2) What instruction manual should be used to provide additional IPsec filters? (Source: Securing the Windows Operating System)
- A) CCM-OS-OptionalSecurity.cmd
 - B) CCM-OS-OptionalSecurity-Readme.doc
 - C) Before-CallManager-Upgrade.htm
 - D) IPSec-W2KSQL-Readme.htm
- Q3) Which feature should not be enabled when using antivirus protection software? (Source: Securing the Windows Operating System)
- A) full-scan
 - B) heuristic scan
 - C) e-mail scan
 - D) pagefile scan
- Q4) Which Cisco-provided software tool protects Cisco CallManager against malicious applications? (Source: Securing the Windows Operating System)
- A) CDR
 - B) CER
 - C) CSA
 - D) CRM
- Q5) What parameter has to be set on all service accounts? (Source: Securing the Windows Operating System)
- A) complex password requirement
 - B) minimum password length of six characters
 - C) password never expires
 - D) enforce password history
- Q6) What Microsoft service is most commonly attacked? (Source: Securing the Windows Operating System)
- A) DNS service
 - B) DHCP service
 - C) IIS service
 - D) Active Directory service

- Q7) Which setting on the Cisco IP Telephony Operating System is actually supported by Cisco but not recommended? (Source: Securing the Windows Operating System)
- A) delete the IUSER_Guest account
 - B) delete SQL service accounts
 - C) install third-party utilities
 - D) disable Dr. Watson
- Q8) What is the danger when browsing unsecured and without MLA to the Cisco CallManager Administration window? (Source: Securing Cisco CallManager Administration)
- A) There is no risk.
 - B) With a sniffed username and password, a hacker can log in to the Cisco CallManager Administration window only.
 - C) With a sniffed username and password, a hacker can log in to the Cisco CallManager Administration window as well as to the operating system.
 - D) The hacker can only listen to the conversation.
- Q9) How do you browse securely to the CallManager Administration window? (Source: Securing Cisco CallManager Administration)
- A) <http://CM-IP/SecureCCMAdmin>
 - B) <https://CM-IP/CCMAdmin>
 - C) <https://CM-IP/TTL/CCMAdmin>
 - D) <https://CM-IP/SSL/CCMAdmin>
- Q10) On the certificate details tab, which is not an option when selecting the certificate fields to be displayed?
- A) All
 - B) Extensions Only
 - C) Critical Extensions Only
 - D) Key Information Only
 - E) Properties Only
- Q11) When you are renaming a newly installed certificate, what should the name be? (Source: Securing Cisco CallManager Administration)
- A) httpcert.cer
 - B) httpsert.cer
 - C) httpscert.cert
 - D) httpscert.certificate
- Q12) Which is not a valid access level in MLA? (Source: Securing Cisco CallManager Administration)
- A) no access
 - B) read-only
 - C) read-write
 - D) full access
- Q13) After you enable MLA, what is the new administrator account? (Source: Securing Cisco CallManager Administration)
- A) MLAAdministrator
 - B) Administrator
 - C) Windows NT Administrator account
 - D) CCMAdministrator

- Q14) Which functional group is not a default group? (Source: Securing Cisco CallManager Administration)
- A) Standard Device
 - B) Standard Service
 - C) Standard Gateway
 - D) Standard Plugin
 - E) Standard RoutePlan
- Q15) Which user group is not a default group? (Source: Securing Cisco CallManager Administration)
- A) PhoneAdministration
 - B) FullAccess
 - C) SuperUserGroup
 - D) GatewayAdministration
 - E) ServerMaintenance
- Q16) Which should be done first when you create a new functional and user group for special purposes? (Source: Securing Cisco CallManager Administration)
- A) Create a new user group.
 - B) Create a new functional group.
 - C) Create a new privilege matrix.
 - D) Configure administration access.
- Q17) Which two of the following are types of toll fraud? (Choose two.) (Source: Preventing Toll Fraud)
- A) voice mail-to-voice mail transfer
 - B) Call Forward All
 - C) transfer from voice mail
 - D) transfer to an internal destination
 - E) transfer to a conference system
- Q18) Which two fields have to be defined in the Call Forward All field? (Choose two.) (Source: Preventing Toll Fraud)
- A) Destination
 - B) Partition
 - C) Calling Search Space
 - D) Hunt List
- Q19) Which is not defined when configuring time periods? (Source: Preventing Toll Fraud)
- A) Start Time
 - B) End Time
 - C) Duration Time
 - D) Period Name
- Q20) When you are restricting external call transfers, which statements are correct? (Source: Preventing Toll Fraud)
- A) Route Pattern and Hunt List can be classified as OnNet or OffNet.
 - B) Calls must be classified in order to use call-transfer restrictions.
 - C) Transfer Restrictions, restricted OnNet-to-OffNet transfer, and OffNet-to-OffNet transfer can be used.
 - D) Only internal devices must be classified.

- Q21) Which two service parameters can be configured when using ad hoc conference restrictions? (Choose two.) (Source: Preventing Toll Fraud)
- A) Never
 - B) When First OnNet Party Leaves the Conference
 - C) When No OffNet Parties Remain in the Conference
 - D) When Conference Creator Drops Out
- Q22) What is the default value for the Drop Ad Hoc Conference service parameter? (Source: Preventing Toll Fraud)
- A) Never
 - B) Drop Ad Hoc Conference When Creator Leaves
 - C) When No OnNet Parties Remain in the Conference
 - D) When No OffNet Parties Remain in the Conference
- Q23) What is the purpose of FACs? (Source: Preventing Toll Fraud)
- A) time-based call routing
 - B) restricting call routing to destinations based on the time of day
 - C) restricting call routing to destinations based on user codes
 - D) restricting call routing to destinations based on OnNet or OffNet classification
- Q24) Why is it important to block commonly exploited area codes when you want to restrict international calls? (Source: Preventing Toll Fraud)
- A) Commonly exploited countries have special premium numbers as country codes.
 - B) Commonly exploited countries have special country codes that look like area codes of the United States.
 - C) Countries such as the Bahamas can be reached either over the country code or over an area code.
 - D) When these numbers are not blocked, they are treated like normal local telephone calls.
- Q25) What could be of an interest to a hacker planning to attack an IP Phone? (Source: Hardening the IP Phone)
- A) The attacker can learn about the IP telephony environment.
 - B) The attacker can start attacks from the IP Phone, because it is a trusted device.
 - C) With a modified image and configuration file, the attacker can bring down the Cisco CallManager.
 - D) The attacker can sabotage a special user.
- Q26) Which IP Phone does not support configuration file authentication? (Source: Hardening the IP Phone)
- A) Cisco IP Phone 7920
 - B) Cisco IP Phone 7940
 - C) Cisco IP Phone 7960
 - D) Cisco IP Phone 7970
- Q27) Where are IP Phone security settings configured? (Source: Hardening the IP Phone)
- A) Directory Number Configuration
 - B) Phone Configuration
 - C) Phone Security Configuration
 - D) Product Specific Configuration

- Q28) How do you browse to the IP Phone? (Source: Hardening the IP Phone)
- A) <http://IP-Phone's-IP-address>
 - B) <https://IP-Phone's-IP-address>
 - C) <https://IP-Phone's-IP-address/CCMAdmin>
 - D) <https://IP-Phone's-IP-address/Admin>
- Q29) Which statement is not true about gratuitous ARP attacks? (Source: Hardening the IP Phone)
- A) Gratuitous ARP is a man-in-the-middle attack.
 - B) Gratuitous ARP attackers usually operate from the Internet.
 - C) Gratuitous ARP is normally used for HSRP.
 - D) Ettercap is a tool used for gratuitous ARP attacks.
- Q30) Which is not a purpose for the built-in switch in the Cisco IP Phone? (Source: Hardening the IP Phone)
- A) call recording
 - B) lawful interception
 - C) supervisory monitoring
 - D) none of the above—switch is acting like a hub
- Q31) Which of the following statements about authentication and encryption is not true? (Source: Hardening the IP Phone)
- A) It was introduced with Cisco CallManager Release 4.0.
 - B) Media streams use SRTP.
 - C) Signaling uses Secure SCCP.
 - D) TLS was formerly known as SSL.
- Q32) Which two of the following are not cryptographic services? (Choose two.) (Source: Understanding Cryptographic Fundamentals)
- A) authenticity
 - B) confidentiality
 - C) integrity
 - D) nonrepudiation
 - E) resistance against DoS
 - F) defense in depth
- Q33) Which two statements about symmetric encryption are true? (Choose two.) (Source: Understanding Cryptographic Fundamentals)
- A) Symmetric encryption is a good choice for real-time encryption of bulk data.
 - B) Symmetric encryption is commonly used to sign asymmetric keys.
 - C) Symmetric encryption uses asymmetric keys.
 - D) RSA is an example of a symmetric encryption algorithm.
 - E) ASE is an example of a symmetric encryption algorithm.
 - F) With symmetric encryption, the encryption key equals the decryption key.

- Q34) Which two statements about asymmetric encryption are true? (Choose two.) (Source: Understanding Cryptographic Fundamentals)
- A) Asymmetric encryption is considerably faster than symmetric encryption.
 - B) Asymmetric encryption keys should have about half the lifetime of symmetric encryption keys.
 - C) With asymmetric encryption, the private key can only encrypt data, while the public key can only decrypt data.
 - D) With asymmetric encryption, either of the two keys can be used for encryption and the other key can be used for decryption.
 - E) NSA is an example of an asymmetric encryption algorithm.
 - F) Asymmetric encryption is often used to create signatures.
- Q35) Which two statements about hash functions are true? (Choose two.) (Source: Understanding Cryptographic Fundamentals)
- A) A hash digest can never be reverted to the hashed data.
 - B) It is computationally difficult to revert a hash digest to the hashed data.
 - C) Data can be encrypted if hashed with a secret key.
 - D) Data can be signed by appending a hash of the data.
 - E) AES can use SHA-1 for data encryption.
 - F) AES can use MD5 for signing data.
- Q36) Which of the following statements does not apply to digital signatures? (Source: Understanding Cryptographic Fundamentals)
- A) Digital signatures provide data authenticity.
 - B) Digital signatures provide data integrity.
 - C) Digital signatures provide nonrepudiation.
 - D) Digital signatures do not provide data confidentiality.
 - E) Digital signatures are based on asymmetric cryptographic algorithms.
 - F) Digital signatures are created by hashing the result of an asymmetric encryption.
- Q37) What problem does PKI solve? (Source: Understanding PKI)
- A) the lack of a common encryption standard for Internet applications
 - B) the problem that asymmetric encryption techniques do not work without a PKI
 - C) the fact that Diffie-Hellman is not secure
 - D) the problem of scalable, secure key exchange
 - E) the problem of manually issuing bulk certificates
 - F) the performance problem when using RSA
- Q38) Which two statements about trusted introducing are incorrect? (Choose two.) (Source: Understanding PKI)
- A) The trusted introducer has to be trusted by all other members of the system.
 - B) The trusted introducer has to trust all other members of the system.
 - C) The trusted introducer guarantees for the authenticity of entities it is introducing to others.
 - D) Only the trusted introducer has to trust the root of the system.
 - E) The trusted introducer is the root of a system.
 - F) Any entity of the system can guarantee the authenticity of any other member.

- Q39) Which statement about a certificate is true? (Source: Understanding PKI)
- A) A certificate includes the identity of the owner of the certificate and the symmetric key of the owner.
 - B) A certificate includes the public key of the issuer.
 - C) A certificate includes the identity of the owner of the certificate and the private key of the owner.
 - D) A certificate includes the identity of the issuer of the certificate, the identity of the owner of the certificate, and the public key of the owner.
 - E) A certificate does not include any keys in cleartext.
 - F) A certificate includes an encrypted private key of the owner and a cleartext public key of the issuer.
- Q40) Which are the two valid options to secure enrollment in a PKI? (Choose two.) (Source: Understanding PKI)
- A) Perform the enrollment from a trusted device only.
 - B) Perform the enrollment in both directions.
 - C) Perform the enrollment over a trusted network.
 - D) Use self-signed certificates on all devices.
 - E) Do not send the private key in the enrollment.
 - F) Perform mutual out-of-band authentication between the PKI user and CA.
- Q41) Which is true about certificate revocation? (Source: Understanding PKI)
- A) Any entity of a PKI system that receives an untrusted certificate can request revocation of that certificate.
 - B) The CA periodically revokes all expired certificates.
 - C) Certificate revocation is needed when the public key has been transferred without a certificate.
 - D) Certificate revocation is needed whenever the private key is not trustworthy anymore.
 - E) Certificate revocation is needed whenever the public key is not trustworthy anymore.
 - F) Certificate revocation is the process of adding a user to the PKI.
- Q42) What is the certificate of a web server used for when you are using SSL? (Source: Understanding PKI)
- A) It is used to authenticate the client.
 - B) The public key of the server is used by the client when encrypting the data sent to the server.
 - C) The private key of the server is used by the client when encrypting the data sent to the server.
 - D) It is used to authenticate the server and to protect the challenge response traffic during client authentication.
 - E) It is used to authenticate the server and to encrypt the symmetric session keys used for the asymmetric encryption of the data stream.
 - F) It is used to authenticate the server and to encrypt the symmetric session keys used for the authentication and encryption of the data stream.

- Q43) Which two of the following are not security threats to an IP telephony system? (Choose two.) (Source: Understanding Cisco IP Telephony Authentication and Encryption Fundamentals)
- A) loss of privacy
 - B) impersonation
 - C) integrity
 - D) loss of integrity
 - E) loss of control
 - F) DoS
- Q44) Identify the two correct mappings of application—protocol—security features. (Choose two.) (Source: Understanding Cisco IP Telephony Authentication and Encryption Fundamentals)
- A) secure signaling—SRTP—device authentication, integrity
 - B) secure signaling—TLS—device authentication, integrity, privacy
 - C) secure media—SRTP—privacy, confidentiality, security
 - D) secure media—TLS—privacy, confidentiality, security
 - E) secure media—TLS—privacy, integrity
 - F) secure media—SRTP—privacy, integrity
- Q45) Which two statements about PKI topologies in Cisco IP telephony are true? (Choose two.) (Source: Understanding Cisco IP Telephony Authentication and Encryption Fundamentals)
- A) MICs are self-signed by the IP Phone.
 - B) Cisco IP Phone 7940, 7960, and 7970 models can have MICs and LSCs.
 - C) The CAPF has a self-signed certificate.
 - D) Cisco IP Phone 7940, 7960, and 7970 models can only have LSCs.
 - E) The CTL is signed by the Cisco manufacturing CA.
 - F) MICs are signed by CAPF.
- Q46) Which statement about enrollment in the IP telephony PKI is true? (Source: Understanding Cisco IP Telephony Authentication and Encryption Fundamentals)
- A) MICs are issued by CAPF itself or by an external CA.
 - B) LSCs are issued by the Cisco CTL client or by CAPF.
 - C) CAPF enrollment supports the use of authentication strings.
 - D) CAPF itself has to enroll with the Cisco CTL client.
 - E) Enrollment of IP Phones occurs automatically if the cluster is in secure-only mode.
 - F) LSCs can be issued by an external CA when using the CTL client as a proxy.
- Q47) Which of the following entities uses a smart token for key storage? (Source: Understanding Cisco IP Telephony Authentication and Encryption Fundamentals)
- A) CTL
 - B) CTL client
 - C) CAPF in proxy mode
 - D) CAPF in CA mode
 - E) Cisco IP Phone 7940 and 7960
 - F) Cisco IP Phone 7970

- Q48) What are the authentication features of TLS in Cisco IP telephony? (Source: Understanding Cisco IP Telephony Authentication and Encryption Fundamentals)
- A) two-way device authentication
 - B) two-way device authentication and signed media messages
 - C) one-way device authentication and signed signaling message
 - D) two-way device authentication and signed signaling messages
 - E) one-way device authentication and signed media messages
 - F) signed signaling messages
- Q49) What are prerequisites for SRTP encryption in Cisco IP telephony? (Source: Understanding Cisco IP Telephony Authentication and Encryption Fundamentals)
- A) mutual device authentication between the IP Phones using SRTP
 - B) TLS device authentication, TLS message authentication, TLS message encryption, and SRTP packet authentication
 - C) mutual device authentication between the IP Phones using TLS
 - D) TLS message authentication and SRTP device authentication
 - E) TLS device authentication, TLS message authentication, and TLS message encryption
 - F) TLS device authentication, TLS message encryption, and SRTP packet authentication
- Q50) During an encrypted call between two IP Phones, which two of the following does not happen? (Choose two.) (Source: Understanding Cisco IP Telephony Authentication and Encryption Fundamentals)
- A) mutual certificate exchange between Cisco CallManager and each IP Phone
 - B) mutual certificate exchange between the IP Phones
 - C) SRTP packet authentication and encryption
 - D) encrypted transmission of SRTP session keys between the IP Phones
 - E) TLS packet authentication and encryption
 - F) encrypted transmission of TLS session keys between Cisco CallManager and the IP Phones
- Q51) Which is the most accurate list of tasks required to configure a Cisco CallManager cluster for security? (Source: Configuring Cisco IP Telephony Authentication and Encryption)
- A) enable services, set cluster to mixed mode, create a signed CTL, and deploy certificates to the IP Phones
 - B) enable services, set cluster to secure-only mode, create a signed CTL, and deploy certificates to the IP Phones
 - C) enable extended services, set cluster to authenticated or encrypted mode, create a signed CTL, and deploy certificates to the IP Phones
 - D) disable extended services, set cluster to mixed mode, create a signed CTL, and deploy certificates to the IP Phones
 - E) enable services, set cluster to mixed mode, create a signed CTL, deploy certificates to the IP Phones, and set the device security mode
 - F) run the auto-secure feature

- Q52) Which two services must be enabled when configuring a Cisco CallManager cluster for security? (Choose two.) (Source: Configuring Cisco IP Telephony Authentication and Encryption)
- A) Cisco CAPF
 - B) Cisco Authority Provider Function
 - C) Cisco CTL Provider
 - D) Cisco CTL Proxy
 - E) Cisco CTL Client Provider
 - F) Cisco Extended Functions
- Q53) What are the needs for the PC when you are installing Cisco CTL Client? (Source: Configuring Cisco IP Telephony Authentication and Encryption)
- A) Windows 2000 operating system, at least one USB port, Smart Card Service enabled
 - B) Windows XP operating system, at least two USB ports, Smart Card Service enabled
 - C) Windows 2000 operating system, at least two USB ports, Smart Card Service disabled
 - D) installation on Cisco CallManager publisher server only, two available USB ports, Smart Card Service enabled
 - E) Windows 2000 operating system, PCMCIA slot, Smart Card Service enabled
 - F) Windows 2000 operating system, at least one USB port, Cisco VT Advantage camera, Smart Card Service enabled
- Q54) When is update of the configuration using the Cisco CTL client not needed? (Source: Configuring Cisco IP Telephony Authentication and Encryption)
- A) when an LSC of the IP Phone is upgraded
 - B) when a security token is added to the system
 - C) when a Cisco CallManager has been removed
 - D) when an IP address of the Cisco TFTP server has been changed
 - E) when changing from MICs to LSCs on all Cisco IP Phone 7970 models
 - F) when changing from MICs to LSCs on all Cisco IP Phone 7960 models
- Q55) Which two statements about LSCs are correct? (Choose two.) (Source: Configuring Cisco IP Telephony Authentication and Encryption)
- A) On a Cisco IP Phone 7970, a MIC has priority over an LSC.
 - B) On a Cisco IP Phone 7960, an LSC has priority over a MIC.
 - C) The CAPF issues LSCs if used as a CA and MICs if used as a proxy.
 - D) The certificate operation of the CAPF can be set to Install, Upgrade, or Delete.
 - E) The certificate operation of the CAPF can be set to Install/Upgrade, Delete, or Troubleshoot.
 - F) CAPF authentication can be configured to be done by authentication string, null string, or existing certificates.

- Q56) Which two combinations of device security modes and resulting call type are correct? (Choose two.) (Source: Configuring Cisco IP Telephony Authentication and Encryption)
- A) Phone 1: Non Secure, phone 2: Authenticated; call: authenticated
 - B) Phone 1: Non Secure, phone 2: Encrypted; call: authenticated
 - C) Phone 1: Authenticated, phone 2: Non Secure; call: nonsecure
 - D) Phone 1: Encrypted, phone 2: Authenticated; call: authenticated
 - E) Phone 1: Authenticated, phone 2: Encrypted; call: encrypted
 - F) Phone 1: Encrypted, phone 2: Non Secure; call: encrypted
- Q57) Which two of the following options are not search criteria when you are creating a CAPF report? (Choose two.) (Source: Configuring Cisco IP Telephony Authentication and Encryption)
- A) authentication mode
 - B) certificate operation status
 - C) device name
 - D) certificate lifetime
 - E) authentication string
 - F) device security mode
- Q58) Which two of the following options are not search criteria when you are searching for IP Phones using the Find and List Phones window? (Choose two.) (Source: Configuring Cisco IP Telephony Authentication and Encryption)
- A) authentication mode
 - B) LSC status
 - C) device name
 - D) directory number
 - E) authentication string
 - F) device security mode

Module 1 Self-Check Answer Key

- Q1) A
- Q2) D
- Q3) B
- Q4) C
- Q5) C
- Q6) C
- Q7) D
- Q8) C
- Q9) B
- Q10) D
- Q11) B
- Q12) C
- Q13) D
- Q14) A
- Q15) B
- Q16) B
- Q17) B, C
- Q18) A, C
- Q19) C
- Q20) A
- Q21) A, D
- Q22) A
- Q23) C
- Q24) B
- Q25) A
- Q26) B
- Q27) D
- Q28) A
- Q29) B
- Q30) D
- Q31) C
- Q32) E, F
- Q33) A, F
- Q34) D, F
- Q35) A, F

- Q36) F
- Q37) D
- Q38) D, F
- Q39) D
- Q40) C, F
- Q41) D
- Q42) F
- Q43) C, E
- Q44) B, F
- Q45) C, D
- Q46) C
- Q47) B
- Q48) D
- Q49) B
- Q50) B, D
- Q51) E
- Q52) A, C
- Q53) A
- Q54) A
- Q55) E, F
- Q56) C, D
- Q57) C, D
- Q58) A, E

Module 2

Enabling IP Video Telephony

Overview

You can now take full advantage of your IP network to deliver enterprise-class business communications that extend voice and video to every user in their organization. Cisco CallManager Release 4.1 brings video telephony functionality to Cisco IP Phones, providing Cisco IP Phone users with the ability to add video to their communications experience.

Cisco Video Telephony (VT) Advantage is a video telephony solution comprising the Cisco VT Advantage software application and Cisco VT Camera, a video telephony Universal Serial Bus (USB) camera. With the Cisco VT Camera attached to a PC colocated with a Cisco IP Phone, users can place and receive video calls on their enterprise IP telephony network.

This module discusses video telephony in Cisco CallManager environments. It also describes the Cisco VT Advantage software, the installation process, and troubleshooting Cisco VT Advantage.

Module Objectives

Upon completing this module, you will be able to make IP video telephony calls with Cisco VT Advantage and describe the basic components and characteristics of video calls and Cisco CallManager configuration parameters that enable video. This ability includes being able to meet these objectives:

- Describe the characteristics and features of video calls and identify their bandwidth requirements
- Configure Cisco VT Advantage

Introducing IP Video Telephony

Overview

Companies that want to enable video calls can install and use products from the Cisco enterprise video products portfolio. Video communication capabilities are integrated into Cisco CallManager Release 4.0—extending several voice features to video to benefit end users, network administrators, and enterprises as a whole. A common IP infrastructure for all communications not only provides an enterprise with reduced cost of ownership but with a faster return on investment (ROI) as users more readily and easily adapt to a system that can be deployed to the desktop.

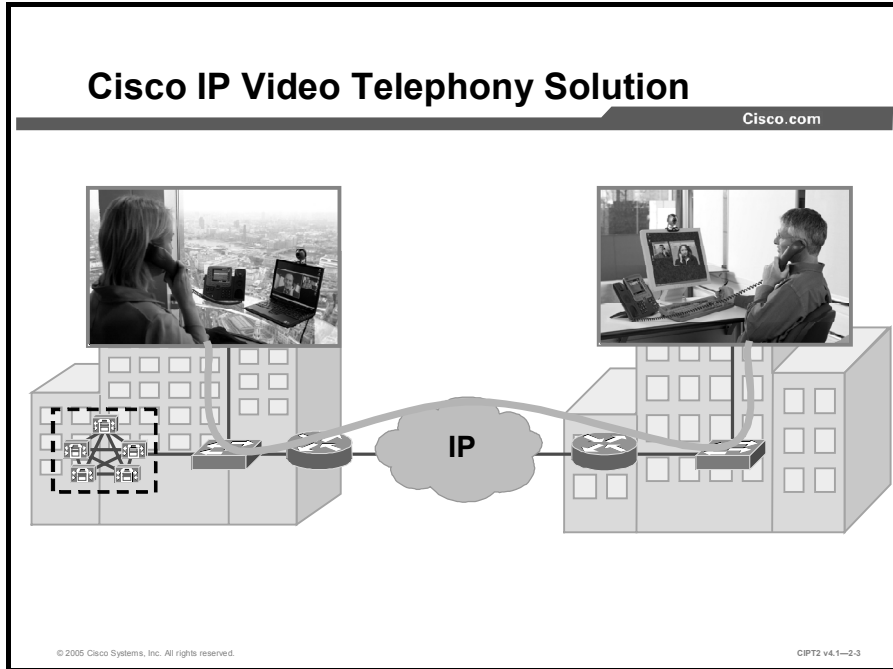
Objectives

Upon completing this lesson, you will be able to describe the characteristics and features of video calls and identify their bandwidth requirements. This ability includes being able to meet these objectives:

- Classify the functions and components of the Cisco IP video telephony solution
- Characterize a video call in terms of the RTP stream types and codecs, and describe audio and video bandwidth requirements
- Compare an H.323 video call in a Cisco CallManager environment with an SCCP video call
- Describe the two main factors that determine the bandwidth requirement for video calls and calculate bandwidth requirements
- Implement call admission control within a cluster using the locations and regions of Cisco CallManager Administration
- Describe call admission control between clusters using a gatekeeper

IP Video Telephony Solution Components

This topic describes Cisco IP video telephony solution components.

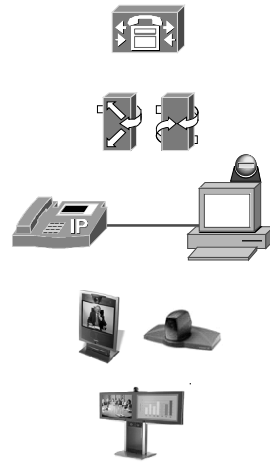


Cisco introduced its IP video telephony solution in Cisco CallManager Release 4.0. With this solution, video is fully integrated into Cisco CallManager, and there are new endpoints available from Cisco and its strategic partners. Video is now just as easy to deploy, manage, and use as a Cisco IP Phone.

IP Video Telephony Solution Components

Cisco.com

- Cisco CallManager Release 4.0 or later:
 - Providing single dial plan and call control
 - Managing video resources
- Cisco IP/VC Release 3.2 plus Cisco IP/VC 3540:
 - Integration with Cisco CallManager via SCCP
 - Enables ad hoc conferencing for video devices
 - Configurable as H.323, SCCP, or H.323 and SCCP
 - Gateway for H.320 or H.323 video calls
- Cisco VT Advantage client:
 - H.263-compliant
 - Interoperates with H.323
 - Requires Cisco IP Phones 7940, 7960, or 7970
- Video endpoints (SCCP) developed under Cisco license:
 - Emulates Cisco IP Phones 7960 (including softkeys, directory, XML services)
 - Available from TANDBERG
- H.323 endpoints:
 - Available from partners



© 2005 Cisco Systems, Inc. All rights reserved.

C IPT2 v4.1—2-4

The Cisco IP video telephony solution consists of products and solutions:

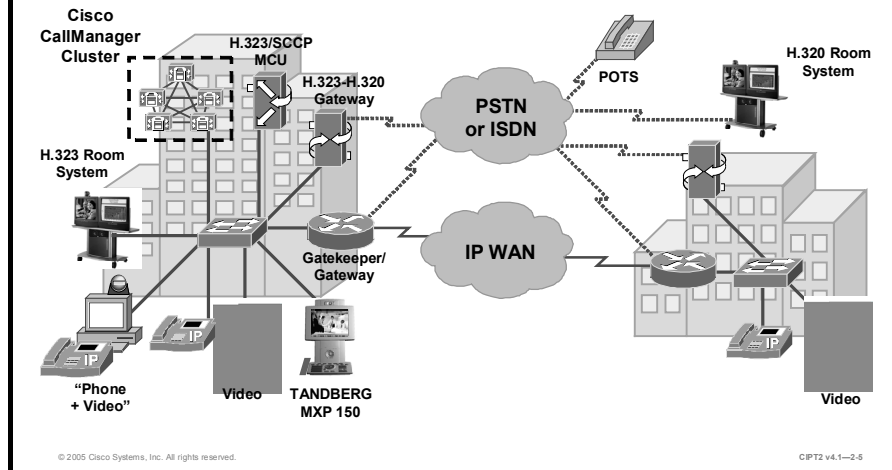
- Cisco CallManager Release 4.0 or later. Cisco CallManager is the call-routing intelligence and provides a single dial plan for voice and video devices.
- Cisco IP/VC 3500 Series Multipoint Control Units (MCUs) for both H.323 and Skinny Client Control Protocol (SCCP, or Skinny) conference calls. The MCUs are responsible for mixing the various video and voice streams in a videoconference. In a videoconference, all devices send their streams to the MCU; the MCU mixes these streams into a single picture and sends the mixed stream back to the endpoints. The Cisco IP/VC 3500 Series MCU can send streams in Continuous Presence mode to the endpoints if the MCU is extended with the Enhanced Media Processor (EMP). Continuous Presence mode enables an enhanced and simultaneous view of conference participants, with a choice of 26 different layouts
- Cisco IP/VC 3500 Series H.320 gateways interconnect the IP world with the ISDN world. To interconnect the H.323 with the H.320 (ISDN) world, a video gateway is required. Unlike a normal voice gateway, a video gateway is able to bond bearer channels (B channels). A video call needs at least 128 kbps, at lowest quality, in each direction; the default for an adequate video call is 384 kbps. For a 384-kbps call, the video gateway needs to open six ISDN B channels at the same time, which is called B-channel bonding. The IP/VC 3500 Series H.320 gateways support B-channel bonding. The IP/VC 3500 Series H.320 gateways require an H.323 gatekeeper to register.
- A Cisco IOS H.323 gatekeeper is required to register H.323 devices. The main tasks of an H.323 gatekeeper are endpoint registration, bandwidth management, and directory number (DN) resolution. Many video devices, such as H.323 MCUs or H320 video gateways, require an H.323 gatekeeper for registration.

- Cisco Video Telephony (VT) Advantage is a video telephony solution comprising the Cisco VT Advantage software application and Cisco VT Camera, a video telephony Universal Serial Bus (USB) camera. With the Cisco VT Camera attached to a PC colocated with a Cisco IP Phone, users can place and receive video calls on the enterprise IP telephony network. Users make calls from Cisco IP Phones using familiar telephone interfaces, but calls are enhanced with video on a PC, without requiring any extra button-pushing or mouse-clicking.
- TANDBERG SCCP endpoints are developed by the videoconference equipment vendor TANDBERG under Cisco license.
- The existing range of H.323-compliant products from vendors such as Polycom, TANDBERG, Sony, VCON, and VTEL Products. (Most H.323 video devices require a gatekeeper to register.)

Cisco CallManager Release 4.0 and later adds support for video in both the SCCP and H.323 protocols. Cisco CallManager can now manage H.323 endpoints, MCUs, and gateways, providing the system administrator with PBX-style control over all call routing and bandwidth management for those devices.

Video-Enabled IP Telephony: The Big Picture

Cisco.com



The video telephony solution consists of end-user devices, infrastructure, and applications.

The end-user devices include video phones, soft video phones for remote workers, and desktop environments that incorporate existing telephones and desktop computers. Additionally, the existing H.323 endpoints that the customers already own will become part of the video telephony environment.

Cisco CallManager is the center of the infrastructure and supports both voice and video telephony. Cisco CallManager provides a single dial plan for all endpoints; there is no need for an additional video dial plan. The same applications are still supported: voice mail, conferencing, and scheduling for audio and video resources are possible.

The video stream mixing is accomplished by the MCU. In a Cisco CallManager environment, the MCU can be SCCP or H.323 or SCCP- and H.323-controlled. The main difference is that the H.323-controlled MCU needs an H.323 gatekeeper to register. In both cases, the MCU features can be extended with EMP boards to support Continuous Presence and transcoding.

To allow external H.320 parties to participate in a videoconference, a video gateway, such as the Cisco IP/VC 3521 BRI Videoconferencing Gateway or IP/VC 3526 PRI Videoconferencing Gateway, is required. The normal voice gateways used in the Cisco CallManager environment do not support ISDN B-channel bonding and cannot route video calls from and to the public switched telephone network (PSTN).

Video Calls

This topic describes video call characteristics in terms of Real-Time Transport Protocol (RTP) stream types, the signaling protocols and codecs used, and the audio and video bandwidth requirements.

Video Calls

Cisco.com

Video call is like a telephone call:

- **Unified voice and video dial plans**
- **Calls can be made to H.323 or SCCP video and audio terminals**
- **Automatic codec, format, and bit-rate negotiation**
- **Single DN for voice and video**

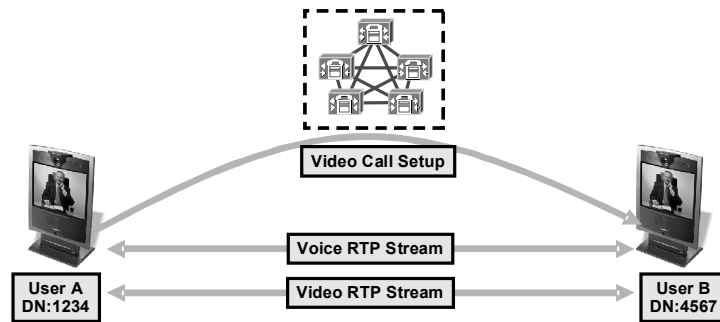
© 2005 Cisco Systems, Inc. All rights reserved. CIPT2 v4.1-2.6

Using video endpoints in the Cisco CallManager system is, from the perspective of a user, as easy as placing a telephone call. Video terminals can be either H.323- or SCCP-controlled and are able to communicate with each other regardless of the protocol controlling the device. All video devices use the same dial plan as all other devices in the Cisco CallManager system. For Cisco CallManager, video devices are treated like voice devices, with the same configuration options. For Cisco VT Camera, the same DN as the associated IP Phone is used. There is no additional number to remember to be able to reach someone over the video system. The video signaling is transparent to the user, and the devices negotiate their video capabilities, such as codec, format, and bit rate used for the video call, with no additional user action.

Cisco CallManager Video Calls

Cisco.com

- A video call is between two video-enabled endpoints.
- A videoconference is between more than two video-enabled endpoints.



© 2005 Cisco Systems, Inc. All rights reserved.

C IPT2 v4.1—2.7

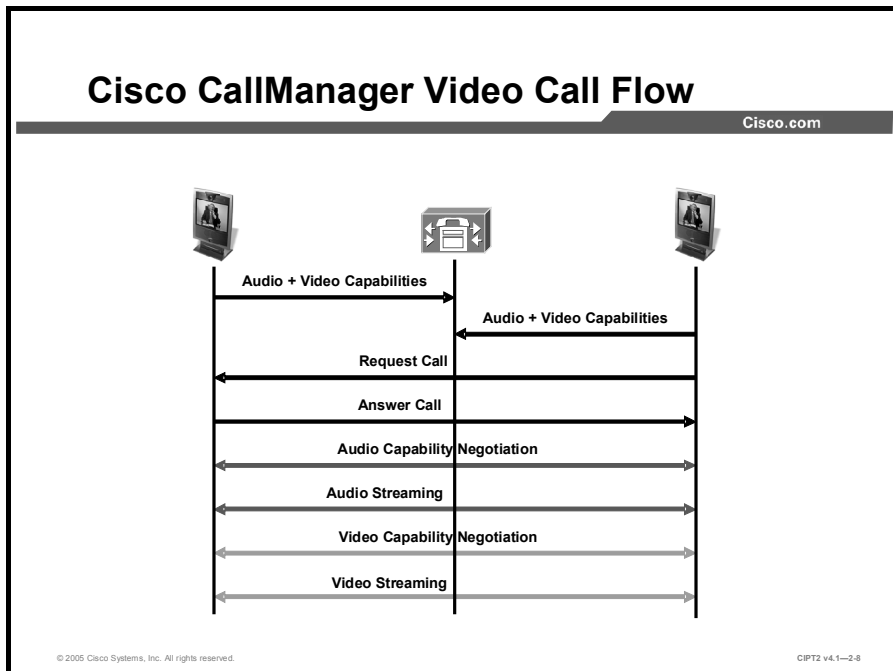
A video telephony call can be established between any two video-enabled endpoints. If one of the endpoints is not video-enabled, the call is set up as a normal voice call. When both endpoints are video-enabled, Cisco CallManager signals the voice and video capabilities to both endpoints, and the endpoints directly build two RTP streams, one for voice and one for video. Call control for video calls operates the same way as the call control that governs voice calls.

Note The term “video call” is sometimes confused with the term “videoconferencing.”
A videoconference is a video call with at least three participants.

For videoconferences in the Cisco CallManager system, extra hardware is required. The device that mixes the video streams is an MCU.

Cisco CallManager Video Call Flow

Cisco.com



The typical video call includes two or three RTP streams in each direction. In a basic video call, there are two unidirectional RTP streams for voice and two unidirectional RTP streams for video. The call can include these stream types:

- **Audio:** These are the same codecs as used in audio-only calls, G.711 and G.729, plus additional codecs, G.722 and G.728.
- **Video:** The video codecs used are H.261, H.263, H.264, and Cisco Wideband codecs. The video codec is a software module that enables the use of compression for digital video. There is a complex balance between the quality of the video, the video call rate, the complexity of the encoding and decoding algorithms, robustness to data losses and errors, ease of editing, random access, the state of the art of compression algorithm design, end-to-end delay, and a number of other factors.
- **Far-end camera control (FECC):** FECC is used only for H.323 devices and is optional. FECC enables a user to control the camera of the far side during an active video call. This feature must be supported by both video-enabled H.323 devices. When FECC is used, two more unidirectional RTP streams are sent between the video devices. The two additional RTP streams are used for the camera control parameters.

Example

The video-enabled endpoints report their video and audio capabilities to Cisco CallManager. Cisco CallManager now treats the endpoints simply as video phone devices. When a call is placed or received between two video-enabled devices, Cisco CallManager signals for both audio and video streams. First the audio capabilities, such as audio codec information and audio bit rate, are signaled and negotiated, and then the audio stream is set up. After the audio stream is set up, the video capabilities, such as video codec information and video channel bit rate, are negotiated, and the devices exchange their video streams separately from the audio. In this example, the video call has four RTP streams—two RTP streams for voice and two RTP streams for video transmission.

Cisco CallManager Supported Video Codecs

Cisco.com

Codec	Standard codecs: H.261, H.263+, H.264	Cisco proprietary codec: Cisco wideband
Supported Video Call Speed	128–1,544 kbps	7 Mbps
Resolution	CIF, QCIF, 4CIF, 16CIF, SQCIF	CIF
Frame Rate	15–30 fps	15–30 fps

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1—2-9

Cisco CallManager supports several standard video codecs and a Cisco proprietary video codec.

H.263 is a video codec specified by the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) as a low-bit-rate encoding solution for videoconferencing. It was first designed to be used in H.324-based systems (PSTN and other circuit-switched network video environments) but has since found use in these other solutions as well:

- H.323 (IP-based videoconferencing)
- H.320 (ISDN-based videoconferencing)
- Real-Time Streaming Protocol (RTSP)
- Session Initiation Protocol (SIP)

H.263 was developed as an evolutionary improvement based on experience with H.261, the previous ITU-T standard for video compression, and the Moving Picture Experts Group-1 (MPEG-1) and Moving Picture Experts Group-2 (MPEG-2) standards. The first version of H.263 was completed in 1995, and it provided a suitable replacement for H.261 at all bit rates. H.263 was further enhanced in H.263 version 2 (H.263v2, also known as H.263+ or H.263 1998) and H.263 version 3 (H.263v3, also known as H.263++ or H.263 2000).

The next enhanced codec specified by the ITU-T after H.263 is the H.264 standard. Because H.264 provides a significant improvement in capability beyond H.263, the H.263 standard is now considered primarily a legacy design (although this is a recent development). Most new videoconferencing products include H.261, H.263, and H.264 capabilities.

The video codecs supported by Cisco CallManager Release 4.1 include H.261, H.263, and H.264. These codecs exhibit the parameters and typical values listed in this table.

Video Codec Parameters

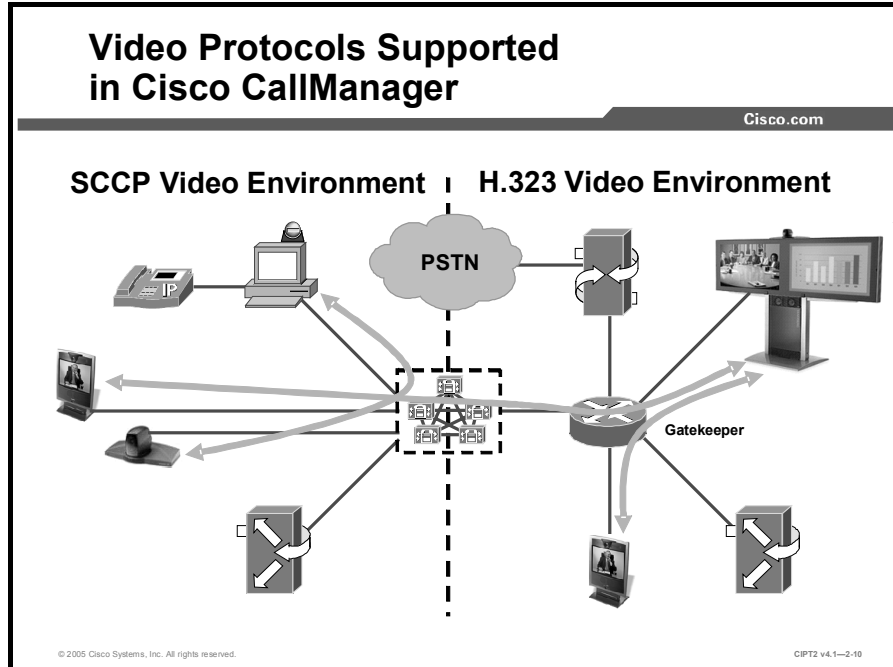
Parameter	Values
Video call speed	128 kbps, 384 kbps, 768 kbps, and 1.544 Mbps
Resolution	Common Intermediate Format (CIF); resolution of 352 x 288 pixels Quarter CIF (QCIF); resolution of 176 x 144 pixels 4CIF (resolution of 704 x 576 pixels) Sub QCIF (SQCIF); resolution of 128 x 96 pixels 16CIF (resolution of 1408 x 1152 pixels)
Frame rate	15 frames per second (fps) 30 fps

The Cisco wideband codec can be described as follows:

- Is a proprietary codec that is a fixed-bit-rate codec and runs on a PC that is linked to a phone
- Enables the PC to associate with a call that the phone receives
- Can only be used by the Cisco VT Camera

Video Protocols Supported in Cisco CallManager

This topic describes the various protocols supported by Cisco CallManager and explains their interworking and differences.



Cisco CallManager Release 4.0 added support for video in both SCCP and H.323 protocol. Calls can be made from SCCP client to SCCP client, between H.323 clients, and between SCCP and H.323 clients.

SCCP and H.323 Endpoint Characteristics

Cisco.com

SCCP Clients	H.323 Clients
Register with Cisco CallManager	Register with H.323 gatekeeper
Send dialed number digit by digit	Send entire dialed number at once
Are configured in Cisco CallManager Administration	Are configured through user interface
Advertise their capabilities when registering	Advertise their capabilities on a call-by-call basis
Offer PBX-style features	Offer basic call capabilities in interaction with Cisco CallManager

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-2-11

H.323 and SCCP endpoints have these characteristics:

- H.323 devices typically register with an H.323 gatekeeper (such as the Cisco IOS gatekeeper). The H.323 gatekeeper maintains the registration state of each endpoint, but it directs all call requests to Cisco CallManager. SCCP devices register directly with Cisco CallManager.
- H.323 devices send the complete dialed number all at once in their H.225 setup messages. SCCP devices send each dialed digit one by one as they are entered on the keypad. The difference is subtle but worth noting because it affects the experience of the user. Dialing on an H.323 device is much like dialing on a cell phone—the user enters the entire number and then presses the Call or Dial button to initiate the call. SCCP devices are more like a traditional telephone, in which the user goes off-hook, receives a dial tone from Cisco CallManager, and then starts dialing digits.
- H.323 devices are configured through the user interface of each endpoint. Changes to the configuration or software or firmware loads must be done locally on each endpoint (or, in some cases, through Simple Network Management Protocol [SNMP] or other vendor-specific management applications). SCCP devices are centrally controlled and configured in Cisco CallManager Administration. The configuration and software or firmware loads are then pushed to the endpoints via the TFTP. TANDBERG SCCP devices that receive their configurations via TFTP are the exception; however, software or firmware upgrades must be done manually (or through TANDBERG management applications).
- H.323 devices advertise their capabilities to Cisco CallManager on a call-by-call basis. SCCP devices advertise their capabilities when they register with Cisco CallManager and whenever their capabilities change. Cisco CallManager then decides, on a call-by-call basis, which types of media channels are negotiated between the endpoints.
- H.323 video devices offer basic call capabilities in interaction with Cisco CallManager. SCCP devices offer PBX-style features, such as hold, transfer, conference, park, pickup, and group pickup.

- For both types of endpoints, the signaling channels are routed through Cisco CallManager, but the media streams (audio and video channels) flow directly between the endpoints using RTP.
- H.323 and SCCP endpoints can call one another. Cisco CallManager provides the signaling translation between the two protocols and negotiates common media capabilities (common codecs).
- SCCP endpoints can invoke supplementary services, such as placing the call on hold, transferring the call, and conferencing with another party. H.323 devices that support receiving Empty Capability Set (ECS) messages may be the recipients of such features (that is, they may be placed on hold, transferred, or conferenced), but they cannot invoke those features.
- H.323-to-SCCP calls are not the only types of calls allowed by Cisco CallManager. Any device can call any other device, but video calls are supported only on SCCP and H.323 devices. Specifically, video is not supported in these protocols in Cisco CallManager Release 4.1:
 - Computer telephony integration (CTI) applications (Telephony Application Programming Interface [TAPI] and Java TAPI [JTAPI])
 - Media Gateway Control Protocol (MGCP)
 - SIP

SCCP Video Call Characteristics

Cisco.com

- **SCCP video devices report video capabilities to Cisco CallManager.**
- **Cisco CallManager system administration determines video call bandwidth control.**
- **Supports H.261, H.263+, H.264 and Cisco wideband video codec.**
- **Supports G.711, G.723.1, G.728, G.729, G.722, Cisco wideband audio codec, and GSM.**
- **Out-of-band dual-tone multifrequency (DTMF).**

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-2-12

SCCP video exhibits these characteristics:

- If a call is placed from an SCCP phone that reported video capabilities to Cisco CallManager and the other end supports video as well (another SCCP phone with video capabilities or an H.323 device), Cisco CallManager automatically signals the call as a video call.
- For SCCP video calls, system administration determines video call bandwidth by using regions. The system does not ask users for bit rate.
- In Cisco CallManager Release 4.1, H.264 support was added for SCCP video devices. H.264 contains a number of features that allow it to compress video much more effectively than older codecs. This capability allows H.264 to deliver better video call quality over less bandwidth. Cisco CallManager supports the H.261 and H.263+ codecs as well.
- Cisco CallManager Release 4.1 supports the audio codecs G.711, G.722, G.723.1, G.728, G.729, Cisco wideband codec, and Global System for Mobile Communications (GSM).
- The wideband video codec of Cisco VT Camera reduces PC CPU utilization, unlike the resource-intensive H.263 and H.264 codecs. The Cisco wideband codec is used primarily in LAN, not over WAN links.
- Cisco CallManager uses out-of-band H.245 alphanumeric dual-tone multifrequency (DTMF). DTMF may not work between SCCP and third-party H.323 devices, because many H.323 devices pass DTMF in-band.

H.323 Video Call Characteristics

Cisco.com

- **Call forwarding, dial plan, and other call routing-related features work with H.323 endpoints.**
- **H.323 video endpoints can be configured as H.323 phones, H.323 gateways, or H.323 trunks.**
- **Trunk interaction with H.323 clients has functions that are identical for audio and video calls.**
- **Neither video MTPs nor video transcoders exist currently.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-2-13

H.323 video exhibits these characteristics:

- Call forwarding, dial plan, and other call routing-related features work with H.323 endpoints. Cisco CallManager remains the central call-routing intelligence.
- In Cisco CallManager, H.323 endpoints can be configured as H.323 telephones, H.323 gateways, or H.323 trunks. Many H.323 devices request a gatekeeper for registration.
- Some vendors implement call setup such that they cannot increase the bandwidth of a call when the call is transferred or redirected. In such cases, if the initial call is audio, users may not receive video when they are transferred to a video endpoint.
- Video H.323 clients that use trunks to other Cisco CallManager systems or other H.323 systems can use the same features as audio-only H.323 clients.
- Currently, neither video media termination points (MTPs) nor video transcoders exist. If an audio transcoder or MTP is required for a call, that call will be audio only.

H.323 Video Call Characteristics (Cont.)

Cisco.com

- **H.323 video endpoints cannot initiate hold, resume, transfer, park, and other similar features.**
- **If an H.323 device supports ECS, the device can be set on hold, park, and so on.**
- **Supports H.323 dynamic E.164 alias addressing.**
- **Supports H.261 and H.263.**
- **Supports G.711, G.723.1, G.728, G.729, and G.722.**
- **FECC.**
- **Out-of-band DTMF (H.245 alphanumeric).**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-2-14

H.323 video exhibits these additional characteristics:

- H.323 video endpoints cannot initiate hold, resume, transfer, park, or offer other similar features. Only if an H.323 endpoint supports ECS can the endpoint be held, parked, and so on.
- Dynamic H.323 addressing within Cisco CallManager provides a facility to register H.323 video terminals on Cisco CallManager when the video terminal receives its IP address through a Dynamic Host Configuration Protocol (DHCP) server. Endpoints are tracked based on their E.164 address registration with an adjacent video gatekeeper. The E.164 address is a static identifier that remains constant from the perspective of both gatekeeper and Cisco CallManager. The feature became available with Cisco CallManager Release 4.1. To move to a converged voice and video dial plan, it is highly desirable that Cisco CallManager become the entity that manages call routing and digit manipulation for both the voice and video endpoints, regardless of call-signaling protocol. Earlier releases of Cisco CallManager required that an H.323 video terminal be configured on Cisco CallManager based on static IP address information. As a support and mobility issue, this design could not facilitate a scalable method for endpoint management because configuration information was accurate only as long as the DHCP lease did not expire with the endpoint in question.
- Cisco CallManager Release 4.1 supports H.261 and H.263; H.264 is supported only for SCCP endpoints.
- H.323 video clients support the voice codecs G.711, G.722, G.723.1, G.728, and G.729.
- FECC enables a user to control the camera of the far side during an active video call. For FECC, a separate RTP stream is set up. This feature was introduced in H.323 version 5 (H.323v5) as Annex Q.

- Cisco CallManager uses out-of-band H.245 alphanumeric DTMF. DTMF may not work because many H.323 devices pass DTMF in-band. If an H.323 device uses in-band DTMF signaling, Cisco CallManager will not convert it to out-of-band signaling, and the DTMF signaling will fail. Both sides need to use a common scheme; either both devices need to use out-of-band signaling or the H.323 device needs to support both methods and autodetect the method to use.

SCCP vs. H.323 in Cisco CallManager

Cisco.com

The features supported in a video call depend on the signaling protocol used.

	SCCP	H.323
Call Features (Hold, Park, Transfer)	Yes	Yes (only passive, with H.323 endpoints supporting ECS)
Videoconferencing	MCU required	MCU required
H.320 Interworking	H.323 video gateway required	H.323 video gateway required
FECC	N/A	Yes
DTMF	Yes (out-of-band)	Yes (out-of-band)
Mid-Call Video	Yes	Yes (only if H.323 supports request in active call)

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1—2-15

The call-related features of the Cisco IP video telephony integration strongly depend on the protocol in use. FECC, for example, is an H.323 feature supported only by H.323 devices and is not available on SCCP devices.

Videoconferencing in general requires an MCU. The Cisco IP/VC 3540 MCU supports both protocol stacks: H.323 and SCCP. This can be configured in the MCU Administration window.

The Cisco IP/VC 3521 and 3526 videoconferencing gateways bridge the gap between the installed base of ISDN videoconferencing group and room systems and IP-based H.323 systems. The gateways connect H.320 video systems on ISDN to H.323 systems on IP by translating calls initiated from the PSTN to their equivalent on the packet network, and vice versa.

To enable SCCP to call H.320 endpoints, an H.323-based video gateway is necessary as well.

Cisco CallManager uses out-of-band signaling for DTMF. If an H.323 device uses in-band DTMF signaling, Cisco CallManager will not convert it to out-of-band signaling; therefore, the DTMF signaling will fail. Both sides need to use a common scheme—either both need to use out-of-band signaling or the H.323 device needs to support both methods and autodetect which method to use.

Beginning in Cisco CallManager Release 4.1, mid-call video is supported. Mid-call video allows an active voice call to become a video call if the video capabilities are added during the active call (for instance, if the Cisco VT Advantage software is turned on). Cisco VT Advantage will then associate with the phone and try to set up a video stream:

- If both parties are SCCP video endpoints, the call immediately becomes a video call.
- If the other party is an H.323 endpoint, the SCCP endpoint tries to request a video channel. If the H.323 endpoint rejects the incoming channel or does not open a channel, the call becomes either one-way video or audio only.

Bandwidth Management

This topic describes the two main factors that determine the bandwidth requirement for video calls and explains how to calculate video bandwidth requirements.

Bandwidth Management

Cisco.com

- **Bandwidth management is important in the packet-switched network to ensure the quality of each voice and video call.**
- **Bandwidth calculation considerations:**
 - **Video call speed is the sum of audio and video channels.**
 - **Video call bandwidth consists of video call speed and packetization overhead:**
 - **Actual bandwidth required on the link**

© 2005 Cisco Systems, Inc. All rights reserved.C IPT2 v4.1-2-16

Bandwidth management with Cisco CallManager call admission control enables you to control the audio and video quality of calls over a WAN link by limiting the number of calls that are allowed on that link simultaneously.

In a packet-switched network, audio and video quality can begin to degrade when a link carries too many active calls and the bandwidth is oversubscribed. Call admission control regulates audio and video quality by limiting the number of calls that can be active on a particular link at the same time. Call admission control does not guarantee a particular level of audio or video quality on the link, but it does allow you to regulate the amount of bandwidth that active calls on the link consume.

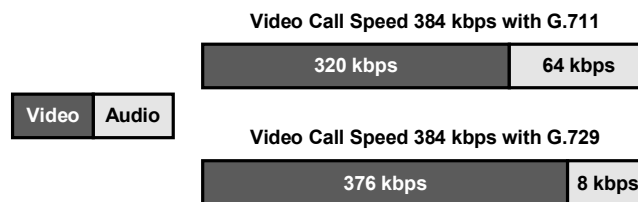
The actual bandwidth required is more than just the speed of the video call. The speed of the video call is just the payload, but the final packet also includes some amount of overhead for header information that encapsulates the payload into RTP segments, User Datagram Protocol (UDP) frames, IP packets, and finally a Layer 2 transport medium (such as Ethernet frames, ATM cells, or Frame Relay frames).

Note	References to the video call bandwidth include the sum of the video call speed and all packetization[0] overhead (RTP, UDP, IP, and Layer 2).
-------------	---

Video Call Bandwidth Requirement

Cisco.com

- Video call includes two channels:
 - Audio channel
 - Video channel
- The bit rate available for the video channel depends on the negotiated audio codec and the overall video call speed.



© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-2-17

The Media Channels of a Video Call

A typical video call consists of two media channels: one for the video stream and one for the audio stream. These channels are referred to as logical channels in the H.323 protocol, and each logical channel is negotiated separately. For the call to succeed, Cisco CallManager checks that audio is successfully signaled; if video cannot be negotiated, the call will be an audio-only call.

The audio channel consists of the actual audio bit rate. This bit rate is dictated by the audio codec in use. In the case of a G.711 codec, the bit rate is 64 kbps, while in the case of a G.729 codec, it is 8 kbps. For an audio channel, only the pure audio data is considered, not the packetization overhead.

The bit rate available for the video channel depends on the negotiated audio codec and the video call speed. The video channel bit rate is the speed of the video call minus the bit rate of the codec used for the audio channel. In the case of a 384-kbps video call with an audio channel that uses G.711, the bit rate left for the video channel is 320 kbps (384 kbps minus 64 kbps). In the case of an audio channel using the G.729 codec, the payload of the same video call (384 kbps) leaves 376 kbps for the video channel (384 kbps minus 8 kbps).

This table lists possible video call speeds, their possible audio channel codecs, and the associated video channel bit rates.

Video Call Speeds and the Associated Audio and Video Codecs

Video Call Speed	Audio Codec and Rate	Video Codec and Rate
128 kbps	G.711 at 64 kbps	H.261 or H.263 at 64 kbps
128 kbps	G.729 at 8 kbps	H.261 or H.263 at 120 kbps
128 kbps	G.728 at 16 kbps	H.261 or H.263 at 112 kbps
384 kbps	G.729 at 8 kbps	H.261 or H.263 at 376 kbps
384 kbps	G.711 at 64 kbps	H.261 or H.263 at 320 kbps

Video Call Speed	Audio Codec and Rate	Video Codec and Rate
768 kbps	G.729 at 8 kbps	H.261 or H.263 at 760 kbps
768 kbps	G.711 at 64 kbps	H.261 or H.263 at 704 kbps
1.472 Mbps	G.729 at 8 kbps	H.261 or H.263 at 1.464 Mbps
1.472 Mbps	G.711 at 64 kbps	H.261 or H.263 at 1.408 Mbps
7 Mbps	G.729 at 8 kbps	Wideband at 7 Mbps (minus 8 kbps for the audio stream)
7 Mbps	G.711 at 64 kbps	Wideband at 7 Mbps (minus 64 kbps for the audio stream)

Example

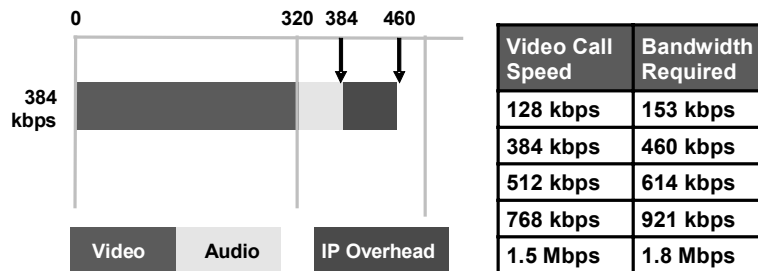
A 384-kbps video call may be G.711 at 64 kbps (for audio) plus 320 kbps (for video). If the audio codec for a video call is G.729 (at 8 kbps), the video rate increases to maintain a total bandwidth of 384 kbps. If the call involves an H.323 endpoint, the H.323 endpoint may use less than the total video bandwidth that is available. An H.323 endpoint may always choose to send at less than the maximum bit rate for the call.

Note None of these values include packetization overhead.

Calculating the Total Bandwidth

Cisco.com

To calculate the total bandwidth of a video call, including Layer 3 and Layer 2 overhead, add about 20 percent to the speed of the video call.



© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-2-18

The two main factors that influence bandwidth requirements for video calls are the media channels and the bandwidth used per call.

Actual Bandwidth Used Per Video Call

To calculate the exact overhead ratio for video, it is recommended that you add about 20 percent to the video call speed regardless of which type of Layer 2 medium the packets are traversing. The additional 20 percent gives plenty of headroom to allow for the differences among Ethernet, ATM, Frame Relay, PPP, High-Level Data Link Control (HDLC), and other transport protocols and also some cushion for the bursty nature of video traffic.

Here are the key factors for calculating the actual bandwidth that is required for a video call:

- A video call consists of the audio channel and the video channel.
- The speed of a video call does not include any packetization overhead.
- For the actual bandwidth required for a video call, add 20 percent to the speed of the video call.

The table shows the recommended bandwidth values to use for some of the more popular video call speeds, incorporating this 20 percent margin.

Video Call Speed and Actual Bandwidth Requirements

Video Call Speed Requested by Endpoint	Actual Bandwidth Required on the Link
128 kbps	153.6 kbps
256 kbps	307.2 kbps
384 kbps	460.8 kbps
512 kbps	614.4 kbps
768 kbps	921.6 kbps
1.5 Mbps	1.766 Mbps
7 Mbps	8.4 Mbps

Call Admission Control Settings in Cisco CallManager

Cisco.com

	Cisco CallManager Region	Cisco CallManager Location	H.323 Gatekeeper
Audio-Only Call Configuration	Audio codec only	Audio codec bit rate + Layer 3 overhead	Twice the audio codec bit rate
Example: G.711 Call	G.711	80 kbps	128 kbps
Video Call Configuration	Audio codec and video call speed	Video call speed	Twice the video call speed
Example: 384-kbps Video Call	G.711 and 384 kbps	384 kbps	768 kbps

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-2-19

Enter the proper bandwidth information on Cisco CallManager.

- The location settings for call admission control have also been enhanced, compared to earlier Cisco CallManager releases not supporting video, to provide for accounting of video bandwidth on a per-call and aggregate basis.
- The location setting for call admission control defines the overall bandwidth allowed for all video calls to a certain location. That is the video call speed for all video calls. To allow five video calls with a bandwidth of 384 kbps for each video call (defined in the Cisco CallManager regions), the value to enter in the Cisco CallManager location is 1920 kbps.
- For video calls, the negotiated bandwidth for a video-enabled device typically includes both audio and video; for example, a 384-kbps video call comprises 64-kbps audio and 320-kbps video channels.
- For voice-only calls, the region uses the same setting that is used for the audio channel in video calls. The negotiated bandwidth for an IP telephony device includes the “real” audio bandwidth including IP overhead; for example, a G.711 64-kbps audio call uses 80 kbps, and this value has to be entered in the Cisco CallManager region.

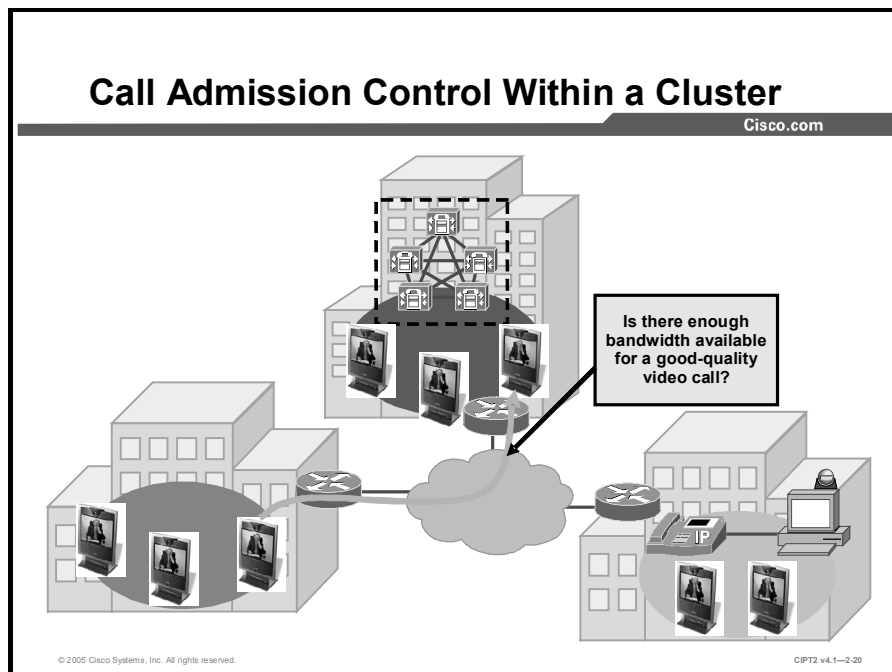
Enter the proper bandwidth information on an H.323 gatekeeper.

- The H.323 specification dictates that the bandwidth values must be entered as twice the call bit rate. For example, a 384-kbps video call would be entered as 768 kbps in the gatekeeper.
- A G.711 audio-only call would be entered as 128 kbps in the gatekeeper.

Note Call admission control behavior changed in Cisco CallManager Release 3.2(2)c and Cisco IOS Software Release 12.2(2)XA. Before that release, Cisco CallManager asked for bit rate plus Layer 3 overhead, and Cisco IOS gateways asked for 64 kbps, regardless of the type of call.

Call Admission Control Within a Cluster

This topic describes how to implement call admission control for video calls within a cluster using the locations and regions features of Cisco CallManager.

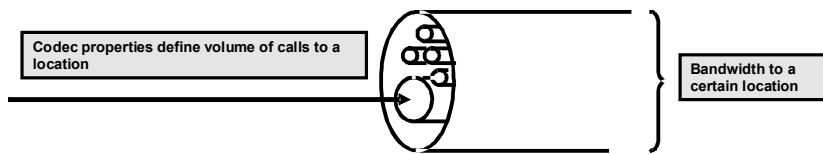


Why do you need to configure call admission control for video calls? The answer to this question is quite simple. If you do not control the number of video and voice calls over your WAN links, periodically you will see decreased video and voice throughout the whole system. With call admission control, you control the number of calls on the WAN link and ensure that all calls, video and audio-only, are processed throughout the network with acceptable quality.

Call Admission Control Within a Cluster (Cont.)

Cisco.com

- **Regions**
 - The Cisco CallManager region specifies the maximum bandwidth used by a call:
 - Between Cisco CallManager regions
 - Within a Cisco CallManager region
- **Locations**
 - The location defines the maximum bandwidth to and from a location.
 - The number of permitted calls depends on the settings of the region (bandwidth per call).



Cisco CallManager uses regions and locations to implement call admission control:

- Regions define the maximum bandwidth allowed per call. This value is configurable for calls within each region and for calls between any pair of regions.
- Locations define the maximum bandwidth allowed for all calls to and from a location.

In Cisco CallManager, devices derive their region setting with the associated device pool configuration. Locations are configured on a per-device basis.

Note Calls between devices at the same location do not need call admission control because the assumption is that these devices reside on the same LAN that has “unlimited” available bandwidth. However, for calls between devices at different locations, the assumption is that there is an IP WAN link in between that has limited available bandwidth.

Regions

Cisco.com

- **Audio Codec:**
 - Specifies the audio codec with the highest allowed codec bit rate
 - Applies to audio channels of audio and video calls
- **Video Call Bandwidth:**
 - Specifies the maximum video call speed (without overhead)
- **For video calls between different vendors, G.711 might be the only common audio codec.**

Region: San Jose
Status: Update completed
Update Delete Restart Devices

Region Information
Region Name* San Jose

Call Information
The maximum audio codec/video bandwidth supported within this region and between 2 other regions are:

Region	Audio Codec	Video Call Bandwidth
Dallas	G.711	<input type="radio"/> None <input checked="" type="radio"/> 384 kbps
San Francisco	G.729	<input type="radio"/> None <input checked="" type="radio"/> 128 kbps
San Jose (Within this Region)	G.711	<input type="radio"/> None <input checked="" type="radio"/> 768 kbps

Items per page: 10 First Previous Next Last Page 1 of 1
* indicates required item

Affects which audio codec is used for video calls as well

When you are configuring a region, you set two fields in Cisco CallManager Administration: the Audio Codec and the Video Call Bandwidth fields. Note that the audio setting specifies a codec type, while the video setting specifies the bandwidth that you want to allow. However, even though the notation is different, the Audio Codec and Video Call Bandwidth fields actually perform similar functions. The Audio Codec value defines the maximum bit rate allowed for audio-only calls and for the audio channel in video calls.

For instance, if you set the Audio Codec value for a region to G.711, Cisco CallManager allocates 64 kbps as the maximum bandwidth allowed for the audio channel for that region. In this case, Cisco CallManager permits calls using G.711, G.728, or G.729. However, if you set the Audio Codec value to G.729, Cisco CallManager allocates only 8 kbps as the maximum bandwidth allowed for the audio channel; in addition, Cisco CallManager permits calls using only G.729, because G.711, G.722, and G.728 all require more than 8 kbps.

The Video Call Bandwidth value defines the maximum bit rate for the video call, that is, the bit rate of the voice and video channels. For instance, if you want to allow video calls at a speed of 384 kbps using G.711 audio, you would set the Video Call Bandwidth value to 384 kbps and the Audio Codec value to G.711. The bit rate that would be used by the video channel thus would be 320 kbps.

If the Video Bandwidth value is set to None for the region, Cisco CallManager will either terminate the call or allow the call to pass as an audio-only call, depending on whether the called device has the Retry Video Call as Audio option enabled.

In summary, the Audio Codec field defines the maximum bit rate used for the audio channel of audio-only calls and for the audio channel of video calls, while the Video Call Bandwidth field defines the maximum bit rate allowed for video calls and includes the audio portion of the video call.

Note Video endpoints typically support only G.711 and G.722, while audio-only endpoints typically support only G.711 and G.729. Because you cannot configure the audio codec for audio and video calls separately, often the only common audio codec for mixed environments is G.711.

Locations

Cisco.com

Audio bandwidth settings apply to audio-only calls, not to video calls:

Specify audio codec bit rate plus Layer 3 overhead

Video bandwidth setting applies to video calls only:

Bit rate is video call speed

The screenshot shows the Cisco CallManager Administration interface for the 'Location Configuration' page. The page title is 'Location Configuration' and the location is 'San Francisco'. The status is 'Update completed'. There are buttons for 'Copy', 'Update', 'Delete', and 'Resync Bandwidth'. The 'Location Information' section shows 'Location Name*' as 'San Francisco'. The 'Audio Calls Information' section shows 'Audio Bandwidth*' with radio buttons for 'Unlimited', '48', and 'kbps'. A note below states: 'If the audio quality is poor or choppy, lower the bandwidth setting. For ISDN use multiples of 56 kbps or 64 kbps.' The 'Video Calls Information' section shows 'Video Bandwidth*' with radio buttons for 'None', 'Unlimited', and '128 kbps'. A note below states: '* indicates required item'. Navigation links include 'Add a New Location', 'Back to Find Locations', and 'Dependency Records'.

When configuring locations, you also set two fields in Cisco CallManager Administration: the Audio Bandwidth and the Video Bandwidth values. Unlike regions, however, audio bandwidth for locations applies only to audio-only calls, while video bandwidth again applies to the video call (that is, audio and video channels).

Note The audio and video bandwidth are kept separate, because if both types of calls shared a single allocation of bandwidth, it is very likely that audio calls would take all of the available bandwidth and leave no room for any video calls, or vice versa.

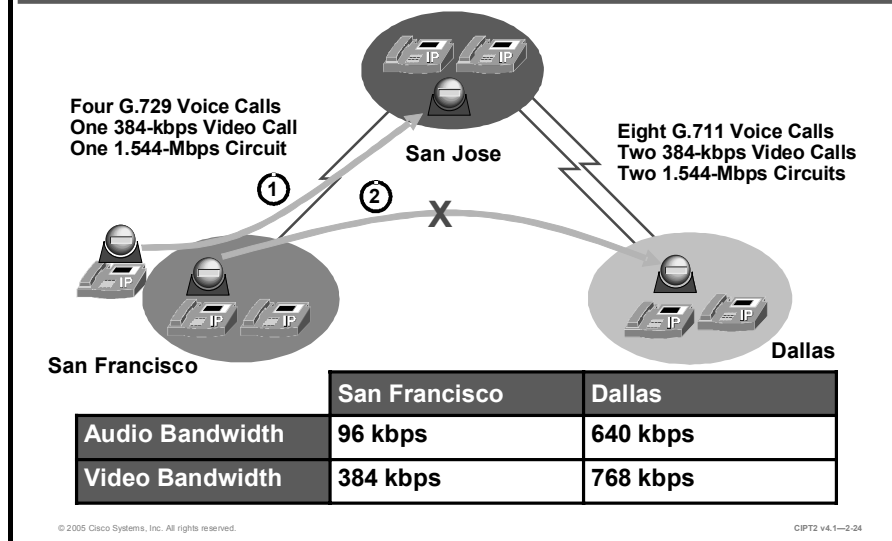
Both the Audio Bandwidth and the Video Bandwidth fields offer three options: None, Unlimited, or a field that accepts numeric values. However, the values entered in these fields use two different calculation models:

- For the Audio Bandwidth field, the value entered has to include the Layer 3 overhead required for the call. For instance, if you want to permit a single G.729 call to or from a location, you would enter the value 24 kbps. For a G.711 call, you would enter the value 80 kbps. The payload of a G.711 voice call is 64 kbps; the 80-kbps value is the 64-kbps payload plus 16-kbps RPT plus UDP plus IP plus Layer 2 overhead.
- The value in the Video Bandwidth field, by contrast, is entered without any overhead. For instance, for a 128-kbps call, enter the value 128 kbps; for a 384-kbps call, enter the value 384 kbps. As with the values used in the Video Bandwidth field for regions, it is recommended that you always use increments of 56 kbps or 64 kbps for the Video Bandwidth field for locations.

Note The value None in the Video Bandwidth field indicates that video calls are not allowed between this location and other locations. Video calls can, however, be placed within this location.

Video Call Bandwidth Example: Locations

Cisco.com



This figure illustrates an example of audio and video bandwidth requirements for a company with a three-site network. The San Francisco location has a 1.544-Mbps T1 circuit connecting it to the San Jose main campus. The system administrator wants to allow four G.729 voice calls and one 384-kbps video call to or from that location.

The Dallas location has two 1.544-Mbps T1 circuits connecting it to the San Jose main campus, and the administrator wants to allow eight G.711 voice calls and two 384-kbps video calls to or from that location.

For this example, the administrator would set the San Francisco and Dallas locations to the values in the table.

Bandwidth Example

Location	Number of Audio Calls Desired	Audio Bandwidth Field Value	Number of Video Calls Desired	Video Bandwidth Field Value
San Francisco	Four using G.729	96 kbps (4 * 24 kbps)	One at 384 kbps	384 kbps
Dallas	Eight using G.711	640 kbps (8 * 80 kbps)	Two at 384 kbps	768 kbps

First, a video device in San Francisco calls a video device in San Jose. Call admission control allows exactly one 384-kbps video call between San Francisco and any other location. The video call is active.

Next, another video device from San Francisco tries to set up a video call to a video device in Dallas. Call admission control does not allow a second video call from San Francisco to any other location and denies the video call.

If the call fails because of insufficient location bandwidth, it will not be retried with lower-bit-rate codecs. In this scenario, with no further configuration of the Cisco CallManager, the call will be rejected.

Retry Video Call as Audio

Cisco.com

- When Cisco CallManager detects insufficient bandwidth for a video call, it can retry the call as audio only.
- Retry Video Call as Audio is configurable on:
 - Cisco IP Phone 7940, 7960, and 7970
 - H.323 devices
 - H.323 gateways (IP/VC)
 - Gatekeeper-controlled trunks
 - H.225 trunks

Phone Configuration

Device Information

MAC Address: 001523D3F1E5

Description: faulhaber

Owner User ID: [empty]

Device Pool: STA LAN

Calling Search Space: <None>

AAR Calling Search Space: <None>

Media Resource Group List: <None>

User Hold Audio Source: <None>

Network Hold Audio Source: <None>

Location: Blenheim

User Locale: <None>

Network Locale: <None>

Device Security Mode: Use System Default

Signal Packet Capture Mode: None

Packet Capture Duration: 60

Built In Bridge: Default

Privacy:

Retry Video Call as Audio

The Retry Video Call as Audio setting appears as a check box in Cisco CallManager Administration. This setting is enabled by default on all device types and applies to these scenarios only:

- The region is configured not to allow video.
- The location is configured not to allow video, or the requested video speed exceeds the available video bandwidth for that location.
- The requested video speed exceeds the zone bandwidth limits of the gatekeeper.

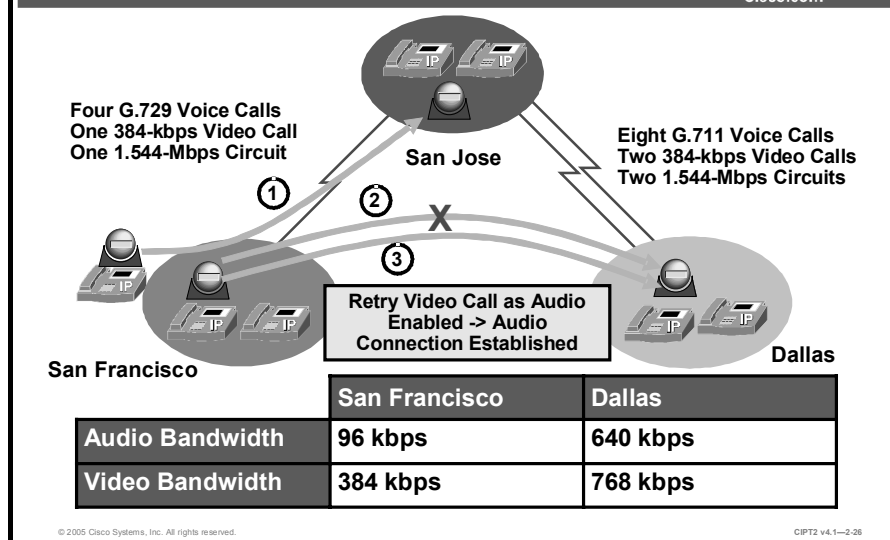
When this option is activated (checked), if there is not enough bandwidth to reach the device (for example, if the Cisco CallManager regions or locations do not allow video for that call), Cisco CallManager will retry the call as an audio-only call. When this option is deactivated (unchecked), Cisco CallManager will not retry the call as audio only but will instead either reject the call or reroute the video call by whatever automated alternate routing (AAR) path is configured.

The Retry Video Call as Audio option takes effect only on the terminating (called) device, allowing flexibility for the calling device to have different options (retry or AAR) for different destinations.

Note The called device determines the result. In other words, when one device calls another and any of the discussed insufficient bandwidth conditions applies, Cisco CallManager looks at the destination device to see whether the Retry Video Call as Audio option is enabled.

Video Call Bandwidth Example: Retry Video Call as Audio

Cisco.com



This figure illustrates an example of video bandwidth requirements for a company with a three-site network. The San Francisco location has a 1.544-Mbps T1 circuit connecting it to the San Jose main campus. The system administrator wants to allow four G.729 voice calls and one 384-kbps video call to or from that location.

For this example, the administrator would set the San Francisco and Dallas locations to the values shown in the table.

Bandwidth Example

Location	Number of Audio Calls Desired	Audio Bandwidth Field Value	Number of Video Calls Desired	Video Bandwidth Field Value
San Francisco	Four using G.729	96 kbps (4 * 24 kbps)	One at 384 kbps	384 kbps
Dallas	Eight using G.711	640 kbps (8 * 80 kbps)	Two at 384 kbps	768 kbps

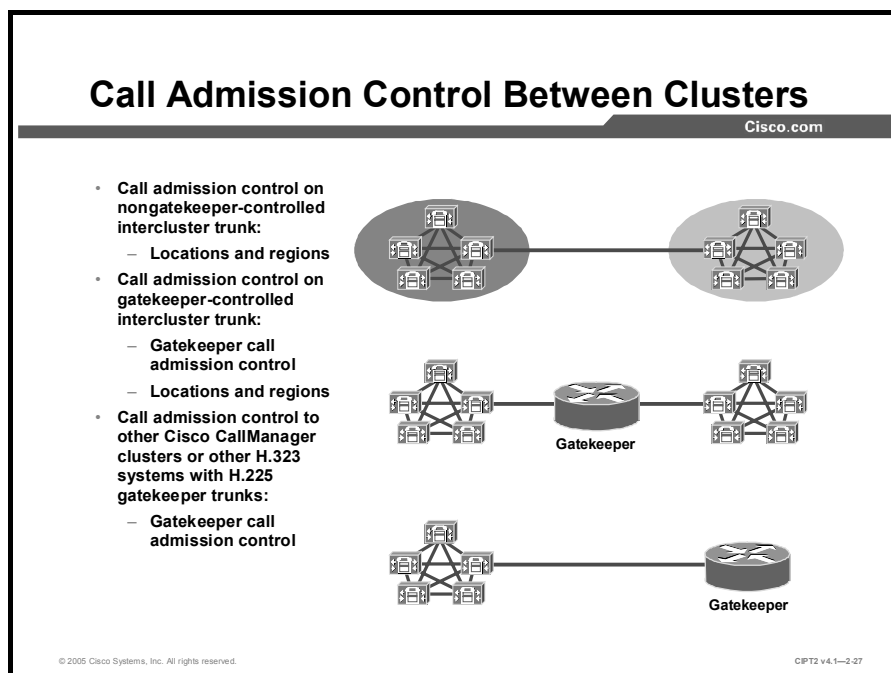
First, a video device in San Francisco calls a video device in San Jose. Call admission control allows exactly one 384-kbps video call between San Francisco and any other location. The video call is active.

Next, another video device from San Francisco tries to set up a video call to a video device in Dallas. Call admission control does not allow a second video call from San Francisco to any other location and denies the video call.

The improvement made in this scenario is that the video endpoints have the Retry Video Call as Audio feature enabled in Cisco CallManager. Enabling this feature requires checking the appropriate check box in the device configuration windows. In this scenario, with Retry Video Call as Audio configured on both Cisco IP Phones, the second (unsuccessful) video call will be retried as an audio-only call (independent of the direction of the call). This retry applies only if there is enough bandwidth configured on the location settings to process the call as audio only.

Call Admission Control Between Clusters

This topic describes how to configure call admission control for video calls between clusters.



Calls between Cisco CallManager clusters use intercluster trunks. Cisco CallManager Release 4.1 supports these types of trunks:

- **Nongatekeeper-controlled intercluster trunks:** This trunk type is specifically designed for communications between Cisco CallManager clusters and should not be used with other types of H.323 devices. The name implies that there is no gatekeeper between the clusters to regulate the bandwidth used between them. Therefore, the only way to provide call admission control for this type of trunk is by using Cisco CallManager locations. To have Cisco CallManager control call admission control, the intercluster trunk has to be in a separate Cisco CallManager location than the devices that use the intercluster trunk.
- **Gatekeeper-controlled intercluster trunks:** This trunk type is specifically designed for communications between Cisco CallManager clusters and should not be used to register other H.323 endpoints or devices. The name implies that there is a gatekeeper between the clusters to regulate the bandwidth used between them. To provide call admission control, you configure an H.323 zone in the gatekeeper for each of the Cisco CallManager clusters and assign zone bandwidth limits to each zone. If the gatekeeper-controlled intercluster trunk is not in the same location as the devices, the location settings need to be reconsidered. A device will need to get its call admission control permissions first from Cisco CallManager, because the device is in a different location than the trunk, and call admission control will be carried out at the gatekeeper.
- **H.225 gatekeeper-controlled trunks:** The H.225 gatekeeper-controlled trunk is designed for use with any H.323 device other than a Cisco CallManager cluster. In an H.225 gatekeeper-controlled trunk scenario, only the gatekeeper has control over call admission.

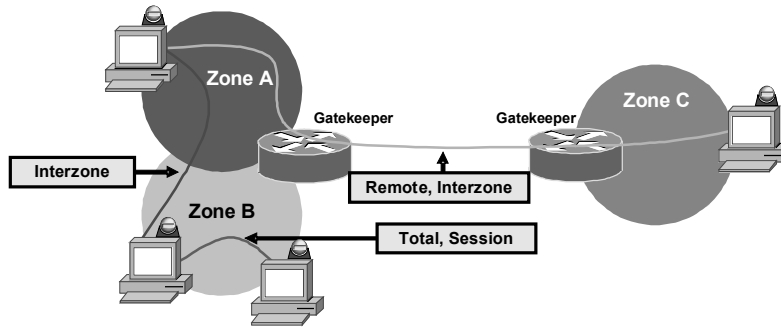
- **SIP trunks:** SIP trunks are designed for use with any SIP device, including other Cisco CallManager clusters, either directly or via a Cisco SIP Proxy Server.

Note Because Cisco CallManager Release 4.1 does not support video over the SIP protocol, this lesson does not cover SIP trunks.

Gatekeeper Call Admission Control Options

Cisco.com

- Gatekeeper call admission control is based on zones:
 - Local and remote zones
- Different options to limit the bandwidth:
 - Interzone, remote, total, session



© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-2-28

H.323 gatekeepers are hierarchical in nature. A gatekeeper can have one or more local zones. Using multiple zones allows you to group the devices that use the gatekeeper and gives better call admission control options (intrazone and interzone limitations). Zones that are served by another gatekeeper are called *remote zones*. These zones can be configured with different call admission control settings as well.

The Cisco gatekeeper may reject calls from an endpoint because of bandwidth limitations. Rejection may occur if the gatekeeper determines that the bandwidth available on the network is not sufficient to support the call. This function also operates during an active call when a terminal requests additional bandwidth or reports a change in bandwidth used for the call.

The Cisco gatekeeper maintains a record of all active calls so that it can manage the bandwidth resources in its zones.

When an endpoint or gateway is configured to use an H.323 gatekeeper, it first sends an admission request (ARQ) to the gatekeeper. The gatekeeper checks whether there is bandwidth available. If the available bandwidth is sufficient for the call, an admission confirmation (ACF) is returned, otherwise an admission rejection (ARJ) is returned.

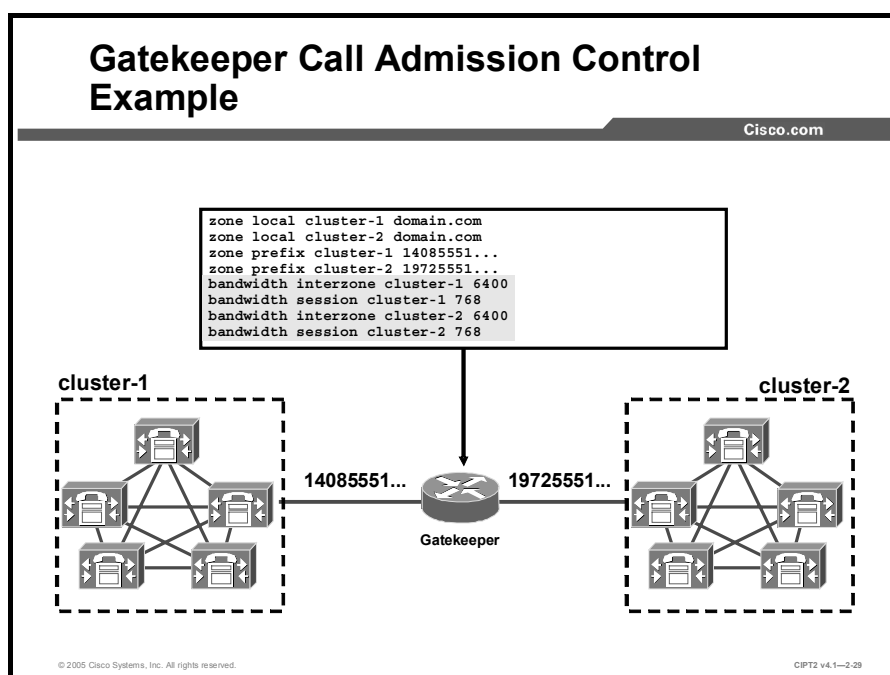
As of Cisco IOS Software Release 12.3(1), these are the types of zone bandwidth limitations that can be configured on the Cisco gatekeeper:

- **Interzone:** The maximum bandwidth of all calls from a local zone to all other zones (local or remote)
- **Total:** The maximum bandwidth of all calls within a local zone
- **Session:** The maximum bandwidth allowed for a single session within a local zone
- **Remote:** The maximum bandwidth for all calls from all local zones to all remote zones

The first three limitations can be configured individually for each local zone. However, you can also specify the default configuration for all local zones that are not configured explicitly.

Gatekeeper Call Admission Control Example

Cisco.com



The intercluster trunk gatekeeper provides address resolution and bandwidth control between Cisco CallManager clusters.

For example, suppose that your network has two Cisco CallManager clusters connected via a digital signal level 3 (DS-3) WAN link. Also assume that you want to allow a maximum of twenty G.711 audio calls and five 384-kbps video calls between the two clusters. In this case, configure one zone per cluster using the **bandwidth interzone** command to restrict the bandwidth between the two zones to the total of twenty G.711 calls plus five 384-kbps video calls. If you want to set the maximum bandwidth per call in a local zone, use the **bandwidth session** command.

Example Values for Twenty G.711 Audio Calls and Five 384-kbps Video Calls

Desired Calls	Gatekeeper Bandwidth Value
20 * G.711 audio calls	128 kbps * 20 = 2560 kbps
5 * 384-kbps video calls	768 kbps * 5 = 3840 kbps
20 * G.711 audio + 5 * 384-kbps video calls	2560 kbps + 3840 kbps = 6400 kbps

The bandwidth value that you have to enter is twice the bit rate of the call. For example, a G.711 audio call that uses 64 kbps would be denoted as 128 kbps in the gatekeeper, and a 384-kbps video call would be denoted as 768 kbps. The table shows the bandwidth values for some of the most popular call speeds.

Bandwidth Values for Frequently Used Call Speeds

Call Speed	Gatekeeper Bandwidth Value
G.711 audio call (64 kbps)	128 kbps
G.729 audio call (8 kbps)	16 kbps
128-kbps video call	256 kbps

Call Speed	Gatekeeper Bandwidth Value
384-kbps video call	768 kbps
512-kbps video call	1024 kbps
768-kbps video call	1536 kbps

Note You cannot avoid having more G.711 calls active than desired because the bandwidth for voice and video is not managed separately. It can happen that more G.711 calls are active than desired and that they consume the configured bandwidth actually reserved for video calls, leaving no bandwidth for video calls.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **The Cisco video telephony solution supports SCCP and H.323 devices. For videoconferences, an MCU is required.**
- **The typical video call includes two or three RTP streams in each direction.**
- **SCCP clients offer PBX features, and H.323 clients support basic call functionality.**
- **For the needed bandwidth, add 20 percent to the speed of the video call.**
- **Call admission control within a cluster is done through Cisco CallManager locations and regions.**
- **Call admission control between clusters is done through gatekeeper control.**

© 2005 Cisco Systems, Inc. All rights reserved. CIPT2 v4.1-2-30

Lesson 2-2

Configuring Cisco VT Advantage

Overview

Cisco Video Telephony (VT) Advantage is a video telephony solution comprising the Cisco VT Advantage software application and Cisco VT Camera, a video telephony Universal Serial Bus (USB) camera. With the Cisco VT Camera attached to a PC colocated with a Cisco IP Phone, users can place and receive video calls on the enterprise IP telephony network. Customers can take full advantage of their IP networks to deliver enterprise-class business communications that extend voice and video to every user in the organization.

Objectives

Upon completing this lesson, you will be able to configure Cisco VT Advantage. This ability includes being able to meet these objectives:

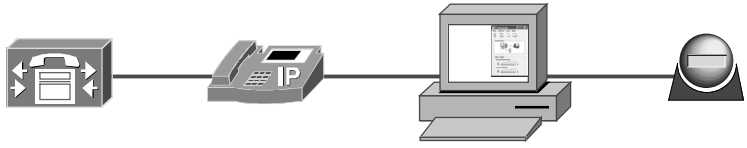
- Describe the features and functions of Cisco VT Advantage
- Explain how placing and receiving calls works with Cisco VT Advantage
- Configure Cisco CallManager for video
- Configure feature settings in Cisco CallManager to support video on Cisco IP Phones
- Install the Cisco VT Advantage application and identify the hardware and software required to run it

Cisco VT Advantage Overview

This topic describes Cisco VT Advantage software.

Cisco VT Advantage Overview

Cisco.com



- **Cisco VT Advantage adds video capabilities to an IP Phone.**
- **It uses a software on a PC connected to the IP Phone.**
- **The PC has video camera connected.**

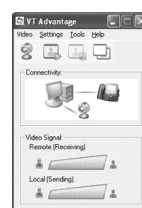
© 2005 Cisco Systems, Inc. All rights reserved. CIPT2 v4.1-2.3

Cisco VT Advantage brings video telephony functionality to the Cisco IP Phone 7940, 7960, and 7970 models. Cisco VT Advantage software coupled with the Cisco VT Camera (a USB camera) allows a PC connected to a Cisco IP Phone to add video to telephone calls without requiring any extra button-pushing or mouse-clicking. When registered to Cisco CallManager, the Cisco VT Advantage-enabled Cisco IP Phone has the features and functionality of a full-featured IP video phone. Supplementary services, such as call forward, transfer, hold, and mute, are also available for video calls and are all initiated through the Cisco IP Phone. Cisco VT Advantage is intended for desktop-to-desktop IP video telephony environments, not as a general-purpose videoconferencing solution for use in conference rooms.

Cisco VT Advantage Components

Cisco.com

- **Cisco CallManager:**
 - Cisco CallManager Release 4.0(1) with Service Release 2 or later
- **Cisco IP Phone 7940G, 7960G, or 7970G**
- **PC with video camera and software:**
 - Cisco VT Advantage camera connected to PC via USB
 - Cisco VT Advantage software installed on PC



© 2005 Cisco Systems, Inc. All rights reserved.

C IPT2 v4.1—2-4

To deploy Cisco VT Advantage, the minimum requirement is Cisco CallManager Release 4.0(1) with Service Release 2 or higher. Currently, video can be enabled on Cisco IP Phone 7940G, 7960G, and the 7970G models. The Cisco VT Camera is connected to a PC (via USB) where Cisco VT Advantage software is installed. Cisco VT Advantage software works only with the Cisco VT Camera.

Note Cisco VT Advantage and the Cisco IP Communicator (Softphone running on a PC) can run on the same PC.

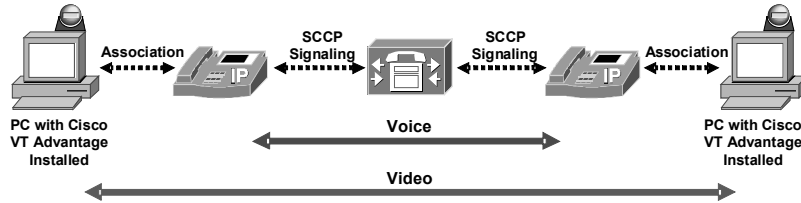
Note Cisco VT Advantage is not supported to interconnect with Cisco IP Communicator.

Cisco VT Advantage software provides the user with an easy-to-use graphical interface, with these options:

- **Receive Only Mode:** Users can choose to view incoming video only and not transmit video.
- **Video Check:** Users can check their video before calls are placed or received.
- **Mute Video on Audio Mute:** When users mute the audio on the IP Phone, video is automatically paused until the audio on the IP Phone is restored.
- **Video Signal Indicators:** The quality of the incoming and outgoing video is graphically displayed.
- **Connectivity Indicator:** Graphics are used to indicate the state of the connections from the PC to its associated Cisco IP Phone and Cisco VT Camera.

Cisco VT Advantage Component Interaction

Cisco.com



- Cisco VT Advantage software on PC associates with IP Phone
- IP Phone registers as a video capable phone
- Audio on the IP Phone
- Video on the PC

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-2.5

Users can operate the Cisco IP Phone as they normally do. The Cisco VT Advantage software is controlled from the PC connected directly to the access port labeled “10/100 PC” on the back of the Cisco IP Phone. The PC and the Cisco IP Phone that is registered in Cisco CallManager as a video-enabled device build an association. The voice Real-Time Transport Protocol (RTP) streams flow between the two IP Phones, as in a normal voice call. The video streams flow between the two PCs where the Cisco VT Advantage software is installed.

Cisco VT Advantage Supported Multimedia Standards

Cisco.com

- **H.263 video codec (from 128 kbps to 1.5 Mbps)**
- **Cisco wideband codec (7 Mbps)**
- **Supports video formats up to 30 fps:**
 - **VGA (640 x 480)**
 - **CIF (352 x 288)**
 - **SIF (320 x 240)**
 - **QCIF (176 x 144)**
 - **QSIF (160 x 120)**
- **H.323 interoperability (AVVID certified)**

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1—2-6

Cisco VT Advantage, like any other application that runs on a PC, has an impact on system performance that should be taken into consideration. Cisco VT Advantage supports two types of video codecs: H.263 and the Cisco VT Camera wideband video codec. Of these two types, the Cisco VT Camera wideband video codec places the least demand on the PC. Therefore, if your network has plenty of available bandwidth, you can use the Cisco VT Camera wideband video codec and save on PC CPU and memory resources.

When you are using a codec that has to be compressed, more CPU power is needed. The H.263 codec is more demanding of PC system resources, but it requires less bandwidth. Therefore, if you want to use H.263 compressed video to conserve bandwidth on the network, you should ensure that your PCs have enough CPU and memory resources available. The Cisco VT Advantage H.263 codec supports a range of speeds up to 1.5 Mbps.

In summary, you must balance PC performance with network utilization when deploying Cisco VT Advantage.

The table lists the video codecs that Cisco VT Advantage supports.

Video Codecs Supported by Cisco VT Advantage

Codec	Parameters
H.263	Bandwidth: Up to 1.5 Mbps Resolution: Common Intermediate Format (CIF) and Quarter CIF (QCIF) Frame rate: Up to 30 frames per second (fps)
Cisco VT Camera wideband video codec	Bandwidth: 7 Mbps Resolution: 320 x 240 Frame rate: Up to 30 fps

Protocols Used by Cisco VT Advantage

Cisco.com

- **Cisco Audio Session Tunnel—association and signaling between IP Phone and VT Advantage**
- **Cisco Discover Protocol—Discovery between IP Phone and PC**
- **RTP—Media transport (video to Cisco VT Advantage, audio to phone)**
- **SCCP—Signaling between IP Phone and Cisco CallManager**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1—2.7

Cisco VT Advantage supports several industry-standard and Cisco networking protocols required for video communication. The table displays an overview of the supported networking protocols.

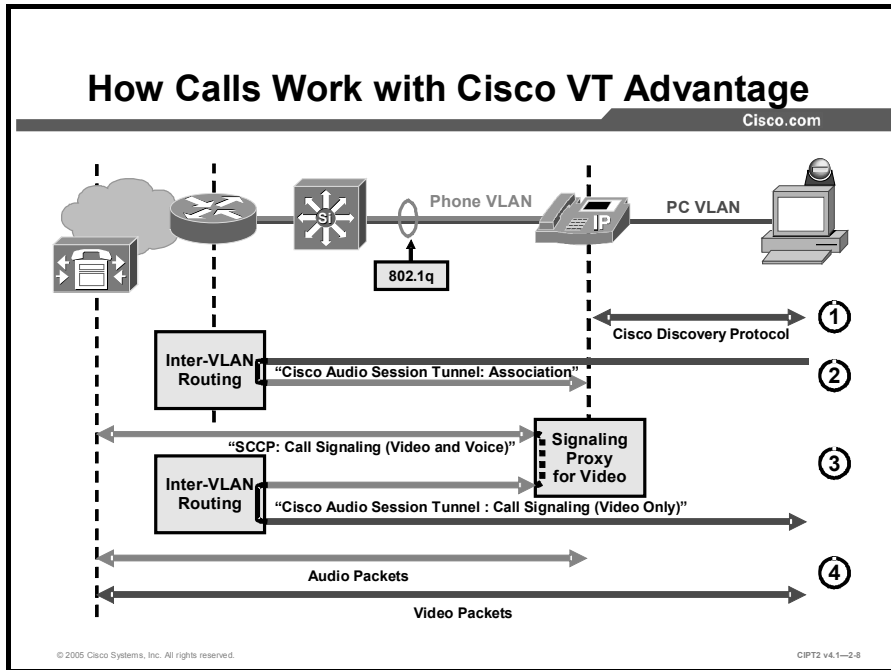
Overview of the Supported Networking Protocols

Networking Protocol	Description	Usage Notes
Cisco Audio Session Tunnel	<ul style="list-style-type: none"> ■ Allows communication between the Cisco IP Phone and associated software, such as Cisco VT Advantage. ■ Uses source and destination port 4224. ■ Uses TCP. ■ Cisco proprietary protocol. 	<ul style="list-style-type: none"> ■ Cisco Audio Session Tunnel is used between Cisco VT Advantage and the IP Phone: <ul style="list-style-type: none"> — To build an association (after the PC discovers the IP Phone using Cisco Discovery Protocol) — To send signaling information for video streams from the IP Phone to Cisco VT Advantage (after the IP Phone receives the signaling messages for both audio and video from Cisco CallManager) ■ Cisco Audio Session Tunnel signaling messages include these: <ul style="list-style-type: none"> — Call video stream start and stop — Call hold and resume

Networking Protocol	Description	Usage Notes
Cisco Discovery Protocol	<ul style="list-style-type: none"> ■ A device-discovery protocol that runs on all Cisco manufactured equipment. ■ A Layer 2 protocol. ■ Works only between directly connected neighbors. ■ Using Cisco Discovery Protocol, a device can advertise its existence to other devices and receive information about other devices in the network. ■ Cisco proprietary protocol. 	<ul style="list-style-type: none"> ■ Cisco VT Advantage uses Cisco Discovery Protocol to communicate its capabilities to the Cisco IP Phone, and the Cisco IP Phone uses Cisco Discovery Protocol to communicate information, such as its IP address, to Cisco VT Advantage.
RTP	<ul style="list-style-type: none"> ■ A standard for using User Datagram Protocol (UDP) to transport real-time data, such as interactive voice and video, over data networks. 	<ul style="list-style-type: none"> ■ The RTP protocol is used to encapsulate and stream the audio (between Cisco IP Phones) and video (between Cisco VT Advantage endpoints).
Skinny Client Control Protocol (SCCP, or Skinny)	<ul style="list-style-type: none"> ■ A Cisco protocol using low-bandwidth messages that allows the exchange of signaling messages between IP devices and the Cisco CallManager. ■ Works on TCP port 2000. ■ Cisco proprietary protocol. 	<ul style="list-style-type: none"> ■ Cisco VT Advantage does not use SCCP itself. It uses Cisco Audio Session Tunnel to send signaling messages to the Cisco IP Phone, which acts as a proxy and passes the signaling messages to Cisco CallManager using SCCP.

How Calls Work with Cisco VT Advantage

This topic describes how calls work, when using Cisco VT Advantage.



When a Windows PC has Cisco VT Advantage installed, it should be connected to the secondary Ethernet port (that is, PC port) of a Cisco IP Phone 7940G, 7960G, or 7970G model. In most configurations, the PC will be in a different VLAN (the port or native VLAN) than the Cisco IP Phone (located in the voice or auxiliary VLAN). In such configurations, all IP-based communication between Cisco VT Advantage and the Cisco IP Phone has to be routed between the VLANs, and only Cisco Discovery Protocol is exchanged directly:

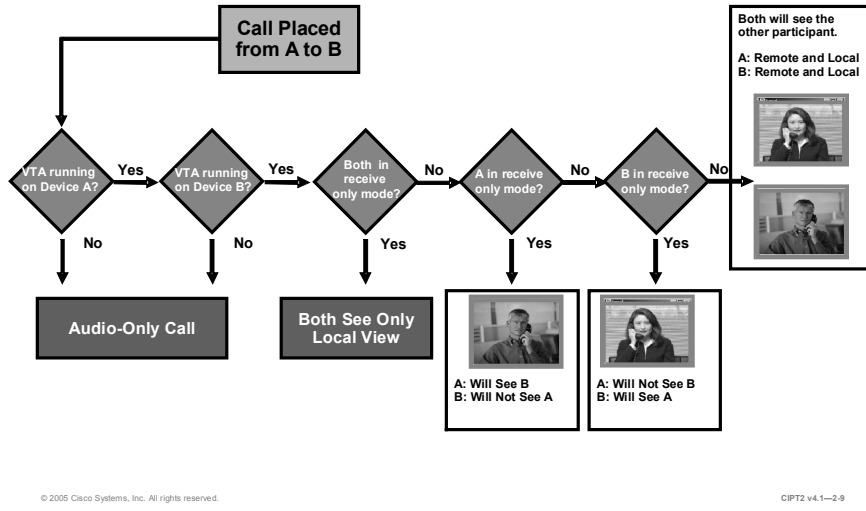
Step 1 Cisco Discovery Protocol exchange takes place so that Cisco VT Advantage and the Cisco IP Phone can discover one another. A Cisco Discovery Protocol driver is installed on the PC during the installation of Cisco VT Advantage. This allows the Cisco VT Advantage application to dynamically learn the IP address of the Cisco IP Phone during the Cisco Discovery Protocol exchange, and associate with it. This serves as both an ease-of-use feature for the end user and for security. The use of Cisco Discovery Protocol to facilitate the association process allows it to occur automatically, without the user having to configure the Cisco VT Advantage application. This allows for mobility of the application between different IP Phones on the network. The user may plug into the PC port of any supported Cisco IP Phone on the network (if permitted by the administrator) and begin making video telephony calls. Cisco Discovery Protocol also provides a measure of security in that the IP Phone will respond only to association messages from a Cisco VT Advantage client that matches the IP address of the device that is connected to its PC port (that is, its Cisco Discovery Protocol neighbor), minimizing the risk of someone else associating with your Cisco IP Phone over the network and receiving video when calls are placed on your IP Phone. The Cisco IP Phone begins listening for Cisco Audio Session Tunnel messages on TCP port 4224.

- Step 2** After Cisco Discovery Protocol discovery, Cisco VT Advantage and the IP Phone exchange Cisco Audio Session Tunnel protocol messages over TCP/IP. Cisco VT Advantage sends a Cisco Audio Session Tunnel message to the IP Phone, which is in a different IP network (VLAN). The packet first travels through the PC VLAN to the default gateway, where it is routed toward the IP Phone (using the voice VLAN). The Cisco Audio Session Tunnel protocol allows Cisco VT Advantage to associate with the IP Phone and receive event messages from the IP Phone when calls are placed or received. After this association process occurs between the Cisco VT Advantage client and the IP Phone, the IP Phone updates its registration status with Cisco CallManager, advising Cisco CallManager of its video capabilities.
- Step 3** When the Cisco IP Phone receives signaling information for video calls, it acts as a proxy toward Cisco VT Advantage for the setup of the video streams. Only the signaling is proxied, but when the RTP endpoints (IP addresses and UDP RTP port numbers) are negotiated, the IP Phone specifies the IP address of the PC for the video stream and its own IP address for the audio stream. When Cisco CallManager tells the Cisco IP Phone to open the video channel, (communicating to the IP Phone using the voice VLAN) the IP Phone proxies those messages to Cisco VT Advantage using Cisco Audio Session Tunnel protocol. These Cisco Audio Session Tunnel messages have to be routed between the voice and the PC VLAN again.
- Step 4** After the voice and video channels have been successfully set up, the audio stream is sent to the IP address of the IP Phone (to the voice VLAN) while the video stream is sent directly to the PC IP address (to the PC VLAN).

Note Firewalls or access control lists (ACLs) must permit TCP port 4224 to allow the exchange of Cisco Audio Session Tunnel messages.

Cisco VT Advantage Video Modes

Cisco.com



For privacy, the participants can switch to a mode called receive-only mode to prevent a camera picture being sent to the other end of the call.

The table shows various scenarios of the calling or the called party activating or disabling receive-only mode.

Cisco VT Advantage Video Modes

Cisco VT Advantage Mode on Your PC	Cisco VT Advantage Mode on the PC of the Other User	Result
Enabled	Enabled	When you place or answer a call, two video windows open on your PC—you will see yourself in the Local Video window and the other party in the Remote Video window.
Receive-only	Enabled	When you place or answer a call, you will see the other party in the Remote Video window. The Local Video window will not display. The other party will see a blank image in the Remote Video window.
Enabled	Receive-only	When you place or answer a call, you will see yourself in the Local Video window and a blank image in the Remote Video window. The other party will not see a Local Video window.
Receive-only	Receive-only	No one will see the other party; this mode is similar to a telephone call.

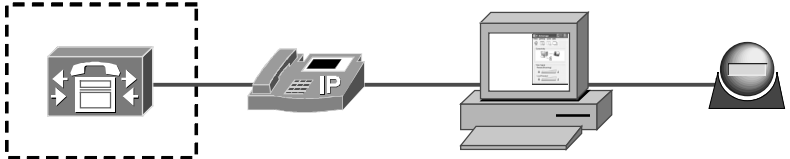
Note When Cisco VT Advantage is not running on your PC or on the PC of the remote peer, the call functions as a regular telephone call without video.

Configuring Cisco CallManager for Video

This topic describes the steps to configure Cisco CallManager to support Cisco VT Advantage.

Configuring Cisco CallManager for Video

Cisco.com



The diagram illustrates the components of a video IP telephony environment. From left to right, it shows a video IP phone (enclosed in a dashed box), an IP phone, a Cisco CallManager server (represented by a computer monitor and tower), and a video camera. A horizontal line connects all four devices, indicating network connectivity.

To enable video in your existing voice network, start with Cisco CallManager configuration.

© 2005 Cisco Systems, Inc. All rights reserved. CIP12 v4.1-2-10

When you are setting up a video IP telephony environment, you first have to configure video in Cisco CallManager. Cisco VT Advantage requires Cisco CallManager to handle video call processing.

Cisco CallManager Considerations When Enabling Video

Cisco.com

- **Update locations and regions configuration.**
- **Reconsider call routing.**
- **Configure separation of MRGL—in connection with SCCP MCUs only.**
- **Reconsider DSCP values.**
- **Consider using deployment tool to propagate Cisco VT Advantage software.**

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1—2-11

Assuming that you already have a Cisco CallManager environment, to enable video on Cisco CallManager, you must update your locations and regions settings to adjust your bandwidth settings. Media Resource Group Lists (MRGLs) are used to control the access to multipoint control units (MCUs). Only devices that are allowed to use an MRGL are able to use the resources in the MRGL. Further, you have to reconsider the call-routing configuration when using, for example, automated alternate routing (AAR). Another important point that arises during the consideration of video is the Differentiated Services Code Point (DSCP) settings for quality of service (QoS).

In large Cisco CallManager environments, you have to consider whether it makes sense to use the Cisco VT Advantage Deployment Tool to make Cisco VT Advantage software available for download in Cisco CallManager.

Configuring Video Bandwidth Properties in Cisco CallManager

Cisco.com

Region Configuration

Region: San Jose
Status: Update completed
[Update] [Delete] [Reset Devices]

Region Information

Region Name* San Jose

Call Information

The maximum audio codec/video bandwidth supported within this region and between further regions are:

Region	Audio Codec	Video Call Bandwidth
Dallas	G.711	<input type="radio"/> None <input checked="" type="radio"/> 384 kbps
San Francisco	G.729	<input type="radio"/> None <input checked="" type="radio"/> 128 kbps
San Jose (Within this Region)	G.711	<input type="radio"/> None <input checked="" type="radio"/> 768 kbps

Items per page: 10 of 1
Page 1 of 1
* indicates required item

Location Configuration

Location: San Francisco
Status: Update completed
[Copy] [Update] [Delete] [Resync Bandwidth]

Location Information

Location Name* San Francisco

Audio Calls Information

Audio Bandwidth* Unlimited 48 kbps
If the audio quality is poor or choppy, lower the bandwidth setting. For 120M use multiples of 56 kbps or 64 kbps.

Video Calls Information

Video Bandwidth* None Unlimited 128 kbps
* indicates required item

When enabling video, update regions and locations configuration by setting the video bandwidth parameters.

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-2-12

When adding video to your existing IP telephony network, you will most likely have to add bandwidth to your physical links, redesign your QoS policy, and update your call admission control settings according to the new policy. Set these parameters by configuring regions and locations also on video, following these guidelines:

- Regions define the bandwidth that will be used by devices within the same region and between devices in different regions. This allows you to configure Cisco CallManager for high-quality video within one area of the network, and lower-quality video between that area and another area separated by a WAN:

In the example, G.711 and 768 kbps are used within the San Jose region, G.729 and 128 kbps are used for calls to San Francisco, and G.711 and 384 kbps are used for calls to Dallas.

- Although regions define the maximum bandwidth that can be used per call, the administrator may also define how much bandwidth will be allowed for all calls on a per-site basis. This is done by configuring locations in Cisco CallManager Administration.

In the example, the maximum bandwidth for video calls is set to 128 kbps, while the maximum bandwidth for audio calls is set to 48 kbps. This value applies for all calls to or from San Francisco.

The combined video and audio bandwidth is then deducted from the value in the Video Bandwidth field for the location. If the location does not have enough bandwidth to allow the video call, Cisco CallManager checks the Retry Video Call as Audio setting. If the feature is enabled, the call continues as audio, with audio region and audio location checks being made. If not, the call either fails (with busy tone played and a “Bandwidth Unavailable” message displayed to the user) or AAR tries to reroute the call.

Call-Routing Considerations

Cisco.com

- **Existing dial plan and call-routing features are used:**
 - **Route or hunt lists or AAR groups can try different paths also for video calls.**
 - **Retry Video Call as Audio option has a higher preference than AAR.**
- **MRGL:**
 - **Video conferences must use the videoconference bridge as the first conference resource.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1—2-13

One of the advantages of using Cisco VT Advantage is that the existing dial plan can be used.

If the bandwidth needed by an endpoint for a video call is not available, by default the call is retried as an audio call. To use route or hunt lists or AAR groups to try different paths for such video calls instead of retrying them as audio calls, uncheck the **Retry Video Call as Audio** check box in the configuration settings for the applicable gateways, trunks, and IP Phones.

Video-enabled IP Phones should have a separate MRGL with the videoconference bridge as the first choice. If the nonvideo-enabled IP Phones use the videoconference bridge as a first choice, you run the risk of having no videoconference resources available for videoconference calls because all the videoconference resources are occupied by audio-only conferences. It is recommended that you create two separate MRGLs—one for video-enabled IP Phones and one for nonvideo-enabled IP Phones.

QoS Considerations for Video Calls

Cisco.com

- **Enabling video in the network requests updates of your QoS policy:**
 - This can include new DSCP values.
- **Set DSCP values according to your updated QoS policy under Cisco CallManager > Service Parameters.**
- **Audio streams in audio-only calls default to EF.**
- **Video streams and associated audio streams in video calls default to AF41.**

Clusterwide Parameters (System - QoS)	
Parameter Name	Parameter Value
Priority Class*	Normal Priority
DSCP for Audio Calls*	EF DSCP (101110)
DSCP for Video Calls*	AF-41 DSCP (100010)

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-2-14

Video is as time-critical as voice. In a voice- and video-enabled network, you have to prioritize voice and video packets so that you do not experience quality issues. Both voice and video must be of higher priority than data, for example.

Note The Cisco Voice Over IP (CVOICE) and Implementing Cisco Quality of Service (QoS) courses describe QoS and corresponding parameters such as DSCP in more detail.

DSCP packet marking includes these characteristics:

- Audio streams in audio-only calls default to Expedited Forwarding (EF) class.
- Video streams and associated audio streams in video calls default to Assured Forwarding, Class 4, with low drop precedence (AF41)

You can change these defaults using service parameters.

These service parameters affect DSCP packet marking:

- **DSCP for Audio Calls (for media RTP streams):** This parameter specifies the DSCP value for audio calls.
- **DSCP for Video Calls (for media RTP streams):** This parameter specifies the DSCP value for video calls.

Deployment Tool

Cisco.com

- **A tool for simple, scalable deployment of the Cisco VT Advantage software**
- **Makes the Cisco VT Advantage installer available on the Cisco CallManager publisher for download**
- **The Cisco VT Advantage Deployment Tool has the following features:**
 - **AutoUpdate**
 - **Proxy**
 - **Error Reporting Tool**

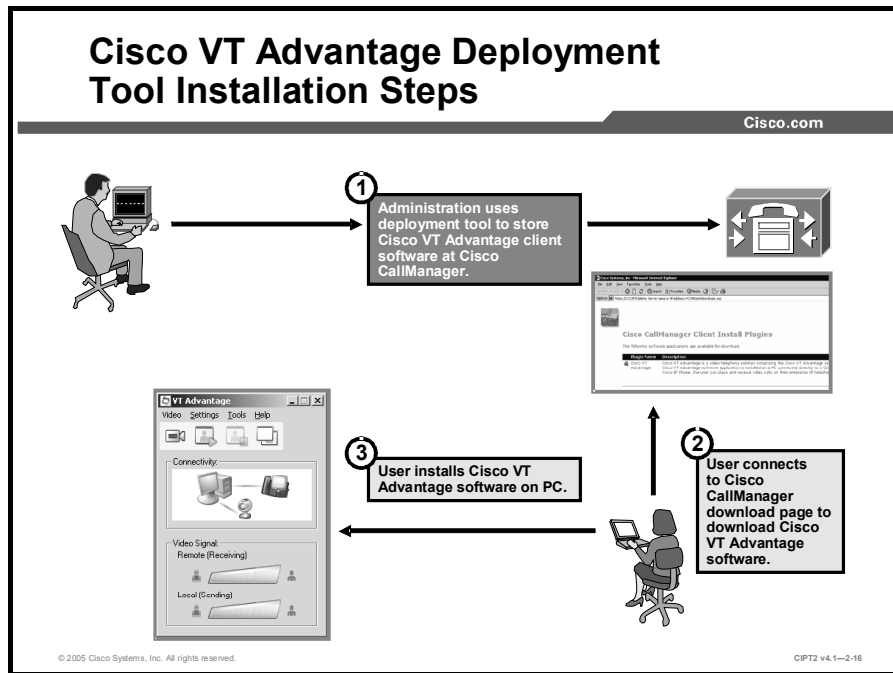
© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1—2-15

For simplified and scalable deployment of Cisco VT Advantage client installation software, you can use the Cisco VT Advantage Deployment Tool. Administrators can use this tool to make the Cisco VT Advantage installer program available on a Cisco CallManager publisher server. The installer program will then reside in the CCMPluginsClient website that is mapped to the C:\CiscoPlugins\Client\CVTA directory. This website is set up with the correct permissions to allow anonymous access to the Cisco VT Advantage Installer executable file to facilitate installation for your technicians and users.

The Cisco VT Advantage Deployment Tool lets you set these options for the installation:

- **AutoUpdate:** Sets the AutoUpdate option so that users are notified automatically about updates to Cisco VT Advantage
- **Proxy:** Sets proxy server information for users needing to use a proxy server to reach the Cisco CallManager publisher server
- **Error Reporting Tool:** Sets the e-mail or FTP addresses where users send reports generated by the Error Reporting Tool



The deployment tool is published by the administrator in Cisco CallManager. End users can access a download window to install the tool on the PC.

To publish Cisco VT Advantage to Cisco CallManager, the administrator must complete this step:

- Step 1** Download the latest available Cisco VT Advantage Deployment Tool from Cisco.com. Run the DeployMan.exe file to set up Cisco VT Advantage for end users. The Cisco VT Advantage installer program is now stored in Cisco CallManager and a download link will be made available on Cisco CallManager user-accessible installation pages.

To install Cisco VT Advantage on a PC, users must complete these steps:

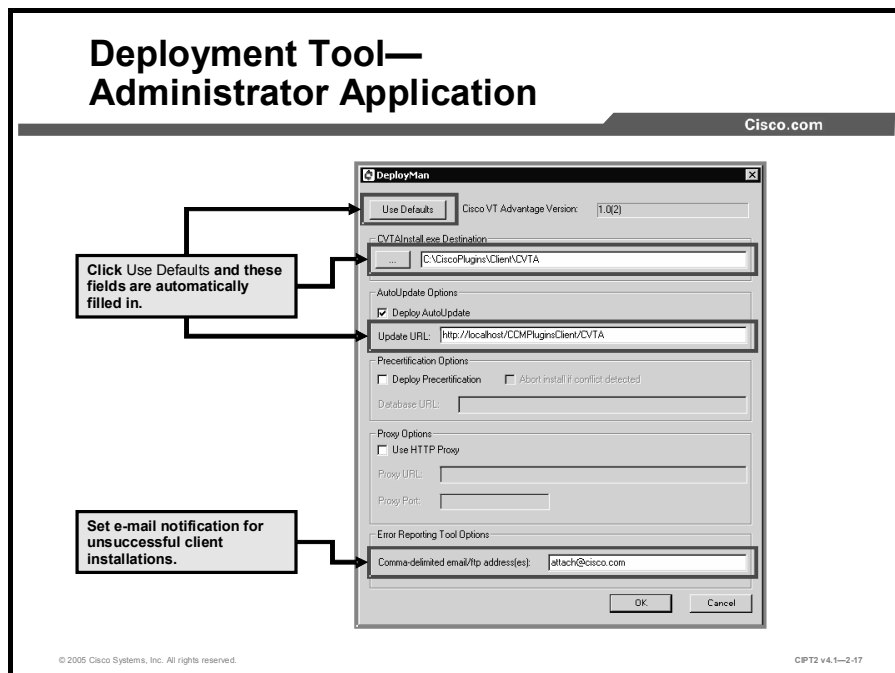
- Step 1** Access the Cisco CallManager user installation page and download the Cisco VT Advantage software:

<https://<CCM Publisher Server name or IP address>/CCMUser/downloads.asp>

This URL is found in the Services Help screen on Cisco IP Phone models that support Cisco VT Advantage.

- Step 2** Install Cisco VT Advantage software on the PC.

Deployment Tool— Administrator Application



When you click the Use Defaults button in the DeployMan main window, the Cisco VT Advantage Deployment Tool must be running on the Cisco CallManager publisher server. If this is not the case, change the path in the CVTInstall.exe Destination field by referring to the C:\CiscoPlugins\Client\CVTA directory at the publisher via a network file share. The Choose Host Name dialog appears. Enter the hostname (or IP address) of the Cisco CallManager publisher server. This value populates the Update URL field for the AutoUpdate feature.

These fields are automatically populated with default values:

- Cisco VT Advantage Version
- CVTInstall.exe Destination
- Update URL
- Comma-Delimited E-Mail/FTP Addresses

Make sure that the Update URL field in the AutoUpdate Options area contains the hostname (or IP address) of the Cisco CallManager publisher server. If you do not want to use AutoUpdate, uncheck the Deploy AutoUpdate check box.

The Precertification Options area will be usable only in later versions of the deployment tool, even though it is shown in the GUI of the current version (1.0).

If users in the network need to use a proxy server to reach the Cisco CallManager publisher server, check the **Use HTTP Proxy** check box and fill in the Proxy URL and Proxy Port fields with the appropriate values.

In the Comma-Delimited E-Mail/FTP Addresses field of the Error Reporting Tool option, enter the e-mail or FTP addresses to which error reports generated by users can be sent. You can enter multiple addresses separated by commas. The default e-mail address is `attach@cisco.com`—this e-mail address is used by the Cisco Technical Assistance Center (TAC) to pick up files sent by customers.

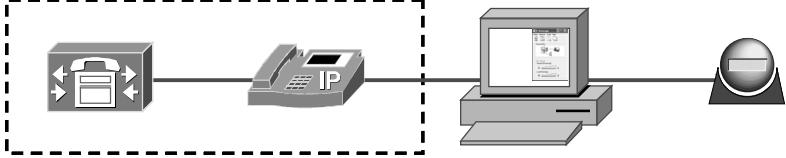
When you have filled in all necessary options, click **OK** to make the Cisco VT Advantage installation program available to users.

Configuring Cisco IP Phones for Cisco VT Advantage

This topic describes the steps that are necessary to enable video on Cisco IP Phones.

Configuring Cisco IP Phones for Cisco VT Advantage

Cisco.com



**Configure Cisco IP Phones in Cisco
CallManager configuration to support Cisco
VT Advantage.**

© 2005 Cisco Systems, Inc. All rights reserved. CIP12 v4.1-2.18

In addition to the global Cisco CallManager parameters that are needed for a video-enabled IP telephony network, you have to configure the individual devices (IP Phones) to support video calls. The Cisco IP Phone requires Cisco CallManager for call processing and the appropriate phone load to support video on the IP Phone.

Configuring IP Phones in Cisco CallManager

Cisco.com

- **Verify that your phone loads support video:**
 - **Cisco IP Phone 7940G, 7960G, or 7970G**
- **Enable PC port.**
- **Enable video support.**
- **Check or uncheck Retry Video Call as Audio.**
- **Verify the IP Phone configuration.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1—2-19

When you are configuring IP Phones for video in Cisco CallManager, these settings have to be configured:

- Make sure that a phone load that supports video is installed on each Cisco IP Phone that will be video-enabled.
- The port labeled “10/100 PC” on the back of the Cisco IP Phone connects a PC or a workstation to the IP Phone so that they can share a single network connection. Make sure that this feature is enabled on Cisco IP Phones that operate with Cisco VT Advantage.
- The Cisco IP Phone has to be configured to support video calls.
- Check or uncheck the Retry Video Call as Audio check box. When the Retry Video Call as Audio box is checked, a Cisco IP Phone that cannot obtain the bandwidth that it needs for a video call will retry the call as an audio call.
- Verify that the Cisco IP Phone is video-enabled after configuring the IP Phone in Cisco CallManager configuration.

Verify the Phone Loads

Cisco.com

- IP Phone load 6.0(3) or later for Cisco IP Phone 7940G and 7960G.
- IP Phone load 6.0(1) or later for Cisco IP Phone 7970G.

Device Type	Load Information	Device Pool	Phone Template
Cisco 7940	P00306000300	STA-LAN	Standard 7940
Cisco 7960	P00306000300	STA-LAN	Standard 7960
Cisco 7961		Default	Standard 7961
Cisco 7970	TERM70_6-0-2ES6-1S	Default	Standard 7970

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-2-20

As shown in the figure, use phone load 6.0(3) or later for the Cisco IP Phone 7940 and 7960 models. For the Cisco IP Phone 7970, use the phone load 6.0(1) or later. To verify the phone loads, choose **Cisco CallManager Administration > System > Device Defaults**.

Phone Loads

Field Name	Description
Device Type	Name of the device in Cisco CallManager.
Load Information	Enter the ID number of the firmware load that is used with a particular type of hardware device. If you install an upgrade or patch load, you must update the load information for each type of device that uses the new load.
Device Pool	Choose the device pool that is associated with each type of device. The device pool defines common characteristics for all devices in the pool.
Phone Template	Choose the phone button template that is used by each type of Cisco IP Phone. The template defines which keys on the phone perform particular functions.

Note To download the latest phone loads, go to Cisco.com.

Required Phone Configuration Settings for Cisco VT Advantage Support

Cisco.com

- **PC port:**
 - Enabled by default
 - **Must be enabled for Cisco VT Advantage**
- **Video capabilities:**
 - Disabled by default
 - **Enable to allow Cisco VT Advantage to associate with IP Phone**
- **Both settings are found at the Phone Configuration page**

Product Specific Configuration	
Disable Speakerphone	<input type="checkbox"/>
Disable Speakerphone and Headset	<input type="checkbox"/>
Forwarding Delay*	Disabled
PC Port*	Enabled
Settings Access*	Enabled
Gratuitous ARP*	Enabled
PC Voice VLAN Access*	Enabled
Video Capabilities*	Enabled
Auto Line Select*	Disabled
Web Access*	Enabled

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1—2-21

The IP Phone configuration settings that are required for video support can be found in the IP Phone configuration window of Cisco CallManager Administration (choose **Device > Phone**).

Tip The IP Phone settings need not be configured before Cisco VT Advantage can be loaded on the client PC. But the preferred sequence is to configure the IP Phone first and then install the Cisco VT Advantage software.

- Because the PC that has Cisco VT Advantage installed needs to be physically connected to a PC port of the IP Phone, ensure that the PC port of the IP Phone is not disabled under the Cisco CallManager IP Phone configuration. By default, the PC port is enabled.
- When the Video Capabilities field is set to Enabled, the phone will participate in video calls when connected to an appropriately equipped PC. Make sure that this feature is enabled on Cisco IP Phones that operate with Cisco VT Advantage. Video capability is disabled by default.

Enabling Retry Video Call as Audio

Cisco.com

- A video-enabled IP Phone can be configured to retry video calls as audio calls if the video call cannot be set up.
- This parameter is enabled by default.
- The parameter is configured at the Phone Configuration page.

User Hold Audio Source	< None >
Network Hold Audio Source	< None >
Location	Stamberg
User Locale	< None >
Network Locale	< None >
Device Security Mode	Use System Default
Signal Packet Capture Mode	None
Packet Capture Duration	60
Built In Bridge	Default
Privacy	Default
<input checked="" type="checkbox"/> Retry Video Call as Audio	

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-2-22

A video-enabled Cisco IP Phone can be configured to retry video calls as audio calls if the video call cannot be set up. The Retry Video Call as Audio check box is located in the Phone Configuration window, and this feature is activated by default. To enable the Retry Video Call as Audio feature, choose **Cisco CallManager Administration > Device > Phone**.

If you uncheck this check box, a video call that fails to connect as a video call does not try to establish an audio-only call instead.

Verification of Phone Configuration

Cisco.com

- A video-enabled IP Phone shows a small camera on its display.
- The symbol is visible when the phone is configured to support video calls.
 - It does not indicate that Cisco VT Advantage has been associated with the IP Phone.



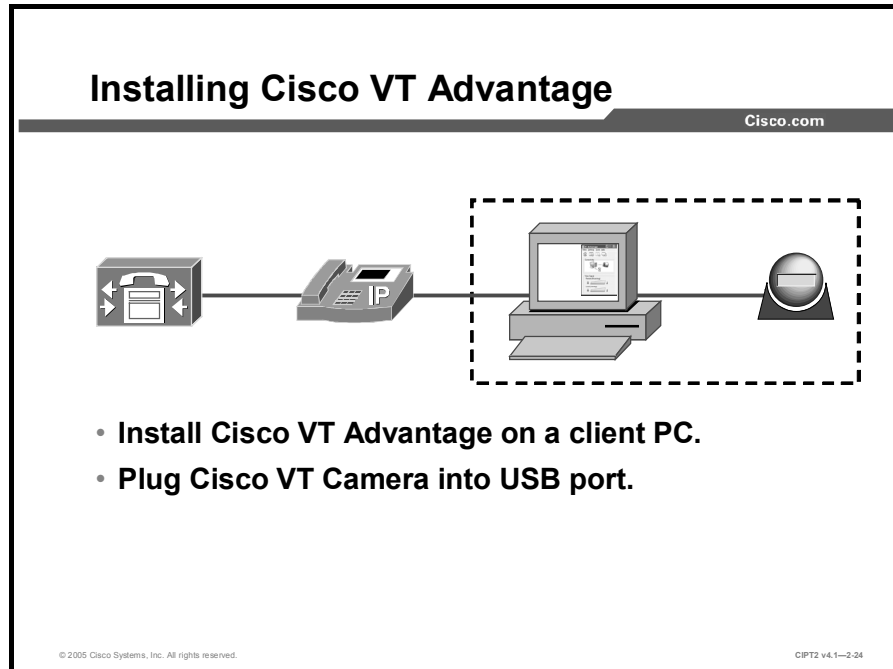
© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1—2-23

An IP Phone enabled for video displays a video camera icon in the lower-right corner of its liquid crystal display (LCD) screen. A PC with Cisco VT Advantage installed does not have to be connected to the IP Phone to produce the video camera icon. The camera icon is displayed as soon as video is enabled for the IP Phone in Cisco CallManager configuration.

Installing Cisco VT Advantage

This topic describes the Cisco VT Advantage installation process on the PC.



After configuring Cisco CallManager and the Cisco IP Phone, you need to install Cisco VT Advantage on the PC. Hardware and software requirements have to be considered before you launch the installation.

Cisco VT Advantage Setup Procedure

Cisco.com

1. Consider hardware requirements.
2. Consider software requirements.
3. Install Cisco VT Advantage software and hardware.
4. Verify Cisco VT Advantage installation.

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1—2-25

When installing VT Advantage, use this setup procedure:

- Step 1** Consider the hardware requirements to install Cisco VT Advantage.
- Step 2** Consider the software requirements to install Cisco VT Advantage.
- Step 3** Verify the preparation checklist to ensure that all necessary preinstallation tasks have been completed successfully. After the verification, install the Cisco VT Advantage software and hardware.
- Step 4** Verify the Cisco VT Advantage installation using Cisco VT Advantage tools.

Cisco VT Advantage Hardware Requirements

Cisco.com

- **PC:**
 - At least 1-GHz CPU
 - At least 256-MB memory
 - 40-MB free disc space
 - At least one USB port
 - Connected to a Cisco IP Phone 7940G, 7960G, or 7970G
- **Cisco VT Camera:**
 - Connected to a USB port of the PC

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1—2-26

In addition to the Cisco IP Phone, you need these hardware components to use Cisco VT Advantage:

- PC
- Cisco VT Camera

Cisco IP Phone

Cisco VT Advantage is supported on the Cisco IP Phone 7940, 7960, and 7970 models.

PC Hardware Requirements

This table describes the hardware requirements for the PC where the Cisco VT Advantage software is installed.

PC Feature	Minimum Requirements
CPU	<ul style="list-style-type: none">■ 1.0-GHz or higher Pentium III or compatible processor (Streaming Single Instruction Stream, Multiple Data Stream [SIMD] Extensions support required)■ 1.4-GHz or higher Pentium III or compatible processor recommended
System memory	256 MB minimum
Free disk space	40 MB
Universal Serial Bus (USB) port	At least one free USB (1.1 or 2.0 compliant) port
Video display	Video-capable graphics card at 800 x 600 x 16 bits or better
Network	10/100-Mb Ethernet network interface card (NIC)

Note Do *not* connect the Cisco VT Camera to your PC until prompted to do so during the installation.

Cisco VT Camera

The Cisco VT Camera must be connected to the PC during the installation of the Cisco VT Advantage software on the PC.

Note Cisco VT Advantage supports only the Cisco VT Camera, and the Cisco VT Camera works only with the Cisco VT Advantage software.

Cisco VT Advantage Software Requirements

Cisco.com

Operating system:

Windows 2000 with Service Pack 3 or later

Windows XP with Service Pack 1 or later

Cisco VT Advantage software—sources:

Downloaded from Cisco CallManager (if the deployment tool was used)

Downloaded from Cisco.com

Distributed on CD or a file server

The Cisco VT Advantage software must be installed on the PC connected directly to the Cisco IP Phone.

PC Feature Requirements

The minimum requirement for the operating system of the PC is either Microsoft Windows 2000 Professional with Service Pack 3.0 or later or Windows XP Professional with Service Pack 1.0 or later.

Cisco VT Advantage Software

The Cisco VT Advantage Software can be downloaded in two ways:

- From the Cisco CallManager publisher (if the administrator used the deployment tool):
 - The default URL for the software download when Cisco VT Advantage is deployed with the deployment tool, is
<https://<CCM Publisher Server name or IP address>/CCMUser/downloads.asp>.
- From Cisco.com:
 - To download the Cisco VT Advantage software from Cisco.com, users need a valid Cisco.com account.
 - Alternatively, the administrator can download the Cisco VT Advantage software and provide it to users via CD, file server, or any other means.

Cisco VT Advantage Installation Preparation Checklist

Cisco.com

- **Ensure the following:**
 - **The Cisco IP Phone is connected.**
 - **The Cisco IP Phone is video-enabled.**
 - **The PC is connected to the Cisco IP Phone.**
- **Verify IP connectivity between IP Phone and PC:**
 - **Check reachability using ping.**
 - **Ensure that Cisco Audio Session Tunnel protocol is not filtered.**

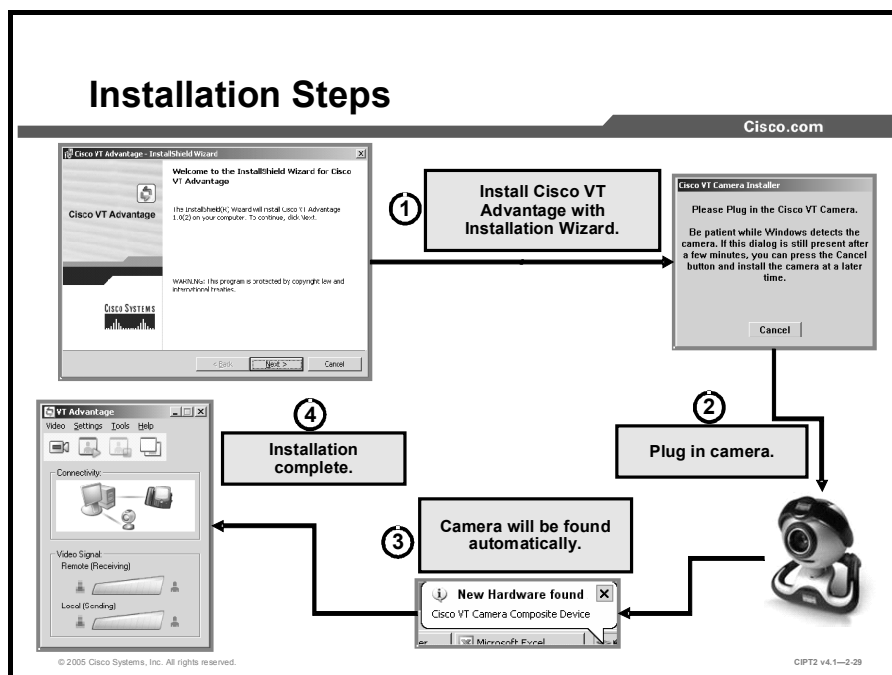
© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1—2-28

Check these points before installing Cisco VT Advantage software on a PC:

- Ensure that the Cisco IP Phone is properly connected to the corporate telephony network. You could do a short audio test call to ensure that the IP Phone is working correctly.
- Ensure that the Cisco IP Phone is video-enabled. If the LCD screen on the Cisco IP Phone displays the video camera icon on the status line, the phone is video-enabled.
- Ensure that the Ethernet port of the PC is connected to the PC port of the IP Phone because this connection is mandatory for Cisco VT Advantage.
- For the Cisco Audio Session Tunnel protocol to operate between Cisco VT Advantage and the IP Phone, the PC must be capable of reaching the IP Phone over TCP/IP. Typical IP telephony designs use separate voice and data VLANs, as well as ACLs or firewalls between those VLANs to secure the IP telephony network.

Note Do not forget to enable the port 4224 on your firewall.



After launching the previously downloaded installation file, complete these steps:

- Step 1** Find the URL from which to download the Cisco VT Advantage Installer by following the appropriate steps for your Cisco IP Phone model:
- On a Cisco IP Phone 7940 or 7960:
 - Press the **?** or **i** Help button and then press the **Services** button.
 - Use the **Navigation** button to scroll to the end of the help text. The instructions provide the URL for downloading software.
 - Write down the URL and exit the IP Phone Help display.
 - On a Cisco IP Phone 7970:
 - Press the **?** Help button and then quickly press the **Services** button.
 - When the Services Topics screen appears, press the **PC Client Software Plugins** menu item on the touchscreen. The instructions provide the URL for downloading software.
 - Write down the URL and exit the IP Phone Help display.

Note The default URL, when Cisco VT Advantage is deployed with the deployment tool, is <https://<CCM Publisher Server name or IP address>/CCMUser/downloads.asp>.

- Step 2** Open your web browser, enter the URL in the address field, and press **Enter**.
- Step 3** On the Cisco CallManager Client Install Plugins page, click the **Cisco VT Advantage Installer Plug-In** icon. The camera should *not* be connected at this time.
- Step 4** Follow the instructions presented in the dialog boxes to complete the installation of Cisco VT Advantage:
- In the Welcome window, click **Next** to start the installation wizard.

- In the License Agreement window, select **I Accept the Terms in the License Agreement**, and click **Next**.
- In the Customer Information window, enter the user information, select the desired option, and click **Next**.
- In the Destination Folder window, accept the default installation folder or click **Change** to enter a different installation folder. When you are done, click **Next**.
- In the Ready to Install window, click **Install**. Depending on the setup of your PC, you might see messages for the installation of the Cisco Media Termination Driver and the Cisco VT Camera software that differ, based on the operating system of the PC:
 - **Windows 2000:** If a “Digital Signature Not Found” message appears, the driver software has no Microsoft digital signature that would affirm that the software has been tested with Windows and that the software has not been altered since it was tested. Click **Yes** to continue.
 - **Windows XP:** If a “Hardware Installation” message appears, the software that you are installing has not passed Windows Logo testing to verify its compatibility with Windows XP. To continue the installation, click **Continue Anyway**.

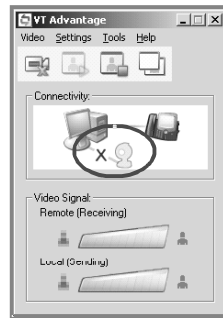
Step 5 Plug the Cisco VT Camera into an available USB port on the PC. As soon as you plug in the camera, the operating system finds it automatically. A window appears offering the creation of a shortcut to the application. Choose the desired option and then click **Next**.

Step 6 A window appears indicating that the installation has completed. Confirm the message by clicking **Finish**. If you are prompted to restart the PC, click **Yes** to restart the PC.

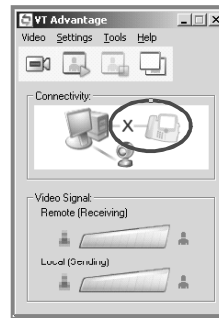
Cisco VT Advantage Installation Verification

Cisco.com

After starting the Cisco VT Advantage software, verify the camera and IP Phone connection status.



Camera Not Connected



Phone Not Connected

© 2005 Cisco Systems, Inc. All rights reserved.

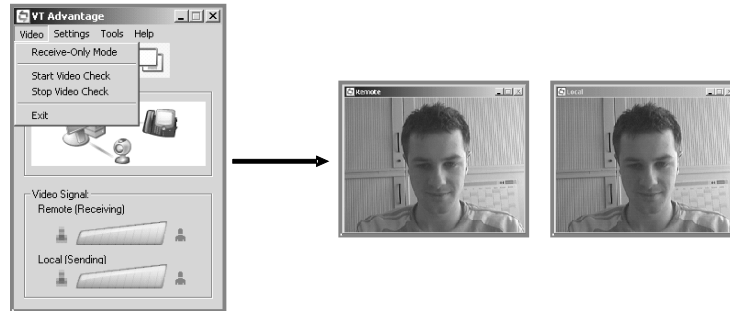
CIPT2 v4.1-2-30

When the Cisco VT Advantage application is started verify its connectivity, if a connection to the Cisco IP Phone or to the Cisco VT Camera is not working, a red X is displayed over the corresponding connecting line. If the connections are functioning, the corresponding lines are shown without the red X and the lines themselves are green.

Cisco VT Advantage Installation Verification (Cont.)

Cisco.com

- After verifying the camera connection status, run a video check:
 - You should see the camera input in both windows, the remote and the local view.

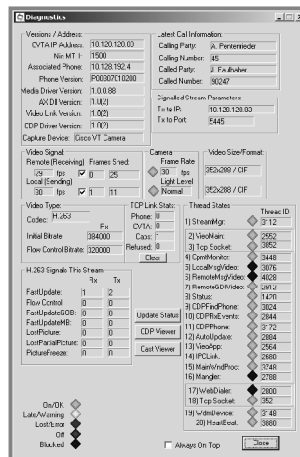


When you have ensured that the camera connection is functioning, you should run a video check. To start the video check, choose **Video > Start Video Check**. While the video check is being performed, two green bars are displayed (one for the sending video signal and the other for the receiving video signal) when the system is working. In addition, two popup windows show the local and remote views. During the video check, you will see the same image in both windows.

Active Call Verification with the Diagnostic Tool

Cisco.com

- During the call, you should see local and Remote view.
- You can open a call diagnostic window by double-clicking the Cisco VT Advantage application window.



After a successful video check, you should be able to place and receive calls. Place a test call to another IP phone with Cisco VT Advantage enabled, and verify the local and remote views. While in a call, you can launch the diagnostic tool. The diagnostic tool provides some technical details about the current state of the Cisco VT Advantage software that is running on the PC, as well as some indications about the Cisco VT Camera frame rate and light level.

To use the diagnostic tool, open the Cisco VT Advantage main window and double-click the video signal quality bars. The Diagnostics window appears.

When users report seeing a low signal quality bar, you can check the Cisco VT Camera frame rate and light level. Look near the center of the Diagnostics window for the Camera area. It contains two fields:

- **Frame Rate:** Indicates the frames per second reported by the camera. The values are 5, 10, 15, 20, 25, or 30. The LED colors correspond to the frame rate: Green is 30 fps, yellow is 5, 10, 15, 20, or 25 fps, and black is blank or off.
- **Light Level:** Indicates the lighting conditions reported by the camera. The values are Off, Normal, and Low Light. The LED colors correspond to the light levels: Black is off, green is normal, and red is low light. Increasing the lighting conditions near the camera should result in a higher frame rate and a normal light level. When you are troubleshooting some Cisco VT Advantage problems with the assistance of Cisco TAC representatives, they might ask you to provide them with the information displayed in the Diagnostics window.

Low Frame Rate Example

A low frame rate can be caused by low light conditions. The Cisco VT Camera is normally set for automatic exposure. When the lighting is low, the camera has to expose each frame for a longer time, resulting in a lower frame rate. To test for this issue with the diagnostic tool, double-click the signal quality bars. The Diagnostics window appears. The Video Signal area at the middle left of the window contains fields showing the current number of frames per second being processed. At this point, all the data is coming from the camera, so if the value is less than 15 fps, the problem most likely is the lighting conditions. Improving the lighting near the camera should result in a higher frame rate and a normal light level.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Cisco VT Advantage associates with the Cisco IP Phone and registers as a video capable phone on Cisco CallManager.**
- **The IP Phone acts as an SCCP proxy between Cisco VT Advantage and Cisco CallManager.**
- **Configure Cisco CallManager locations and regions for video.**
- **Configure the Cisco IP Phones in Cisco CallManager for video.**
- **During the installation process, wait until you are prompted to plug in the Cisco VT Camera.**

© 2005 Cisco Systems, Inc. All rights reserved. CPT2 v4.1—2-33

Module Summary

This topic summarizes the key points discussed in this module.

Module Summary

Cisco.com

- **The use of video telephony in a Cisco CallManager environment requires additional components and configuration steps on the Cisco CallManager.**
- **Cisco VT Advantage software is installed on a PC. To use Cisco VT Advantage, enable video on an IP Phone in Cisco CallManager configuration.**

© 2005 Cisco Systems, Inc. All rights reserved.CP72 v4.1--2.1

This module described the characteristics of video calls, such as the media channels used in the video call, gave an overview of the protocols used for video calls, and covered the configuration of Cisco CallManager for video telephony and the requirements for managing bandwidth for video calls using Cisco CallManager and an H.323 gatekeeper. The module also covered the installation of Cisco VT Advantage, including the installation of Cisco VT Advantage software on a PC and the configuration of Cisco CallManager for use with Cisco VT Advantage software.

References

For additional information, refer to these resources:

- Cisco Systems Inc. *Cisco IP Video Telephony Solution Reference Network Design (SRND) for Cisco CallManager 4.0*.
<http://www.cisco.com/univercd/cc/td/doc/solution/esm/iptele/vt40/>.
- Cisco Systems Inc. Cisco CallManager documentation.
http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm.
- Cisco Systems Inc. *Cisco CallManager System Guide, Release 4.1(3)*.
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_book09186a00803be4ee.html.

- Cisco Systems Inc. Cisco VT Advantage product overview.
<http://www.cisco.com/en/US/products/sw/voicesw/ps5662/index.html>.
- Cisco Systems Inc. *Cisco VT Advantage Administration Guide, (1.0(2))*.
http://www.cisco.com/en/US/products/sw/voicesw/ps5662/products_administration_guide_book09186a00803149e5.html.

Module 2 Self-Check

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module 2 Self-Check Answer Key.

- Q1) What is the video payload in a video call with 384 kbps and G.711? (Source: Introducing IP Video Telephony)
- A) 300 kbps
 - B) 320 kbps
 - C) 376 kbps
 - D) 384 kbps
- Q2) To enable video calls with a requested speed of 256 kbps, what would the recommended bandwidth setting be on Cisco CallManager locations? (Source: Introducing IP Video Telephony)
- A) 307.2 kbps
 - B) 256 kbps
 - C) 512 kbps
 - D) 281.6 kbps
- Q3) Which video codec will be used when an SCCP and H.323 device communicate? (Source: Introducing IP Video Telephony)
- A) H.263
 - B) H.264
 - C) Cisco wideband codec
 - D) H.261
- Q4) How is call admission control performed between Cisco CallManager clusters with a nongatekeeper-controlled intercluster trunk? (Source: Introducing IP Video Telephony)
- A) gateway
 - B) Cisco CallManager locations
 - C) gatekeeper
 - D) MCU
 - E) intercluster trunk
- Q5) Which device performs call admission control within a cluster? (Source: Introducing IP Video Telephony)
- A) gateway
 - B) Cisco CallManager locations
 - C) gatekeeper
 - D) MCU
 - E) intercluster trunk
- Q6) Which device is needed to integrate H.320 into the Cisco video solution? (Source: Introducing IP Video Telephony)
- A) MCU
 - B) video gateway
 - C) MGCP gateway
 - D) H.323 gatekeeper

- Q7) What does the icon of a video camera on the Cisco IP Phone status line mean? (Source: Configuring Cisco VT Advantage)
- A) The Cisco VT Camera is connected to the PC, and the PC is connected to the Cisco IP Phone
 - B) The Cisco IP Phone has web access.
 - C) The Cisco IP Phone is configured with video capabilities.
 - D) The Cisco IP Phone is receiving a video call.
- Q8) Into which port should the PC with Cisco VT Advantage client software installed be plugged? (Source: Configuring Cisco VT Advantage)
- A) Cisco Catalyst switch port
 - B) Cisco IP Phone access port
 - C) MCU port
 - D) videoconferencing port
- Q9) Which protocols are supported by Cisco VT Advantage? (Choose two.) (Source: Configuring Cisco VT Advantage)
- A) Cisco Audio Session Tunnel
 - B) FTP
 - C) RTP
 - D) SSH
 - E) TFTP
- Q10) Which SCCP Cisco endpoints are video-capable? (Choose three.) (Source: Configuring Cisco VT Advantage)
- A) Cisco IP Phone 7902
 - B) Cisco IP Phone 7910
 - C) Cisco IP Phone 7912
 - D) Cisco IP Phone 7920
 - E) Cisco IP Phone 7940
 - F) Cisco IP Phone 7960
 - G) Cisco IP Phone 7970
- Q11) Which of the following IP Phone settings are enabled by default in Cisco CallManager? (Choose two.) (Source: Configuring Cisco VT Advantage)
- A) video capabilities
 - B) PC port
 - C) Retry Video Call as Audio
 - D) video calling search space
 - E) AAR
- Q12) Video calls using 384 kbps need to be supported across a gatekeeper-controlled trunk. What value should be entered into the gatekeeper to support this bandwidth? (Source: Configuring Cisco VT Advantage)
- A) 192 kbps
 - B) 384 kbps
 - C) 512 kbps
 - D) 768 kbps

Module 2 Self-Check Answer Key

- Q1) B
- Q2) B
- Q3) A
- Q4) B
- Q5) B
- Q6) B
- Q7) C
- Q8) B
- Q9) A, C
- Q10) E, F, G
- Q11) B, C
- Q12) D

Module 3

Monitoring and Managing IP Telephony

Overview

To manage, maintain, and troubleshoot a Cisco CallManager system, administrators often need to analyze an enormous amount of data, various system behaviors, system performance, and so on. To gather, handle, and analyze all of these different kinds of information, administrators use supporting tools.

Module Objectives

Upon completing this module, you will be able to classify and use system maintenance tools that can be used in Cisco CallManager environment. This ability includes being able to meet these objectives:

- Use database tools and be able to classify other tools to maintain your Cisco CallManager system
- Use Microsoft Performance Monitor to display Cisco CallManager system and device statistics and use RTMT to monitor devices, call activities, servers, and services
- Configure and use Cisco CallManager Serviceability alarms and traces on Cisco CallManager systems for troubleshooting and maintenance
- Configure CAR
- Use additional management and monitoring tools

Lesson 3-1

Introducing Database Tools and Cisco CallManager Serviceability

Overview

Phone communication is one of the most critical services for businesses today. It is necessary to maintain and troubleshoot Cisco CallManager installations as fast as possible to reduce the risk of system outages. Administrators need tools to easily gather information about system behavior and reestablish broken connections.

This lesson introduces database tools that allow administrators to manage the Microsoft Structured Query Language (SQL) databases used by Cisco CallManager. It gives an overview of how to use Cisco CallManager Serviceability and other tools that can be used to maintain the Cisco CallManager system.

Objectives

Upon completing this lesson, you will be able to use database tools and classify other tools to maintain your Cisco CallManager system. This ability includes being able to meet these objectives:

- Examine the database structure and replication status and reactivate broken database connections
- Identify the purpose of the major services that Cisco CallManager Serviceability provides
- Explain how to use the Control Center to start and stop services
- Explain how to use the Service Activation window tools to enable and disable services
- Classify the tools used to monitor Cisco CallManager by their function

Database Management Tools

This topic describes tools to maintain Cisco CallManager Microsoft SQL 2000 database.

Database Services

Cisco.com

- **Cisco CallManager uses Microsoft SQL 2000 Enterprise to store:**
 - System configuration
 - Device configuration
 - CDRs
- **One member of cluster (publisher) replicates data to all other members (subscribers)**

```
graph TD; Admin[Admin Page] --> Publisher[(Publisher)]; Publisher --> Subscriber1[(Subscriber)]; Publisher --> Subscriber2[(Subscriber)];
```

© 2005 Cisco Systems, Inc. All rights reserved.CIPT2 v4.1-3.3

On Cisco CallManager systems, Microsoft SQL 2000 Enterprise databases are used to store system and device configuration as well as Call Detail Records (CDRs).

To maintain data consistency throughout the cluster, the publisher database server uses one-way, or unidirectional, replication to each subscriber. All information is stored on one server (the publisher server) and replicated to the other servers (subscriber servers) in the cluster. Replicating the SQL database is a core function inside Cisco CallManager clusters.

Configuration changes on Cisco CallManager systems are possible only while the publisher server is available. To make sure that CDRs are written even if the publisher server is offline, every server stores CDR information locally in flat files.

Cisco CallManager writes information to the publisher database only if Cisco CallManager web components are installed or Cisco CallManager Administration is performed directly on the publisher server. All entries that are made using the Cisco CallManager Administration page of the subscriber are written to the database on the publisher server. If the publisher is down, no updates can be made in the Cisco CallManager Administration page of the subscriber server.

When you are building a publisher server, Cisco CallManager itself may or may not be installed. If the publisher server does not have Cisco CallManager installed, Cisco refers to the server as a *glass house*. This configuration could be the best solution in large clusters.

The publisher occasionally acts as a backup system for the configuration. This configuration is typically used only in smaller clusters.

The publisher (either running Cisco CallManager or not [glass house]) holds the only copy of the database that is allowed to be written to. All subscribers replicate with the database of the publisher only, so they are in read-only mode.

CDR records are *not* written into a database of the subscriber, but they are written locally in *transaction files* at the subscribers (but not directly in the CDR database). Those files are periodically processed and inserted in the Microsoft SQL 2000 database by the CDR Insert service on the publisher server. If the publisher server is down, transaction files reside on the subscriber server to be processed as soon as the publisher is available again. After CDRs are processed, they are replicated from publisher to subscriber database.

Database Management Tools Overview

Cisco.com

- **Tools:**
 - **Microsoft SQL 2000 Enterprise Manager**
 - **DBLHelper**
- **Functions:**
 - **Verify proper working of databases**
 - **Examine database structure and replication**
 - **Reestablish replication between a publisher and a subscriber**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-3.4

There are two tools to maintain the Cisco CallManager database services that are based on Microsoft SQL 2000:

- **Microsoft SQL 2000 Enterprise Manager:** Provided by Microsoft and included in each Microsoft SQL 2000 installation
- **DBLHelper:** Provided by Cisco and needs to be requested from Cisco Technical Assistance Center (TAC) to resolve Cisco CallManager database issues

Both tools allow administrators to verify proper working of Cisco CallManager Microsoft SQL 2000 databases. Microsoft SQL 2000 Enterprise Manager and DBLHelper can be used when administrators need to examine the database structure and replication, and can sometimes be used to reactivate broken database connections.

In many cases, the reason for a broken database connection is publisher downtime. For example, administrators may take the publisher off the network to perform a software upgrade and restore it later.

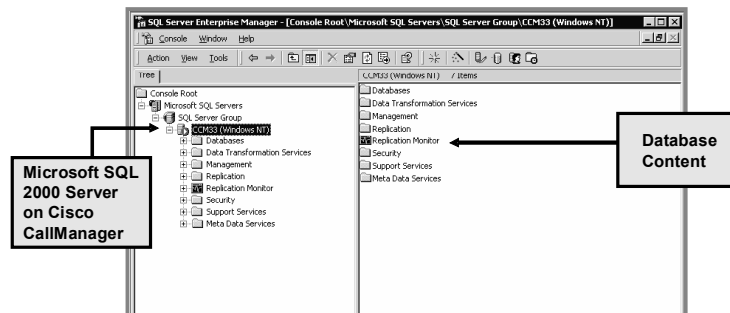
Note After reloading a Cisco CallManager publisher server, verify the database connection. A broken connection would not cause any obvious problem in system activity. Usually, users become aware of a broken connection only if the publisher becomes unresponsive again and any system changes are lost—for example, call forwarding instructions that are months out of date are active or newly added phones are unavailable.

When you are troubleshooting Cisco CallManager SQL databases, it is beneficial to use both tools together.

Microsoft SQL 2000 Enterprise Manager

Cisco.com

SQL Server Enterprise Manager is part of Microsoft SQL 2000 Enterprise.



© 2005 Cisco Systems, Inc. All rights reserved.

C:PT2 v4.1—3-6

Microsoft SQL 2000 Enterprise Manager is included in the Microsoft SQL 2000 Enterprise software; choose **Start > Programs > Microsoft SQL Server > Enterprise Manager**. It is the primary administrative tool for Microsoft SQL Server 2000 and provides a Microsoft Management Console (MMC)-compliant user interface that allows users to do the following:

- Define groups of servers running SQL Server
- Register individual servers in a group
- Configure all SQL Server options for each registered server
- Create and administer all SQL Server databases, objects, logins, users, and permissions in each registered server
- Define and execute all SQL Server administrative tasks on each registered server
- Design and test SQL statements, batches, and scripts interactively by invoking SQL Query Analyzer
- Invoke the various wizards defined for SQL Server

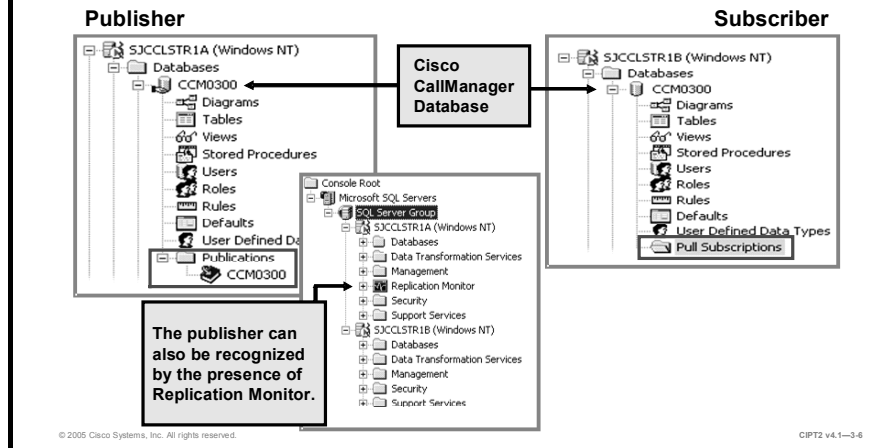
Note Because the Cisco CallManager installation includes the database and database structure needed for Cisco CallManager servers, it is not necessary to create new databases.

Caution Do not change the structure of the Cisco CallManager database. The Cisco CallManager will malfunction or, in the worst case, stop responding.

Using Enterprise Manager to Determine Server Function

Cisco.com

Microsoft SQL Enterprise Manager displays different information on publishers and on subscribers.



The Microsoft SQL database name of Cisco CallManager is CCM03xx, where xx starts at 00 and increases incrementally with each Cisco CallManager upgrade (for example, upgrading from release 4.0 to 4.1).

Microsoft SQL Server 2000 Enterprise Manager provides two ways to determine whether a server is the publisher or the subscriber. One method is to expand the hierarchy down to the database—Microsoft SQL Servers\SQL Server Group\<Server_Name>\Databases\CCM03xx:

- For a publisher, a Publications folder is displayed in the Database browse list. To see all of the subscribers, choose CCM03xx.
- For a subscriber, a Pull Subscriptions folder is displayed in the Database browse list.

The second way to determine whether the server is the publisher or subscriber is to check whether the Replication Monitor is present on the specific Microsoft SQL server. The Replication Monitor is present only on the publisher and monitors the status of database replication between the publisher and the subscribers.

DBLHelper

Cisco.com

- **DBL Helper is a Cisco tool for reestablishing replication between a publisher and a subscriber.**
 - **Republishes or reinitializes replication**
 - **Shows the current status of the SQL databases**
 - **Indicates whether there is a DNS entry or a LMHOST file entry to match IP addresses with server names**
- **If DBLHelper cannot repair the SQL replication, you can consider using Microsoft SQL Enterprise Manager:**
 - **Far more complex**
 - **Needs considerable experience with Microsoft SQL**

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1—3.7

In the event that the subscriber stops replicating data from the publisher, you need to rebuild the relationships between the publisher and subscriber. The DBLHelper utility, a tool provided by Cisco, republishes or reinitializes a nonfunctioning subscription between the publisher and the subscriber databases.

For DBLHelper to work, the SQL account password and administrative rights must be the same on the publisher and the subscriber.

Microsoft SQL 2000 Enterprise Manager could also be used to recreate broken database connections between Cisco CallManager servers in the cluster, but this process is far more complex than using DBLHelper. The recommendation is to first try repairing the replication using DBLHelper. Only if DBLHelper cannot fix the problem you should use the Microsoft SQL 2000 Enterprise Manager. For more information on how to use the Microsoft SQL 2000 Enterprise Manager to repair replications, search for “Reestablishing a Broken Cisco CallManager Cluster SQL Subscription” on Cisco.com.

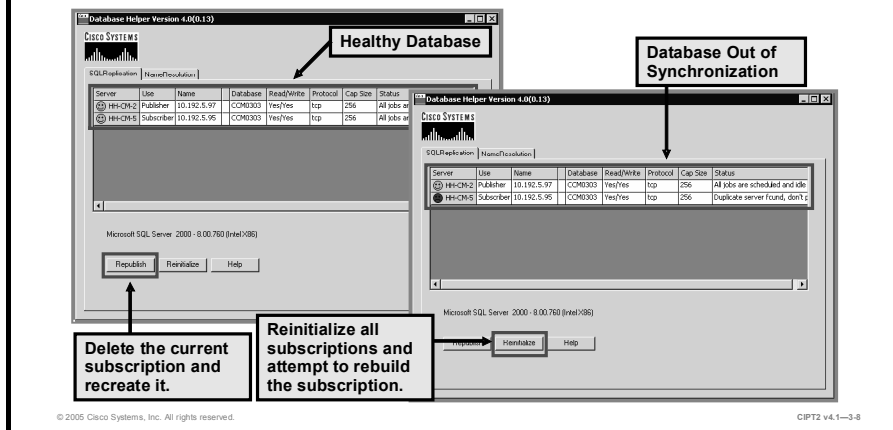
Even though most documents returned by the search (such as http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a0080094aeb.shtml or http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00801e7ddf.shtml) refer to Cisco CallManager Release 3.x, they also apply to Cisco CallManager Release 4.x.

Note If you are upgrading from an earlier version of Cisco CallManager, DBLHelper.exe is usually located on the Cisco CallManager server in the C:\Program Files\Cisco Systems, Inc\Cisco CallManager Upgrade Assistant\DbReplCheck folder. Otherwise, contact Cisco TAC for the latest version of DBLHelper.

DBLHelper Window

Cisco.com

The DBLHelper window shows the current status of database replication.



In the figure, DBLHelper shows two different states of Cisco CallManager Microsoft SQL 2000 databases. On the left, running DBLHelper.exe found that the replication was working. This status is depicted by the two green smile icons.

On the right, a red (lower) smile icon indicates that databases are out of synchronization. In this case, database connections need to be reestablished.

Clicking the Republish button deletes the current subscription and recreates it. Clicking the Reinitialize button reinitializes all subscriptions and starts the snapshot agent. It also begins an attempt to rebuild the subscription with the current database. To get more information about the current tab, click the Help button, which shows some additional information.

Note If there is more than one subscriber and only one has a broken database connection, use the Republish button to republish only the broken connection. If you use the Reinitialize button, all subscriptions will be reinitialized, which could cause a long system outage.

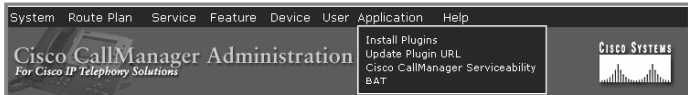
Cisco CallManager Serviceability Overview

This topic describes the Cisco CallManager Serviceability tool.

Cisco CallManager Serviceability Overview

Cisco.com

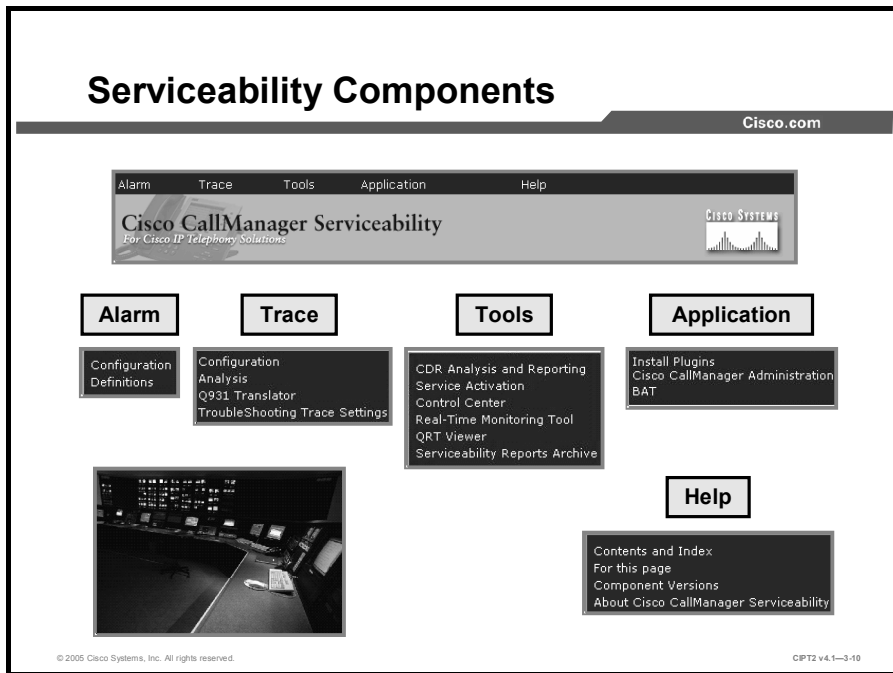
- **Used for Cisco CallManager maintenance**
- **Available on each Cisco CallManager**
- **Available from:**
 - **Application menu on the Cisco CallManager Administration page**
 - **Start > Programs > Cisco CallManager 4.1 > Cisco Service Configuration**
 - **https://<CallManager_IP>/CCMService/**



© 2005 Cisco Systems, Inc. All rights reserved. CPT2 v4.1-3-9

The Cisco CallManager Serviceability tool is available on each Cisco CallManager. It is the main tool used by administrators to maintain the Cisco CallManager installation.

To access Cisco CallManager Serviceability tool, choose the **Application** menu in Cisco CallManager Administration, choose **Start > Programs > Cisco CallManager 4.1 > Cisco Service Configuration** from the Cisco CallManager system, or use a browser to go directly to **https://<CallManager_IP>/CCMService**.



Cisco CallManager Serviceability provides these services:

- Alarm
- Trace
- Tools
- Application
- Help

Alarm

The Alarm service stores information about Cisco CallManager service events for troubleshooting and provides alarm message definitions. Alarms can be forwarded to trace files, Microsoft Windows 2000 Event Viewer, and a syslog server for further analysis:

- With the Configuration menu item, the Cisco CallManager Serviceability alarms allow configuration of Cisco CallManager to write an event to a trace file or the Windows 2000 Event Viewer when an incident occurs, such as the failure of a telephone to register. Alarms for Cisco CallManager servers can be configured in a cluster or for the services in each server.
- The Definitions application contains alarm definitions and the recommended actions in a Microsoft SQL Server 2000 database. The system administrator can search the database for the definitions of all alarms. Definitions include the alarm name, description, recommended action, severity, parameters, and monitors.

Trace

The Trace service allows you to save detailed log of Cisco CallManager events for troubleshooting system problems. Trace data can be configured, collected, and analyzed:

- Use the Configuration application to specify the trace parameters; for example, the Cisco CallManager server within the cluster, the Cisco CallManager service on the server, the debug level, and the specific trace fields.
- Use the Analysis application to provide greater trace detail on a signal distribution layer (SDL) trace, system diagnostic interface (SDI) trace, a Cisco CallManager service type, or the time and date of a trace. You can choose a specific log file from the list and choose information from that log file, such as host address, IP address, trace type, and request a device name.
- The Q.931 Translator application filters incoming data from Cisco CallManager SDI logs and translates the data into Cisco IOS messages. The Q.931 Translator application displays the message in the message translator interface.
- Use the Troubleshooting Trace application to choose the services in Cisco CallManager for which troubleshooting trace settings, which are predetermined in the alarms configuration, need to be set.

Tools

The Tools service offers these applications:

- The CDR Analysis and Reporting (CAR) application supports analysis and reporting of CDRs. CAR generates reports for quality of service (QoS), traffic, and billing information.
- The Service Activation application can activate and deactivate all of the Cisco CallManager services for all Cisco CallManager servers.
- The Control Center application allows starting, stopping, and viewing the status of Cisco CallManager services.
- The Real-Time Monitoring Tool (RTMT) application monitors the real-time behavior of all components in a Cisco CallManager cluster and displays on-screen feedback through a Java-based application.
- The QRT Viewer application allows filtering, formatting, and viewing problem reports. Cisco IP Phones can be configured with a Quality Report Tool (QRT) softkey so that users can report problems with IP Phone calls (for example, poor quality). When users press the QRT softkey on the IP Phone, they are presented with a list of problem categories. Users can then choose the appropriate problem category, and the system logs the event in an Extensible Markup Language (XML) file.
- The Serviceability Reports Archive application generates five daily reports in Cisco CallManager Serviceability: Device Statistics, Server Statistics, Service Statistics, Call Activities, and Alerts. Each report provides a summary that consists of various charts that display the statistics for that particular report.

Application

The Application service in Cisco CallManager Serviceability offers several applications.

- The Install Plugins application can help to extend the functionality of Cisco CallManager by providing links to software plug-ins that are either installed in Cisco CallManager itself or on a client PC.

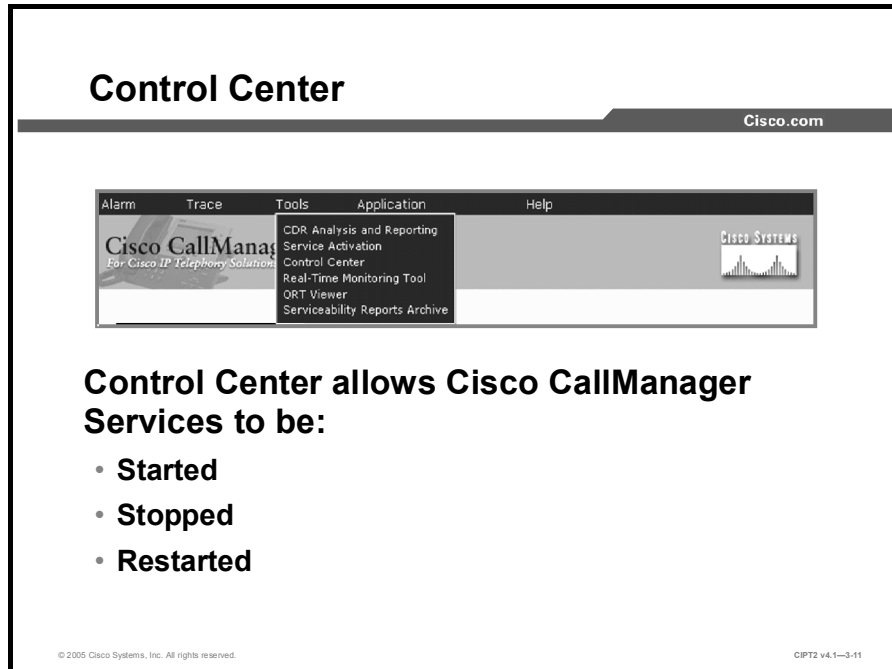
- The Cisco CallManager Administration menu item provides a convenient, direct link to the Cisco CallManager Administration page.
- The Bulk Administration Tool (BAT) application adds multiple telephones and users to Cisco CallManager and performs bulk modifications.

Help

The Help service provides online assistance for every option in Cisco CallManager Serviceability. Moreover, it can be used to display the latest installed component version information for all Cisco CallManager servers in the cluster.

Control Center

This topic describes how the Cisco CallManager Control Center is used.



On the Control Center, Cisco CallManager services can be started, stopped, or restarted. For example, restarting a Cisco CallManager service could be necessary if you change central Cisco CallManager functionalities, such as intercluster trunks or intersite bandwidth settings.

Control Center (Cont.)

Cisco.com

Control Center Service Activation

Server: 10.192.5.97
Status: Ready

Start Stop Restart

Service Name	Status	Activation Status
NT Service		
<input type="radio"/> Cisco CallManager	▶	Activated
<input type="radio"/> Cisco Tftp	▶	Activated
<input type="radio"/> Cisco Messaging Interface	▶	Activated
<input type="radio"/> Cisco IP Voice Media Streaming App	▶	Activated
<input checked="" type="radio"/> Cisco CTIManager	▶	Activated
<input type="radio"/> Cisco Telephony Call Dispatcher	▶	Activated
<input type="radio"/> Cisco MOH Audio Translator	▶	Activated
<input type="radio"/> Cisco RIS Data Collector	▶	Activated
<input type="radio"/> Cisco Database Layer Monitor	▶	Activated
<input type="radio"/> Cisco CDR Insert	▶	Activated
<input type="radio"/> Cisco Extended Functions	▶	Activated
<input type="radio"/> Cisco Serviceability Reporter	▶	Activated
<input type="radio"/> Cisco CTL Provider	▶	Deactivated
<input checked="" type="radio"/> Cisco Certificate Authority Proxy Function	▶	Deactivated
Tomcat Web Service		
<input type="radio"/> Cisco Extension Mobility	N/A	Activated
<input type="radio"/> Cisco IP Manager Assistant	N/A	Activated
<input type="radio"/> Cisco WebDialer	N/A	Activated

© 2005 Cisco Systems, Inc. All rights reserved. CPT2 v4.1—3-12

To start, stop, or restart a service, first select the service and then start, stop, or restart it by clicking the appropriate button.

The status column shows whether a service is started (a Right arrow in the Activation Status column) or stopped (a square in the status column). In addition, the Activation Status column tells how the service is configured. A status of Activated or Deactivated indicates whether the service is configured to be started at Windows startup.

Note Services with a status shown as Deactivated and Started are not activated in Service Activation but are still started at Windows startup.

You cannot start Cisco Tomcat web services using the Control Center. To start them, you could use the Microsoft Windows 2000 Server Services Management Console. Additionally, with Cisco CallManager Release 4.0 or later, Cisco Tomcat Web Application Manager allows you to start, stop, or restart Tomcat services. To access Tomcat Web Application Manager, go to http://<CallManager_IP>/manager/list.

Starting and stopping a Cisco CallManager service causes all Cisco IP Phones and gateways that are currently registered to that Cisco CallManager service to fail over to their secondary Cisco CallManager service. Starting and stopping a Cisco CallManager service causes other installed applications (such as Conference Bridge or Cisco Messaging Interface) that are homed to that Cisco CallManager to start and stop as well.

Note If you are upgrading Cisco CallManager, all services are stopped during the upgrade process. Services that had been started before the upgrade began are started again afterward. Those that had not been started remain deactivated. Service configurations are not lost during the upgrade process.

Caution Stopping a Cisco CallManager service also stops call processing for all devices that are controlled by that service. When a Cisco CallManager service is stopped, active calls from an IP Phone to another IP Phone continue; calls in progress from an IP Phone to a Media Gateway Control Protocol (MGCP) gateway also continue, while other types of calls, such as calls to an H.323 gateway, are dropped.

Service Activation

This topic describes how to manage services on Cisco CallManager systems.

Service Activation

Cisco.com

- **Cisco CallManager Service Activation allows you to activate and deactivate specific Cisco CallManager services.**
- **Services MMC is used to manage common Windows services.**

Service Activation

Servers: 10.192.5.97

Service Name	Activation Status
<input type="checkbox"/> Cisco CallManager	Activated
<input type="checkbox"/> Cisco Tftp	Activated
<input type="checkbox"/> Cisco Messaging Interface	Activated
<input type="checkbox"/> Cisco IP Voice Media Streaming App	Activated
<input type="checkbox"/> Cisco CTManager	Activated
<input type="checkbox"/> Cisco Telephony Call Dispatcher	Activated
<input type="checkbox"/> Cisco MCH Audio Translator	Activated
<input type="checkbox"/> Cisco SIS Data Collector	Activated
<input type="checkbox"/> Cisco Database Layer Monitor	Activated
<input type="checkbox"/> Cisco CDR Insert	Activated
<input type="checkbox"/> Cisco Extended Functions	Activated
<input type="checkbox"/> Cisco Serviceability Reporter	Activated
<input type="checkbox"/> Cisco CTL Provider	Deactivated

Services

Name	Description	Status	Start	Type	Path
Background Intelligent Transfer Service	Transfers files in the background.	Stopped	Automatic	LocalSystem	
Device Driver Installer	Device Driver Installer	Stopped	Automatic	LocalSystem	
Cisco CallManager		Started	Automatic	SCCMService	
Cisco CDR Insert and Reporting Scheduler	The reporting scheduler.	Started	Automatic	SCCMService	
Cisco CDR Insert		Started	Automatic	SCCMService	
Cisco Certificate Authority Proxy Function		Started	Automatic	SCCMService	
Cisco CT Manager		Started	Automatic	SCCMService	
Cisco CT Provider		Stopped	Automatic	LocalSystem	
Cisco Database Layer Monitor		Started	Automatic	SCCMService	
Cisco Database Layer Monitor		Started	Automatic	SCCMService	
Cisco Extended Functions		Started	Automatic	SCCMService	
Cisco IP Voice Media Streaming App		Started	Automatic	SCCMService	
Cisco Messaging Interface		Started	Automatic	SCCMService	
Cisco MCH Audio Translator		Started	Automatic	SCCMService	
Cisco SIS Data Collector		Started	Automatic	SCCMService	
Cisco Serviceability Reporter		Started	Automatic	LocalSystem	
Cisco Serviceability Reporter		Started	Automatic	SCCMService	
Cisco Telephony Call Dispatcher		Started	Automatic	SCCMService	
Cisco TFTP		Started	Automatic	SCCMService	
Network	Supports Outlook.	Stopped	Automatic	LocalSystem	
Remote Event System	Provides system events.	Started	Automatic	LocalSystem	
Computer Browser	Hardware-aware browser.	Started	Automatic	LocalSystem	
RPC Endpoint Mapper		Started	Automatic	LocalSystem	

© 2005 Cisco Systems, Inc. All rights reserved. CIPT2 v4.1-3-13

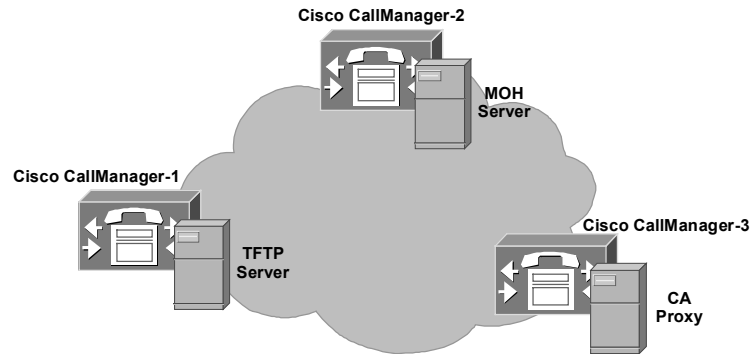
There are two tools that allow you to manage services running on the Cisco CallManager system:

- The Cisco CallManager Serviceability Service Activation tool is used to activate or deactivate specific services on Cisco CallManager.
- The Services MMC is used to handle common Windows services. The Services MMC can be found at Start > Settings > Control Panel > Administrative Tools on the Cisco CallManager system.

Distributed Service Provision

Cisco.com

Service Activation can be used to distribute services across Cisco CallManager servers within the cluster.



© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-3-14

To optimize the performance of Cisco CallManager servers within a cluster, you can distribute services to servers across the cluster. For example, place the TFTP server service on one server, the Certificate Authority Proxy Function (CAPF) service on another server, and music on hold (MOH) services on a third server where no Cisco CallManager service is running, and so on.

Distribution of services can also be used for security purposes. Some services (such as those that provide IP Phone services with access to the Internet) must be exposed to the outside for proper operation, while others, such as the Cisco CallManager service, should not be exposed. If the exposed server is under attack, the attack would not have any impact on the other servers (for instance, the server routing calls that is running the Cisco CallManager service).

Service Activation Page

Cisco.com

Service Activation Control Center

Servers Server: 10.192.5.97
Status: Ready
Update Set Default

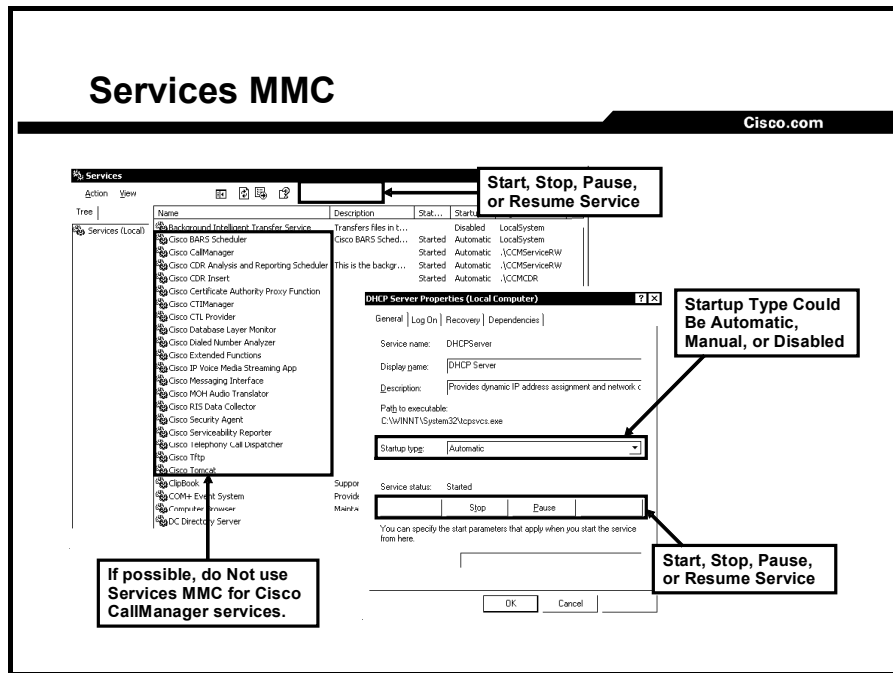
Service Name	Activation Status
NT Service	
<input checked="" type="checkbox"/> Cisco CallManager	Activated
<input checked="" type="checkbox"/> Cisco Tftp	Activated
<input checked="" type="checkbox"/> Cisco Messaging Interface	Activated
<input checked="" type="checkbox"/> Cisco IP Voice Media Streaming App	Activated
<input checked="" type="checkbox"/> Cisco CTIManager	Activated
<input checked="" type="checkbox"/> Cisco Telephony Call Dispatcher	Activated
<input checked="" type="checkbox"/> Cisco MOH Audio Translator	Activated
<input checked="" type="checkbox"/> Cisco RIS Data Collector	Activated
<input checked="" type="checkbox"/> Cisco Database Layer Monitor	Activated
<input checked="" type="checkbox"/> Cisco CDR Insert	Activated
<input checked="" type="checkbox"/> Cisco Extended Functions	Activated
<input checked="" type="checkbox"/> Cisco Serviceability Reporter	Activated
<input type="checkbox"/> Cisco CTL Provider	Deactivated
<input type="checkbox"/> Cisco Certificate Authority Proxy Function	Deactivated
Tomcat Web Service	
<input checked="" type="checkbox"/> Cisco Extension Mobility	Activated
<input checked="" type="checkbox"/> Cisco IP Manager Assistant	Activated
<input checked="" type="checkbox"/> Cisco WebDialer	Activated

© 2005 Cisco Systems, Inc. All rights reserved. CPT2 v4.1—3-15

Services that should be available on the Cisco CallManager server can be selected in the Service Activation window.

Note If the Cisco CallManager and Cisco CTIManager services are deactivated on the Service Activation page, the Cisco CallManager where the service was deactivated no longer exists in the database. This means that the Cisco CallManager cannot be chosen for configuration operations in Cisco CallManager Administration because it will not be displayed in the GUI. If the services are then reactivated on the same Cisco CallManager, the database recreates the Cisco CallManager and adds a "CM_" prefix to the server name or IP address; for example, if the Cisco CallManager or CTIManager service is reactivated on a server with an IP address of 10.192.5.97, then "CM_10.192.5.97" is displayed in Cisco CallManager Administration. The Cisco CallManager with the new "CM_" prefix can now be chosen in Cisco CallManager Administration.

Caution When you deactivate the Cisco CallManager service, the server is removed from Cisco CallManager groups but *not* added back after reactivation. So after activation or reactivation, you must add the server to Cisco CallManager groups, otherwise no devices will register to it.



The Services MMC can be used to enable, disable, restart, pause, or resume Microsoft Windows services, including all Cisco CallManager services.

Caution Even if it is possible, do not use the Services MMC to manage Cisco CallManager services that could be handled using Cisco CallManager Serviceability, because doing so could harm the stability and functionality of the Cisco CallManager system.

To change the startup type of a service, perform these tasks:

- Step 1** From the Services MMC, double-click the service.
- Step 2** Choose the correct startup type from the **Startup type** drop-down menu.
- Step 3** Click **Apply** to save the settings.

Caution Disabling Windows services can cause malfunctioning or cause serious problems on the system. Only services that are really not needed on a particular server should be disabled (for example, Dynamic Host Configuration Protocol [DHCP] server if you are using DHCP server on a router or another server).

Tools Overview

This topic gives an overview of tools that can be used to maintain the Cisco CallManager system.

Tools Overview

Cisco.com

- **Administrators need tools to easily maintain their Cisco CallManager.**
- **Microsoft provides many tools that allow management of the Microsoft systems.**
- **Cisco provides many additional tools for Cisco CallManager management.**

© 2005 Cisco Systems, Inc. All rights reserved. CPT2 v4.1—3-17

There are several tools that make administration easier when you are managing Cisco CallManager system status or configuration. Some of those tools are provided by Cisco Systems, while others are Microsoft tools included in the Windows 2000 Server operating system used by Cisco CallManager.

Tools Overview (Cont.)

Cisco.com

	Function	Device
Microsoft SQL 2000 Enterprise Manager	Verify proper working of databases	Any Microsoft SQL 2000 Server in the domain
DBLHelper	Verify proper replication between databases	Cisco CallManager publisher server
Services MMC	Manage services	Actual Windows 2000 server
Microsoft Event Viewer	Identify system-level events and errors	Actual Windows 2000 server
Microsoft Performance Monitor	Monitor system and device statistics	Actual Windows 2000 server

© 2005 Cisco Systems, Inc. All rights reserved.

CIP72 v4.1-3-18

Microsoft SQL 2000 Enterprise Manager can be used to verify the proper working of the databases and to evaluate the Microsoft SQL environment. This tool can be used on any Windows 2000 Server in the domain to access the SQL database. By default, it is installed on every server that has Microsoft SQL 2000 installed.

DBLHelper allows the verification and recreation of the replication process between the Cisco CallManager publisher and subscriber databases. This tool needs to be run on the Cisco CallManager publisher server. Beginning with CallManager Release 4.0, this tool is available only from Cisco TAC.

The Services MMC allows for management of services on Windows 2000 Server. Each Windows 2000 Server has its own Services MMC preinstalled. Even though administrators can create their own MMC to manage services on any other system, it is recommended that you use the preinstalled MMC on each server locally. Otherwise, you risk confusion, because all the servers look the same.

Microsoft Event Viewer allows identification of system-level events and errors. Each event and error of the Windows 2000 system is stored in Microsoft Event Viewer. Different kinds of messages are grouped into a system log, an application log (where most information related to Cisco CallManager is stored), and a security log. Because Event Viewer is also an MMC snap-in, an MMC that includes Event Viewer can be created on any system but, it is not recommended to manage remote systems.

Microsoft Performance Monitor shows system and application statistics and is available on every Microsoft Windows 2000 system. Although it is also an MMC snap-in for Microsoft Windows 2000 Server, it can be used only on the server itself because it uses an ActiveX control. To monitor performance statistics of remote systems, use the local snap-in as an alternative and include remote counters.

Tools Overview (Cont.)

Cisco.com

	Function	Device
RTMT Client	Real-time monitoring of Cisco CallManager system	Any PC on the network
Password Changer Tool	Change the CCMA administrator password	Cisco CallManager publisher server
CAR Tool	Analyze Cisco CallManager CDRs	Cisco CallManager Web page via browser
Dialed Number Analyzer	Analyze calls in a Cisco CallManager dial plan	Cisco CallManager Web page via browser
QRT	Create quality problem reports	Cisco CallManager Web page via browser

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1—3-19

The RTMT client allows you to monitor Cisco CallManager activities in real time. This Java-based tool can be installed on any Windows PC. It is available in the Install Plugins window of Cisco CallManager Serviceability.

The Password Changer tool available on the Cisco CallManager server allows changing the administrator passwords on Cisco CallManager systems. This tool needs to be run on Cisco CallManager publisher server.

The CAR tool allows analysis of CDRs written on Cisco CallManager. CAR is available from Cisco CallManager Serviceability and can be accessed using the Microsoft Internet Explorer web browser on any PC on the network.

Dialed Number Analyzer analyzes how inbound and outbound calls are handled in the Cisco CallManager call-routing configuration. It resides on the Cisco CallManager web server and can be accessed using Internet Explorer on any PC on the network.

QRT Viewer application allow you to filter, format, and view problem reports. It is located on the Cisco CallManager web server and can be accessed using Internet Explorer on any PC on the network.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Microsoft SQL 2000 Enterprise Manager and DBLHelper can be used to verify proper working of databases.**
- **Cisco CallManager Serviceability is used to manage the Cisco CallManager system.**
- **Control Center can be used to start, stop, or restart services related to Cisco CallManager.**
- **Service Activation and Services MMC allow you to manage all services on Cisco CallManager.**
- **There are many tools provided by Cisco and Microsoft that allow management and troubleshooting of the Cisco CallManager server.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIP12 v4.1-3-20

Monitoring Performance

Overview

Growing demands to the telephony systems increase hardware usage on the telephony system platform. If those demands rise too much, they could cause system overloads. Telephony systems are among those that most directly affect businesses, and overloads that lead to system outages could be extremely costly. Therefore, administrators must be able to monitor system performance.

This lesson covers tools that are used to monitor Cisco CallManager systems. Further, this lesson describes Microsoft tools that are available on the Windows system, Real-Time Monitoring Tool (RTMT) from Cisco, and how they work together.

Objectives

Upon completing this lesson, you will be able to use Microsoft Performance Monitor to display Cisco CallManager system and device statistics and use RTMT to monitor devices, call activities, servers, and services. This ability includes being able to meet these objectives:

- Define a performance object and counter and describe their interaction with Microsoft Performance Monitor and RTMT
- Use Microsoft Event Viewer to identify system-level events and errors
- Use Microsoft Performance Monitor to monitor system and device statistics
- Explain the major monitoring categories that RTMT provides
- Use the default RTMT configuration and create customized configuration profiles
- Identify components of the RTMT window

Performance Counters and Objects

This topic describes defines performance counters and objects and their interaction with Microsoft Performance Monitor and RTMT.

Performance Counters and Objects

Cisco.com

- **Performance counters enable you to track selected system performance data.**
- **Performance objects are specific areas of system functionality.**
- **Counters and objects can be used for:**
 - **System maintenance**
 - **System analysis**
 - **System troubleshooting**
- **Counters are based on:**
 - **System events**
 - **System utilization**

© 2005 Cisco Systems, Inc. All rights reserved. CIPT2 v4.1-3.3

Performance counters reflect the performance data of Cisco CallManager. A counter is a variable whose name is stored in the registry. Each counter is related to a specific area of system functionality. Examples include busy time of the processor, memory usage, and the number of bytes received over a network connection. Each counter is uniquely identified through its name and its path or location. In the same way that a file path includes drives, directories, subdirectories, and file names, a counter path consists of four elements: the machine, the object (for example, processor or IP), the object instance (type of counter value; for example, interrupt), and the counter name (special counter itself).

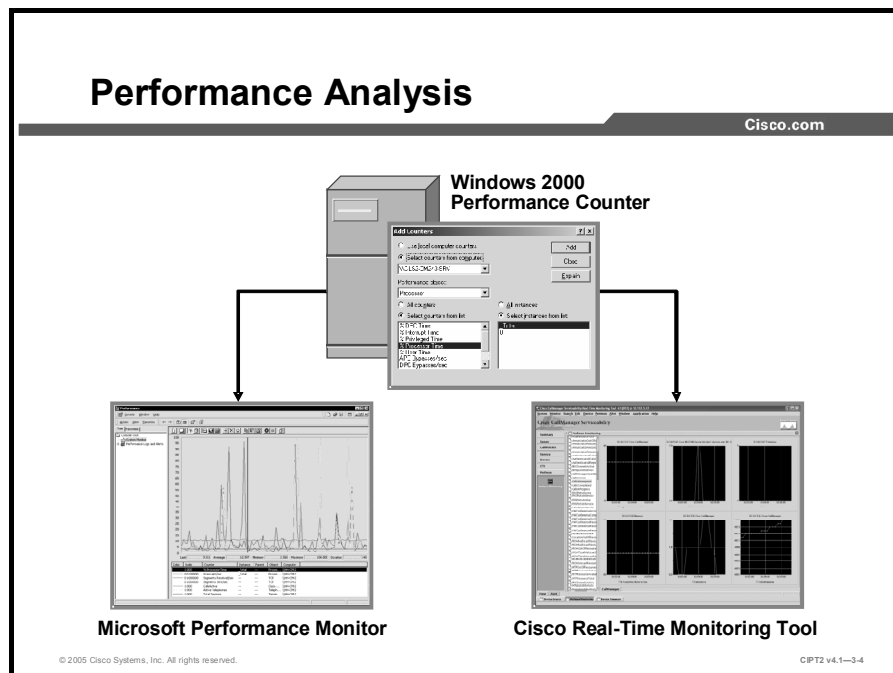
Performance counters and objects are ideal for administrators for system maintenance, analysis, and troubleshooting tasks:

- An administrator needs to reset a voice gateway. With performance counters, it is possible to watch the system until the last call is disconnected and then reset the gateway.
- A user reports that using Cisco CallManager Extension Mobility to log on to the phone takes a very long time. In analyzing the statistics produced with performance counter data, the administrator discovers high processor usage and memory allocation due to problems with processes on the system.
- An administrator is dealing with a slow system. The system engineer has to decide whether system expansion is necessary or whether the current extensive system usage is only a one-time situation. To find out, the administrator should watch system for a while.

Note All performance counter values are based on system events and utilization information provided by the Microsoft Windows 2000 platform.

Performance Analysis

Cisco.com



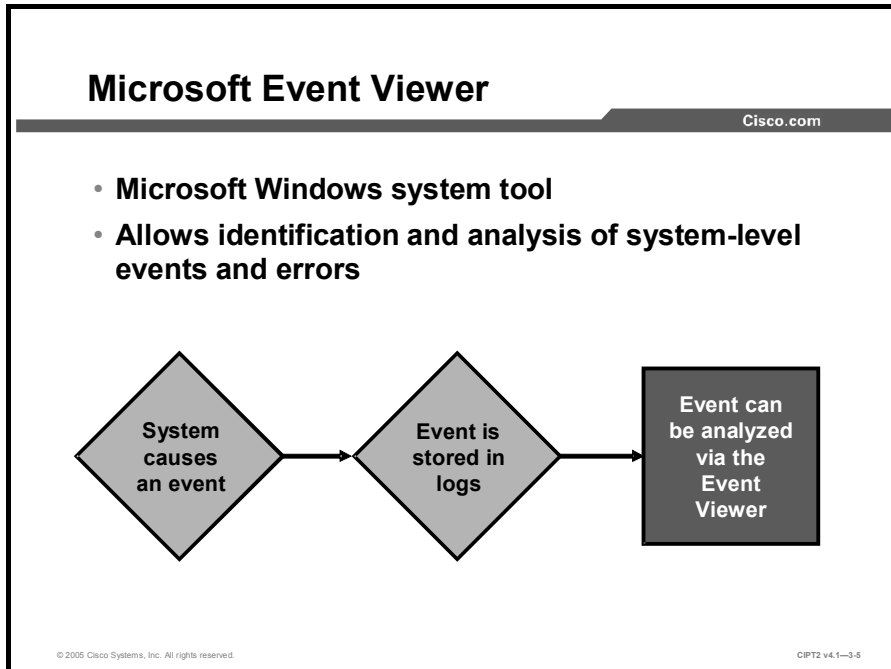
Microsoft Performance Monitor and Cisco RTMT use Windows 2000 performance counters to monitor the system. Microsoft Performance Monitor reports both general and specific information in real time, while RTMT monitors Cisco CallManager performance by periodically polling Windows 2000 performance counter values.

RTMT provides optimized monitoring of performance objects and devices related to Cisco CallManager. The device information includes device registration status, IP address, description, and model type. RTMT provides cluster-wide information that is stored in eight tables. The tables include IP Phones, gateway devices, media, H.323 devices, Session Initiation Protocol (SIP) trunks, hunt lists, computer telephony integration (CTI), and voice messaging.

RTMT also displays object and counter information that is kept by each Cisco CallManager node in the cluster. RTMT directly monitors the performance objects and counters.

Microsoft Event Viewer

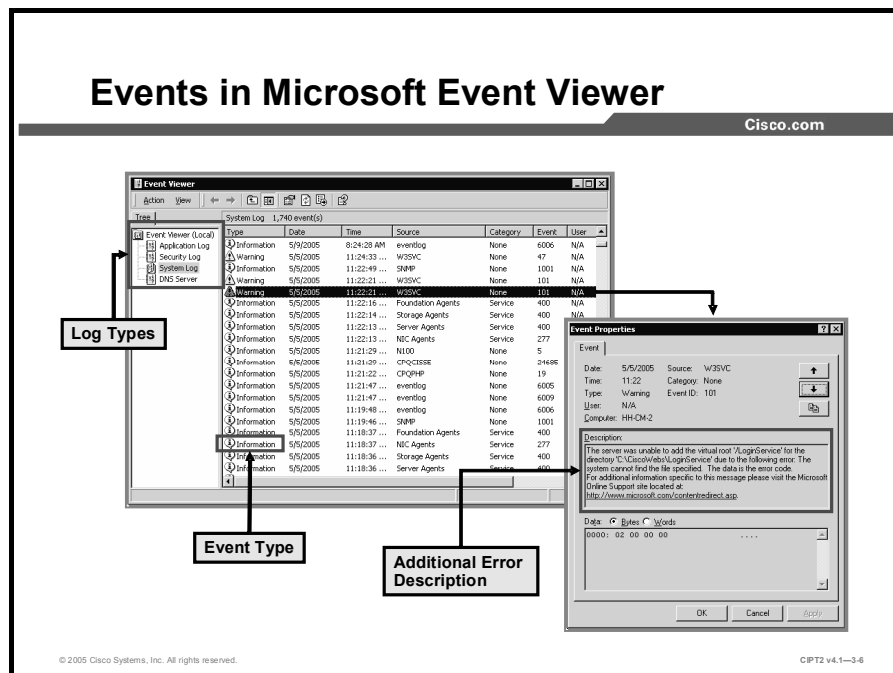
This topic describes how Microsoft Event Viewer works and how it is used.



Microsoft Event Viewer is a Microsoft Windows system tool. It is available by default on every Windows NT-based system (Windows NT, Windows 2000, Windows XP, and Windows 2003). Beginning with the introduction of Windows 2000, Microsoft Event Viewer has been based on Microsoft Management Console (MMC). It is possible to create an MMC that includes the Microsoft Event Viewer of each remote system. But keep in mind that using more than one Microsoft Event Viewer on one system often leads to confusion and is normally not recommended.

Windows stores information related to an event or error in Microsoft Event Viewer. Microsoft Event Viewer can be used to gather, identify, and analyze Microsoft Windows 2000 system events and information about hardware, software, and system problems. Because Cisco CallManager runs as a Windows service, information about Cisco CallManager events and errors can also be stored into Event Viewer.

Events in Microsoft Event Viewer



Microsoft Event Viewer, available at Start > Settings > Control Panel > Administrative Tools > Event Viewer, can help identify problems at the system level. For example, to pinpoint a problem, use Event Viewer to look for events involving Cisco CallManager Administration on the Internet Information Server (IIS) server.

Log Types

Microsoft Event Viewer uses log types to group different kinds of logs:

- **Application logs:** Contain events logged by applications or programs, such as Cisco CallManager.
- **System logs:** Report events logged by the Windows 2000 system components, such as the failure of an operating system component or driver.
- **Security logs:** Hold information records of security events. (Cisco CallManager does not report events in this log.)

Event Types

To classify events, the Microsoft Event Viewer provides three event types. Each is marked with its own icon. The Microsoft Event Viewer event types are as follows:

- **Error:** An indicator of a problem, such as the loss of data or failure to initialize properly
- **Warning:** An event that might indicate a problem or a future problem, such as when a service is stopped or started, which is not necessarily an error
- **Information:** System information messages that may include hostnames, the version of the database in use, or startup success

Microsoft Performance Monitor

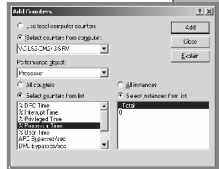
This topic describes Microsoft Performance Monitor and how it can be used to monitor the Cisco CallManager system.

Microsoft Performance Monitor Application

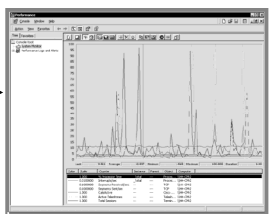
Cisco.com

- **Application that displays real time performance data of operating system and application components**
- **Can be used to collect Cisco CallManager statistics**

Windows 2000 Performance Counter



→



Microsoft Performance Monitor

© 2005 Cisco Systems, Inc. All rights reserved. CIPT2 v4.1-3-7

Microsoft Performance Monitor is a Windows 2000 Server application that uses Windows 2000 performance counters to create statistics. It displays the activities and status of the system. Microsoft Performance Monitor reports both general and specific information in real time. You can use Microsoft Performance Monitor to collect and display system and device statistics for any Cisco CallManager installation.

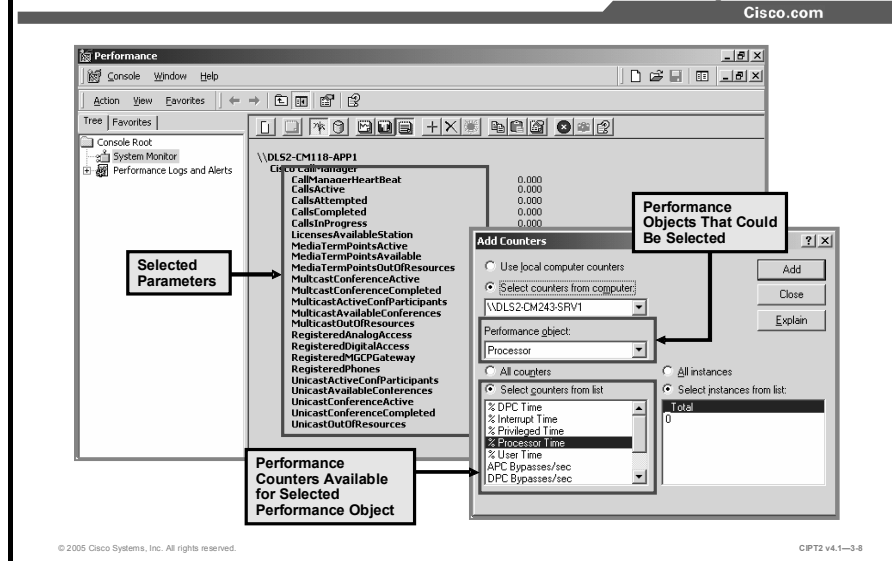
Microsoft Performance Monitor, like the Cisco CallManager Serviceability tool, monitors and logs resource counters from the Cisco CallManager nodes in the network and displays the counters in real time. The update interval could be set to a period between 1 second and 45 days.

Microsoft Performance Monitor can collect data from multiple systems at once and store it in a single log file. The monitor can then export this log file to a tab-separated values (TSV) file or a comma-separated values (CSV) file that you can view in most spreadsheet applications.

To access Microsoft Performance Monitor, choose **Start > Settings > Control Panel > Administrative Tools** and choose **Performance**.

Note Extensive monitoring (monitoring a very large number of counters and using short interval times) could cause rising processor usage. Therefore, it is recommended that you use Microsoft Performance Monitor only for special situations and not as a network management tool.

Microsoft Performance Monitor—Report



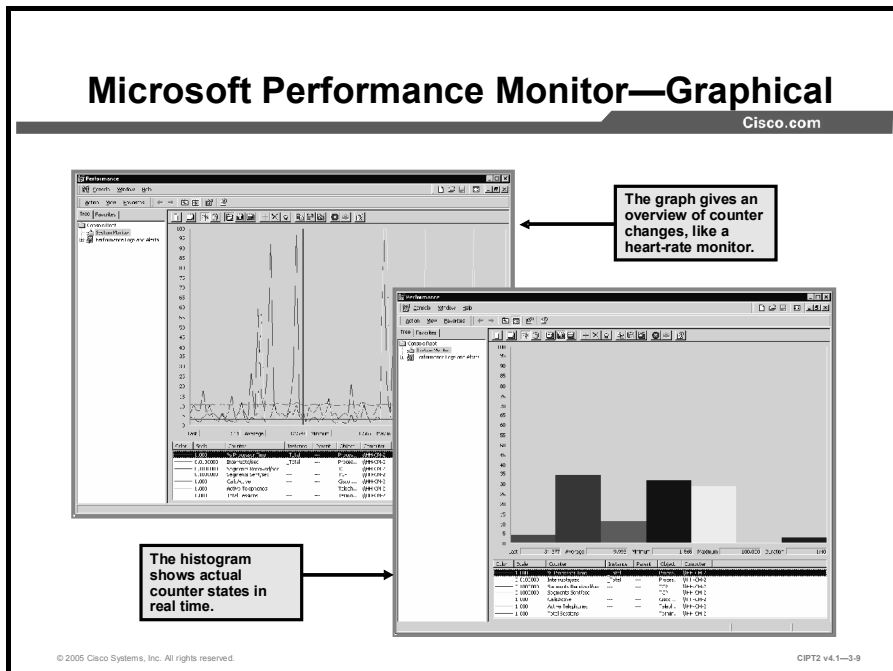
Microsoft Performance Monitor needs to be customized for the parameters related to monitoring Cisco CallManager by choosing the objects, counters, and instances to include.

Within Microsoft Performance Monitor, alarms can be enabled to report certain value thresholds. For example, the number of telephone devices active on Cisco CallManager can be set to a particular level. If the number of devices exceeds that level, the monitor sends a network message alert to the administrator or the person in charge. To create such an alert threshold, right-click **Performance Logs and Alerts > Alerts** and choose **New Alert Settings**.

Note Data collection must be enabled in Cisco CallManager for Microsoft Performance Monitor to collect data. To verify that data collection is enabled, check the current settings in the Cisco Real-Time Information Server (RIS) Data Collector Service Parameters Configuration window in Cisco CallManager Administration. By default, the Data Collection Enabled parameter is set to True.

Microsoft Performance Monitor—Graphical

Cisco.com



Microsoft Performance Monitor provides two kinds of graphical views for a visual overview of how the system is currently in use and how it changes:

- Graphs
- Histograms

Graphs

Graphs are ideal to see the current status of the counters and how they have changed over the most recent period. You can specify the period for status updates and include it in the graph. Using this tool is similar to using a heart-rate monitor. It displays the heartbeat of the monitored performance objects.

Histograms

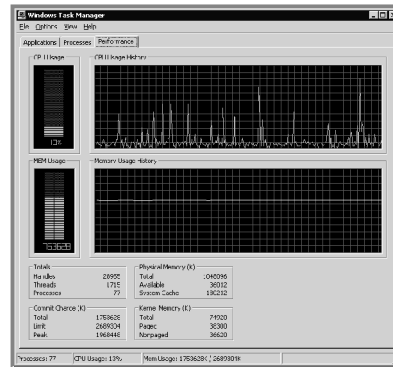
In contrast to graphs, the histogram view shows only the current status of the selected performance object counters. Because it uses only a single bar for each counter, the histogram view is ideal for monitoring many performance counters. To switch between the graph and histogram views, use the graph and histogram icons from the system monitor toolbar or press Ctrl-G (graph) and Ctrl-B (histogram) alternately.

Windows Task Manager

Cisco.com

Task Manager provides:

- Graphical view of CPU and memory usage
- Additional performance counter values in plain text



© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-3-10

In addition to Microsoft Performance Monitor, Windows Task Manager can be used to get a fast view of the base performance values of CPU and memory usage. The Performance tab of Task Manager shows the CPU and memory usage of the system as graph and histogram. Moreover, it provides some additional counter values, such as paged kernel memory in plain text. It is an ideal tool to get a quick impression of system health and activity, for example, if the system is working very slowly.

To access Windows Task Manager, right-click the taskbar or press Ctrl -Shift-Esc.

Note Windows Task Manager influences system performance because it also monitors all system processes and running programs. Therefore it is recommended that you use it only to get a snapshot of the current situation and not as for prolonged monitoring.

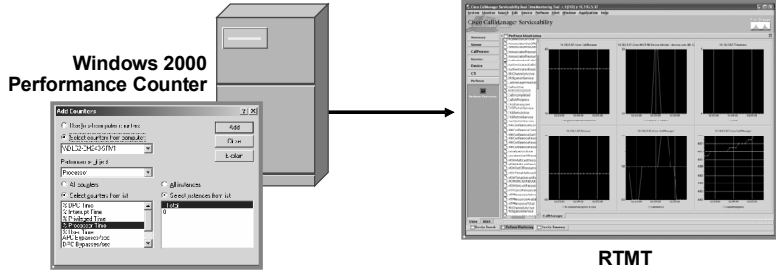
Real-Time Monitoring Tool Overview

This topic gives an overview of the RTMT.

RTMT Overview

Cisco.com

- **Java-based stand-alone tool**
- **Uses Windows 2000 performance counter values to monitor behavior of Cisco CallManager in real time**
- **Allows creation of personalized monitoring profiles**
- **Can generate e-mail alerts and daily reports**



RTMT

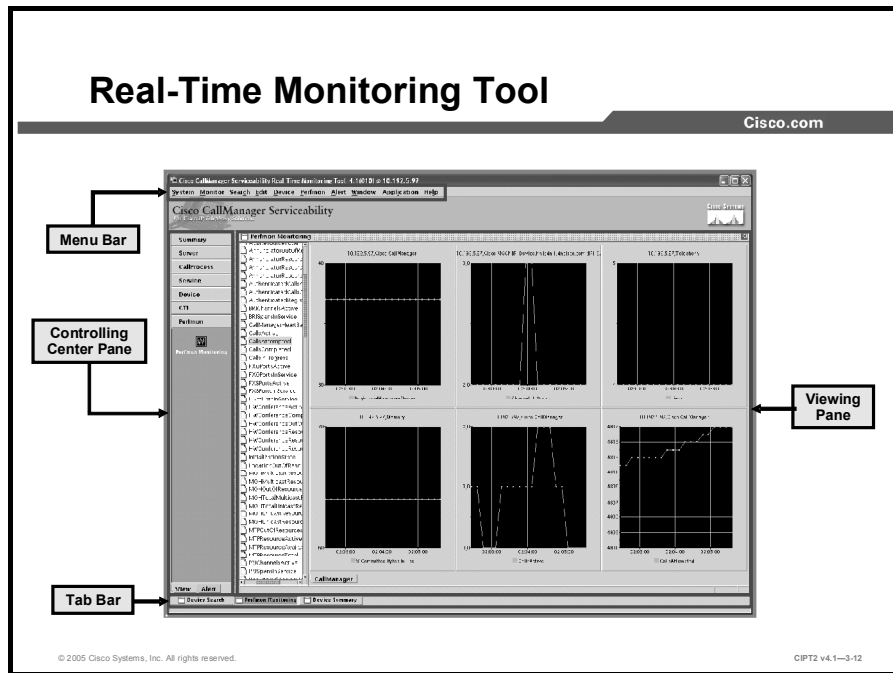
© 2005 Cisco Systems, Inc. All rights reserved. CPT2 v4.1-3-11

With Cisco RTMT, the Cisco CallManager Serviceability tool provides a client-side stand-alone Java plug-in that monitors real-time behavior of the components in a Cisco CallManager cluster. RTMT monitors a set of management objects by continuously polling the Windows 2000 performance counter values. It can generate various alerts in the form of e-mails for values that exceed or fail to reach user-configured thresholds. RTMT can also generate daily reports for these objects. The e-mail alerts work independently of the stand-alone Java front end. Therefore, it is not necessary to run the RTMT window all the time to grant e-mail notification.

To download RTMT, choose **Cisco CallManager RTMT** from the Cisco CallManager Install Plugins page in the Application menu of Cisco CallManager Administration and Cisco CallManager Serviceability.

After successful installation, you can launch RTMT by double-clicking the RTMT shortcut on the Windows desktop or by choosing Start > Programs > Cisco CallManager Serviceability > RTMT.

Note To reduce the impact on the Cisco CallManager server, it is strongly recommended that you run RTMT on an administrator PC and not locally on the Cisco CallManager server. Moreover, RTMT should not run constantly.



The RTMT application is divided into four parts:

- Menu bar
- Controlling center pane
- Viewing pane
- Tab bar

Menu Bar

The RTMT menu bar, located at the top of the RTMT window, uses drop-down menus that provide specific monitoring.

Controlling Center Pane

The controlling center pane, located on the left side of the window, includes the View tab and the Alert tab. The View tab includes several different monitoring categories, while the Alert tab offers only the Alert category.

On the View tab of the controlling pane, RTMT arranges the preconfigured monitoring objects into seven major categories:

- **Summary:** The Summary category shows the activities of several predetermined monitoring objects in the Cisco CallManager cluster, such as memory and CPU usage, registered phones, calls in progress, and active gateway ports and channels.
- **Devices:** The Devices category monitors phones, gateways, and media devices on each Cisco CallManager node and cluster. Monitored objects include the number of registered phones, gateways, and media resources for each Cisco CallManager node and cluster.
- **CallProcess:** The CallProcess category monitors all call activity for each Cisco CallManager node and cluster. Monitored objects include CallsAttempted, CallsCompleted, and CallsInProgress for each Cisco CallManager node and cluster.

- **Servers:** The Servers category monitors CPU usage, disk space usage, and critical services on each Cisco CallManager server. Monitored objects include CPU and memory usage on each server and the disk space usage for all logical drives on each server.
- **Services:** The Services category monitors CTIManager information for each CTIManager, Cisco TFTP server information, directory server information, and heartbeat rate information. Monitored objects include TotalTftpRequests and TotalTftpRequestsAborted.
- **CTI:** The CTI category provides CTI search and a CTIManager monitoring window that displays the number of open devices, lines, and CTI connections.
- **Perfmon:** The Perfmon category provides performance monitoring similar to Microsoft Performance Monitor.

Viewing Pane

In the viewing pane, located to the right of the controlling center pane and occupying most of the window area, RTMT displays the currently selected monitoring object.

Tab Bar

The tab bar, located at the bottom of the window, allows switching among all monitoring objects currently monitored in the viewing pane.

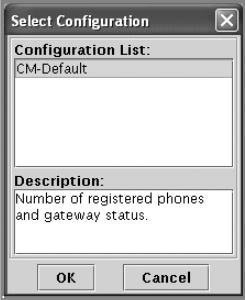
Real-Time Monitoring Configuration Profiles

This topic describes how to configure profiles in RTMT.

Real-Time Monitoring Configuration Profiles

Cisco.com

- Configuration Profiles allow you to save monitoring configurations that are used several times.
- When starting RTMT, the desired profile needs to be selected.

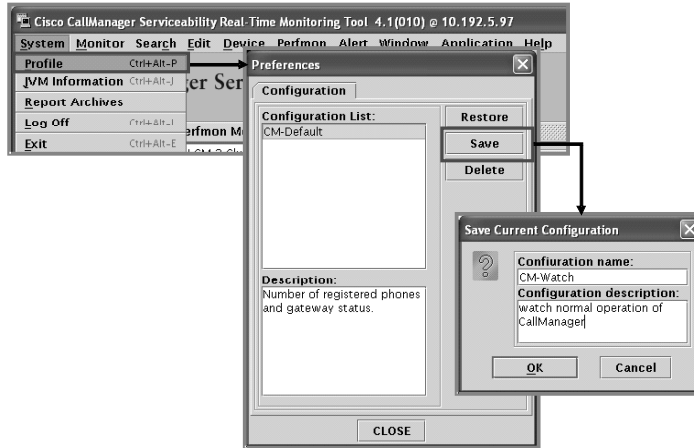


© 2005 Cisco Systems, Inc. All rights reserved. CIP12 v4.1-3-13

RTMT allows you to save monitoring configurations so that they do not need to be recreated every time you start RTMT. When you start RTMT, you can select the desired profile. The CM-Default profile is preconfigured. Its parameters include the number of registered phones and gateway status.

Save Real-Time Monitoring Configuration

Cisco.com



To save the current monitoring configurations:

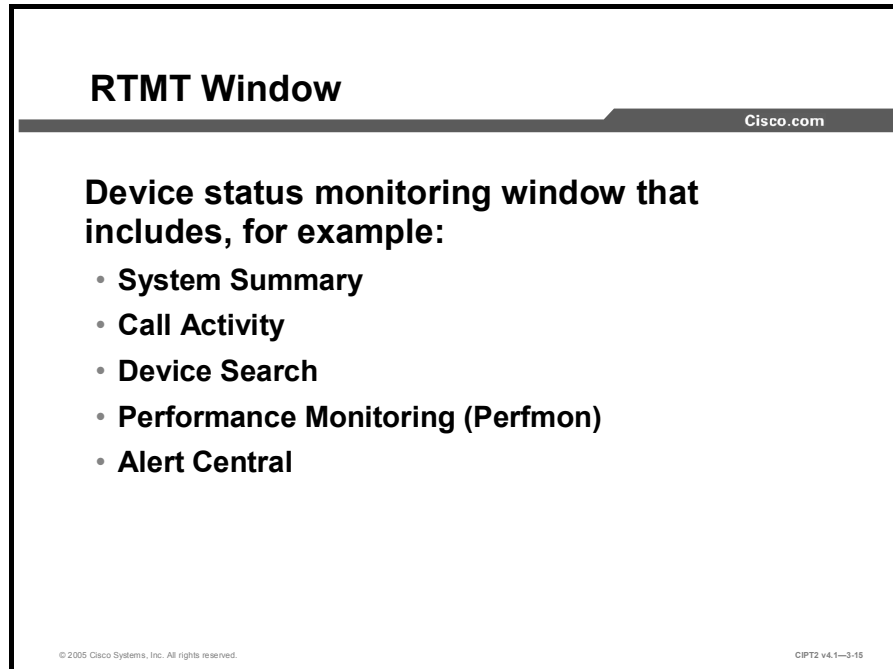
- Step 1** Choose **System > Profile** (or press **Ctrl-Alt-P**) to open the Preferences window.
- Step 2** In the Preferences Window, choose **Save**. The Save Current Configuration window opens.
- Step 3** Enter a name and a meaningful description for the configuration that will allow you to easily identify it later, and click **OK** to save your configuration.

To make a copy of an existing configuration:

- Step 1** Choose **System > Profile** (or press **Ctrl-Alt-P**) to open the Preferences window.
- Step 2** Select the configuration that should be duplicated.
- Step 3** Click **Restore** to load the configuration.
- Step 4** Click **Save**, enter a name and description for the configuration, and click **OK**.

Real-Time Monitoring Tool Window

This topic describes the RTMT window and how it is used.

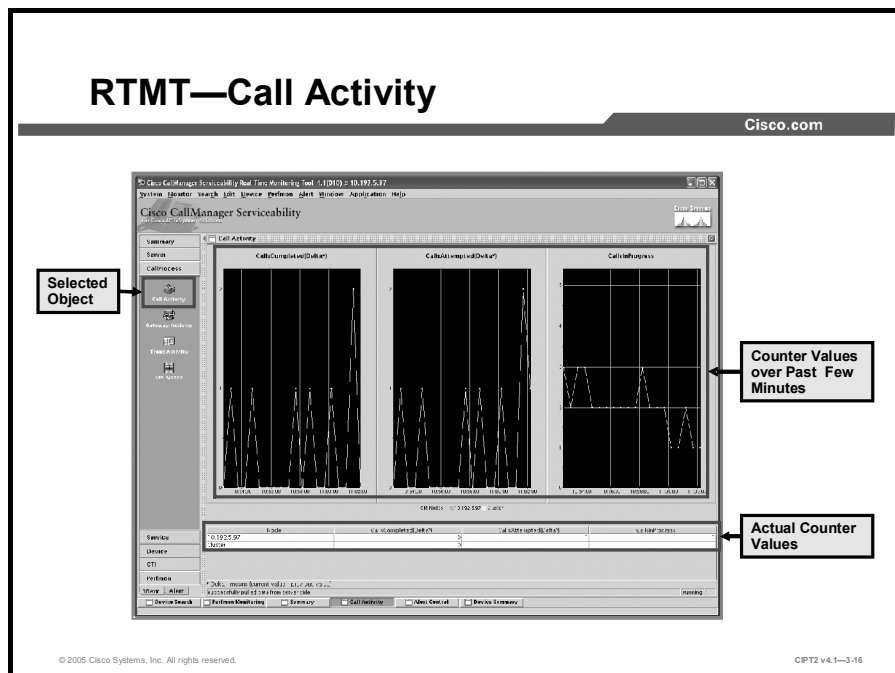


The RTMT window monitors various aspects of Cisco CallManager performance by periodically polling Windows 2000 performance counter values. RTMT discovers devices regardless of their registration status, such as registered or failed, in the cluster. The tool searches by device name, device description, IP address, IP subnet, or directory number (DN) and monitors the status of discovered devices.

Some of the most useful monitoring objects on the RTMT window are these:

- **Summary:** Gives administrators a quick overview of their Cisco Voice over IP (VoIP) system
- **Call Activity:** Shows active calls as well as attempted and completed calls.
- **Device Search:** Allows administrators to define criteria for identifying which devices to display for analysis
- **Perfmon:** Allows system performance to be displayed within the RTMT window, which eliminates the need for a Microsoft Performance Monitor window to be running at the same time
- **Alert Central:** Displays current status and history of all the alerts in the Cisco CallManager cluster

RTMT—Call Activity



The Call Activity window allows you to monitor call activity for each Cisco CallManager node in the cluster in real time. To display the Call Activity window, complete these tasks:

- Step 1** In the controlling center pane at the left, click the **View** tab.
- Step 2** Click **CallProcess**.
- Step 3** Click the **Call Activity** icon.

The Call Activity monitoring window displays the activity of call activity for each Cisco CallManager node in the cluster and draws a history graph for the past few minutes.

RTMT—Device Search

The screenshot shows the Cisco CallManager Serviceability Real-Time Monitoring Tool (RTMT) interface. The 'Device Search' tab is active, displaying a table of registered IP phones. A search filter is applied to show only registered phones. One specific device is highlighted with a callout: 'Cisco IP Phone 7960 with Five DNs'. Another callout points to the 'Status' column, indicating 'Only Registered Phones'.

Name	Status	DirNumber	IpAddress	Model	TimeStamp
SEP000248CCD551	Registered	90124	10.192.4.131	Cisco 7960	10:56:27 AM 05/24/05
SEP000248CCD552	Registered	90138	10.192.4.133	Cisco 7960	10:56:27 AM 05/24/05
SEP000248CCD553	Registered	90130	10.192.4.142	Cisco 7960	10:56:39 AM 05/24/05
SEP000E9B9D1865	Registered	901641	10.192.7.38	Cisco 7910	10:54:29 AM 05/24/05
SEP000AF4AD7460	Registered	90134	10.192.4.139	Cisco 7960	03:41:54 PM 05/26/05
SEP000BBE3E319A	Registered	90136,96015,96013	10.192.4.130	Cisco 7960	10:56:28 AM 05/24/05
SEP000BBE3FE1EF	Registered	90118	10.192.4.12	Cisco 7960	10:56:28 AM 05/24/05
SEP000BBE3FE1F2	Registered	901671,98113,98115,90110,90125	10.192.4.4	Cisco 7960	02:26:26 PM 05/26/05
SEP000BBE3FE250	Registered	90122	10.192.4.10	Cisco 7960	10:56:28 AM 05/24/05
SEP000BBE3FE259	Registered	90120	10.192.4.133	Cisco 7960	10:56:39 AM 05/24/05
SEP000BBE3FE3FB	Registered	901621,9843,9845	10.192.7.34	Cisco 7960	10:56:29 AM 05/24/05
SEP000BBE3FE460	Registered	901658	10.192.7.35	Cisco 7960	10:56:36 AM 05/24/05
SEP000CCED0003E	Registered	90122	10.192.4.9	Cisco 7960	10:56:39 AM 05/24/05
SEP000CE3A82B2	Registered	90128	10.192.4.144	Cisco 7960	01:53:12 PM 05/24/05
SEP000CE3A82B8	Registered	90132	10.192.4.7	Cisco 7960	10:56:27 AM 05/24/05
SEP000D282E5F59	Registered	901629	10.192.4.128	Cisco 7920	09:09:14 AM 05/25/05
SEP000D29512E3B	Registered	90143	10.192.4.2	Cisco 9912	10:56:46 AM 05/24/05
SEP000D29F1C86	Registered	90131	10.192.4.129	Cisco 7960	10:56:39 AM 05/24/05
SEP000D651CE5E	Registered	90123	10.192.4.146	Cisco 7960	10:56:29 AM 05/24/05
SEP000D651CF87	Registered	90149	10.192.4.143	Cisco 7960	01:51:51 PM 05/24/05
SEP000D651D7791	Registered	90157	10.192.4.136	Cisco 7960	10:56:28 AM 05/24/05
SEP000E38412607	Registered	901610	10.192.2.33	Cisco 2870	10:54:59 AM 05/24/05

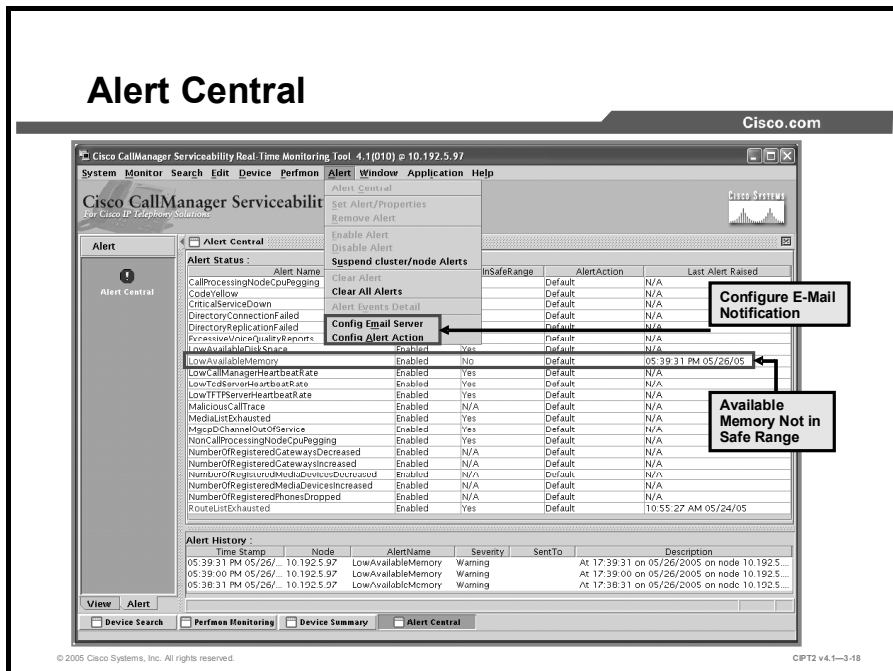
The devices to monitor can be selected based on shared characteristics, such as a status of registered or rejected. RTMT device monitoring can be further refined to narrow the search characteristics to DNs or subnet. In addition, you can select the attributes to monitor, such as Node or StatusReason, and all others can be left out. Select only certain values to monitor because doing so saves time and eliminates unnecessary data in the monitor window. To access these configuration parameters, select the device for which you want to view monitoring information. The monitor then prompts you to enter the characteristics to narrow the search.

The figure shows an example of a device search for IP Phones. It includes only registered IP Phones with some additional information about them. The search result shows that the IP Phone SEP000BBE3FE1F2 is a Cisco 7960 IP Phone and that it has five numbers configured. Further, it shows that the IP Phone has an IP address of 10.192.4.4.

To create a search, complete these tasks:

- Step 1** In the controlling center pane at the left, click the **Device** tab.
- Step 2** Click **Device Search**.
- Step 3** Double-click **Phone** in the white pane and follow the instructions.

Alert Central



In RTMT, you can configure alert notification for Perfmon counter value thresholds and schedule alert checks and status changes of devices (for example, a port is out of service).

The Alert tab in the controlling center pane of the RTMT monitor window includes the Alert Central category. Alert Central provides both the current status and the history of all the alerts in the Cisco CallManager cluster.

The figure shows a sample alert monitor for a system where the available memory of the system is not in the safe range. In this situation, it is strongly recommended that you upgrade the memory on the machine to guarantee safe operation. To allow administrators to qualify the message (to determine whether this is a one-time event because of a special situation or a continuing problem), RTMT also provides a time stamp of the most recent memory leak alert and a history of the most recent messages.

The Alert tab should be used in conjunction with the Alert menu in the RTMT menu bar to configure e-mail notification. Set up the e-mail server (Simple Mail Transfer Protocol [SMTP] server) to send e-mails. You must also configure the alert e-mail recipients and enable notification via the Alert Action configuration.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Performance counters can be analyzed for easy maintenance of Cisco CallManager.**
- **Microsoft Event Viewer can help you identify problems at the system level.**
- **Microsoft Performance Monitor shows system parameters, including Cisco CallManager values.**
- **RTMT is a stand-alone Java plug-in that provides information about Cisco CallManager.**
- **RTMT configurations can be saved in configuration profiles.**
- **The RTMT window monitors various aspects of Cisco CallManager performance.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-3-19

Configuring Alarms and Traces

Overview

Administrators who install or maintain Cisco CallManager sometimes have to deal with technical or design issues on their systems. To troubleshoot and monitor those issues, Cisco CallManager provides alarms and traces similar to the functionality of the **show** and **debug** commands of Cisco IOS software.

This lesson describes how to configure traces on the Cisco CallManager system and discusses tools that allow you to analyze those traces.

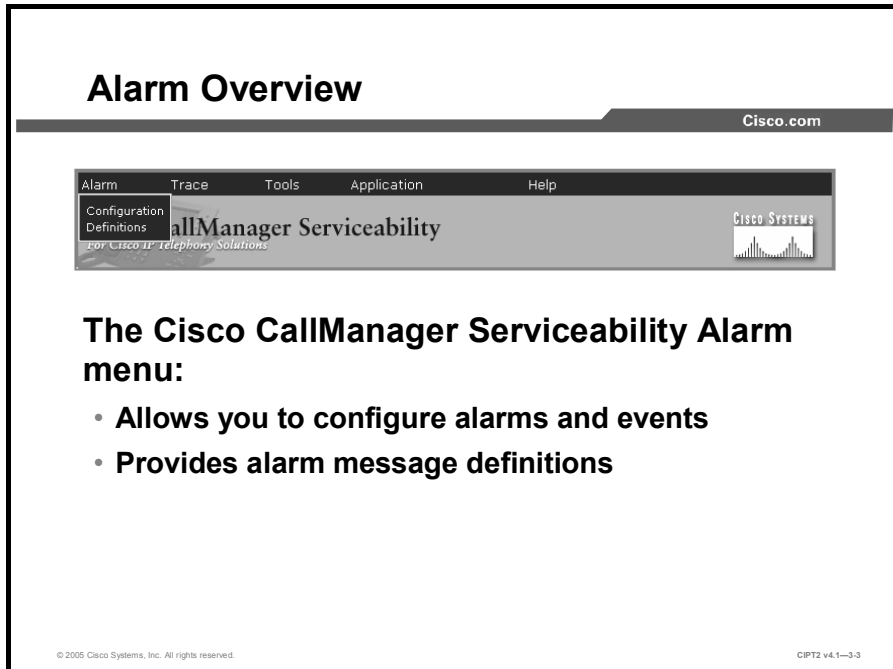
Objectives

Upon completing this lesson, you will be able to configure and use Cisco CallManager Serviceability alarms and traces on Cisco CallManager systems for troubleshooting and maintenance. This ability includes being able to meet these objectives:

- Identify the functions of the Cisco CallManager Serviceability Alarm interface and its event levels and destinations
- Configure alarms for Cisco CallManager services
- Identify and configure the trace functions of the Cisco CallManager Serviceability Trace tool and services
- Conduct a trace analysis and display trace records in XML format
- Collect and compress Cisco CallManager service trace files
- Explain the features and functions of the Bulk Trace Analysis tool
- Identify and explain additional trace tools and describe when to use each of them

Alarm Overview

This topic gives an overview of the Alarm function of Cisco CallManager Serviceability.



The Cisco CallManager Serviceability Alarm menu provides a web-based interface that has two main functions:

- To allow configuration of alarms and events
 - Administrators can define what kind of information should be logged.
 - Administrators can define where to store alarms and events.
- To provide alarm message definitions
 - Administrators can evaluate what kind of information (such as parameter and kind of events) are included in which alarm.

Both functions assist you in troubleshooting and monitoring your Cisco CallManager system. You can configure alarms for services (for example, Cisco CallManager, Cisco TFTP, or Cisco CTIManager), for all Cisco CallManager servers in the cluster or for each server individually.

Aim of Cisco CallManager Serviceability Alarms

Cisco.com

- **Configure Cisco CallManager to direct alarms to:**
 - Event log
 - Syslog server
 - SDI or SDL trace log files
- **Log level can be different for each destination**
- **Provide information for troubleshooting Cisco CallManager system**
- **Provide information that could be given to someone else**

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1—3-4

Alarms are used to provide the run-time status and state of the system and to take corrective action for problem resolution; for example, to determine whether phones are registered and working. Alarms contain information such as an explanation and recommended action. Alarm information includes the application name, machine name, and cluster name to help you troubleshoot problems that are not on the local Cisco CallManager.

The Alarm interface can be configured to send alarm information to multiple destinations, and each destination can have its own alarm event level (from debug to emergency). Alarms can be directed to the Microsoft Windows 2000 Event Log, a syslog server, system diagnostic interface (SDI) trace log files, or signal distribution layer (SDL) trace log files.

Note SDL trace files are available only for Cisco CallManager and the CTIManager service.

When a service issues an alarm, the Alarm interface sends the alarm to the chosen monitors. Each monitor forwards the alarm or writes it to its final destination (such as a log file). This information can be used for troubleshooting and also be passed over to another person for assistance (for example, the Cisco Technical Assistance Center [TAC]).

Alarm Event Levels

Cisco.com

Level	Name	Description
7	Emergency	System unusable
6	Alert	Immediate action needed
5	Critical	Critical condition detected
4	Error	Error condition
3	Warning	Warning condition detected
2	Notice	Normal but significant condition
1	Informational	Information messages only
0	Debug	Detailed event information used for debugging by Cisco TAC engineers

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-3-5

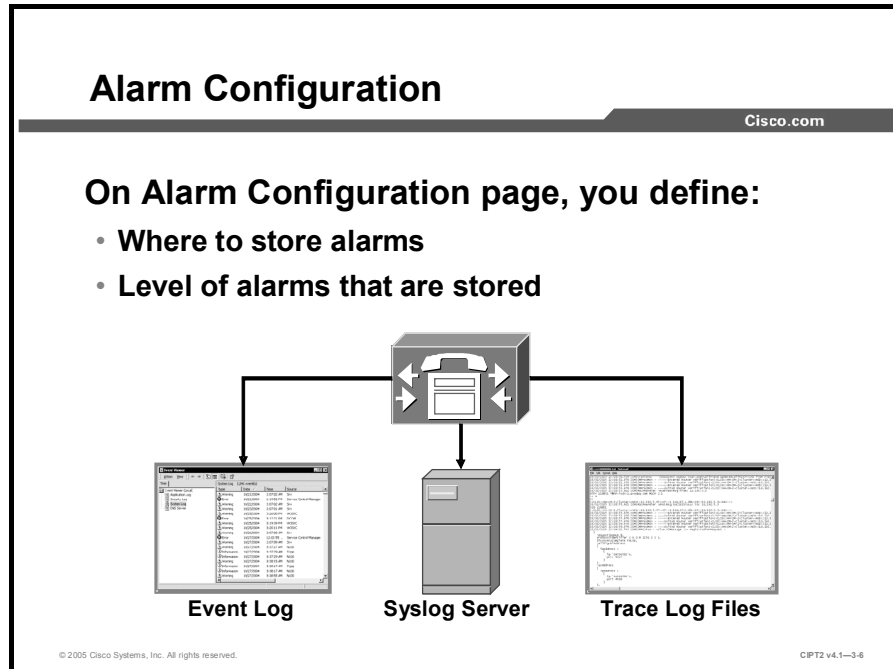
There are several alarm levels on Cisco CallManager that can be turned on. These alarm levels are equivalent to the widely used syslog severity levels.

When the alarm event level is set to a certain value, it means that alarms that match the configured level and alarms that match more severe levels are generated. In other words, an alarm level of 0 (debug) means all alarms of 0 or higher, and an alarm level of 4 means all alarms of level 4 or higher. So if you configure an alarm level of 5, all critical, alert, and emergency alarms are logged.

The table shows all available levels and describes the kind of information that generates the alarm. As you can also see from the table, each level can be identified by its name (debug to emergency) or by its number (0 to 7).

Alarm Configuration

This topic describes configuration of alarms on Cisco CallManager.

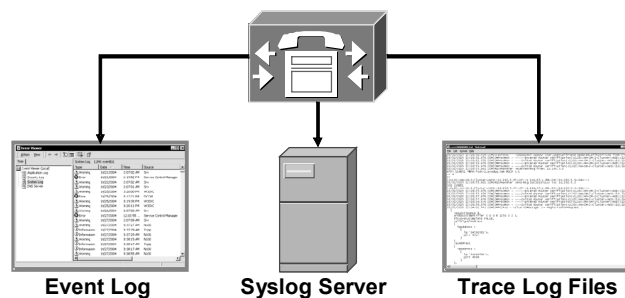


Alarm Configuration

Cisco.com

On Alarm Configuration page, you define:

- Where to store alarms
- Level of alarms that are stored



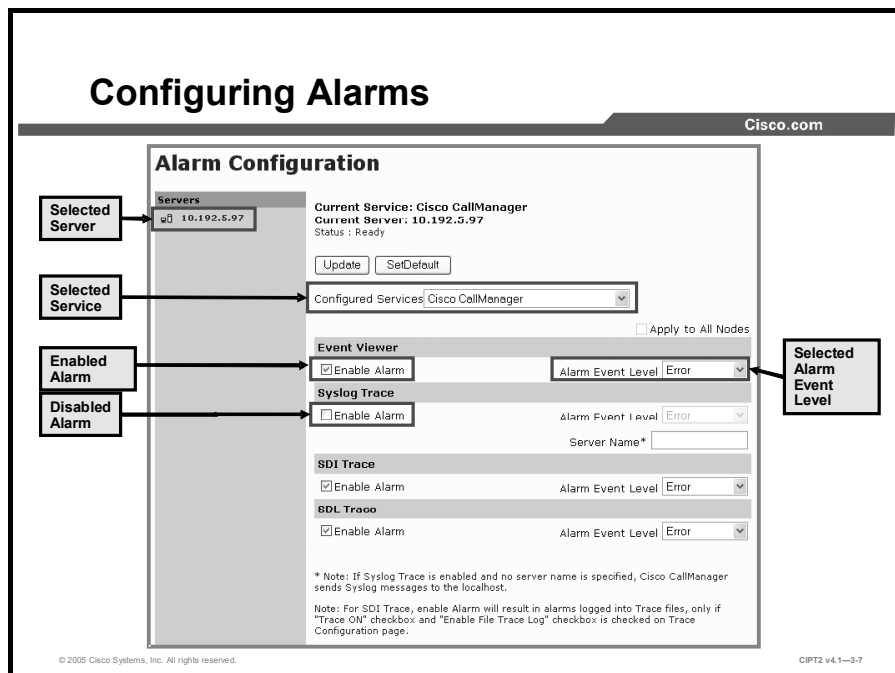
© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-3-6

The Alarm Configuration window in Cisco CallManager Serviceability is used to define where alarms are stored and which level of alarms should be stored. The alarm level can be defined for each destination individually.

Destinations for alarms are as follows:

- Locally on the Cisco CallManager system in Microsoft Windows Event Log
- Locally on the Cisco CallManager system in trace log files
- Remotely on any syslog server; for example, Kiwi Syslog Daemon, a third-party application that runs on Windows systems



To configure alarms on Cisco CallManager, follow this procedure:

- Step 1** From Cisco CallManager Serviceability, choose **Alarm > Configuration**.
- Step 2** Choose the appropriate server, which will then be displayed under Servers on the left side of the window and at the top of the window. A box with available services for alarms appears.
- Step 3** From the Configured Services drop-down list, choose the service to configure the alarm for. The chosen service is displayed at the top of the window in the Current Service area, along with the currently chosen server. A list of alarm monitors with event levels, similar to the one shown in the figure, appears.
- Step 4** Check the check box for each desired alarm destination.

Note Only the Cisco CallManager and CTIManager services have the check box for Enable Alarm for SDL Trace available.

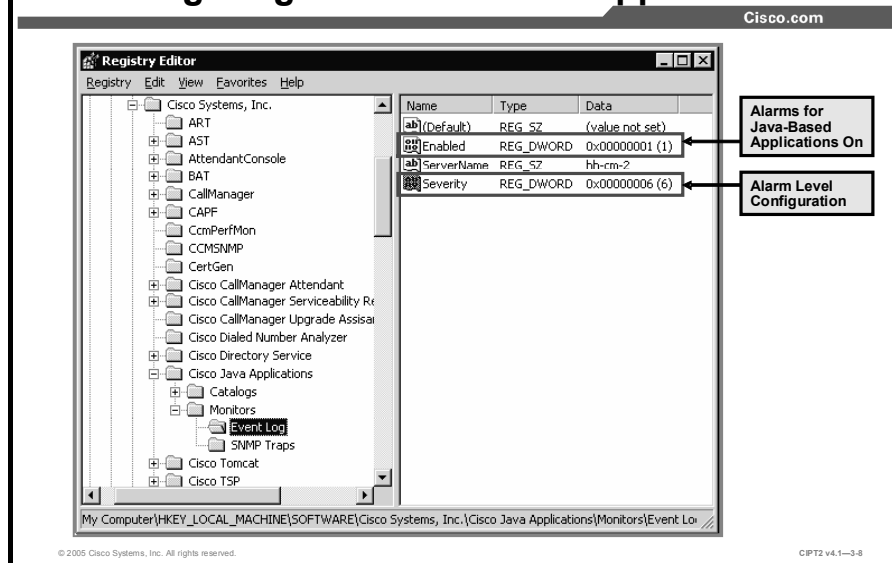
Step 5 In the Alarm Event Level drop-down menu, click the **Down** arrow and choose the desired alarm event level for each of the available alarms.

Step 6 Save the configuration by clicking the **Update** button.

Note To apply the current settings for selected services to all nodes in a cluster, check the **Apply to All Nodes** check box.

Tip To restore the default Cisco CallManager settings, click the **SetDefault** button and then the **Update** button.

Configuring Alarms for Java Applications



Alarms for Java-based applications, such as Java Telephony Application Programming Interface (JTAPI), cannot be configured using the alarm configuration web pages. Use the registry editor provided with the operating system to view the alarm configuration and to change registry entries. The registry can be accessed by running the RegEdit32.exe or RegEdit.exe registry editors. Go to HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\Cisco Java Applications\Monitors\Event Log in the registry and set these values:

- Set the Enabled key to a value of 0 to turn off Event Log or to 1 to turn it on.

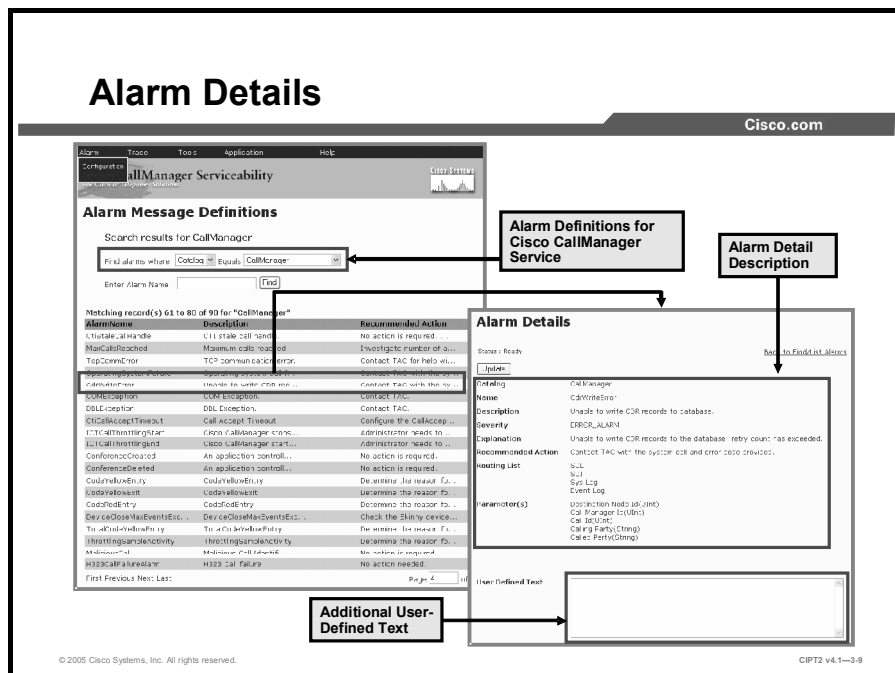
Note By default, Event Log is enabled for Java-based applications.

- Set the Severity key to a value between 0 and 7 to set the alarm event level.

Note The default severity level for Java-based applications on Cisco CallManager systems is 6.

If you change the registry entries, you must restart Java applications for the configuration changes to take effect.

Caution It is recommended that you not change the Simple Network Management Protocol (SNMP) Trap and Catalog configurations. Those settings influence SNMP traps generated by the Cisco CallManager system. Those traps are used by network management applications, such as CiscoWorks. Changing the settings could cause malfunctioning of the entire network management system.



Alarm definitions describe alarm messages. The definitions show what the alarms mean and how to recover from them.

To reach the alarm message definition details for an alarm, complete these steps:

- Step 1** From Cisco CallManager Serviceability, choose **Alarm > Definition**.
- Step 2** From the Equals drop-down menu, choose the service for which to check alarm definitions and click **Find**.
- Step 3** From the window that appears (an example is shown in the figure), select the alarm to see details.

Cisco CallManager stores alarm definitions and recommended actions in a Structured Query Language (SQL) server database. You can search the database for definitions of all the alarms. The definition includes the alarm name, description, explanation, recommended action, severity, parameters, and monitors. This information aids you in troubleshooting problems that Cisco CallManager encounters.


Note Administrators can add their own text to the alarm definition by simply entering information in the User Defined Text pane.

Trace Configuration

This topic explains the trace functionality in Cisco CallManager systems and how it is used.

Trace Configuration

Cisco.com



Cisco CallManager trace functionality:

- Allows detailed configuration of trace parameters
- Assists in analyzing of trace files
- Allows you to enable troubleshooting traces

© 2005 Cisco Systems, Inc. All rights reserved. CIP12 v4.1-3-10

Cisco CallManager Serviceability provides a web-based trace tool to assist the system administrator and support personnel in troubleshooting Cisco CallManager problems. Cisco CallManager Serviceability Trace provides three main functions:

- **Configuration:** This function allows you to configure a variety of options when enabling traces. Options include the level of trace details and the trace file format (.xml or .txt).
- **Analysis and Q.931 Translator:** These functions allow you to analyze trace files.

Note The web-based Trace Analysis tool allows only analysis of Extensible Markup Language (XML) files; the Q.931 Translator analyzes both text and XML files.

- **Troubleshooting Trace Settings:** This function allows you to enable troubleshooting traces. With this feature, you can easily set up traces on multiple servers but there are fewer options available than in the Trace Configuration function.

Types of Traces

Cisco.com

- **SDI traces:**
 - **Contain information about services and run-time events**
 - **Usually used for development purposes**
- **SDL traces:**
 - **Contain information about call processing**
 - **Are only available for:**
 - **Cisco CallManager service**
 - **CTIManager service**
 - **Ideal for troubleshooting**

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1—3-11

Traces for Cisco CallManager services can be based on debug levels, specific trace fields, and Cisco CallManager devices, such as phones or gateways. Two types of traces are available, SDI trace and SDL trace.

SDI Trace

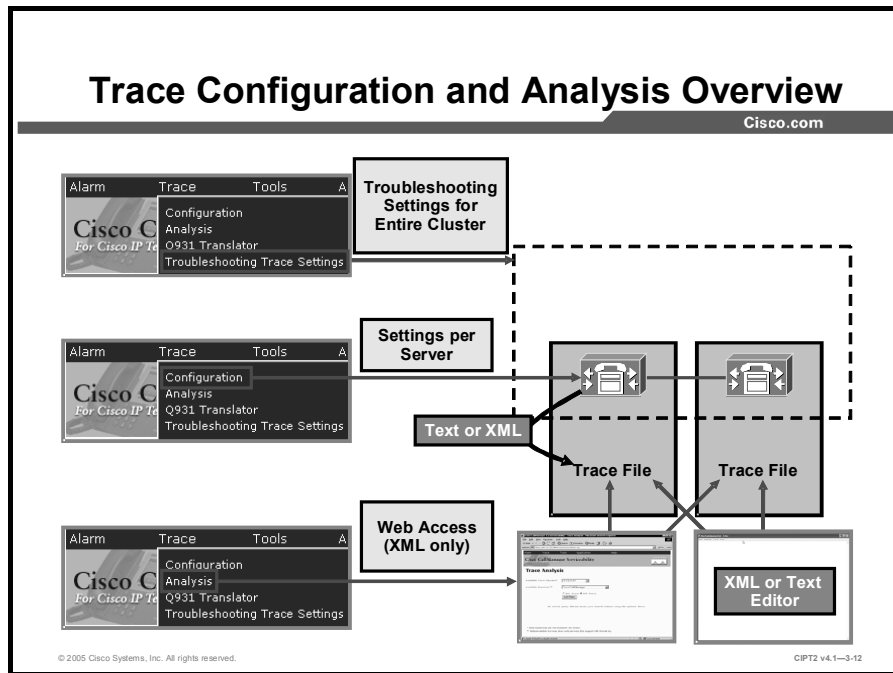
SDI traces are also known as Cisco CallManager trace log files. Every Cisco CallManager service includes a default trace log file. The system traces SDI information from the services and logs run-time events and traces to a log file. SDI traces are used by programmers for development purposes.

SDL Trace

SDL traces contain call-processing information from Cisco CallManager and Cisco CTIManager services. The system traces the SDL of the call and logs state transitions in a log file. This log information helps administrators to troubleshoot problems on the Cisco CallManager system.

Note In most cases, extensive SDL traces will be gathered only when Cisco TAC requests it.

Caution Enabling traces decreases system performance; therefore, enable higher level trace only for troubleshooting.



The figure provides an overview of trace configuration and analysis options.

- **Troubleshooting trace settings:** Allows you to enable troubleshooting traces by server and by service for all servers from a single page.
- **Trace configuration:** Allows detailed trace configuration per server. The configuration options include the trace file format (.xml or .txt).
- **Analysis:** Can be done from stored trace files (XML only).
- **XML or text editors:** Can be used to examine the content of the stored trace files.

Trace Configuration

Cisco.com

- **Set the debug level.**
- **Select components.**
- **Specify output filename and type.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1—3-13

Cisco CallManager provides many services for tracing. With each service, tracing tailored to that service is enabled. Each service can be enabled individually for each server within the Cisco CallManager cluster.

Perform these tasks in the Cisco CallManager Serviceability Trace Configuration window to configure custom settings for a trace:

- Step 1** In Cisco CallManager Serviceability, choose **Trace > Configuration** and choose the server to configure the trace settings for.
- Step 2** From the Configured Services list, choose the service to change the trace settings for. The Trace Configuration window opens. A sample output of that window is displayed in the figure.
- Step 3** To enable traces for the specified service, check the **Trace On** check box.
- Step 4** Choose the desired debug level from the Debug Trace Level drop-down menu.
- Step 5** Choose the trace fields to include in the trace files. This additional information is different for each service.

Note It is recommended that you enable XML-formatted output for Cisco CallManager services and Cisco CTIManager services to support extended trace file analysis (for example, with Cisco CallManager Serviceability Trace Analysis).

Tip Click the **SetDefault** button to revert to the default values. To apply the current settings for chosen services to all nodes in a cluster, check the **Apply to All Nodes** check box.

You can set the path and filename for the trace file. To allow creation of more than one file, Cisco CallManager uses the entered filename and adds an eight-digit string, starting with 00000000, that is incremented with each new file.

Troubleshooting Trace Settings

Cisco.com

- Cisco CallManager allows setting up troubleshooting traces for each service on each server individually from a single page.

Service Is Not Activated on Any Server of the Cluster

Service for Which Traces Are Enabled Only on One Server

Service for Which Traces Are Enabled on Both Servers

Troubleshooting Trace Setting

Status: Ready

Apply Troubleshooting Traces

Services	Select all Nodes for a Service	10.192.5.97	10.192.5.95
Check all Services for a Node	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Cisco Certificate Authority Proxy Function	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Cisco CTL Provider	<input type="checkbox"/>	N/A	N/A
Cisco Extended Functions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Cisco CDR Insert	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Cisco Database Layer Monitor	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Cisco RIS Data Collector	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Cisco MOH Audio Translator	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Cisco Telephony Call Dispatcher	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Cisco CTIManager	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Cisco IP Voice Media Streaming App	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Cisco Messaging Interface	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Cisco Tftp	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Cisco CallManager	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Cisco Extension Mobility	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Cisco IP Manager Assistant	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Cisco WebDialer	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

© 2005 Cisco Systems, Inc. All rights reserved.

CPRT2 v4.1-3-14

To enable or disable troubleshooting traces on different servers throughout the cluster, use the Troubleshooting Trace Setting window from the Cisco CallManager Serviceability Trace menu. This window is usually used for troubleshooting when more than one server needs to be monitored. Each service can be selected or deselected individually for each server.

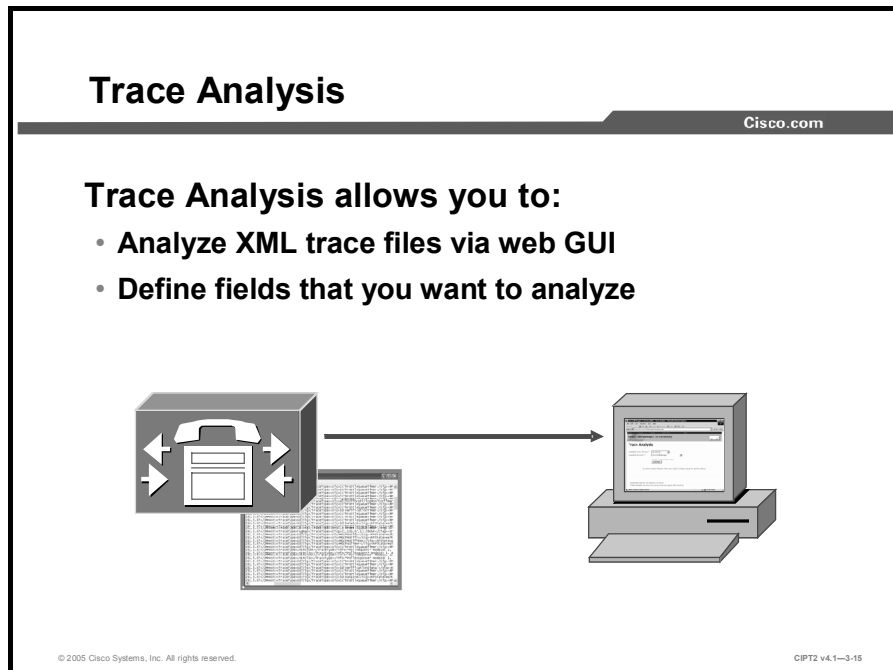
The table describes the logging of each service that can be turned on or off in the Troubleshooting Trace Settings window.

Service Logging

Service	Logging
Cisco CallManager	Logs Cisco CallManager signaling information to trace files
Cisco Call Detail Records (CDRs) Insert	Logs information about writing of CDRs
Cisco Certificate Authority Proxy Function (CAPF)	Logs information about issues of Cisco CAPF
Cisco CTIManager	Logs information about issues on CTIManager of the Cisco CallManager
Cisco Certificate Trust List (CTL) Provider	Logs information about issues of Cisco CTL Provider
Cisco Database Layer Monitor	Logs information about database usage of Cisco CallManager
Cisco Extended Functions	Logs information about issues referring to any of the Cisco CallManager extended functions, such as Quality Report Tool (QRT)
Cisco CallManager Extension Mobility	Logs information about issues of the Cisco CallManager Extension Mobility service and Extension Mobility application
Cisco IP Manager Assistant (IPMA)	Logs information about issues and usage of Cisco IPMA functionality on Cisco CallManager
Cisco IP Voice Media Streaming Application	Logs information about issues of the Cisco IP Voice Media Streaming Application in conjunction with every involved device
Cisco Messaging Interface	Logs information about issues of Cisco Messaging Interface
Cisco Music on Hold (MOH) Audio Translator	Logs information about issues with MOH on Cisco CallManager
Cisco Real-Time Information Server (RIS) Data Collector	Logs information about issues involving collecting real-time information on Cisco CallManager
Cisco Telephony Call Dispatcher (TCD)	Logs information about issues with attendant consoles and pilot points on Cisco CallManager
Cisco TFTP	Logs information about issues with the TFTP server service of Cisco CallManager
Cisco WebDialer	Logs information about issues with the click-to-dial functionality on Cisco CallManager systems

Trace Analysis

This topic describes analysis of trace files using the Trace Analysis tool in Cisco CallManager Serviceability.



The Trace Analysis tool is a postprocessing tool that allows analyzing of XML trace files via a web GUI. The tool is available from the Cisco CallManager Serviceability Trace menu and provides trace details to help narrow your investigation of system problems.

When you are using the Trace Analysis tool, it is possible to specify what kind of information is needed to analyze the Cisco CallManager trace files. When troubleshooting, this makes it easier to go through the trace files and get the necessary information.

Trace Analysis—Selection

Cisco.com

Trace Analysis

Available Cisco Servers* 10182597

Available Services** Cisco CallManager

SDL Trace SDI Trace

List Files

Matching record(s) 1 to 20 of 250

File Name	Size
SDL001_100_000106.xml	96513
SDL001_100_000104.xml	97610
SDL001_100_000104.xml	94315
SDL001_100_000103.xml	98203
SDL001_100_000102.xml	81827
SDL001_100_000101.xml	70108
SDL001_100_000100.xml	69968
SDI001_100_000099.xml	70434
SDL001_100_000098.xml	70206
SDL001_100_000097.xml	71108
SDL001_100_000096.xml	69901
SDL001_100_000095.xml	73684

SDL Trace Analysis

Selection Criteria

CallManager Host ALL

Device Name ALL

IP Address ALL

Trace Type ALL

Signal Name ALL

Fields to Display

Line Number Date and Time CMNode TraceType

Signal Receiving Process Sending Process Receiving Process State

Correlation Tag Application Name Information Device Name

IP Address

Select Defaults Display Records

© 2005 Cisco Systems, Inc. All rights reserved. CIPT2 v4.1—3-16

In the Trace Analysis window, choose what kind of information to analyze and from which trace file by following these steps:

- Step 1** Choose a Cisco CallManager server for which trace files should be analyzed.
- Step 2** Choose the desired service
- Step 3** Define whether to analyze SDI or SDL traces and click the **List Files** button to get the list of all available SDI or SDL files that meet the criteria.
- Step 4** Choose the file to analyze.
- Step 5** Open the Cisco CallManager Serviceability web GUI of the Trace Analysis tool. In the web GUI, define what information to list for the analysis.
- Step 6** To process the records that meet your criteria, click **Display Records**.

Note The Trace Analysis tool supports only trace files containing less than 2 MB of data.

Trace Analysis—Result

Cisco.com

SDL Trace Records

[Back to Selection](#)

LINE NO	DATE AND TIME	DM NODE	TRACE TYPE	SIGNAL	RECEIVING PROCESS	SENDING PROCESS	RECEIVING PROCESS STATE
6191212	05/04/22 15:51:07.624	10.192.5.97	SdlSig	SdlDataInd	StationInit(1,100,118,1)	SdlTCPConnection(1,100,131,12)	wait
6191213	05/04/22 15:51:07.624	10.192.5.97	SdlSig	SdlDataInd	StationInit(1,100,118,1)	SdlTCPConnection(1,100,131,248)	wait
6191214	05/04/22 15:51:07.624	10.192.5.97	SdlSig	StationKeypadButton	StationCdp(1,100,117,320)	StationD(1,100,116,1)	restart0
6191215	05/04/22 15:51:07.624	10.192.5.97	SdlSig	StationKeypadButton	StationCdp(1,100,116,2791)	StationD(1,100,117,320)	overlap_sending2
6191216	05/04/22 15:51:07.624	10.192.5.97	SdlSig	CcInfoInd	LineControl(1,100,47,288)	StationCdp(1,100,116,2791)	restart0
6191217	05/04/22 15:51:07.624	10.192.5.97	SdlSig	StationOutputStopTone	StationD(1,100,117,320)	StationCdp(1,100,116,2791)	restart0
6191218	05/04/22 15:51:07.624	10.192.5.97	SdlSig	StationOutputSelectSoftKeys	StationD(1,100,117,320)	StationCdp(1,100,116,2791)	restart0
6191219	05/04/22 15:51:07.624	10.192.5.97	SdlSig	CcInfoInd	LineCdp(1,100,46,2668)	LineControl(1,100,47,288)	call_initiated1
6191220	05/04/22 15:51:07.624	10.192.5.97	SdlSig	CcInfoInd	Cc(1,100,21,1)	LineCdp(1,100,46,2668)	wait
6191221	05/04/22 15:51:07.624	10.192.5.97	SdlSig	CcInfoInd	Cdcc(1,100,22,2585)	Cc(1,100,21,1)	tcc_wait_digits1
6191222	05/04/22 15:51:07.624	10.192.5.97	SdlSig	DaReq	Da(1,100,28,1)	Cdcc(1,100,22,2585)	wait
6191223	05/04/22 15:51:07.624	10.192.5.97	SdlSig	DaRes	Dcc(1,100,22,2585)	Da(1,100,28,1)	info_da
6191224	05/04/22 15:51:07.624	10.192.5.97	SdlSig	SdlWriter	SdlTCPConnection(1,100,131,948)	StationD(1,100,117,320)	active

Annotations:
 - "User Is Dialing" points to the SdlDataInd signal in rows 6191212 and 6191213.
 - "Cisco CallManager Initiates Call" points to the CcInfoInd signal in row 6191219.

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1—3-17

From the selections that you made for trace analysis, Cisco CallManager creates a web page giving all the desired data.

An example is shown in the figure. This sample output includes, for example, information about a user who is dialing using overlap sending, followed by a call-initiated message that indicates that Cisco CallManager initiated the call.

View Trace Files with an Editor

Cisco.com

The screenshot displays the 'Trace Output Settings' dialog box and a Windows Explorer window. The 'Trace Output Settings' dialog has the following options:

- Enable File Trace Log
- Enable XML Formatted Output for "Trace Analysis"
- File Name: isco\Trace\CCM\ccm.txt
- Maximum No. of Files: 250
- Maximum No. of Lines per File: 2000
- Maximum No. of Minutes per File: 5
- Enable Debug Output String

The Windows Explorer window shows the directory C:\Program Files\Cisco\Trace\CCM. The file list is as follows:

Name	Size	Type	Modified
cm00000189.txt	433 KB	Text Document	2/10/2005 12:05 PM
cm00000190.txt	398 KB	Text Document	2/10/2005 12:10 PM
cm00000191.txt	189 KB	Text Document	2/10/2005 12:15 PM
cm00000192.txt	26 KB	Text Document	3/30/2005 12:00 PM
cm100000000.txt	144 KB	Text Document	3/30/2005 12:03 PM
cm100000001.txt	136 KB	Text Document	3/30/2005 12:08 PM
cm200000000.txt	25 KB	Text Document	3/30/2005 12:08 PM
cm300000000.txt	71 KB	Text Document	4/8/2005 10:54 AM
cm300000001.txt	91 KB	Text Document	4/8/2005 10:57 AM
cm300000002.txt	4 KB	Text Document	4/12/2005 2:58 PM
cm00000193.txt	23 KB	Text Document	4/12/2005 2:58 PM
cm00000194.txt	143 KB	Text Document	4/12/2005 3:02 PM
cm100000002.txt	35 KB	Text Document	4/12/2005 3:03 PM
cm600000000.txt	31 KB	Text Document	4/12/2005 3:03 PM
cm600000001.txt	221 KB	Text Document	4/13/2005 7:47 AM
22 object(s)	2.67 MB		My Computer

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-3-18

You can directly open trace files from the folders where they are stored (subdirectories under C:\Program Files\Cisco\Trace). You can use text editors (for XML and .txt files) or XML viewers or editors to view XML files.

Trace files in .txt format cannot be analyzed by using the Trace Analysis tool. They can be analyzed by the Q.931 Translator tool; however, this tool interprets only Q.931 messages. To examine other messages from stored .txt trace files, you have to use a text editor.

Trace Collection


This topic describes how to configure and use trace collection on Cisco CallManager systems.

Trace Collection

Cisco.com

Trace collection allows you to:

- **Select which traces should be written**
- **Collect traces of all Cisco CallManager nodes in the cluster**

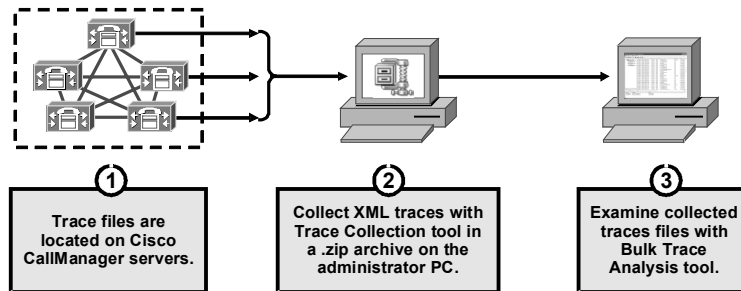


© 2005 Cisco Systems, Inc. All rights reserved. CIP12 v4.1-3-19

To analyze trace files of a Cisco CallManager system locally on an administrator PC, it is necessary to collect trace files from the Cisco CallManager file system and copy them to the PC of the administrator. Instead of manually copying all trace files from all servers of the cluster, you can use the Trace Collection tool, which automates this process.

Remote Analysis of Trace Files

Cisco.com



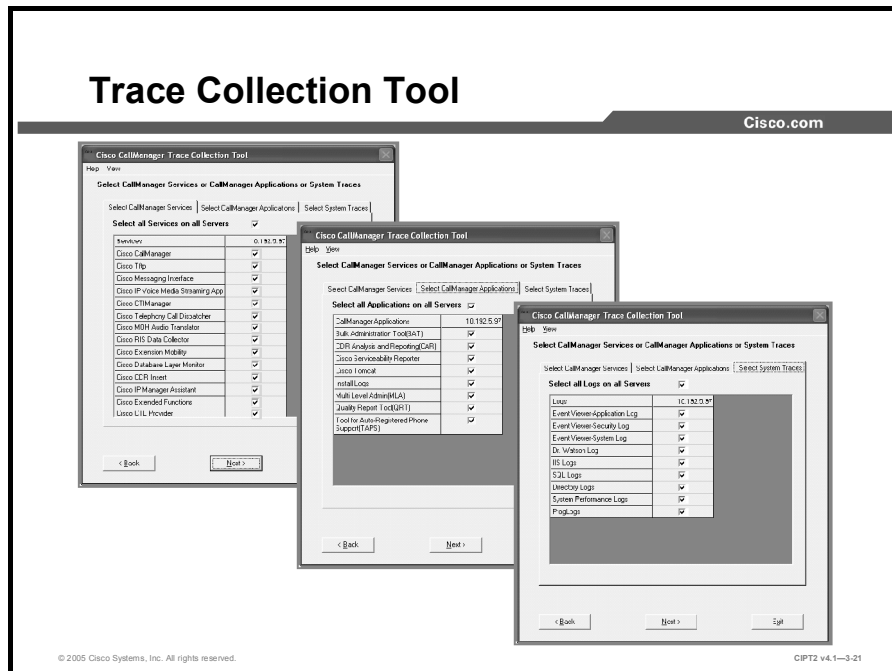
© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-3-20

If you want to analyze trace files from multiple servers on your administrator PC, use the Trace Collection tool to transfer the trace files to your local PC, where they can then be analyzed by the Bulk Trace Analysis tool or a text editor. There are three steps involved:

- Step 1** When traces are enabled, Cisco CallManager writes trace information to the local trace files.
- Step 2** The Trace Collection tool can be used to download all trace files (including XML trace files) from all Cisco CallManager systems in the cluster.
- Step 3** The Bulk Trace Analysis tool allows analysis of XML trace files at the administrator PC. You can view text files using a text editor.

Trace Collection Tool



The Trace Collection tool allows you to collect trace information for any Cisco CallManager service of any Cisco CallManager throughout the cluster, including the time and date of the trace for that service. It can be run on any PC on the network and is available from the Cisco CallManager Install Plugins window.

After the Trace Collection tool is installed on the PC, enter the IP address, username, and password for Cisco CallManager. As soon as the connection to the server is established, the window shown in the figure appears.

Three tabs are available in the Cisco CallManager Trace Collection tool window. Each has its own function, as described in the table.

Functions of Tabs in the Cisco CallManager Trace Collection Tool Window

Tab	Function
Select CallManager Services	Provides a grid of services for the Cisco CallManager nodes in the cluster. Choose all or some of the services for which traces should be collected by checking the appropriate check boxes.
Select CallManager Applications	Provides the list of Cisco CallManager applications for which traces can be collected. Choose all or some of the applications in this tab.
Select System Traces	Provides a list of all system logs from which data can be selected.

Downloading and Compressing Trace Files

After selecting the desired system logs, define the date range for the data to be selected to help minimize the amount of data that needs to be collected.

Click the **Collect Traces** button for the application to start downloading and compressing all files locally to the PC. All files are added to the system primary hard drive (C:\) to an archive named CiscoCallManagerTraceCollection.zip.

Caution Selecting all kinds of data from all Cisco CallManager servers on the system leads to extremely long download times, extensive file-compression processing, and large compressed files.

Bulk Trace Analysis


This topic describes how to analyze trace files locally on a PC by using the Bulk Trace Analysis tool.

Bulk Trace Analysis

Cisco.com

Stand-alone application that:

- **Is available from Cisco CallManager Plugins window**
- **Allows analyzing trace files locally on any PC**
- **Allows analyzing files more conveniently than with the Trace Analysis web GUI**



The diagram illustrates the workflow of the Bulk Trace Analysis tool. On the left, a Cisco CallManager system is represented by a server rack icon with a telephone handset and bidirectional arrows. An arrow points from this system to a PC on the right, which has a monitor displaying a data table. Below the CallManager icon is a document icon representing a trace file. The PC icon includes a keyboard and mouse. At the bottom left of the diagram area, there is a small copyright notice: '© 2005 Cisco Systems, Inc. All rights reserved.' At the bottom right, there is a reference code: 'CIP12 v4.1-3-22'.

The Bulk Trace Analysis tool is a postprocessing tool that allows analyzing XML trace files on every PC locally. Trace files that should be analyzed first need to be downloaded. To do this, use the Trace Collection tool. It can be downloaded from the Cisco CallManager Install Plugins window and works similarly to the Trace Analysis web GUI on Cisco CallManager, but it has some extra features. These extra features allow the user of the Bulk Trace Analysis tool to analyze files more easily than with the Trace Analysis web GUI. This tool is ideal to analyze trace files received from external sources, because only the trace files are needed for the analysis and not access to the Cisco CallManager system where they were created.

Bulk Trace Analysis Features

Cisco.com

- **Multiple files can be analyzed in parallel.**
- **Multiple views can be created from the content of the same file simultaneously.**
- **Views can be customized more extensively than with the Trace Analysis web GUI.**
- **Reports can be saved and printed.**
- **It does not affect Cisco CallManager processing power because it runs on a PC.**
- **Files larger than 2 MB are supported.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1—3-23

The Bulk Trace Analysis tool supports these features that are not provided within the Trace Analysis web GUI on Cisco CallManager:

- It creates reports of information that can be analyzed for troubleshooting, using multiple trace files as the input source data.
- It allows multiple views of a single report to compare and analyze multiple issues simultaneously and concentrate on essential fields.
- It allows users to customize report formats, sort trace information by type, and filter information by special trace tags as well as date and time.
- It allows saving and printing of reports for further analysis.
- It works without using Cisco CallManager processing power because it runs locally on a PC.
- It can be used to analyze large trace files (larger than 2 MB).

Using Bulk Trace Analysis

Cisco.com

The screenshot displays the Cisco Bulk Trace Analysis Tool interface. On the left, a tree view shows a report named 'Task:SCU82.ct' with three sub-views: 'View(1)', 'View(2)', and 'View(3)'. A box labeled 'Report' points to the main report name, and a box labeled 'Special View of a Report' points to the sub-views. The main window contains a table with the following columns: Line, Date, CMHost, TraceF., sig, PPSState, RPhoc, and SPhoc. The table lists various trace events such as 'SdIaNotificationTime', 'CtThrottleQueueTime', 'SdIaAtaind', 'SdIaNotification', and 'CtThrottleQueueTime'. A box labeled 'Analysis Result Similar to Trace Analysis Web GUI Result' points to the table. At the bottom, a task log shows three tasks: 'Task:SCU82.ct', 'Task:SCU84.ct', and 'Task:SCU86.ct', all with a status of 'process finished'.

Line	Date	CMHost	TraceF.	sig	PPSState	RPhoc	SPhoc
614154	05/04/22 15:06:25.714	10.192.5.97	SdIaI	SdIaNotificationTime	nonzero	CMHocMon(1,100,23,1)	SdIaTimeService(1,100,3,1)
614155	05/04/22 15:06:25.701	10.192.5.97	SdIaI	CtThrottleQueueTime	wait	Cct(1,100,2,1)	SdIaTimeService(1,100,3,1)
614156	05/04/22 15:06:25.868	10.192.5.97	SdIaI	CtThrottleQueueTime	wait	Cct(1,100,2,1)	SdIaTimeService(1,100,3,1)
614157	05/04/22 15:06:25.904	10.192.5.97	SdIaI	SdIaAtaind	wait	StationM(1,100,118,1)	SdIaCPConnector(1,100,13,2)
614158	05/04/22 15:06:26.011	10.192.5.97	SdIaI	CtThrottleQueueTime	wait	Cct(1,100,2,1)	SdIaTimeService(1,100,3,1)
614159	05/04/22 15:06:26.120	10.192.5.97	SdIaI	SdIaAtaind	wait	StationM(1,100,118,1)	SdIaCPConnector(1,100,13,1)
614160	05/04/22 15:06:26.136	10.192.5.97	SdIaI	CtThrottleQueueTime	wait	Cct(1,100,2,1)	SdIaTimeService(1,100,3,1)
614161	05/04/22 15:06:26.201	10.192.5.97	SdIaI	CtThrottleQueueTime	wait	Cct(1,100,2,1)	SdIaTimeService(1,100,3,1)
614162	05/04/22 15:06:26.306	10.192.5.97	SdIaI	CtThrottleQueueTime	wait	Cct(1,100,2,1)	SdIaTimeService(1,100,3,1)
614163	05/04/22 15:06:26.421	10.192.5.97	SdIaI	DeviceConfigurationMonitoringTime	wait	StationM(1,100,118,1)	SdIaTimeService(1,100,3,1)
614164	05/04/22 15:06:26.511	10.192.5.97	SdIaI	CtThrottleQueueTime	wait	Cct(1,100,2,1)	SdIaTimeService(1,100,3,1)
614165	05/04/22 15:06:26.605	10.192.5.97	SdIaI	SdIaAtaind	wait	StationM(1,100,118,1)	SdIaCPConnector(1,100,13,4)
614166	05/04/22 15:06:26.636	10.192.5.97	SdIaI	CtThrottleQueueTime	wait	Cct(1,100,2,1)	SdIaTimeService(1,100,3,1)
614167	05/04/22 15:06:26.651	10.192.5.97	SdIaI	SdIaAtaind	wait	StationM(1,100,118,1)	SdIaCPConnector(1,100,13,1)
614168	05/04/22 15:06:26.693	10.192.5.97	SdIaI	SdIaAtaind	wait	StationM(1,100,118,1)	SdIaCPConnector(1,100,13,4)
614169	05/04/22 15:06:26.690	10.192.5.97	SdIaI	SdIaNotification	nonzero	CMHocMon(1,100,23,1)	CMHocMon(1,100,23,1)
614170	05/04/22 15:06:26.714	10.192.5.97	SdIaI	SdIaAtaind	wait	StationM(1,100,118,1)	SdIaCPConnector(1,100,13,5)
614171	05/04/22 15:06:26.714	10.192.5.97	SdIaI	SdIaAtaind	wait	StationM(1,100,118,1)	SdIaCPConnector(1,100,13,2)
614172	05/04/22 15:06:26.701	10.192.5.97	SdIaI	CtThrottleQueueTime	wait	Cct(1,100,2,1)	SdIaTimeService(1,100,3,1)
614173	05/04/22 15:06:26.726	10.192.5.97	SdIaI	SdIaAtaind	wait	StationM(1,100,118,1)	SdIaTimeService(1,100,3,1)
614174	05/04/22 15:06:26.886	10.192.5.97	SdIaI	CtThrottleQueueTime	wait	Cct(1,100,2,1)	SdIaTimeService(1,100,3,1)
614175	05/04/22 15:06:27.011	10.192.5.97	SdIaI	CtThrottleQueueTime	wait	Cct(1,100,2,1)	SdIaTimeService(1,100,3,1)
614176	05/04/22 15:06:27.093	10.192.5.97	SdIaI	SdIaAtaind	wait	StationM(1,100,118,1)	SdIaCPConnector(1,100,13,5)
614177	05/04/22 15:06:27.136	10.192.5.97	SdIaI	CtThrottleQueueTime	wait	Cct(1,100,2,1)	SdIaTimeService(1,100,3,1)
614178	05/04/22 15:06:27.214	10.192.5.97	SdIaI	H250CTTheorightMonitorTime	nonzero	H250(1,100,40,1)	SdIaTimeService(1,100,3,1)

© 2005 Cisco Systems, Inc. All rights reserved. CIPT2 v4.1-3-24

The figure shows three SDL reports, each with multiple views.

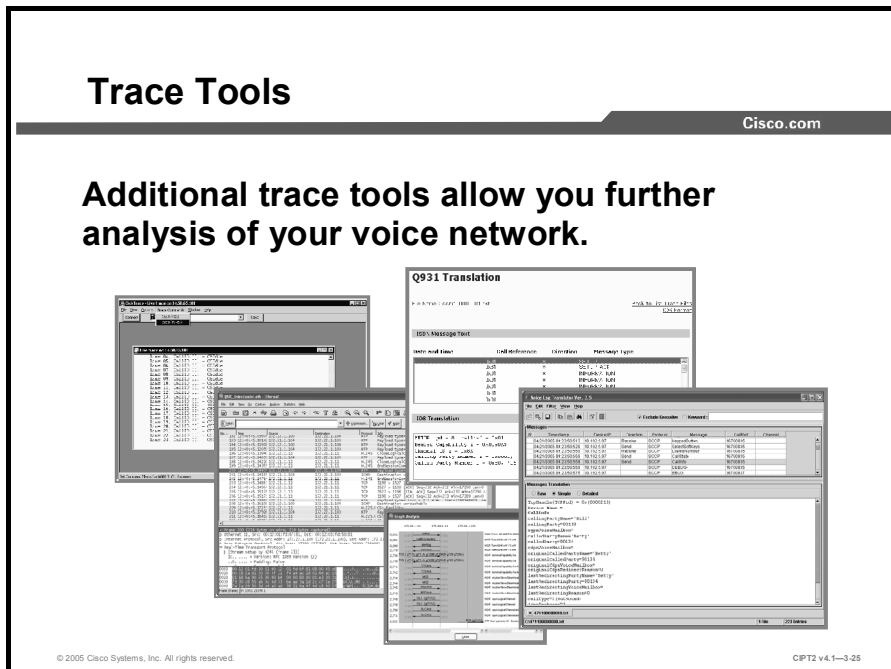
To create such a report, choose **File > New Report**. In the window that appears, choose whether to create an SDI or an SDL report and where the file for analysis is located.

To add new views for the report, choose **View > New View**. In the window that appears, choose which kind of information should be included in the new view.

To change the order of the columns or to add or remove columns, choose **View > Customize Header** and make the selections from the new window.

Trace Tools

This topic gives an overview of some additional trace tools that can be used for Cisco CallManager troubleshooting and maintenance.



There are many additional trace tools provided by Cisco and other vendors that allow you to analyze the voice network. Examples of those additional tools are as follows:

- Q.931 Translator
- Voice Log Translator
- Dick Tracy
- Ethereal

Trace Tools Overview

Cisco.com

	Use	Available From
Q.931 Translator	Analyzes Q.931 messages from Cisco CallManager logs	Cisco CallManager Serviceability
Voice Log Translator	Analyzes voice flows from Cisco CallManager logs	Cisco TAC
Dick Tracy	Analyzes voice flow on T1/E1 and FXS ports on Cisco Catalyst 6500 systems	Cisco.com
Ethereal	Packet sniffer and analyzer, which also allows you to analyze voice traffic on the network	Ethereal.com

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1—3-26

The table gives an overview of some additional trace tools, what they can be used for, and where they are available.

Q.931 Translator

The Q.931 Translator allows analysis of Q.931 messages from text or XML log files created on Cisco CallManager systems. The tool shows the ISDN messages and their Cisco IOS translation. The Q.931 Translator can be used to save Cisco IOS translations to another log file for further investigation. To access the Q.931 Translator, choose **Cisco CallManager Serviceability > Trace > Q931 Translator**.

Voice Log Translator

Voice Log Translator, a tool formerly known as X-Log, is a stand-alone application that can be used to analyze the complete voice flow from Cisco CallManager log files. The tool is based on Q.931 Translator but adds some additional functionality, such as Signaling Connection Control Part (SCCP) support for easier troubleshooting of voice flow issues. The Voice Log Translator tool is available only from Cisco TAC to troubleshoot voice flows on nonfunctioning Cisco CallManager systems.

Dick Tracy

The Dick Tracy tool allows you to capture and analyze voice flows on T1/E1 or Foreign Exchange Station (FXS) ports of Cisco Catalyst 6500 Series switch systems. To download the Dick Tracy tool from Cisco.com, you must hold a valid Cisco.com account.

Ethereal

Ethereal is one of the most powerful network capture and analysis tools. It supports analysis of nearly all types of packets captured from the network. For voice analysis, it includes special features, such as painting graphs of Voice over IP (VoIP) signaling flows or saving G.711 Real-Time Transport Protocol (RTP) streams as .au files for playback with media players. Ethereal is available for free at <http://www.ethereal.com>.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **There are eight alarm levels available on Cisco CallManager.**
- **Alarm configuration allows you to define where alarms should be saved and what level should be included.**
- **Administrators can define the kind of information to be written to trace files and the format that those files should have.**
- **To analyze trace files, Cisco CallManager Serviceability includes the Trace Analysis tool.**
- **The Trace Collection tool allows you to download and compress and save Cisco CallManager trace files to an administrator PC.**
- **The Bulk Trace Analysis tool allows you to analyze Cisco CallManager trace files locally on a PC.**
- **Additional trace tools provided by Cisco and other vendors allow administrators to further analyze their voice network.**

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1—3-27

Lesson 3-4

Configuring CAR

Overview

The Call Detail Record (CDR) Analysis and Reporting (CAR) tool is a powerful application that gives an overview of the call volume of users or departments. CAR can also generate reports for special route patterns and features such as Client Matter Codes (CMC) and Forced Authorization Codes (FAC).

Objectives

Upon completing this lesson, you will be able to configure CAR. This ability includes being able to meet these objectives:

- Describe the uses, features, and operation of the CAR tool
- Explain the contents of CDR and CMR
- Explain the three levels of CAR users and the reporting capabilities of each
- Explain the types of CAR reports and which user levels can generate them
- Configure CAR system parameters
- Configure the system schedule to schedule daily, weekly, and monthly reports
- Configure CAR alerts when the database size exceeds a configured threshold
- Generate, view, or mail user reports using CAR

CAR Overview

This topic describes the CAR tool.

CAR Tool

Cisco.com

- **Formerly known as Administrative Reporting Tool (ART)**
- **Generates reports for QoS, traffic, and CDR**
- **Reports are available in two formats:**
 - **PDF (limited to 5000 records)**
 - **CSV (limited to 20,000 records)**
- **Not installed by default:**
 - **Has to be installed on the publisher**
 - **Uses Cisco Tomcat service**

© 2005 Cisco Systems, Inc. All rights reserved.CIPT2 v4.1-3.3

The Cisco CallManager Serviceability CAR tool, formerly known as Administrative Reporting Tool (ART), generates reports of information for quality of service (QoS), traffic, user call volume, billing, and gateways.

CAR reports are generated in either portable document format (PDF) or comma-separated values (CSV) format. The PDF format limits the number of records in the CAR reports to 5000, and CSV format limits the number of records to 20,000. If the number of records exceeds these limits, a message warns that the results are truncated. To avoid truncating reports, reduce the date range and regenerate the reports.

If CAR is running on your system before you upgrade to a new version of Cisco CallManager, the upgrade process automatically upgrades CAR. If Cisco CallManager is being installed for the first time, CAR has to be installed manually from the Cisco CallManager Administration > Application > Install Plugins menu. CAR must be installed on the Cisco CallManager publisher that hosts the CDR database. CAR uses the Cisco Tomcat service.

CDRs and CMRs

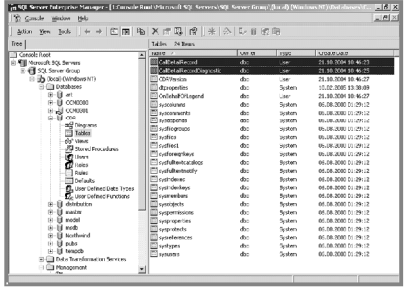
This topic describes the differences between CDRs and Call Management Records (CMRs), and where to find the tables in the database.

CDRs and CMRs

Cisco.com

Access the CDRs with the Microsoft SQL Server Enterprise Manager

- CDRs and CMRs are stored in the SQL database.
- CDRs include information about the call in the CallDetailRecord table.
- CMRs include information about the call quality in the CallDetailRecordDiagnostic table.
- There is a CMR entry generated for each CDR entry.



© 2005 Cisco Systems, Inc. All rights reserved. CPT2 v4.1-3-4

CDRs and CMRs are both stored in the CDR database, accessible with the Microsoft SQL Server Enterprise Manager. Choose **Start > Programs > Microsoft SQL Server > Enterprise Manager** to open the Microsoft SQL Server Enterprise Manager on the Cisco CallManager publisher.

Both types of records store information about a call. The CDR table stores details about the call itself. The CMR table stores information about QoS parameters for the same call. The CDR and CMR tables are called CallDetailRecord and CallDetailRecordDiagnostic. For every CDR entry, a CMR entry is also generated.

When you purge the CDR database, the related entries for a call in the CallDetailRecord and CallDetailRecordDiagnostic tables are both deleted.

Note For example, a consultative call transfer generates three entries (call, consultative call, and transferred call) for the transferred call in the CallDetailRecord table.

SQL CDR and CMR Tables in Detail

Cisco.com

- CDR table has 68 information fields:
 - Calling party
 - Called party
 - Duration
 - Features like CMC, FAC
- CMR table has 18 information fields about QoS:
 - Packets sent or received
 - Packet loss
 - Jitter and latency

CDR table

CallDetailRecord
cdrRecordType
globalCallID_callManagerId
globalCallID_callId
origLegCallIdentifier
dateTimeOrigination
origNodeid
origSpan
origAddr
origPort
callingPartyNumber
origCause_location
origCause_value
origMediaTransportAddress_IP
origMediaTransportAddress_Port
origMediaCap_payloadCapability
origMediaCap_maxFramesPerPacket
origMediaCap_g723BRate
destLegIdentifier
destNodeid
destSpan
destAddr
destPort
originalCalledPartyNumber
finalCalledPartyNumber
destCause_location
destCause_value
destMediaTransportAddress_IP
destMediaTransportAddress_Port
destMediaCap_payloadCapability
destMediaCap_maxFramesPerPacket
destMediaCap_g723BRate
dateTimeConnect
dateTimeDisconnect
lastRedirectIn
pkid
originalCalledPartyNumberPartition

CMR table

CallDetailRecordDiagnostic
cdrRecordType
globalCallID_callManagerId
globalCallID_callId
nodeid
directorNum
callIdentifier
dateTimestamp
numberPacketsSent
numberOctetsSent
numberPacketsReceived
numberOctetsReceived
numberPacketsLost
jitter
latency
pkid
directorNumPartition
deviceName
globalCallID_ClusterID

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-3-5

The CallDetailRecord table stores a lot of information about a call. Each record has a unique identifier called the *pkid* that enables you to find and identify a single record. The CallDetailRecord table also contains information about the calling party, called party, duration of or information about call forwarding, CMC, and FAC, to name the most important fields of a record. In total, the CallDetailRecord table contains 68 information fields.

The number of columns for the CallDetailRecordDiagnostic table is, in contrast to the CallDetailRecord table, very small—it has only 18 information fields. A unique identifier (*pkid*) for every call is included in the CallDetailRecordDiagnostic table as well. The *pkid* for a call in the CallDetailRecordDiagnostic table is not the same as the *pkid* for the same call in the CallDetailRecord table. To reference a call in the tables, use the *oriLegCallIdentifier* and *destLegIdentifier* field information. Among other things, information about the packets sent and received, jitter, and latency are stored for QoS reports.

CAR Users

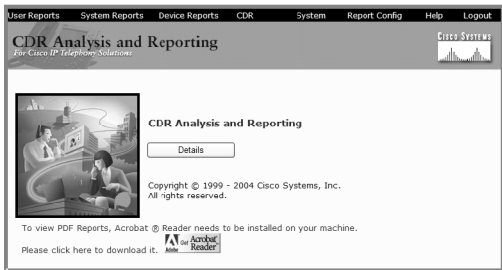
This topic describes the various levels of CAR users.

CAR Users

Cisco.com

The menu available in CAR depends on the user level:

- Administrator
- Manager
- Individual user



© 2005 Cisco Systems, Inc. All rights reserved. CPT2 v4.1--3-6

The available menu in CAR depends on the level of the user. CAR provides reporting capabilities for three levels of users:

- Administrators generate system reports for load balancing, system performance, and troubleshooting. The administrator can also grant administrator access to other users, configure the dial plan and gateway, and set the system preferences.
- Managers generate reports for users, departments, and QoS. The reports provide information for budgeting or security purposes and for determining the voice quality of the calls in their department.
- Individual users generate a billing report for their own calls.

CAR Report Types and User Levels

This topic describes the various types of reports and who can generate them.

CAR Report Types

Cisco.com

- **User reports:**
 - **Bills and Top N**
 - **Cisco IPMA, CTI, and IP Phone services**
- **System reports:**
 - **QoS, traffic, and malicious calls**
 - **Features like MLPP, CMC, and FAC**
 - **System overview**
- **Device reports:**
 - **Gateway and route plan**
 - **Conference and voice messaging**

© 2005 Cisco Systems, Inc. All rights reserved.CIPT2 v4.1-3-7

There are three report types available in CAR:

- The User reports menu allows you to generate reports for bills, Top N users, Cisco IP Manager Assistant (IPMA), computer telephony integration (CTI), and phone services. Bills can be generated for individual users, groups of users, or all users. With the Top N report, it is easy to find, for example, the top five users with the highest cost, highest call duration, or highest number of calls.
- The System reports menu allows you to generate reports for QoS, traffic, and malicious calls. With these reports, it is possible to find part of the network where QoS does not work properly or where there is more traffic than planned in the design phase. Reports for Multilevel Precedence and Preemption (MLPP), CMC, and FAC are also available for information about the cost of projects or controlled long-distance calls with authorization codes.
- Device reports are used to generate information about the gateway, route plans, conferences, and voice messaging. These kinds of reports are useful for the administrator in optimizing the network.

Report and User Type Matrix

Cisco.com

	Administrator	Manager	User
User Reports	✓	Bills, Top N	Only their own bills
System Reports	✓	QoS	✗
Device Reports	✓	✗	✗

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1—3-8

The administrator can generate all types of reports: user reports, system reports, and device reports. Managers can generate only parts of the user and system reports, such as billing, Top N, and QoS reports, and only for employees who report directly or indirectly to the manager. Users can check only their own bills in general or in detail, and send the report by e-mail.

CAR System Parameter Configuration

This topic describes the CAR system parameters in detail.

CAR System Parameter Configuration

Cisco.com

- **Granting and revoking administration rights**
- **Mail server parameters**
- **Dial-plan configuration**
- **Gateway configuration**
- **System preferences**

System Parameters	>	Admin Rights
Scheduler	>	Mail Parameters
Database	>	Dial Plan Configuration
Log Screens	>	Gateway Configuration
Control Center	>	System Preferences

© 2005 Cisco Systems, Inc. All rights reserved. CIPT2 v4.1-3.8

CAR administrators are configured by using the CAR tool itself. Choose **System Parameters > Admin Rights** to assign administrative rights to any user in the Cisco CallManager user database. The manager and user levels are not configured in the CAR tool. These roles are based on the user configuration in the global directory. In Cisco CallManager Administration, choose **User > Global Directory** to edit users in the global directory. For each user, you can configure the user ID of the manager of the user in the Manager User ID field. Users who are configured as managers are assigned to the manager level in CAR. All other users are assigned to the user level in CAR.

It is possible to send alarms and e-mails to administrators. To send reports via e-mail, you must configure the mail server.

CAR classifies external calls based on the outside number. By default, the number is interpreted according to the North American Numbering Plan (NANP). For instance, if the number matches a NANP long-distance call, it is shown as such. You can configure alternative dial plans in CAR using the Dial Plan Configuration menu.

In the gateway configuration, provide the maximum number of ports information for each gateway to enable CAR to generate utilization reports.

Use the system preferences to specify generic parameters, such as the company name, that will be inserted in every report.

Administration Rights and Mail Parameters

Cisco.com

- **Grant or revoke administration rights:**
 - Search for users
 - Add or delete CAR administrators
- **Specify mail parameters:**
 - Mail ID and password
 - Mail domain
 - Mail server name

The screenshot displays two web forms. The top form, titled 'Grant/Revoke CAR Admin Rights', includes a search field for user IDs, a list of 'CAR Administrators' with 'Remove' and 'Remove All' buttons, and an 'Update' button. The bottom form, titled 'Mail Parameters', contains input fields for Mail ID, Password, Confirm Password, Mail Domain, and Mail Server Name, along with an 'Update' button. A status indicator shows 'Update completed!'.

Choose **System Parameters > Admin Rights** to grant or revoke administrative rights to users from the Lightweight Directory Access Protocol (LDAP) directory. You can search for users in the LDAP directory or directly enter the user ID. As stated earlier, access rights for managers and users are not granted in the CAR tool but are derived from the roles configured in Cisco CallManager Administration.

Reports can be sent by e-mail. To enable this feature, choose **System Parameters > Mail Parameters** and configure the e-mail account information. Enter the mail ID and the password that is used by the CAR tool. This e-mail account must exist on the mail server. You also need to specify the mail domain and the mail server name. The mail domain is added automatically when a user enters only the name of the recipient without the mail domain. Every time a report is sent with the CAR tool, this account will be used.

Dial-Plan Configuration

Cisco.com

- Define the toll-free numbers.
- Specify a clause to set the call type.
- Configure the clause with:
 - Activation check box
 - Condition
 - Number of digits
 - Pattern
- Restore the dial plan to the defaults.

Dial Plan Configuration

Toll Free Numbers: 1800.1855.1866.1877.1888

Add Rows Delete Rows

	Condition	No of Digits	Pattern	Call Type
<input type="checkbox"/>	=	5	!	On Net
<input type="checkbox"/>	=	7	!	Local
<input type="checkbox"/>	=	10	T1	Others
<input type="checkbox"/>	=	10	0*	Local
<input type="checkbox"/>	=	10	!	Long Distance
<input type="checkbox"/>	=	11	T1	Others
<input type="checkbox"/>	=	11	XG!	Local
<input type="checkbox"/>	=	11	!	Long Distance
<input type="checkbox"/>	>	3	011!	International

Add Rows Delete Rows

Status: Ready

Update Restore Defaults

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1—3-11

The default dial plan in CAR specifies the NANP. To configure the dial plan, define the parameters for outgoing call classifications. Call classifications include International, Local, Long Distance, On Net, and Others. For example, if local calls in the area are six digits in length, specify a row in the dial plan as follows:

- Condition: =
- No. of Digits: 6
- Pattern: !
- Call Type: **Local**

The table describes the parameters in the Dial Plan Configuration window and lists their possible values.

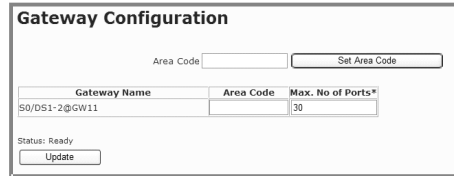
Explanation of Parameters

Parameter	Possible Values	Description
Condition	> < =	Condition of the rule—greater than (>), less than (<), or equal to (=) the specified value in the No. of Digits field.
No. of Digits	NA A digit	Number of digits in the directory number (DN) to which this rule should be applied. If the number of digits does not affect the rule, specify NA.
Pattern	G T ! X	Used for the call classification: <ul style="list-style-type: none">■ “G” means that the call is classified as specified in the rule (that is, G is a wildcard for the gateway area codes specified in the “Gateway Configuration” section).■ “T” retrieves toll-free numbers.■ “!” signifies multiple digits.■ “X” signifies a single-digit number.
Call Type	International Local Long Distance On Net Others	Choose this call type if the condition is satisfied.
Toll Free Numbers	Digits	Numbers in the dial plan that can be placed without a charge.

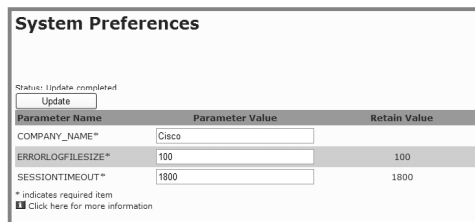
Gateway and System Preferences

Cisco.com

- **Gateway configuration:**
 - Area code
 - Maximum number of ports
- **System preferences:**
 - Company name for the bills
 - Log file size for errors
 - Session timeout



The screenshot shows the 'Gateway Configuration' form. It includes an 'Area Code' input field with a 'Set Area Code' button. Below this is a table with columns for 'Gateway Name', 'Area Code', and 'Max. No of Ports*'. The first row contains the text 'S0/DS1-2@GW11' in the 'Gateway Name' column and '30' in the 'Max. No of Ports*' column. At the bottom of the form, it says 'Status: Ready' and has an 'Update' button.



The screenshot shows the 'System Preferences' form. It has a status indicator 'Status: Update completed' and an 'Update' button. Below is a table with columns for 'Parameter Name', 'Parameter Value', and 'Retain Value'. The table contains three rows: 'COMPANY_NAME*' with value 'Cisco', 'ERRORLOGFILESIZE*' with value '100', and 'SESSIONTIMEOUT*' with value '1800'. A note at the bottom states '* indicates required item' and provides a link for more information.

Parameter Name	Parameter Value	Retain Value
COMPANY_NAME*	Cisco	
ERRORLOGFILESIZE*	100	100
SESSIONTIMEOUT*	1800	1800

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-3-12

Configure the gateways in CAR before using the CAR gateway reports, and update the gateway configuration every time a new gateway is added to the Cisco CallManager Administration. When you delete gateways in Cisco CallManager Administration, they are automatically deleted in CAR. CAR uses the area code information to determine whether calls are local or long distance. Provide the maximum number of ports information for each gateway to enable CAR to generate the utilization reports. Remember, “G” is a wildcard for the gateway area codes used in dial-plan configuration.

Note CAR uses the values provided for the gateway when the gateway was added in Cisco CallManager Administration. Therefore, some gateways will already have an area code setting or have a zero for maximum number of ports, depending on the details specified when the gateway was added in Cisco CallManager Administration.

CAR provides default system preferences, such as these:

- **COMPANY_NAME:** The company name is used as header information in reports.
- **ERRORLOGFILESIZE:** The maximum size of the error log file in kilobytes, with a range from 1 to 9999. The default value is 100.
- **SESSIONTIMEOUT:** The time in seconds that must pass without any activity before a user is logged out of CAR, with a range from 60 to 86,400 (1 minute to 24 hours). The default value is 1800 (30 minutes).


Report Scheduling

This topic describes how to load CDRs and then generate daily, weekly, and monthly reports.

Report Enabling and Scheduling

Cisco.com

- **Specify if and when to load the CDRs from flat files into the database.**
- **Schedule report types for:**
 - **Days**
 - **Weeks**
 - **Months**



```
System Parameters >
Scheduler > CDR Load
Database > Daily
Log Screens > Weekly
Control Center > Monthly
```

© 2005 Cisco Systems, Inc. All rights reserved. CIP12 v4.1-3-13

Every Cisco CallManager writes the CDR data first locally into flat files. A flat file is a temporary file without a file extension. Flat files store call information to import the data on the publisher server into the CDR database. The CDR and CMR flat files are stored in the C:\Program Files\Cisco\CallDetail\ folder on Cisco CallManager.

At a specified time, the flat files are transferred to the Cisco CallManager publisher. Loading CDR data from flat files into the CDR database on the Cisco CallManager publisher can cause performance degradation on the Cisco CallManager server. It is recommended that you use the default loading time or schedule the loading to occur at a time when Cisco CallManager performance will be least affected. By default, CDR data loads every day from midnight to 5 a.m.

Disable CDR loading when you are installing or upgrading the system in the same off hours during which CDR loading normally occurs. Because loading CDRs drains Cisco CallManager resources, CDR loads can be suspended until other operations complete. Of course, the CDR data is not updated when CDR loading is disabled. Be sure to enable CDR loading again as soon as possible. The CAR tool does not affect CDR generation in Cisco CallManager.

Reports can be generated for these periods:

- Days
- Weeks
- Months

Enable and Disable CDR Load

Cisco.com

- **Enable or disable the loading of CDRs.**
- **Specify the CDR load parameters:**
 - Time
 - Loading interval
 - Duration
- **The CDRs should be loaded in nonbusiness hours.**
- **Restore the defaults.**

CDR Load

Disable Loader

Load CDR & CMR

Time* 00 Hr 00 Min Time to start loading of CDRs

Loading Interval* Every 15 minutes Loading Interval

Duration* 01 Min Duration of a loading cycle

Uninhibited Loading of CDR

From* 00 Hr 00 Min Time range for continuous loading of CDRs

To* 23 Hr 59 Min

Status: Ready
Note: Changes made, will take effect at midnight. Restart the Cisco CDR Analysis and Reporting Scheduler service, for the changes to take effect immediately.

Update Restore Defaults

* indicates required item

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1—3-14

The CDR Load menu can be used to enable and disable the CDR load. Disable loading if you are upgrading the Cisco CallManager in the time specified for CDRs to load, otherwise the CDR load will consume a lot of resources.

Configure the Load CDR & CMR area parameters:

- Configure the time when the CAR tool should start to load CDR data from the CDR database into the CAR database.
- The loading interval specifies how often the CDR entries will be loaded. The minimum interval is 15 minutes and the maximum is 24 hours.
- You can define the duration of the loading interval defined to limit the loading time to a maximum length to minimize the impact on Cisco CallManager resources during business hours.

When the loading interval is too long, the waiting time for the next cycle may be too long. Therefore, CAR is not a real-time troubleshooting tool.

In the Uninhibited Loading of CDR area, set the time range for loading CDR data without limitation of the load interval or duration time. Real-time data is not possible. When the reports are not time-critical, set this range to nonbusiness hours, because CDR uses a large volume of Cisco CallManager resources. When there are changes in the CDR load menu for troubleshooting, you can reverse the changes easily with the Restore Defaults button.

Configure the Schedulers

Cisco.com

Configure the schedulers at different times:

- **Daily—Time and Life**
- **Weekly—Day of Week, Time, and Life**
- **Monthly—Day of Month, Time, and Life**

The image shows three screenshots of scheduler configuration forms. Each form has a title, a table for configuration, a status field, a note, and two buttons.

Daily Scheduler

Process	Time	Life
Daily Report Generation*	01:00 AM	02 Day(s)

Status: Ready
Note: Changes made will take effect at midnight. Restart the Cisco CDR Analysis and Reporting Scheduler service, for the changes to take effect immediately.

Update Restore Defaults

Weekly Scheduler

Process	Day of Week	Time	Life
Weekly Report Generation*	Sunday	04:00 AM	02 Week(s)

Status: Ready
Note: Changes made will take effect at midnight. Restart the Cisco CDR Analysis and Reporting Scheduler service, for the changes to take effect immediately.

Update Restore Defaults

Monthly Scheduler

Process	Day of Month	Time	Life
Monthly Bill Generation*	1	03:00 AM	02 Month(s)
Other Monthly Reports*	1	02:00 AM	02 Month(s)

Status: Ready
Note: Changes made will take effect at midnight. Restart the Cisco CDR Analysis and Reporting Scheduler service, for the changes to take effect immediately.

Update Restore Defaults

The schedules can be configured on a daily, weekly, and monthly basis, and they are all preconfigured. The schedulers are preconfigured as follows:

- Daily reports are generated every day at 1 a.m.
- Weekly reports are generated every Sunday at 4 a.m.
- Monthly bills are generated on the first day in the month at 3 a.m., and other reports are generated at 2 a.m., also on the first day in the month.

The Life field in the schedule configuration specifies the number of days, weeks, or months (depending on the type of the schedule) that the reports are stored on the system. Choose the desired value; for example, for weeks, from 0 to 12. After the configured lifetime has elapsed, the reports are deleted.

System Database Configuration

This topic describes CDR database alerts and how to purge the database.

System Database Configuration

Cisco.com

- **Activate CAR and CDR database alerts**
- **Database purging:**
 - **Disable**
 - **Automatic**
 - **Manual**

```
graph LR; A[System Parameters] --> B[Scheduler]; A --> C[Database]; A --> D[Log Screens]; A --> E[Control Center]; C --> F[CAR Database Alert]; C --> G[CDR Database Alert]; C --> H[Manual Purge]; C --> I[Configure Automatic Purge];
```

© 2005 Cisco Systems, Inc. All rights reserved. CPT2 v4.1—3-16

In the System > Database menu, configure CAR to notify an administrator when the CAR database size or CDR database size exceeds a percentage of the maximum number of records. Set the message and the maximum number of records, and specify the alert percentage. The maximum number of records for the CDR database from CAR cannot be edited. Sometimes the database has to be purged to reallocate the database space. Database purging can be disabled, done manually, or done automatically.

CDR and CAR Database Alerts

Cisco.com

- Specify a value for when to notify the administrator when the CDR entries reach the limit.
- Enter the e-mail address of one or more recipients.
- Define the mail subject and message.

The screenshot shows a web-based configuration window titled "CDR Database Alert". It contains the following fields and controls:

- Max number of rows in CDR Table:** 1,500,000
- Notify Users when number of rows reaches*:** 80 %
- Mail to Administrator**
- To...:** CARAdministrator
- Cc...:** (empty)
- Mail Subject:** Alert for CDR database
- Mail Message:** The number of rows in CallDetailRecord table in the CDR database has crossed the threshold limit.
- Status:** Ready
- Buttons:** Update, Restore Defaults

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1—3-17

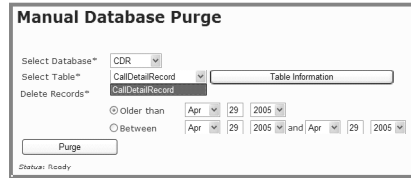
With the database alerts, CAR informs the administrator about predefined alert thresholds:

- For a CAR database alert, the maximum number of rows in the billing table is 2,000,000 rows. A notification is sent when 80 percent of the rows are used. By default, the CAR administrator receives an e-mail, and the users specified in the CC field are also notified. The predefined e-mail subject is "Alert for CAR database." Also, the e-mail message is predefined as "Number of rows in Billing table in the CAR database has crossed the threshold limit."
- For a CDR database alert, the alert mechanism works in the same way, and the threshold is predefined at 80 percent also. The difference is that the maximum number of rows is 1,500,000.

Database Purges

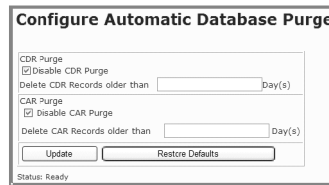
Cisco.com

- **Manual purging parameters:**
 - **View table information first**
 - **Database**
 - **Table**
 - **Date range**
- **Automatic purging parameters:**
 - **Disable**
 - **Enable**
 - **Restore defaults**



The 'Manual Database Purge' window contains the following fields and controls:

- Select Database*: CDR (dropdown)
- Select Table*: CallDetailRecord (dropdown) with a 'Table Information' button to its right.
- Delete Records*: CallDetailRecord (dropdown)
- Radio buttons for 'Older than' and 'Between'.
- Date pickers for 'Older than' (Apr 29 2005) and 'Between' (Apr 29 2005 and Apr 29 2005).
- Purge button.
- Status: Ready.



The 'Configure Automatic Database Purge' window contains the following fields and controls:

- CDR Purge section:
 - Disable CDR Purge
 - Delete CDR Records older than [] Day(s)
- CAR Purge section:
 - Disable CAR Purge
 - Delete CAR Records older than [] Day(s)
- Update button.
- Restore Defaults button.
- Status: Ready.

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1—3-18

Storage in the database is limited, so the database has to be purged from time to time. Do this operation manually in the Manual Database Purge configuration area, following these steps:

- Step 1** In CAR, choose **System > Database > Manual Purge**. Choose the database in the Select Database drop-down list. The two possible options are CAR and CDR.
- Step 2** Choose the table to purge using the Select Table drop-down list. Possible values are the CallDetailRecord, Tbl_Billing_Data, Tbl_Error_Log, and Tbl_Purge_History tables. The Table Information button displays an overview of the number of records in each of the tables and shows when the first and last records were stored in the database.
- Step 3** To delete records, use the Delete Records option. Database entries older than the date specified in the Older Than field or from the range of dates specified in the Between fields will be deleted.
- Step 4** Click the **Purge** button.

The databases can also be purged automatically by configuring the parameters in the Configure Automatic Database Purge area. All data older than the specified number of days will be deleted from the CDR or CAR database. In most cases, third-party products are used for billing. Make sure that the database is not purged before the billing system has replicated the data. Some billing products are also able to delete the data after a successful replication. Be aware that there is no way to restore the deleted database entries after the purge. Automatic purging of both the CDR and CAR databases is disabled by default.

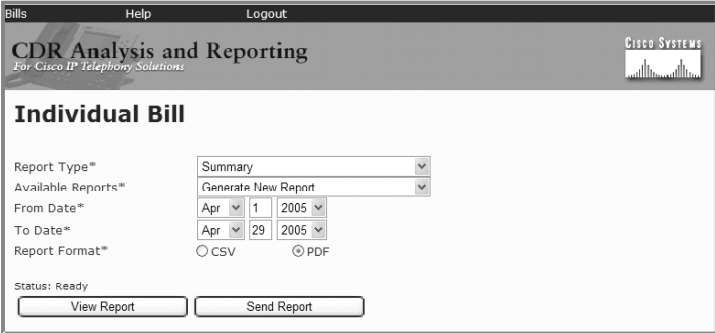
User Report Configuration

This topic describes how users can generate a report of their own bills.

User Report Configuration

Cisco.com

- Browse to <https://<CCM IP address>/ART>.
- Users can only see their own bills (data privacy).
- View or send reports via e-mail.



© 2005 Cisco Systems, Inc. All rights reserved. CIP72 v4.1-3-19

To access the CAR tool, browse to <https://CM/ART> and log in with your username and password. A single user has limited access to the CDR database and can generate only a report for his or her own calls. This limitation helps ensure the privacy of the call data for users.

A user can generate an individual bill in a summary or detailed form. To generate a report, choose either the CSV or PDF report format, set the time range, and click the **View Report** button. For a PDF report, Adobe Acrobat Reader must be installed on the PC from which the user is browsing to CAR. To send the report by e-mail, click the **Send Report** button.

View Report

Cisco.com

- The report is in PDF format.
- The report type is detailed.

Individual Bill - Detail							
From Date: Apr 1, 2005				Date: Apr 29, 2005			
To Date: Apr 29, 2005				Page: 1 of 1			
Date	Orig. Time	Orig.	Dest.	Call Classification	QoS	Duration (sec)	Charge
Bill for John Doe							
Apr 28, 2005	11:48:52 AM	2017	2018	Internal	NA	1	0.00
Apr 28, 2005	11:48:59 AM	2017	2018	Internal	NA	4	0.00
Apr 28, 2005	11:49:09 AM	2017	2018	Internal	NA	3	0.00
Apr 28, 2005	11:52:01 AM	2017	2018	Internal	NA	4	0.00
Apr 28, 2005	11:52:08 AM	2017	2018	Internal	NA	3	0.00
Apr 28, 2005	11:52:14 AM	2017	2018	Internal	NA	3	0.00
Apr 28, 2005	11:59:59 AM	2017	2018	Internal	NA	4	0.00
Apr 28, 2005	12:00:06 PM	2017	2018	Internal	NA	5	0.00
Apr 28, 2005	12:00:13 PM	2017	2018	Internal	NA	4	0.00
Apr 28, 2005	12:10:49 PM	2017	2018	Internal	NA	5	0.00
Apr 28, 2005	12:10:57 PM	2017	2018	Internal	NA	4	0.00
Total for John Doe						40	0.00

© 2005 Cisco Systems, Inc. All rights reserved.

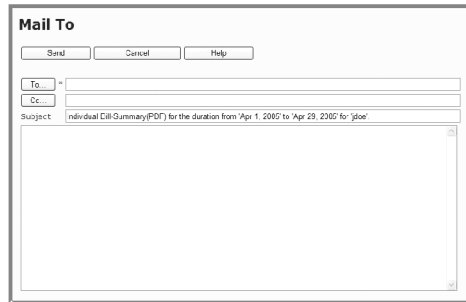
CIPT2 v4.1—3-20

In this example, the user clicked the View Report button after specifying PDF format, and the individual bill was generated. As the figure shows, the user made all the calls shown on April 28, 2005, between 11:48 a.m. and 12:11 p.m. All the calls were internal, and the destination was extension 2018. The calls were very short—the longest lasted only 5 seconds. This implies there was a problem or the user made only some test calls.

Send Report

Cisco.com

- **Enter the recipients of the report.**
- **The PDF is automatically attached.**
- **The subject is predefined.**
- **Optionally add a message to the e-mail.**
- **Click Send.**



The screenshot shows a 'Mail To' dialog box with the following elements:

- Buttons: Send, Cancel, Help
- To: [Empty text field]
- CC: [Empty text field]
- Subject: Individual Call Summary(PDF) for the duration from 'Apr 1, 2005' to 'Apr 23, 2005' for 'jdoe'
- Message body: [Large empty text area]

© 2005 Cisco Systems, Inc. All rights reserved.

CIP72 v4.1-3-21

Alternatively, the user could click the Send Report button to display a window for sending an e-mail after the user specifies the recipients. The user could also send copies by specifying the relevant e-mail addresses in the CC field. The subject of the mail is predefined. Users can add information in the text field if necessary and click Send to e-mail this report to the specified recipients.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **CAR was formerly known as ART and has to be installed on the publisher server.**
- **The CDRs are stored in the CallDetailRecord table and the CMRs in the CallDetailRecordDiagnostic table.**
- **Three kinds of users are defined: users, managers, and administrators.**
- **Three types of reports are available: user, system, and device reports.**

© 2005 Cisco Systems, Inc. All rights reserved. CPT2 v4.1—3-22

Summary (Cont.)

Cisco.com

- **CAR administrators are assigned that access level assigned using the CAR tool. Configure the gateways and the dial plan before generating any reports.**
- **Disable CDRs when you are upgrading Cisco CallManager. Define the time to generate the daily, weekly, and monthly reports.**
- **The database alert informs the administrator when the threshold is exceeded. Purge the database manually or automatically.**
- **User reports can be generated in summary or in detail and can be sent via e-mail.**

© 2005 Cisco Systems, Inc. All rights reserved. CPT2 v4.1—3-23

Lesson 3-5

Using Additional Management and Monitoring Tools

Overview

Management and monitoring tools are available to help system administrators monitor, troubleshoot, and manage the health of an IP telephony network. This lesson explains Cisco CallManager tools such as dependency records, Password Changer tool, and Cisco Dialed Number Analyzer. The Quality Report Tool (QRT), a tool used by end users to report IP Phone issues to administrators, is also covered.

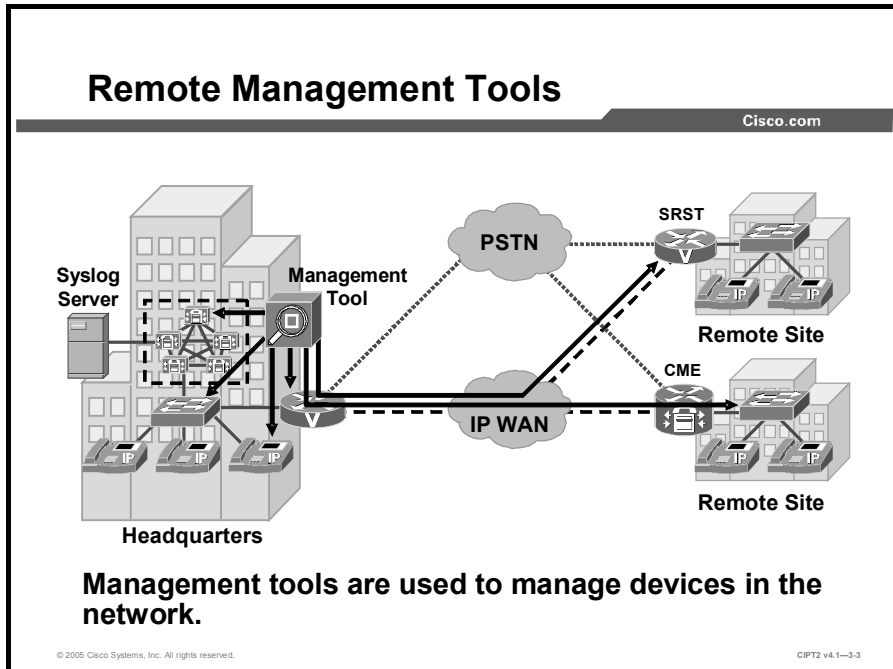
Objectives

Upon completing this lesson, you will be able to use additional management and monitoring tools. This ability includes being able to meet these objectives:

- Explain the use of SNMP, syslog, and CiscoWorks ITEM in remotely managing and maintaining a Cisco CallManager system
- Explain the use of dependency records, enable them, and access them
- Use the Password Changer tool to change passwords
- Use the Cisco Dialed Number Analyzer to analyze inbound and outbound calls in a Cisco CallManager dial plan
- Configure the QRT feature to display IP Phone problem reports from users

Remote Management Tools

This topic describes remote management tools that are used to monitor a network.



Network management software, such as CiscoWorks IP Telephony Environment Monitor (ITEM) or syslog servers, performs specific tasks to monitor and manage the health and availability of devices in a network. These tools are typically used in large-scale data networks (such as computer networks and telecommunication networks).

CiscoWorks ITEM Overview

Cisco.com

CiscoWorks ITEM can be used to:

- **Manage network devices:**
 - Gateways, switches
- **Manage IP telephony devices:**
 - Cisco CallManager, Unity, IP Phones
- **Monitor devices:**
 - Send alarms and alerts to e-mail addresses, pagers, and CiscoWorks clients

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1—3-4

CiscoWorks ITEM is a powerful suite of applications and tools that continuously evaluate and report on the operational health of the Cisco IP telephony implementation. CiscoWorks ITEM is used to manage Cisco Architecture for Voice, Video and Integrated Data (AVVID) and Cisco IOS software-based IP telephony environments. CiscoWorks ITEM provides the following:

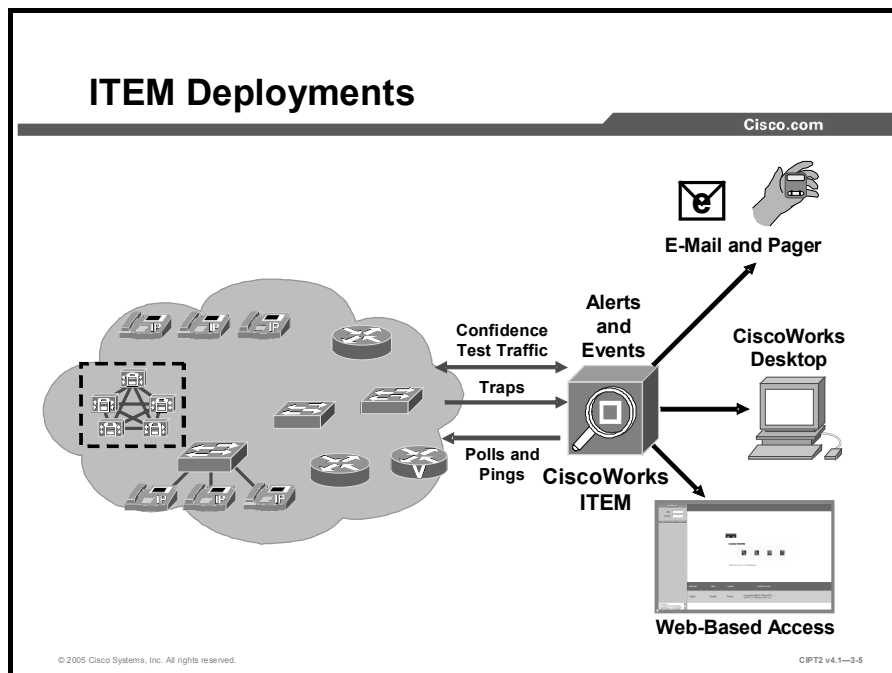
- Proactive health and fault monitoring of converged IP networks and IP telephony implementations
- Powerful tools to effectively manage the day-to-day customer care responsibilities of help-desk personnel
- The ability to capture performance and capacity management data

CiscoWorks ITEM consists of a product suite:

- **CiscoWorks IP Telephony Monitor (ITM):** Monitors Cisco voice elements in the network to alert operations personnel to potential problems and to help minimize downtime. It also includes CiscoWorks Common Services, a common foundation for data storage, login, access privileges, and navigation and launch management for all CiscoWorks applications.
- **CiscoWorks IP Phone Information Utility (IPIU):** Provides operational status and implementation details about an individual IP Phone. It also provides security reports that document IP Phone moves, adds, and changes, as well as information about the physical and logical connections of every Cisco IP phone installed in a given network.
- **CiscoWorks IP Phone Help Desk Utility (IPHDU):** Reports operational status and implementation details about individual IP Phones. It works in conjunction with IPIU to make read-only access to Cisco IP Phone installation details available to help-desk personnel.
- **CiscoWorks ITEM Gateway Statistics Utility (GSU):** Collects performance and behavior statistics about IP telephony gateways controlled by Cisco CallManager and Cisco IOS software, which can be processed by third-party software to produce utilization and capacity management reports.

- **CiscoWorks WAN Performance Utility (WPU):** Measures the performance, latency, and availability of multiprotocol IP networks on an end-to-end and hop-by-hop (router-to-router) basis.

Several optional components can be downloaded from Cisco.com.



CiscoWorks ITEM also provides real-time fault detection and determination about the underlying Cisco IP fabric on which the IP telephony implementation executes. CiscoWorks ITEM reports faults that occur on Cisco network devices, often identifying problems before users of network services realize that a problem exists. CiscoWorks ITEM supports more than 200 types of the most popular Cisco routers, switches, access servers, and hubs. For each of these supported devices, CiscoWorks ITEM automatically looks for a broad spectrum of common problems at the device and VLAN level, all without ever requiring operations managers to write rules or set polling or threshold values. CiscoWorks ITEM can listen to traps or can send polls and pings to get information for devices. CiscoWorks ITEM can send alerts and events automatically to an e-mail client or a pager. To monitor the network, CiscoWorks ITEM can be accessed via a web-based interface or a CiscoWorks desktop client.

Network management systems (NMSs) use Simple Network Management Protocol (SNMP), an industry-standard interface, to exchange management information between network devices. SNMP is an application-layer protocol, part of the TCP/IP protocol suite. SNMP enables administrators to remotely manage network performance, find and solve network problems, and plan for network growth.

There are three versions of SNMP:

- SNMP Version 1 (SNMPv1)
- SNMP Version 2 (SNMPv2)
- SNMP Version 3 (SNMPv3)

SNMPv1 and SNMPv2 have a number of common features, but SNMPv2 offers enhancements, such as additional protocol operations. Standardization of SNMPv3 is pending.

SNMP Basics

An SNMP-managed network comprises three key components:

- **Managed devices:** A managed device designates a network node that contains an SNMP agent and resides on a managed network. Managed devices collect and store management information and make it available by using SNMP.
- **Agents:** An agent, as network management software, resides on a managed device. An agent contains local knowledge of management information and translates it into a form that is compatible with SNMP.
- **NMSs:** A NMS comprises an SNMP management application together with the computer on which it runs. An NMS executes applications that monitor and control managed devices. An NMS provides the bulk of the processing and memory resources that are required for network management. These NMSs share compatibility with Cisco CallManager:
 - CiscoWorks2000
 - HP OpenView
 - Third-party applications that support SNMP and Cisco CallManager SNMP interfaces

This list specifies Cisco CallManager SNMP trap messages that are sent to an NMS that is specified as a trap receiver:

- Cisco CallManager failed
- Phone failed
- Phones status update
- Gateway failed
- Media resource list exhausted
- Route list exhausted
- Gateway Layer 2 change
- Quality report
- Malicious call

SNMP itself is a simple request-and-response protocol. NMSs can send multiple requests without receiving a response. Six SNMP operations are defined in the table.

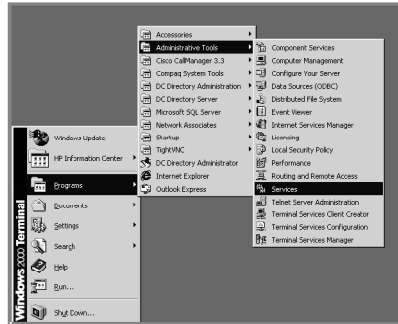
SNMP Operations

Operation	Definition
Get	Allows the NMS to retrieve an object instance from the agent.
GetNext	Allows the NMS to retrieve the next object instance from a table or list within an agent. In SNMPv1, when an NMS wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
GetBulk	New for SNMPv2. The GetBulk operation was added to make it easier to acquire large amounts of related information without initiating repeated get-next operations. GetBulk was designed to virtually eliminate the need for GetNext operations.
Set	Allows the NMS to set values for object instances within an agent.
Trap	Used by the agent to asynchronously inform the NMS of some event. The SNMPv2 Trap message is designed to replace the SNMPv1 Trap message.
Inform	New for SNMPv2. The Inform operation was added to allow one NMS to send Trap information to another.

SNMP Configuration on Cisco CallManager

Cisco.com

- **SNMP service must be enabled for each device that should be monitored.**
- **On Cisco CallManager, choose Start > Programs > Administrative Tools > Services and choose SNMP Service.**



© 2005 Cisco Systems, Inc. All rights reserved.

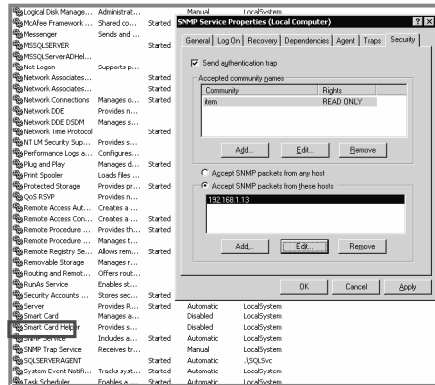
CIPT2 v4.1-3-6

Administrators have to enable SNMP for each device in the network that they want to monitor. For example, if you want to monitor Cisco CallManager with SNMP, on the Cisco CallManager server, click **Start > Programs > Administrative Tools > Services**. In the service menu, search for the SNMP service and open the service to configure it.

SNMP Service Configuration

Cisco.com

- Click Add to enter the accepted community names (such as, “item”)
- Click Accept SNMP Packets from These Hosts (for example, IP address 192.168.1.13)



© 2005 Cisco Systems, Inc. All rights reserved.

C IPT2 v4.1—3-7

Cisco CallManager supports SNMPv1 and SNMPv2. SNMPv1 lacks authentication capabilities (SNMPv2 increases the security capabilities of SNMP, and SNMPv3 supports authentication and encryption), which results in vulnerability to a variety of security threats:

- Masquerading consists of an unauthorized entity attempting to perform management operations by assuming the identity of an authorized management entity.
- Modification of information involves an unauthorized entity attempting to alter a message generated by an authorized entity so that the message results in unauthorized accounting management or configuration management operations.
- Message sequence and timing modifications occur when an unauthorized entity reorders, delays, or copies and later replays a message generated by an authorized entity.
- Disclosure results when an unauthorized entity extracts values stored in managed objects, or learns of notifiable events by monitoring exchanges between managers and agents.

Because SNMPv1 does not implement authentication, many vendors do not implement Set operations, thus reducing SNMP to a monitoring facility.

The first thing you need to do is enable SNMP access. Enable access by configuring community strings, which act somewhat like passwords. The difference is that there can be several community strings and that each of them may grant a different form of access.

A community string can be the following:

- **Read-only:** Gives read access to all objects in the MIB except the community strings but does not allow write access
- **Read-write:** Gives read and write access to all objects in the MIB but does not allow access to the community strings
- **Read-write-all:** Gives read and write access to all objects in the MIB, including the community strings

To define the SNMP read community string, complete these steps:

- Step 1** Choose **Start > Programs > Administrative Tools > Services**.
- Step 2** Choose the **SNMP** service, double-click the service name, and choose **Security**.
- Step 3** In the Security window, define community strings and assign them read permission.

This would now be the read community string. In the example in the figure, the community string is “item.”

Cisco Systems supports numerous MIBs that organize and distribute information for a variety of network management devices.

You can use the MIB table that supports Cisco CallManager to provide all of the management interfaces for monitoring and managing your Cisco CallManager network. This MIB table is periodically updated, reflecting the current status of your Cisco CallManager network:

- **Using the CISCO-CCM-MIB:** To perform network management, you can use the CISCO-CCM-MIB to get provisioning and statistical information about Cisco CallManager, its associated devices (for example, IP Phones and gateways), and its configuration.
- **Using the CISCO-CDP-MIB:** You can use the Cisco CallManager SNMP agent to implement the Cisco Discovery Protocol MIB, CISCO-CDP-MIB. This MIB enables Cisco CallManager to advertise itself to other Cisco devices on the network, allowing discovery of other Cisco CallManager installations on the network.

Note To get more information about the actual MIB tables, go to Cisco.com and search for CISCO-CCM-MIB.

Syslog Overview

Cisco.com

Syslog provides:

- Logging of events (such as information and errors) to a syslog server over the IP network
- Local logging of network events to files

Syslog messages can be sent to one of the following:

- CiscoWorks server
- Third-party syslog server
- Local host (Remote Syslog Analyzer Collector [RSAC] software must be installed)

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1—3-8

Syslog allows logging of errors or other events across the network to various destinations.

Syslog provides an orderly presentation of information that assists in the diagnosis and troubleshooting of system problems. These messages can be saved in a file or sent to, for example, a CiscoWorks server, a third-party syslog server (such as Kiwi Syslog Daemon), or the host itself.

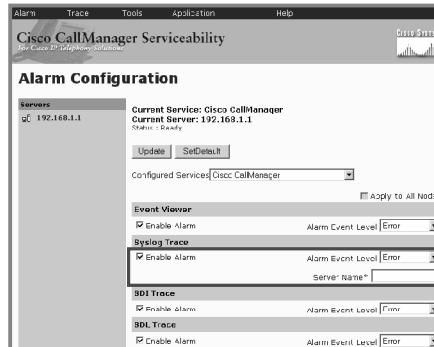
Note Kiwi Syslog Daemon is a freeware Windows syslog server. It receives, logs, displays, and forwards syslog messages from hosts, such as routers, switches, UNIX hosts, and any other syslog-enabled device. For more information, go to <http://www.kiwisyslog.com>.

When the local host is used, Remote Syslog Analyzer Collector (RSAC) software must be installed. RSAC can be installed on a remote UNIX or Microsoft Windows 2000 or Windows NT machine to process syslog messages.

Sending Alarms to a Syslog Server

Cisco.com

- Located in Cisco CallManager Serviceability
- Syslogs sent to local host if server name is not specified
- Configure event level to select syslog messages (Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug)



© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1-3.9

Cisco CallManager syslog messages are configured in Cisco CallManager Serviceability. To configure alarms, choose **Cisco CallManager Serviceability > Alarm > Configuration**.

The table lists alarm events that can be configured in the alarm trap.

Configurable Alarm Events

Name	Destination Description
Enable Alarm for Event Viewer	Windows 2000 Event Viewer program. The program logs Cisco CallManager errors in the application logs within Event Viewer, and provides a description of the alarm and a recommended action.
Enable Alarm for Syslog	Check the Enable Alarm check box in the Syslog Trace area of the Alarm Configuration window to enable the syslog messages and configure the syslog server name. If this destination is enabled and no server name is specified, Cisco CallManager sends syslog messages to the local host. Cisco CallManager stores alarm definitions and recommended actions in a Standard Query Language (SQL) server database. The system administrator can search the database for definitions of all the alarms. The definitions include the alarm name, description, explanation, recommended action, severity, parameters, and monitors This box is unchecked by default.
Enable Alarm for System Diagnostic Interface (SDI) Trace	The SDI trace library. Ensure that this alarm destination is configured in Trace configuration of Cisco CallManager Serviceability.
Enable Alarm for Signal Distribution Layer (SDL)	The SDL trace library. This destination applies only to the Cisco CallManager and Cisco CTIManager services. Configure this alarm destination using Trace SDL configuration.

The table lists alarm levels used by Cisco CallManager.

Alarm Event Levels

Level	Name	Description
7	Emergency	This level designates the system as unusable.
6	Alert	This level indicates that immediate action is needed.
5	Critical	Cisco CallManager detects a critical condition.
4	Error	This level signifies that an error condition exists.
3	Warning	This level indicates that a warning condition is detected.
2	Notice	This level designates a normal but significant condition.
1	Informational	This level designates information messages only.
0	Debug	This level designates detailed event information used for debugging by Cisco Technical Assistance Center (TAC) engineers.

The Cisco CallManager Serviceability Alarms window provides a web-based interface that has two main functions:

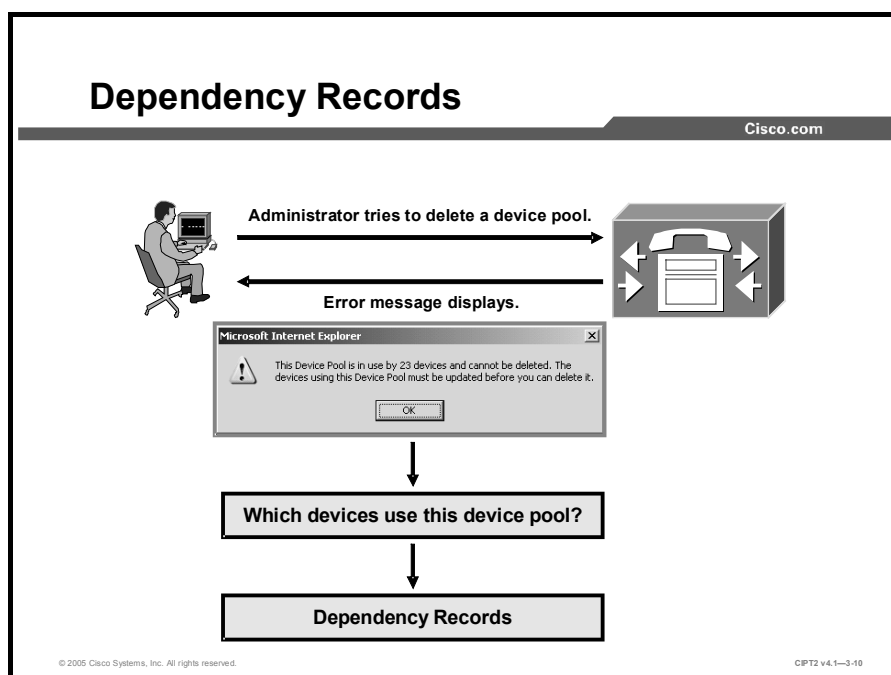
- To configure alarms and events
- To provide alarm message definitions

Both functions assist the system administrator and support personnel in troubleshooting Cisco CallManager problems. Alarms can be configured for Cisco CallManager servers in a cluster and for services for each server, such as Cisco CallManager, Cisco TFTP, and Cisco CTIManager.

Alarms can be forwarded to a Serviceability Trace file. The administrator configures alarms and trace parameters and provides the information to a Cisco TAC engineer. Administrators can direct alarms to the Windows 2000 Event Log, syslog, an SDI trace log file, an SDL trace log file (for Cisco CallManager and CTIManager only), or to all these destinations.

Dependency Records

This topic describes the use of dependency records in a Cisco CallManager environment.



In Cisco CallManager Administration, numerous configuration elements are referenced by other elements (for example, a route pattern refers to a route list, which refers to a route group, which refers to a gateway). In many cases, you cannot delete or even modify such elements if they are currently referenced elsewhere in the system. It can be difficult and time-consuming to find out which configuration element is referencing the element that you are trying to delete or modify. The mechanism that allows you to determine, delete, change, or modify a record in Cisco CallManager is called dependency records. Dependency records help you to determine which records in the Cisco CallManager database use other records. For example, which devices (such as computer telephony integration [CTI] route points or IP Phones) use a particular calling search space?

To delete a record from Cisco CallManager, you can use dependency records to show which records are associated with the record that you want to delete. You can then reconfigure those records so that they are associated with a different record.

Example

The administrator tries to delete a device pool. A message is displayed that some devices still use this pool. The administrator clicks the dependency records link to find out which devices use this device pool.

Enabling Dependency Records

Cisco.com

- **Choose** Cisco CallManager Administration > Service > Service Parameters.
- **Set the value to True to display dependency records.**
- **Displaying dependency records leads to high CPU usage and takes time; it executes in a low-priority thread.**

CCMAdmin Parameters		
Parameter Name	Parameter Value	Suggested Value
Enable Dependency Records*	<input type="text" value="True"/>	False

© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1—3-11

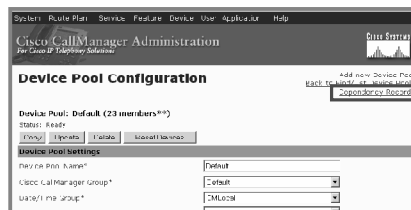
Because dependency records are disabled by default, they must be activated in the Cisco CallManager Administration Service Parameter window if you want to use the feature. Set the Enable Dependency Records parameter to True to activate dependency records and display them as an option in Cisco CallManager Administration (Cisco CallManager Administration page > System > Enterprise Parameters).

Caution Displaying dependency records leads to high CPU usage and takes some time because it executes in a low-priority thread. If you are monitoring CPU usage, you may see high CPU usage alarms. To avoid possible performance issues, display dependency records only during off-peak hours or during the next maintenance window. Close and reopen the web browser for the parameter change to take effect.

Accessing Dependency Records

Cisco.com

- **Dependency records can be found on every configuration window in Cisco CallManager.**
- **In this example, click the Dependency Records link to see all devices or items using device pool "Default."**



© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1—3-12

To access dependency records from a Cisco CallManager configuration window, click the **Dependency Records** link. The Dependency Records Summary window appears. This window displays the number and type of records that use the record that is shown in the Cisco CallManager configuration window.

Note If the dependency records are not enabled, the Dependency Records Summary window displays a message that no information about the record exists.

Dependency Records Summary

Cisco.com

- The window lists all records that refer to the record where you clicked the dependency record link.
- The list is in summary style and only shows the depending records by type and number.
- To get detailed information, click an entry.
- Click a single entry on the Detail page to go to the configuration page of the device.

The image shows two overlapping windows from a Cisco management interface. The top window is titled "Dependency Records Summary" and displays a table of records. The bottom window is titled "Dependency Records - Detail" and shows a detailed view of a specific record.

Dependency Records Summary

6/2 Record(s) are using Device Pool Default

Refresh Close Close and Go Back

Record Count	Record Type
39	Device Defaults
5	Phone
4	Gateway
1	Conference Bridge
1	Media Termination Point/Transcoder
10	Cisco-voice Mail Port

Dependency Records - Detail

5 Phone(s) are using Device Pool Default

Matching record(s) 1 to 5 of 5

Device Name	Description
SEP30055600121	Auto 2036
SEP30055600117	Phone1-7
SEP30055600111	Phone1-1
SEP30055600111	Auto 2035
SEP30055600122	Auto 2037

Page 1 of 1

To display detailed dependency records information, click the corresponding record; for example, click the Phone record. The Dependency Records Detail window appears.

After you click the dependency records link in an administration window, you will see a list of all records that refer to the item that you selected. This list is in summary style and shows the depending records only by type and number. You can click an entry of the summary list to view the detailed list of dependent records. You can click a single device in the dependency records detail window to go to the configuration window of the device. To return to the original configuration window, click the **Back to <configuration window name>** link.

Dependency Records Buttons

Three buttons are available in the Dependency Records Summary window:

- **Refresh:** Updates the window with the most up-to-date information.
- **Close:** Closes the window but does not return to the Cisco CallManager configuration window in which the user clicked the Dependency Records link.
- **Close and Go Back:** Closes the window and returns to the Cisco CallManager configuration window in which the user clicked the Dependency Records link.

Password Changer Tool

This topic describes the Password Changer tool of Cisco CallManager.

Password Changer Tool

Cisco.com

- **Tool to change the passwords for:**
 - **CCMSysUser**
 - **CCMAdministrator**
 - **IPMASysUser**
 - **Directory Manager**
- **Must be run on the publisher database server**
- **Run on all servers in cluster when changing Directory Manager password**
- **Installed by default**

© 2005 Cisco Systems, Inc. All rights reserved.CPT2 v4.1-3-14

The Password Changer tool is used to change the CCMAdministrator, IPMASysUser, CCMSysUser, or the Directory Manager accounts. The Password Changer tool is stored by default on every Cisco CallManager server in the cluster. When you want to change the Directory Manager password, you must change it on every Cisco CallManager server in the cluster (publisher and subscriber). For the other accounts, the password must be changed only on one server in the cluster.

Note The CCMAdministrator account is used only when you are using multilevel administration access (MLA). The Microsoft Windows administrator account is used when MLA is not used. When you change the password for the Windows administrator account, you have to use the new password when you log in to Cisco CallManager Administration. The Windows administrator account cannot be changed with the Cisco Password Changer tool, while the passwords for users in the DC-Directory of Cisco CallManager can. When Cisco CallManager is integrated in a Lightweight Directory Access Protocol (LDAP) directory, the users are changed directly in the corresponding LDAP directory.

These users can be changed with the Password Changer tool:

- **CCMAdministrator:** CCMAdministrator is used as the administrator account when you are using MLA.
- **CCMSysUser:** Cisco Extended Functions, Cisco Tomcat, and Cisco CallManager Extension Mobility services use a special user, cn=CCMSysUser and mail=CCMSysUser (Netscape) or SAMAccountName=CCMSysUser (Microsoft Active Directory), to authenticate with Cisco CallManager.
- **IPMASysUser:** IPMASysUser is used by Cisco IP Manager Assistant (IPMA) to authenticate with Cisco CallManager.

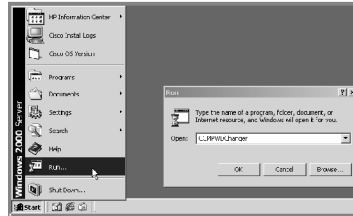
- **Directory Manager:** Directory Manager is the superuser account for the integrated LDAP database in Cisco IP telephony systems. In Cisco CallManager, it is the DC-Directory.

The CCMAAdministrator, CCMSysUser, and the IPMASysUser accounts can be found in the Organizational Unit (OU) ou=users in the DC-Directory of Cisco CallManager. The Directory Manager account can be found under o=cisco.com in the DC-Directory.

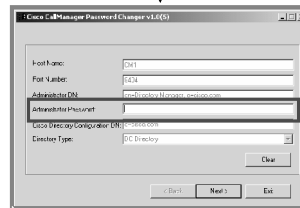
Start Password Changer Tool

Cisco.com

① Choose Cisco CallManager Publisher > Start > Run > CCMFWDChanger.



② Enter the DC-Directory administrator password to get access to the Password Changer tool.



© 2005 Cisco Systems, Inc. All rights reserved.

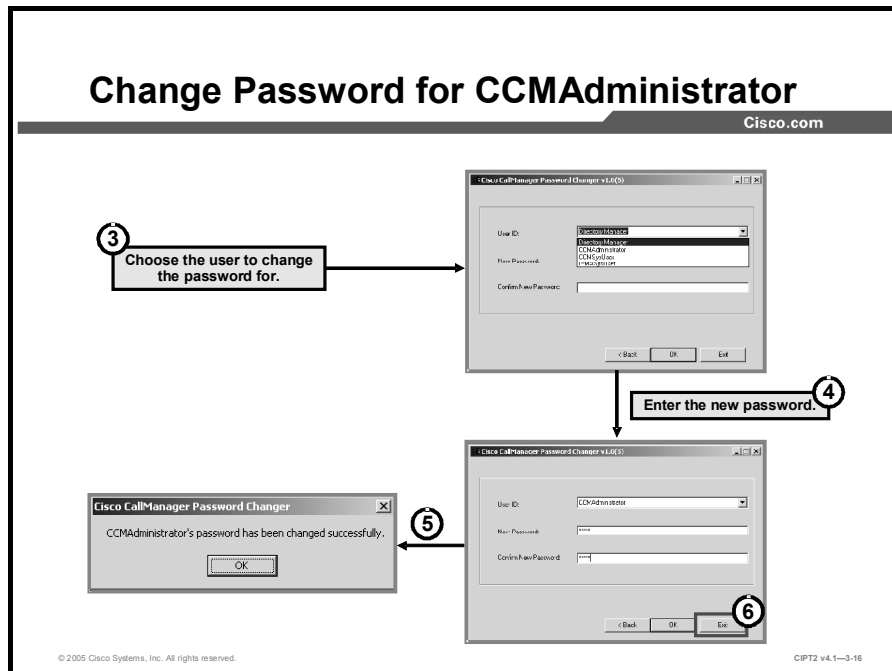
CIPT2 v4.1-3-15

To start the Password Changer tool, complete these steps:

- Step 1** Choose **Start > Run > CCMFWDChanger** in Cisco CallManager.
- Step 2** After a few seconds, you will be able to enter the DC-Directory administrator password (not the administrator password that is used to access the server). Click **Next**.

Change Password for CCMAdministrator

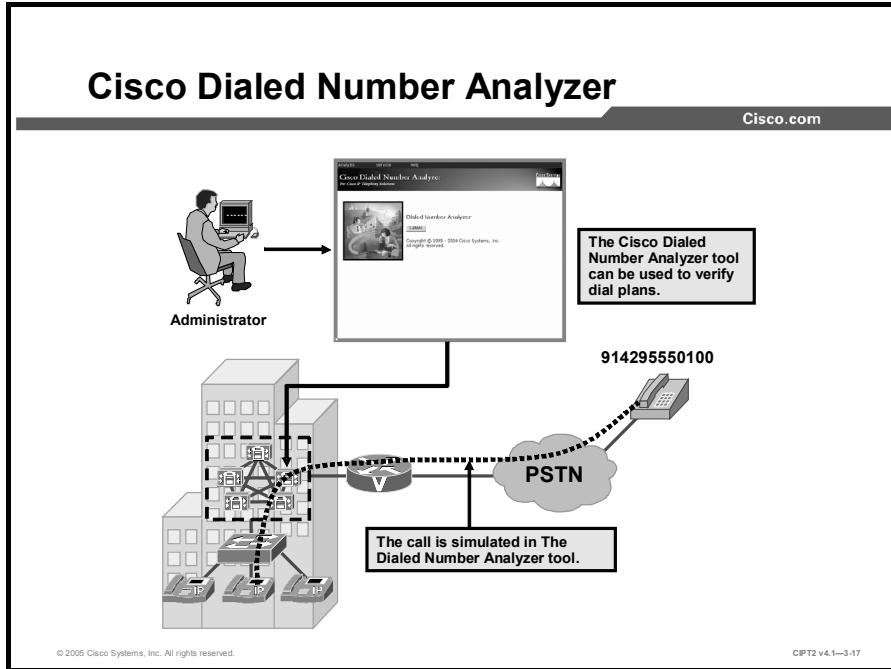
Cisco.com



- Step 3** Choose the user whose password you want to change.
- Step 4** Enter the new password twice.
- Step 5** A message notifies you that the password for the user has been successfully changed. Click **OK** to close the window.
- Step 6** After finishing all password changes, click **Exit** to leave the Password Changer tool. The next time that you log in to Cisco CallManager Administration, the new passwords take effect.

Cisco Dialed Number Analyzer

This topic describes the Cisco Dialed Number Analyzer.



The Dialed Number Analyzer is installed as a plug-in in Cisco CallManager. The tool allows you to test a Cisco CallManager dial-plan configuration prior to deploying it. The tool simulates, for example, internal-to-internal calls and internal-to-external calls. You can also use the tool to analyze dial plans after the dial plan is deployed or to test dial plans before deployment.

A dial plan can be very complex, involving multiple devices, translation patterns, route patterns, route lists, route groups, calling- and called-party transformations, and device-level transformations. Because of this complexity, a dial plan may contain errors. You can use Dialed Number Analyzer to test a dial plan by providing dialed digits as input. The tool analyzes the dialed digits and shows details of the calls. You can use these results to diagnose the dial plan, identify problems, if any, and tune the dial plan before it is deployed.

Cisco Dialed Number Analyzer Overview

Cisco.com

- **A tool that can be used to:**
 - **Diagnose the dial plans in a deployed system**
 - **Tune predeployment dial plans**
 - **Trace path for given dialed digits**
- **Tool considers different types of the calls, such as:**
 - **IP Phone to IP Phone**
 - **Gateway to IP Phone**
 - **IP Phone to gateway**
 - **Gateway to gateway**
 - **Calls to feature-specific patterns**

© 2005 Cisco Systems, Inc. All rights reserved.

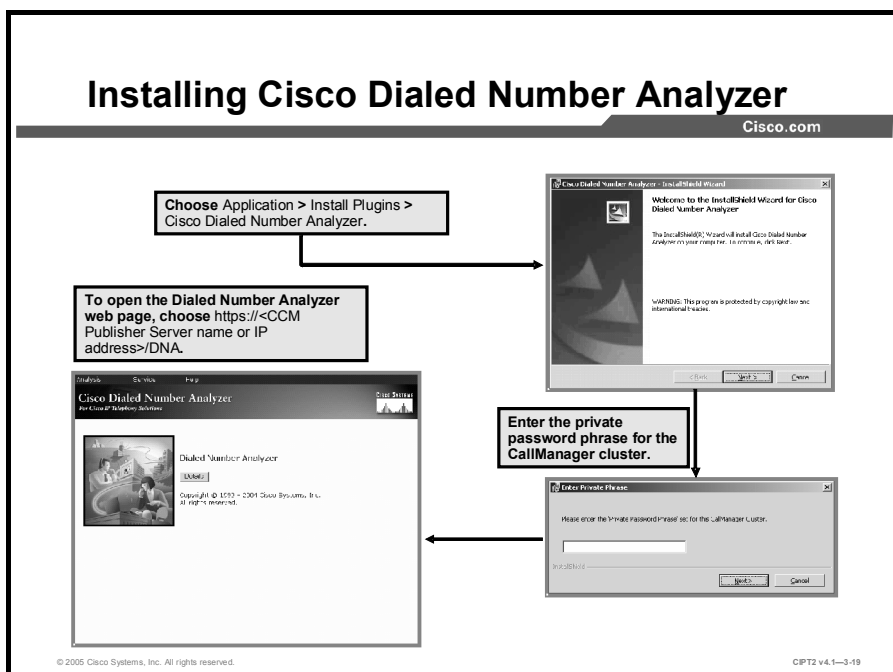
CIP72 v4.1—3-18

Cisco Dialed Number Analyzer runs as a service that can be accessed from the server on which it is installed or from a remote PC. It runs as a low priority and does not affect Cisco CallManager performance.

With the Cisco Dialed Number Analyzer tool, you can analyze various types of calls, such as IP Phone-to-IP Phone, gateway-to-IP Phone, IP Phone-to-gateway, and gateway-to-gateway calls. Further, you can analyze calls to feature-specific patterns, such as CTI route points or pilot points, as well.

Installing Cisco Dialed Number Analyzer

Cisco.com



Dialed Number Analyzer includes a separate executable file that is available in the Cisco CallManager plug-ins window. You can install Dialed Number Analyzer if Cisco CallManager Release 3.3(4) or later has been installed. You can install Dialed Number Analyzer on any Cisco CallManager node in a cluster, either publisher or subscriber. Install Dialed Number Analyzer preferably on the publisher to use the actual SQL database that is used by all Cisco CallManager servers. During the installation, you have to enter the Cisco CallManager cluster private password phrase. When Dialed Number Analyzer is installed, it installs as a service called Cisco Dialed Number Analyzer. You can start and log in to Dialed Number Analyzer from the server on which it is installed or from a remote PC by using a web browser (Microsoft Internet Explorer 6.0 or later versions).

The Dialed Number Analyzer tool can be installed from the Cisco CallManager Plugins web page at Application > Install Plugins > Cisco Dialed Number Analyzer.

To access the Dialed Number Analyzer tool, go to <http://<cmaddress>/dna/main.asp>, where <cmaddress> specifies the node name or IP address of the device on which Dialed Number Analyzer is installed. In the User Name field, enter a valid user ID and a password (for the administrator account to get access to Cisco CallManager Administration).

Using the Cisco Dialed Number Analyzer

Cisco.com

The screenshot shows the Cisco Dialed Number Analyzer web interface. At the top, there is a navigation menu with 'Analysis', 'Service', and 'Help'. Below this is a sidebar with a tree view containing 'Analyzer', 'Gateways', 'Phones', 'Trunks', 'Dump DA Information', and 'View File'. The main content area is titled 'Number Analyzer' and contains a form titled 'Analyzer Input'. The form has the following fields: 'Calling Party*' with the value '1001', 'Dialed Digits*' with the value '1002', 'Calling Search Space' with a dropdown menu showing 'alt-unrestricted-css', 'Device Time Zone' with a dropdown menu showing '(GMT-08:00) Pacific Time (US & Canada); Tijuana', 'Time Zone' with a dropdown menu showing '(GMT) Greenwich Mean Time; Dublin, Edinburgh, London, Lisbon', 'Date' with dropdowns for '2005', 'Feb', and '27', and 'Time' with dropdowns for '16', '44', '25', and '807'. Below the form are two buttons: 'Do Analysis' and 'Clear'. Four callout boxes with arrows point to specific parts of the interface: 'Insert test calling number.' points to the 'Calling Party*' field; 'Insert test dialed digits.' points to the 'Dialed Digits*' field; 'Select calling search space for inserted numbers.' points to the 'Calling Search Space' dropdown; and 'Click Do Analysis to start the analysis.' points to the 'Do Analysis' button. At the bottom left of the screenshot is the copyright notice '© 2005 Cisco Systems, Inc. All rights reserved.' and at the bottom right is the version number 'CIP72 v4.1-3.20'.

The analysis involves entering calling-party and called-party digits in the Dialed Number Analyzer tool and choosing a calling search space for the analysis. Dialed Number Analyzer uses this calling search space and analyzes the dialed digits. You need not choose specific devices or provide any other input. Dialed Number Analyzer allows you to analyze a route pattern, translation pattern, directory number (DN), or CTI route point. Further, beginning with Cisco CallManager Release 4.1, the Dialed Number Analyzer tool supports Call Coverage, H.323 FastStart, Hospitality, trunk-to-trunk transfer, Forced Authorization Codes (FAC) and Client Matter Codes (CMC), BRI, Multilevel Precedence and Preemption (MLPP), U.S. Department of Defense (DoD) requirements, Q signaling (QSIG), and time-of-day features.

In this example, a call between 1001 and 1002 with the calling search space alt-unrestricted-css is analyzed. The Calling Party and the Dialed Digits fields are mandatory. When you want to test, for example, time-of-day routing, you can specify a time zone as well. After you have chosen all values, click the **Do Analysis** button to start the analysis.

Cisco Dialed Number Analyzer Example for a Routed Call—Summary View

Cisco.com

The screenshot displays the Cisco Dialed Number Analyzer interface. The main window is titled "Cisco Dialed Number Analyzer" and "Dialed Number Analyzer Results". It features an "Expand All" button and a "Collapse All" button. The results are organized into a tree view under "Results Summary".

- Results Summary
 - Calling Party Information
 - Dialed Digits = 1002
 - Match Result = RouteThisPattern
 - Matched Pattern Information
 - Called Party Number = 1002
 - Time Zone = (GMT-08:00) Pacific Time (US & Canada); Tijuana
 - InterDigit Timeout = NO
 - OffNet Pattern (and Outside Dial Tone) = NO
 - Call Flow
 - Alternate Matches

Callouts on the left side of the interface provide context for the data:

- "Click Expand All to get more information about the call." points to the "Expand All" button.
- "Is the call routed or restricted?" points to the "Match Result = RouteThisPattern" field.
- "Is the call an OnNet or an OffNet call?" points to the "OffNet Pattern (and Outside Dial Tone) = NO" field.

© 2005 Cisco Systems, Inc. All rights reserved. CPT2 v4.1—3-21

The result of the analyzed call between 1001 and 1002 is displayed in a compact version. For complete information, click the **Expand All** button. The match result information is the first point to check. Is the call routed correctly or is it restricted? `RouteThisPattern` means that the call is routed correctly. The time zone, especially important when using time-of-day routing, as specified in the analyzer window, is shown again. Further, for troubleshooting, the `OffNet` pattern value is interesting. When you want to block `OffNet`-to-`OffNet` transfers, you can check this information for whether the correct classification is being used. In this case, the call between 1001 and 1002 is internal, and the call is not classified as `OffNet`.

Cisco Dialed Number Analyzer Example for a Routed Call—Detailed View

Cisco.com

The screenshot displays the 'Dialed Number Analyzer Results' interface. It is divided into several sections:

- Results Summary:** Contains 'Calling Party Information' (Calling Party: 1001, Partition: , Device CSS: , Line CSS: alt-unrestricted-css, AAR Group Name: , AARCSS:) and 'Matched Pattern Information' (Pattern: :002, Partition: alt-devices-pa).
- Time Schedule:** Shows 'Called Party Number = 1002', 'Time Zone = (GMT-08:00) Pacific Time (US & Canada); Tijuana', and 'InterDigit Timeout = NO'.
- Call Flow:** Shows 'Directory number :uv= 1uvuz', 'Partition = alt-devices-pa', and 'Device Destination = OnNet'.
- Forwarding Information:** Lists 'ForwardAll : DN = VoiceMail = No CSS =', 'ForwardBusy : internal : uv = voicemail = No CSS =', 'External : DN = VoiceMail = No CSS =', 'ForwardNoAnswer : internal : DN = VoiceMail = No CSS =', and 'External : DN = VoiceMail = No CSS ='.
- Alternate Matches:** Shows 'Partition :name= alt-internal-pa' and 'Pattern : Route Pattern = [1-7]XXXX', 'Pattern Type = Translation', 'TranslationPartition = [78A8E17C-FECC-4EFD-9461-02CD8F2759F4]', 'CallManager Device Type = AccessDevice', 'PatternPrecedenceLevel = Routine', 'OutsideDialtone =', and 'DeviceOverride ='.
- ForwardNoCoverage:** Shows 'Internal : DN = VoiceMail = No CSS =', 'External : DN = VoiceMail = No CSS =', 'CFDF : DN = VoiceMail = No CSS =', and 'Dialing Group Number : Device Type = Cisco IP Communicator, Device Status = Registered, Device Name = SEP005056000112'.

Callouts in the image point to specific fields:

- 'Calling search space of the Calling Party' points to 'Line CSS = alt-unrestricted-css'.
- 'Matching Number and Partition' points to 'Pattern = :002' and 'Partition = alt-devices-pa'.
- 'Are any forward fields defined for DN 1002?' points to the 'Forwarding Information' section.
- 'Type, Status, and Name of the Device' points to the 'Dialing Group Number' section.

After you click the Expand All button, you see more detailed information for the call. In the Calling Party Information area, the calling-party number (1001) and the corresponding line calling search space (alt-unrestricted-css) can be seen. In the Matched Partition Information area, the matching number (1002) and the partition (alt-devices-pa) where the number is located are shown. The Forwarding Information area gives information about all forwarding possibilities. This information can be helpful when you are checking for toll fraud in call forwarding. When two internal devices call each other, the device type is displayed as well.

Cisco Dialed Number Analyzer Example for a Non-Routed Call

Cisco.com

Analysis Service Help

Number Analyzer

Analyzer Input

Calling Party* 1001

Dialed Digits* 914045550100#

Calling Search Space alt-unrestricted-css

Device Time Zone (GMT-07:00) Arizona

Time Zone (GMT) Greenwich Mean Time: Dublin, Edinburgh, London, Lisbon

Date 2005 - Jun - 26 (YYYY - MON - DD)

Time 23 : 41 : 39 : 926 (HH : MM : SS : MS)

* indicates required item

Do Analysis Clear

© 2005 Cisco Systems, Inc. All rights reserved. CPT2 v4.1-3-23

In this example, instead of an internal number, the calling party 1001 calls an external destination (914045550100#). The calling search space for this call is alt-unrestricted-css. After you have specified all values, click the **Do Analysis** button. When you want to test time-of-day routing as well, specify a test time.

The administrator configured normal business hours as between 8 a.m. and 6 p.m. All calls within this period are routed normally. Between 6 p.m. and 8 a.m., all calls to external destinations are blocked.

With the Dialed Number Analyzer tool, time-of-day routing can be tested. In the first test, 10:45 a.m. is used as the current time. When the system is configured correctly, the call should be routed. For the second test, 11:44 p.m. is used. The Dialed Number Analyzer tool should show the administrator that the call is not routed.

Cisco Dialed Number Analyzer Example for a Blocked Call—Summary View

Cisco.com

Click Expand All to get more information about the call.

Expand All Collapse All

Results Summary

- Calling Party Information
 - Dialed Digits = 914045550100#
 - Match Result = BlockThisPattern
- Matched Pattern Information
 - Called Party Number = 914041234567#
 - Time Zone = (GMT-07:00) Arizona
 - End Device = S0/DS1-0@SDA000E3879D34E
 - Device Destination =
 - InterDigit Timeout = NO
 - OffNet Pattern (and Outside Dial Tone) = NO
- Call Flow
- Alternate Matches

Is the call routed or restricted?

© 2005 Cisco Systems, Inc. All rights reserved. CIP72 v4.1—3-24

The result of the analysis is displayed in a compact form. To see all the information, click the **Expand All** button. The match result, the first information that you should look at to determine whether the call is routed correctly or restricted, is `BlockThisPattern`, which shows that the call is blocked.

Cisco Dialed Number Analyzer Example for a Blocked Call—Detailed View

Cisco.com

Dialed Number Analyzer Results

Expand All Collapse All

- Results Summary
 - Calling Party Information
 - Calling Party = 1001
 - Partition =
 - Device CSS =
 - Line CSS = atl-unrestricted-css
 - AAR Group Name =
 - AARCSS =
 - Dialed Digits = 914045550100#
 - Match Result = BlockThisPattern
 - Matched Pattern Information
 - Pattern = 914041234567#
 - Partition = atl patn po
 - Time Schedule =
 - Called Party Number = 914041234567#
 - Time Zone = (GMT-07:00) Arizona
 - End Device = S0/DS1-0@SDA000E3879D34E
 - Device Destination =
 - InterDigit Timeout = NO
 - OffNot Pattern (and Outside Dial Tone) = NO
- Call Flow

© 2005 Cisco Systems, Inc. All rights reserved. CIPT2 v4.1-3-25

Expanding gives you more information about the call. In the example, the call is blocked. The reason why the call is blocked can be found in the Matched Pattern Information area. The route pattern 914045550100# matches. The route pattern has a blocking statement for this telephone number, so the call is blocked.

Tip With the Dialed Number Analyzer tool, you can determine why the call is blocked quickly and easily. The Dialed Number Analyzer tool is the best tool for dial-plan troubleshooting.

Quality Report Tool

This topic describes QRT, which is used by end users to report IP Phone problems.

QRT Overview

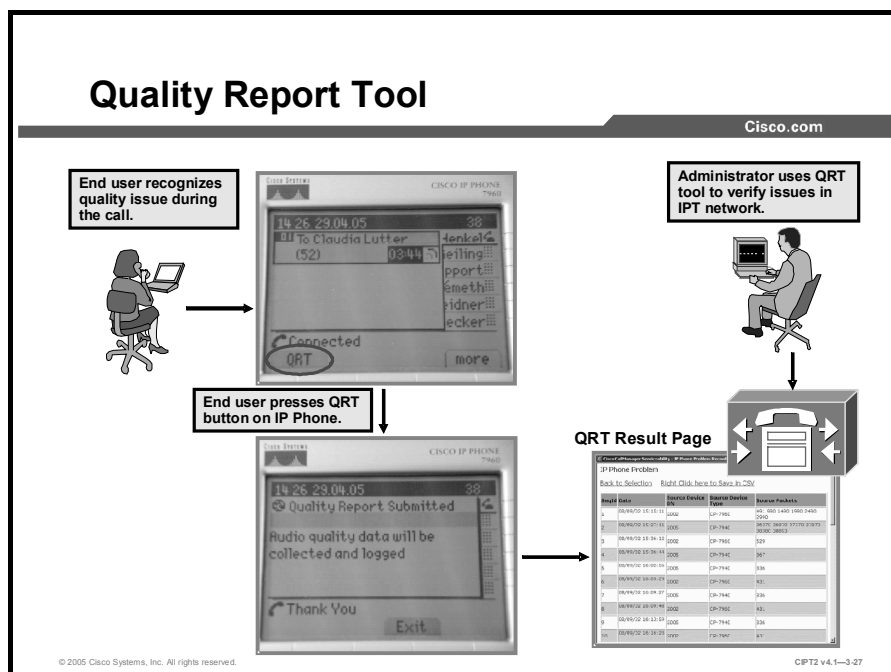
Cisco.com

- **QRT is a voice-quality and general problem-reporting tool for Cisco CallManager IP Phones.**
- **QRT is a feature that extends to IP Phones as a Microsoft Windows NT service.**
- **The Cisco Extended Functions service is needed for the QRT feature.**
- **QRT records are created when the end user presses the QRT button on the IP Phone.**

© 2005 Cisco Systems, Inc. All rights reserved. CIPRT2 v4.1-3-26

QRT is a voice-quality and general problem-reporting tool for Cisco CallManager IP Phones. The Cisco Extended Functions service supports the QRT feature. The QRT Viewer, located in the Tools menu of Cisco CallManager Serviceability, allows administrators to filter, format, and view problem reports that are generated.

Administrators can configure Cisco IP Phones with QRT, which is installed as part of the Cisco CallManager installation, so that users can report problems with IP Phone calls. Users report issues by using a Cisco IP Phone softkey that is labeled "QRT." Any Cisco IP Phone that supports an HTTP web server also includes support for QRT. The IP Phone must be in the Connected, Connected Conference, Connected Transfer, or On Hook state for the QRT softkey to be available.



QRT helps users report voice-quality and general problems to administrators. QRT is a feature that extends to Cisco IP Phones as a Microsoft Windows NT service. Cisco Extended Functions, which supports the QRT feature, must be enabled in the Cisco CallManager service activation window. To enable Cisco Extended Functions, choose **Cisco CallManager Serviceability > Tools > Service Activation** and activate the service called Cisco Extended Functions.

When a user presses the QRT softkey, QRT opens various windows for feedback. It is possible that while the user is interacting with the QRT screen, another application, such as Cisco Call Back or Cisco IP Manager Assistant (IPMA), or function keys, such as settings, directories, messages, and so on, could overwrite the QRT screen. In this situation, QRT cannot send the feedback. To send feedback in such cases, the user has to press the QRT softkey again.

If a user presses the QRT softkey to generate a report and forgets to stop the logging process (the user must manually stop the logging process by pressing the End softkey on the Cisco IP Phone), the QRT tool periodically checks all IP Phones that are generating reports and closes them. This action prevents the device from consuming large amounts of resources that, over time, could impact CTI performance. Currently, the default setting is to check every hour and to close devices that have remained open for more than an hour.

QRT records are written only when the end user presses the QRT softkey on the IP Phone, selects a problem, and sends the report to the administrator. Otherwise, no records are written and the administrator can not troubleshoot the problem. The figure shows the logging process of an audio call between two IP Phones.

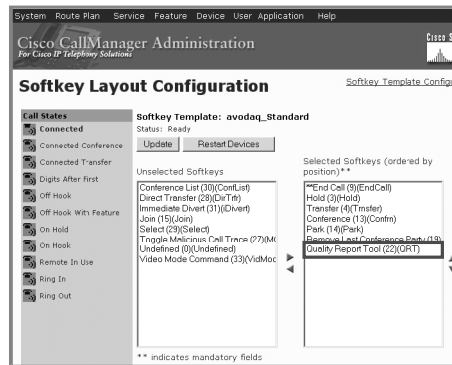
Depending on how the system administrator configured QRT for the Cisco IP Phone, users can use the QRT softkey in either of the two ways described in the table.

Issue	What To Do
To quickly report an audio problem with a current call while on a call, press More > QRT .	Your IP Phone system will collect and log call data for the current call and route this information to your system administrator.
To report a problem with your phone calls, press More > QRT .	Select the problem that you want to report from the list of problem categories. Some problem categories include a reason code that you can select to provide more details about the problem. Your IP Phone system will store the information in a database or file and the administrator can run reports to diagnose the problem.

Activating the QRT Softkey Button

Cisco.com

- **Modify IP Phone softkey template**
- **Add QRT to:**
 - **Connected**
 - **Connected Conference**
 - **Connected Transfer**
 - **On Hook**



© 2005 Cisco Systems, Inc. All rights reserved.

CIPT2 v4.1—3-28

The system administrator may temporarily configure a Cisco IP Phone with QRT to troubleshoot problems with calls. Reconfigure the softkey layout for the IP Phone (choose **Cisco CallManager Administration > Device > Device Settings > Softkey Template > softkey_template_name > Softkey Layout**) to activate the QRT softkey. Users can now report problems by using the QRT softkey during or after a call.

When the administrator modifies the softkey templates to activate the QRT softkey, the softkey should be added to the following call states:

- Connected
- Connected Conference
- Connected Transfer
- On Hook

Queries with QRT

Cisco.com

- Select a time period for QRT reporting.
- Select criteria for the schedule.
- Select fields to display in the query.

The screenshot shows the 'IP Phone Problem Reporting' interface. It includes a 'Selection Criteria' section with dropdown menus for 'Extension Number', 'Device', and 'Category'. Below this is a 'Fields to Display' section with a 'List of Fields' dropdown menu and a 'Selected Fields' list. At the bottom, there is a 'Display Results' button. A smaller window below shows 'Available Cisco Servers' with a dropdown menu, 'From' and 'To' date and time fields, and a 'Get Logs' button.

Administrators can view the IP Phone problem reports that are generated by QRT by using QRT Viewer.

Note QRT collects streaming data only once per call. Therefore, if user A calls user B and both submit reports for that call, only the first report includes streaming data (for example, delay, jitter, and ports being used).

- Step 1** To open the IP Phone Problem Reporting window, choose **Cisco CallManager Administration > Application > Cisco CallManager Serviceability > Tools > QRT Viewer**.
- Step 2** Choose the Cisco CallManager server for which you want to view a problem report. Enter a start and end date in the Date fields. In the Time fields, you can specify the time for those dates, if needed.
- Step 3** Click the **Get Logs** button.
- Step 4** From the Extension Number, Device, and Category drop-down menus, choose the extension numbers, the devices, and the problem categories that you want to include in the report.
- Step 5** From the List of Fields drop-down menu, select the fields that you want to include in the report and click the **Down** arrow to move the selected fields to the Selected Fields pane.

QRT Result Page

Cisco.com

- Displays all cases for the selected time period
- Category and Reason Code columns are fields to look at first
- Only issues where the end user pressed the QRT button displayed
- Result can be saved in a CSV file

SeqId	Date	Category	Reason Code	Source Device DN	Dest. Device DN	Calling Party Number	Final Called Party Number
1	02/25/05 14:08:48	Problems with current call		90246		90246	90113
2	04/14/05 15:31:30	Problems with current call		38	45	45	38
3	04/21/05 12:51:36	Problems with last call	I heard echo	40			
4	04/26/05 10:19:27	Problems with last call	Low volume on my end	9966	71		
5	04/29/05 12:11:58	Problems with current call		52	38	52	38
6	04/29/05 14:26:54	Problems with current call		38	52	38	52
7	04/29/05 14:46:00	Can't make calls	I get fast busy	52			
8	04/29/05 14:46:09	Can't make calls	I don't get dialtone	52			

© 2005 Cisco Systems, Inc. All rights reserved.

CPT2 v4.1-3-30

The QRT output displays all IP Phone problems for the specified time frame. For the filters set in the query, all issues within the time frame are displayed. In the figure, the red outline shows an issue where the IP Phone with the DN 52 was not able to make a call because no dial tone was played.

When you choose All from the Category field, all problems are displayed. The Category and Reason Code columns are the areas that you should look at first. These two columns describe the problem and the reason. The output can be saved in a comma-separated values (CSV) file.

Note Because QRT reports are based only on entries in the QRT database and records are added to that database only if a user presses the QRT softkey, QRT cannot detect any problems on its own; it relies completely on user activity.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- Remote management tools, such as CiscoWorks ITEM, SNMP, and syslog, are used to monitor and manage devices in a network.
- CiscoWorks ITEM is a suite of tools to monitor devices in an IP telephony network.
- Dependency records help in figuring out which devices are associated with other devices.
- Password Changer tool can change passwords of CCMSysUser, CCMAdministrator, IPMASysUser, and Directory Manager.
- DNA is a tool to diagnose, tune, and trace dial plans.
- QR telephony helps administrators identify and resolve problems in an IP telephony network. End users can use this tool to send errors and information to the administrator.

© 2005 Cisco Systems, Inc. All rights reserved. CIP12 v4.1-3-31

Module Summary

This topic summarizes the key points discussed in this module.

Module Summary

Cisco.com

- **Cisco CallManager databases can be handled with Microsoft SQL 2000 Enterprise Manager and Cisco DBLHelper.**
- **You can monitor Cisco CallManager in real time using the Microsoft Windows 2000 performance counters.**
- **For post processing purposes, trace files on Cisco CallManager can be used to diagnose system problems.**
- **CAR allows you to monitor and analyze call-related information.**
- **Additional management and monitoring tools are available for Cisco CallManager maintenance.**

© 2005 Cisco Systems, Inc. All rights reserved.CIPT2 v4.1-3-1

This module described tools and functions that can be used by administrators to maintain a Cisco CallManager system.

References

For additional information, refer to these resources:

- Cisco Systems Inc. *Cisco CallManager Administration Guide, Release 4.1(3)*.
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_book09186a00803be4ec.html.
- Cisco Systems Inc. *Cisco CallManager System Guide, Release 4.1(3)*.
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_book09186a00803be4ee.html.

Module 3 Self-Check

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module 3 Self-Check Answer Key.

- Q1) Which two tools are available on Cisco CallManager systems to manage the SQL database? (Choose two.) (Source: Introducing Database Tools and Cisco CallManager Serviceability)
- A) Microsoft SQL 2000 Enterprise Manager
 - B) Cisco SQL 2000 Enterprise Manager
 - C) SQL 2000 System Manager
 - D) DBAHelper
 - E) DBLHelper
- Q2) Which of the following statements is true? (Source: Introducing Database Tools and Cisco CallManager Serviceability)
- A) Cisco CallManager Serviceability needs to be installed from the Cisco CallManager Install Plugins window.
 - B) Cisco Call Manager Serviceability provides a configuration interface to configure extension DNs.
 - C) Cisco CallManager Serviceability allows you to start, stop, or restart all Microsoft Windows 2000 services.
 - D) Cisco CallManager Serviceability provides services to monitor alarms, generate Cars, and collect and analyze traces.
- Q3) Which two of the following services can be started, stopped, or restarted via the Cisco CallManager Control Center? (Choose two.) (Source: Introducing Database Tools and Cisco CallManager Serviceability)
- A) Cisco CallManager
 - B) Cisco DHCP
 - C) Cisco TFTP
 - D) Cisco Extension Mobility
 - E) Cisco WebDialer
- Q4) Where can Cisco CallManager Services be activated and deactivated? (Choose two.) (Source: Introducing Database Tools and Cisco CallManager Serviceability)
- A) in DBLHelper
 - B) in Cisco CallManager Control Center
 - C) in NT Services MMC
 - D) in Microsoft Service Activation Tool
 - E) in Cisco CallManager Service Activation
- Q5) Where should DBLHelper be run on? (Source: Introducing Database Tools and Cisco CallManager Serviceability)
- A) only on Cisco CallManager publisher server
 - B) only on Cisco CallManager subscriber server
 - C) on Cisco CallManager publisher or subscriber server
 - D) on every PC in the network

- Q6) List at least three items for which performance counters can be used in Cisco CallManager. (Source: Monitoring Performance)
-
-
-
- Q7) Which two of the following statements about Microsoft Event Viewer are true? (Choose two.) (Source: Monitoring Performance)
- A) Microsoft Event Viewer is needs to be installed separately and is included in the Microsoft Windows 2000 support pack.
 - B) Microsoft Event Viewer assists administrators in troubleshooting Cisco CallManager systems.
 - C) Microsoft Event Viewer is limited to the most recent 100 events per log type.
 - D) Microsoft Event Viewer stores system errors and warnings.
 - E) There are four log types in Microsoft Event Viewer.
- Q8) How can Microsoft Performance Monitor be used to maintain Cisco CallManager systems? (Choose three.) (Source: Monitoring Performance)
- A) to monitor Microsoft Windows 2000 events
 - B) to monitor Cisco CallManager events
 - C) to monitor events in real time
 - D) to analyze call flows
 - E) to analyze CDRs
 - F) to analyze trace files
 - G) to analyze Cisco CallManager configuration
- Q9) What can RTMT be used for? (Choose two.) (Source: Monitoring Performance)
- A) Cisco CallManager performance monitoring
 - B) Cisco CallManager configuration
 - C) Cisco CallManager performance manipulation
 - D) alert e-mail generation
 - E) service activation
- Q10) Which two of the following statements about saving of configurations on RTMT are true? (Choose two.) (Source: Monitoring Performance)
- A) If administrators exit RTMT, the active configuration is stored automatically.
 - B) Multiple configuration profiles can be stored.
 - C) RTMT needs to be restarted to load a saved configuration.
 - D) Configuration profiles can be identified by their number and date.
 - E) Configuration profiles can be identified by their name and description.

- Q11) Which of the following statements about the RTMT window is true? (Source: Monitoring Performance)
- A) The RTMT window supports tabs to allow many different elements to be viewed at one time.
 - B) When switching between RTMT window tabs, real-time information graphs on inactive (hidden) tabs are stopped.
 - C) The RTMT window provides performance monitoring similar to the Microsoft Performance Monitor.
 - D) The RTMT window includes a link to start the Microsoft Performance Monitor MMC.
 - E) The RTMT window includes an alert central.
 - F) RTMT needs to be downloaded from Cisco.com.
 - G) To get information about RTMT, go to <http://www.cisco.com/go/rtmt>.
- Q12) What does Cisco CallManager Serviceability Alarm provide? (Choose two.) (Source: Configuring Alarms and Traces)
- A) configuration of alarms
 - B) alarm analysis
 - C) alarm message definitions
 - D) configuration of traces
 - E) alarm modification
- Q13) When you are configuring alarms on Cisco CallManager Serviceability, which of the following statements is true? (Source: Configuring Alarms and Traces)
- A) An e-mail address to use for sending alerts to can be defined.
 - B) It is possible to define which fields should be included in written SDI and SDL trace files.
 - C) More than one destination can be used to write alarm logs in parallel, and each of them can use its own alarm level.
 - D) Alarm levels are predefined on Cisco CallManager and cannot be changed.
- Q14) What is the difference between configuring alarms for Java applications and configuring alarms for other services on Cisco CallManager? (Source: Configuring Alarms and Traces)
-
- Q15) Which three of the following statements about SDI and SDL traces are true? (Choose three.) (Source: Configuring Alarms and Traces)
- A) SDI traces log services and run-time events.
 - B) SDL traces log services and run-time events.
 - C) SDI traces log call-processing information.
 - D) SDL traces log call-processing information.
 - E) SDI and SDL traces can be written to plain-text and XML files.
 - F) SDI and SDL traces can be written to plain-text files only.
 - G) SDI and SDL traces can be written to XML files only.

- Q16) What does the Trace Collection tool do? (Source: Configuring Alarms and Traces)
- A) collects traces from Cisco CallManager systems and writes them to remote hosts
 - B) allows you to configure the kind of information that should be collected and written to trace files
 - C) downloads and compresses trace files from Cisco CallManager systems to a computer
 - D) saves disk space on Cisco Call Manager by deleting trace files after downloading them
- Q17) What can you do with the web-based Trace Analysis tool in Cisco Call Manager Serviceability? (Choose two.) (Source: Configuring Alarms and Traces)
- A) analyze plain-text-formatted SDI trace files
 - B) analyze plain-text-formatted SDL trace files
 - C) analyze XML-formatted SDI trace files
 - D) analyze XML-formatted SDL trace files
 - E) analyze files larger than 2 MB
- Q18) What extra functionality does the Bulk Trace Analysis tool provide that is not included in the web-based Trace Analysis tool? Give three examples. (Source: Configuring Alarms and Traces)
-
-
-
- Q19) What is the difference between Q.931 Translator and Voice Log Translator? (Source: Configuring Alarms and Traces)
- A) Q.931 Translator supports SCCP.
 - B) Voice Log Translator supports MGCP.
 - C) Voice Log Translator can be used to analyze log files without access to the Cisco CallManager system.
 - D) Q.931 translator is provided for free, but to use Voice Log Translator, you must pay a special license fee.
- Q20) Which three statements about the CAR tool are true? (Choose three.) (Source: Configuring CAR)
- A) PDF reports are limited to 5000 records.
 - B) PDF reports are limited to 10,000 records.
 - C) CSV reports are limited to 20,000 records.
 - D) CSV reports are limited to 25,000 records.
 - E) CAR has to be installed on the publisher only.
 - F) CAR does not have to be installed on the publisher.
- Q21) Which statement about CMR and CDR is true? (Source: Configuring CAR)
- A) Both are stored permanently in flat files.
 - B) CMR stores call details.
 - C) CDR stores QoS parameters.
 - D) They are related to each other.

- Q22) Which username and password combination is used for the first login to CAR?
(Source: Configuring CAR)
- A) cisco and cisco
 - B) cisco and dipsy
 - C) admin and admin
 - D) admin and cisco
- Q23) Which is a valid CAR report type? (Source: Configuring CAR)
- A) QoS reports
 - B) CDR reports
 - C) database reports
 - D) device reports
- Q24) What is the first thing to do after the first login to CAR? (Source: Configuring CAR)
- A) Grant access rights.
 - B) Configure the mail server.
 - C) Configure the dial plan.
 - D) Adjust the system preferences.
- Q25) When is the CDR data loaded by default? (Source: Configuring CAR)
- A) from midnight to 1 a.m.
 - B) from midnight to 3 a.m.
 - C) from midnight to 5 a.m.
 - D) in nearly real time
- Q26) The CAR and CDR database alerts the CARAdministrator by default when _____ percent of the maximum number of rows is reached. (Source: Configuring CAR)
- A) 70
 - B) 75
 - C) 80
 - D) 85
 - E) 90
- Q27) Which call type is valid in individual bills? (Source: Configuring CAR)
- A) On Net
 - B) Intersite
 - C) MLPP
 - D) Video
- Q28) What is an advantage of Management Tools? (Source: Using Additional Management and Monitoring Tools)
- A) Management tools automatically repair devices if a configuration problem exists.
 - B) Management tools are used as a central component in a network to manage and monitor devices.
 - C) Management tools are used to verify configuration of network devices.
 - D) Management tools, such as Cisco ITEM, are used to analyze dial plans.

- Q29) What is the purpose of the dependency records tool? (Source: Using Additional Management and Monitoring Tools)
- A) Dial plans can be analyzed with the dependency records tool.
 - B) It helps to find dependency between devices in Cisco CallManager.
 - C) Users and profiles that are interacting with each other can be displayed with the dependency records tool.
 - D) Collaborating system services in Cisco CallManager can be displayed with the dependency records tool.
- Q30) Which user passwords can be changed with the Password Changer tool? (Source: Using Additional Management and Monitoring Tools)
- A) IPMAAdminUser
 - B) CCMAAdminUser
 - C) CCMAAdministrator
 - D) CCMUser
- Q31) The Cisco Dialed Number Analyzer tool can be used to analyze which of the following? (Source: Using Additional Management and Monitoring Tools)
- A) Dial plans in an IP telephony environment
 - B) Erlang b and Erlang c values
 - C) Cars
 - D) Dialed service numbers called by users
- Q32) Complete the following sentence to make it true:
When using QRT, reports are created _____. (Source: Using Additional Management and Monitoring Tools)
- A) automatically for all users
 - B) in a round-robin fashion for all users
 - C) when an administrator activates QRT Viewer
 - D) when an end user presses the QRT button on the IP Phone

Module 3 Self-Check Answer Key

- Q1) A, E
- Q2) D
- Q3) A, C
- Q4) C, E
- Q5) A
- Q6) System maintenance, system analysis, and system troubleshooting
- Q7) B, D
- Q8) A, B, C
- Q9) A, D
- Q10) B, E
- Q11) A, C, E
- Q12) A, C
- Q13) C
- Q14) Alarms for Java applications cannot be configured in Cisco CallManager Serviceability. They need to be configured directly in the Windows 2000 registry.
- Q15) A, D, E
- Q16) C
- Q17) C, D
- Q18) Works without using Cisco CallManager system processing power
Creates reports of information using multiple trace files
Allows multiple views of a single report
Allows customizing and analyzing views
Allows saving and printing of reports
Can be used to analyze trace files larger than 2 MB
- Q19) C
- Q20) A, C, E
- Q21) D
- Q22) C
- Q23) D
- Q24) A
- Q25) C
- Q26) C
- Q27) A
- Q28) B

- Q29) B
- Q30) C
- Q31) A
- Q32) D

CIPT2

Cisco IP Telephony Part 2

Version 4.1

Lab Guide

CLS Production Services: 09.20.05

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco 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



Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCSP, 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, ASIST, 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, Empowering the Internet Generation, 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, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO 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. (0501R)

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.

Lab Guide

Overview

This guide presents the instructions and other information concerning the activities for this course. You can find the solutions in the lab activity Answer Key.

Outline

This guide includes these activities:

- Lab 1-1: Securing the Windows Operating System
- Lab 1-2: Securing Cisco CallManager Administration
- Lab 1-3: Preventing Toll Fraud
- Lab 1-4: Hardening the IP Phone
- Lab 1-5: Configuring Cisco IP Telephony Authentication and Encryption
- Lab 2-1: Enabling Cisco VT Advantage
- Lab 3-1: Monitoring Performance
- Lab 3-2: Configuring Alarms and Traces
- Lab 3-3: Configuring CAR
- Lab 3-4: Enabling Dependency Records, Configuring Cisco Dialed Number Analyzer, and Using QRT

Lab 1-1: Securing the Windows Operating System

Complete this lab activity to practice what you learned in the related module.

Activity Objective

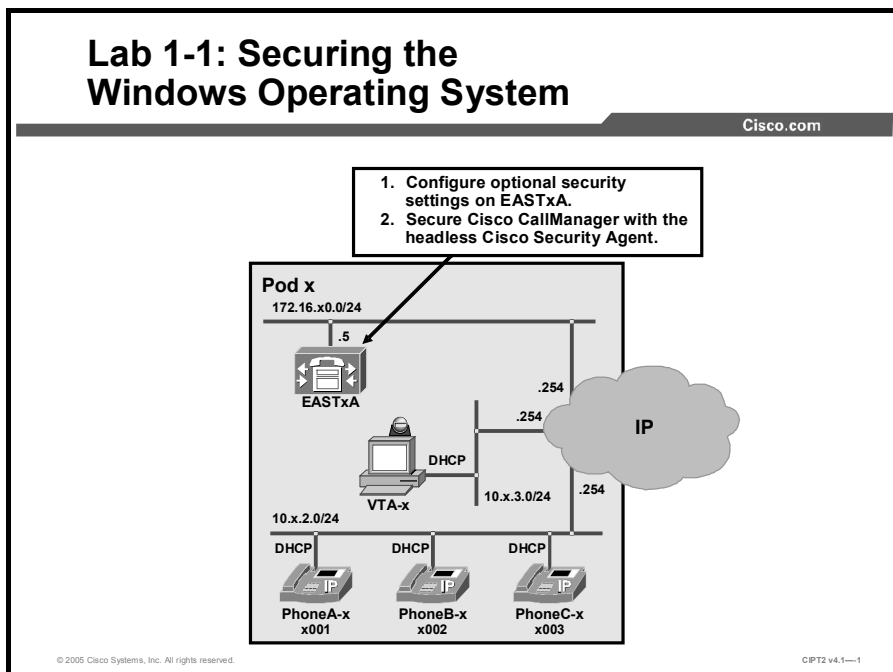
In this activity, you will employ several mechanisms to make the operating system more secure. After completing this activity, you will be able to meet these objectives:

- Configure the Cisco IP Telephony Operating System with optional security settings
- Install the headless Cisco Security Agent

Visual Objective

In this activity, you will harden the operating system for a Cisco CallManager installation. To do so, you will install the headless Cisco Security Agent and run the optional security script. All tasks have to be performed on Cisco CallManager.

The figure illustrates what you will accomplish in this activity.



Note All numbers that relate to your pod number are indicated with an x in this document. These are: the last digit of all device names, the second octet of all IP addresses, the first digit of all DNs, and the first digit of PSTN subscriber numbers.

Required Resources

These are the resources and equipment required to complete this activity:

- The lab devices shown in the Visual Objectives figure and detailed in the table

Lab Devices and Their Roles

Device	Device Role in the Activity
EASTxA	Cisco CallManager publisher that serves the IP Phones

- The device credentials in the table, to log in to the lab devices that require authentication

Credentials for Device Access

Device	Username and Password
EASTxA	administrator lab auditor lab

Job Aids

These job aids are available to help you complete the lab activity.

- The lab devices use the IP address allocation scheme shown in the table.

IP Address Allocation Scheme

Device	IP Address
Voice server network	172.16.x0.0/24
IP Phone network	10.x.2.0/24
Data network	10.x.3.0/24
Default gateway	Node address .254 (for all networks)
EASTxA	172.16.x0.5
VTA-x	DHCP-assigned (10.x.3.0)

- The table describes the files and folders to change when using a separate Auditors group.

Auditors Group Files and Folders

Files and Folders
C:\WINNT\system32\LogFiles\W3SVC1
C:\WINNT\system32\config\AppEvent.Evt
C:\WINNT\system32\config\SecEvent.Evt
C:\WINNT\system32\config\SysEvent.Evt
C:\WINNT\system32\inetrv\urlscan\logs
C:\Program Files\Cisco\Tomcat\logs\lsapi.log

Task 1: Configure Optional Security Settings

In this task, you will secure the Cisco IP Telephony Operating System with some optional security settings. The optional security guide is located in Cisco CallManager in the C:\utils\SecurityTemplates folder.

You will configure parts of the settings described in the CCM-OS-OptionalSecurity-Readme.htm guide. You will change the message and title for a dialog box that appears for users attempting to log in, create an Auditor group, configure log file access control, and enable the screen saver password.

Activity Procedure

Configuring a Login Legal Message

You will set a default Microsoft legal notice that appears at login. Configure this setting by completing these steps:

Step 1 From the VTA-x PC, start a remote session to the Cisco CallManager server EASTxA using the VNC application. To launch VNC, choose **Start > Programs > RealVNC > VNC Viewer 4 > Run VNC Viewer** or use the icon **VNC Viewer 4** from the Quick Launch toolbar. Enter the IP address of your Cisco CallManager server (EASTxA) and click **OK**. When the connection opens, log in to EASTxA with the username **administrator** and the password **lab**, as shown in the “Credentials for Device Access” table in the Required Resources section.

Note To send the Ctrl-Alt-Delete sequence to the host that you access through your VNC remote session, click the **VNC** icon at the top-left corner of the VNC application and choose **Send Ctrl-Alt-Del** from the VNC application menu.

Step 2 On EASTxA, choose **Start > Programs > Administrative Tools > Local Security Policy > Security Settings > Local Policies > Security Options > Message Text for Users Attempting to Log On**.

Step 3 Enter **This system is under the administrative control of Cisco Systems, any unauthorized access will be prosecuted** and click **OK**.

Step 4 Choose **Message title for users attempting to log on**, enter **Cisco Legal Department**, and click **OK**.

Note Both the message text and the message title must be set for the screen to be displayed.

Step 5 Close the Local Security Settings window.

Creating an Auditor Group and User

In the next steps, you will create and configure the Auditor group and add an auditor user to the Auditor group.

Step 6 Choose **Start > Programs > Administrative Tools > Computer Management > Local Users and Groups**.

Step 7 Right-click **Users** and choose **New User**.

Step 8 Enter **auditor** in the User Name and Description fields. Enter **lab** in the Password and Confirm Password fields, deselect **User Must Change Password at Next Login**, and click **Create** to add the user. Close the New User window.

Step 9 In the Computer Management application under Local Users and Groups, right-click **Groups** and choose **New Group**.

Step 10 Enter **Auditors** in the Group Name and Description fields, and click **Add** to display the Select Users or Groups window.

Step 11 From the list of available users and groups, choose user **Auditor**, click **Add**, and confirm your change by clicking **OK**. In the New Group window, click **Create** to create the Auditors group, which now has the user Auditor as a member. Then close the New Group window and the Computer Management application.

Allowing Only Members of the Auditor Group to Manage the Auditing and Security Logs

In the next steps, you will change the local security policy to prevent administrators from managing the auditing and security logs. You will allow auditors to manage these logs.

Step 12 Choose **Start > Programs > Administrative Tools > Local Security Policy > Security Settings > Local Policies > User Rights Assignment > Manage Auditing and Security Log**.

Step 13 Deselect the **Administrators** group and then click **Add**. In the Select Users or Groups window, choose the **Auditors** group, click **Add**, and confirm the choice by clicking **OK**.

Step 14 You again see the Manage Auditing and Security Log window, and you see the group Auditors listed below the group Administrators. Ensure that only the Auditors group has the Local Policy Setting check box checked, and click **OK**.

Note The screen does not refresh immediately. You will see the changes only when you next open the application.

Step 15 Close the Local Security Settings window.

Configuring File ACLs to Allow Only Auditors to Modify Log Files

In the next steps, you will modify file ACLs to limit file access rights to certain files and folders, as listed in the “Auditor Files and Folders” table in the Job Aids section. After these changes, the Administrators group will not be able to modify (delete or erase) log files but will have permissions only to view the log files. Members of the Auditors group will have full control over these log files.

Step 16 Choose **Start > Programs > Accessories > Windows Explorer** to open the Windows Explorer application. For each folder listed in the table “Auditor Files and Folders” in the Job Aids, complete the following steps.

Step 17 Right-click the file or the folder, click **Properties > Security**, and deselect **Allow Inheritable Permissions from Parent to Propagate to This Object**. Choose **Copy** to copy previously inherited permissions to this object.

Note When setting the file access rights for multiple files of the same folder, you can change all the files at once. To do so, choose the desired files (by clicking the files while pressing and holding the Ctrl key) before right-clicking your selection and clicking **Properties > Security**.

Step 18 Ensure that the **Administrators** group is selected in the Name list and deselect the **Full Control, Modify, and Write** permissions. If you are setting the attributes on a folder, also deselect the **List Folder Contents** permission. The Administrators group should only have Read and **Read & Execute** permissions. Click **Apply** to confirm the changes that you have made so far.

Step 19 Click **Add** to open the Select Users or Groups window. From the Name list, choose the Auditors group, and click **Add** and **OK**. You will again see the Property window of the file or folder and see the Auditors group highlighted in the Name list.

Step 20 Click **Full Control** in the Allow column of the Permissions list and click **OK** to confirm your changes.

Permitting Auditors to Use the Microsoft Event Viewer Application

Next you will permit auditors to start MMC so that they can launch management applications, such as Microsoft Event Viewer.

Step 21 Using the same tools that you used in the previous steps, add Read & Execute and Read permissions to the auditors group for the MMC executable file C:\WINNT\system32\mmc.exe.

Note When you activate the Read & Execute permission, the Read permission is added automatically.

Configuring Screen Saver Password Protection

In the next steps, you will enable screen saver password protection.

Step 22 Right-click your Microsoft Windows desktop and choose **Properties**.

Step 23 Click the **Screen Saver** tab.

Step 24 Choose **Logon Screen Saver** from the Screen Saver list. Do not choose any other screen saver.

Step 25 Choose **Password Protected** and click **OK** to close the window.

Note The screen saver settings apply to the currently logged-in user only.

Activity Verification

You have completed this task when you attain these results:

- When you log in to the Cisco IP Telephony Operating System, you see the message “This system is under the administrative control of Cisco Systems, any unauthorized access will be prosecuted”.
- Only users in the Auditor group have permission to view the security event log.
- The screen saver is password-protected and you have to reauthenticate when accessing the PC again.

Specifically, complete these steps:

- Step 1** If you are still connected to EASTxA, disconnect first. Then connect to EASTxA again from the VTA-x PC using VNC and log in to EASTxA using the Administrator account. In Event Viewer, try to view the security log. You should not be able to view the log.
- Step 2** Log in to EASTxA using the Auditor account. In Event Viewer, try to view the security log. You should be allowed to view the security log.
- Step 3** Right-click the Windows desktop and choose **Properties**. Configure the screen saver to wait **1 minute** before becoming active. Wait 1 minute and then verify that you are required to enter a password after the screensaver becomes active.

Task 2: Install Cisco Security Agent

In this task, you will further protect the operating system from DoS attacks against Cisco CallManager and misbehaving applications. To secure Cisco CallManager against these threats, you will install the headless Cisco Security Agent on the Cisco CallManager operating system.

Activity Procedure

Complete these steps:

- Step 1** On the VTA-x PC, start a remote session to EASTxA using the VNC application. To launch VNC, choose **Start > Programs > RealVNC > VNC Viewer 4 > Run VNC Viewer** or click the icon **VNC Viewer 4** from the Quick Launch toolbar. Enter the IP address of your Cisco CallManager server (EASTxA) and click **OK**. When the connection opens, log in to EASTxA with the credentials shown in the “Credentials for Device Access” table in the Required Resources section.
- Step 2** Open the folder **Software\Cisco CSA** located on the desktop of EASTxA and execute the **CiscoCM-CSA-4.0.3.728-1.1.10-K9.exe** file.
- Step 3** Click **Next** at the Welcome window, and then accept the license agreement by clicking **Yes**.
- Step 4** Click **Next** to accept the default destination folder (C:\Program Files\Cisco).

Note Cisco CallManager policy rules are directory-specific, so you must use the default directory.

Step 5 Ensure that **Network Shim** is selected and click **Next**. In the window that allows you to review the installation settings, click **Next** to start the installation.

Step 6 When the installation has finished, you are prompted to restart your computer. Ensure that the **Yes, I want to restart my computer now** option is selected and click **Finish**. Your server reboots.

Activity Verification

You have completed this task when you attain these results:

- Cisco Security Agent is installed and the Cisco Operating System Version utility displays the proper version of the installed Cisco Security Agent .
- When Cisco Security Agent is disabled, entering the URL `http://172.16.x0.5/://` displays an HTTP error message “404 - File not found.”
- When Cisco Security Agent is enabled, entering the URL `http://172.16.x0.5/://` displays an HTTP error message “403 - Forbidden.”

Note `Http://<IP address>/://` is a common web server exploit that is blocked by Cisco Security Agent .

- When Cisco Security Agent is disabled, a trace route to the Cisco CallManager server of the other pod works.
- When Cisco Security Agent is enabled, a trace route to the Cisco CallManager server of the other pod does not work properly (indicates timeouts for all hops in the path) because Cisco Security Agent blocks incoming Time-to-Live (TTL)-exceeded Internet Control Message Protocol (ICMP) packets.
- All blocked actions are logged in the Cisco Security Agent log files located at `C:\Program Files\Cisco\CSA Agent`.

Specifically, complete these steps:

Step 1 On the VTA-x PC, open a VNC connection to EASTxA.

Step 2 On EASTxA, choose **Start > Cisco OS Version** and execute the **MCSver.exe**. This displays the current version of Cisco Security Agent .

Step 3 Disable Cisco Security Agent by right-clicking the **CSA Agent** icon on the taskbar and choosing **Suspend Security**. When prompted to confirm, click **Yes**.

Step 4 Stop the Cisco Security Agent service in the Services applet. Choose **Start > Programs > Administrative Tools > Services** and locate the **Cisco Security Agent** service. Stop the CSA service by right-clicking **Cisco Security Agent** and choosing **Stop**.

Note For the URL test, it is enough to suspend Cisco Security Agent to disable protection against malicious URLs. For the trace route test, you have to stop the service because suspending Cisco Security Agent will not disable protection against TTL-exceeded ICMP packets.

- Step 5** On the VTA-x PC, open Internet Explorer and enter the URL **http://172.16.x0.5/://**. Internet Explorer should display the error message “404 - File not found.”
- Step 6** On EASTxA (from within the VNC session initiated on the VTA-x PC), open a command console (choose **Start > Run**, enter **cmd**, and click **OK**). At the C:\> prompt, enter **tracert** and the IP address of the Cisco CallManager server of the other pod (that is, if you are in pod 1, enter the IP address of the server in pod 2: 172.16.20.5) and press the Enter key. The trace route works and all hops are displayed. Leave the command shell open.
- Step 7** Enable the Cisco Security Agent again by right-clicking the **CSA** icon and choosing **Resume Security**.
- Step 8** Repeat Step 5. This time, Internet Explorer displays the error message “403 - Forbidden.”
- Step 9** Repeat Step 6. This time, the trace route shows timeouts for all entries but the last one.
- Step 10** Open the Cisco Security Agent log files and verify the actions that were blocked by Cisco Security Agent. The Cisco Security Agent log files are located in C:\Program Files\Cisco\CSAgent\log\securitylog.txt.

Lab 1-1 Answer Key: Securing the Windows Operating System

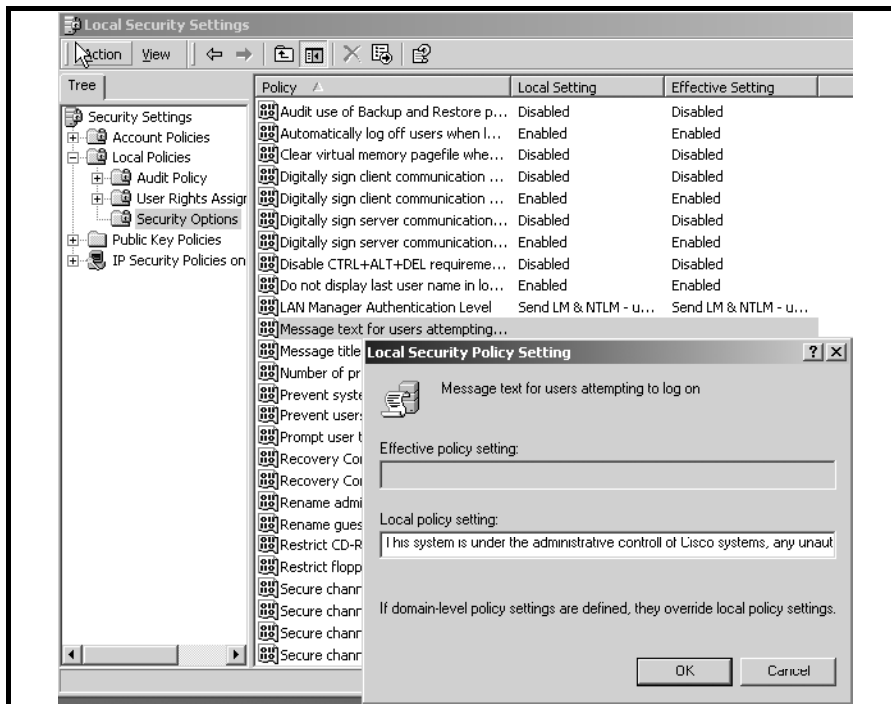
When you complete this activity, your solution will be similar to this, with differences that are specific to your device or workgroup.

Task 1: Configure Optional Security Settings

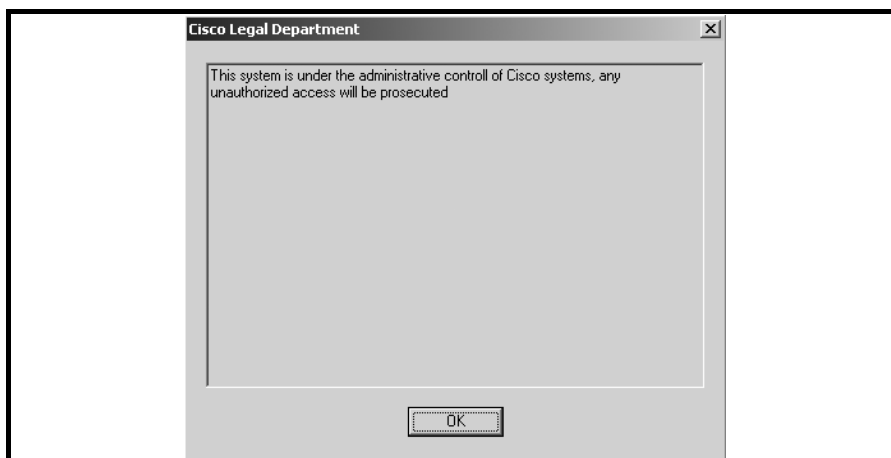
This procedure enables you to complete the activities described in the task.

Configuring a Login Legal Message

The legal note is configured in the **Local Security Policy Setting** window.

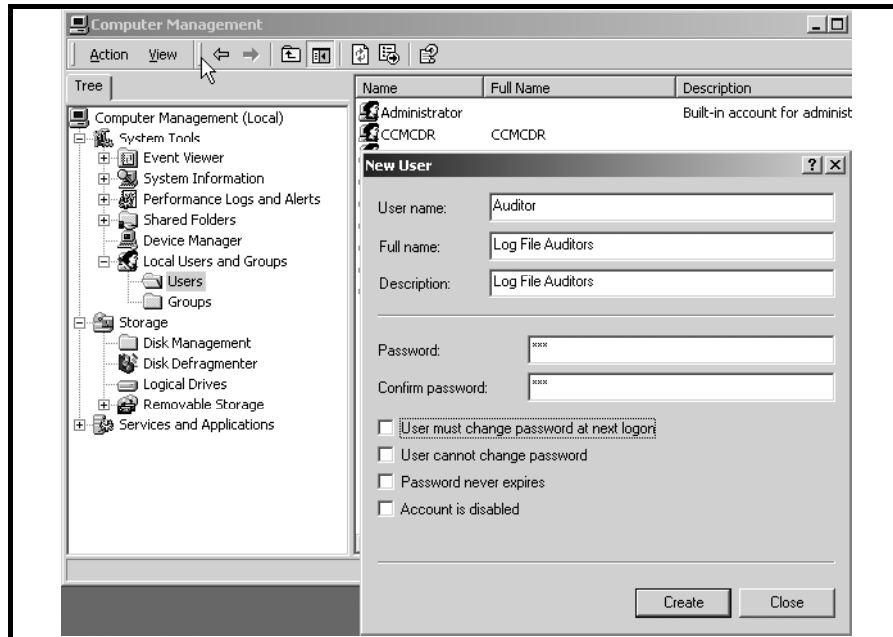


The login message is displayed when you log in to the Cisco IP Telephony Operating System. The message text that you configured is shown in the Local Policy Setting field and the message title that you configured is shown at the top of the dialog box.

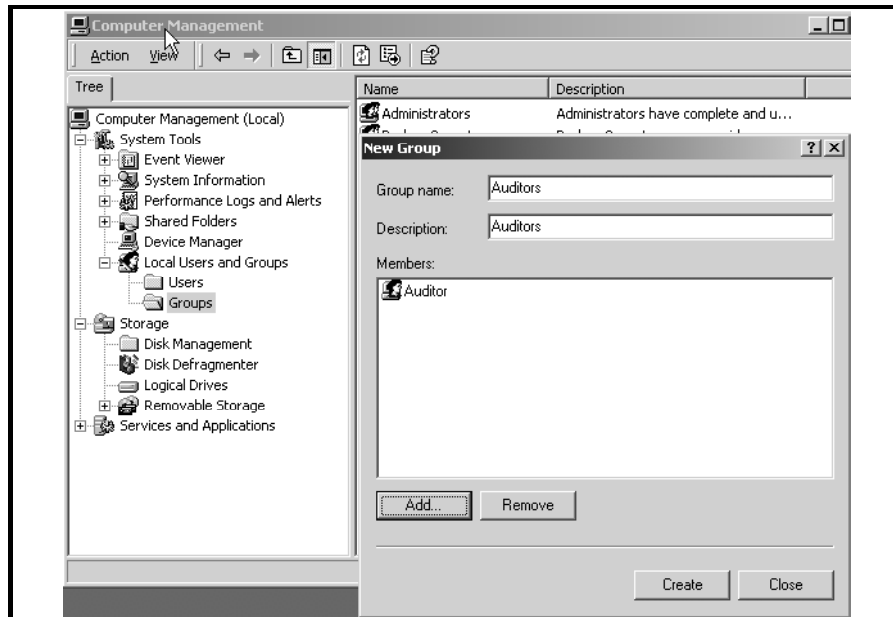


Creating an Auditor Group and User

Create an Auditor user.

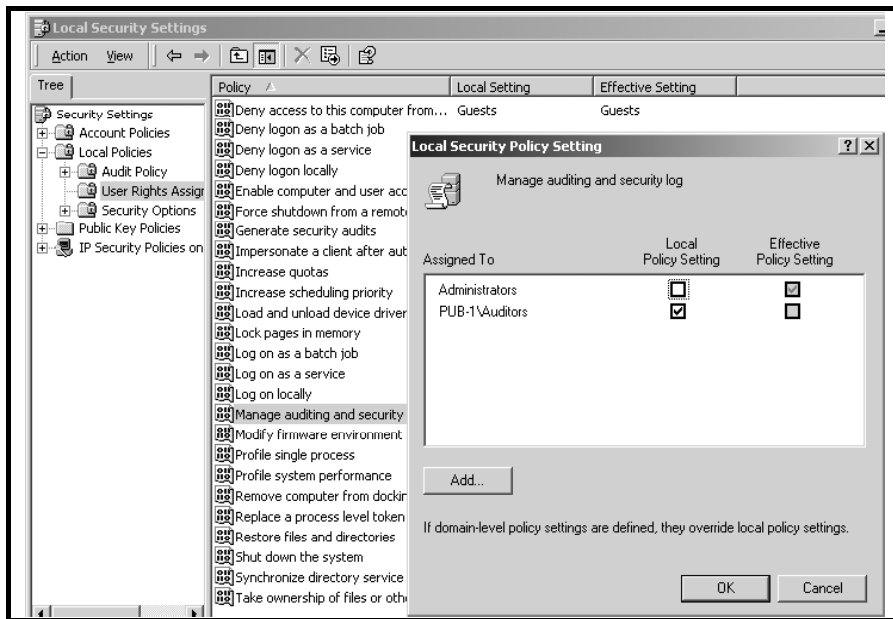


Create an Auditors group and place the Auditor user in that group.



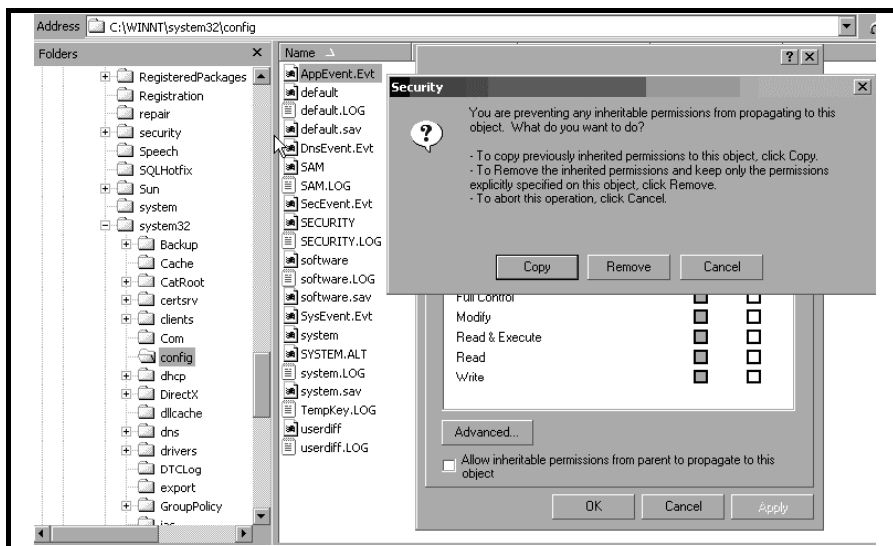
Allowing Only Members of the Auditor Group to Manage the Auditing and Security Logs

Change the permissions for managing and auditing the security log.

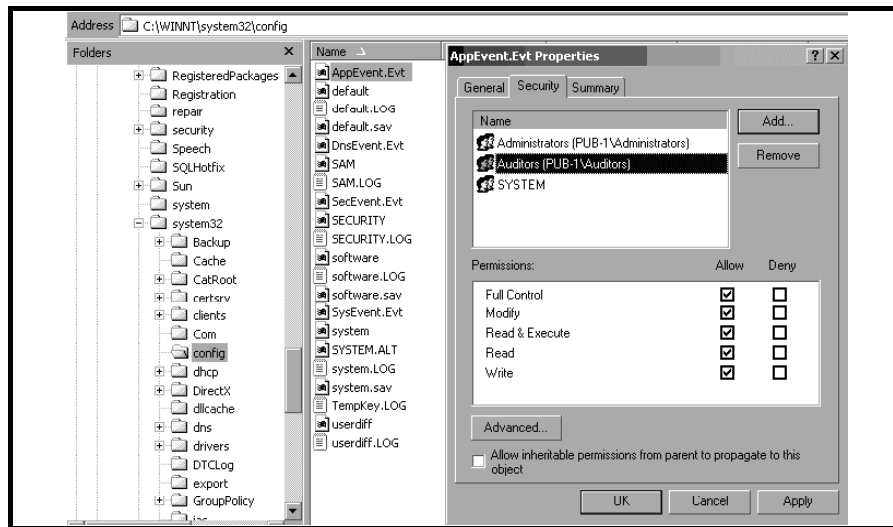


Configuring File ACLs to Allow Only Auditors to Modify Log Files

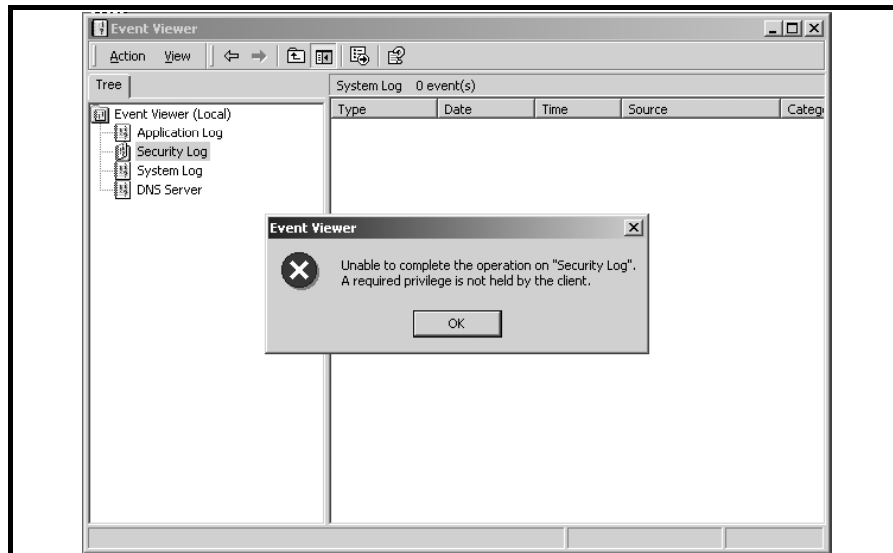
Change the Windows NTFS permissions for the log files after you disable inherited permissions.



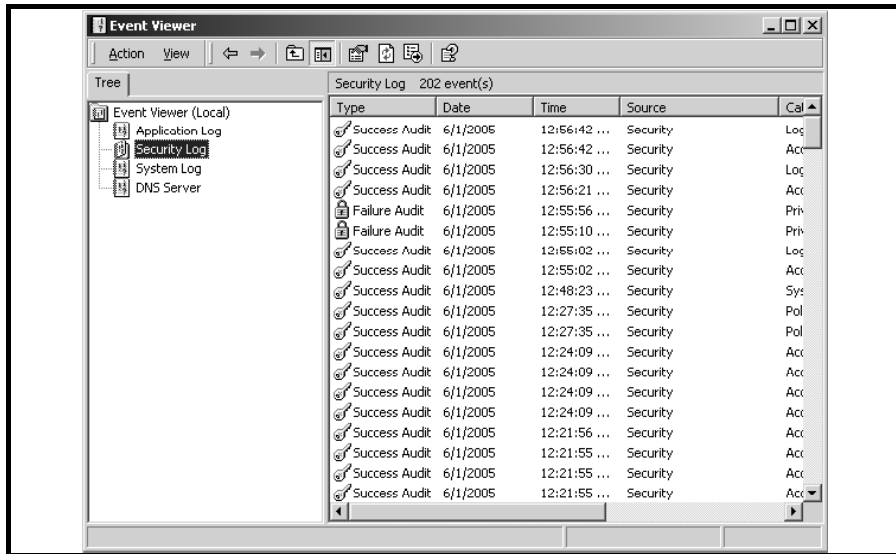
Add the Auditor group and set the appropriate Windows NTFS permissions.



The Administrators group is no longer able to view the Event Viewer security logs.

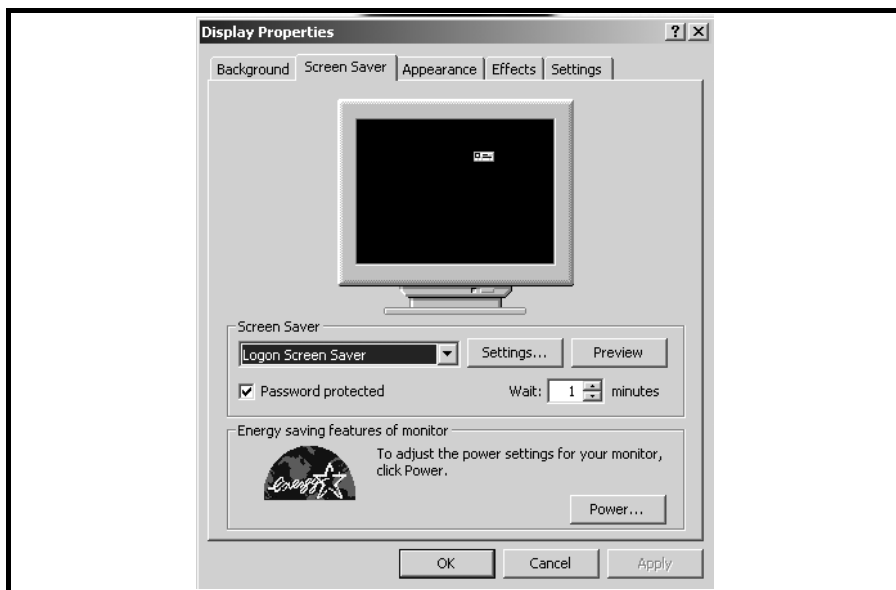


The Auditors group is able to view the Event Viewer security logs.



Configuring Screen Saver Password Protection

Enable password protection for the login screen saver.

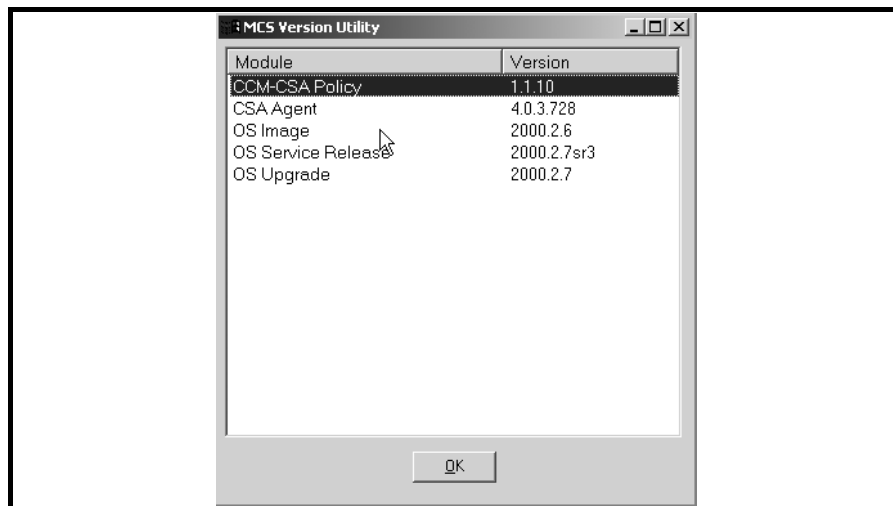


Task 2: Install Cisco Security Agent

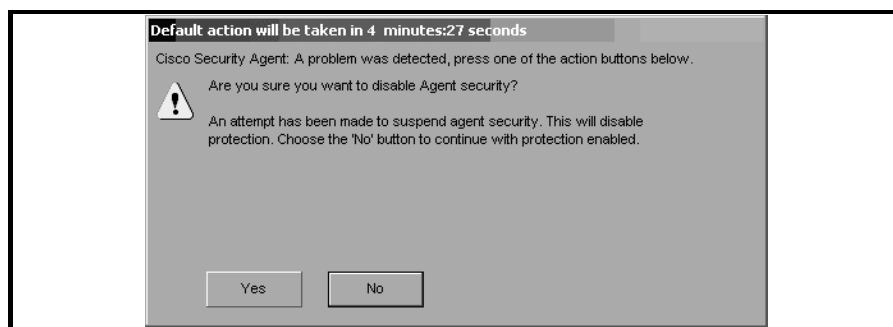
This procedure enables you to complete the activities described in the task.



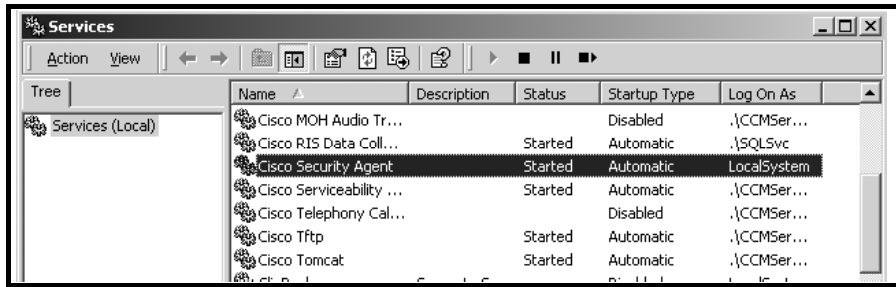
The MCSvr.exe should look similar to this figure.



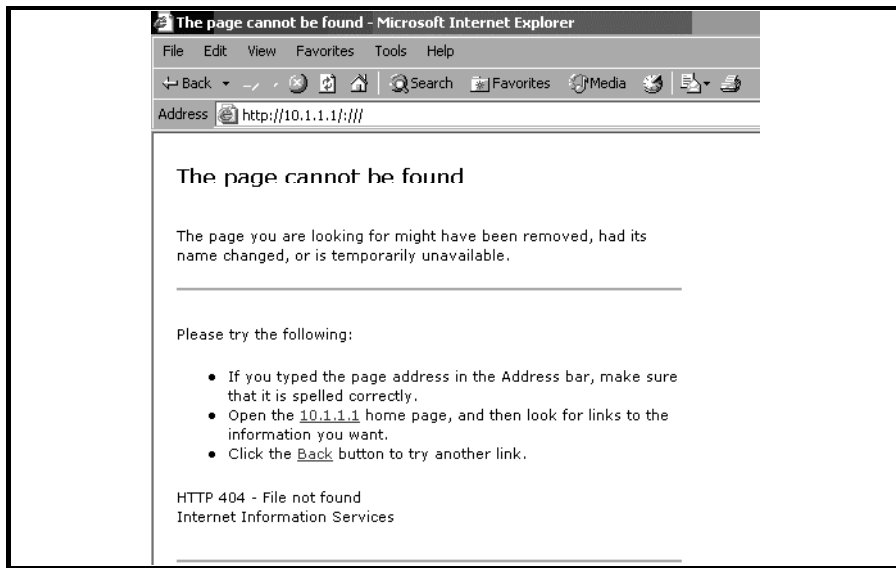
Disable Cisco Security Agent.



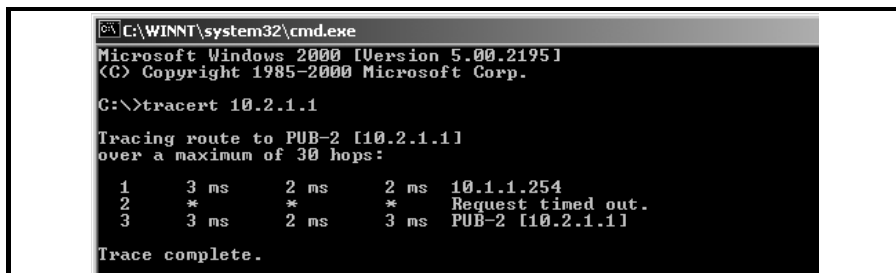
Disable the Cisco Security Agent service.



When Cisco Security Agent is disabled, the URL `http://EASTxA/://` should look like this figure.



When Cisco Security Agent is disabled, a trace route to the Cisco CallManager in the other pod should look like this figure.



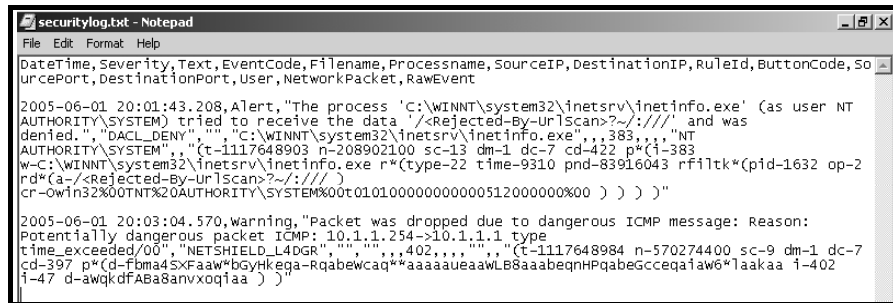
When Cisco Security Agent is active, the URL `http://EASTxA/://` should look like this figure.



When Cisco Security Agent is active, a trace route to the Cisco CallManager in the other pod should look like this figure.



The log files of Cisco Security Agent contain more detailed information on the blocked actions. The first entry describes the blocking of the URL exploit, and the second entry describes the trace route ICMP blocking.



Lab 1-2: Securing Cisco CallManager Administration

Complete this lab activity to practice what you learned in the related module.

Activity Objective

In this activity, you will protect the management access to Cisco CallManager by using HTTPS and secure Cisco CallManager Administration with the MLA feature. After completing this activity, you will be able to meet these objectives:

- Locate the HTTPS certificate on the server and identify certificate fields
- Configure the browser client to trust the HTTPS certificate from Cisco CallManager Administration
- Enable MLA access on the publisher server and change the Cisco CallManager Administrator password
- Add users to the Cisco CallManager database
- Assign privileges to user groups
- Add users to MLA user groups

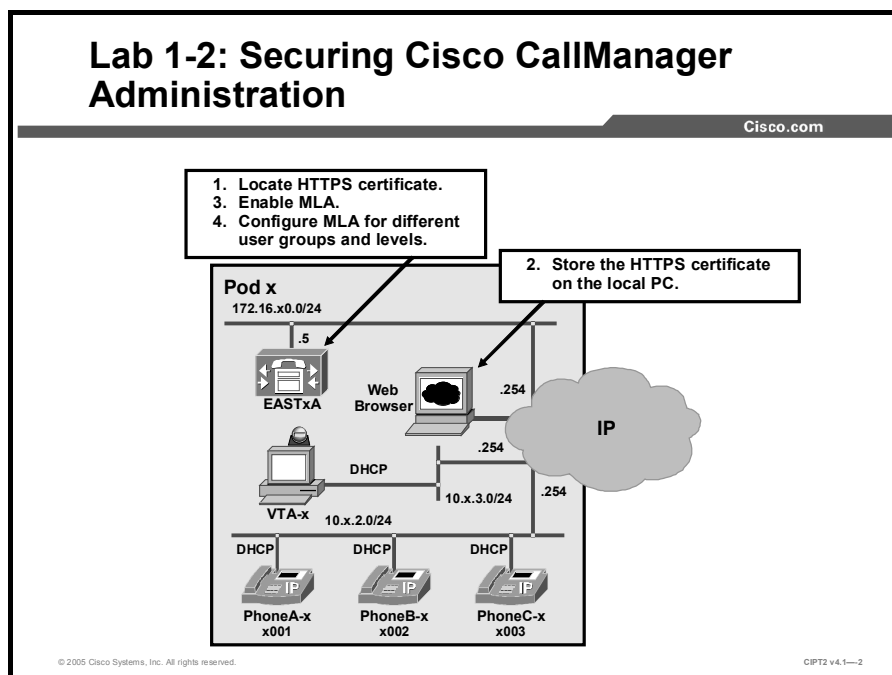
Visual Objective

In this activity, you will learn how to use HTTPS to securely manage Cisco CallManager and how to implement and configure Cisco CallManager MLA to secure the administrative functions. You will identify the Cisco CallManager certificate and configure a client browser to use this certificate for HTTPS. Also, you will enable MLA on the Cisco CallManager server to provide different levels of administration for different users.

The figure illustrates what you will accomplish in this activity.

Lab 1-2: Securing Cisco CallManager Administration

Cisco.com



Required Resources

These are the resources and equipment required to complete this activity:

- The lab devices shown in the Visual Objectives figure and detailed in the table

Lab Devices and Their Roles

Device	Device Role in the Activity
EASTxA	Cisco CallManager publisher that serves the IP Phones
VTA-x	PC with Internet Explorer browser

- The device credentials in the table, to log in to the lab devices that require authentication

Credentials for Device Access

Device	Username and Password
EASTxA	administrator lab PhoneAdmin lab123 HuntAdmin lab123 CCMAdministrator lab
VTA-x	administrator lab

Job Aid

This job aid is available to help you complete the lab activity.

- The lab devices use the IP address allocation scheme shown in the table.

IP Address Allocation Scheme

Device	IP Address
Voice server network	172.16.x0.0/24
IP Phone network	10.x.2.0/24
Data network	10.x.3.0/24
Default gateway	Node address .254 (for all networks)
EASTxA	172.16.x0.5
VTA-x	DHCP-assigned (10.x.3.0)

Task 1: View the HTTPS Certificate

In this task, you will locate the HTTPS certificate on the Cisco CallManager server and identify important certificate fields, such as the certificate expiration date, and write down the certificate fingerprint.

Activity Procedure

Complete these steps:

- Step 1** On the VTA PC, connect to Cisco CallManager EASTxA via a VNC connection. VNC.exe is located on the desktop of the VTA-x PC. Double-click the **VNC** icon and enter the IP address of EASTxA.
- Step 2** On EASTxA, in Windows Explorer, locate the **HTTPS** certificate in C:\Program Files\Cisco\Certificates.
- Step 3** Double-click the **https-cert.cer** certificate and choose the **Details** tab to examine the certificate properties.

Step 4 Locate the thumbprint (fingerprint) of the certificate and write it in the space provided:

Note This fingerprint should be out-of-band verified before the certificate is installed on a client PC when you browse to the web server.

Activity Verification

You have completed this task when you attain these results:

- You located the HTTPS certificate in Cisco CallManager and viewed its content as described in the activity procedure.
- You wrote down the certificate fingerprint.

Task 2: Save the HTTPS Certificate in the Trusted Folder on the Browser Client

You will save the HTTPS certificate in the trusted folder on the browser client so that the Security Alert dialog box does not display each time that you access the web application.

Activity Procedure

Complete these steps:

Step 1 On the VTA-x PC, log in to EASTxA using Internet Explorer and the URL **https://EASTxA/ccmadmin**.

Step 2 When the Security Alert dialog box appears, click **View Certificate** and verify that the certificate is the same on the client side as on the Cisco CallManager side. Do this by comparing the fingerprint of the received certificate with the fingerprint of the certificate that is installed on the Cisco CallManager server (which you wrote down in Step 4 of Task 1).

Note A difference between the fingerprint of the certificate that is installed on your Cisco CallManager server and the fingerprint of the certificate that you receive when browsing to the server would indicate a man-in-the-middle attack.

Step 3 In the Certificate pane, click **Install Certificate** and click **Next**.

Step 4 Click the **Place All Certificates in the Following Store** radio button; click **Browse**.

Step 5 Browse to **Trusted Root Certification Authorities**, click **OK**, click **Next**, and click **Finish**.

Step 6 To install the certificate, click **Yes** (a message states that the import was successful) and click **OK**.

Step 7 In the lower-right corner of the dialog box, click **OK**.

Step 8 To trust the certificate so that the dialog box does not appear again, click **Yes**.

Activity Verification

You have completed this task when you attain these results:

- You can successfully log in to Cisco CallManager using HTTPS.
- The certificate that you received when browsing to Cisco CallManager matched the actual certificate of the Cisco CallManager.

Task 3: Enable Multilevel Administration Access

In this task, you will enable MLA for Cisco CallManager and change the password for the administrator.

Activity Procedure

Complete these steps:

- Step 1** On the VTA-x PC, connect to the Cisco CallManager on EASTxA using the URL **https://EASTxA/ccmadmin**.
- Step 2** In Cisco CallManager Administration, choose **User > Access Rights > Configure MLA Parameters**.
- Step 3** Enable MLA. In the MLA Enterprise Parameter Configuration window, set the Enable MultiLevelAdmin parameter to **True**.
- Step 4** The new administrative account requires you to set a new password for the CCMAAdministrator account. Enter **lab** as the new CCMAAdministrator password and click **Update** to save the changes.
- Step 5** On the VTA-x PC, connect to EASTxA using a VNC session. Choose **Start > Programs > Administrative Tools > Services**.
- Step 6** Select and right-click the **Worldwide Web Publishing Service**, choose **Stop** to stop the service, then choose **Start** to restart the service.

Note You can also use the **Restart** button to stop and automatically start the service.

- Step 7** Exit the VNC session to EASTxA.

Activity Verification

You have completed this task when you attain this result:

- You can log in to Cisco CallManager using the CCMAAdministrator account.

Specifically, complete this step:

- Step 1** On the VTA-x PC, open Internet Explorer and log in to Cisco CallManager administration on EASTxA. Use the username CCMAAdministrator and the password lab.

Task 4: Add Users to MLA

In this task, you will add a user to an existing MLA group to delegate IP Phone administration to that user.

Activity Procedure

Complete these steps:

- Step 2** On the VTA-x PC, use Internet Explorer to connect to Cisco CallManager administration on EASTxA.
- Step 3** Choose **Users > Add a New User** and create a new user with these values:
 - Last name: **PhoneAdmin**
 - UserID: **PhoneAdmin**
 - Password: **lab123**
 - PIN: **12345**
- Step 4** Click **Insert** to add the new user to the Cisco CallManager database.
- Step 5** From Cisco CallManager Administration, choose **User > Access Rights > User Group**.
- Step 6** In the **User Group Configuration** window, choose the **PhoneAdministration** group.
- Step 7** Verify that the **PhoneAdministration** group is selected. Next, add a new user to the group by clicking the **Add User to Group** link in the upper-right corner.
- Step 8** A search field is displayed, where you can search for all users in the system. Search for the user **PhoneAdmin**, choose the user, and add the selected user to the **PhoneAdministration** group.
- Step 9** After you adding the user to the group, all users in the PhoneAdministration group are displayed.

Activity Verification

You have completed this task when you attain this result:

- The PhoneAdmin user has permissions to create, delete, or modify IP Phones in Cisco CallManager Administration.

Specifically, complete these steps:

- Step 1** On the VTA-x PC, use Internet Explorer to connect to Cisco CallManager administration on EASTxA.
- Step 2** Choose **Users > Access Rights > User Group** and choose **PhoneAdministration**.
- Step 3** Click the **Key** symbol to the right of the PhoneAdmin user.
- Step 4** Verify that the PhoneAdministration group has full access to the functional groups Standard Phone and Standard User Management but no access to any other functional groups.
- Step 5** Exit the Cisco CallManager web GUI and reconnect to the Cisco CallManager on EASTxA using the PhoneAdmin account.
- Step 6** Choose **Devices > Phone** and choose **Add a New Phone**. Create a dummy telephone to verify that you have the proper rights to do so.

- Step 7** Choose **Route Plan > Translation Pattern** to create a new translation pattern. The Insert button is dimmed, and it is not possible to insert the new translation pattern.

Task 5: Assign Privileges to User Groups

In this task, you will create a new user group that will be responsible for managing hunt groups, and you will assign rights to this group. You will need to configure a user group and a functional group and assign the appropriate rights to these groups.

Activity Procedure

Complete these steps:

- Step 1** On the VTA-x PC, use Internet Explorer to connect to Cisco CallManager administration on EASTxA using the CCMAAdministrator account.
- Step 2** Choose **Users > Access Rights > User Group** and add a new user group called **HuntAdmins**. Click **Insert**.
- Step 3** Click **Add a New Functional Group** and create the new functional group **HuntGroup**.
- Step 4** Choose these permissions for HuntGroup:
- Route/Hunt > Route Pattern
 - Route/Hunt > Line Group
 - Route/Hunt > Route Group
 - Route/Hunt > Route List
 - Route Plan Report
 - Class of Control > Time Period
 - Class of Control > Time Schedule
 - Route/Hunt > Hunt List
 - Route/Hunt > Hunt Pilot
- Do not add any other permissions for this functional group.
- Step 5** Click **Insert** to create the new functional group **HuntGroup**.
- Step 6** Return to the User Group configuration window by choosing **Users > Access Rights > User Group** and choose the user group **HuntAdmins**.
- Step 7** Verify that the **HuntAdmins** group is selected and map the functional group **Hunt Group** to the user group **HuntAdmins** by clicking **Assign Privileges** in the upper-right corner. All functional groups are displayed.
- Step 8** Choose the functional group **Hunt Group** and assign the **Full Access** option for HuntAdmins. For all other functional groups, assign **Read Only**. Click **Update**.

Activity Verification

This task will be verified after you finish Task 6.

Task 6: Add Users to User Groups

In this task, you will add a user to the newly created MLA HuntAdmin group.

Activity Procedure

Complete these steps:

- Step 1** On the VTA-x PC, connect to the Cisco CallManager system on EASTxA using the CCMAAdministrator account.
- Step 2** Choose **Users > Add a New User** and create a new user with these values:
 - Last name: **HuntAdmin**
 - User ID: **HuntAdmin**
 - Password: **lab123**
 - PIN: **12345**
- Step 3** Click **Insert** to add the new user to the Cisco CallManager database.
- Step 4** Choose **Users > Access Rights > User Group**, choose **HuntAdmins** and click **Add a User to Group** in the upper-right corner.
- Step 5** Search for the user **HuntAdmin**, choose the user, and add the user to the **HuntAdmins** group.

Activity Verification

You have completed this task when you attain this result:

- The HuntAdmin user can create, delete, or modify hunt groups.

Specifically, complete these steps:

- Step 1** On the VTA-x PC, connect to the Cisco CallManager system on EASTxA.
- Step 2** Choose **Users > Access Rights > User Group** and choose **HuntAdmins**. Click the **Key** symbol to the right of the HuntAdmin user.
- Step 3** Verify that the HuntAdmins group has full access to the functional group HuntGroup, but only read access to all other functional groups.
- Step 4** Exit the Cisco CallManager web GUI and reconnect to the Cisco CallManager on EASTxA using the HuntAdmin account.
- Step 5** Choose **Route Plan > Route/Hunt** and create a new hunt list. Use these values:
 - Hunt List Name: **HQSales01**
 - Description: **Headquarter Sales 01**
 - Cisco CallManager Group: **Default**
- Step 6** Click **Insert** to create the hunt list. Now, hunt groups can be added to the hunt list HQSales01.
- Step 7** Choose **Route Plan > Translation Pattern** to create a new translation pattern. The Insert button is dimmed and it is not possible for the user HuntAdmin to create a new translation pattern.

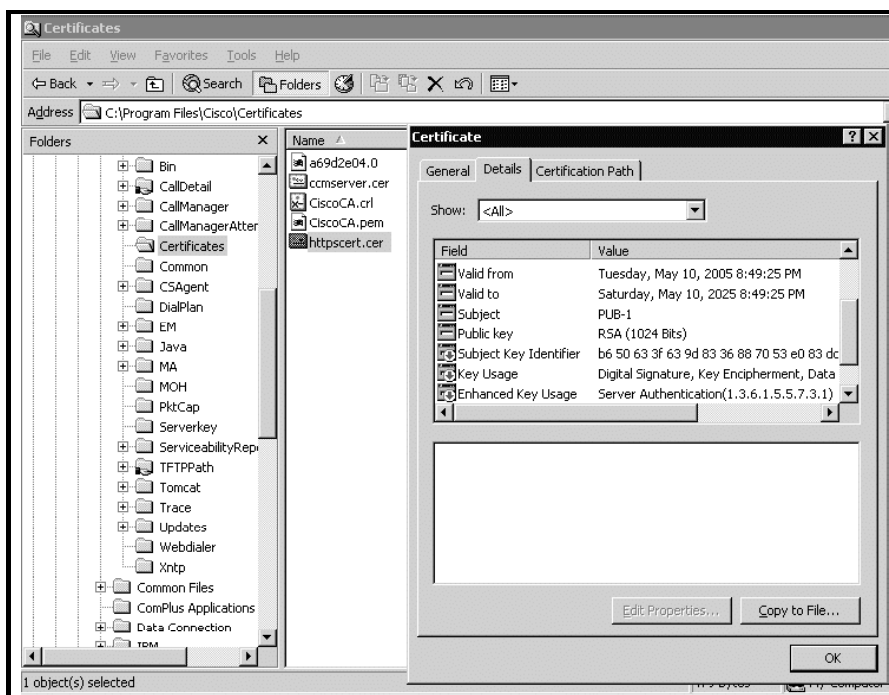
Lab 1-2 Answer Key: Securing Cisco CallManager Administration

When you complete this activity, your solution will be similar to this, with differences that are specific to your device or workgroup.

Task 1: View the HTTPS Certificate

This procedure enables you to complete the activities described in the task.

The details of the httpscert.cer certificate are shown in the figure.



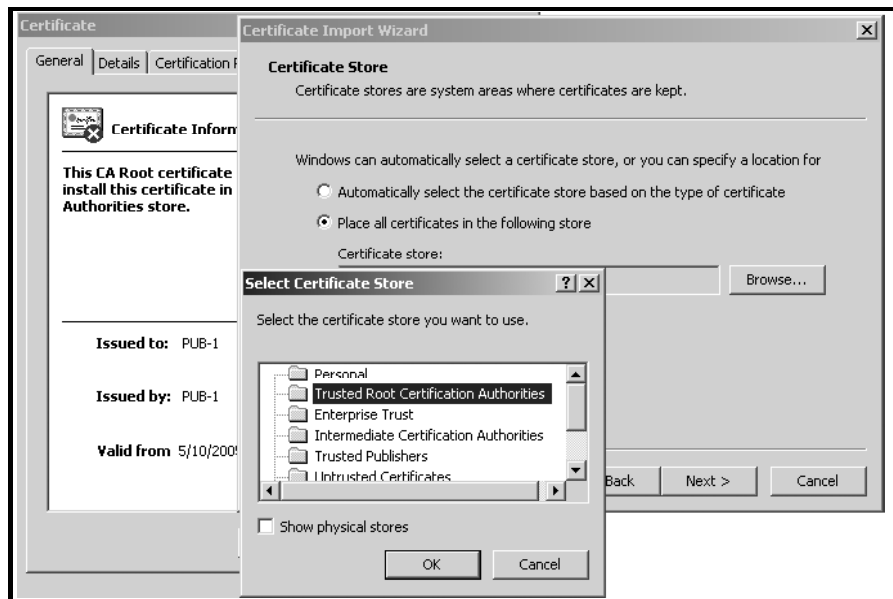
Task 2: Save the HTTPS Certificate in the Trusted Folder on the Browser Client

This procedure enables you to complete the activities described in the task.

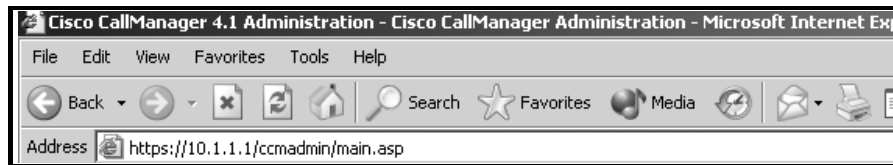
Install the certificate.



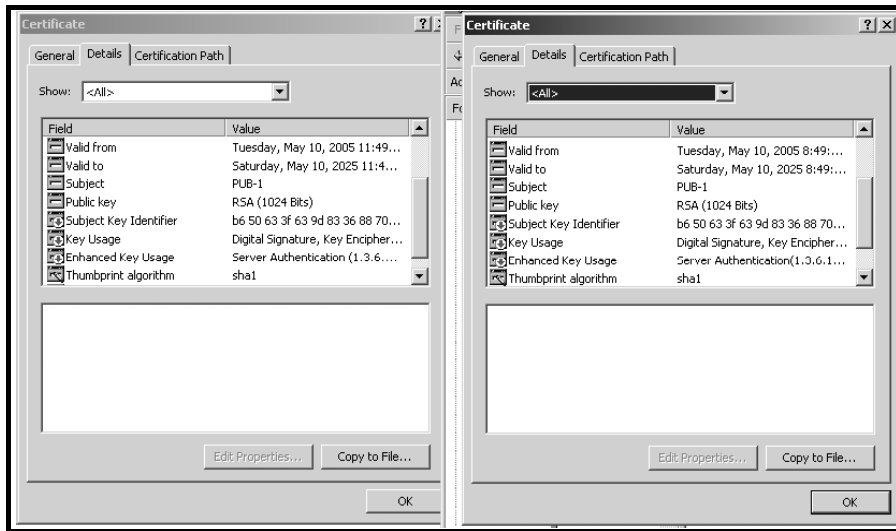
Save the HTTPS certificate to the trusted folder.



The first task verification is to open the browser and access Cisco CallManager on EASTxA at <https://EASTxA/ccmadmin>.



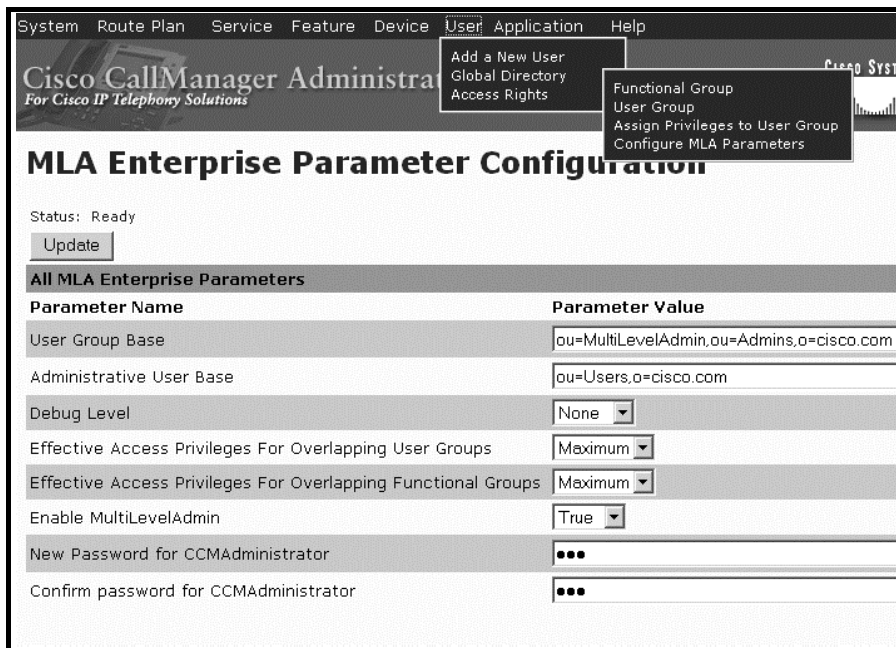
The second task verification is to verify that the certificate parameters match on both sides.



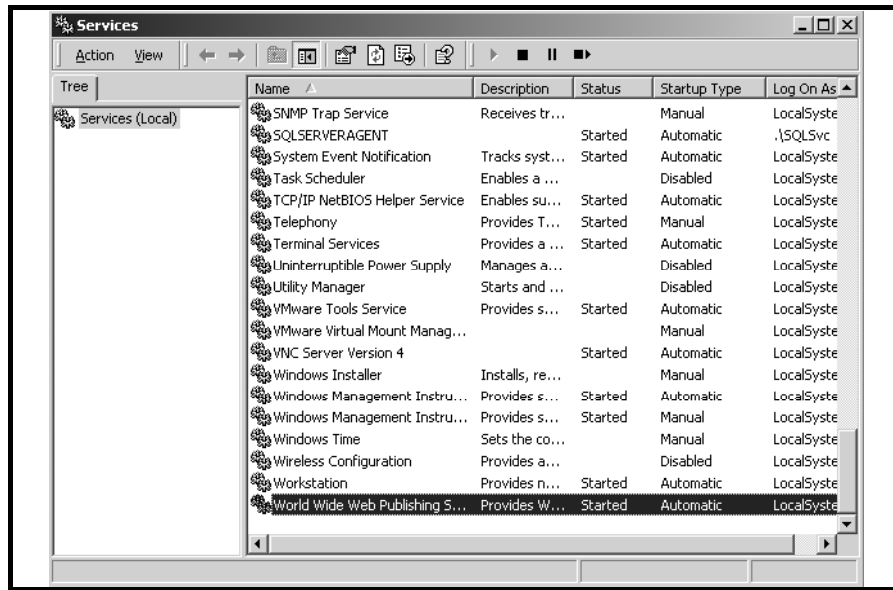
Task 3: Enable Multilevel Administration Access

This procedure enables you to complete the activities described in the task.

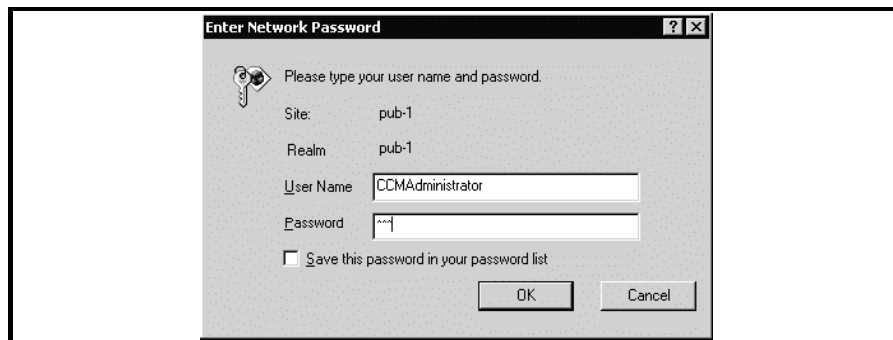
Enable MLA on the Cisco CallManager GUI.



Do not forget to restart the web service on EASTxA.



Log in to the Cisco CallManager system on EASTxA using the CCMAAdministrator account.



Task 4: Add Users to MLA

This procedure enables you to complete the activities described in the task.

Add a new user.

User Configuration

Application Profiles of

<No Application Profiles>

Application Profiles can be accessed after the new User is inserted in the directory.

User : New User

Status: Ready

First Name

Last Name*

User ID*

User Password*

Confirm Password*

PIN *

Confirm PIN *

Map the user PhoneAdmin to the predefined group PhoneAdministration.

User Group Configuration

[Add a User to Group](#)
[Add a New Functional Group](#)
[Assign Privilege](#)

User Groups

<Add a New User Group>

- PhoneAdministration
- ReadOnly
- ServerMonitoring
- SuperUserGroup
- ServerMaintenance
- GateWayAdministration

User Group: PhoneAdministration

Status: Ready

Users in the group

Last Name	First Name	User ID	Permissions
<input type="checkbox"/> PhoneAdmin	PhoneAdmin	PhoneAdmin	

Verify the permission settings for the PhoneAdmin user.

Privileges Report

[Back to User Group Configuration](#)

Permissions for User: PhoneAdmin PhoneAdmin

Functional Groups

User Groups	Standard Plugin	Standard User Privilege Management	Standard User Management	Standard Feature	Standard System
PhoneAdministration	Read Only	Read Only	Full Access	Read Only	Read Only
Net Permissions	Read Only	Read Only	Full Access	Read Only	Read Only

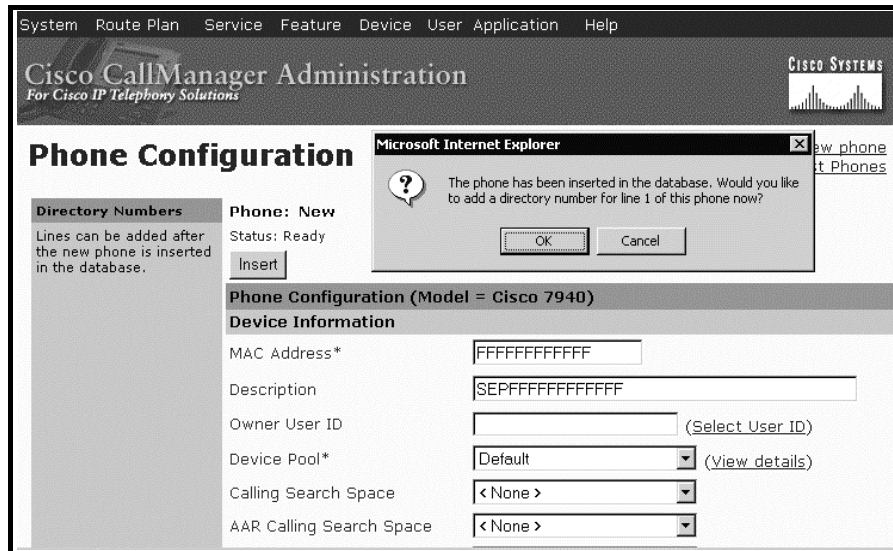
Functional Groups

User Groups	Standard Service Management	Standard Service	Standard Serviceability	Standard Gateway	Standard RoutePlan
PhoneAdministration	Read Only	Read Only	Read Only	Read Only	Read Only
Net Permissions	Read Only	Read Only	Read Only	Read Only	Read Only

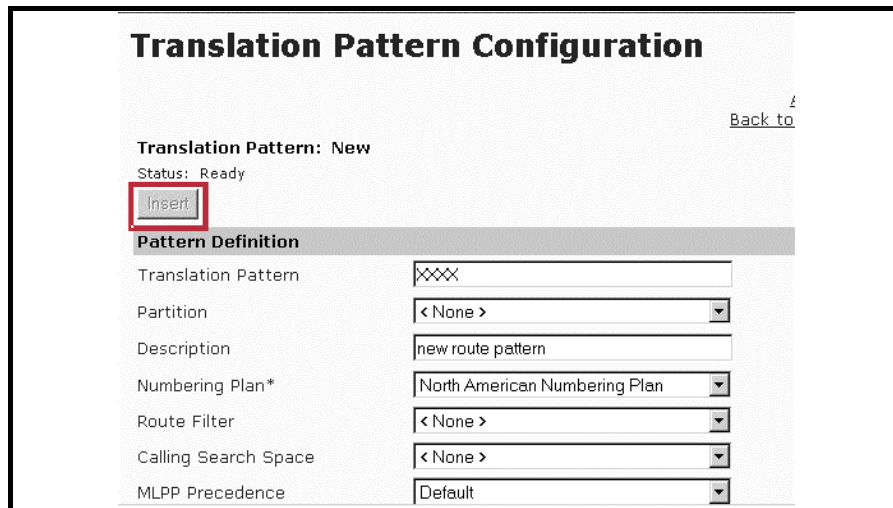
Functional Groups

User Groups	Standard Phone
PhoneAdministration	Full Access
Net Permissions	Full Access

Log in to the Cisco CallManager system on EASTxA with the PhoneAdmin account, and create and insert a dummy IP Phone.



Attempt to create a translation pattern.



It is not possible to create the translation pattern with the PhoneAdmin account, because the Insert button is dimmed and it is not possible to insert the new translation pattern.

Task 5: Assign Privileges to User Groups

This procedure enables you to complete the activities described in the task.

After adding the new user group HuntAdmins, configure the functional group HuntGroup and provide it with the appropriate permissions.

Functional Group Configuration

[Add a New User Group](#)
[Assign Privileges](#)

Functional Groups

<Add a New Functional Group>

- Standard Plugin
- Standard User Privilege Management
- Standard User Management
- Standard Feature
- Standard System
- Standard Service Management
- Standard Service
- Standard Serviceability
- Standard Gateway

Functional Group: Insert

Status: Ready

Functional Group Name*

Cisco CallManager Administration

System

- Server
- Cisco CallManager
- Cisco CallManager Group
- Date/Time Group
- Device Defaults
- Region
- Device Pool
- Enterprise Parameters
- Location
- SRST

Assign the appropriate privileges to the user group HuntAdmins.

Assign Privileges to User Group

[View Privileges Report](#)
[Add a New Functional Group](#)
[Add a New User Group](#)

User Groups

- PhoneAdministration
- ReadOnly
- ServerMonitoring
- HuntAdmins**
- SuperUserGroup
- ServerMaintenance
- GateWayAdministration

User Group: HuntAdmins

Status: Ready

Functional Group	Access Privilege
Standard User Privilege Management	Read Only
Standard Serviceability	Read Only
Standard Phone	Read Only
HuntGroup	Full Access
Standard System	Read Only
Standard Service	Read Only
Standard RoutePlan	Read Only
Standard Service Management	Read Only
Standard User Management	Read Only
Standard Plugin	Read Only
Standard Feature	Read Only
Standard Gateway	Read Only

Verify the status of the user groups with the Privileges Report.

Privileges Report Back to Assign Privileges					
Functional Groups					
User Groups	Standard Plugin	HuntGroup	Standard User Privilege Management	Standard User Management	Standard Feature
PhoneAdministration	Read Only	No Access	Read Only	Full Access	Read Only
ReadOnly	Read Only	No Access	Read Only	Read Only	Read Only
ServerMonitoring	Read Only	No Access	Read Only	Read Only	Read Only
HuntAdmins	Read Only	Full Access	Read Only	Read Only	Read Only
SuperUserGroup	Full Access	Full Access	Full Access	Full Access	Full Access
ServerMaintenance	Full Access	No Access	Read Only	Read Only	Full Access
GateWayAdministration	Read Only	No Access	Read Only	Read Only	Read Only

Functional Groups					
User Groups	Standard System	Standard Service Management	Standard Service	Standard Serviceability	Standard Gateway
PhoneAdministration	Read Only	Read Only	Read Only	Read Only	Read Only
ReadOnly	Read Only	Read Only	Read Only	Read Only	Read Only
ServerMonitoring	Read Only	Read Only	Read Only	Full Access	Read Only
HuntAdmins	Read Only	Read Only	Read Only	Read Only	Read Only
SuperUserGroup	Full Access	Full Access	Full Access	Full Access	Full Access
ServerMaintenance	Full Access	Full Access	Full Access	Read Only	Read Only
GateWayAdministration	Read Only	Read Only	Read Only	Read Only	Full Access

Functional Groups		
User Groups	Standard RoutePlan	Standard Phone
PhoneAdministration	Read Only	Full Access
ReadOnly	Read Only	Read Only
ServerMonitoring	Read Only	Read Only
HuntAdmins	Read Only	Read Only
SuperUserGroup	Full Access	Full Access
ServerMaintenance	Read Only	Read Only

Task 6: Add Users to User Groups

This procedure enables you to complete the activities described in the task.

Add the HuntAdmin user to the HuntAdmins group.

User Group Configuration

User Group: HuntAdmins
1 matching record(s)

Query: Basic Search = hunt

Refine Search

Last Name	First Name	User ID
<input checked="" type="checkbox"/> HuntAdmin	HuntAdmin	11111

Verify the permissions for the HuntAdmin user.

Privileges Report						Back to User Group Configuration
Permissions for User: HuntAdmin HuntAdmin						
Functional Groups						
User Groups	Standard Plugin	HuntGroup	Standard User Privilege Management	Standard User Management	Standard Feature	
HuntAdmins	Read Only	Full Access	Read Only	Read Only	Read Only	
Net Permissions	Read Only	Full Access	Read Only	Read Only	Read Only	
Functional Groups						
User Groups	Standard System	Standard Service Management	Standard Service	Standard Serviceability	Standard Gateway	
HuntAdmins	Read Only	Read Only	Read Only	Read Only	Read Only	
Net Permissions	Read Only	Read Only	Read Only	Read Only	Read Only	
Functional Groups						
User Groups	Standard RoutePlan		Standard Phone			
HuntAdmins	Read Only		Read Only			
Net Permissions	Read Only		Read Only			

Tip If you experience difficulty when you log in using the HuntAdmin account, put the HuntAdmin account in an existing, predefined MLA user group, update, and log in with the HuntAdmin account. Log off again and put the HuntAdmin account in the HuntAdmins user group.

When the HuntAdmin user is logged in to the Cisco CallManager system, you can create a Hunt List.

Hunt List Configuration		Add a new Hunt List
		Back to Find/List Hunt Lists
		Dependency Records
Hunt List Details	Hunt List: HQSales01	
	Status: Insert completed	
	<input type="button" value="Copy"/> <input type="button" value="Update"/> <input type="button" value="Delete"/> <input type="button" value="Reset"/>	
	Hunt List Information	
	Hunt List Name*	<input type="text" value="HQSales01"/>
	Description	<input type="text" value="Headquarter Sales 01"/>
	Cisco CallManager Group*	<input type="text" value="Default"/>
	<input checked="" type="checkbox"/> Enable this Hunt List (change effective on Update; no reset required)	
	Hunt List Member Information	
	<input type="button" value="Add Line Group"/>	
	Selected Groups* (ordered by highest priority)	<div style="border: 1px solid black; height: 40px; width: 100%;"></div>

Creating a translation pattern is not possible for the HuntAdmin user, because the missing permissions cause the Insert button to appear dimmed.

Translation Pattern Configuration

[Add a New](#) | [Back to Find/List T](#)

Translation Pattern: New
Status: Ready

Pattern Definition

Translation Pattern	<input type="text" value="9XXX"/>
Partition	<input type="text" value="< None >"/>
Description	<input type="text"/>
Numbering Plan*	<input type="text" value="North American Numbering Plan"/>
Route Filter	<input type="text" value="< None >"/>
Calling Search Space	<input type="text" value="< None >"/>

Lab 1-3: Preventing Toll Fraud

Complete this lab activity to practice what you learned in the related module.

Activity Objective

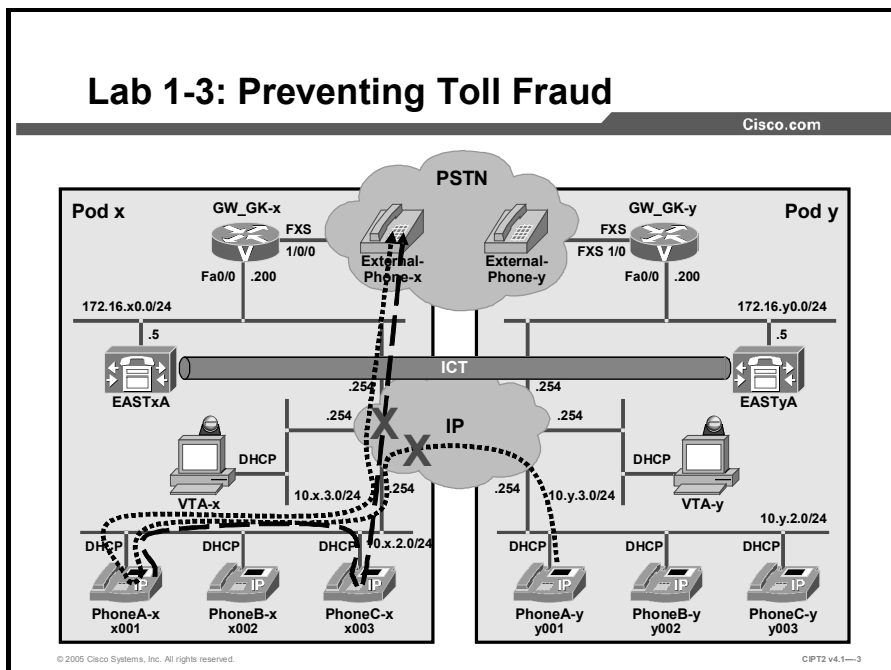
In this activity, you will prevent toll fraud. After completing this activity, you will be able to meet these objectives:

- Using partitions and calling search spaces, restrict call forwarding based on user classes and configure route patterns to block commonly exploited area codes
- Configure Cisco CallManager to route calls to different locations based on the time of day when a call is made
- Design and implement FAC levels to require user authorization for different classes of calls
- Provide external call transfer blocking by setting service parameters and configuring gateways, trunks, and route patterns as OffNet (external) devices
- Configure Cisco CallManager Administration to drop a conference call when the last OnNet party leaves the call

Visual Objective

First you will configure different partitions and calling search spaces to prevent toll fraud when calls are forwarded to external destinations. Second, you will configure time-of-day routing for business hours and FAC for international dialing. Finally, you will restrict call transfers and change conferencing behavior.

The figure illustrates what you will accomplish in this activity.



Required Resources

These are resources and equipment required to complete this activity:

- The lab devices shown in the Visual Objectives figure and detailed in the table

Lab Devices and Their Roles

Device	Device Role in the Activity
EASTxA	Cisco CallManager publisher that serves the IP Phones
VTA-x	PC where the Cisco VT Advantage software has to be installed
PhoneA-x	Video-enabled IP Phone that has PC with Cisco VT Advantage connected to it
PhoneB-x, PhoneC-x	IP Phones

- The device credentials in the table, to log in to the lab devices that require authentication

Credentials for Device Access

Device	Username and Password
EASTxA	administrator lab
Cisco CallManager Administration	ccadministrator lab
VTA-x	administrator lab

Job Aids

These job aids are available to help you complete the lab activity.

- The table lists the DNs needed to place calls in the lab activity.

Directory Numbers

Device	Directory Number
PhoneA-x	x001, where x = your pod number
PhoneB-x	x002, where x = your pod number
PhoneC-x	x003, where x = your pod number
PhoneA-y	y001, where y = your partner pod number
PhoneB-y	y002, where y = your partner pod number
PhoneC-y	y003, where y = your partner pod number

- The lab devices use the IP address allocation scheme shown in the table.

IP Address Allocation Scheme

Device	IP Address
Voice server network	172.16.x0.0/24
IP Phone network	10.x.2.0/24
Data network	10.x.3.0/24
Default gateway	Node address .254 (for all networks)
EASTxA	172.16.x0.5
GW_GK-x	172.16.x0.200
PhoneA-x	DHCP-assigned (network 10.x.2.0)
PhoneB-x	DHCP-assigned (network 10.x.2.0)
PhoneC-x	DHCP-assigned (network 10.x.2.0)
VTA-x	DHCP-assigned (network 10.x.3.0)

- At the beginning of this lab activity, no partitions or calling search spaces are configured. All devices and route patterns are using the default <None> partition and the default <None> calling search space. In this lab activity, you will change the calling search space and partition configuration as shown in the table.

Partition and Route Pattern Scheme

Partition Name	Description	Assigned DNs and Route Patterns
<None>	<None>	x001 x002 x003 yXXX 9.555X009
National_general	National calling for general employees	9.[^0]!#
National_executives	National calling for executives and managers. (The route pattern is used only for national calls. “^0” means that after the 9 is dialed, no 0 can follow.)	9.[^0]!#
International	International calling. (The route pattern is used for international calls. An international call from the United States to foreign countries is classified with 9011.)	9.011!#
Fraud_Prevention	Blocked frequently exploited area codes	9.1242xxxxxx# 9.1345xxxxxx# 9.1664xxxxxx#

Note You must dial “#” at the end of the each number when dialing an external telephone number.

- During the lab activity, you will configure calling search spaces as shown in the table.

Calling Search Space Overview

Calling Search Space Name	Description	Partition Order in Calling Search Space
general	Calling search space for general employees	National_general Fraud_Prevention International <None>
executives_and_managers	Calling search space for executives and managers	National_executives International <None>
CFA_general	Call forwarding for general employees	Fraud_Prevention <None>
CFA_executives	Call forwarding for executives and managers	National_executives <None>

- At the beginning of this lab activity, no call forwarding restrictions are configured. During the activity, you will apply calling search spaces and call forwarding restrictions as shown in the table.

IP Phone Configuration

Phone	Partition	Calling Search Space	Call Forward All Calling Search Space
PhoneA-x	<None>	executives_and_manager	CFA_executives_and_manager
PhoneB-x	<None>	executives_and_manager	CFA_general
PhoneC-x	<None>	general	CFA_general

Frequently Exploited Area Codes

Route Pattern	Bahamas	Cayman Islands	Montserrat
Route pattern	9.1242xxxxxx#	9.1345xxxxxx#	9.1664xxxxxx#
Partition	Fraud_Prevention	Fraud_Prevention	Fraud_Prevention
Description	Bahamas	Cayman Islands	Montserrat
Gateway	GW_GK-x	GW_GK-x	GW_GK-x
Route option	<ul style="list-style-type: none"> ■ Block this pattern ■ Call Rejected 	<ul style="list-style-type: none"> ■ Block this pattern ■ Call Rejected 	<ul style="list-style-type: none"> ■ Block this pattern ■ Call Rejected

- Additionally, you will use *Cisco CallManager Administration Guide, Release 4.1(3)*.

Task 1: Restrict Call Forward All and Block Commonly Exploited Area Codes

In this task, you will create partitions and calling search spaces to restrict call forwarding. All IP Phone DNs should use the values for partitions, calling search spaces and Call Forward All described in the Job Aids section. Additionally, you will configure blocking of commonly exploited area codes. The area codes for Bahamas, Cayman Islands, and Montserrat will be blocked for all IP Phones using the “general” calling search space.

Activity Procedure

Complete these steps:

Step 1 From VTA-x use Internet Explorer to access Cisco CallManager administration on EASTxA and choose **Route Plan > Class of Control > Partition**. Click **Add a New Partition**.

Step 2 Using the partition configuration data from the “Partition and Route Pattern Scheme” table (in the job Aids section of the lab), enter all the partition names in this format:

<partitionName>, <description>

<partitionName>, <description>

...

Note Do not add any partitions or calling search spaces called <None>. These partitions and calling search spaces exist by default and cannot be added.

Step 3 Click **Insert** and then click **OK** to add the partitions to the Cisco CallManager database.

Step 4 In the Cisco CallManager Administration window on EASTxA, choose **Route Plan > Class of Control > Calling Search Space**. Click **Add a New Calling Search Space**. Repeat these substeps for each calling search space that is listed in the “Calling Search Space Overview” table:

1. Use the “Calling Search Space Overview” table (in the Job Aids section) to enter a calling search space name and description. Use the information in the “Calling Search Space Overview” table to choose the appropriate partitions.
2. Use the **Arrow** keys to place the partitions in the same order as that shown in the “Calling Search Space Overview” table and click **Insert** to add the calling search space.
3. Click **Add a New Calling Search Space** to open the CSS Configuration window.

Note Do not add any partitions or calling search spaces called <None>. These partitions and calling search spaces exist by default and cannot be added.

Step 5 In the Cisco CallManager Administration window on EASTxA, choose **Route Plan > Route/Hunt > Route Pattern**. and add the existing route patterns to the respective partitions.

Step 6 Click **Find** to list all route patterns. Choose the route pattern **9.[^0]!#** and change the partition from <None> to **National_general**. Click **Update** to save the changes.

Step 7 Click **Copy** to copy the route pattern. Change the partition from **National_general** to **National_executives**. Change the description from **Copy of 9.[^0]!#** to **PSTN**. Leave all other fields at their current values and click **Insert** to add the route pattern.

Step 8 Click **Back to Find/List Route Patterns** to list all route patterns. Choose the route pattern **9.011!#** and change the partition from <None > to **International**. Click **Update** to save the changes.

Step 9 Click **Add a New Route Pattern** to create a new route pattern. Create three route patterns reflecting the information in the “Frequently Exploited Area Codes” table. After you add all necessary information (as described in the table) in the route pattern configuration window, click **Insert** to create the route pattern. Repeat this process for each route pattern described in the “Frequently Exploited Area Codes” table (in the Job Aids section).

Note Use all values described in the “Frequently Exploited Area Codes” table. All other values in the route pattern configuration can be left at their default values.

- Step 10** In Cisco CallManager Administration on EASTxA, choose **Device > Phone**.
- Step 11** Click **Find** to list the IP Phones that are registered in Cisco CallManager.
- Step 12** Choose the IP Phone with the description “PhoneA-x.” The Phone Configuration window appears.
- Step 13** Click **Line 1 – x001** in the left column to access the Directory Number configuration window.
- Step 14** Change the calling search space from <None> to **executives_and_manager**.
- Step 15** Choose **CFA_executives** in the Forward All Calling Search Space field.
- Step 16** Click **Update** at the top of the window. Reset the IP Phone by clicking **Reset**, and press **OK** twice to confirm the reset.
- Step 17** Choose **Configure Device** to return to the Phone Configuration window. Then click **Back to Find/List Phones**.
- Step 18** Choose the IP Phone with the description “PhoneB-x.” The Phone Configuration window appears.
- Step 19** Click **Line 1 – x002** in the left column to access the Directory Number configuration window.
- Step 20** Change the calling search space from <None> to **executives_and_manager**.
- Step 21** Choose **CFA_general** in the Forward All Calling Search Space field.
- Step 22** Click **Update** at the top of the window. Reset the IP Phone by clicking **Reset**, and press **OK** twice to confirm the reset.
- Step 23** Choose **Configure Device** to return to the Phone Configuration window. Click **Back to Find/List Phones**.
- Step 24** Choose the IP Phone with the description “PhoneC-x.” The Phone Configuration window appears.
- Step 25** Click **Line 1 – x003** in the left column to access the Directory Number configuration window.
- Step 26** Change the calling search space from <None> to **general**.
- Step 27** Choose **CFA_general** in the Forward All Calling Search Space field.
- Step 28** Click **Update** at the top of the window. Reset the IP Phone by clicking **Reset**, and press **OK** twice to confirm the reset.

Activity Verification

You have completed this task when you attain these results:

- Forwarding from PhoneA-x to a PSTN destination works.
- Forwarding from PhoneB-x to a PSTN destination does not work.
- Forwarding from PhoneC-x to a PSTN destination does not work.
- Forwarding from PhoneC-x to PhoneA-x works.

- PhoneA-x reaches all international destinations described in the “Frequently Exploited Area Codes” table.
- PhoneB-x and PhoneC-x cannot reach the international destinations described in the “Frequently Exploited Area Codes” table.

Specifically, complete these steps:

Step 1 Forward the x001 destination number of PhoneA-x to External-Phone-x (using a national number, such as 914085551009#). Place a call from PhoneB-x to PhoneA-x (x001). The call should be routed to the PSTN destination.

Note Do not use 9555X009 because this route pattern is in no partition and therefore can be accessed by all phones.

Step 2 Forward the x002 destination number of PhoneB-x to External-Phone-x (using a national number, such as 914085551009#). The call forwarding configuration should be restricted.

Step 3 Forward the x003 destination number of PhoneC-x to External-Phone-x (using a national number, such as 914085551009#). The call forwarding configuration should be restricted.

Step 4 Forward the x003 destination number of PhoneC-x to PhoneA-x (x001). Place a call from PhoneB-x to PhoneC-x (x003). The call should be routed to PhoneA-x.

Step 5 Disable all call forwarding from PhoneA-x, PhoneB-x, and PhoneC-x.

Step 6 Place a call from PhoneA-x to the international destination 912421234567#. The call should be routed.

Step 7 Place a call from PhoneA-x to the international destination 916641234567#. The call should be routed.

Step 8 Place a call from PhoneC-x to the international destination 913451234567#. The call should be rejected.

Step 9 Place a call from PhoneC-x to the international destination 916641234567#. The call should be rejected.

Note All configured route patterns starting with access code 9 are routed to External-Phone-x.

Task 2: Configure Time-of-Day Routing

In this task, you will configure time-of-day routing in Cisco CallManager. Normal office hours are between 8 a.m. and 5 p.m. All external calls within this time period should be routed normally; external calls placed outside this period should be blocked, but only for regular employees. Internal calls are allowed at all times. Further, on Christmas (December 25) and New Year’s Day (January 1), you will not allow external calls through the whole day for regular employees.

Activity Procedure

Complete these steps:

- Step 1** In Cisco CallManager Administration on EASTxA, choose **Route Plan > Class of Control > Time Period**.
- Step 2** Choose **Add a New Time Period** to create a time period.
- Step 3** Enter **OfficeHours** in the Time Period Name field. Choose a start time of **8 am** and an end time of **5 pm**. Repeat this time period from Monday to Friday by clicking the **Week From** radio button and choosing **Mon Through Fri**.
- Step 4** Click **Insert** to create the new time period.
- Step 5** Click **Add a New Time Period** to create the ChristmasDay time period.
- Step 6** Enter **ChristmasDay** in the Time Period Name field. Choose a start time of **No Office Hours** and an end time of **No Office Hours**. Click the **Year On** radio button and choose **Dec 25**.
- Step 7** Click **Insert** to create the new time period.
- Step 8** Choose **Add a New Time Period** to create the NewYearsDay time period.
- Step 9** Enter **NewYearsDay** in the Time Period Name field. Choose a start time of **No Office Hours** and an end time of **No Office Hours**. Click the **Year On** radio button and choose **Jan 1**.
- Step 10** Click **Insert** to create the new time period.
- Step 11** In Cisco CallManager on EASTxA, choose **Route Plan > Class of Control > Time Schedule**.
- Step 12** Choose **Add a New Time Schedule** to create a time schedule.
- Step 13** Enter **ToD_employees** in the Time Period Name field. Choose **OfficeHours**, **ChristmasDay**, and **NewYearsDay** from the available time periods and use the arrow to put them into the Selected time Periods pane.
- Step 14** Click **Insert** to create the new time schedule.
- Step 15** In Cisco CallManager Administration on EASTxA, choose **Route Plan > Class of Control > Partition**.
- Step 16** Click **Find** to list all available partitions.
- Step 17** Choose the **National_general** partition to change the settings of this partition.
- Step 18** Choose the **ToD_employees** time schedule. Click the **Originating Device** radio button. The local time of the IP Phone that places the call will be used to define the time zone.
- Step 19** Click **Update** to apply the changes to the partition.
- Step 20** Choose **Device > Phone** and click **Find** to list all IP Phones.
- Step 21** Select all IP Phones and click **Restart Selected**, **Restart**, and **OK**.

Activity Verification

You have completed this task when you attain these results:

- PhoneA-x and PhoneB-x can call all external destinations either within office hours or beyond office hours.
- PhoneC-x can call all external destinations only within normal office hours.

Specifically, complete these steps:

- Step 22** Place a call from PhoneA-x to a national number, such as 914085551009#. The call should be routed to the destination.
- Step 23** Place a call from PhoneB-x to a national number, such as 914085551009#. The call should be routed to the destination.
- Step 24** Place a call from PhoneC-x to a national number, such as 914085551009#. The call should be routed to the destination.
- Step 25** Change the time on Cisco CallManager to 11 p.m. In Cisco CallManager Administration on EASTxA, choose **System > Device Pool** and click the device pool **Default**. Click **Reset Devices** to reset the all the devices in the device pool. Verify that the IP Phones show the correct time on the LCD screen. Place a call from PhoneC-x to the external destination 9555x009#.
- Step 26** Place a call from PhoneA-x to a national number, such as 914085551009#. The call should be routed to the destination.
- Step 27** Place a call from PhoneB-x to a national number, such as 914085551009#. The call should be routed to the destination.
- Step 28** Place a call from PhoneC-x to a national number, such as 914085551009#. The call should not be routed to the destination.
- Step 29** Change the time on Cisco CallManager back to the actual time. In Cisco CallManager Administration on EASTxA, choose **System > Device Pool** and click the device pool **Default**. Click **Reset Devices** to reset the all the devices in the device pool. Verify that the IP Phones show the correct time on the LCD screen.

Task 3: Use FAC

In this task, you will configure forced authorization codes to restricted call access. You will configure an authorization code for international calls. You will set the authorization level in the route pattern to 30 and require all IP Phones to use the authorization code to dial international numbers. You will set the FAC authorization level in the FAC configuration to 50.

Activity Procedure

Complete these steps:

- Step 1** In Cisco CallManager Administration on EASTxA, choose **Feature > Forced Authorization Code**.
- Step 2** Click **Add a New Forced Authorization Code** to add a new code.
- Step 3** Enter the code name **international**, an authorization code of **4321**, and an authorization level of **50**. Click **Insert**.
- Step 4** In Cisco CallManager on EASTxA, choose **Route Plan > Route/Hunt > Route Pattern**.

- Step 5** Click **Find** to list all available route patterns. Click the route pattern **9.011!#**.
- Step 6** Check the **Require Forced Authorization Code** check box and set an authorization level of **30**.
- Step 7** Click **Update** to save the changes.

Activity Verification

You have completed this task when you attain these results:

- PhoneA-x, PhoneB-x, and PhoneC-x can dial national destinations without entering an authorization code.
- PhoneA-x, PhoneB-x, and PhoneC-x have to enter an authorization code when dialing international destinations.

Specifically, complete these steps:

- Step 8** Place a call from any of your IP Phones to External-Phone-x (using a national number, such as 914085551009#). The call should be routed to External-Phone-x without requiring an authorization code.
- Step 9** Place a call from any of your IP Phones to the international number 90114981513685830#. Insert the authorization code 1234#. The call should not be routed to the other site.
- Step 10** Place a call from any of your IP Phones to the international number 90114981513685830#. Insert the authorization code 4321#. The call should be routed to the other site.

Note All configured route patterns starting with access code 9 are routed to External-Phone-x.

Task 4: Restrict External Transfers

In this task, you will restrict external call transfers by classifying devices as OnNet or OffNet. Trunks and route patterns will be classified as OffNet devices. You will set the service parameter for transfer restrictions to block external to external call transfers.

Activity Procedure

Complete these steps:

- Step 11** In Cisco CallManager Administration on EASTxA, choose **Device > Gateway**.
- Step 12** Choose **Show Endpoints** and click **Find** to list all available gateways.
- Step 13** Click the endpoint with the description **PSTN GW Pod-x** and change the parameter for call classification to **OffNet**.
- Step 14** Click **Update** to save the changes. Choose **Reset Gateway** and click **Reset** to reset the gateway and activate the changes.
- Step 15** In Cisco CallManager Administration on EASTxA, choose **Device > Trunk**.
- Step 16** Click **Find** to list all available trunks. Choose the trunk **ICT**.

- Step 17** Change the parameter for call classification from OnNet to **OffNet**.
- Step 18** Click **Update** to save the changes. Choose **Reset Trunk** and click **Reset** to reset the trunk and activate the changes.
- Step 19** Choose **Route Plan > Route/Hunt > Route Pattern**.
- Step 20** Click **Find** to list all available route patterns. You should find two entries for the route pattern 9.[^0]!#.
- Step 21** Choose route pattern yXXX and verify that the call classification parameter is set to OnNet. If it is not, set it to **OnNet** and click **Update**.

Note By configuring the route pattern yXXX as OnNet but configuring the trunk as OffNet you classify outgoing calls to the other cluster as OnNet and incoming calls from the other cluster as OffNet.

- Step 22** Click **Back to Find/List Route Patterns** to return to the list of route patterns. You should find two entries for the route pattern 9.[^0]!#.
- Step 23** Click the first route pattern 9.[^0]!#. Verify that the call classification parameter is set to OffNet. If it is not, set it to **OffNet** and click **Update**.
- Step 24** Click **Back to Find/List Route Patterns** to return to the list of route patterns.
- Step 25** Click the second route pattern 9.[^0]!#. Verify that the call classification parameter is set to OffNet. If it is not, set it to **OffNet** and click **Update**.
- Step 26** Click **Back to Find/List Route Patterns** to list all route patterns again. Choose route pattern 9.011!# to change it.
- Step 27** Verify that the call classification parameter is set to OffNet. If it is not, set it to **OffNet** and click **Update**.

Note You only configured the call classification for the PSTN route pattern as OffNet to classify outgoing calls to the PSTN as OffNet. You did not configure the call classification on the gateway itself (which would be applicable for incoming calls from the PSTN). The MGCP-controlled FXS port cannot be classified. This does not have any effect because in this lab only calls to the PSTN are placed.

- Step 28** Choose **Service > Service Parameters**.
- Step 29** From the Server drop-down list, choose the first available server. Choose **Cisco CallManager** in the Service drop-down menu.
- Step 30** Press **Ctrl-F** and search for **Block OffNet To OffNet Transfer**.
- Step 31** Change the parameter for Block OffNet To OffNet Transfer from False to **True**.
- Step 32** At the top of the window, click **Update** to save the changes.

Activity Verification

You have completed this task when you attain these results:

- OffNet-to-OnNet call transfers work.

- OffNet-to-OffNet call transfers do not work.
- When you check the Allow Device Override check box for the route pattern yXXX, call transfers to the other pod work.

Specifically, complete these steps:

- Step 33** Place a call from PhoneC-x (x003) to External-Phone-x (using a national number, such as 914085551009#). Press the **Transfer** button on PhoneC-x and try to transfer External-Phone-x to PhoneB-x (x002). The call transfer should work, because it is an OffNet-to-OnNet call.
- Step 34** Place a call from PhoneC-x (x003) to External-Phone-x (using a national number, such as 914085551009#). Press the **Transfer** button on PhoneC-x and try to transfer External-Phone-x to your partner pod to PhoneA-y (y001). The call transfer should work, because it is an OffNet-to-OnNet call.
- Step 35** Ask those in your partner pod to place a call from their PhoneA-y (y001) to your PhoneA-x (x001). Accept the call, press the **Transfer** button on PhoneA-x, and try to transfer PhoneA-y (y001) to External-Phone-x (using a national number, such as 914085551009#). The call transfer should be restricted, because it is an OffNet-to-OffNet call.
- Step 36** In Cisco CallManager Administration on EASTxA, choose **Device > Gateway**. Click **Find** and choose the gateway **GW_GK-x**. Click the endpoint identifier **1/0/0** to open the gateway configuration for the specified module. In gateway configuration, choose **Call Classification** and change the value from OffNet to **OnNet**. Click **Update** to save your changes, and click **Reset Gateway** to reset that gateway.
- Step 37** In Cisco CallManager Administration on EASTxA, choose **Device > Trunk**. Click **Find** to list all available trunks. Choose the trunk **ICT**. Change the parameter for call classification from OnNet to **OffNet**. Click **Update** to save the changes. Choose **Reset Trunk** and click **Reset** to reset the trunk and activate the changes.
- Step 38** Choose **Route Plan > Route/Hunt > Route Pattern**. Click **Find** to list all available route patterns. Choose the first available yXXX router pattern. Check the **Allow Device Override** check box and click **Update** to save your changes.
- Step 39** Ask those in your partner pod to place a call from their PhoneA-y (y001) to your PhoneA-x (x001). Accept the call, press the **Transfer** button on PhoneA-x, and try to transfer PhoneA-y (y001) to External-Phone-x (95551009#). The call transfer should work, because it is an OffNet-to-OnNet call.
- Step 40** Place a call from PhoneC-x (x003) to External-Phone-x (using a national number, such as 914085551009#). Press the **Transfer** button on PhoneC-x and try to transfer External-Phone-x to your partner pod to PhoneA-y (y001). The call transfer should not work anymore, because now it is an OffNet-to-OffNet call.

Note It can take a while until the new configuration is working. If you want to speed up this process, choose **Application > Cisco CallManager Serviceability > Tools > Control Center** and restart the Cisco CallManager service. If you restart the Cisco CallManager service, you have to reset the trunk connections on Cisco CallManager for both EASTxA and EASTyA. Choose **Application > Cisco CallManager Administration > Device > Trunk** and reset the trunk named "ICT." (Ask one of those working in your partner pod to reset the trunk, too.)

- Step 41** In Cisco CallManager Administration on EASTxA, choose **Device > Trunk**. Click **Find** to list all available trunks. Choose the trunk **ICT**. Change the parameter for call classification from OffNet to **OnNet**. Click **Update** to save the changes. Choose **Reset Trunk** and click **Reset** to reset the trunk and activate the changes.

Task 5: Drop Conference Call When Last OnNet Party Leaves

In this task, you will configure conference restrictions. When the last OnNet party leaves the conference, the conference should immediately end. You will set the service parameter for ad hoc conference restrictions to “When No OnNet Parties Remain in the Conference.”

Activity Procedure

Complete these steps:

- Step 1** In Cisco CallManager Administration on EASTxA, choose **Service > Service Parameters**.
- Step 2** From the Server drop-down list, choose the first available server.
- Step 3** Choose **Cisco CallManager** in the Service drop-down menu
- Step 4** Press **Ctrl-F** and search for “Drop Ad Hoc Conference.”
- Step 5** Change the Drop Ad Hoc Conference parameter to **When No OnNet Parties Remain in the Conference**.
- Step 6** At the top of the window, click **Update** to save the changes.

Activity Verification

You have completed this task when you attain this result:

- An ad hoc conference ends when the last OnNet party leaves the conference.

Specifically, complete these steps:

- Step 7** Create a conference where PhoneA-x is the conference creator. Add PhoneC-x, PhoneA-y from the other pod, and External-Phone-x (using a national number, such as 914085551009#) to the conference.
- Step 8** Hang up PhoneA-x. The conference still works.
- Step 9** Hang up PhoneB-x. The conference still works.
- Step 10** Hang up PhoneC-x. The conference ends, because External-Phone-x and PhoneA-y from the other pod both are OffNet devices and no OnNet device is left in the conference.

Lab 1-3 Answer Key: Preventing Toll Fraud

When you complete this activity, your solution will be similar to this, with differences that are specific to your device or workgroup.

Task 1: Restrict Call Forward All and Block Commonly Exploited Area Codes

The configuration for restricting call forwarding and blocking commonly exploited area codes should look similar to these figures.

Configure partitions.

System Route Plan Service Feature Device User Application Help

Cisco CallManager Administration
For Cisco IP Telephony Solutions

Find and List Partitions [Add a New Partition](#)

4 matching record(s) for Partition Name begins with ""

Find Partitions where Partition Name

and show items per page
To list all items, click Find without entering any search text.

Matching record(s) 1 to 4 of 4

<input type="checkbox"/>	Partition Name	Description
<input type="checkbox"/>	Fraud_Prevention	Blocking Partiton for Fraudulent Area...
<input type="checkbox"/>	International	International calling
<input type="checkbox"/>	National_executives	National calling for Executives and M...
<input type="checkbox"/>	National_general	National calling for Generals

Configure calling search spaces.

System Route Plan Service Feature Device User Application Help

Cisco CallManager Administration
For Cisco IP Telephony Solutions

Find and List Calling Search Spaces [Add a New Calling Search Space](#)

4 matching record(s) for CSS Name begins with ""

Find Calling Search Spaces where CSS Name

and show items per page
To list all items, click Find without entering any search text.

Matching record(s) 1 to 4 of 4

<input type="checkbox"/>	CSS Name	Description	Copy
<input type="checkbox"/>	CFA_executives	Call Forwarding for executives and ma...	<input type="button" value="Copy"/>
<input type="checkbox"/>	CFA_general	Call Forwarding for general employees	<input type="button" value="Copy"/>
<input type="checkbox"/>	executives_and_manager	CSS for executives and manager	<input type="button" value="Copy"/>
<input type="checkbox"/>	general	CSS for general employees	<input type="button" value="Copy"/>

Find route patterns.

System Route Plan Service Feature Device User Application Help

Cisco CallManager Administration
For Cisco IP Telephony Solutions

Find and List Route Patterns [Add a New Route Pattern](#)

8 matching record(s) for Pattern begins with ""

Find Route Patterns where begins with

and show items per page
To list all items, click Find without entering any search text.

Matching record(s) 1 to 8 of 8

<input type="checkbox"/>	Route Pattern	Partition	Description	Route Filter	Gateway/Route List	Copy
<input type="checkbox"/>	2XXX		to Pod-2 ove...	ICT		
<input type="checkbox"/>	9.[^0]!#	National_executives	to PSTN		AALN/S1/SU0/0@GW_...	
<input type="checkbox"/>	9.[^0]!#	National_general	to PSTN		AALN/S1/SU0/0@GW_...	
<input type="checkbox"/>	9.011!#	International	to PSTN		AALN/S1/SU0/0@GW_...	
<input type="checkbox"/>	9.1242XXXXXXXX#	Fraud_Prevention	Bahamas		AALN/S1/SU0/0@GW_...	
<input type="checkbox"/>	9.1345XXXXXXXX#	Fraud_Prevention	Cayman Islands		AALN/S1/SU0/0@GW_...	
<input type="checkbox"/>	9.1664XXXXXXXX#	Fraud_Prevention	Montserrat		AALN/S1/SU0/0@GW_...	
<input type="checkbox"/>	9.5551009		to PSTN		AALN/S1/SU0/0@GW_...	

Configure a route pattern to block a commonly exploited area code (Bahamas).

Route Pattern Configuration [Add a New Route Pattern](#)
[Back to Find/List Route Patterns](#)

Route Pattern: 9.1242XXXXXXXX#
Status: Ready
Note: Any update to this Route Pattern automatically resets the associated gateway or Route List

Pattern Definition

Route Pattern*

Partition

Description

Numbering Plan*

Route Filter

MLPP Precedence

Gateway or Route List* (Edit)

Route Option
 Route this pattern
 Block this pattern

Configure a route pattern to block a commonly exploited area code (Cayman Islands).

[Add a New Route Pattern](#)
[Back to Find/List Route Patterns](#)

Route Pattern Configuration

Route Pattern: 9.1345XXXXXX#
Status: Ready
Note: Any update to this Route Pattern automatically resets the associated gateway or Route List

Pattern Definition

Route Pattern*	<input type="text" value="9.1345XXXXXX#"/>
Partition	<input type="text" value="Fraud_Prevention"/>
Description	<input type="text" value="Cayman Islands"/>
Numbering Plan*	<input type="text" value="North American Numbering Plan"/>
Route Filter	<input type="text" value="< None >"/>
MLPP Precedence	<input type="text" value="Default"/>
Gateway or Route List*	<input type="text" value="AALN/S1/SU0/0@GW_GK-1"/> (Edit)
Route Option	<input type="radio"/> Route this pattern <input checked="" type="radio"/> Block this pattern <input type="text" value="Call Rejected"/>

Configure a route pattern to block a commonly exploited area code (Montserrat).

[Add a New Route Pattern](#)
[Back to Find/List Route Patterns](#)

Route Pattern Configuration

Route Pattern: 9.1664XXXXXX#
Status: Ready
Note: Any update to this Route Pattern automatically resets the associated gateway or Route List

Pattern Definition

Route Pattern*	<input type="text" value="9.1664XXXXXX#"/>
Partition	<input type="text" value="Fraud_Prevention"/>
Description	<input type="text" value="Montserrat"/>
Numbering Plan*	<input type="text" value="North American Numbering Plan"/>
Route Filter	<input type="text" value="< None >"/>
MLPP Precedence	<input type="text" value="Default"/>
Gateway or Route List*	<input type="text" value="AALN/S1/SU0/0@GW_GK-1"/> (Edit)
Route Option	<input type="radio"/> Route this pattern <input checked="" type="radio"/> Block this pattern <input type="text" value="Call Rejected"/>

Configure a line for PhoneA-x. (PhoneA-y is similar to this configuration but has a different DN.)

Directory Number: 1001		
Status: Ready		
Note: Any update to this Directory Number automatically resets the associated devices		
<input type="button" value="Update"/>	<input type="button" value="Remove from Device"/>	<input type="button" value="Reset Devices"/>
Directory Number		
Directory Number*	<input type="text" value="1001"/>	
Partition	<input type="text" value=" < None >"/>	
Directory Number Settings		
Voice Mail Profile	<input type="text" value=" < None >"/> (Choose <None> to use default)	
Calling Search Space	<input type="text" value=" executives_and_manager"/>	
AAR Group	<input type="text" value=" < None >"/>	
User Hold Audio Source	<input type="text" value=" < None >"/>	
Network Hold Audio Source	<input type="text" value=" < None >"/>	
Auto Answer	<input type="text" value=" Auto Answer Off"/>	
Call Forward and Pickup Settings		
	Voice Mail	Coverage/ Destination
Forward All	<input type="checkbox"/>	<input type="text" value=" CFA_executives"/>

Configure a line for PhoneB-x. (PhoneB-y is similar to this configuration but has a different DN.)

Directory Number: 1002
 Status: Ready
 Note: Any update to this Directory Number automatically resets the associated devices

Update Remove from Device Reset Devices

Directory Number

Directory Number* 1002
 Partition < None >

Directory Number Settings

Voice Mail Profile < None >
 (Choose <None> to use default)

Calling Search Space executives_and_manager
 AAR Group < None >
 User Hold Audio Source < None >
 Network Hold Audio Source < None >
 Auto Answer Auto Answer Off

Call Forward and Pickup Settings

	Voice Mail	Coverage/ Destination	Calling Search Space
Forward All	<input type="checkbox"/>		CFA_general

Configure a line for PhoneC-x. (PhoneC-y is similar to this configuration but has a different DN.)

Directory Number: 1003
 Status: Ready
 Note: Any update to this Directory Number automatically resets the associated devices

Update Remove from Device Reset Devices

Directory Number

Directory Number* 1003
 Partition < None >

Directory Number Settings

Voice Mail Profile < None >
 (Choose <None> to use default)

Calling Search Space general
 AAR Group < None >
 User Hold Audio Source < None >
 Network Hold Audio Source < None >
 Auto Answer Auto Answer Off

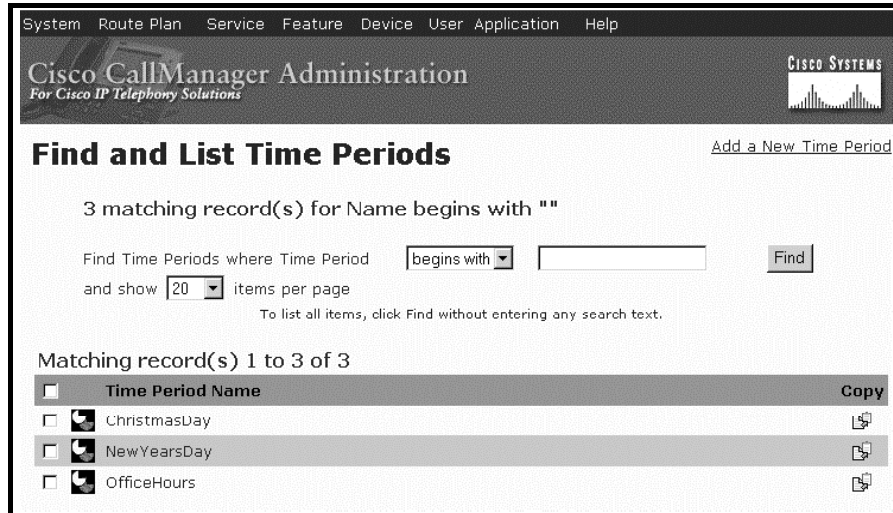
Call Forward and Pickup Settings

	Voice Mail	Coverage/ Destination	Calling Search Space
Forward All	<input type="checkbox"/>		CFA_general

Task 2: Configure Time-of-Day Routing

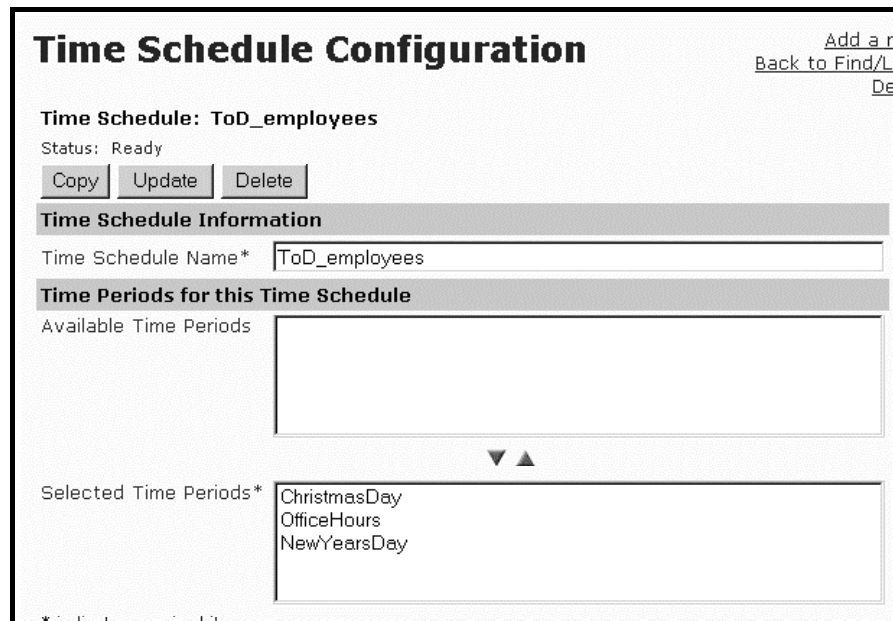
The time-of-day routing configuration should look similar to these figures.

Configure a time period.



The screenshot shows the Cisco CallManager Administration interface. At the top, there is a navigation menu with items: System, Route Plan, Service, Feature, Device, User, Application, and Help. Below the menu is the Cisco CallManager Administration logo and the Cisco Systems logo. The main heading is "Find and List Time Periods" with a link "Add a New Time Period" on the right. The search results show "3 matching record(s) for Name begins with ''". Below this, there is a search filter "Find Time Periods where Time Period begins with" and a "Find" button. A dropdown menu shows "20" items per page. A note says "To list all items, click Find without entering any search text." Below the search results, it says "Matching record(s) 1 to 3 of 3". A table lists three time periods: ChristmasDay, NewYearsDay, and OfficeHours, each with a checkbox and a "Copy" button.

Configure a time schedule.



The screenshot shows the "Time Schedule Configuration" page. At the top right, there are links "Add a r", "Back to Find/L", and "De". The main heading is "Time Schedule Configuration". Below the heading, it says "Time Schedule: ToD_employees" and "Status: Ready". There are three buttons: "Copy", "Update", and "Delete". Below this is a section "Time Schedule Information" with a text field "Time Schedule Name*" containing "ToD_employees". Below that is a section "Time Periods for this Time Schedule". It has two text areas: "Available Time Periods" (empty) and "Selected Time Periods*" containing "ChristmasDay", "OfficeHours", and "NewYearsDay".

Activate the time schedule for the National_general partition.

System Route Plan Service Feature Device User Application Help

Cisco CallManager Administration
For Cisco IP Telephony Solutions

Partition Configuration [Add a New Partition](#)
[Back to Find/List Partitions](#)
[Dependency Relationships](#)

Partition: National_general
Status: Ready

Partition Name*
Description
Time Schedule
Time Zone Originating Device
 Specific Time Zone

Task 3: Use FAC

The FAC configuration should look similar to these figures.

Configure an authorization code.

Forced Authorization Code Configuration [Add a New Code](#)
[Back to Find/List Codes](#)

Forced Authorization Code: 4321

Status :Ready

Forced Authorization Code Information

Authorization Code Name*
Authorization Code*
Authorization Level*
* indicates required item

Configure a route pattern for FAC.

Pattern Definition	
Route Pattern*	9.011#
Partition	International
Description	to PSTN
Numbering Plan*	North American Numbering Plan
Route Filter	< None >
MLPP Precedence	Default
Gateway or Route List*	AALN/S1/SU0/0@GW_GK-1 (Edit)
Route Option	<input checked="" type="radio"/> Route this pattern <input type="radio"/> Block this pattern — Not Selected —
Call Classification*	OffNet <input type="checkbox"/> Allow Device Override
	<input checked="" type="checkbox"/> Provide Outside Dial Tone <input type="checkbox"/> Allow Overlap Sending <input type="checkbox"/> Urgent Priority
	<input checked="" type="checkbox"/> Require Forced Authorization Code
Authorization Level	30

Task 4: Restrict External Transfers

The configuration for restricting external transfers should look similar to these figures.

Classify the trunk.

Trunk Configuration	
System Route Plan Service Feature Device User Application Help Cisco CallManager Administration For Cisco IP Telephony Solutions	
Add a New Trunk Back to Find/List Trunk Dependency Records	
Product: Inter-Cluster Trunk (Gatekeeper Controlled) Device Protocol: Inter-Cluster Trunk Status: Ready <input type="button" value="Update"/> <input type="button" value="Delete"/> <input type="button" value="Reset Trunk"/>	
Device Information	
Device Name*	ICT
Description	ICT to Pod-2
Device Pool*	Default
Call Classification*	OffNet
Media Resource Group List	< None >
Location	Trunk
AAR Group	< None >
Tunneled Protocol	< None >

Configure the service parameter.

Block OffNet To OffNet Transfer*	True	False
----------------------------------	------	-------

Configure device override for route pattern yXXX

System Route Plan Service Feature Device User Application Help

Cisco CallManager Administration
For Cisco IP Telephony Solutions

CISCO SYSTEMS

Route Pattern Configuration

[Add a New Route Pattern](#)
[Back to Find/List Route Patterns](#)

Route Pattern: 2XXX
Status: Ready
Note: Any update to this Route Pattern automatically resets the associated gateway or Route List

Pattern Definition

Route Pattern*

Partition

Description

Numbering Plan*

Route Filter

MLPP Precedence

Gateway or Route List* (Edit)

Route Option
 Route this pattern
 Block this pattern

Call Classification* Allow Device Override

Provide Outside Dial Tone Allow Overlap Sending Urgent Priority

Task 5: Drop Conference Call When Last OnNet Party Leaves

The configuration for dropping conference calls when the last OnNet party leaves the call should look similar to these figures.

Configure the service parameter.

Drop Ad Hoc Conference*

Lab 1-4: Hardening the IP Phone

Complete this lab activity to practice what you learned in the related module.

Activity Objective

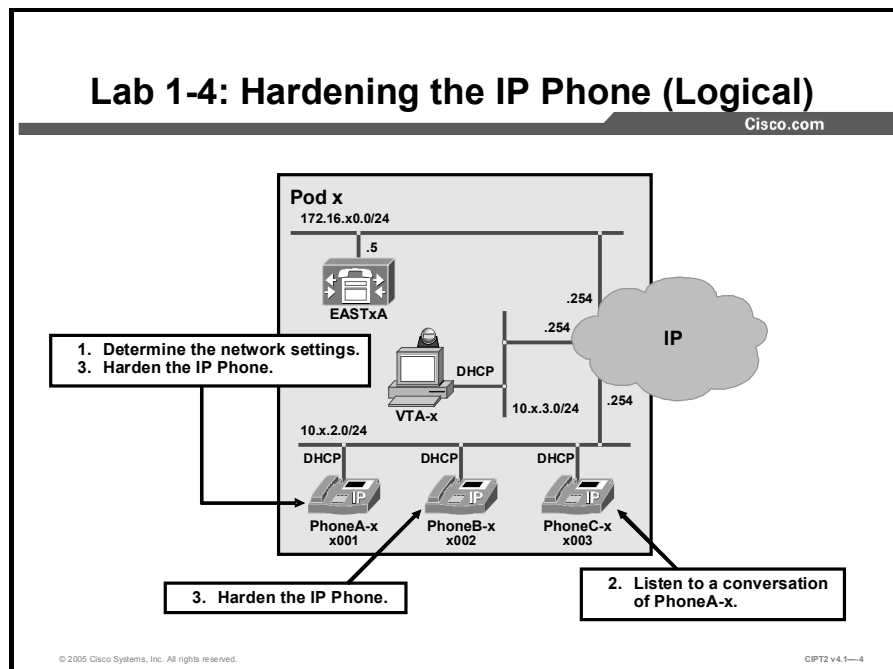
In this activity, you will investigate various attack methods and then harden the Cisco IP Phone. After completing this activity, you will be able to meet these objectives:

- Use the IP Phone Settings button to obtain network configuration information, access the IP Phone over the web, and access the network through the PC port
- Using Ethereal, capture IP telephony packets and convert the packets for playback over the speakers of the computer
- From Cisco CallManager Administration, disable the IP Phone PC port, Settings button, web access, gratuitous ARP, and PC access to the voice VLAN

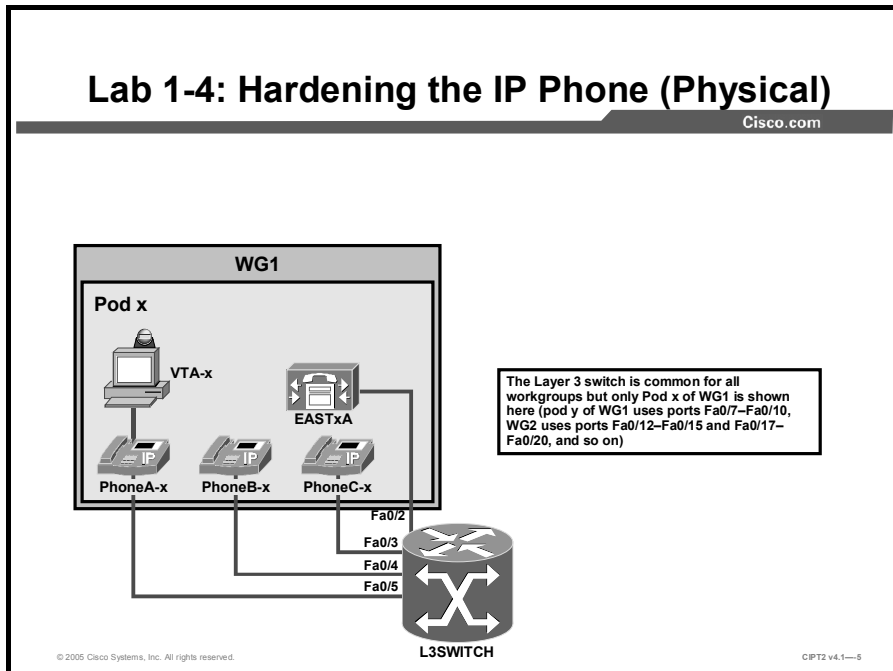
Visual Objective

In this activity, you will determine the current security status of the IP Phones. Then you will harden PhoneA-x and PhoneB-x and connect VTA-x to PhoneA-x. With the installed sniffer on VTA-x, you will be able to play back an audio stream. To test the security features of the PhoneB-x, you will temporarily attach VTA-x to PhoneB-x

The figure illustrates what you will accomplish in this activity.



This figure illustrates how the devices used in this lab are physically connected.



Required Resources

These are the resources and equipment required to complete this activity:

- The lab devices shown in the Visual Objectives figure and detailed in the table

Lab Devices and Their Roles

Device	Device Role in the Activity
EASTxA	Cisco CallManager as a point of administration.
PhoneA-x	IP Phone to be hardened for testing.
PhoneB-x	IP Phone to be hardened for testing.
VTA-x	PC to use for browsing to EASTxA, PhoneA-x, and PhoneB-x. The sniffer Ethereal is preinstalled on VTA-x for playing back an audio stream.

- The device credentials in the table, to log in to the lab devices that require authentication

Credentials for Device Access

Device	Username and Password
EASTxA	administrator lab
Cisco CallManager Administration	ccmadministrator lab
VTA-x	administrator lab

Job Aid

This job aid is available to help you complete the lab activity.

- The table lists the DNs needed to place calls in the lab activity.

Directory Number Allocation Scheme

Device	Directory Number
PhoneA-x	x001, where x = your pod number
PhoneB-x	x002, where x = your pod number
PhoneC-x	x003, where x = your pod number

Task 1: Discover Default Phone Functionality

To discover the IP Phone configuration, you will access its network parameters and also browse its web server. Then you will access the network from the PC connected to the integrated switch in the IP Phone.

Activity Procedure

Complete these steps:

- Step 1** Discover the IP Phone configuration settings:
1. Start discovery of the network settings on PhoneA-x by pressing the **Settings** button on PhoneA-x.
 2. Display the network settings by using the Navigation key to scroll down to **Network Configuration** and pressing **Select**, or press IP Phone key **3**.
- Step 2** Get an overview of the various network parameters by scrolling down in the menu. Find the values needed to build a topology map and fill out the provided table.

IP Phone Network Settings

Network Settings	IP Address
IP address	
DHCP server	
DNS server	
TFTP server	
Default router	
Active Cisco CallManager	
Operational VLAN ID	

- Step 3** Discover the same information without physical access to the PhoneA-x. On PC VTA-x, open a web browser and connect to the IP Phone at the IP address discovered in Step 1. In the browser, enter **http://<IPPhoneIPAddress>**. Determine whether there are any additional parameters that can be retrieved from this information.
- Step 4** Attach VTA-x to PhoneA-x, if it has not been attached. On VTA-x, open a web browser and connect to the active Cisco CallManager of PhoneA-x. Enter **https://172.16.x0.5/CCMAdmin** in the address field of the browser to verify access to the network.

Activity Verification

You have completed this task when you attain these results:

- You have filled out the “IP Phone Network Settings” table after pressing the Settings button of PhoneA-x to discover the network. You verified the information by browsing to the PhoneA-x.
- After connecting VTA-x to the PhoneA-x built-in switch, you were able to browse the Cisco CallManager Administration page.

Task 2: Play Back an IP Telephony Conversation

You will use the Ethereal sniffer, installed on the PC attached to PhoneA-x, to capture a telephone conversation. Then you will extract the real-time data and play back the conversation.

Activity Procedure

Complete these steps:

- Step 1** On VTA-x, launch the Ethereal application and click the **Start a New Live Capture** button, followed by the **OK** button. A new window opens and displays the captured packets in a statistical form.
- Step 2** Place a call from PhoneA-x to another IP Phone, hold a short conversation, and hang up PhoneA-x.
- Step 3** Click **Stop** within Ethereal to terminate the live capture.

- Step 4** Search for RTP packets. If there are none, search the first Skinny message and then the first UDP packet with the negotiated ports in the Skinny messages. Right-click and choose **Decode as**. Decode the packets as **RTP** and click **Apply** to display the relevant UDP packets as RTP data.
- Step 5** Identify the RTP streams by clicking one of the RTP packets, then click **Statistics > RTP > Show All Streams** in the menu. When the new window opens, click the first entry, press and hold the Shift key and click the second entry, and then click **Analyze**.
- Step 6** An RTP stream analysis window opens. Click the **Save Payload** button and enter a filename with the extension .au. Then double-click the newly created file in Windows Explorer, where the file was saved. The Microsoft Windows Media Player will play back the conversation.

Activity Verification

You have completed this task when you attain these results:

- You have successfully captured a conversation and you can see Skinny messages and several UDP messages in the capture.
- The conversation was saved to the hard disk. You used Windows Media Player to play back the previously saved file.

Task 3: Disable Default Phone Settings

In this task, you will harden PhoneA-x and PhoneB-x with different levels of security by disabling unneeded services. With the different levels of security, you will determine the mode of action of a specific parameter. You will use the IP Phone-specific configuration parameters available in Cisco CallManager.

Activity Procedure

Complete these steps:

- Step 1** On PC VTA-x, open a web browser and connect to Cisco CallManager Administration at <https://172.16.x0.5/CCMAdmin>.
- Step 2** Choose **Device > Phone**.
- Step 3** Click **Find** to list all IP Phones. Choose **PhoneA-x**.
- Step 4** Scroll down to **Product Specific Configuration**. Disable these parameters:
- Settings Access
 - Gratuitous ARP
 - PC Voice VLAN Access
 - Web Access
- Step 5** Reset the IP Phone.
- Step 6** Click **Back to Find/List Phones** and choose **PhoneB-x**. Scroll down to **Phone Specific Configuration**. Change these parameters:
- Restrict the Settings access.
 - Disable the PC port.

- Step 7** Reset both IP Phones to activate the new configuration.
- Step 8** On VTA-x, launch the Ethereal application. Start a new capture and make a new call. Then terminate the call and stop the capturing of packets in Ethereal. In Ethereal, search for Skinny messages. You should not find any, because the PC Voice VLAN Access parameter was disabled.
- Step 9** On PhoneA-x, attempt to view the network settings using the Settings button. Describe the difference in the results for PhoneA-x and PhoneB-x and contrast them to your findings in Task 1.
- Step 10** On PC VTA-x, launch a web browser and connect to the web server on PhoneA-x. You should not be able to view the settings because web access has been disabled.
- Step 11** Unplug VTA-x from PhoneA-x and attach VTA-x to PhoneB-x.
- Step 12** On VTA-x, choose **Start > Run**, enter **cmd**, and click **OK**.
- Step 13** In the newly opened window, enter **ipconfig**. You should get the information that the cable is unplugged because the PC port parameter of PhoneB-x has been disabled. After verifying that information, reconnect VTA-x to PhoneA-x.

Activity Verification

You have completed this task when you attain these results:

- You verified in Step 8 that PC voice VLAN access was disabled and in Step 10 that web access was disabled. You verified in Steps 11 to 13 that the PC port on PhoneB-x was disabled and reattached VTA-x to PhoneA-x.
- You have described the differences that you observed in Step 9 when you accessed the Settings menu on PhoneA-x and PhoneB-x.

Lab 1-4 Answer Key: Hardening the IP Phone

When you complete this activity, your solution will be similar to this, with differences that are specific to your device or workgroup.

Task 1: Discover Default Phone Functionality

Your table should include the values in the table.

IP Phone Network Settings

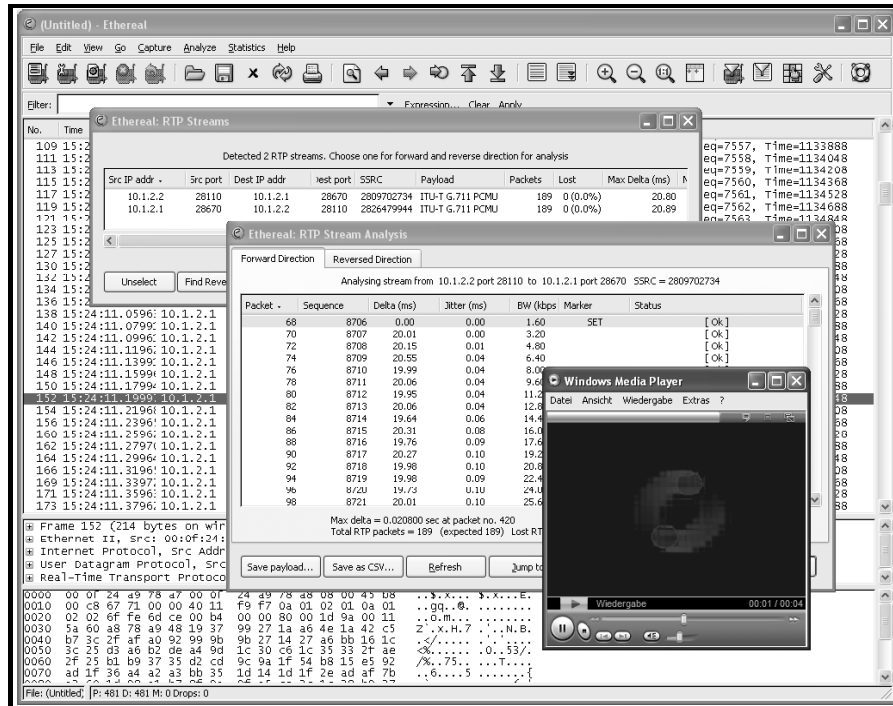
Network Settings	IP Address
IP address	The active IP address of PhoneA-x.
DHCP server	The IP address of the DHCP server that provided the IP configuration for PhoneA-x.
DNS server	The IP address of the DNS server. This field could be empty if the DHCP server did not assign a DNS server.
TFTP server	The IP address of the TFTP server., usually the IP address of EASTxA (172.16.x0.5).
Default router	The IP address of the default router, which needs to be located within the same subnet as PhoneA-x. If all devices of the pod are located within one subnet, this field could be empty.
Active Cisco CallManager	The IP address of EASTxA (172.16.x0.5).
Operational VLAN ID	The VLAN in which PhoneA-x resides.

The web GUI of PhoneA-x should look like this figure.

Cisco Systems		Network Configuration	
		Cisco Systems, Inc. IP Phone CP-7940G (SEP000F24A978A7)	
Device Information	DHCP Server	10.0.2.1	
Network Configuration	BOOTP Server	No	
Network Statistics	MAC Address	000F24A978A7	
Ethernet	Host Name	SEP000F24A978A7	
Port 1 (Network)	Domain Name		
Port 2 (Access)	IP Address	10.1.2.2	
Port 3 (Phone)	Subnet Mask	255.255.255.0	
Device Logs	TFTP Server 1	10.1.1.1	
Debug Display	Default Router 1	10.1.2.254	
Stack Statistics	Default Router 2		
Status Messages	Default Router 3		
Streaming Statistics	Default Router 4		
Stream 1	Default Router 5		
Stream 2	DNS Server 1		
	DNS Server 2		
	DNS Server 3		
	DNS Server 4		
	DNS Server 5		
	Operational VLAN Id	281	
	Admin. VLAN Id		
	CallManager 1	10.1.1.1 Active	
	CallManager 2		
	CallManager 3		
	CallManager 4		
	CallManager 5		
	Information URL		
	Directories URL		
	Messages URL		
	Services URL		
	DHCP Enabled	Yes	
	DHCP Address Released	No	
	Alternate TFTP	No	
	Erase Configuration	NO	
	Forwarding Delay	NO	
	Idle URL		
	Idle URL Time	0	
	Authentication URL	http://10.1.1.1/CCMCIP/authenticate.asp	
	Proxy Server URL		
	PC Port Disabled	NO	
	SW Port Configuration	AUTO	
	PC Port Configuration	AUTO	
	TFTP Server 2		
	User Locale	English_United_States	
	Network Locale	United_States	
	Handset Only Mode	No	
	User Locale Version	4.1(3)	
	Network Locale Version	4.1(3)	
	GARP Enabled	Yes	
	Voice VLAN Enabled	Yes	
	Auto Line Select Enabled	No	
	Video Capability Enabled	No	
	DSCP For Call Control	CS3	
	DSCP For Configuration	CS3	
	DSCP For Services	default	
	Security Mode	Non Secure	
	Web Access	Enabled	
	Connection Monitor Duration	120	
	PC VLAN		

Task 2: Play Back an IP Telephony Conversation

The captured RTP stream should be played back on your system.



Task 3: Disable Default Phone Settings

Your table should contain the values in the table.

IP Phone Settings Button

Configuration	Value
Configuration on PhoneA-x	The Settings button does nothing.
Configuration on PhoneB-x	The Settings button works, but only the contrast and ring type settings are accessible.
Initial configuration (PhoneC-x)	All settings are accessible through the Settings button.

Lab 1-5: Configuring Cisco IP Telephony Authentication and Encryption

Complete this lab activity to practice what you learned in the related module.

Activity Objective

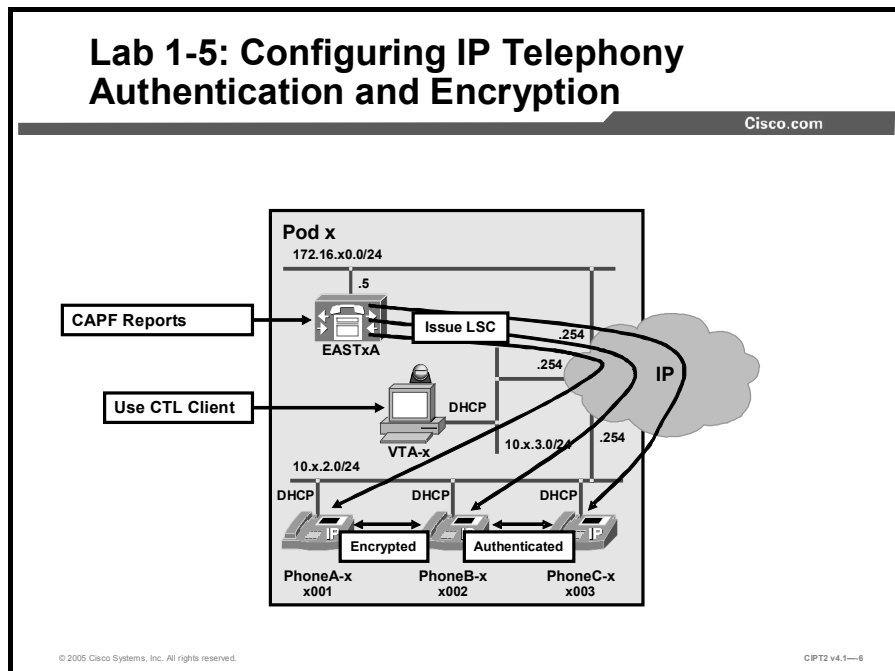
In this activity, you will configure a Cisco CallManager cluster for secure calls by using authentication and encryption on IP Phones supporting these features. After completing this activity, you will be able to meet these objectives:

- Activate Cisco CTL Provider service on each server in the cluster
- Install the Cisco CTL client on an administrator PC
- Configure the Cisco CTL client to set the cluster security mode and create the CTL file
- Use CAPF to install an LSC on three IP Phones of your cluster
- Verify that the LSC is installed on the IP Phone
- Set two IP Phones to encrypted device security mode and a third one to authenticated security mode
- Generate a CAPF report

Visual Objective

You will enable a Cisco CallManager cluster for security by creating a signed CTL, issuing certificates to IP Phones, and installing the certificates on the IP Phones using authentication strings. You will place authenticated and encrypted calls and generate CAPF reports.

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment that are required to complete this activity:

- The lab devices shown in the Visual Objectives figure and detailed in the table

Lab Devices and Their Roles

Device	Device Role in the Activity
EASTxA	Cisco CallManager publisher server
VTA-x	PC used by the administrator to configure the publisher server
PhoneA-x, PhoneB-x, PhoneC-x	IP Phones that will use LSC and place secured calls

- The device credentials in the table, to log in to the lab devices that require authentication

Credentials for Device Access

Device	Username and Password
EASTxA	administrator lab
Cisco CallManager Administration	ccadministrator lab
VTA-x	administrator lab

Job Aids

These job aids are available to help you complete the lab activity.

- The lab devices use the IP address allocation scheme shown in the table.

IP Address Allocation Scheme

Device	IP Address
Voice server network	172.16.x0.0/24
IP Phone network	10.x.2.0/24
Data network	10.x.3.0/24
Default gateway	Node address .254 (for all networks)
EASTxA	172.16.x0.5
GW_GK-x	172.16.x0.200
PhoneA-x	DHCP-assigned (network 10.x.2.0)
PhoneB-x	DHCP-assigned (network 10.x.2.0)
PhoneC-x	DHCP-assigned (network 10.x.2.0)
VTA-x	DHCP-assigned (network 10.x.3.0)

- The table lists the DN's needed to place calls in the lab.

Directory Numbers

Device	Directory Number
PhoneA-x	x001
PhoneB-x	x002
PhoneC-x	x003

Task 1: Activate Services Required for Security

In this task, you will activate the Cisco CTL Provider service on the Cisco CallManager server EASTxA.

Activity Procedure

Complete these steps:

- Step 1** On PC VTA-x, open a web browser and connect to Cisco CallManager Service Configuration at <https://172.16.x0.5/CCMSERVICE/serviceconfig.asp>. When prompted for a username and password, provide the credentials from the “Credentials for Device Access” table located in the Required Resources section of this lab activity. The Cisco CallManager Serviceability Service Activation window appears.
- Step 2** Choose your publisher server (the IP address of EASTxA) from the Servers list in the Service Activation window. A list of the services available for your publisher server appears.
- Step 3** Locate the Cisco CTL Provider service and check that check box.
- Step 4** Locate the Cisco CAPF service and check that check box.
- Step 5** Click **Update** to activate the selected services. Wait until you see an updated window with “Status: Update completed” above the Update button.
- Step 6** Close the Service Activation window.

Activity Verification

You have completed this task when you attain these results:

- Cisco CTL Provider is activated and running on your Cisco CallManager publisher server.
- Cisco CAPF is activated and running on your Cisco CallManager publisher server.

Specifically, complete these steps:

- Step 1** In your browser session to EASTxA, click **Control Center** in the top-right corner of the Cisco CallManager Serviceability window to display the Control Center window. A list of services available at your publisher server is shown on that window.
- Step 2** Locate the Cisco CTL Provider service in the list of services. Verify that the service is activated and running.

- Step 3** Locate the Cisco CAPF service in the list of services. Verify that the service is activated and running.

Task 2: Install the Cisco CTL Client

In this task you will install the Cisco CTL client application on the PC of an administrator (VTA-x).

Activity Procedure

Complete these steps:

- Step 1** Connect to VTA-x. When prompted for a username and password, provide the appropriate credentials from the “Credentials for Device Access” table in the Required Resources section of this lab activity.

Start the Smart Card Service

- Step 2** Choose **Start > Settings > Control Panel > Administrative Tools**. The Administrative Tools window appears.
- Step 3** Double-click **Services** on the list of available administrative tools. The Services window appears.
- Step 4** Locate the **Smart Card** service on the list of available services. Right-click it and choose **Properties**. The Smart Card Properties window appears.
- Step 5** Set the startup type to Automatic and click **Apply**.
- Step 6** Click the **Start** button. Wait until you see an updated window with the message “Service status: Started” above the Start button. Click **OK** and close the Smart Card Properties and Services windows.

Install the Cisco CTL Client Application

- Step 7** Start Internet Explorer from the icon on the Quick Launch toolbar.
- Step 8** Browse to **https://172.16.x0.5/CCMAdmin/Main.asp**. When prompted for a username and password, provide the credentials from the “Credentials for Device Access” table in the Required Resources section of this lab activity. The Cisco CallManager Administration window appears.
- Step 9** Choose **Application > Install Plugins**. The Install Plugins page appears.
- Step 10** Locate the **Cisco CTL Client** plug-in from the list of available plug-ins. Click the icon in front of the plug-in name. A File Download window appears. Click **Open**. The Cisco CTL Client InstallShield Wizard window appears. Click **Next** to proceed with the installation.
- Step 11** After the files have been extracted, the Cisco CTL Client Setup window appears, where you are asked to disable any installed intrusion-detection software. Click **Yes** to proceed.
- Step 12** You see the Welcome window. Click **Next** to view the License Agreement window. Click **I accept the license agreement** and click **Next**.

- Step 13** You are prompted for a destination folder. Keep the default installation folder and click **Next**. The next window informs you that the Smart Card service has to be enabled. Confirm by clicking **Next**.
- Step 14** The software is installed and the installation finishes with a window telling you that the Cisco CTL client has been successfully installed. Click **Finish** to close the window.

Activity Verification

You have completed this task when you attain this result:

- The Cisco CTL client application is installed on the administrator PC (VTA-x).

Specifically, complete this step:

- Step 1** Verify that a shortcut (Cisco CTL Client) to the application has been created on the desktop of VTA-x.

Task 3: Enable Security Using the Cisco CTL Client

In this task, you will use Cisco CTL client to set the cluster to mixed security mode, add security tokens, and sign the CTL.

Activity Procedure

Complete these steps:

- Step 1** Connect to VTA-x. When prompted for a username and password, provide the appropriate credentials from the “Credentials for Device Access” table in the Required Resources section of this lab activity.
- Step 2** Double-click the **Cisco CTL Client** shortcut on the desktop to start the Cisco CTL client application.
- Step 3** In the Cisco CallManager Server window, enter the IP address of your Cisco CallManager publisher server (**172.16.x0.5**). Enter **lab** for the password and click **Next**.
- Step 4** In the Cluster Security Mode window, click **Set CallManager Cluster to Mixed Mode** and click **Next**.
- Step 5** You will be prompted to insert a security token. Insert the first security token into an available USB port on your PC and click **OK**. Wait until you see the Security Token window.
- Step 6** In the Security Token window, click **Add**. The CTL Entries window appears.
- Step 7** In the CTL Entries window, click **Add Tokens**.
- Step 8** You are prompted to insert the second security token into a USB port. Remove the first security token, then insert the second security token into an available USB port on your PC and click **OK**. Wait until you see the Security Token window.
- Step 9** In the Security Token window, click **Add**. The CTL Entries window appears.
- Step 10** Verify that your CTL entries list contains the CAPF, your Cisco CallManager, the Cisco TFTP server, and two security tokens. Click **Finish**.

- Step 11** You will be prompted for a password that allows access to the security token. Enter the default security token password of **Cisco123** (case-sensitive) and click **OK** to allow the CTL client software to sign the CTL file using the currently inserted security token.
- Step 12** When the CTL file has been signed, you see a window that displays the server, file location, and status of the CTL file on your server. A note at the bottom of the window tells you to reload your Cisco CallManager server.
- Step 13** Click **Done** to close the CTL client application.
- Step 14** From the VTA-x PC, start a remote session to the Cisco CallManager server EASTxA using the VNC application. To launch VNC, choose **Start > Programs > RealVNC > VNC Viewer 4 > Run VNC Viewer** or click the icon **VNC Viewer 4** from the Quick Launch toolbar. Enter the IP address of your Cisco CallManager server (EASTxA) and click **OK**. When the connection opens, log in to EASTxA with the credentials shown in the “Credentials for Device Access” table in the Required Resources section.
- Step 15** Choose **Start > Shutdown**, and the Shutdown Windows window appears. Click **Restart** and click **OK**. EASTxA restarts, and your VNC connection is disconnected.

Note Restarting the server will take a few minutes.

Activity Verification

You have completed this task when you attain these results:

- The cluster security mode displayed in the Enterprise Parameters window is 1.
- You verify that the IP Phone has a CTL.

Specifically, complete these steps:

- Step 1** From VTA-x, browse to **https://172.16.x0.5/CCMAdmin/Main.asp**. When prompted for a username and password, provide the credentials from the “Credentials for Device Access” table in the Required Resources section of this lab activity. The Cisco CallManager Administration window appears.
- Step 2** Click **System > Enterprise Parameters**. The Enterprise Parameters window is displayed.
- Step 3** Locate the cluster security mode setting and verify that its value is 1.

Task 4: Generate Phone Certificates with CAPF

In this task, you will generate LSCs using CAPF and install them in the IP Phone.

Activity Procedure

Complete these steps:

- Step 1** From VTA-x, browse to **https://172.16.x0.5/CCMAdmin/Main.asp**. When prompted for a username and password, provide the credentials from the “Credentials for Device Access” table in the Required Resources section of this lab activity. The Cisco CallManager Administration window appears.

Configuring Cisco CallManager CAPF for Issuing LSC to the IP Phones

- Step 2** Choose **Device > Phone**. The Find and List Phones window is displayed.
- Step 3** Click **Find**. All IP Phones known to the system are displayed.
- Step 4** Click **PhoneA-x**. The Phone Configuration window is displayed.
- Step 5** Locate the CAPF Information area.
- Step 6** Set the Certificate Operation field to **Install/Upgrade**.
- Step 7** Ensure that the Authentication Mode field is set to By Authentication String.
- Step 8** Click **Generate String**. The Authentication String field is populated with an automatically generated authentication string.
- Step 9** Write down the authentication string for PhoneA-x at the corresponding field under Step 14.
- Step 10** Locate the Product Specific Configuration area.
- Step 11** Set the Settings Access field to **Enabled** if it is not already configured this way.

Note The Settings Access field has to be set to Enabled to allow the installation of an LSC on an IP Phone when using manual authentication (by authentication strings). If settings access was not fully enabled (if the field was set to Restricted or Disabled), it should be set back to the previously configured value after the installation of the LSC has finished. In the lab environment, this step is omitted, and settings access will remain (fully) enabled for the rest of the lab activity.

- Step 12** Click **Update** at the top of the window, and reset the IP Phone by clicking **Reset Phone, Reset, and OK**.
- Step 13** Repeat Steps 2 through 12 for PhoneB-x and PhoneC-x.
- Step 14** Ensure that you wrote down the authentication strings of all three IP Phones here:

PhoneA-x authentication string: _____

PhoneB-x authentication string: _____

PhoneC-x authentication string: _____

Installing LSC on the IP Phones

- Step 15** On PhoneA-x, press **Settings** to access the Settings menu.
- Step 16** Scroll to the Security Configuration option and press the **Select** softkey.
- Step 17** Unlock the IP Phone configuration by pressing ****#**.
- Step 18** Scroll to LSC and press the **Update** softkey. You are prompted to enter the authentication string.
- Step 19** At the Authentication String prompt, enter the authentication key for the IP Phone (from Step 14 of this task) and press the **Submit** softkey. Be patient while the IP Phone generates its RSA keys and requests a certificate signed by the CAPF. When

the signed certificate is installed, you will see the message “Success” at the lower-left corner of the IP Phone display.

Step 20 Click the **Exit** softkey to return to the main Settings menu, and click the **Exit** softkey again to return to the normal IP Phone display.

Step 21 Repeat Steps 15 through 20 for the two other IP Phones.

Activity Verification

You have completed this task when you attain this result:

- All three IP Phones of your cluster have successfully received a certificate.

Specifically, complete these steps:

Step 1 On EASTxA, in Cisco CallManager Administration, choose **Device > Phone**. The Find and List Phones window is displayed.

Step 2 Populate the fields of the Find and List Phones window to find IP Phones where the LSC status is Upgrade Success and click **Find**. The result should list all three IP Phones in your cluster.

Note Further verification of this task is done during Task 5.

Task 5: Verify That an LSC Is Installed

In this task, you will verify that the LSC is installed on the IP Phones.

Activity Procedure

Complete these steps:

Step 1 On PhoneA-x, press the **Settings** button to view the Settings menu.

Step 2 Scroll to the Security Configuration option and press the **Select** softkey. The Security Configuration menu appears.

Step 3 Locate the LSC entry and verify that it displays the status Installed.

Step 4 Repeat Steps 1 through 3 for PhoneB-x and PhoneC-x.

Activity Verification

You have completed this task when you attain this result:

- You verify that all three IP Phones of your cluster have an LSC installed.

Note The verification steps of this task have been the steps of the activity procedure.

Task 6: Configure the Device Security Mode

In this task, you will configure the device security mode of the IP Phones to support authenticated calls or encrypted calls.

Activity Procedure

Complete these steps:

- Step 1** From VTA-x, browse to **https://172.16.x0.5/CCMAdmin/Main.asp**. When prompted for a username and password, provide the credentials from the “Credentials for Device Access” table in the Required Resources section of this lab activity. The Cisco CallManager Administration window appears.
- Step 2** Choose **Devices > Phones** and display the Phone Configuration window for **PhoneA-x**.
- Step 3** Locate the Device Security Mode parameter and set it to **Encrypted**.
- Step 4** Click **Update** at the top of the window, and reset the IP Phone by clicking **Reset Phone, Reset**, and **OK**.
- Step 5** Repeat Steps 2 through 4 for PhoneB-x.
- Step 6** Repeat Steps 2 through 4 for PhoneC-x, but in Step 3, set the Device Security Mode parameter to **Authenticated**.

Activity Verification

You have completed this task when you attain these results:

- The device security mode for PhoneA-x and PhoneB-x is set to Encrypted, and the device security mode for PhoneC-x is set to Authenticated.
- When you place calls between PhoneA-x and PhoneB-x, the call is encrypted.
- When you place calls between PhoneA-x or PhoneB-x and PhoneC-x, the call is authenticated.
- When you create a conference call with PhoneA-x, PhoneB-x, and PhoneC-x, the call is not secured.

Specifically, complete these steps:

- Step 1** From VTA-x, browse to **https://172.16.x0.5/CCMAdmin/Main.asp**. When prompted for a username and password, provide the credentials from the “Credentials for Device Access” table in the Required Resources section of this lab activity. The Cisco CallManager Administration window appears.
- Step 2** Choose **Device > Phone**. The Find and List Phones window is displayed.
- Step 3** Populate the fields of the Find and List Phones window to find IP Phones where the Device Security Mode field is not empty and click **Find**. The result should list all three IP Phones in your cluster, including the information about their device security mode setting. Verify that the device security mode of PhoneA-x and PhoneB-x is Encrypted, while the device security mode of PhoneC-x is Authenticated.
- Step 4** Place calls between PhoneA-x and PhoneB-x. During a call, the IP Phones should show the Encryption symbol (a closed lock) on their displays.
- Step 5** Place calls between PhoneA-x or PhoneB-x and PhoneC-x. The two IP Phones in the call should show the Authentication symbol (a shield) on their displays.
- Step 6** Establish a conference with all three IP Phones of your cluster.

Task 7: Create a CAPF Report

In this task, you will create a CAPF report listing all IP Phones that successfully installed or upgraded an LSC.

Activity Procedure

Complete these steps:

- Step 1** From VTA-x, browse to **https://172.16.x0.5/CCMAdmin/Main.asp**. When prompted for a username and password, provide the credentials from the “Credentials for Device Access” table in the Required Resources section of this lab activity. The Cisco CallManager Administration window appears.
- Step 2** Choose **Device > Device Settings > CAPF Report**. The CAPF Report window is displayed.
- Step 3** Populate the fields of the CAPF Report window to find IP Phones where the Certificate Operation Status field is set to Upgrade Success, and click **Find**. All IP Phones of your cluster should be displayed.
- Step 4** Click **View Report in File**. A popup window asks you to open or save the generated report file.
- Step 5** Click **Save** and store the file on the Windows desktop.
- Step 6** Double-click the file on the desktop. It opens so that you can view the content.

Activity Verification

You have completed this task when you attain this result:

- You created a report, saved it to the desktop, and then viewed the content of the saved file.

Note The verification steps of this task have been part of the activity procedure.

Lab 1-5 Answer Key: Configuring Cisco IP Telephony Authentication and Encryption

When you complete this activity, your solution will be similar to this, with differences that are specific to your device or workgroup.

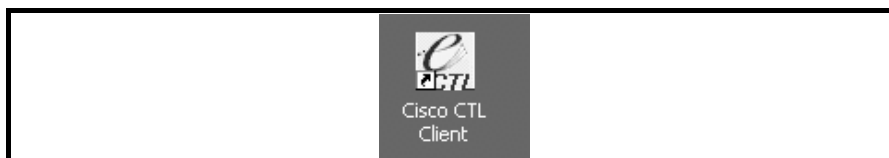
Task 1: Activate Services Required for Security

When you are viewing the Cisco CallManager services from the Control Center, your screen should look like this figure.

Service Name	Status	Activation Status
NT Service		
<input type="radio"/> Cisco CallManager	▶	Activated
<input type="radio"/> Cisco Tftp	▶	Activated
<input type="radio"/> Cisco Messaging Interface	■	Deactivated
<input type="radio"/> Cisco IP Voice Media Streaming App	▶	Activated
<input type="radio"/> Cisco CTIManager	■	Deactivated
<input type="radio"/> Cisco Telephony Call Dispatcher	■	Deactivated
<input type="radio"/> Cisco MOH Audio Translator	■	Deactivated
<input type="radio"/> Cisco RIS Data Collector	▶	Activated
<input type="radio"/> Cisco Database Layer Monitor	▶	Activated
<input type="radio"/> Cisco CDR Insert	■	Deactivated
<input type="radio"/> Cisco Extended Functions	■	Deactivated
<input type="radio"/> Cisco Serviceability Reporter	▶	Activated
<input type="radio"/> Cisco CTL Provider	▶	Activated
<input type="radio"/> Cisco Certificate Authority Proxy Function	▶	Activated

Task 2: Install the Cisco CTL Client

After you have installed the Cisco CTL client you should see a shortcut on your desktop.

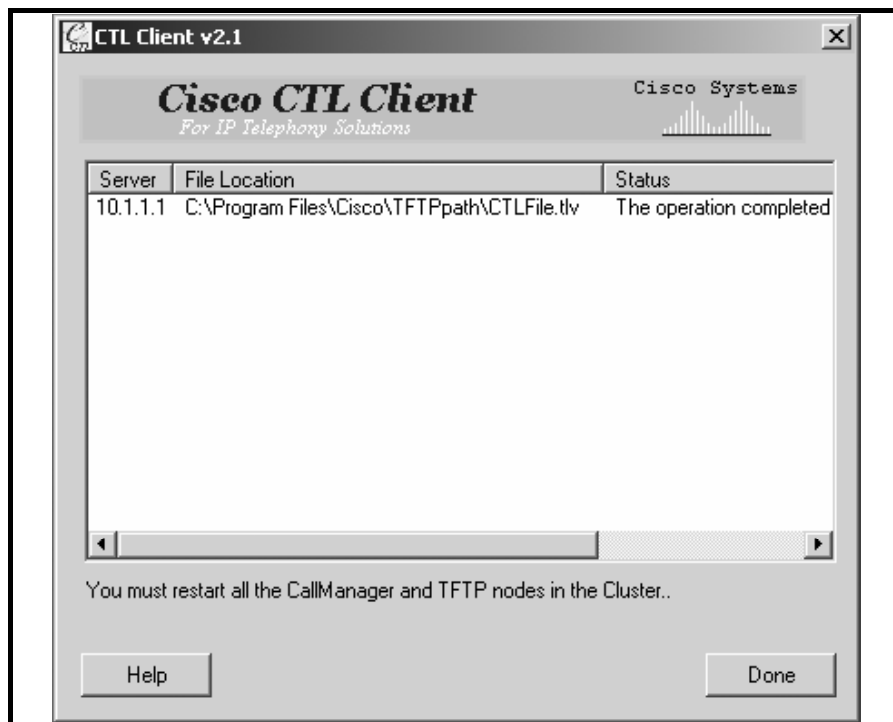


Task 3: Enable Security Using the Cisco CTL Client

After adding both security tokens, your list of CTL entries should look like this figure.

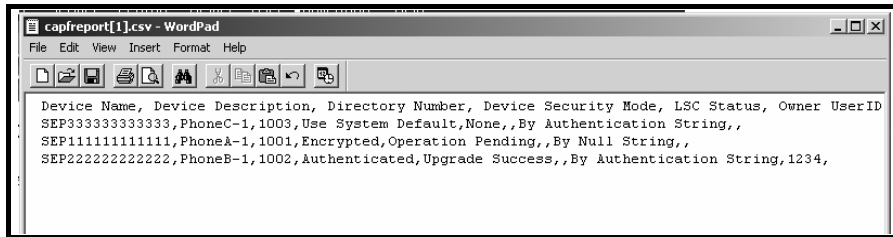


After signing the CTL, you should see a window similar to this figure.



Task 7: Create a CAPF Report

When you open a CAPF report saved in CSV file format and you view it in an editor, it should look similar to this figure.



Lab 2-1: Enabling Cisco VT Advantage

Complete this lab activity to practice what you learned in the related module.

Activity Objective

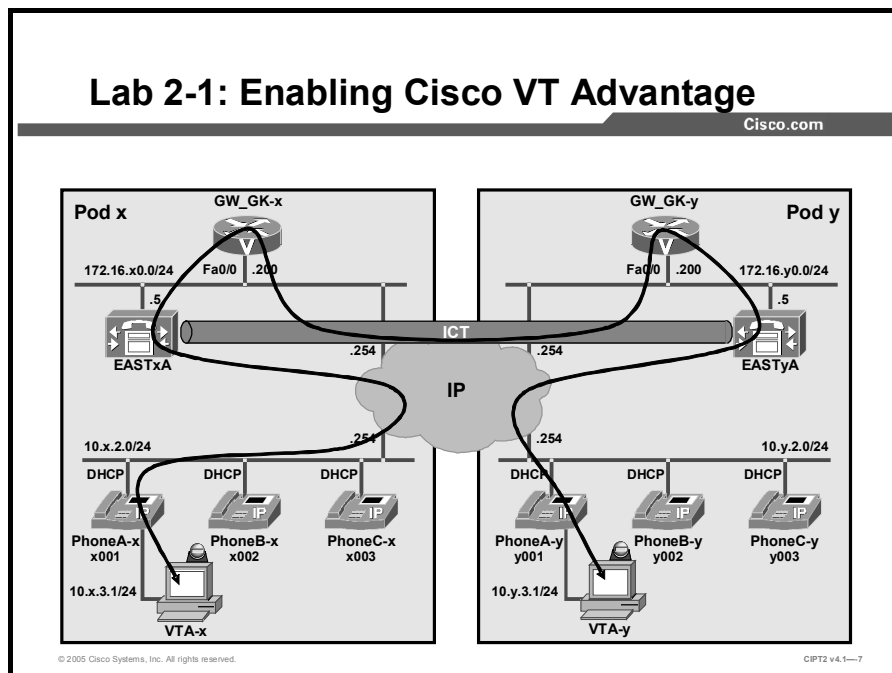
In this activity, you will use Cisco VT Advantage to make video telephony calls. After completing this activity, you will be able to meet these objectives:

- Enable video capabilities on Cisco IP Phones
- Deploy the Cisco VT Advantage installer program on the Cisco CallManager publisher
- Install Cisco VT Advantage
- Check Cisco VT Advantage connections and video signal quality
- Configure call admission control in a centralized deployment using the locations and regions feature of Cisco CallManager
- Configure call admission control using a Cisco IOS gatekeeper

Visual Objective

In this activity, you will install the Cisco VT Advantage software, configure a gatekeeper-controlled intercluster trunk, configure bandwidth management, and make video calls over the intercluster trunk.

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment that are required to complete this activity:

- The lab devices shown in the Visual Objectives figure and detailed in the table

Lab Devices and Their Roles

Device	Device Role in the Activity
EASTxA	Cisco CallManager publisher that serves the IP Phones
VTA-x	PC where the Cisco VT Advantage software has to be installed
PhoneA-x	Video-enabled IP Phone that has PC with Cisco VT Advantage connected to it
PhoneB-x, PhoneC-x	IP Phones

- The device credentials in the table, to log in to the lab devices that require authentication

Credentials for Device Access

Device	Username and Password
EASTxA	administrator lab
Cisco CallManager Administration	ccadministrator lab
VTA-x	administrator lab
VTA user on EASTxA	CARuser lab123
GW_GK-x login enable	lab lab

Job Aids

These job aids are available to help you complete the lab activity.

- The table lists the DNs needed to place calls in the lab activity.

Directory Numbers

Device	Directory Number
PhoneA-x	x001, where x = your pod number
PhoneB-x	x002, where x = your pod number
PhoneC-x	x003, where x = your pod number
PhoneA-y	y001, where y = your partner pod number
PhoneB-y	y002, where y = your partner pod number
PhoneC-y	y003, where y = your partner pod number

- The lab devices use the IP address allocation scheme shown in the table.

IP Address Allocation Scheme

Device	IP Address
Voice server network	172.16.x0.0/24
IP Phone network	10.x.2.0/24
Data network	10.x.3.0/24
Default gateway	Node address .254 (for all networks)
EASTxA	172.16.x0.5
GW_GK-x	172.16.x0.200
PhoneA-x	DHCP-assigned (network 10.x.2.0)
PhoneB-x	DHCP-assigned (network 10.x.2.0)
PhoneC-x	DHCP-assigned (network 10.x.2.0)
VTA-x	DHCP-assigned (network 10.x.3.0)

Task 1: Enable Video Capabilities

In this task, you will enable the IP Phones to support video calls when connected to an appropriately equipped PC. You will enable the video capabilities of PhoneA-x.

Activity Procedure

Complete these steps:

- Step 1** From VTA-x use Internet Explorer to access Cisco CallManager administration on EASTxA, choose **Device > Phone**. The Find and List Phones window displays. Click **Find** to list all the IP Phones in your cluster if none are visible.
- Step 2** Click the IP Phone with the description **PhoneA-x**. The Phone Configuration window displays.
- Step 3** Scroll down to the bottom of the Phone Configuration window and in the Video Capabilities drop-down menu, choose **Enabled**.
- Step 4** Verify that the PC port is enabled.

- Step 5** Click **Update** at the top of the window. Click **OK** to confirm the changes that you made, and reset the IP Phone by clicking **Reset Phone** and **Reset**. Finally, click **OK** to confirm the reset.

Activity Verification

You have completed this task when you attain this result:

- You verify that PhoneA-x shows the video camera icon on its display.

Task 2: Deploy the Cisco VT Advantage Installer Program

In this task, you will make the Cisco VT Advantage Installer program available on the Cisco CallManager publisher EASTxA so that users can install Cisco VT Advantage on their PCs. The deployment tool is stored in the software folder on the desktop of the Cisco CallManager publisher.

Activity Procedure

Complete these steps:

- Step 1** From VTA-x connect to EASTxA using VNC. On the Cisco CallManager publisher (EASTxA), double-click the installer named **cvta-DeployMan_1-0-2.exe** (which can be found in the software folder on the desktop) to set up deployment of Cisco VT Advantage. The DeployMan main window is displayed.
- Step 2** In the DeployMan main window, click **Use Defaults** to use the default values for the DeployMan tool. The default settings assume that the tool is running on the Cisco CallManager publisher. Further, the default values use the default VTAinstall.exe destination and the default update URL. Click **OK**.
- Step 3** The Choose Host Name dialog box appears. Choose the IP address of the Cisco CallManager publisher server from the drop-down menu. This value populates the Update URL field for the AutoUpdate feature. Click **OK**.

These fields are automatically filled in with default values:

- Cisco VT Advantage Version
 - CVTAInstall.exe Destination
 - Update URL
 - Comma-delimited e-mail and FTP addresses
- Step 4** Click **OK** twice at the Success window. The Cisco VT Advantage install plug-in is now available.
- Step 5** Choose **User > Add a New User** in Cisco CallManager Administration.
- Step 6** Enter **VTAuser** as the user ID, **lab123** as the password, fill out the other relevant fields, and click **Insert**.

Activity Verification

You have completed this task when you attain this result:

- Cisco VT Advantage software is available on the CCMUser page.

Specifically, complete these steps:

- Step 1** From VTA-x, open a web browser and browse to the Cisco CallManager Client Install Plugins website at <https://172.16.x0.5/CCMUser>. Log in using **VTAuser** as the user ID and **lab123** as the password.
- Step 2** Choose **Download/Install Plugins** and verify that the Cisco VT Advantage plug-in is listed.

Task 3: Install Cisco VT Advantage

In this task, you will install Cisco VT Advantage on the client PC.

Note	Before you install Cisco VT Advantage, the Cisco IP Phone must be connected to the network and video must be enabled on the IP Phone (the camera icon displayed on the IP Phone).
-------------	---

You will download the Cisco VT Advantage software from the Cisco CallManager Client Install Plugins website at <http://172.16.x0.5/CCMUser/downloads.asp> and install it on the PC VTA-x.

Activity Procedure

Complete these steps:

- Step 1** Ensure that the camera is not yet plugged into a USB port. Do not plug it in until requested to do so.
- Step 2** Log in to VTA-x and browse to the Cisco CallManager Client Install Plugins website (which can be accessed at <http://172.16.x0.5/CCMUser>).
- Step 3** On the Cisco CallManager Client Install Plugins website, click the **Cisco VTA Installer Plugin** icon.
- Step 4** Click **Save** in the File Download window, and save the executable to desktop of your PC.
- Step 5** Access the VTA-x desktop and double-click **CVTAInstaller.exe** to start the installer.
- Step 6** After the Cisco VT Advantage Installer program starts, click **Next** in the Welcome window.
- Step 7** In the License Agreement window showing a disclaimer, choose **I Accept the terms in the license agreement** and click **Next**.
- Step 8** In the Customer Information window, accept the default parameters and click **Next**.
- Step 9** In the Destination Folder window, accept the default installation folder path and click **Next**.
- Step 10** In the Ready to Install Program window, click **Install**.
- Step 11** Depending on the setup of your PC, you might see messages for installation of Cisco Media Termination Driver and the Cisco VT Camera software.

Note If the Cisco VT Advantage software is already installed, remove all components before you install the VT Advantage software again.

- Step 12** If a Hardware Installation dialog box appears, click **Continue Anyway**.
- Step 13** Plug the Cisco VT Camera USB cable into an available USB port on the PC when prompted to do so.
- Step 14** In the Shortcut Options window, review and choose all options, and then click **Next**.

The displayed options are as follows:

- Automatically start Cisco VT Advantage on startup
- Create Cisco VT Advantage shortcut on the desktop
- Create a Cisco VT Advantage shortcut on the Quick Launch bar

- Step 15** In the InstallShield Wizard Complete window, click **Finish**.

Activity Verification

You have completed this task when you attain this result:

- You can start the Cisco VT Advantage program on the VTA-x PC.

Specifically, complete these steps:

- Step 1** The Cisco VT Advantage program can be started from the shortcut icon, from the desktop icon, from the Quick Launch toolbar, or by choosing **Start > Programs > Cisco VT Advantage > Cisco VT Advantage**.
- Step 2** When you have successfully started Cisco VT Advantage, close the window.

Task 4: Check the Cisco VT Advantage Connections and Video Signal Quality

In this task, you will use tools built into Cisco VT Advantage to check connectivity to the IP Phone and verify good signal quality.

Activity Procedure

Complete these steps:

- Step 1** Connect to VTA-x. Right-click the **Cisco VT Advantage** icon in the system tray of your PC and choose **Open Cisco VT Advantage**.
- Step 2** Choose **Video > Start Video Check** and start the video check tool.
- Step 3** After starting the video check, you should see two windows with the same image. One window is the local view and the other one is the remote view.
- Step 4** Check the local and remote video signal indicators. The strongest possible signal is when the bar is solid green. The poorest signal quality is when the bar is solid gray.
- Step 5** To stop the video check, click **Video > Stop Video Check**.

- Step 6** Disconnect the Ethernet cable connected at the back of the PC (or at the access port on the back of the IP Phone). In the Cisco VT Advantage main window, observe that the connecting line to the IP Phone displays a red X.
- Step 7** Plug the Ethernet cable back in. It takes a few moments for the connecting line to turn green again.

Activity Verification

You have completed this task if all tests during the activity procedure succeeded. No specific verifications are needed.

Task 5: Configure Call Admission Control Using Locations and Regions

In this task, you will configure locations and regions to enable call admission control for video calls. The gatekeeper-controlled intercluster trunk is already set up. The trunk uses the location and region “Gateways.” All other devices are in the location “Devices” and the region “Default.” The trunk is configured for voice calls only, because video has not been implemented yet. Your task is to enable call admission control for video calls between the two clusters. The gatekeeper does not have call admission control configured and will not be used in this task.

Activity Procedure

Complete these steps:

- Step 1** From VTA-x use Internet Explorer to access Cisco CallManager administration on EASTxA and choose **System > Region**.
- Step 2** Choose the **Default** region and click **Find**. In the configuration window for this region, choose voice codec **G.711** and a per-call video bandwidth of **384 kbps** for Default Region (within this region). Click **Update** and restart the associated devices.
- Step 3** In Cisco CallManager Administration, choose **System > Location**.
- Step 4** Choose the **Trunk** location in the configuration window of this location and verify that **Unlimited** is selected in the Audio Bandwidth field. In the Video Bandwidth field, enter **384 kbps** to limit the bandwidth used by video calls that are placed to the intercluster trunk to this value. Click **Update** and reset the associated devices.
- Step 5** Click **Back to Find/List Locations** and verify that the Devices location has unlimited bandwidth for voice and video calls.

Activity Verification

You have completed this task when you attain this result:

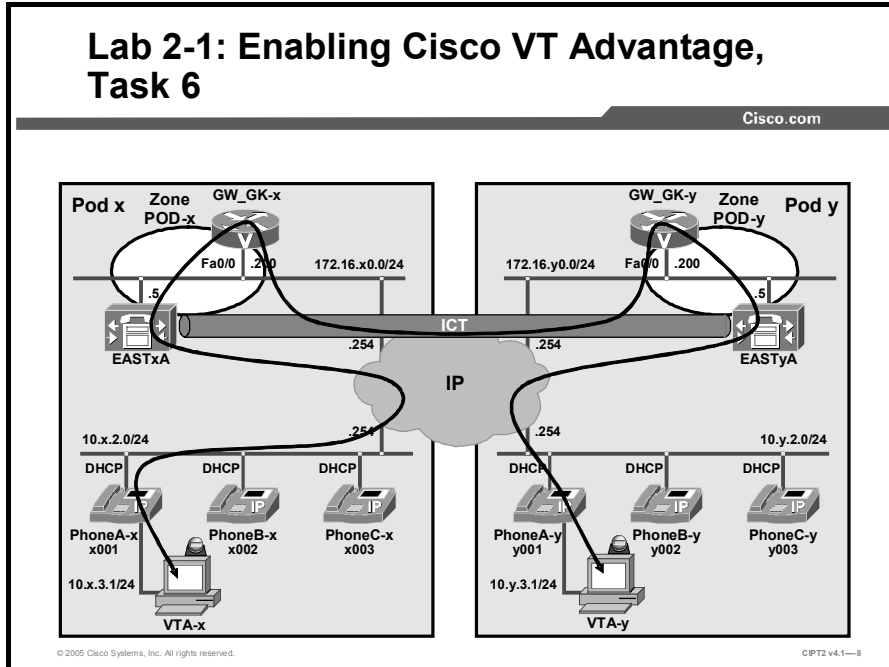
- You have made a successful video call.

Specifically, complete these steps:

- Step 1** Make sure that the other pod is successfully configured as well.
- Step 2** Place a call from PhoneA-1 to PhoneB-1 and vice versa and verify that video is successfully transferred.

Task 6: Configure Call Admission Control Using a Gatekeeper

In this task, you will use a gatekeeper to enable call admission control. The gatekeeper is already set up but is not configured for bandwidth management. The video calls already work between the two clusters. Your task is to enable bandwidth management on the gatekeeper to control the voice and video calls between the two clusters, as illustrated in the figure.



The gatekeeper zones are as shown in the diagram.

- GW_GK-x has a local zone POD-x containing the local Cisco CallManager EASTxA.
- GW_GK-x has a remote zone POD-y containing the remote Cisco CallManager EASTyA.

Activity Procedure

Complete these steps:

- Step 1** Log in to the gatekeeper GW_GK-x and change to enable mode by entering **enable**.
- Step 2** Go to global configuration mode by entering **configure terminal**.
- Step 3** Go to gatekeeper configuration mode by entering **gatekeeper**.
- Step 4** Configure the gatekeeper to allow a maximum of 768 kbps for calls between your local zone and the remote zone by entering **bandwidth interzone zone POD-x 768**.
- Step 5** Configure the gatekeeper to allow a maximum of 768 kbps for calls within your local zone by entering **bandwidth total zone POD-x 768**.
- Step 6** Configure the gatekeeper to allow a maximum of 768 kbps per single call by entering **bandwidth session zone POD-x 768**.

Note The total bandwidth and the session bandwidth do not apply in the actual lab environment, because these settings affect only calls being placed within the local zone. In the lab, however, only interzone calls are placed.

Note The gatekeeper considers twice the video or audio call bandwidth for its calculation. Therefore, this configuration effectively means that during an active video call with a bandwidth of 384 kbps, there is no bandwidth left for any other calls (of any type, including audio-only calls) between the two zones. For audio calls with a G.711 codec, the maximum number of calls allowed between the two zones is six ($6 * 2 * 64 = 768$).

Activity Verification

You have completed this task when you attain these results:

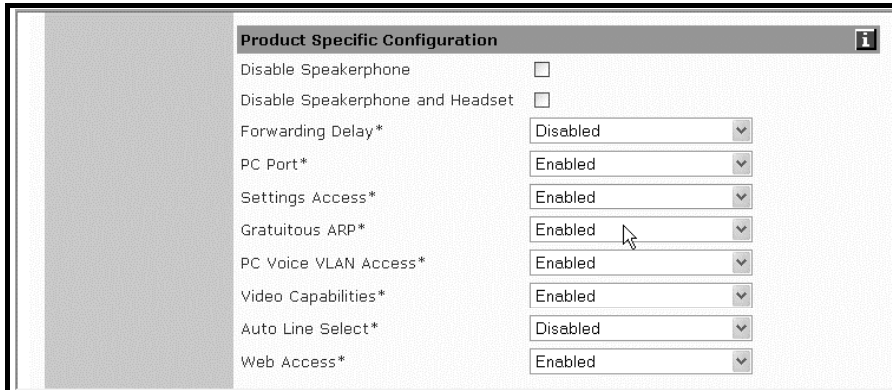
- You have placed a video call from PhoneA-x, with Cisco VT Advantage connected, to PhoneA-y and vice versa.
- You have left the video call active and made a voice call from PhoneB-x to PhoneB-y. This call gets a busy signal because of insufficient bandwidth.
- You have displayed the properties of the active calls with the **show gatekeeper calls** command.
- You have used the **debug h225 asn1** command to verify the call admission control process on the gatekeeper in detail.

Lab 2-1 Answer Key: Enabling Cisco VT Advantage

When you complete this activity, your solution will be similar to this, with differences that are specific to your device or workgroup.

Task 1: Enable Video Capabilities

The Product Specific Configuration window settings of PhoneA-x should look similar to this figure.



The PhoneA-x display should show the camera icon.



Task 2: Deploy the Cisco VT Advantage Installer Program

The Cisco VT Advantage installer should be available from the Cisco CallManager Client Install Plugins website.



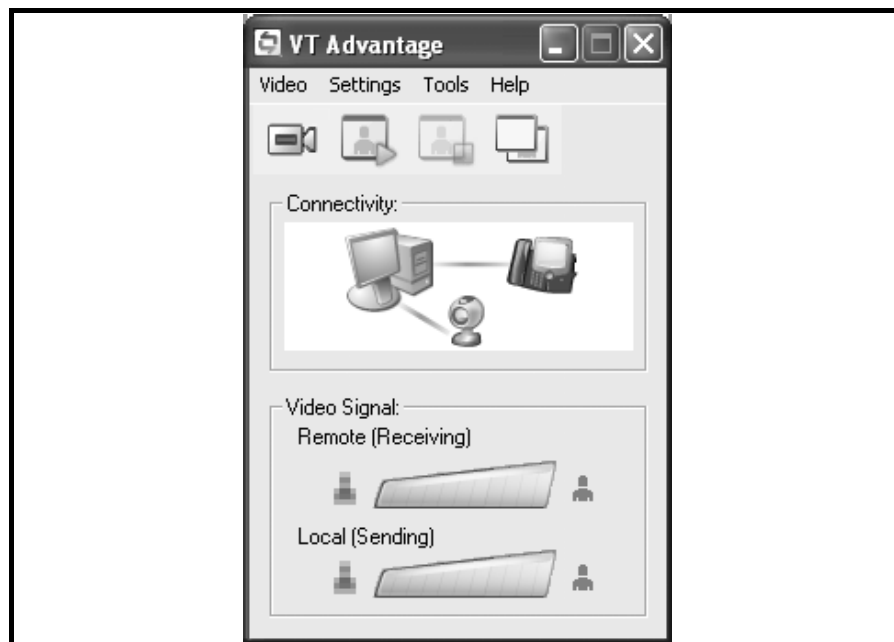
Cisco CallManager Client Install Plugins

The following software applications are available for download.

Plugin Name	Description
 Cisco VT Advantage	Cisco VT Advantage is a video telephony solution comprising the Cisco VT Advantage software application and Cisco VT Camera, a video telephony USB camera. The Cisco VT Advantage software application is installed on a PC connected directly to a Cisco IP Phone. With the Cisco VT Camera attached to a PC co-located with a Cisco IP Phone, the user can place and receive video calls on their enterprise IP telephony network.

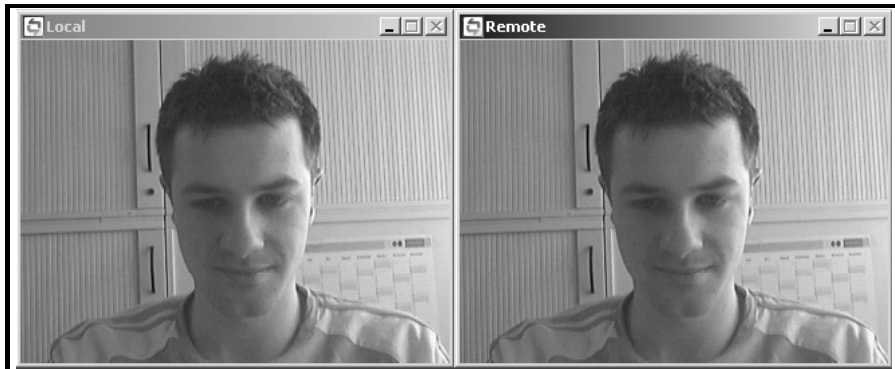
Task 3: Install Cisco VT Advantage

The Cisco VT Advantage application should be available on VTA-x.

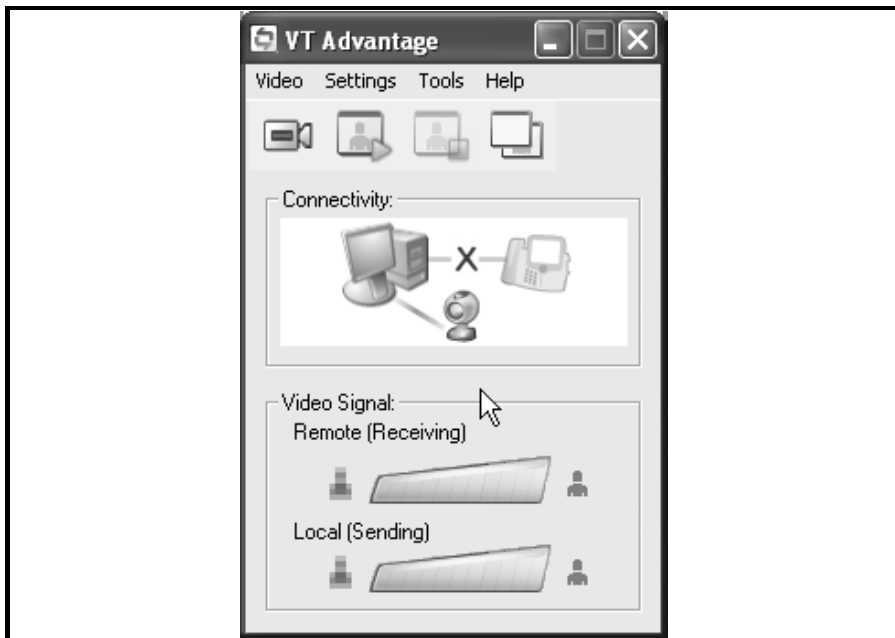


Task 4: Check the Cisco VT Advantage Connections and Video Signal Quality

The video check should show the local camera picture in both windows.

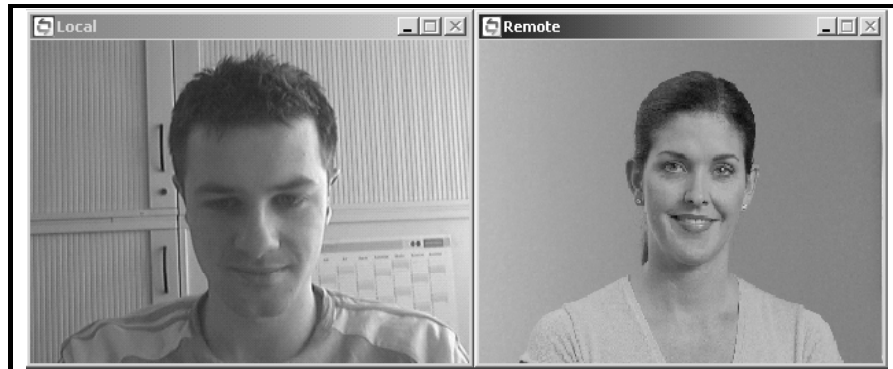


As long as the Ethernet cable of VTA-x is disconnected, the telephone symbol on Cisco VT Advantage should be dimmed.



Task 5: Configure Call Admission Control Using Locations and Regions

The video call should be established successfully.



Task 6: Configure Call Admission Control Using a Gatekeeper

After configuring the gatekeeper to restrict the bandwidth between the two zones, the gatekeeper configuration should look similar to this output (GW_GK-1 is used in the example):

■ GW_GK-1

```
gatekeeper
zone local POD-1 lab.com
zone remote POD-2 lab.com 172.16.20.200 1719
zone subnet POD-1 172.16.10.0/24 enable
no zone subnet POD-1 0.0.0.0/0 enable
zone prefix POD-1 1...
zone prefix POD-2 2...
gw-type-prefix 1#* default-technology
bandwidth interzone zone POD-1 786
bandwidth total zone POD-1 786
bandwidth session zone POD-1 786
no shutdown
```

Note Only the highlighted commands have to be entered during the lab activity. The rest of the commands were preconfigured, because the gatekeeper was already in use (without any bandwidth limitations) before this task.

Lab 3-1: Monitoring Performance

Complete this lab activity to practice what you learned in the related module.

Activity Objective

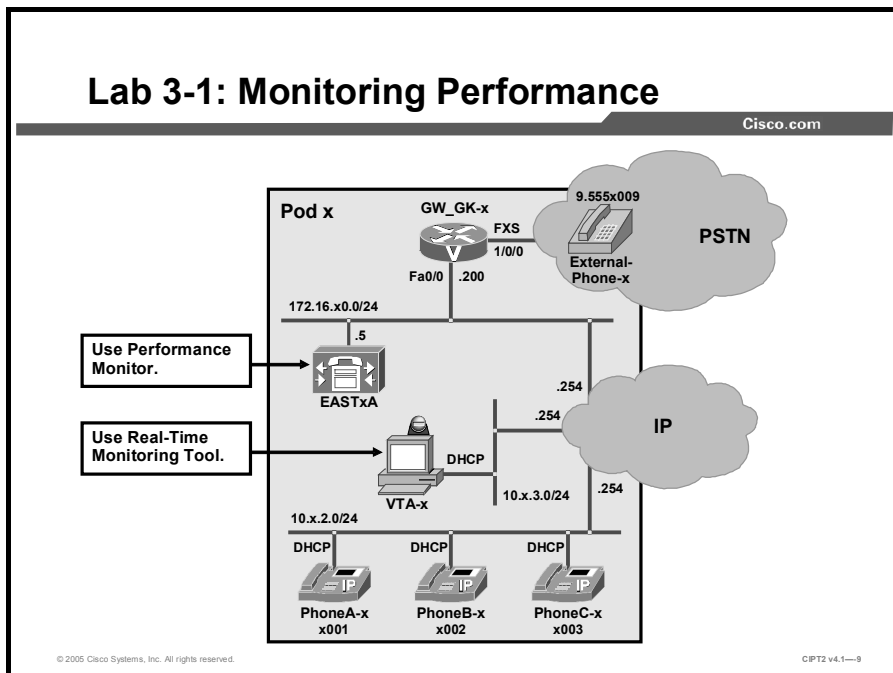
In this activity, you will use Microsoft Performance Monitor and RTMT to monitor, analyze and classify Cisco CallManager activities and system load. After completing this activity, you will be able to meet these objectives:

- Use Microsoft Performance Monitor to monitor calls and the Cisco CallManager heartbeat
- Download the RTMT client-side plug-in from the Cisco CallManager Install Plugins web page and install it
- Log in to RTMT
- Use RTMT to monitor devices, call activities, servers, and services
- Create custom configuration profiles in RTMT

Visual Objective

In this activity, you will become familiar with Cisco CallManager monitoring. You will make VoIP and PSTN calls and monitor the calls using the performance monitor and the real-time monitoring tool.

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and lab devices that are required to complete this activity:

- The lab devices shown in the Visual Objectives figure and detailed in the table

Lab Devices and Their Roles

Device	Device Role in the Activity
EASTxA	Cisco CallManager publisher that serves the IP Phones
GW_GK-x	H.323 gateway
PhoneA-x, PhoneB-x, PhoneC-x	IP Phones
External-Phone-x	PSTN telephone

- The device credentials in the table, to log in to the lab devices that require authentication

Credentials for Device Access

Device	Username and Password
EASTxA	administrator lab
Cisco CallManager Administration	ccadministrator lab
VTA-x	administrator lab

Job Aids

These job aids are available to help you complete the lab activity.

- The table lists the DNs needed to place calls in the lab.

Directory Numbers

Device	Directory Number
PhoneA-x	x001, where x = your pod number
PhoneB-x	x002, where x = your pod number
PhoneC-x	x003, where x = your pod number
PhoneA-y	y001, where y = your partner pod number
PhoneB-y	y002, where y = your partner pod number
PhoneC-y	y003, where y = your partner pod number

- The lab devices use the IP address allocation scheme shown in the table.

IP Address Allocation Scheme

Device	IP Address
Voice server network	172.16.x0.0/24
IP Phone network	10.x.2.0/24
Data network	10.x.3.0/24
Default gateway	Node address .254 (for all networks)
EASTxA	172.16.x0.5
GW_GK-x	172.16.x0.200
PhoneA-x	DHCP-assigned (network 10.x.2.0)
PhoneB-x	DHCP-assigned (network 10.x.2.0)
PhoneC-x	DHCP-assigned (network 10.x.2.0)
VTA-x	DHCP-assigned (network 10.x.3.0)

- Additionally, you will use *Cisco CallManager Administration Guide, Release 4.1(3)*.

Task 1: Use Microsoft Performance Monitor

In this task, you will use the Microsoft Performance Monitor to monitor calls and system heartbeat on your Cisco CallManager server. Therefore, you will monitor the total the processor time, active calls, active FSX port, and some extra counters in Microsoft Performance Monitor.

Activity Procedure

Complete these steps:

- Step 1** From VTA-x use Internet Explorer to access Cisco CallManager administration on EASTxA and choose **Start > Settings > Control Panel > Administrative Tools** and choose **Performance** to launch Microsoft Performance Monitor.
- Step 2** Click the Plus (+) icon in Microsoft Performance Monitor to launch the Add Counters window.
- Step 3** Leave every selection at the default and choose **Add** to add the total system processor time.
- Step 4** From the Performance Object drop-down menu, choose **Cisco CallManager** and click **Add** to add Cisco CallManager active calls.
- Step 5** From **Select Counters from List**, choose **FSXPortsActive** and click **Add** to add Cisco CallManager active FSX ports.
- Step 6** Add some extra counters.
- Step 7** Click **Close** to close the Add Counters window.
- Step 8** Place a few calls among any three IP Phones and the PSTN telephone.

- Step 9** On Cisco CallManager, in Microsoft Performance Monitor, toggle statistics views by pressing **Ctrl-G**, **Ctrl-B**, and **Ctrl-R** to see the differences among them and the responses to your calls.

Activity Verification

You have completed this task when you attain this result:

- You have observed the counters collected by Performance Monitor that reflect the calls placed.

Task 2: Download and Install RTMT Client

In this task, you will download the RTMT client plug-in from the Cisco CallManager Install Plugins web page and install it on the VTA-x PC.

Activity Procedure

Complete these steps:

- Step 1** From your VTA-x PC, use Internet Explorer to access the Cisco CallManager Administration window at **https://172.16.x0.5/ccmadmin**.
- Step 2** Log in to Cisco CallManager Administration.
- Step 3** Choose **Application > Install Plugins**
- Step 4** Choose **Cisco CallManager Real-Time Monitoring Tool**
- Step 5** Choose **Open** and accept all defaults to install RTMT locally on the VTA-x PC.

Activity Verification

You have completed this task when you attain this result:

- You verify that RTMT is installed successfully.

Specifically, complete this step:

- Step 1** On Cisco CallManager, choose **Start > Programs > Cisco CallManager Serviceability** and verify that RTMT is available.

Task 3: Log In to RTMT

In this task, you will start RTMT and log in to it.

Activity Procedure

Complete these steps:

- Step 1** Launch RTMT on the VTA-x PC.
- Step 2** Verify that the IP address in the Host IP Addr. field of the login window is the address of your Cisco CallManager. If not, change it to the correct address.
- Step 3** Enter **CCMAdministrator** as the username and **lab** as the password.
- Step 4** Verify that the Port field is set to **443** and that **Secure Connection** is selected.

- Step 5** Press **OK** to access RTMT.
- Step 6** If a dialog box asks about a certificate, click **Yes**.
- Step 7** If a Mail Server Configuration window opens, click **Cancel** to proceed without mail configuration.

View the RTMT Default Configuration

You will evaluate the default configuration of RTMT.

- Step 8** Choose **CM-Default** in the Select Configuration window of RTMT and click **OK** to launch RTMT using the default configuration. The summary view should appear.

Activity Verification

You have completed this task when you attain this result:

- The active Summary tab displays real-time information.

Task 4: Use RTMT

In this task, you will use RTMT to monitor devices, call activities, servers, and services. You will add the same counters to the Performance tab that you added to Microsoft Performance Monitor, use the Summary tab, place some calls, and perform a device search for IP Phones. Last, you will examine other available tabs.

Activity Procedure

Complete these steps:

- Step 1** On VTA-x, in RTMT, choose **Performance > Open Performance Monitoring** to open the Performance tab at the bottom left of the window.
- Step 2** Expand the folder named with the IP address of your Cisco CallManager into the white pane, and expand **Processor**.
- Step 3** Double-click **% Processor Time**, choose **_Total**, and click **Add** to add the total processor time to the Performance tab.
- Step 4** Expand **Cisco CallManager** and double-click **CallsActive** and **FSXPortsActive** to add those counters.
- Step 5** Choose **Monitor > Cluster Summary** to view the Summary tab.
- Step 6** Place several calls between your IP Phones and view the statistics on both tabs.
- Step 7** Choose **Device > Open Device Search** to open the Device Search tab.
- Step 8** Double-click **Phone** in the white pane to launch the search selection window.
- Step 9** Follow the instructions and choose **Finish**, which should cause a list of all registered IP Phones to be displayed.
- Step 10** Explore RTMT by starting and examining other tabs, such as CPU&Memory.

Activity Verification

You have completed this task when you attain these results:

- Several tabs are open on the tab bar of RTMT.
- The tabs include the suggested content.

Specifically, complete these steps:

- Step 1** Verify that the Performance tab includes graphs for processor time, active calls, and active FSX ports.
- Step 2** Verify that the Summary tab shows real-time graphs related to Cisco CallManager activities.
- Step 3** Verify that the Device Search tab lists all registered IP Phones.
- Step 4** Verify that there are additional tabs available from the tab bar.

Task 5: Create RTMT Profiles

In this task, you will create your own custom configuration profile in RTMT that is based on the configuration that you created in Task 4.

Activity Procedure

Complete these steps:

- Step 1** On VTA-x, in RTMT, press **Ctrl-Alt-P** or choose **System > Profile** to launch the Preferences window.
- Step 2** Click **Save**.
- Step 3** Enter a name and description for your configuration and click **OK** to save your configuration as a new profile.

Activity Verification

You have completed this task when you attain this result:

- You verify that the profile was saved successfully

Specifically, complete these steps:

- Step 1** Press **Ctrl-Alt-P** or choose **System > Profile**, choose **CM-Default**, and click **Restore** to use the CM-Default profile again.
- Step 2** Press **Ctrl-Alt-P** or choose **System > Profile**, choose your custom profile, and click **Restore** to recreate the configuration profile that you used at the end of Task 4.

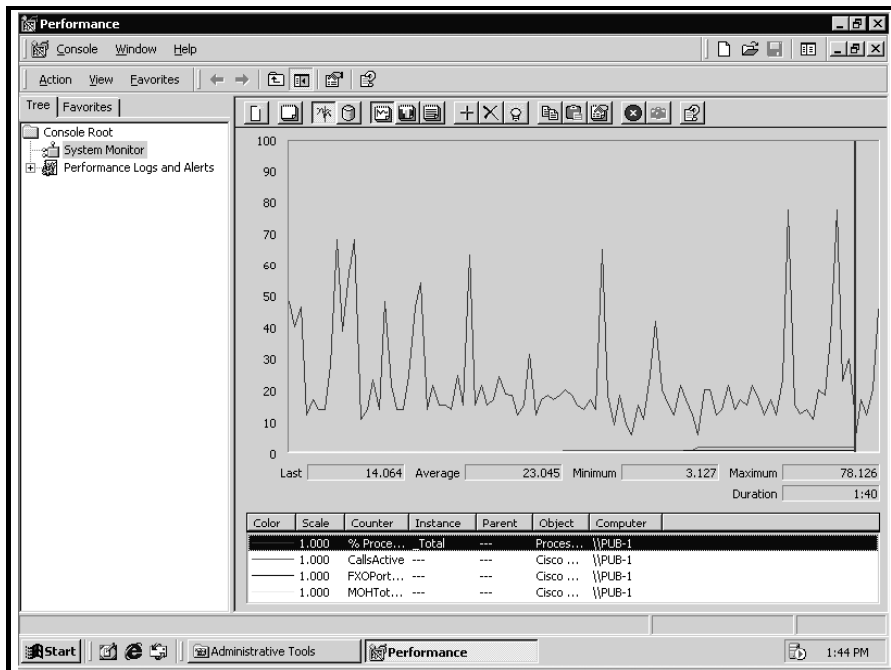
Lab 3-1 Answer Key: Monitoring Performance

When you complete this activity, your solution will be similar to this, with differences that are specific to your device or workgroup.

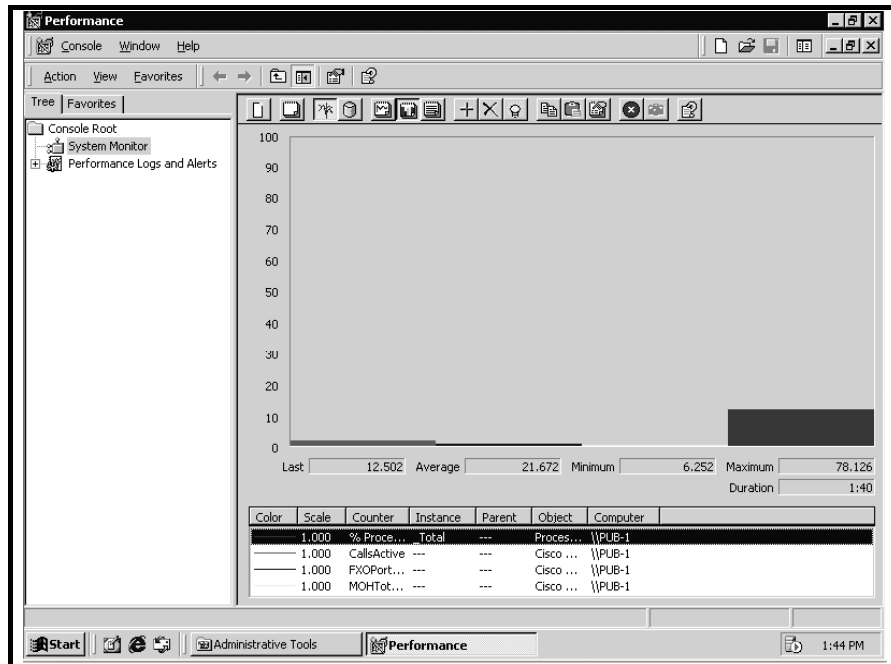
Task 1: Use Microsoft Performance Monitor

The Performance window should look similar to these figures:

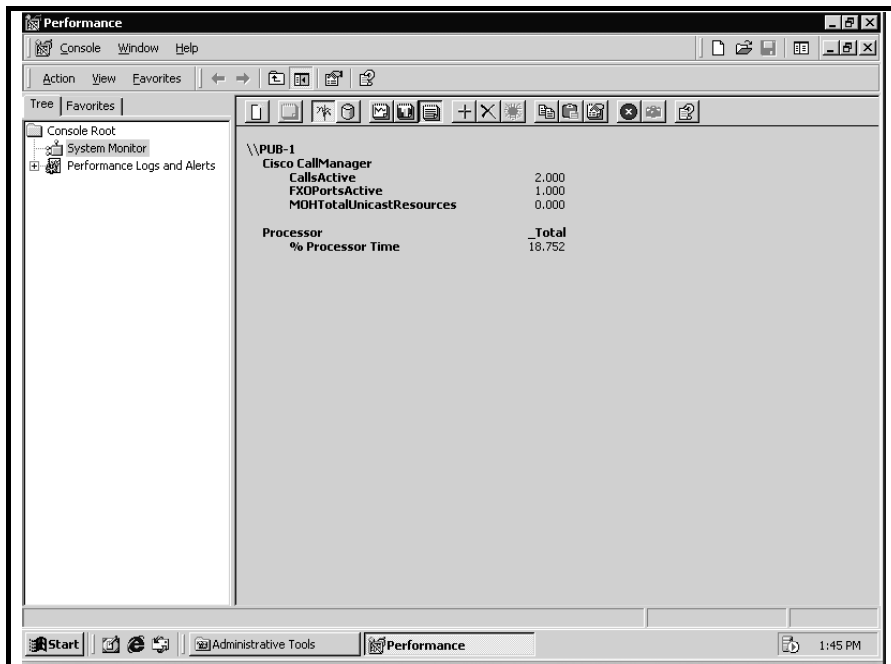
- Graph view



■ Histogram view

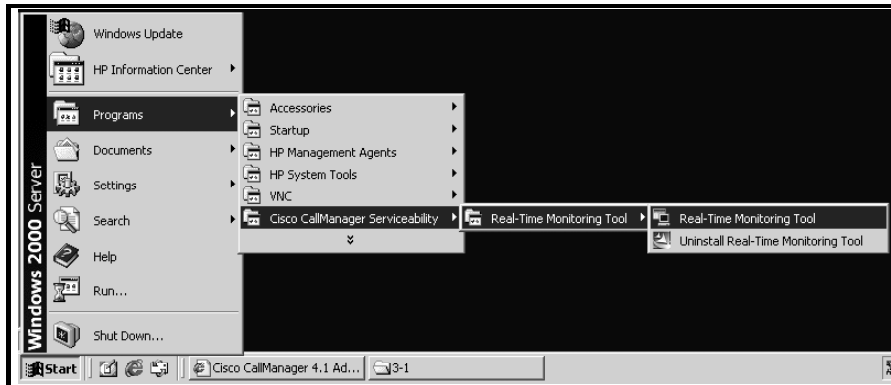


■ Report view



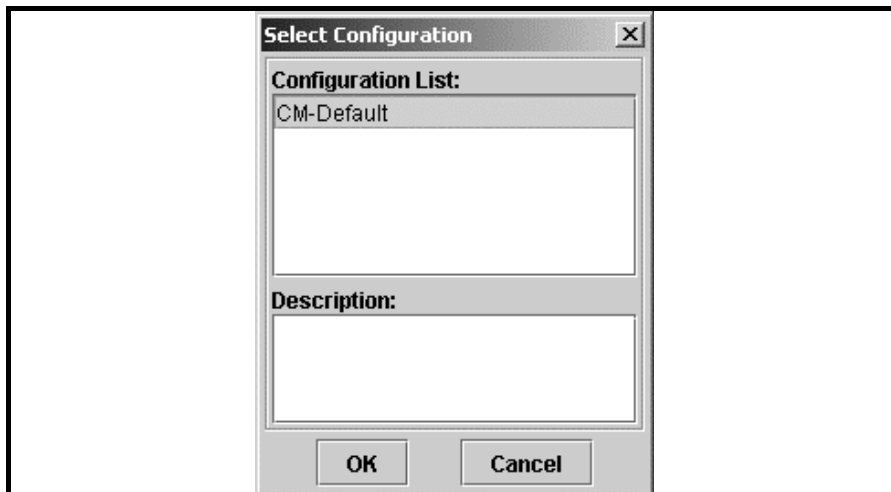
Task 2: Download and Install RTMT Client

RTMT should be installed.



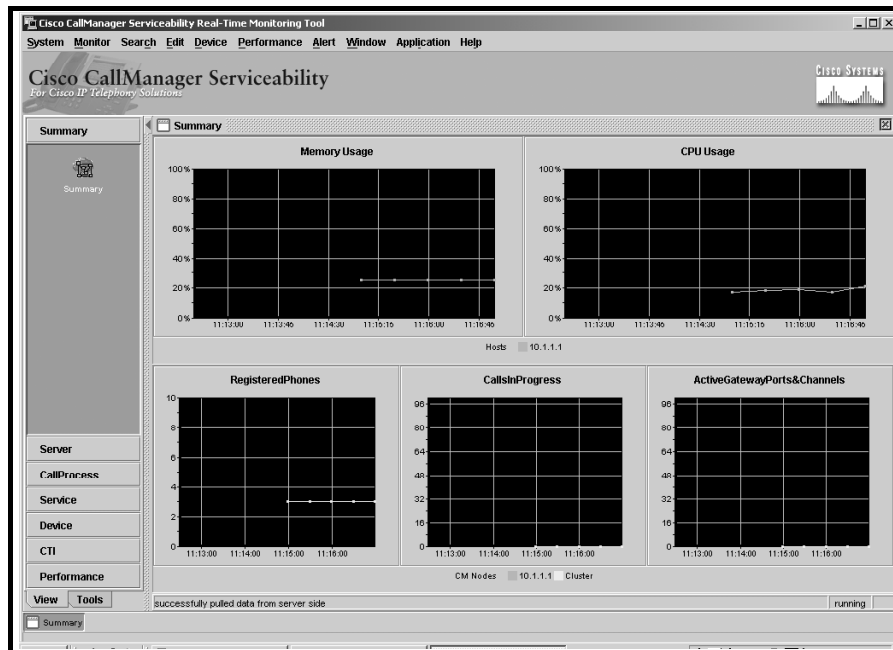
Task 3: Log In to RTMT

After you successfully log in to RTMT, the Select Configuration window should open.



View RTMT Default Configuration

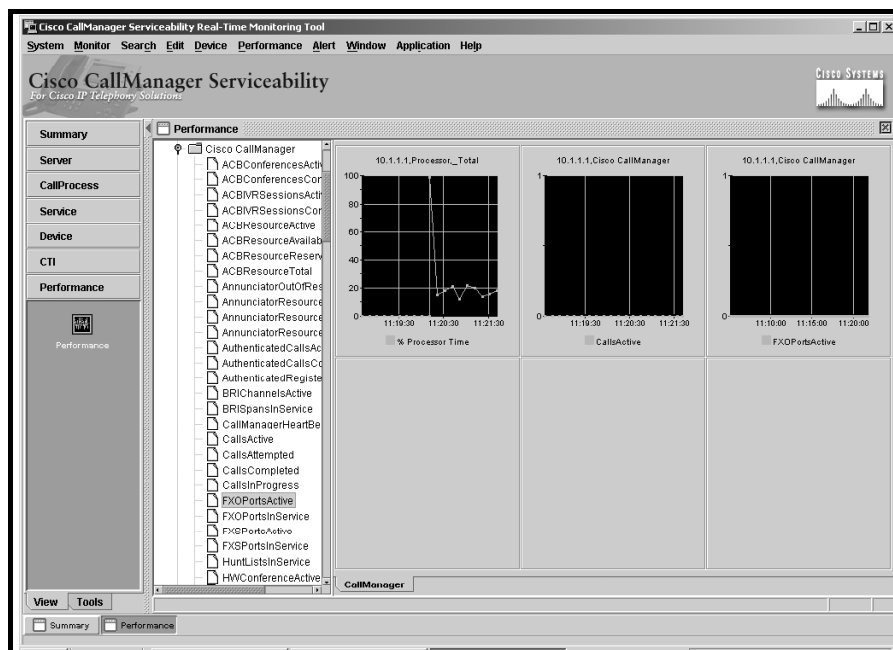
The Summary tab should look similar to this figure.



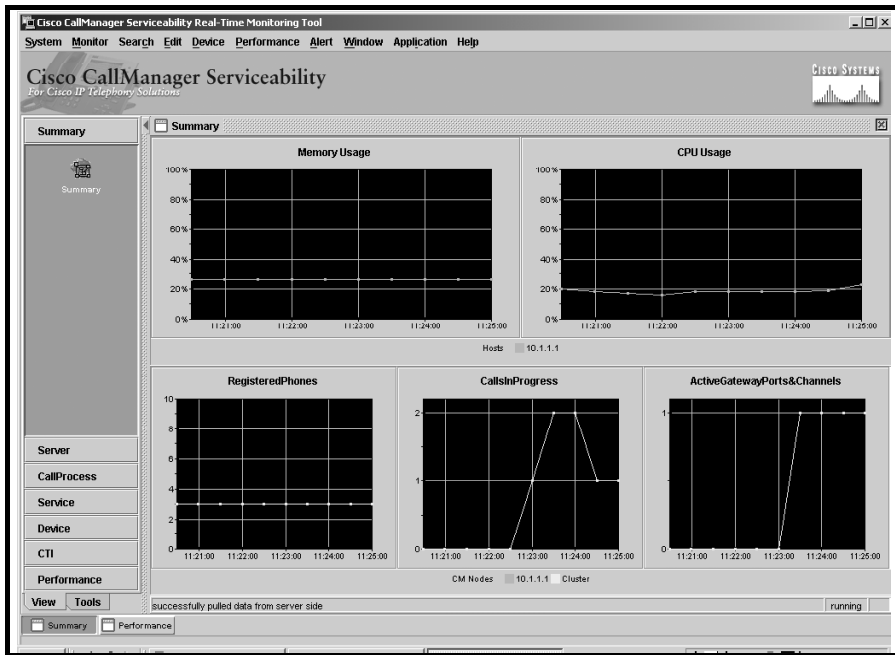
Task 4: Use RTMT

The RTMT tabs should look similar to these figures:

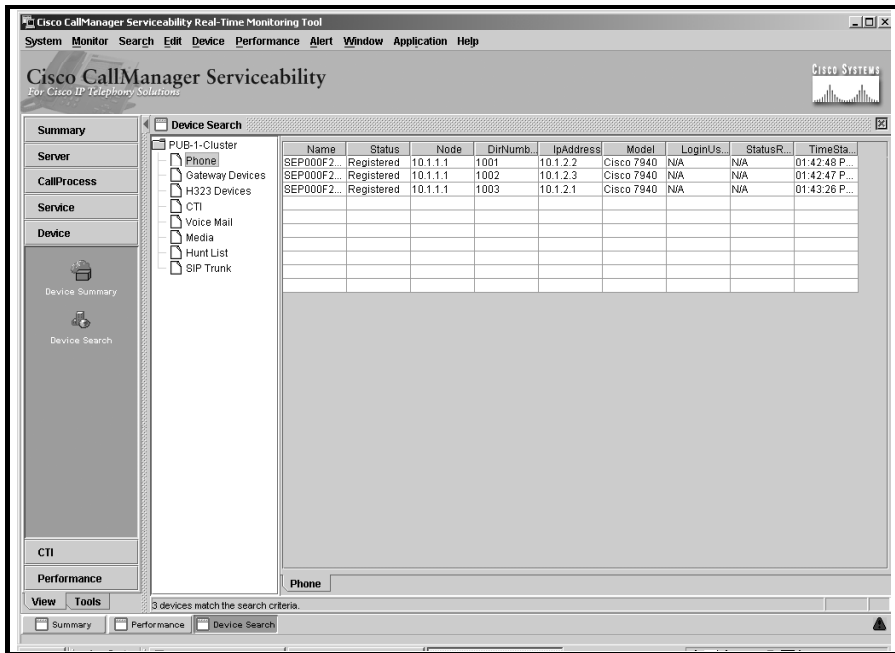
- Performance tab



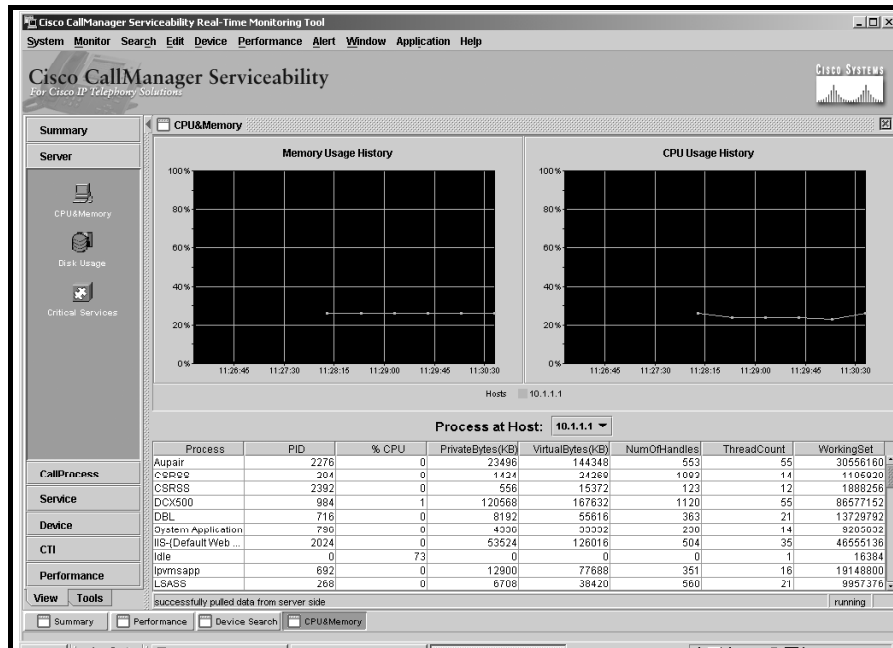
■ Summary tab



■ Device Search tab



- Other tabs (in this case, CPU&Memory):



Task 5: Create RTMT Profiles

The Preferences window should include a personal configuration similar to the one shown in this figure.



Lab 3-2: Configuring Alarms and Traces

Complete this lab activity to practice what you learned in the related module.

Activity Objective

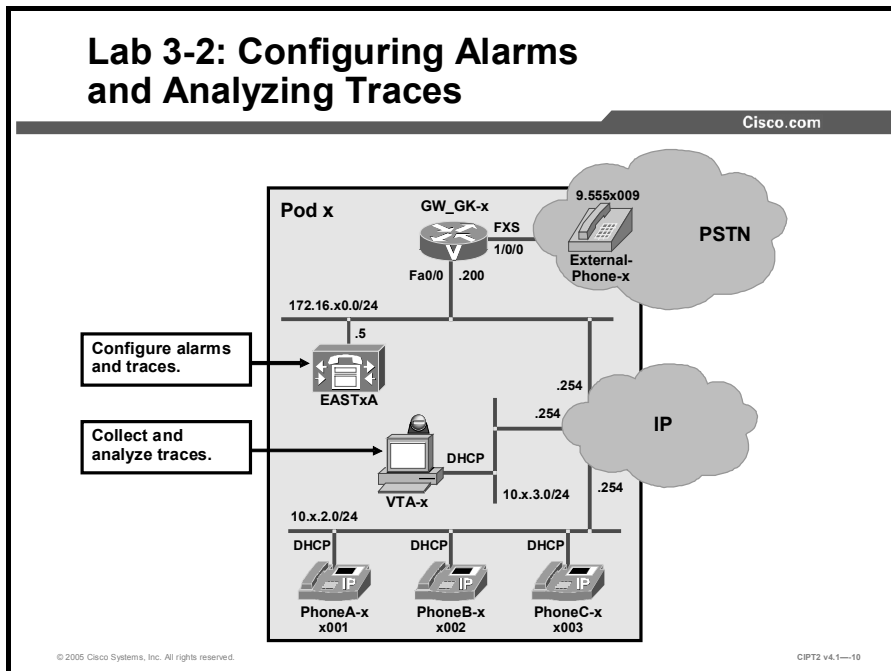
In this activity, you will configure, download, and analyze alarms and traces that are created on Cisco CallManager. After completing this activity, you will be able to meet these objectives:

- Configure the Cisco CallManager Serviceability Alarm interface to forward alarms of one level to Event Viewer and of another level to a Serviceability trace file
- Load the Trace Collection tool plug-in and establish a secure connection to the Trace Collection tool
- Configure trace parameters for the Cisco CallManager service
- Select, collect, and compress the trace files
- Obtain the trace results from an SDL trace file
- View and analyze trace information

Visual Objective

In this activity, you will become familiar with Cisco CallManager alarms and traces. You will place test calls and analyze the trace files by using the Bulk Trace Analysis tool.

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment that are required to complete this activity:

- The lab devices shown in the Visual Objectives figure and detailed in the table

Lab Devices and Their Roles

Device	Device Role in the Activity
EASTxA	Cisco CallManager publisher that serves the IP Phones
GW_GK-x	H.323 gateway
PhoneA-x, PhoneB-x, PhoneC-x	IP Phones
External-Phone-x	PSTN telephone

- The device credentials in the table, to log in to the lab devices that require authentication

Credentials for Device Access

Device	Username / password
EASTxA	administrator lab
Cisco CallManager Administration	ccadministrator lab
VTA-x	administrator lab

Job Aids

These job aids are available to help you complete the lab activity.

- The table lists the DNs needed to place calls in the lab activity.

Directory Numbers

Device	Directory Number
PhoneA-x	x001, where x = your pod number
PhoneB-x	x002, where x = your pod number
PhoneC-x	x003, where x = your pod number
PhoneA-y	y001, where y = your partner pod number
PhoneB-y	y002, where y = your partner pod number
PhoneC-y	y003, where y = your partner pod number

- The lab devices use the IP address allocation scheme shown in the table.

IP Address Allocation Scheme

Device	IP Address
Voice server network	172.16.x0.0/24
IP Phone network	10.x.2.0/24
Data network	10.x.3.0/24
Default gateway	Node address .254 (for all networks)
EASTxA	172.16.x0.5
GW_GK-x	172.16.x0.200
PhoneA-x	DHCP-assigned (network 10.x.2.0)
PhoneB-x	DHCP-assigned (network 10.x.2.0)
PhoneC-x	DHCP-assigned (network 10.x.2.0)
VTA-x	DHCP-assigned (network 10.x.3.0)

- Additionally, you will use *Cisco CallManager Administration Guide, Release 4.1(3)*.

Task 1: Configure Alarm Levels and Destinations

In this task, you will configure the Cisco CallManager Serviceability Alarm interface to forward Cisco CallManager service alarms with the alarm level “warning” to Event Viewer and those with the alarm level “debug” to SDL trace files.

Activity Procedure

Complete these steps:

- Step 1** From VTA-x use Internet Explorer to access Cisco CallManager administration on EASTxA and choose **Application > Cisco CallManager Serviceability**.
- Step 2** Choose **Alarm > Configuration** and choose your Cisco CallManager server from the list.
- Step 3** Choose **Cisco CallManager** from the Configured Services drop-down list.
- Step 4** Under Event Viewer, check the **Enable Alarm** check box and choose the Alarm Event Level **Warning** for the Event Viewer to cause Cisco CallManager to send warning messages.
- Step 5** Under SDL Trace, check the **Enable Alarm** check box and set the Alarm Event Level to **Debug**.
- Step 6** Uncheck the **Enable Alarm** check boxes under Syslog Trace and SDI Trace.
- Step 7** Click **Update** to save your configuration.

Activity Verification

You have completed this task when you attain this result:

- You verify that the configured alarm levels and destinations are saved.

Specifically, complete these steps:

- Step 1** Choose **Alarm > Configuration** and choose the Cisco CallManager service for your Cisco CallManager server.
- Step 2** Verify that your changes are shown.

Task 2: Download the Trace Collection Tool

In this task, you will download the Trace Collection tool from the Cisco CallManager Install Plugins page and install it on your Cisco CallManager server.

Activity Procedure

Complete these steps:

- Step 1** On the VTA-x PC, use Internet Explorer to access Cisco CallManager Administration at <https://172.16.x0.5/CCMAdmin/main.asp>.
- Step 2** Log in to Cisco CallManager Administration and choose **Application > Install Plugins**.
- Step 3** Choose **Cisco CallManager Trace Collection Tool**.
- Step 4** Choose **Open** and accept all defaults to install the Trace Collection tool on your VTA-x PC.

Activity Verification

You have completed this task when you attain this result:

- You verify proper installation of the Trace Collection tool.

Specifically, complete this step:

- Step 1** Choose **Start > Programs > Cisco CallManager Serviceability** from your VTA-x PC to confirm that the Trace Collection tool is available.

Task 3: Configure Cisco CallManager Trace Parameters

You will enable XML-formatted SDL traces for the Cisco CallManager service, including all possible trace filters and trace characteristics.

Activity Procedure

Complete these steps:

- Step 1** From VTA-x use Internet Explorer to access Cisco CallManager administration on EASTxA and choose Cisco CallManager Serviceability.
- Step 2** Choose **Trace > Configuration** and choose your Cisco CallManager from the Servers list.

- Step 3** Choose **Cisco CallManager** from the Configured Services list to access the SDI Trace Configuration window for the Cisco CallManager service.
- Step 4** Click the **SDL Configuration** link at the right side of the window to switch to the SDL Trace Configuration window.
- Step 5** Check the **Trace On** check box.
- Step 6** In the Trace Filter Settings and Trace Characteristics areas, check all the check boxes, and choose XML-formatted output.
- Step 7** Reconfigure the maximum number of trace lines to **2000**.
- Step 8** Click **Update** to save your configuration.
- Step 9** Place several calls among your IP Phones to cause the system to write trace files.

Activity Verification

You have completed this task when you attain this result:

- You verify that trace files have been written.

Specifically, complete this step:

- Step 10** On EASTxA, open the C:\Program Files\Cisco\Trace\SDL\CCM folder to view one or more XML-formatted SDL trace files with an actual date and time.

Task 4: Collect and Compress Traces

You will download and compress Cisco CallManager service performance logs and system traces to the VTA-x PC by using the Trace Collection tool.

Activity Procedure

Complete these steps:

- Step 1** On the VTA-x PC, choose **Start > Programs > Cisco CallManager Serviceability > Trace Collection Tool**, and start the Trace Collection tool.
- Step 2** Enter the IP address of your Cisco CallManager.
- Step 3** Enter the username **administrator** and the password **lab**, and click **Next**.
- Step 4** When you receive a warning that the certificate might not be valid, click **Yes** to continue anyway.
- Step 5** The Cisco CallManager Trace Collection Tool window appears, where you can choose the traces and log files that you want to collect. Choose only **Cisco CallManager** from the Select CallManager Services tab to make sure that only Cisco CallManager service-related trace files are downloaded.
- Step 6** Deselect all applications from the Select CallManager Applications tab to prevent downloading of application traces.
- Step 7** Choose only **System Performance Logs** from the Select System Traces tab.
- Step 8** Click **Next**, and at the Collect Traces window set the Compression Factor field to **9 – Highest** and click **Collect Traces** to start file compression and downloading.

- Step 9** A popup window states the size of the files that will be compressed. Click **Yes** to confirm that you want to proceed.
- Step 10** You see a status bar showing the progress of the file-compression operation.
- Step 11** When the zipped files are downloaded, you see a message giving you the number of downloaded files and the location where the .zip file has been stored (by default, the file is named C:\CiscoCallManagerTraceCollection.zip). Click **OK** to confirm. You are returned to the Collect Traces window. Click **Exit** to close the application and confirm the choice by clicking **Yes**. Be patient while the .zip file is generated and downloaded to your PC.
- Step 12** Use Windows Explorer to locate the .zip file. Extract its content and then view some of the downloaded files.

Activity Verification

The verification of successful trace collection was part of the activity procedure.

Task 5: Obtain Trace Results from an SDL Trace File

In this task, you will install the Bulk Trace Analysis tool on the VTA-x PC, extract some XML-formatted SDL trace files from the previously compressed CiscoCallManagerTraceCollection.zip file and create two SDL trace file reports.

Activity Procedure

Complete these steps:

- Step 1** On the VTA-x PC, extract some of the XML-formatted SDL trace files from the CiscoCallManagerTraceCollection.zip file that was created in Task 4.
- Step 2** Use Internet Explorer to access Cisco CallManager Administration at **https://172.16.x0.5/cmadmin**.
- Step 3** Log in to Cisco CallManager Administration and choose **Application > Install Plugins**
- Step 4** Choose **Cisco Bulk Trace Analysis Tool**.
- Step 5** Choose **Open** and install the Trace Collection tool on the VTA-x PC.
- Step 6** After finishing the installation, choose **Start > Programs > Cisco Bulk Trace Analysis Tool** to start the Bulk Trace Analysis tool.
- Step 7** Choose **File > New Report**. The **New File** window opens.
- Step 8** Choose **SDL** in Step 1 in the New File window.
- Step 9** Click **Browse** to choose a source file.
- Step 10** Navigate to the XML-formatted trace files (extracted in the first step of this task), choose one of the files, and open it.
- Step 11** Click **OK** to create a new report.
- Step 12** Repeat Steps 7 through 11 to create a second report using another file.

Activity Verification

You have completed this task when you attain this result:

- You see at least two tasks with one view each on the Workplace Views folder of the Bulk Trace Analysis window.

Specifically, complete this step:

- Step 1** Verify that each task (report) includes analyzed trace output information.

Task 6: Choose Specific Trace Information to View and Analyze

You will create customized views of the previously created SDL trace reports.

Activity Procedure

Complete these steps:

- Step 1** On the VTA-x PC, in the Bulk Trace Analysis tool, choose one of the reports created in Task 5.
- Step 2** Choose **View > New View** to access the Filter window.
- Step 3** Deselect all source devices (SrcDev) except one IP Phone in the selection criteria, and click **OK** to create a view including only that specific IP Phone.
- Step 4** Repeat Steps 2 and 3, using another IP Phone to add trace output for another device within the same file.
- Step 5** Switch to the other report and create another view including only some source IP addresses (SrcIp).
- Step 6** Create your own view according to your personal selection.

Note Do not deselect all possible values of a magnifier because then nothing will match your criteria.

- Step 7** Analyze the differences between the views of your reports.

Activity Verification

You have completed this task when you attain this result:

- You verify that the views were successfully created.

Lab 3-2 Answer Key: Configuring Alarms and Traces

When you complete this activity, your solution will be similar to this, with differences that are specific to your device or workgroup.

Task 1: Configure Alarm Levels and Destinations

Your configuration should be similar to this figure.

The screenshot shows the Cisco CallManager Serviceability web interface. At the top, there is a navigation bar with links for Alarm, Trace, Tools, Application, and Help. The main header displays "Cisco CallManager Serviceability" and "For Cisco IP Telephony Solutions" along with the Cisco Systems logo. The page title is "Alarm Configuration".

On the left, a "Servers" sidebar lists the server "10.1.1.1". The main content area shows the configuration for the "Current Service: Cisco CallManager" and "Current Server: 10.1.1.1", with a status of "Ready". There are "Update" and "SetDefault" buttons. The "Configured Services" dropdown is set to "Cisco CallManager", and the "Apply to All Nodes" checkbox is unchecked.

The configuration is divided into four sections:

- Event Viewer:** "Enable Alarm" is checked, and the "Alarm Event Level" is set to "Warning".
- Syslog Trace:** "Enable Alarm" is unchecked, and the "Alarm Event Level" is set to "Error". A "Server Name*" field is present but empty.
- SDI Trace:** "Enable Alarm" is unchecked, and the "Alarm Event Level" is set to "Error".
- SDL Trace:** "Enable Alarm" is checked, and the "Alarm Event Level" is set to "Debug".

At the bottom, there are two notes:

- * Note: If Syslog Trace is enabled and no server name is specified, Cisco CallManager sends Syslog messages to the localhost.
- Note: For SDI Trace, enable Alarm will result in alarms logged into Trace files, only if "Trace ON" checkbox and "Enable File Trace Log" checkbox is checked on Trace Configuration page.

Task 2: Download the Trace Collection Tool

The Trace Collection tool should be installed.



Task 3: Configure Cisco CallManager Trace Parameters

Your configuration should look similar to this figure.

The screenshot displays the 'SDL Trace Configuration' page in the Cisco CallManager Serviceability interface. The page includes a navigation bar with 'Alarm', 'Trace', 'Tools', 'Application', and 'Help' tabs. The main content area shows the service configuration for 'Cisco CallManager' on server '10.1.1.1'. The 'Trace On' checkbox is checked, and the 'Apply to All Nodes' checkbox is unchecked. The 'Trace Filter Settings' section contains 16 checkboxes, all of which are checked. The 'Trace Characteristics' section contains 8 checkboxes, all of which are checked. The 'Trace Output Settings' section includes a checked checkbox for 'Enable XML Formatted Output for "Trace Analysis"', a text field for 'Trace Directory Path' containing 'C:\Program Files\Cisco\Trace\SDL\', and two numeric input fields for 'Maximum No. of Trace Files' (250) and 'Maximum No. of Trace Lines' (2000). Two notes are provided at the bottom of the page.

Alarm Trace Tools Application Help

Cisco CallManager Serviceability
For Cisco IP Telephony Solutions

SDI Configuration

Service : Cisco CallManager
Server : 10.1.1.1
Status : Update completed

Update SetDefault

Configured Services: Cisco CallManager

Trace On Apply to All Nodes

Trace Filter Settings

- Enable All Layer 1 Trace
- Enable All Layer 2 Trace
- Enable Layer 2 TCP Trace
- Enable All Layer 3 Trace
- Enable Miscellaneous Polls Trace
- Enable Message Translation Signals Trace
- Enable Gateway Signals Trace
- Enable Network Service Data Trace
- Enable ICCP Admin Trace
- Enable Detailed Layer 1 Trace
- Enable Layer 2 interface Trace
- Enable Detailed Dump Layer 2 Trace
- Enable All Call Control Trace
- Enable Miscellaneous Trace (Database Signals)
- Enable UUIE Output Trace
- Enable CTI Trace
- Enable Network Service Event Trace
- Enable Default Trace

Trace Characteristics

- Enable SDL Link States Trace
- Enable SDL Link Poll Trace
- Enable Signal Data Dump Trace
- Enable SDL Process States Trace
- Enable SDL TCP Event Trace.
- Enable Low-level SDL Trace
- Enable SDL Link Messages Trace
- Enable Correlation Tag Mapping Trace
- Disable Pretty Print Of SDL Trace

Trace Output Settings

- Enable XML Formatted Output for "Trace Analysis"

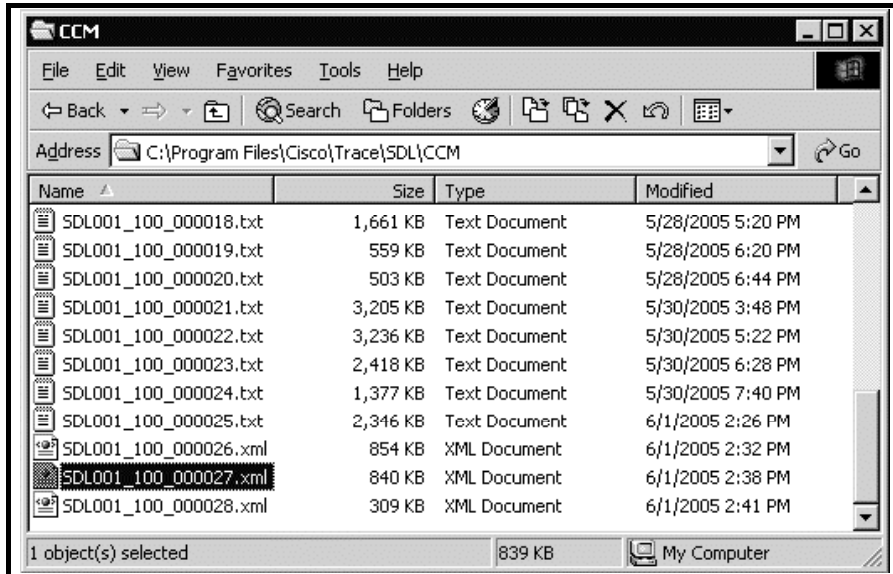
Trace Directory Path: C:\Program Files\Cisco\Trace\SDL\

Maximum No. of Trace Files: 250

Maximum No. of Trace Lines: 2000

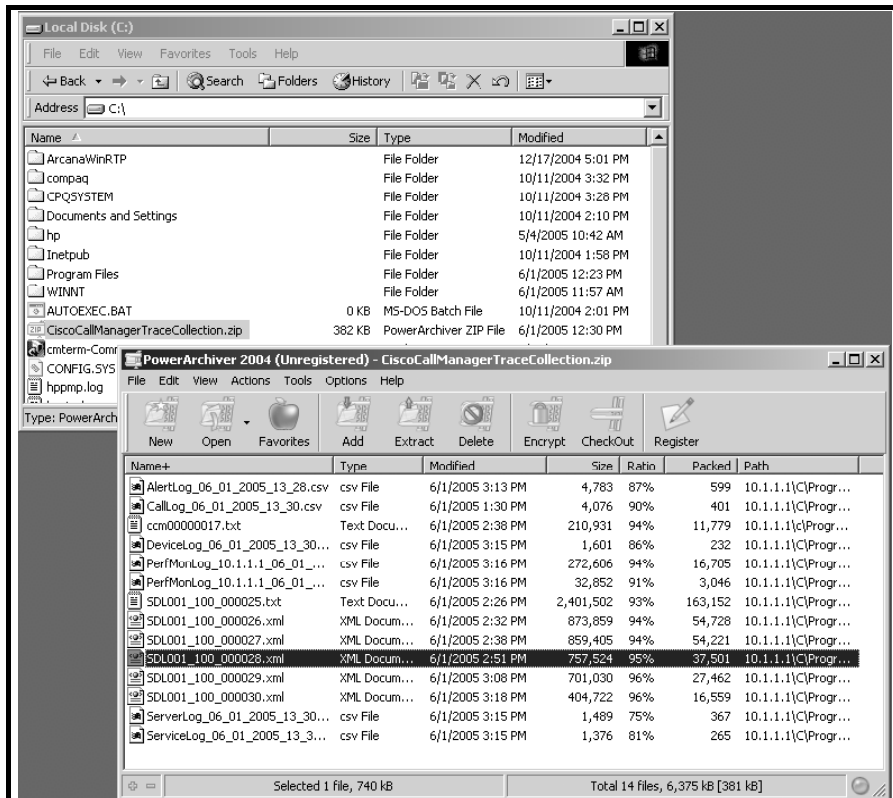
* Note1: Check this box for analysis of trace logs with Trace Analysis.
* Note2: Enabling XML Formatted Output "Trace Analysis" in between the text file logging will result in invalid XML document for the first file log. So it's advisable to check Enable XML Formatted Output when we check the Trace On option.

XML-formatted SDL files should be available on the Cisco CallManager server, similar to the files shown in the figure.



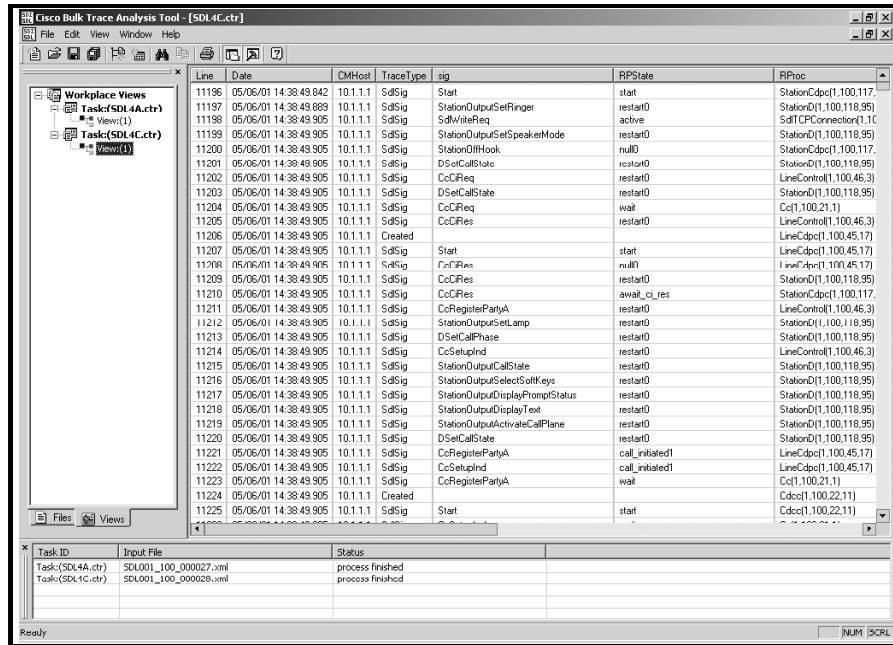
Task 4: Collect and Zip Traces

An archive containing the XML-formatted trace files should be available on the VTA-x PC, similar to the files shown in the figure.



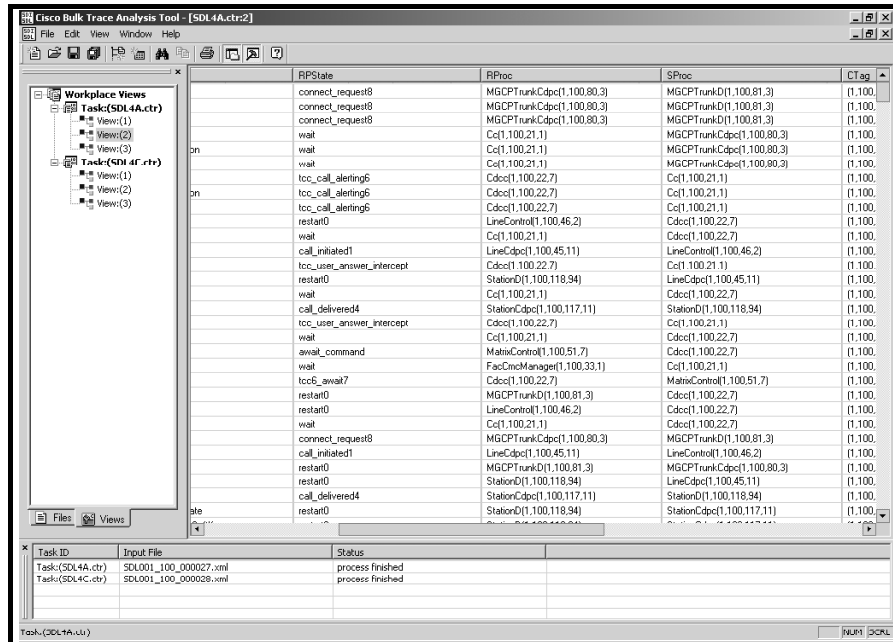
Task 5: Obtain Trace Results from an SDL Trace File

The Bulk Trace Analysis Tool window should look similar to this figure.



Task 6: Choose Specific Trace Information to View and Analyze

The Bulk Trace Analysis Tool window should look similar to this figure.



Lab 3-3: Configuring CAR

Complete this lab activity to practice what you learned in the related lesson.

Activity Objective

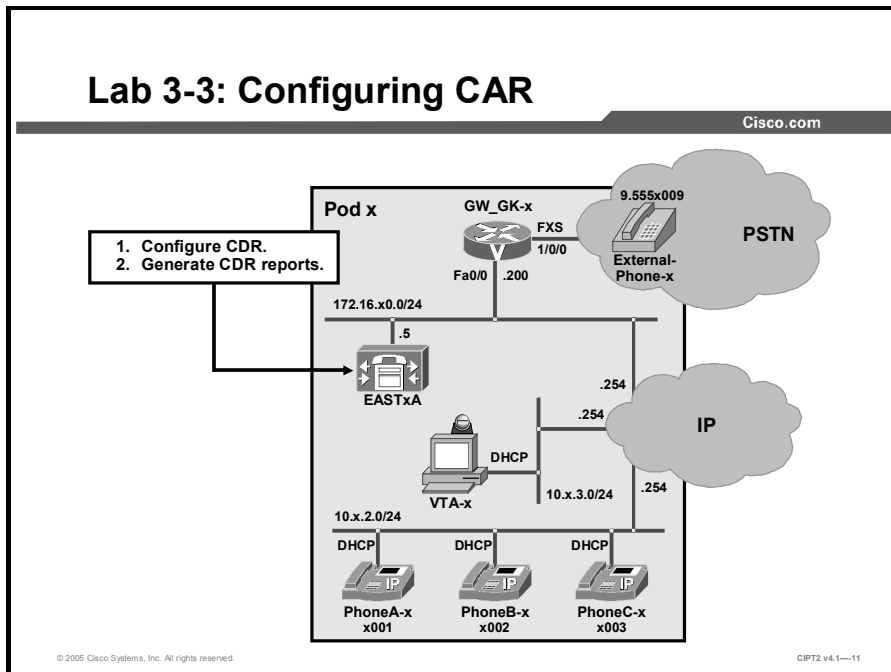
In this activity, you will configure CAR. After completing this activity, you will be able to meet these objectives:

- Enable CDR and install CAR
- Configure CAR system parameters for report generation
- Configure the system scheduler to schedule daily, weekly, and monthly CDR reports, and daily, weekly, and monthly reports
- Set up the CAR database and CDR database notifications and set a message, a maximum number of records, and an alert percentage
- Generate various kinds of reports

Visual Objective

You will enable CDR and install CAR on EASTxA and generate CDRs by making calls between the IP Phones in your pod. You will also make some international calls and enter the relevant forced authorization code. Then you will generate reports to get an overview of the traffic volume and pattern.

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment that are required to complete this activity:

- The lab devices shown in the Visual Objectives figure and detailed in the table

Lab Devices and Their Roles

Device	Device Role in the Activity
EASTxA	CDR and CAR are enabled on EASTxA.
PhoneA-x	IP Phone.
PhoneB-x	IP Phone.
PhoneC-x	IP Phone.
VTA-x	Used to connect to Cisco CallManager Administration and the CAR tool.

- The device credentials in the table, to log in to the lab devices that require authentication

Credentials for Device Access

Device	Username and Password
EASTxA	administrator lab
Cisco CallManager Administration	ccadministrator lab
VTA-x	administrator lab
CAR administrator on EASTxA	CARadmin lab123
CAR user on EASTxA	CARuser lab123

Job Aids

These job aids are available to help you complete the lab activity.

- The table lists the DNs needed to place calls in the lab activity.

Directory Numbers

Device	Directory Number
PhoneA-x	x001, where x = your pod number
PhoneB-x	x002, where x = your pod number
PhoneC-x	x003, where x = your pod number
PhoneA-y	y001, where y = your partner pod number
PhoneB-y	y002, where y = your partner pod number
PhoneC-y	y003, where y = your partner pod number

- The lab devices use the IP address allocation scheme shown in the table.

IP Address Allocation Scheme

Device	IP Address
Voice server network	172.16.x0.0/24
IP Phone network	10.x.2.0/24
Data network	10.x.3.0/24
Default gateway	Node address .254 (for all networks)
EASTxA	172.16.x0.5
GW_GK-x	172.16.x0.200
PhoneA-x	DHCP-assigned (network 10.x.2.0)
PhoneB-x	DHCP-assigned (network 10.x.2.0)
PhoneC-x	DHCP-assigned (network 10.x.2.0)
VTA-x	DHCP-assigned (network 10.x.3.0)

Additionally, you will use *Cisco CallManager Administration Guide, Release 4.1(3)*.

Task 1: Enable CDRs and Install CAR

In this task, you will activate the CDR Insert service and CDR functionality and install the CAR plug-in on Cisco CallManager.

Activity Procedure

Complete these steps:

- Step 1** On VTA-x, launch a web browser and connect to Cisco CallManager Serviceability at <https://EASTxA/CCMService.main.asp>.
- Step 2** Choose **Tools > Service Activation** and choose your Cisco CallManager.
- Step 3** Choose **CDR Insert** and click **Update**.

- Step 4** Switch to the Cisco CallManager Administration page and choose **Service > Service Parameters**. Choose the server **EASTxA** and the service **Cisco CallManager**. The Service Parameter configuration window opens.
- Step 5** Scroll down to the System parameters, find the CDR Enabled Flag parameter, choose **True**, and click **Update**.
- Step 6** Connect to EASTxA to install the CAR plug-in locally on this server by choosing **Application > Install Plugins**. In the new opened window, click the **CDR Analysis and Reporting** plug-in symbol. A file download window opens and you are prompted to open or save the AdministrativeReportingTool.exe file.
- Step 7** Open the file to install the plug-in locally on EASTxA.
- Step 8** When prompted, press **Next** to proceed with the plug-in installation. Enter the private password **lab** and click **Next** twice. Cisco CallManager stops the IISAdmin Service, the CDR Analysis and Reporting Scheduler Service, and the Tomcat service. The CAR database is updated, and the stopped services are restarted.
- Step 9** Click **Finish** to complete the installation.

Activity Verification

You have completed this task when you attain these results:

- The CDR Insert service is running.
- The CDR parameter is enabled on EASTxA to fill the CDR database.
- The CAR tool installation was successful.

Specifically, complete these steps:

- Step 1** Access the Cisco CallManager Serviceability window and choose **Tools > Control Center**.
- Step 2** Choose your Cisco CallManager and verify that the CDR Insert service is running.
- Step 3** Place some calls between your IP Phones.
- Step 4** Verify that you find temporarily flat files in the directory C:\Program Files\Cisco\CallDetail\CDR.
- Step 5** On VTA-x, launch a web browser and connect to **https://172.16.x0.5/art**.
- Step 6** Verify that the CDR Analysis and Reporting login window is displayed.

Task 2: Configure CAR System Parameters

In this task, you will make calls to generate CDR entries and add two new users in Cisco CallManager Administration who will be able to log in to the CAR tool. You will grant administrator rights to a user and configure CAR system parameters.

Activity Procedure

Complete these steps:

- Step 1** From VTA-x use Internet Explorer to access Cisco CallManager administration on EASTxA and choose **User > Add a New User** in Cisco CallManager Administration.
- Step 2** Enter **CARadmin** as the user ID and **lab123** as the password, fill out the other relevant fields, and click **Insert**.
- Step 3** Choose **Device Association**. In the window that appears, click the **Select Device** button to list all available IP Phones.
- Step 4** Choose **PhoneA-x** and click **Update** to associate that IP Phone with the CARadmin user.
- Step 5** Repeat Steps 1 to 4 to create the user ID CARuser and associate that user with PhoneB-x and PhoneC-x.
- Step 6** On VTA-x, launch a web browser and connect to the Cisco CallManager CAR tool at **https://172.16.x0.5/ART**.
- Step 7** Log in as user **admin** with the password **admin**. A successful installation creates a one-time login with these credentials. No other login credentials work at this time.
- Step 8** Choose **Admin Rights**. In the Grant/Revoke CAR Admin Rights window that appears, enter **CARadmin** as the user ID, click **Add** and then click **Update** to grant the chosen user administrator rights. You will be logged out of the CAR tool immediately.
- Step 9** Log in to the CAR tool again with the user ID **CARadmin** and the password **lab123**.
- Step 10** Choose **System > System Parameters > System Preferences** and set the **COMPANY_NAME** parameter to a string of your choice. Click **Update**.

Activity Verification

You have completed this task when you attain these results:

- There are two new users that are associated with the IP Phones.
- The user CARadmin was granted administrator access rights.
- You logged in as CARadmin with administrator access rights and the full menu was available in the CAR tool.

Specifically, complete these steps:

- Step 1** From Cisco CallManager Administration, choose **User > Global Directory** and click **Search** to list all available users.
- Step 2** Choose the user **CARuser**, then choose **Device Association** to list all associated devices and verify that the association is correct.
- Step 3** Repeat Steps 1 and 2 for the user CARadmin.
- Step 4** From the CAR tool, choose **System > System Parameters > Admin Rights**.
- Step 5** Verify that the CAR Administrators field contains only CARadmin.
- Step 6** Verify that there are at least eight menu items on the main menu.

Task 3: Configure the System Scheduler

In this task you will configure CDR loading. Then you will change the default CDR load time for daily, weekly and monthly reports.

Activity Procedure

Complete these steps:

- Step 1** In the Cisco CallManager CAR tool (accessible from VTA-x through a web browser at <https://172.16.x0.5/ART>), login using the username CARadmin and choose **System > Scheduler > CDR Load**. Verify that the Disable Loader check box is not checked.
- Step 2** In the Load CDR & CMR area, configure these values:
 - Set the Time field to **00** hours **00** minutes.
 - Set the Loading Interval field to the shortest interval.
 - Set the Duration field to **2** minutes.
- Step 3** Configure the Uninhibited Loading of CDR area as From **00** hours **00** minutes To **23** hours **59** minutes to enable CDR loading at any time. Click **Update**.
- Step 4** Choose **System > Scheduler > Daily**, set the Daily Report Generation Time to **00** hours **15** minutes, and click **Update**.
- Step 5** Choose **System > Scheduler > Weekly**, set the Weekly Report Generation day to **Monday** and the time to **1** hour **00** minutes. Click **Update**.
- Step 6** Choose **System > Scheduler > Monthly** and verify that the Monthly Bill Generation and the Other Monthly Reports are generated on the first day of the month.
- Step 7** Restart the CAR service.

Activity Verification

You have completed this task when you attain these results:

- You have enabled CDR loading so that the shortest loading interval is used during the whole day.
- You have optimized the daily and weekly report parameters and verified the monthly parameters.

Specifically, complete these steps:

- Step 1** Choose **System > Scheduler > CDR Load** and verify that your configuration was saved.
- Step 2** Choose the related scheduler configuration windows and verify that your configurations were saved.

Task 4: Configure the System Database

In this task, you will configure the system databases to generate alarms when a threshold is reached. You will configure that threshold and the alarm message to be generated, and you will disable automatic database purge.

Activity Procedure

Complete these steps:

- Step 1** In the Cisco CallManager CAR tool (accessible from VTA-x through a web browser at <https://172.16.x0.5/ART>), login using the username CARAdmin and choose **System > Database > CAR Database Alert**. Set these parameters:
- Set the Percent of Max Rows field to **90**.

Note If the CAR database exceeds a predefined percentage of maximum size, you can use the CAR Database Alert function to set the percentage and maximum size.

- Send a copy of the report to the user with administrator access rights.
 - Modify the values in the Mail Subject and Mail Message fields as you choose, and click **Update**.
- Step 2** Choose **System > Database > CDR Database Alert**. Set the CDR parameters to be equivalent to the CAR parameters.
- Step 3** Verify that automatic purge is disabled. Choose **System > Database > Configure Automatic Purge**. Uncheck the **Disable CDR Purge** and **Disable CAR Purge** check boxes; otherwise, the database is automatically purged and you could lose important CDR entries.
- Step 4** Restart CAR service.

Activity Verification

You have completed this task when you attain this result:

- Alerts are enabled for CDRs and CAR

Specifically, complete this step:

- Step 1** Verify that notification parameters are configured correctly.

Task 5: Generate Reports

In this task, you will generate reports and identify differences in the options available to a CAR administrator and a CAR user.

Activity Procedure

Complete these steps:

- Step 1** Place a few calls among any of the three IP Phones in your pod. The calls should last at least 5 seconds. Also make some international calls via your FAC-enabled route pattern **9.011!#** with the authorization code **4321**.
- Step 2** Wait a while to allow the CDRs to be processed.
- Step 3** Log in to the Cisco CallManager CAR tool (accessible from VTA-x through a web browser at <https://172.16.x0.5/ART>), login using the username CARAdmin and, to generate a department bill, choose **User Reports > Bills > Department**. Generate a report with these parameters:

- The Report Type value is **Summary**.
 - The User ID values are **CARuser** and **CARadmin**.
 - The Report Format value is **PDF**.
- Step 4** Click **View Report**. You see all the calls made from the IP Phones in your pod.
- Step 5** Generate the same report described in Step 3, but this time set the report type to **Detailed** and note the differences between the summary and detailed reports.
- Step 6** Generate a Top N report for the number of calls by choosing **User Reports > Top N > Number of Calls**. Generate a report with these parameters:
- The Report Type value is **By Individual Users**.
 - The Available Reports value is **Generate New Report**.
 - The Report Format value is **PDF**.
- Step 7** Click **View Report**. You will see the user with the largest number of calls.
- Step 8** Generate a CMC and FAC report by choosing **System Reports > CMC/FAC > Authorization Level**. Generate a report with these parameters:
- Choose the relevant authorization level.
 - Set the date range.
 - Set the report format to **PDF**.
- Step 9** Click **View Report**. You will see the number of calls and the duration for the various authorization levels.
- Step 10** Log off the CAR tool as CARadmin. Then log in to the Cisco CallManager CAR tool using the **CARuser** username and compare the menus now available in the CAR tool to the menu available to the administrator.
- Step 11** Generate a detailed individual report by choosing **Bill > Individual**.

Activity Verification

You have completed this task when you attain these results:

- All requested reports are created.
- You have identified and described the differences between the user and the administrator login in the CAR menu.

Specifically, complete these steps:

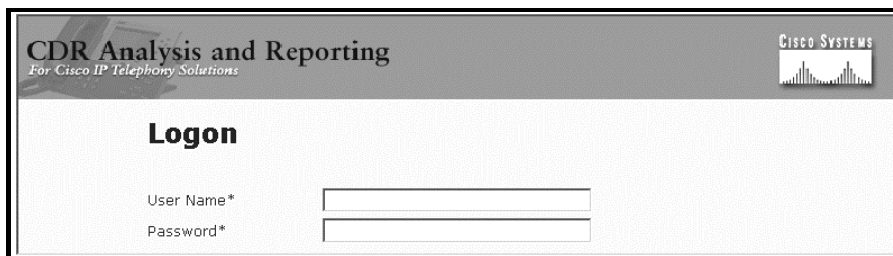
- Step 1** Make sure that you have generated the reports for the department.
- Step 2** Make sure that you have generated a Top N users report.
- Step 3** Make sure that you have generated a FAC report.
- Step 4** Make sure that you have generated an individual report for the user CARuser.
- Step 5** Verify that the CAR main menu has only three items and contains fewer submenu items when you log in as CARuser.

Lab 3-3 Answer Key: Configuring CAR

When you complete this activity, your solution will be similar to this, with differences that are specific to your device or workgroup.

Task 1: Enable CDRs and Install CAR

The CDR Analysis and Reporting Logon window should be displayed.



The screenshot shows the 'Logon' page of the CDR Analysis and Reporting application. The page has a header with the title 'CDR Analysis and Reporting' and the Cisco Systems logo. Below the header, there is a 'Logon' section with two input fields: 'User Name*' and 'Password*'. The 'User Name*' field is currently empty, and the 'Password*' field is also empty.

Task 2: Configure CAR System Parameters

The CAR menu should be similar to the menu in this figure.

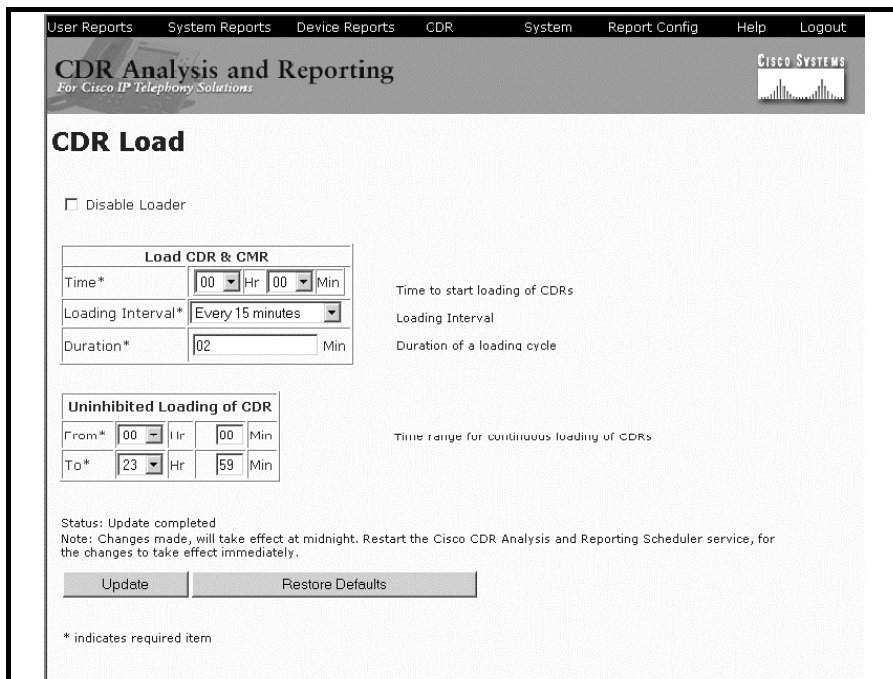


The screenshot shows the main menu of the CDR Analysis and Reporting application. The menu items are: User Reports, System Reports, Device Reports, CDR, System, Report Config, Help, and Logout. The 'CDR' menu item is highlighted. The page also features the title 'CDR Analysis and Reporting' and the Cisco Systems logo.

Task 3: Configure the System Scheduler

The schedule settings should show the configured values:

- CDR load



The screenshot shows the 'CDR Load' configuration page. The page has a header with the title 'CDR Analysis and Reporting' and the Cisco Systems logo. Below the header, there is a 'CDR Load' section. The 'Disable Loader' checkbox is unchecked. The 'Load CDR & CMR' section has three fields: 'Time*' (00 Hr 00 Min), 'Loading Interval*' (Every 15 minutes), and 'Duration*' (02 Min). The 'Uninhibited Loading of CDR' section has two fields: 'From*' (00 Hr 00 Min) and 'To*' (23 Hr 59 Min). The 'Status' is 'Update completed'. A note states: 'Note: Changes made, will take effect at midnight. Restart the Cisco CDR Analysis and Reporting Scheduler service, for the changes to take effect immediately.' There are two buttons: 'Update' and 'Restore Defaults'. A footnote indicates '* indicates required item'.

- Daily schedule

The screenshot shows the 'Daily Scheduler' configuration page. At the top, there is a navigation menu with links: User Reports, System Reports, Device Reports, CDR, System, Report Config, Help, and Logout. The page title is 'CDR Analysis and Reporting For Cisco IP Telephony Solutions' with the Cisco Systems logo on the right. The main heading is 'Daily Scheduler'. Below this is a table for configuration:

Process	Time		Life
Daily Report Generation*	00	15	02

Below the table, the status is 'Update completed'. A note states: 'Note: Changes made, will take effect at midnight. Restart the Cisco CDR Analysis and Reporting Scheduler service, for the changes to take effect immediately.' There are two buttons: 'Update' and 'Restore Defaults'. A footnote at the bottom left says '* indicates required item'.

- Weekly schedule

The screenshot shows the 'Weekly Scheduler' configuration page. It has the same navigation menu and header as the Daily Scheduler page. The main heading is 'Weekly Scheduler'. Below this is a table for configuration:

Process	Day of Week	Time		Life
Weekly Report Generation*	Monday	01	00	02

Below the table, the status is 'Update completed'. A note states: 'Note: Changes made, will take effect at midnight. Restart the Cisco CDR Analysis and Reporting Scheduler service, for the changes to take effect immediately.' There are two buttons: 'Update' and 'Restore Defaults'. A footnote at the bottom left says '* indicates required item'.

Task 4: Configure the System Database

Alerts for CDRs and CAR should show the configured values, and automatic purge should be disabled:

- CAR database alert

The screenshot shows the 'CAR Database Alert' configuration page. At the top, there is a navigation menu with 'User Reports', 'System Reports', 'Device Reports', 'CDR', 'System', 'Report Config', 'Help', and 'Logout'. The page title is 'CDR Analysis and Reporting For Cisco IP Telephony Solutions' with the Cisco Systems logo. The main heading is 'CAR Database Alert'. The configuration includes: 'Max number of rows in Billing Table*' set to 90; 'Notify Users when number of rows reaches*' set to 80.00 % of Max Rows; a checked checkbox for 'Mail to Administrator'; 'To...' field set to CARAdministrator; 'Cc...' field set to CARAdmin; 'Mail Subject' set to CIPT2 CAR Alert; and 'Mail Message' set to 'Number of rows in Billing table in the CAR database has crossed the maximum of 90'. The status is 'Update completed' and there are 'Update' and 'Restore Defaults' buttons. A note at the bottom states '* indicates required item'.

- CDR database alert

The screenshot shows the 'CDR Database Alert' configuration page. At the top, there is a navigation menu with 'User Reports', 'System Reports', 'Device Reports', 'CDR', 'System', 'Report Config', 'Help', and 'Logout'. The page title is 'CDR Analysis and Reporting For Cisco IP Telephony Solutions' with the Cisco Systems logo. The main heading is 'CDR Database Alert'. The configuration includes: 'Max number of rows in CDR Table' set to 1,500,000; 'Notify Users when number of rows reaches*' set to 80.00 % of Max Rows; a checked checkbox for 'Mail to Administrator'; 'To...' field set to CARAdministrator; 'Cc...' field set to CARAdmin; 'Mail Subject' set to CIPT2 CDR Alert; and 'Mail Message' set to 'Number of rows in CallDetailRecord table in the CDR database has crossed the maximum of 90.'. The status is 'Update completed' and there are 'Update' and 'Restore Defaults' buttons. A note at the bottom states '* indicates required item'.

- Automatic database purge

User Reports System Reports Device Reports CDR System Report Config Help Logout

CDR Analysis and Reporting
For Cisco IP Telephony Solutions

Configure Automatic Database Purge

CDR Purge
 Disable CDR Purge
 Delete CDR Records older than Day(s)

CAR Purge
 Disable CAR Purge
 Delete CAR Records older than Day(s)

Status: Ready

* indicates required item

Task 5: Generate Reports

At least five different reports should exist. Each should look similar to these figures:

- Top N users report

Lab

Top 5 Users based on Number of Calls

From Date: Jun 1, 2005
To Date: Jun 3, 2005

Date: Jun 3, 2005
Page: 1 of 1

Report Generation Criteria-
Call Classification: On Net, Internal, Local, Long Distance, International, Incoming, Tandem, Others

User	Charge	Duration (sec)	Calls Made	Calls Received	Total Calls
CARuser	0.00	184	6	7	13
CARadmin	0.00	106	6	2	8

- FAC report

Lab

Authorization Level Call Details

From Date: Jun 3, 2005
To Date: Jun 3, 2005

Date: Jun 3, 2005
Page: 1 of 1

Orig.	Dest.	Orig. Date Time	Duration (sec)	Call Classification	Authorization Code Name
Calls for Authorization Level : 30					
1002	0111234567890#	Jun 3, 2005 6:20:51 PM	26	International	international
1001	011493012437286#	Jun 3, 2005 6:21:49 PM	7	International	international
Total Calls for 30 : 2					

■ Department summary report

Lab Department Bill - Summary							
From Date: Jun 1, 2005 To Date: Jun 3, 2005				Date: Jun 3, 2005 Page: 1 of 1			
Call Classification	Quality of Service					Calls	Charge
	Good	Acceptable	Fair	Poor	NA		
Bill for CARadmin							
Internal	0	0	0	0	4	4	0.00
International	0	0	0	0	1	1	0.00
Local	0	0	0	0	1	1	0.00
Total for CARadmin	0	0	0	0	6	6	0.00
Bill for CARuser							
Internal	0	0	0	0	5	5	0.00
International	0	0	0	0	1	1	0.00
Total for CARuser	0	0	0	0	6	6	0.00

■ Department detailed report

Lab Department Bill - Detail							
From Date: Jun 1, 2005 To Date: Jun 3, 2005				Date: Jun 3, 2005 Page: 1 of 1			
Date	Orig. Time	Orig.	Dest.	Call Classification	QoS	Duration (sec)	Charge
Bill for CARadmin							
Jun 3, 2005	4:08:05 PM	1001	1002	Internal	NA	5	0.00
Jun 3, 2005	5:26:02 PM	1001	1002	Internal	NA	16	0.00
Jun 3, 2005	6:13:15 PM	1001	1002	Internal	NA	13	0.00
Jun 3, 2005	6:20:08 PM	1001	5551009	Local	NA	21	0.00
Jun 3, 2005	6:20:40 PM	1001	1003	Internal	NA	22	0.00
Jun 3, 2005	6:21:49 PM	1001	011493012457286#	International	NA	7	0.00
Total for CARadmin						84	0.00
Bill for CARuser							
Jun 3, 2005	4:08:15 PM	1002	1003	Internal	NA	4	0.00
Jun 3, 2005	5:26:23 PM	1003	1001	Internal	NA	10	0.00
Jun 3, 2005	6:13:36 PM	1003	1001	Internal	NA	12	0.00
Jun 3, 2005	6:19:52 PM	1003	1002	Internal	NA	27	0.00
Jun 3, 2005	6:20:25 PM	1002	1003	Internal	NA	9	0.00
Jun 3, 2005	6:20:51 PM	1002	0111234567890#	International	NA	26	0.00
Total for CARuser						88	0.00

■ Individual report for CARuser

Lab Individual Bill - Detail							
From Date: Jun 1, 2005 To Date: Jun 3, 2005				Date: Jun 3, 2005 Page: 1 of 1			
Date	Orig. Time	Orig.	Dest.	Call Classification	QoS	Duration (sec)	Charge
Bill for CARuser							
Jun 3, 2005	4:08:15 PM	1002	1003	Internal	NA	4	0.00
Jun 3, 2005	5:26:23 PM	1003	1001	Internal	NA	10	0.00
Jun 3, 2005	6:13:36 PM	1003	1001	Internal	NA	12	0.00
Jun 3, 2005	6:19:52 PM	1003	1002	Internal	NA	27	0.00
Jun 3, 2005	6:20:25 PM	1002	1003	Internal	NA	9	0.00
Jun 3, 2005	6:20:51 PM	1002	0111234567890#	International	NA	26	0.00
Total for CARuser						88	0.00

Lab 3-4: Enabling Dependency Records, Configuring Cisco Dialed Number Analyzer, and Using QRT

Complete this lab activity to practice what you learned in the related module.

Activity Objective

In this activity you will use additional tools, such as dependency records and the Password Changer tool for Cisco CallManager that ease administration, and the Cisco Dialed Number Analyzer tool and QRT that help diagnosing IP Phone problems. After completing this activity, you will be able to meet these objectives:

- Enable and view dependency records
- Use the Password Changer tool to change the CCMAAdministrator password
- Use Cisco Dialed Number Analyzer to analyze inbound and outbound calls in a Cisco CallManager dial plan
- Add the QRT softkey to the IP Phone
- Use the QRT softkey to report IP Phone problems
- View Cisco CallManager IP Phone problem reports by using QRT Viewer

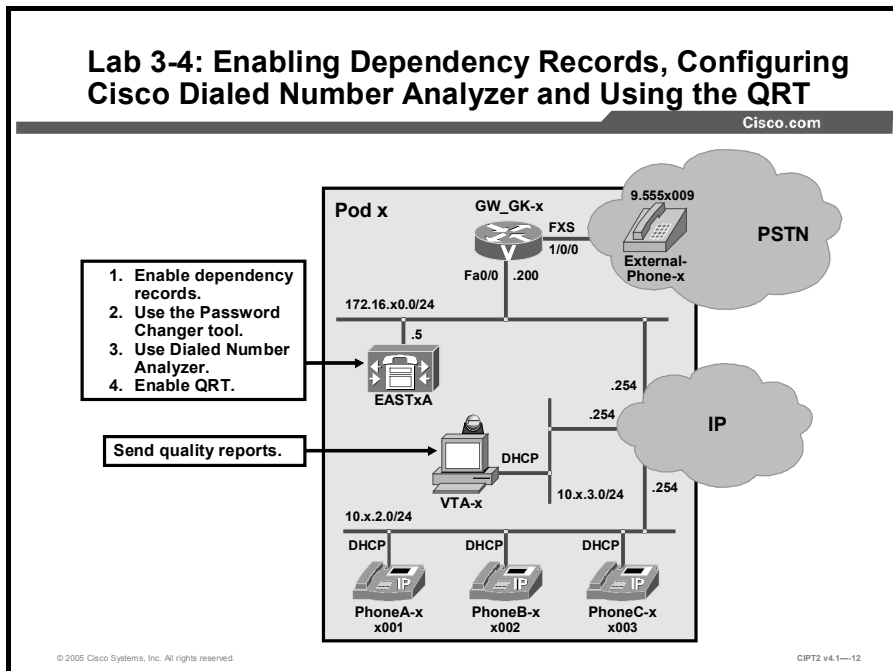
Visual Objective

You will enable dependency records and change the CCMAAdministrator password. Then you will analyze a call with the Cisco Dialed Number Analyzer tool and use QRT to report IP Phone problems.

The figure illustrates what you will accomplish in this activity.

Lab 3-4: Enabling Dependency Records, Configuring Cisco Dialed Number Analyzer and Using the QRT

Cisco.com



Required Resources

These are the resources and equipment that are required to complete this activity:

- The lab devices shown in the Visual Objectives figure and detailed in the table

Lab Devices and Their Roles

Device	Device Role in the Activity
EASTxA	Cisco CallManager publisher that serves the IP Phones
VTA-x	PC where the Cisco VT Advantage software has to be installed
PhoneA-x	Video-enabled IP Phone that has the PC with Cisco VT Advantage connected to it
PhoneB-x, PhoneC-x	IP Phones

- The device credentials in the table, to log in to the lab devices that require authentication

Credentials for Device Access

Device	Username and Password
EASTxA	administrator lab
Cisco CallManager Administration	ccadministrator lab
VTA-x	administrator lab

Job Aids

These job aids are available to help you complete the lab activity.

- The table lists the DNs needed to place calls in the lab activity.

Directory Numbers

Device	Directory Number
PhoneA-x	x001, where x = your pod number
PhoneB-x	x002, where x = your pod number
PhoneC-x	x003, where x = your pod number
PhoneA-y	y001, where y= your partner pod number
PhoneB-y	y002, where y = your partner pod number
PhoneC-y	y003, where y = your partner pod number

- The lab devices use the IP address allocation scheme shown in the table.

IP Address Allocation Scheme

Device	IP Address
Voice server network	172.16.x0.0/24
IP Phone network	10.x.2.0/24
Data network	10.x.3.0/24
Default gateway	Node address .254 (for all networks)
EASTxA	172.16.x0.5
GW_GK-x	172.16.x0.200
PhoneA-x	DHCP-assigned (network 10.x.2.0)
PhoneB-x	DHCP-assigned (network 10.x.2.0)
PhoneC-x	DHCP-assigned (network 10.x.2.0)
VTA-x	DHCP-assigned (network 10.x.3.0)

- Additionally, you will use *Cisco CallManager Administration Guide, Release 4.1(3)*.

Task 1: Enable and View Dependency Records

In this task, you will enable and view dependency records in the Enterprise Parameters window on the EASTxA Cisco CallManager. You will open the default device pool and view the dependency records for that device pool.

Activity Procedure

Complete these steps:

- Step 6** From VTA-x use Internet Explorer to access Cisco CallManager administration on EASTxA and choose **System > Enterprise Parameters**.
- Step 7** Locate the **Enable Dependency Records** parameter and change it from **False** to **True** to activate dependency records.
- Step 8** Click **Update** at the top of the window to save the changes.
- Step 9** Choose **System > Device Pool**.
- Step 10** Click **Find** to list all device pools. Choose the **Default** device pool to open the pool.
- Step 11** In the device pool configuration window, click **Dependency Records** to open the dependency records summary.
- Step 12** In the dependency records overview window, click **Phone** to display all IP Phones that use the device pool Default. Clicking the button opens the Phone Summary window.

Activity Verification

You have completed this task when you attain these results:

- You access the dependency records window through Cisco CallManager Administration.
- You know the number of IP Phones using the device pool Default. You should see at least three IP Phones: PhoneA-x, PhoneB-x, and PhoneC-x.

Task 2: Change the CCMAAdministrator Password

In this task, you will change the CCMAAdministrator password and the Directory Manager password on the EASTxA Cisco CallManager. You will change the CCMAAdministrator password from *lab* to *admin*. You will change the Directory Manager password from *lab* to *cipt2*.

Activity Procedure

Complete these steps:

- Step 1** Open a terminal session to EASTxA from VTA-x (choose **Start > Programs > Accessories > Communications > Remote Desktop Connection**). Use the IP address **172.16.x0.5** for the connection to EASTxA (located on the desktop of your VTA-x PC).
- Step 2** Choose **Start > Run** and enter **CCMPWDChanger**. Click **OK** to open the Password Changer tool. Wait until you are able to enter the password.
- Step 3** In the **Administrator Password** field, enter the directory manager password **lab** and click **Next**.
- Step 4** Enter the user ID **CCMAAdministrator**, and enter the new password **admin** twice. Click **OK** to change the password.
- Step 5** Enter the user ID **Directory Manager** and enter the new password **cipt2** twice. Click **OK** to change the password.
- Step 6** After you change both passwords, click **Exit** to close the Password Changer tool.

Activity Verification

You have completed this task when you attain these results:

- You can use the new password of the Directory Manager account to log in to DC-Directory.
- You can use the new password of the CCMAAdministrator account to log in to Cisco CallManager Administration.

Specifically, complete these steps:

- Step 1** From VTA-x connect to EASTxA using VNC. Choose **Start > Programs > DC Directory Administrator**. Click **Next** to use the default profile. Enter **Directory Manager** as the username and enter the new password **cipt2**. If you are able to log in, the password was changed correctly.
- Step 2** From VTA-x browse to EASTxA Cisco CallManager administration. When you are asked for the username, enter **ccmadministrator** and enter the password **admin**.

Task 3: Analyze Calls with Cisco Dialed Number Analyzer

In this task, you will perform call analysis using the Cisco Dialed Number Analyzer. You will analyze an internal call between PhoneA-x and PhoneB-x and an external call between PhoneA-x and External-Phone-x.

Activity Procedure

Complete these steps:

- Step 1** Use the VNC viewer application on VTA-x and connect to the EASTxA Cisco CallManager. Use the IP address **172.16.x0.5**.
- Step 2** Using Internet Explorer on EASTxA, connect to Cisco CallManager Administration and choose **Application > Install Plugins**. Click the **Cisco Dialed Number Analyzer** icon. Click **Open** when you are asked where the file should be downloaded.
- Step 3** Click **Next** to install the Cisco Dialed Number Analyzer. Enter **lab** as the private password and click **Next**. After the installation is complete, click **Finish** to close the installation program.
- Step 4** Using Internet Explorer on VTA-x, connect to Cisco CallManager Dialed Number Analyzer on EASTxA at **https://172.16.x0.5/DNA**. Log in as **administrator** with the password **lab**.
- Step 5** Choose **Analysis > Analyzer** and enter **x001** as the calling party. Enter **x002** as the dialed digits. Choose **<None>** as the calling search space. To start the analysis, click **Do Analysis**.
- Step 6** Fill out the table with the requested values.

Call Analysis Between Internal Numbers

Result Information	Value
Calling party	
Dialed digits	
Calling search spaces	
Match result	
Partition of the dialed device	
Device type of the dialed device	
Call classification	

- Step 7** Choose **Analysis > Phones** and click **Find** to list all IP Phones. Click **PhoneA-x** to use PhoneA-x for the analysis. Enter **95551009** as the dialed digits to analyze an external call.

Step 8 Fill out the table with the requested values:

Call Analysis Between Internal and External Numbers

Result Information	Value
Calling party	
Dialed digits	
Calling search spaces	
Match pattern	
Called-party transformations	
Device type	
Call classification	

Activity Verification

You have completed this task when you attain this result:

- You have completely filled out the call analysis tables in the activity procedure.

Task 4: Add the QRT Softkey to the Cisco IP Phone

In this task, you will add the QRT softkey to the IP Phones. You will perform this configuration for the softkey template Standard User CIPT2, which you must create.

Activity Procedure

Complete these steps:

- Step 1** Using Internet Explorer on VTA-x, connect to Cisco CallManager Administration on EASTxA.
- Step 2** Choose **Device > Device Settings > Softkey Template** and click **Find** to list all available softkey templates.
- Step 3** Click **Standard User** to open the standard user template. Click **Copy** to copy the template. Change the softkey template name to **Standard User CIPT2**. Click **Insert** to save the template.
- Step 4** Click **Configure Softkey Layout** to configure the softkey layout for the Standard User CIPT2 template.
- Step 5** Click **Connected**, and move **Quality Report Tool** from the Unselected Softkeys pane to the Selected Softkeys pane by selecting it and clicking the Right arrow. Click **Update** to save the changes.
- Step 6** Click **Connected Conference**, and move **Quality Report Tool** from the Unselected Softkeys pane, using the Right arrow, to the Selected Softkeys pane. Click **Update** to save the changes.
- Step 7** Click **Connected Transfer**, and move **Quality Report Tool** from the Unselected Softkeys pane, using the Right arrow, to the Selected Softkeys pane. Click **Update** to save the changes.

- Step 8** Click **On Hook**, and move **Quality Report Tool** from the Unselected Softkeys pane, using the Right arrow, to the Selected Softkeys pane. Click **Update** to save the changes.
- Step 9** Choose **System > Device Pool** and click **Find** to list all available device pools. Choose the **Default** device pool and change the Softkey Template value to **Standard User CIPT2**.
- Step 10** Click **Update** to save your changes. Click **Reset Devices** to reset all devices in the device pool Default.
- Step 11** Choose **Application > Cisco CallManager Serviceability > Tools > Service Activation** to activate QRT. Click the first available server in the left column, and check the **Cisco Extended Functions** check box to activate the service. Click **Update** to save your changes.

Activity Verification

You have completed this task when you attain this result:

- You verify that the QRT softkey is displayed on all IP Phones.

Specifically, complete these steps:

- Step 1** Verify that the QRT softkey for PhoneA-x is displayed. On the IP Phone (in the On Hook state), press the **More** button. Locate the softkey labeled **QRT**. Its presence indicates that the QRT softkey is correctly configured for the IP Phone.
- Step 2** Repeat this verification step for PhoneB-x and PhoneC-x.

Task 5: Generate Problem Reports

In this task, you will generate problem reports using the QRT softkey on the IP Phones. PhoneA-x will generate a report during a call to PhoneB-x, and PhoneC-x will generate a report while it is on hook.

Activity Procedure

Complete these steps:

- Step 1** Place a call from PhoneA-x to PhoneB-x. On PhoneA-x, dial the PhoneB-x number (x002).
- Step 2** During the call between PhoneA-x and PhoneB-x, press the PhoneA-x **More** softkey until the QRT softkey is displayed. Press the **QRT** softkey to write a report. Wait for about 10 seconds so that enough data can be collected and press the **Exit** softkey on PhoneA-x. Hang up PhoneA-x and PhoneB-x.
- Step 3** Press the PhoneB-x **More** softkey until the QRT softkey is displayed (do not take the IP Phone off-hook). Press the **QRT** softkey. Choose **Problems with last call** from the menu and press **I heard echo**. Press the **Exit** softkey.

Note You are not simulating the scenario that an echo was heard on PhoneB-x. You are just reporting that you heard an echo on PhoneB-x.

Step 4 Press the PhoneC-x **More** softkey until the QRT softkey is displayed. Press the **QRT** softkey. Choose **Can't make calls** from the menu and press **I get a busy tone**. Press the **Exit** softkey.

Note You are not simulating the scenario that you heard a busy tone on PhoneC-x. You are just reporting that you heard a busy tone on PhoneC-x.

Activity Verification

You have completed this task when you attain this result:

- You have successfully generated various QRT reports.

Specifically, complete these steps:

Step 1 Press the **QRT** softkey on PhoneA-x, and you see a message on your IP Phone display that the audio quality data will be collected and logged.

Step 2 Press the **QRT** softkey and the corresponding issue message on PhoneC-x. You should get a message that the feedback has been logged.

Note The QRT softkey can be pressed in two situations: during a call and while being on-hook (after a call or after trying to place a call). Depending on the situation, the IP Phone dialog will prompt for different input (for each situation there are different possible problem descriptions), send different information in the problem report (for instance, delay and jitter values are collected if in an active call), and display different information at the IP Phone after sending the problem report ("audio data are collected and logged" versus "feedback has been logged").

Task 6: View IP Phone Problem Reports

In this task, you will inspect previously generated IP Phone problem reports (from Task 5). You will use QRT on the EASTxA Cisco CallManager.

Activity Procedure

Complete these steps:

Step 1 From VTA-x use Internet Explorer to access Cisco CallManager administration on EASTxA and choose **Application > Cisco CallManager Serviceability > Tools > QRT Viewer**.

Step 2 Choose the day that is shown on the IP Phone display of PhoneA-x as the time frame. After you choose the time frame, click **Get Logs**.

Step 3 In the Extension Number field, choose **All** to show all cases for all destination numbers. Choose **All** in the Device and Category fields.

Step 4 In the Fields to Display area, choose any fields that are of interest to you, but choose at least **Date, Category, Reason Code, Source Device Name, Source Device DN, Dest. Device Name, and Dest. Device DN**. After moving them into the Selected Fields pane, click **Display Records**.

Activity Verification

You have completed this task when you attain these results:

- The QRT overview window shows the cases generated in Task 6:
 - **PhoneA-x:** The QRT overview window shows that PhoneA-x had a problem with the current call.
 - **PhoneB-x:** The QRT overview window shows that PhoneB-x produced an echo during a call.
 - **PhoneC-x:** The QRT overview window shows that PhoneC-x resulted in a busy tone when the user tried to place a call.

Lab 3-4 Answer Key: Enabling Dependency Records, Configuring Cisco Dialed Number Analyzer, and Using QRT

When you complete this activity, your solution will be similar to this, with differences that are specific to your device or workgroup.

Task 1: Enable and View Dependency Records

The configuration to enable and view dependency records should look similar to this figure.

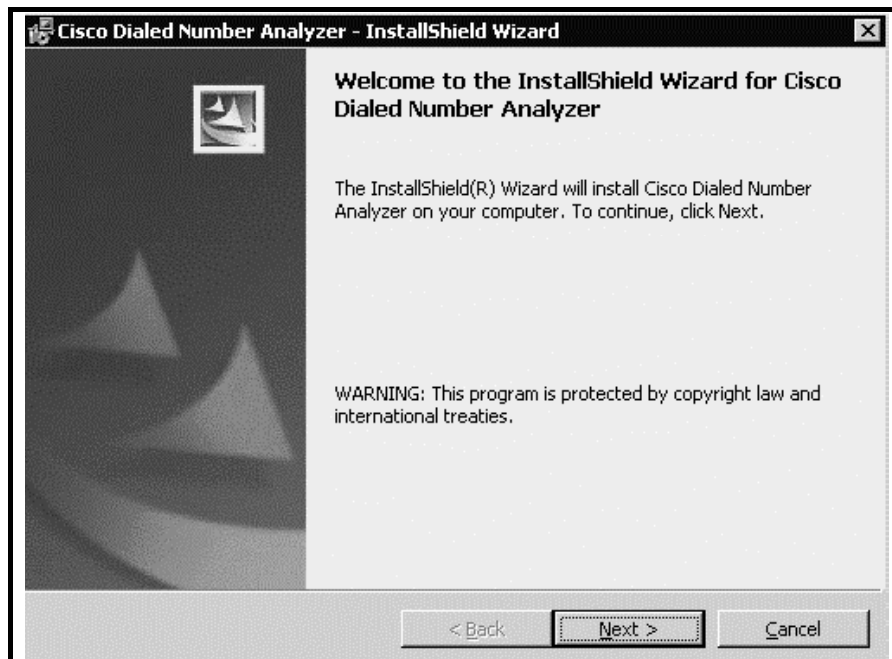


Enable Dependency Records* True False

Task 3: Analyze Calls with Cisco Dialed Number Analyzer

Call analysis results using Cisco Dialed Number Analyzer should look similar to these figures:

- Installation of Cisco Dialed Number Analyzer



- An analysis request for a call from x001 to x002

Analysis Service Help

Cisco Dialed Number Analyzer

For Cisco IP Telephony Solutions

Analyzer

Analyzer Input

Calling Party*

Dialed Digits*

Calling Search Space

Device Time Zone

Time Zone

Date - - (YYYY - MON - DD)

Time : : : (HH : MM : SS : MS)

* indicator, required item

- The result of the analysis for a call from x001 to x002

Cisco Dialed Number Analyzer

For Cisco IP Telephony Solutions

Dialed Number Analyzer Results

- [-] **Results Summary**
 - [+] **Calling Party Information**
 - Dialed Digits = 1002
 - Match Result = RouteThisPattern
 - [+] **Matched Pattern Information**
 - Called Party Number = 1002
 - Time Zone =
 - InterDigit Timeout = NO
 - Allow Device Override = Disabled
 - Outside Dial Tone = NO
 - [+] **Call Flow**
 - [+] **Alternate Matches**

Note Do not allow the results displayed here to confuse you. All values shown are examples only and may be different in your scenario.

- Locating PhoneA-x in Cisco Dialed Number Analyzer by first searching for all IP Phones

The screenshot shows the Cisco Dialed Number Analyzer interface. At the top, there are navigation tabs for 'Analysis', 'Service', and 'Help'. The main header reads 'Cisco Dialed Number Analyzer For Cisco IP Telephony Solutions'. Below this is a section titled 'Find and List Phones'. It displays '3 matching record(s) for Device Name begins with ""'. There is a search form with a dropdown for 'Device Name', a dropdown for 'begins with', and a 'Find' button. Below the search form, it says 'and show 20 items per page' and 'Allow wildcards' is checked. A table of matching records is shown below, with columns for Device Name, Description, Device Pool, Status, and IP Address. The table lists three devices: SEP000F23984C08 (PhoneC-1), SEP000F23AC5700 (PhoneB-1), and SEP000F24F29B2D (PhoneA-1).

Device Name	Description	Device Pool	Status	IP Address
SEP000F23984C08	PhoneC-1	Default	10.1.1.1	10.1.2.2
SEP000F23AC5700	PhoneB-1	Default	10.1.1.1	10.1.2.1
SEP000F24F29B2D	PhoneA-1	Default	10.1.1.1	10.1.2.3

Note Do not allow the results displayed here to confuse you. All values shown are examples only and may be different in your scenario.

- The Phone Line Selection window Dialed Digits field

The screenshot shows the 'Phone Line Selection' window. At the top right, there is a 'Back to Find/L' link. The main content area displays the following information: 'Phone: SEP000F24F29B2D (PhoneA-1)', 'Registration: Registered with Cisco CallManager 10.1.1.1', and 'IP Address: 10.1.2.3'. Below this is a section titled 'Phone Configuration (Model = Cisco 7940)'. Underneath, there is a 'Device Information' section with a table of configuration details. At the bottom, there is a 'Select a Line' section with a table of available lines. The 'Diald Digits*' field is set to '95551009'.

Line	Device Name (Line)	Extension	Partition	Calling Search Space
1	SEP000F24F29B2D (1)	1001	< None >	< None >

- The results of the Cisco Dialed Number Analysis for PhoneA-x

Cisco Dialed Number Analyzer

For Cisco IP Telephony Solutions

Dialed Number Analyzer Results

- [-] **Results Summary**
 - [+] **Calling Party Information**
 - **Dialed Digits** = 95551009
 - **Match Result** = RouteThisPattern
 - [+] **Matched Pattern Information**
 - **Called Party Number** = 5551009
 - **Time Zone** =
 - **End Device** = AALN/S1/SU0/0@GW_GK-1
 - **Call Classification** = OffNet
 - **InterDigit Timeout** = NO
 - **Allow Device Override** = Disabled
 - [+] **Outside Dial Tone**
 - [+] **Call Flow**
 - [+] **Alternate Matches**

Note Do not allow the results displayed here to confuse you. All values shown are examples only and may be different in your scenario.

Task 4: Add the QRT Softkey to the Cisco IP Phone

The configuration of the QRT softkey for the IP Phone should look similar to these figures:

- The new user template Standard User CIPT2

The screenshot shows the Cisco CallManager Administration interface. The main heading is "Find and List Softkey Templates" with a link "Add a New Softkey Template". Below the heading, it indicates "6 matching record(s) for Name begins with """. There are search filters for "Name" and "begins with", and a "Find" button. It also shows "and show 20 items per page, where softkey template is Both". A table lists the matching records:

<input type="checkbox"/>	Name	Description	Copy
<input type="checkbox"/>	Standard IPMA Assistant	Standard template for IPMA assistant inter...	
<input type="checkbox"/>	Standard User	Standard Softkey Template for CallManager ...	
<input type="checkbox"/>	Standard Feature	Standard Softkey Template for CM Combined ...	
<input type="checkbox"/>	Standard User CIPT2	Standard Softkey Template for CallManager ...	

- The softkey layout configuration for the new softkey template

The screenshot shows the "Softkey Layout Configuration" page for the "Standard User CIPT2" template. The status is "Ready". There are "Update" and "Restart Devices" buttons. The page is divided into "Unselected Softkeys" and "Selected Softkeys (ordered by position)**".

Unselected Softkeys:

- Immediate Divert (31)(iDivert)
- Remove Last Conference Party (19)
- Toggle Malicious Call Trace (27)(M...
- Undefined (0)(Undefined)

Selected Softkeys (ordered by position):**

- Hold (3)(Hold)
- **End Call (9)(EndCall)
- Transfer (4)(Trnsfer)
- Park (14)(Park)
- Conference (13)(Confm)
- Conference List (30)(ConfList)
- Select (29)(Select)
- Join (15)(Join)
- Direct Transfer (28)(DirTrfr)
- Video Mode Command (33)(VidMoc
- Quality Report Tool (22)(QRT)

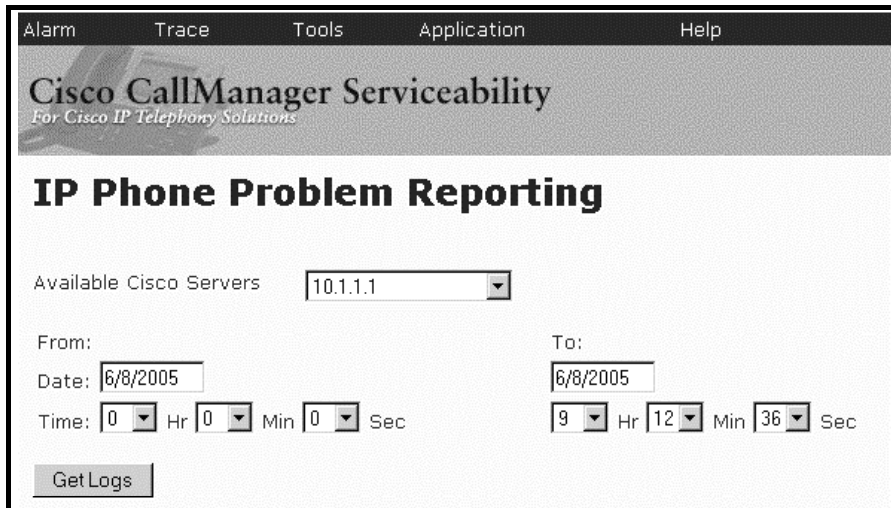
Task 5: Generate Problem Reports

This results of this task cannot be described using figures, because all the steps are carried out on the IP Phones. All tasks on the IP Phones are described in the activity procedure.

Task 6: View IP Phone Problem Reports

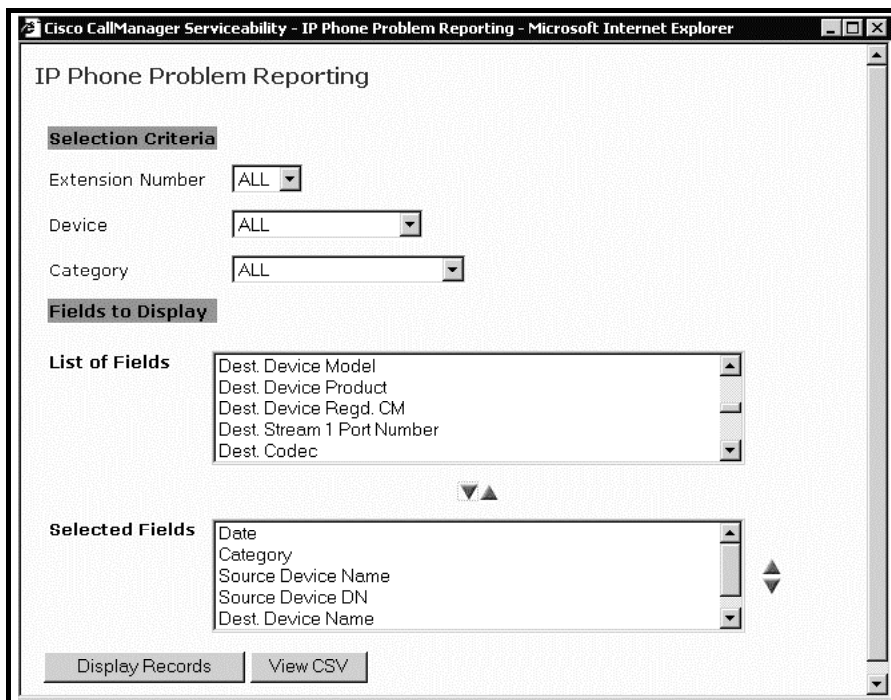
The IP Phone problem reports should look similar to these figures:

- Selecting a time frame for the report



The screenshot shows the Cisco CallManager Serviceability interface for IP Phone Problem Reporting. At the top, there are navigation tabs: Alarm, Trace, Tools, Application, and Help. Below the tabs is the title "Cisco CallManager Serviceability For Cisco IP Telephony Solutions". The main heading is "IP Phone Problem Reporting". Underneath, there is a dropdown menu for "Available Cisco Servers" with "10.1.1.1" selected. Below that are two date and time selection sections. The "From:" section has a date of "6/8/2005" and a time of "0 Hr 0 Min 0 Sec". The "To:" section has a date of "6/8/2005" and a time of "9 Hr 12 Min 36 Sec". At the bottom left of the form is a "Get Logs" button.

- Choosing the fields to display



The screenshot shows the "IP Phone Problem Reporting" page in a Microsoft Internet Explorer browser window. The page has a title bar that reads "Cisco CallManager Serviceability - IP Phone Problem Reporting - Microsoft Internet Explorer". The main heading is "IP Phone Problem Reporting". Below the heading is a "Selection Criteria" section with three dropdown menus: "Extension Number" (set to ALL), "Device" (set to ALL), and "Category" (set to ALL). Below that is a "Fields to Display" section. It contains two list boxes. The "List of Fields" list box contains: "Dest. Device Model", "Dest. Device Product", "Dest. Device Regd. CM", "Dest. Stream 1 Port Number", and "Dest. Codec". The "Selected Fields" list box contains: "Date", "Category", "Source Device Name", "Source Device DN", and "Dest. Device Name". At the bottom of the page are two buttons: "Display Records" and "View CSV".

■ The QRT overview page

IP Phone Problem

[Back to Selection](#) [Right Click here to Save in CSV](#)

SeqId	Date	Category	Source Device Name	Source Device DN	Dest. Device Name	Dest. Device DN
1	06/08/05 08:25:51	Problems with current call	SEP000F24F29B2D	1001	SEP000F23AC5700	1002
2	06/08/05 08:27:00	Problems with last call	SEP000F23AC5700	1002	SEP000F24F29B2D	1001
3	06/08/05 08:27:16	Can't make calls	SEP000F23984C08	1003		

[Back to Selection](#) [Right Click here to Save in CSV](#)