UCSE

Cisco Unified Communications System Engineer

Version 1.3

Student Guide

CLS Production Services: 06.29.05

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

Table of Contents

Volume 1

UCSE

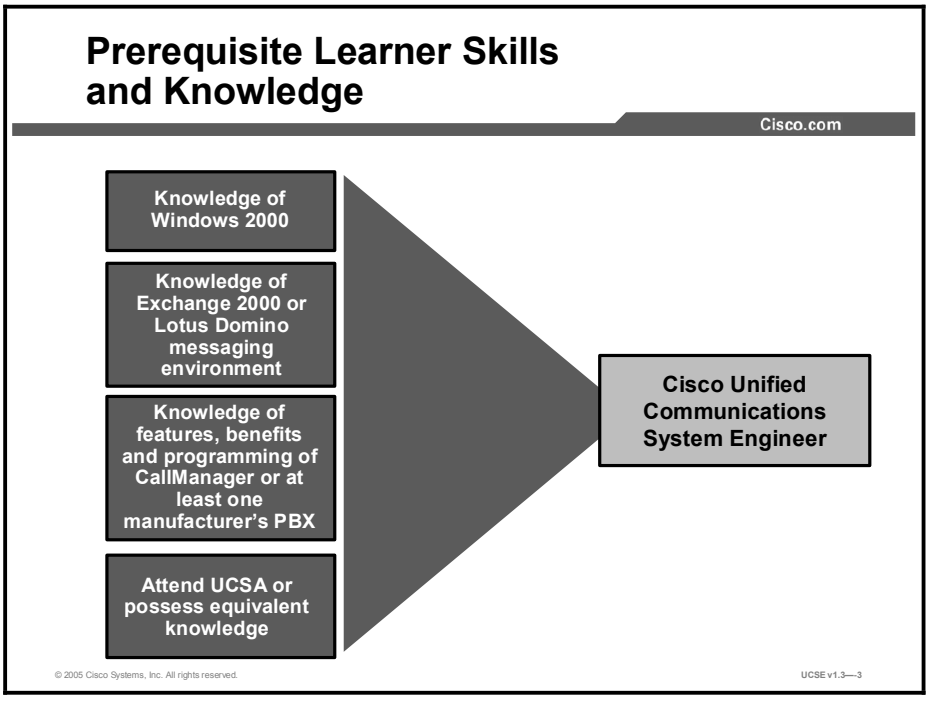
Course Introduction

Overview

The goal of the Cisco Unified Communications System Engineer (UCSE) course is to produce competent system engineers for the Cisco Unity product. Upon completion of this course, system engineers will be able to install, upgrade, configure, maintain, and troubleshoot new and existing Cisco Unity installations. It is the second class in a two-class series, the first being Cisco Unified Communications System Administrator (UCSA). The class partially prepares a student to take the Cisco Unity System Engineer exam (642-104).

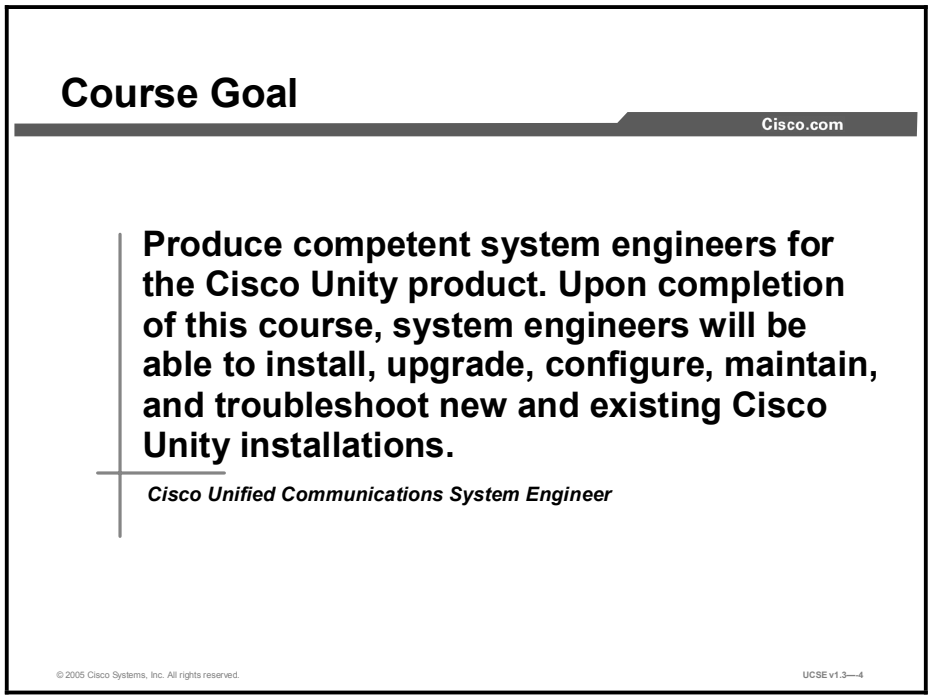
Learner Skills and Knowledge

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.



Course Goal and Objectives

This topic describes the course goal and objectives.

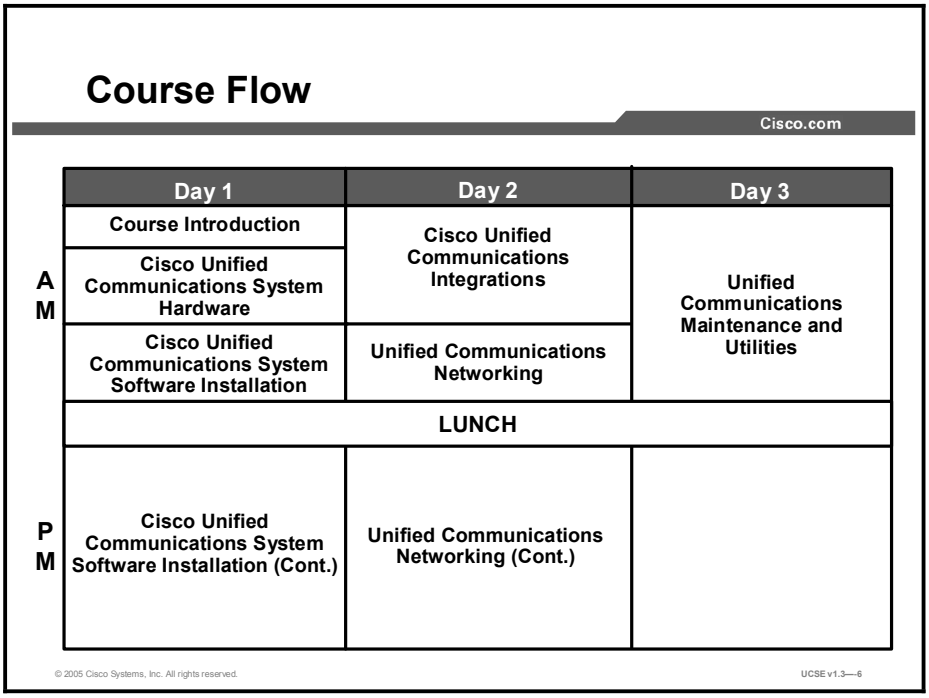


Upon completing this course, you will be able to meet these objectives:

- Determine the appropriate platform to be used as well as the correct voice boards that will meet the minimum hardware requirements for a Cisco Unity system
- Select the correct components and install the software, following the recommended installation sequence, and verify proper operation
- Given an integration scenario with specific components, choose the correct integration type and describe the steps needed to complete the integration
- Select the appropriate type of Cisco Unity networking and subscriber to assure message delivery, message transfer, and directory replication
- Describe and be able to use the appropriate tools to address specific system maintenance, diagnostics, troubleshooting, and reporting problems

Course Flow

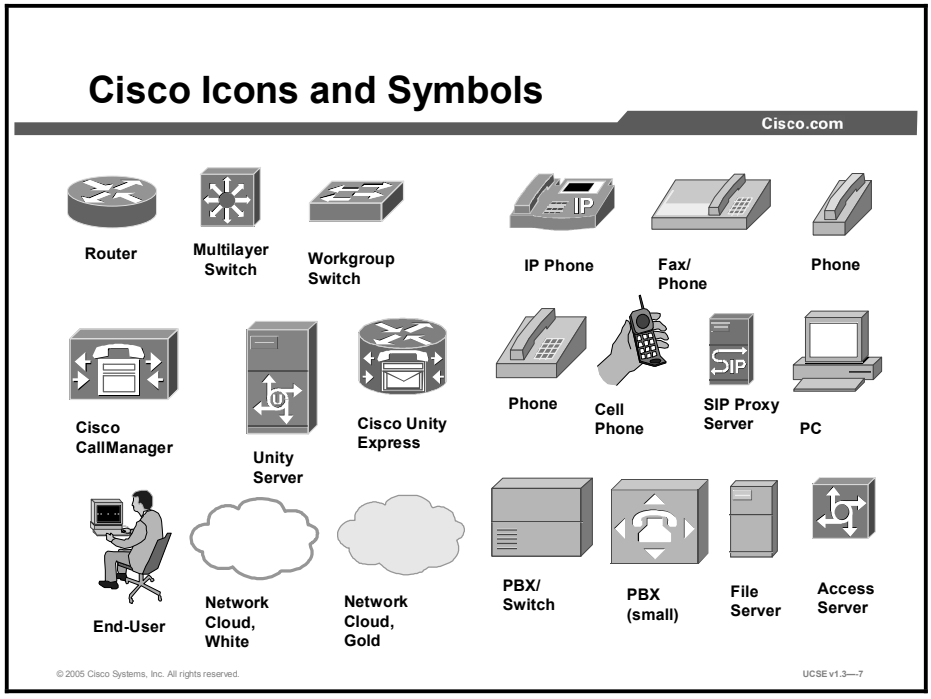
This topic covers the suggested flow of the course materials.



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 exercises. 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.



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 provides three levels of general career certifications for IT professionals with several different tracks to meet individual needs. Cisco also provides focused Cisco Qualified Specialist certifications for designated areas such as cable communications, voice, and security.

There are many paths to Cisco certification, but only one requirement—passing one or more exams demonstrating knowledge and skill. For details, go to http://www.cisco.com/go/certifications.

Module 1

Understanding Cisco Unified Communications System Hardware

Overview

Before installing an operating system or other software, you must first consider the hardware to be used. A system must meet or exceed minimum hardware requirements to perform at acceptable levels. Problems resulting from inadequate hardware can range from unacceptable access times to inability to install the necessary software. Fortunately, it is easy to obtain information about the hardware requirements of a Cisco Unity server. This module describes the platform overlay scheme and the systems that Cisco supplies. The module also describes voice boards, the ancillary hardware needed for a Cisco Unity server working with a circuit-switched PBX, and a Unity Bridge working as an Octel messaging node.

Module Objectives

Upon completing this module, you will be able to determine the appropriate platform to be used as well as the correct voice boards to meet the hardware requirements for a Cisco Unity system. This ability includes being able to meet these objectives:

- Identify if a computer system meets the minimum hardware requirements for a Cisco Unity system, or explain why it does not
- Determine if a voice board that has a particular hardware setup is correct for a Cisco Unity system, or explain how to correct it

Lesson 1

Understanding Unified Communications Server Hardware

Overview

Before installing an operating system or other software, you must first consider the hardware to be used. This lesson describes the platform overlay scheme, as well as the systems that Cisco supplies. By reviewing this information, an engineer will have a good understanding of what it takes to support a Cisco Unity system.

Relevance

A system must meet or exceed minimum hardware requirements to perform at acceptable levels. Problems resulting from inadequate hardware can range from unacceptable access times to inability to install the necessary software.

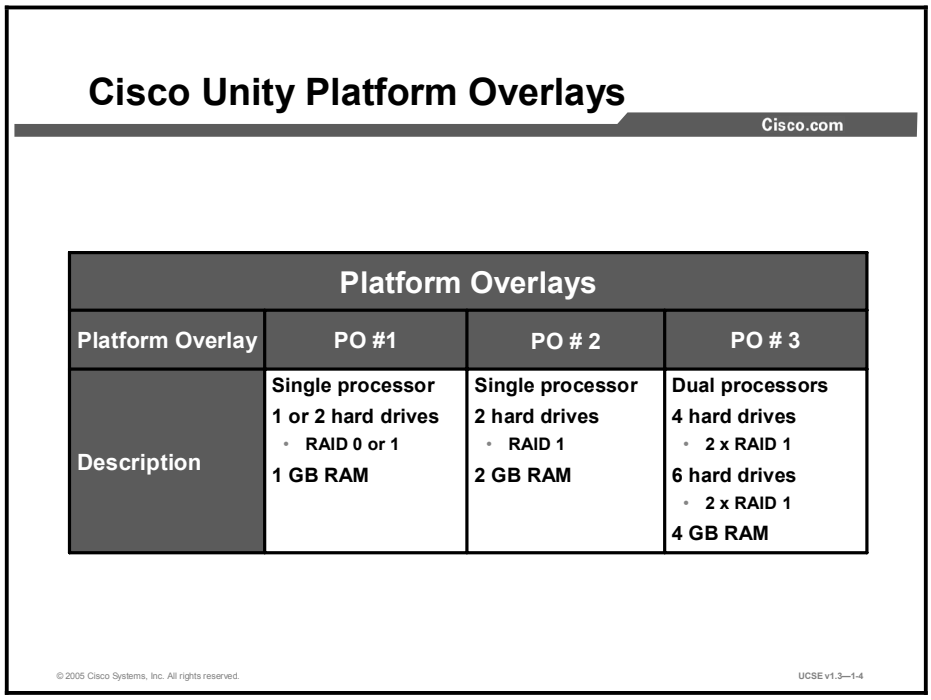
Objectives

Upon completing this lesson, you will be able to determine if a system meets the hardware requirements for a Cisco Unity system or explain why it does not. This ability includes being able to meet these objectives:

- Describe the three platform overlay levels in detail
- Describe the type of information contained on the Cisco Unity Supported Platforms List
- Access the URL for the Cisco Unity Supported Platforms List and display information about the hardware capabilities of a specific server

Cisco Unity Platform Overlays

This topic describes the three platform overlay levels in detail. It gives examples of the types of servers that are qualified at each level and the organization size best served by each.

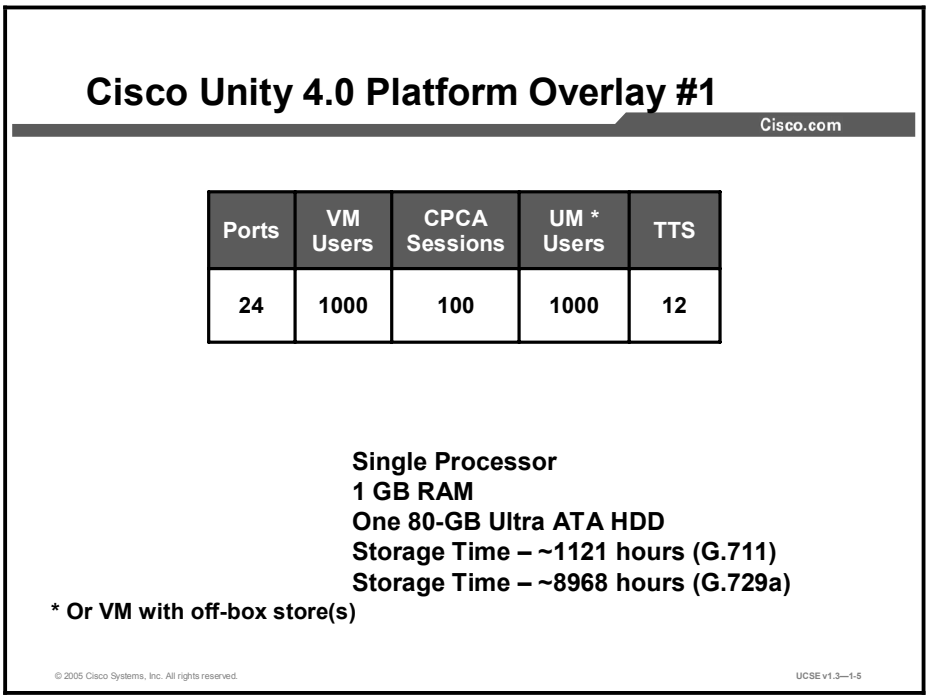


Specifications for computers change frequently. Processor speeds continue to increase; the amount of RAM and available hard drive space continues to increase as well. To address this rapid rate of change, Cisco Systems has chosen to implement platform overlays as a way of describing servers at three different levels of capacity. Platform Overlay #1 is the entry-level server; Platform Overlay #3 is the most robust of the servers. You will look at each platform overlay level in more detail. Examples of servers currently shipped by Cisco Systems and servers available from other suppliers are given at each overlay level. In addition, you will learn about what size of organization could make best use of a server at a particular platform overlay level.

If appropriate, differences between platform overlay levels will be highlighted and explained.

Cisco Unity 4.0 Platform Overlay #1

This topic describes Cisco Unity Platform Overlay #1, which is the basic platform recommended for small systems.

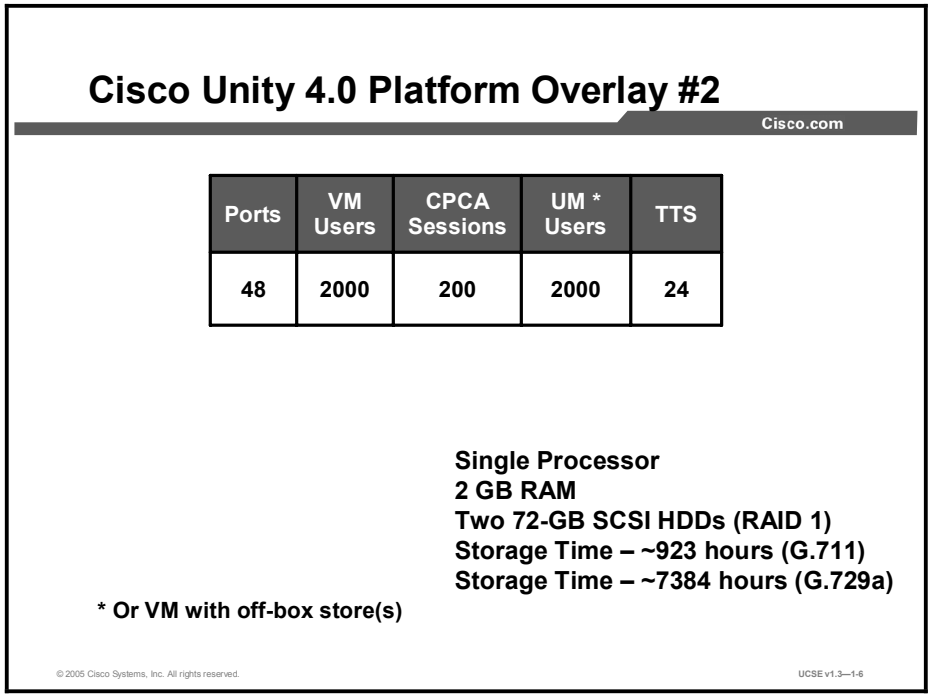


Platform Overlay #1 is an entry-level server appropriate for small systems. It will support up to 24 ports (sessions), 1000 voice-mail or unified messaging users, 12 text-to-speech (TTS) sessions, and 100 Cisco Personal Communications Assistant (CPCA) sessions. The Media Convergence Server (MCS) 7815 system has a single 3.0-GHz Northwood Pentium IV processor, 1.0 GB of RAM, a DVD-ROM drive, and one 80-GB Ultra ATA hard drive.

The storage times given are for voice-mail deployments with a local message store only and are for the two most common recording formats for Cisco Unity messages: G.711 and G.729a. These times assume a 12-GB system partition. Half of addressable drive space is reserved for recovery and Exchange (Voicemail Runtime) Standard Edition. This system would be most appropriate for small office and branch office installations.

Cisco Unity 4.0 Platform Overlay #2

This topic describes Cisco Unity Platform Overlay #2, which is for midsize systems.

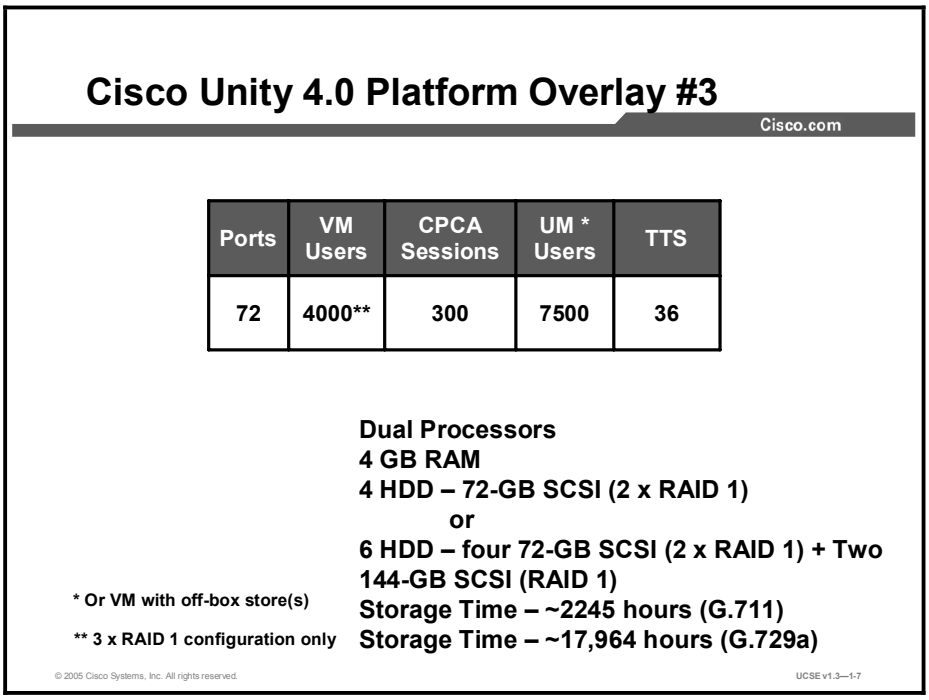


Platform Overlay #2 is appropriate for midsized systems. It will support up to 48 ports (sessions), 2000 voice-mail unified messaging users (or voice-mail users if all message boxes are off-box), 24 text-to-speech sessions, and 200 CPCA sessions. The MCS 7835H and MCS 7835i system has a single Intel Nocona DP-core Xeon 3.4-GHz Pentium IV processor, 2 GB of RAM, a DVD-ROM drive, and two 72-GB SCSI hard drives in a Redundant Array of Independent Disks 1(RAID 1) mirrored configuration.

The storage times given are for voice-mail deployments with a local message store only and are for the two most common recording formats for Cisco Unity messages: G.711 and G.729a. These times assume a 12-GB system partition, half of addressable drive space reserved for recovery and Exchange Standard Edition. This system would be most appropriate for larger office installations where a separate domain controller is needed. The system, with mirrored drives for some fault tolerance, is still somewhat limited in storage space.

Cisco Unity 4.0 Platform Overlay #3

This topic describes Cisco Unity Platform Overlay #3, which is a high-end server that is critical for larger voice-mail and unified messaging systems, for midsize to large customers.

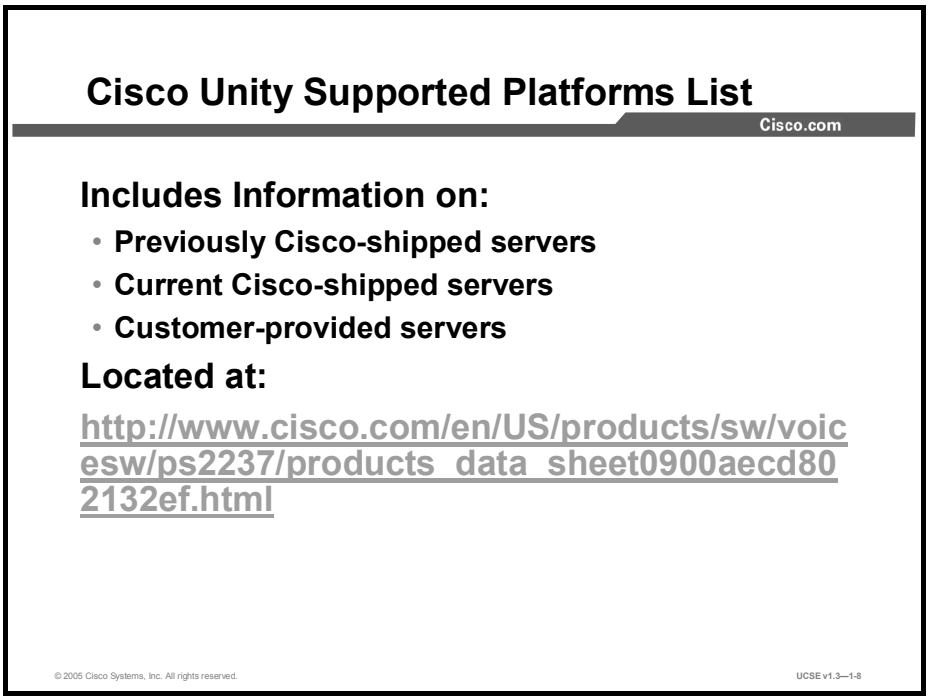


Platform Overlay #3 is appropriate for midsized to large systems. It will support up to 72 ports (sessions), 4000 voice mail or 7500 unified messaging users (or voice-mail users if all message boxes are off-box), 36 text-to-speech sessions, and 300 CPCA sessions. The MCS 7845H and 7845i systems have dual 2.4-GHz Pentium III processors, 4.0 GB of RAM, a DVD-ROM drive, and a choice of hard drive configurations. The systems may have either four 72-GB SCSI drives set up in two RAID 1 configurations, or four 72-GB SCSI drives and two 144-GB SCSI drives with equal capacity drives paired up in a RAID 1 configuration.

The storage times given are for voice-mail deployments with a local message store only and are for the two most common recording formats for Cisco Unity messages: G.711 and G.729a. These times assume a 12-GB system partition, half of addressable drive space reserved for recovery and Exchange Standard Edition. With the addition of a second (or third) mirror set (especially important when used as a voice-mail system or large external message store), this server allows you to separate the Exchange transaction logs from the application logs, allowing for greater performance and minimizing problems from Exchange log stalls.

Cisco Unity Supported Platforms List

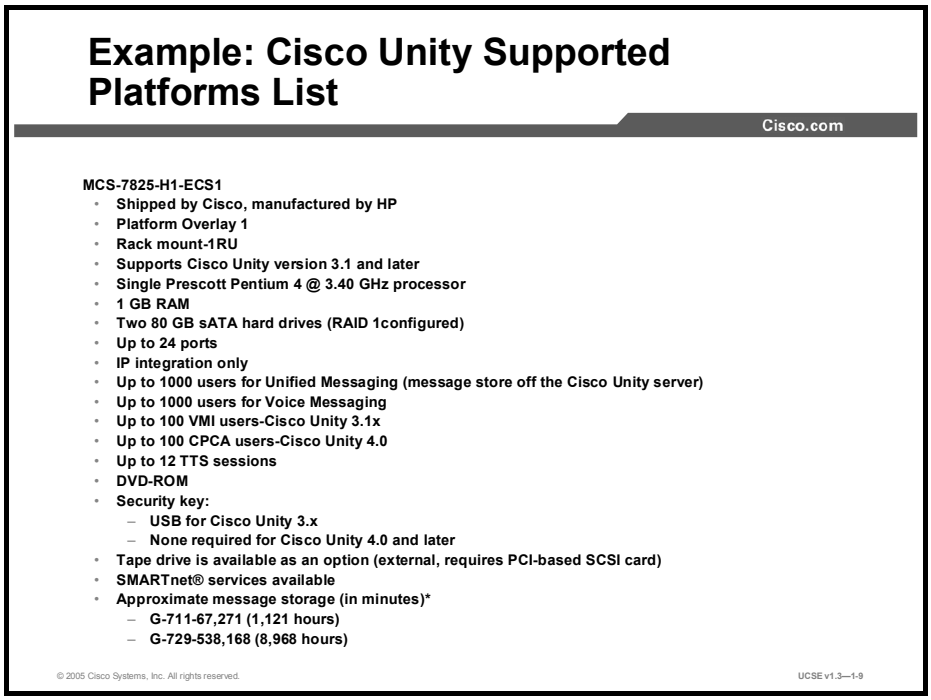
This topic describes the type of information contained on the Cisco Unity Supported Platforms List.



Questions regarding a particular server hardware platform and its ability to run Cisco Unity software are common. Customers may have a server previously shipped by Cisco and want to know if it may be used to run Cisco Unity 4.0, saving the cost of purchasing new server hardware. Customers may elect to purchase servers from a vendor other than Cisco for a variety of reasons. Some of these servers are the same servers that Cisco offers, or original equipment manufacturer (OEM) variants.

Cisco has qualified servers to give partners and end users a variety of choices. The Cisco Unity Supported Platforms List serves as the Cisco hardware compatibility list. The specifications provided for each server are the specifications tested with Cisco Unity. The list is kept up-to-date and contains the most current information about what servers may be used with Cisco Unity, and is available at the following URL:

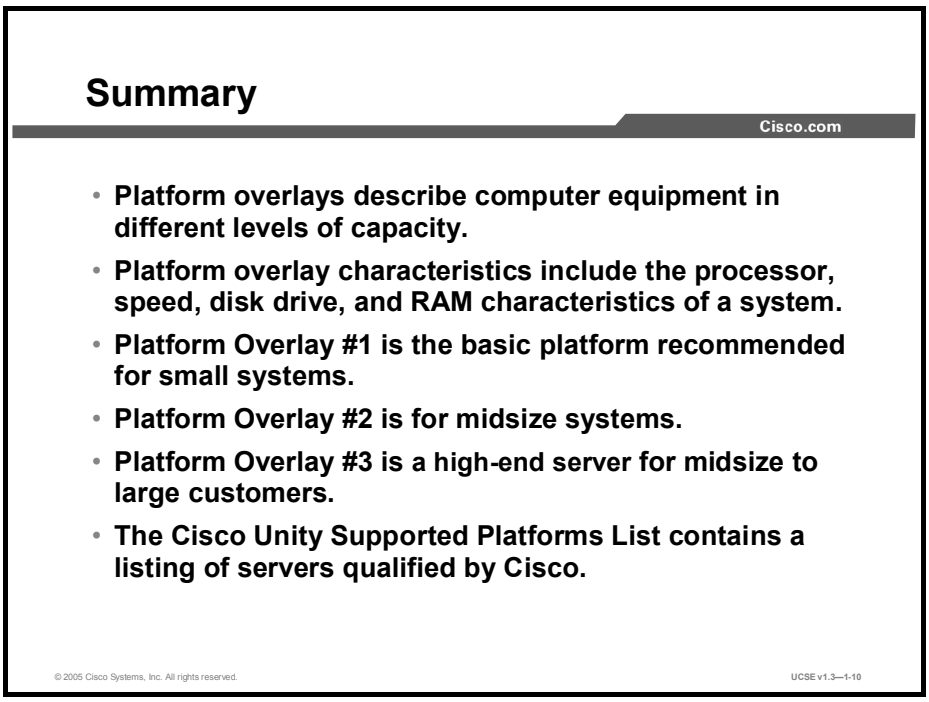
http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_data_sheet0900aecd802132ef.html



The information on the slide is an example of information found on the Cisco Unity Supported Platforms List. Detailed information about the server hardware capabilities, as well as the Cisco Unity feature support levels, is given in the document.

Summary

This topic summarizes the key points discussed in this lesson.



References

For additional information, refer to these resources:

- http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_data_sheet0900aecd802132ef.html

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) Match the Platform Overlay on the left with its description on the right:

A)	Platform Overlay #1	___1. Two processors, 4 GB RAM
B)	Platform Overlay #2	___2. One processor, two hard drives, 2 GB RAM
C)	Platform Overlay #3	___3. One processor, one hard drive, 1.0 GB RAM

Q2) Which of the following Platform Overlays would be appropriate for an application where performance is critical?

A) Platform Overlay #1
B) Platform Overlay #2
C) Platform Overlay #3

Q3) Which of the following Platform Overlays would be appropriate for a midsize company of fewer than 1000 users?

A) Platform Overlay #1
B) Platform Overlay #2
C) Platform Overlay #3

Quiz Answer Key

Q1) A-3; B-2; C-1

Relates to: Cisco Unity Platform Overlays

Q2) C

Relates to: Cisco Unity 4.0 Platform Overlay #3

Q3) B

Relates to: Cisco Unity 4.0 Platform Overlay #2

Lesson 2

Using Unified Communications Voice Boards

Overview

Voice boards enable you to integrate Cisco Unity with a circuit-switched PBX, either alone or in combination with a Cisco CallManager. You may also use voice boards in a Cisco Unity Bridge server to communicate with an Octel voice-mail node. The PBX that you integrate with dictates which voice board(s) you use, and the number of voice-mail ports that will be connected to that switch determines the number of boards.

Relevance

All voice boards in a Cisco Unity system run as a service upon which Cisco Unity is dependent. As you bring a Cisco Unity server on line, the voice board service must first initialize. If, for some reason, the voice boards do not initialize and start their service properly, Cisco Unity will be unable to start. In this lesson, you will learn how to configure voice boards correctly to avoid one cause of these difficulties.

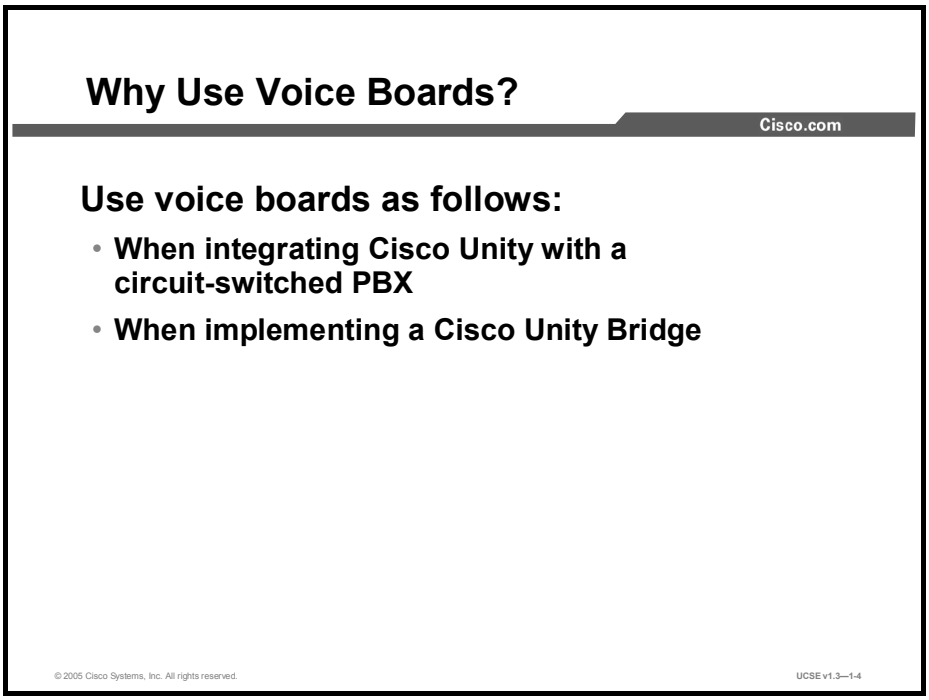
Objectives

Upon completing this lesson, you will be able to determine if the setup is correct for a Cisco Unity system, or explain how to correct it. This ability includes being able to meet these objectives:

- Describe when a voice board is required
- Describe the functions performed by voice boards in a Cisco Unity system
- Describe installing and configuring voice boards
- Describe the Intel Dialogic D/41EPCI, D/41JCT-LS, and D/41JCT-Euro voice boards
- Describe the configuration of the Intel Dialogic D/120JCT-LS and D/120JCT-Euro voice boards
- Describe the configuration of the Intel Dialogic D/240PCI-T1 voice board
- Describe the configuration of the Brooktrout Technology TR114+P4L voice board

Why Use Voice Boards?

This topic describes the situations for which a voice board is necessary and then describes what functions voice boards perform.

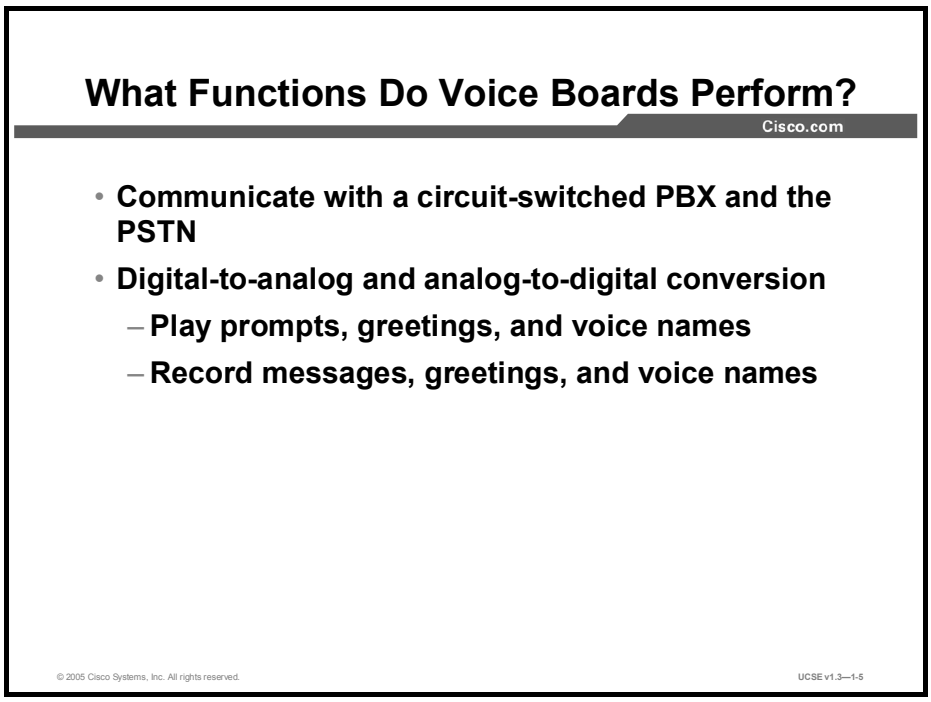


When you integrate a Cisco Unity system with Cisco CallManager, all communications between the two systems take place over the LAN or WAN that they are both connected to. When you connect Cisco Unity with any circuit-switched PBX, you must provide a channel of communication between the devices. Circuit-switched PBXs are designed to provide service to telephone extensions. Any device connected to a PBX must therefore act like a telephone. Voice boards do this for Cisco Unity. You can think of a voice board as a collection of 4, 12, or 24 single-line extensions on one card.

Cisco Unity Bridge communicates with Octel voice-mail systems over the Public Switched Telephone Network (PSTN) using the Octel analog messaging protocol. Voice boards in the Cisco Unity Bridge system provide it with a way to communicate with the PSTN and the Octel system.

What Functions Do Voice Boards Perform?

This topic describes the functions that voice boards perform.



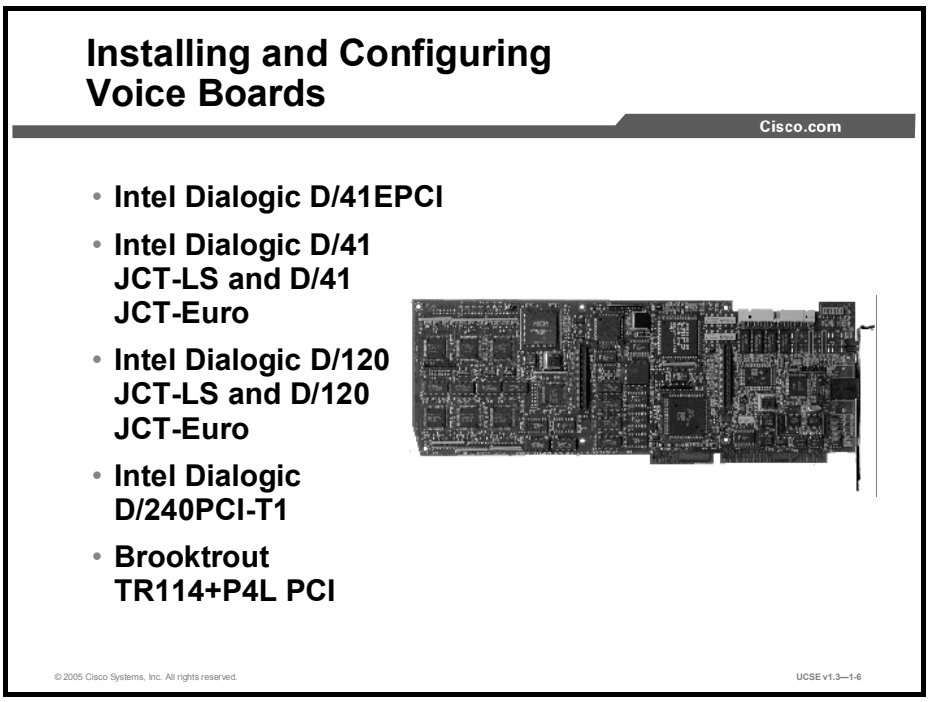
With a combination of hardware and software, voice boards perform the same functions any person performs when using a telephone. A voice board can initiate a call; send dual tone multifrequency (DTMF) tones to dial a number; interpret sound energy on the open phone line as dial tone, ringing, or busy signals; and interpret DTMF tones it receives.

The second function that voice boards perform is digital-to-analog conversion, necessary when playing digital files received from Cisco Unity (such as system prompts or a recorded greeting) over an analog PSTN so that a subscriber or outside caller may understand them. Voice boards also provide analog-to-digital conversion, necessary when a message is spoken over the telephone network and must then be converted into a digital file to reside on a hard drive of a server.

In order for the interface between Cisco Unity and a circuit-switched PBX to work correctly, programming changes need to be made on both Cisco Unity and the PBX. Those configuration changes are detailed in integration guides specific to each PBX. Integration guides are available at the following location:
http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_configuration_guides_list.html

Installing and Configuring Voice Boards

This topic describes installing and configuring voice boards.

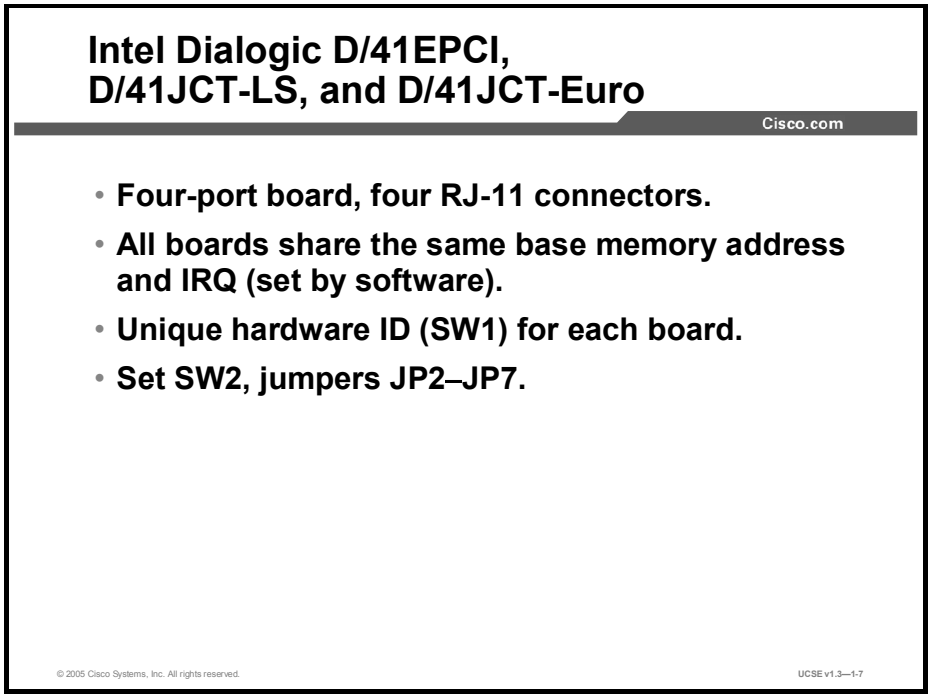


There are several voice boards designed to work with Cisco Unity. The Intel Dialogic boards are primarily used to connect Cisco Unity to a circuit-switched PBX system. The Brooktrout board is primarily used in conjunction with the Cisco Unity Bridge.

If Windows Server 2003 is installed on the Cisco Unity server, voice cards and Dialogic software will not function correctly. Consequently, circuit-switched phone system integrations that use voice cards are not supported for use with a Cisco Unity server on which Windows Server 2003 is installed. Note, however, that IP integrations (Cisco CallManager and session initiation protocol [SIP]) and PBX IP Media Gateway (PIMG) integrations are supported for use with a Cisco Unity server on which Windows Server 2003 is installed.

Intel Dialogic D/41EPCI, D/41JCT-LS, and D/41JCT-Euro Voice Boards

This topic describes the Intel Dialogic D/41EPCI, D/41JCT-LS, and D/41JCT-Euro voice boards.



The Intel Dialogic D/41EPCI, D/41JCT-LS, and D/41JCT-Euro voice cards are used for all circuit-based switches using DTMF or Simplified Message Desk Interface (SMDI) integration. These cards are all four-port digital signal processor (DSP) boards with four RJ-11 connectors.

All of the boards in one system share the same interrupt request (IRQ) and base memory address. You will set SW2 switches to the off position and set jumpers JP2 through JP7 as shown in the *Cisco Unity Installation Guide*. There is a 16-position rotary switch (SW1) that manually identifies each board in a system; set the first board to ID 1, the second to ID 2, and so on.

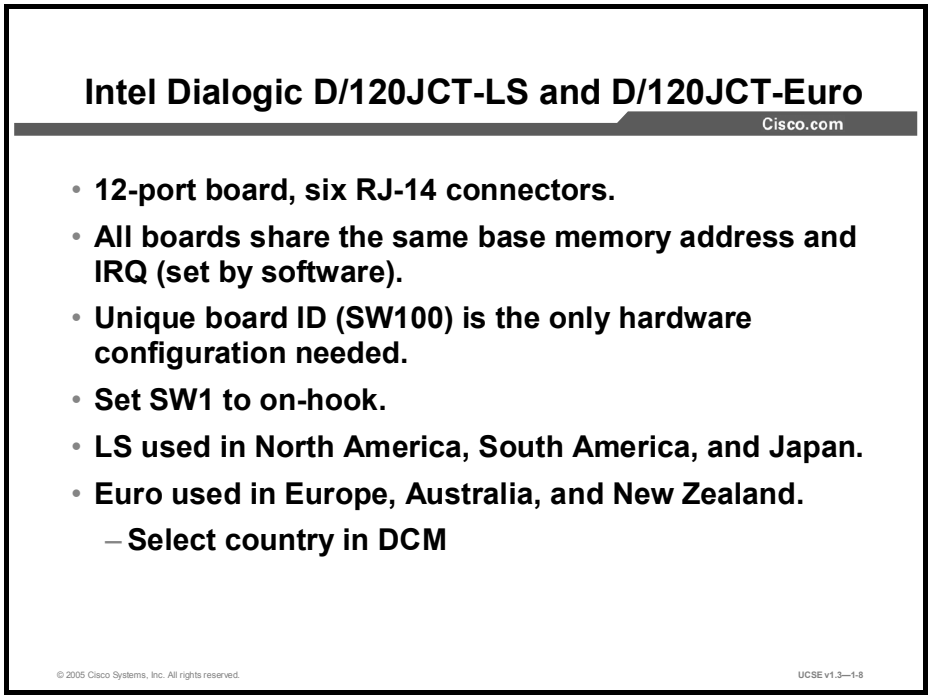
You can configure each board using Dialogic Configuration Manager (DCM). This utility writes information into the registry. Specific information about the configuration of each board in the D/41series is contained in the *Cisco Unity Installation Guide*, Appendix A. For complete diagrams of the connection pinouts for these voice boards, see the *Cisco Unity Installation Guide*: Installing Voice Boards.

Cisco recently announced the end of life of the D/41EPCI card, the four-port analog voice, conventional protocol control information (PCI), five volts direct current (5-VDC) card. Existing Cisco Unity servers upgrading to Version 4.0(5) or later may continue to use the card, but no new cards are being sold. Deployments requiring analog integrations between Cisco Unity software and a legacy PBX should use the newer Universal PCI form factor voice cards(D/41JCT-LS and D/41 JCT-Euro), which are available in both North American and Western European variants. There is no direct replacement for a four-port analog card in the older, non-universal (conventional 5-VDC PCI) form factor.

Cisco will continue to support Cisco Unity installations using the D/41EPCI card through September 25, 2009. For more details about the end-of-sale and end-of-life announcement and other related dates of service use the following link:
http://www.cisco.com/en/US/partner/products/sw/voicesw/ps2237/prod_eol_notice09186a008020b3c8.html

Intel Dialogic D/120JCT-LS and D/120JCT-Euro Voice Boards

This topic describes the Intel Dialogic D/120JCT-LS and D/120JCT-Euro voice boards.



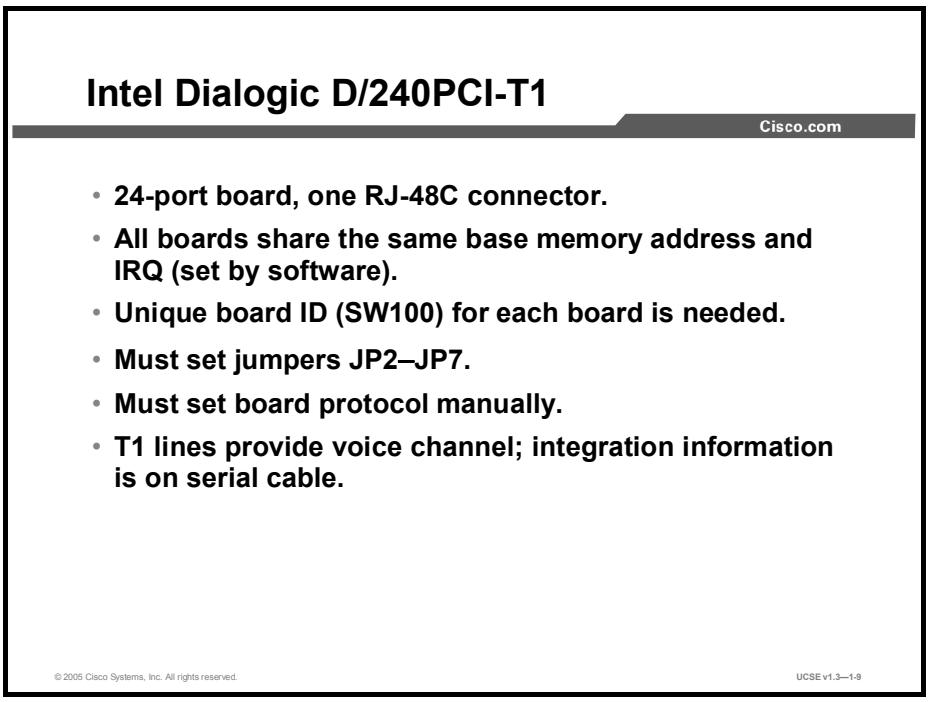
The Intel Dialogic D/120JCT-LS and D/120JCT-Euro voice cards are 12-port DSP boards using six RJ-14 connectors; Ports 1 and 2 use the top connector; Ports 11 and 12 use the bottom.

All of the boards in one system share the same IRQ and base memory address. There is a 16-position rotary switch (SW100) that manually identifies each board in a system; set the first board to ID 1, the second to ID 2, and so on. You must set SW1 to on-hook for each board, otherwise the board will not answer calls.

Configure each board using DCM. The utility writes information into the registry. Specific information about the configuration of each D/120JCT-LS or D/120JCT-Euro board is contained in the *Cisco Unity Installation Guide*, Appendix A. For complete diagrams of the connection pinouts for these voice boards, see the *Cisco Unity Installation Guide*: Installing Voice Boards.

Intel Dialogic D/240PCI-T1 Voice Board

This topic describes the Intel Dialogic D/240PCI-T1 voice board.



The Intel Dialogic D/240PCI-T1 voice board is a 24-port DSP board that uses one RJ-48C connector. All boards in one system share the same IRQ and base memory address. Cisco is migrating toward replacing this board with PIMG technology.

The 16-position rotary switch (SW100) manually identifies each voice board in a system. Set the first board to ID 1, the second to ID 2, and so on.

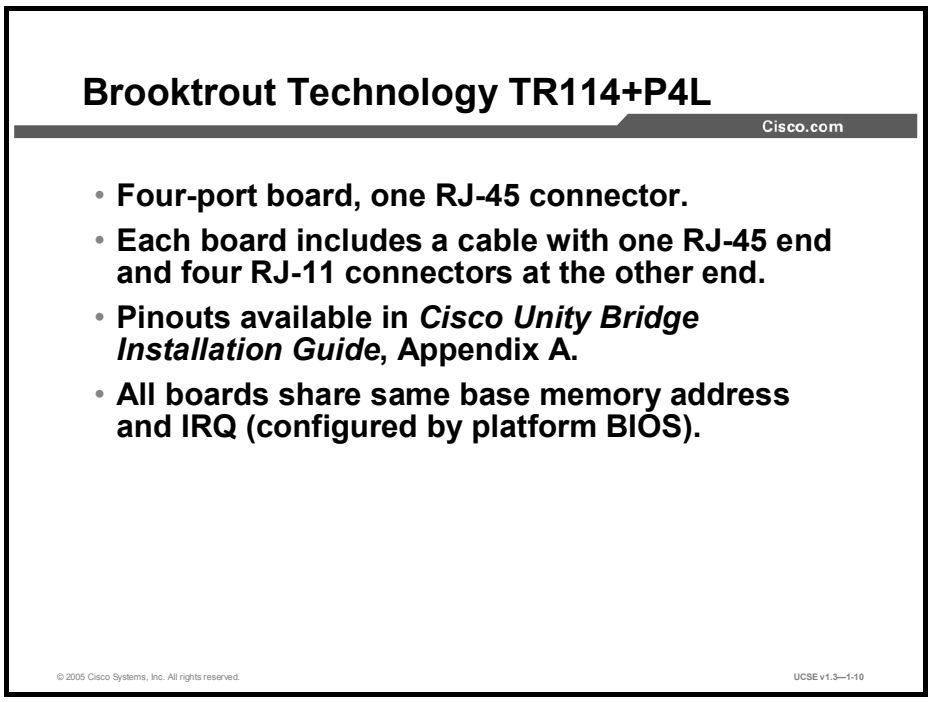
Configure each voice board using the DCM. This utility writes information into the registry. Configure the voice board protocol using the instructions in Appendix A of the *Cisco Unity Installation Guide*. For complete diagrams of the connection pinouts for these voice boards, see the *Cisco Unity Installation Guide*: Installing Voice Boards.

Cisco recently announced the end of life of the D/240PCI-T1 card, the 24-port T1 voice PCI card. Existing Cisco Unity servers upgrading to version 4.0(5) or later may continue to use the card, but no new cards are being sold. There is no direct replacement for a T1 voice card qualified for use with Cisco Unity software. Additional analog (4-port or 12-port) serial or digital integrations between Cisco Unity software and some of the PBXs listed below may be possible. Contact your Cisco account team representative for information about the Cisco Systems out-of-box qualification process.

Cisco will continue to support Cisco Unity installations using the D/240PCI-T1 card through September 25, 2009. For more details about the end-of-sale and end-of-life announcement and other related dates of service, use the following link:
http://www.cisco.com/en/US/partner/products/sw/voicesw/ps2237/prod_eol_notice09186a008020b3c8.html

Brooktrout Technology TR114+P4L Voice Board

This topic describes the Brooktrout Technology TR114+P4L voice board.

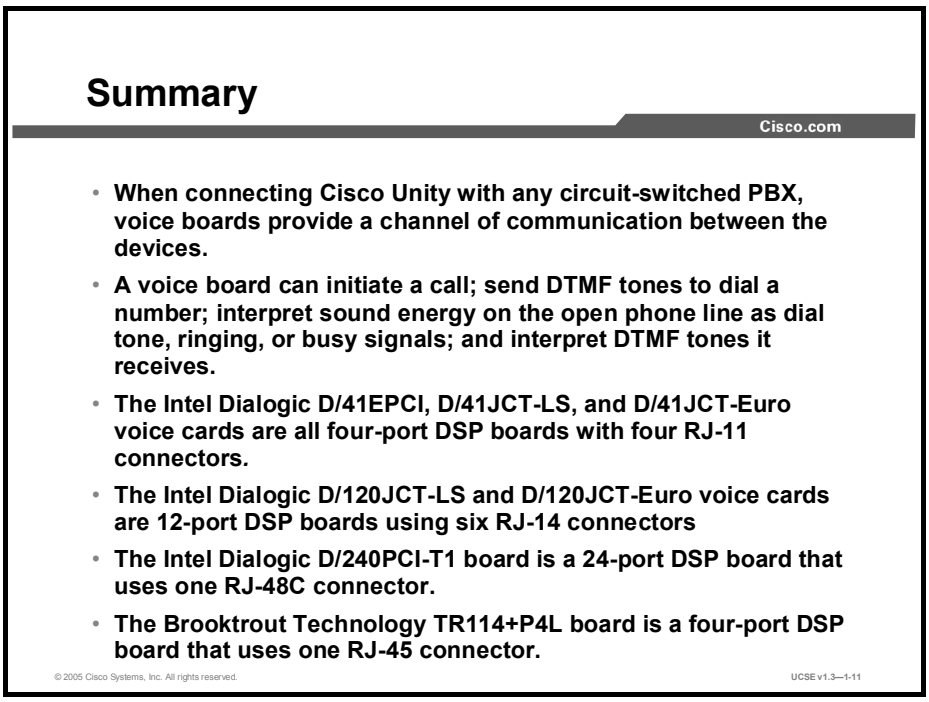


The Brooktrout Technology TR114+P4L voice board is a four-port DSP board that uses one RJ-45 connector. Each board is supplied with a cable that has an RJ-45 plug at one end and four RJ-11 connectors at the other end.

All boards in one system share the same IRQ and base memory address. Specific information about the configuration of the IRQ and memory address is located in the Bridge server hardware documentation.

Summary

This topic summarizes the key points discussed in this lesson.



References

For additional information, refer to these resources:

- *Cisco Unity Installation Guide* (With Microsoft Exchange)
- *Cisco Unity Installation Guide* (With IBM Lotus Domino)
- *Cisco Unity Bridge Installation Guide*

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) Voice cards are used to integrate Cisco Unity with _____ systems.

A) legacy voice mail
B) circuit-switched
C) Cisco CallManager
D) Cisco CallManager Express
E) SIP

Q2) A voice board has the ability to emulate a _____.

A) PBX
B) single-trunk extension
C) single-line extension
D) multi-trunk extension
E) multi-line extension

Q3) When Cisco Unity needs to send signals to a circuit-switched PBX with no digital integration, which hardware is typically used?

A) telephone
B) PSTN
C) hard disk
D) voice board
E) WAV driver

Q4) Which card is typically used to connect to a circuit-switched PBX?

A) Intel Dialogic
B) Brooktrout
C) SoundBlaster
D) Microsoft Media Master

Q5) If multiple Intel Dialogic D/41EPCI voice boards are in the same system, which item must be unique about them?

A) IRQ
B) hardware ID
C) DMA
D) IRQ and DMA

Q6) If multiple Intel Dialogic D/120JCT-LS voice boards are in the same system, which item must be unique about them?

A) IRQ
B) hardware ID
C) DMA
D) IRQ and DMA

Q7) How many ports are on an Intel Dialogic D/240PCI-T1 voice board?

A) 4
B) 8
C) 12
D) 24

Q8) The Brooktrout voice board is only used where in a Cisco Unity integration scenario?

A) Cisco Unity server to circuit-switched PBX
B) Cisco Unity Bridge to circuit-switched PBX
C) Cisco Unity server to Octel voice-mail system
D) Cisco Unity Bridge to Octel voice-mail system

Quiz Answer Key

Q1) B

Relates to: Why Use Voice Boards?

Q2) C

Relates to: What Functions Do Voice Boards Perform?

Q3) D

Relates to: What Functions Do Voice Boards Perform?

Q4) A

Relates to: installing and Configuring Voice Boards

Q5) B

Relates to: Intel Dialogic D/41EPCI, D/41JCT-LS, and D/41JCT-Euro Voice Boards

Q6) B

Relates to: Intel Dialogic D/120JCT-LS and D/120JCT-Euro Voice Boards

Q7) D

Relates to: Intel Dialogic D/240PCI-T1 Voice Board

Q8) D

Relates to: Brooktrout Technology TR114+P4L Voice Card

Module Self-Check

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

Q1) Which of the following Platform Overlays would be appropriate for a small office with 200 users?

A) Platform Overlay #1
B) Platform Overlay #2
C) Platform Overlay #3

Q2) Adding a second mirror drive set allows high-end servers to perform which of the following tasks? (Choose three.)

A) increase processing speed
B) allow greater performance
C) separate the Exchange transaction log from the application logs
D) perform system restore
E) minimize Exchange log stalls

Q3) Which of the following Platform Overlays would be appropriate for a mid-sized company of up to 2000 users?

A) Platform Overlay #1
B) Platform Overlay #2
C) Platform Overlay #3

Q4) Which Platform Overlay is the MCS 7835 in?

A) Platform Overlay #1
B) Platform Overlay #2
C) Platform Overlay #3

Q5) Which tool can be used to determine which platforms are supported?

A) CUSPA
B) CUICA
C) CUDL
D) CUSPL

Q6) Which is required when implementing a Cisco Unity Bridge?

A) Octel Interchange
B) Nortel Net Gateway
C) voice boards for analog connectivity
D) IPX network for digital connectivity

Q7) The voice boards are typically used when integrating with a _____ call processing system?

A) VoFR
B) circuit-switched
C) VoIP
D) VoATM

Q8) Which card is typically used in a Cisco Unity Bridge?

A) Dialogic
B) Brooktrout
C) SoundBlaster
D) Microsoft Media Master

Q9) How many ports are on an Intel Dialogic D/41EPCI voice board?

A) 4
B) 8
C) 12
D) 24

Q10) How many ports are on an Intel Dialogic D/120JCT-LS voice board?

A) 4
B) 8
C) 12
D) 24

Q11) On the Intel Dialogic D/240PCI-T1 voice board, where is the signaling channel?

A) DTMF
B) SCCP
C) SMDI
D) PBX link

Q12) How many ports are on a Brooktrout TR114+P4L voice card?

A) 4
B) 8
C) 12
D) 24

Scoring

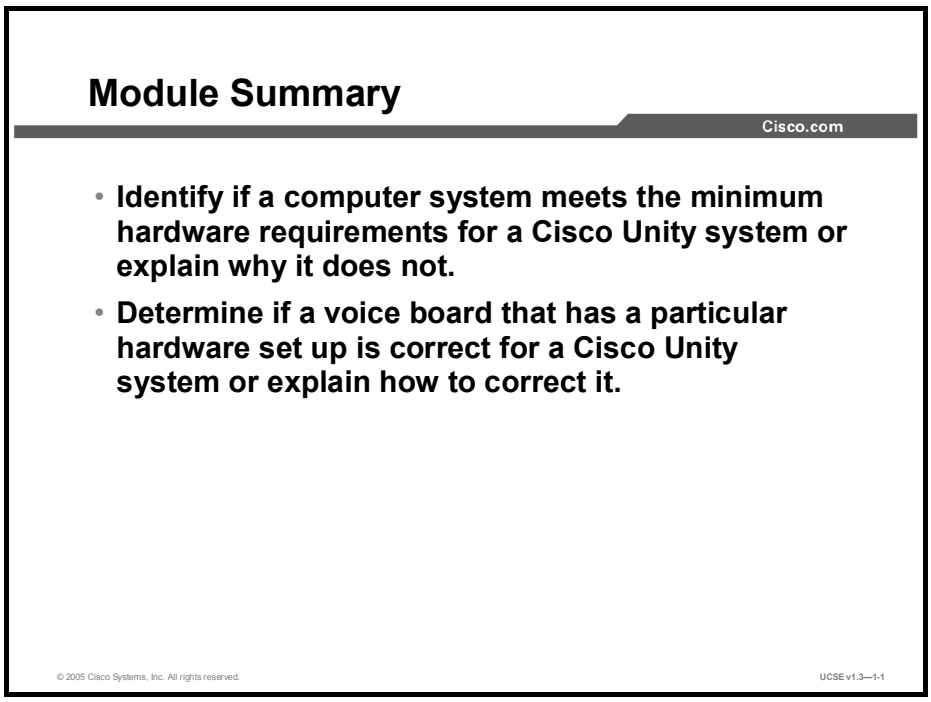
You have successfully completed the quiz for this lesson when you earn a score of 80 percent or better.

Module Self-Check Answer Key

Q1) A
Q2) B, C, E
Q3) B
Q4) A
Q5) D
Q6) C ,D
Q7) B
Q8) B
Q9) A
Q10) C
Q11) C
Q12) A

Module Summary

This topic summarizes the key points discussed in this module.



In this module, you learned that before you install any operating system or other software, you must first consider the hardware to be used. A system must meet or exceed minimum hardware requirements to perform at acceptable levels. Problems resulting from inadequate hardware can range from unacceptable access times to the inability to install the necessary software. The module described the platform overlay scheme as well as systems that Cisco supplies. By reviewing the platform overlay scheme as well as these systems, you should have a good understanding of what it takes to support a Cisco Unity server.

The module also addressed voice boards, the necessary ancillary hardware needed for a Cisco Unity server working with a circuit-switched PBX, or a Unity Bridge working as an Octel messaging node.

References

For additional information, refer to these resources:

- Cisco Unity 4.0 System Requirements, and Supported Hardware and Software found at: http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_system_requirements_hardware09186a0080117617.html

Module 2

Installing Cisco Unified Communications System Software

Overview

This module describes Cisco unified communications architectures, such as the architecture for Cisco Unity for Exchange and Cisco Unity for Domino. It describes the software necessary for a proper installation of all the unified communications products. You will install the Cisco Unity software and describe the various steps of the Cisco Unity System Preparation Assistant (CUSPA) and the Cisco Unity Installation and Configuration Assistant (CUICA). You will also learn the upgrade process for the Cisco unified systems.

Module Objectives

Upon completing this module, you will be able to select the correct components and correctly install the software, and verify proper operation. This ability includes being able to meet these objectives:

- Describe the Cisco unified communications architectures
- Describe the software needed to perform a successful installation of the unified products
- Install the Cisco Unity system
- Describe the use of CUSPA and CUICA
- Describe the upgrade process for the Cisco unified communications products

Lesson 1

Understanding Unified Communications Architecture and Software

Overview

This lesson describes the architecture of the Cisco Unity unified messaging systems.

Relevance

Understanding the Cisco Unity structure will enable you to properly install and maintain the Cisco Unity unified messaging systems. An understanding of the interactions between the software components with which the Cisco unified communications products are built will greatly aid in the troubleshooting of the products.

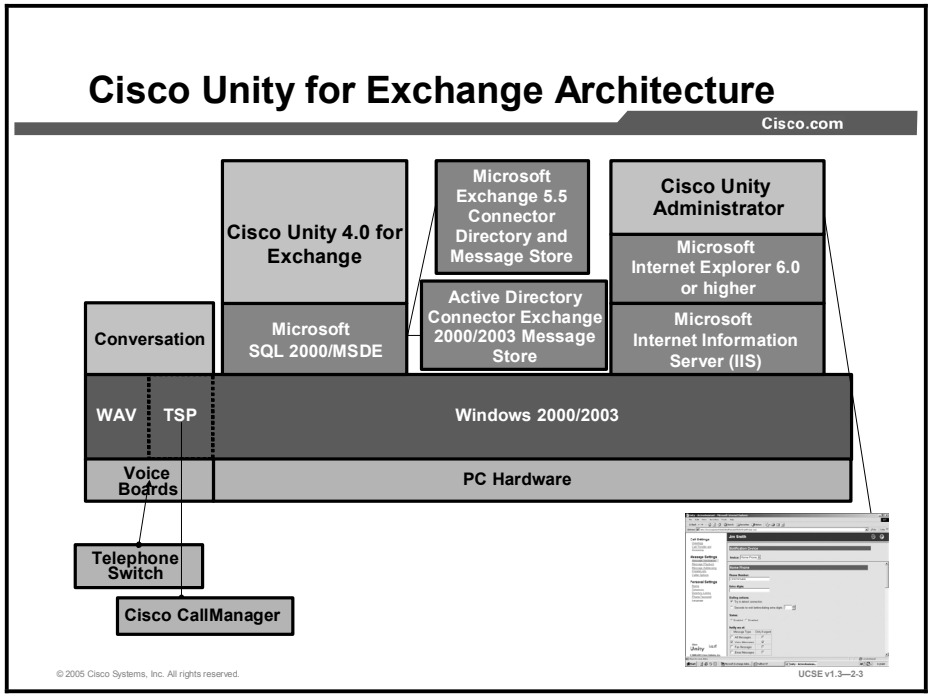
Objectives

Upon completing this lesson, you will be able to define the functional areas correctly and determine whether you have a minimally adequate set of unified communications products to run Cisco Unity, or explain why it is not adequate. This ability includes being able to meet these objectives:

- Describe the Cisco Unity for Exchange architecture
- Describe the system software components used in a Cisco Unity for Exchange installation
- Describe the client software components used in a Cisco Unity for Exchange installation, including VMO and CPCA
- Describe the Cisco Unity for Domino architecture
- Describe the system software components used in a Cisco Unity for Domino installation
- Describe the architectural services provided by DUCS
- Describe the client software components used in a Cisco Unity for Domino installation, including the Lotus ViewMail for Notes

Cisco Unity for Exchange Architecture

This topic describes the Cisco Unity for Exchange architecture.



At the base of any Cisco Unity system is the hardware. Cisco sells Cisco Unity on several platforms, which were discussed in the Unified Communications Server Hardware module. Cisco Unity runs on a Microsoft Windows 2000 Server (or Enterprise) operating system. Cisco Unity uses the Windows 2000 Active Directory to store a minimum amount of user data. The vast bulk of information is stored as a Structured Query Language (SQL) database. When you use the Cisco Unity Active Server Pages (ASPs) to add, delete, or modify a Cisco Unity subscriber, you are modifying the SQL database. Cisco Unity will use either Microsoft SQL 2000 Desktop Engine (MSDE) or Microsoft SQL 2000 software, depending on your Cisco Unity configuration. The information is then passed on to Windows Active Directory through either the Microsoft Exchange Directory Connector for Exchange 5.5 or the Active Directory Connector for Exchange 2000. This choice is made during the Cisco Unity installation process.

Whether you integrate Cisco Unity to a Cisco CallManager or a circuit-based telephone system, you will need a physical connection between Cisco Unity and the telephone system. The physical connection for the Cisco CallManager integration is a connection to the LAN or WAN of the site, while the connections for a circuit-based telephone system are physical voice cards installed on the Cisco Unity server and the appropriate cables to connect to the PBX.

You will also need software drivers and a Telephony Service Provider (TSP) to run the hardware, and a software interface to configure and modify the TSP settings. Cisco Unity Telephony Integration Manager (UTIM) installs the TSP provided by the manufacturer of the device that communicates with the PBX.

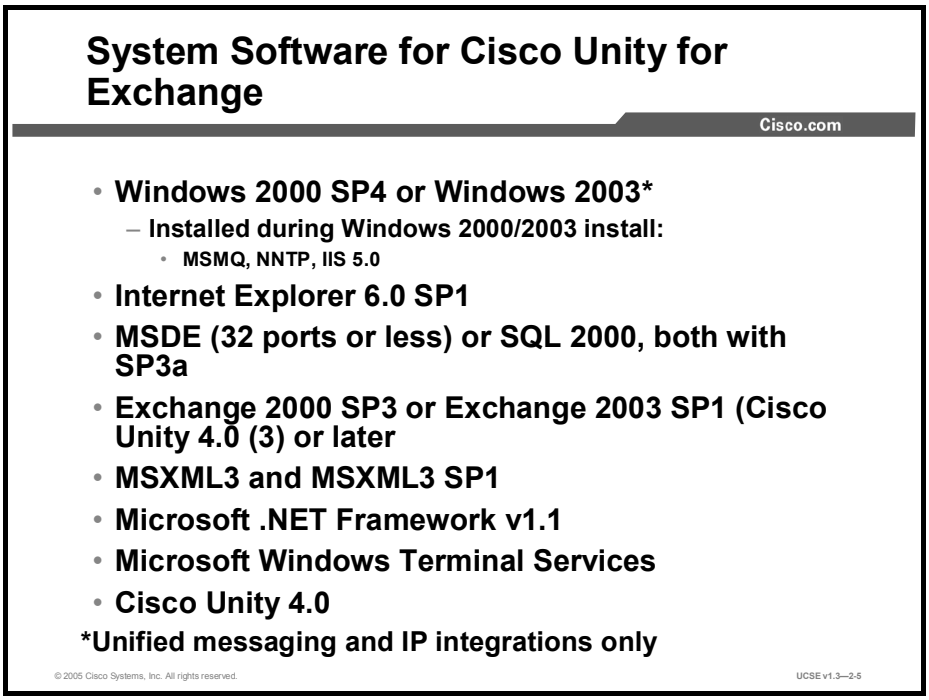
Cisco Unity passes subscriber messages to the appropriate Exchange message store. The message is then placed into the Cisco Unity subscriber Exchange inbox, which is part of the Exchange Information Store.

Subscriber messages are only stored on the Cisco Unity server in some voice-mail-only configurations, or when the Cisco Unity Message Repository (UMR) detects that the Exchange server is not available. Once the UMR detects that Exchange is once again available, the messages are passed through to the Exchange Information Store.

HTML-based console screens allow access to the Cisco Unity system console. Cisco Unity uses Microsoft Internet Explorer 6.0 (recommended) to provide the HTML screens.

System Software for Cisco Unity for Exchange

This topic describes the system software components used in a Cisco Unity for Exchange installation.



Cisco Unity systems use Windows 2000 or Windows 2003 as the operating system. Windows 2000 or 2003 will be installed with different options, depending on your Cisco Unity configuration. In order for Cisco Unity to function properly, the following Windows 2000 or 2003 components must also be installed: Internet Information Services (IIS), Windows 2000 Service Pack 4, Message Queuing Services, Terminal Services, and Network News Transfer Protocol (NNTP). Microsoft Active Directory will need to be installed if Cisco Unity will be in voice-mail-only configuration and therefore in its own domain. If, however, Cisco Unity will be joining an existing domain as a member server, the Active Directory option is not installed on the Cisco Unity server. The Cisco Unity server should not act as a Domain Name System (DNS) or Dynamic Host Configuration Protocol (DHCP) server for the network.

Which Windows 2000 or 2003 CD you use for installation of the operating system depends on where you purchased the Cisco Unity server. If the server you intend to use for Cisco Unity was purchased from Cisco, install Windows 2000 from the platform configuration disk that came with the Cisco Unity server. However, if the server was not purchased from Cisco, use the original equipment manufacturer (OEM) disk that came with the system. The disk contains OEM drivers for HP, Compaq, Dell, or IBM, allowing you to use a retail version of Windows 2000 or 2003.

Microsoft Internet Explorer (IE) 6.0 is the web browser that must be installed on the Windows 2000 server when using IIS. Cisco Unity does not support Netscape Navigator.

The Microsoft extensible markup language (MSXML3 and MSXML SP2) are installed and can be found on the Cisco Unity CD 1 or on the Cisco Unity DVD.

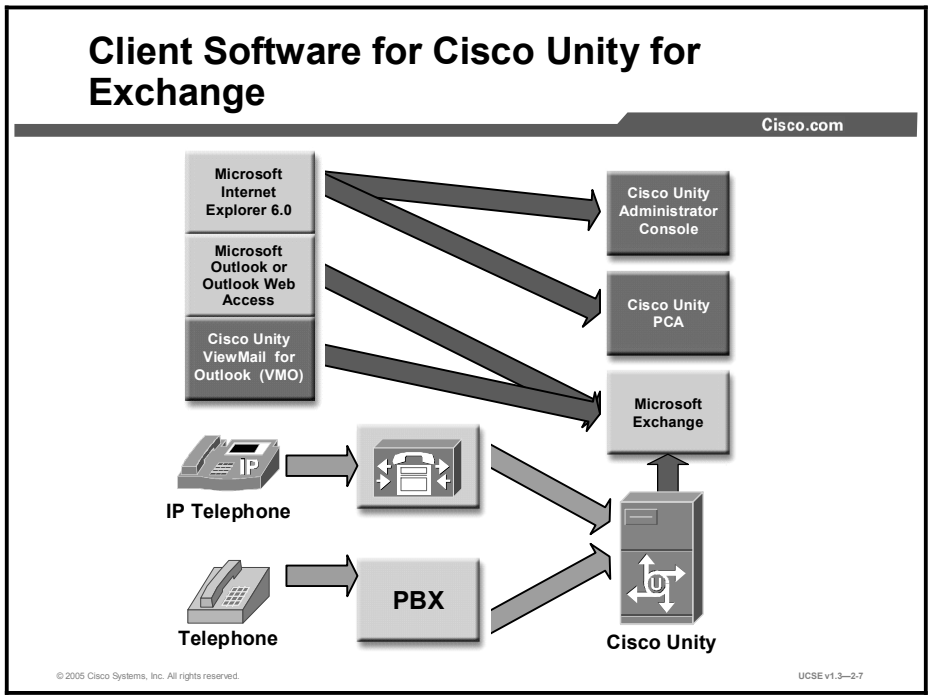
MSDE or Microsoft SQL 2000 SP3 are database storage for all Cisco Unity attributes. Cisco Unity will require MSDE for systems 32 ports or less without the Cisco Unity Failover option. Cisco Unity systems greater than 32 ports or using the failover option requires SQL 2000 with SP3.

Exchange 2000/2003 or Exchange 5.5 is the Microsoft e-mail server. Cisco Unity will use the Message Store of Exchange 2000 or 2003 to store subscriber messages. Cisco Unity can also be installed to integrate Microsoft Exchange 5.5 with SP4. Beginning with the release of Cisco Unity 4.0, Cisco Unity installed in the unified messaging mode will only support Microsoft Exchange 2000 or 2003 in an off-box configuration.

The Microsoft .NET framework supports the new Tabular Data Stream (TDS) proxy in Cisco Unity 4.0(5). The TDS proxy is used to allow Java-based client applications to access the Cisco Unity database without requiring mixed-mode authentication in an SQL server. Enabling mixed-mode security is a security risk for a number of reasons that are well documented by Microsoft.

Client Software for Cisco Unity for Exchange

This topic describes the client software components used in a Cisco Unity for Exchange installation, including VMO and Cisco Personal Communications Assistant (CPCA).



So far this lesson has described the software required on the Cisco Unity server. The lesson will now describe the client or "end-user" workstation.

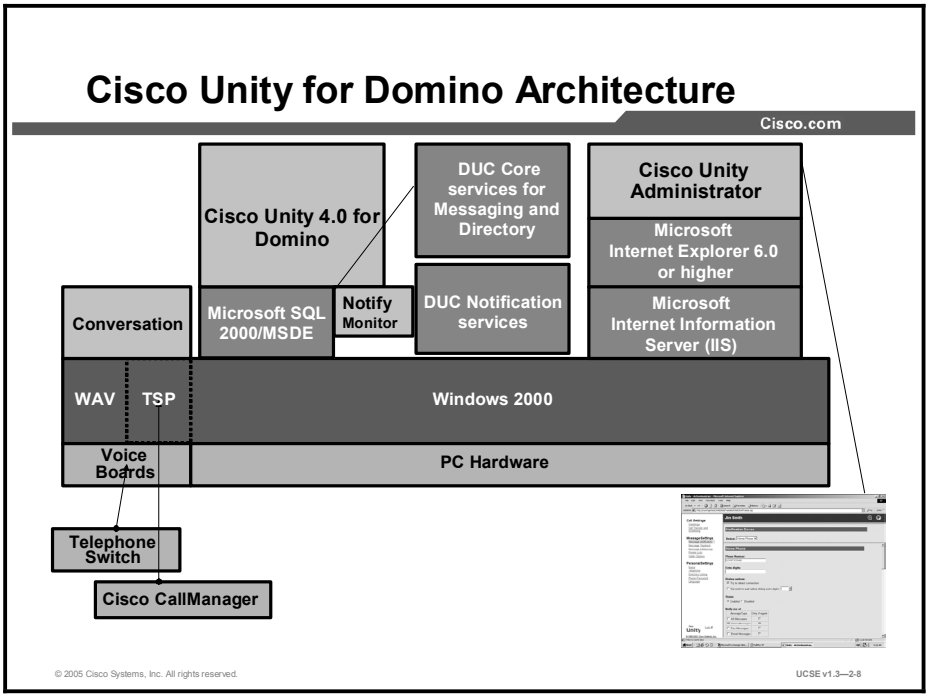
Cisco Unity ViewMail for Outlook (VMO) is a special form in Outlook that has a set of control buttons. With these control buttons, you can listen to, send, reply to, and forward voice messages. VMO can be used with Outlook 98, Outlook 2000, and Outlook XP. VMO cannot be used with Outlook Express or Outlook Web Access because those clients do not support Outlook forms. VMO software can be found on Cisco Unity CD 1 in the ViewMail folder, and is installed on the client workstations rather than the Cisco Unity server.

Clients may also want to access their mailbox settings through the Cisco Unity Assistant part of the Cisco Unity Personal Communications Assistant (CPCA). The Cisco Unity Assistant allows the user to change their mailbox settings through a user-friendly graphical user interface, rather than over the phone. Any mailbox setting available through the telephone is available through the Cisco Unity Assistant. Class of service (CoS) in Cisco Unity controls access to the Cisco Unity Assistant. Additionally the client workstation must be running Internet Explorer 6.0 or above.

Site administrators of Cisco Unity can also access the Cisco Unity Administration screens through their desktop. Cisco Unity CoS controls access to this feature, and the client must have Internet Explorer 6.0 or above on their workstation.

Cisco Unity for Domino Architecture

This topic describes the Cisco Unity for Domino architecture.



The underlying Cisco Unity for Domino architecture is similar to the architecture for Cisco Unity for Exchange. Lotus Domino is IBM's Lotus database and messaging product. Cisco Unity for Domino is the result of collaboration between Cisco Systems and IBM Lotus. As part of this collaboration, IBM Lotus created Domino Unified Communication services (DUC) for Cisco Unity. This component enables Cisco Unity to deliver unified messaging in a Lotus Domino environment.

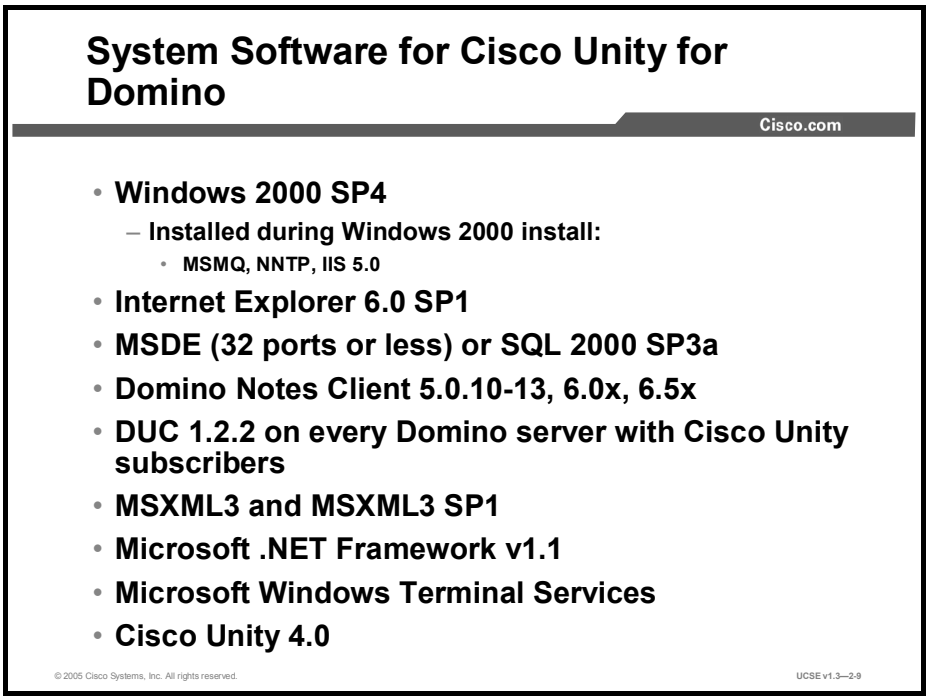
In this configuration, the Microsoft SQL 2000 or MSDE software will communicate with Lotus Domino through a Domino connector that is selected by the installer during the Cisco Unity installation process. Lotus has developed DUC in order for Domino to integrate with Cisco Unity. DUC must be installed on a Domino directory server in every domain, and on each Domino messaging server where a Cisco Unity subscriber mailbox exists. DUC Version 1.2.2 will support Domino versions 5.0.10-13, 6.0.x, or 6.5.x.

Lotus Notes software must also be installed on the Cisco Unity platform. This supplies the message notification function for Cisco Unity for Domino.

The Cisco Unity for Domino configuration will only be supported in a unified messaging environment with Lotus Domino services being installed off the Cisco Unity platform. Domino is not supported if Windows 2003 is installed on the Cisco Unity server.

System Software for Cisco Unity for Domino

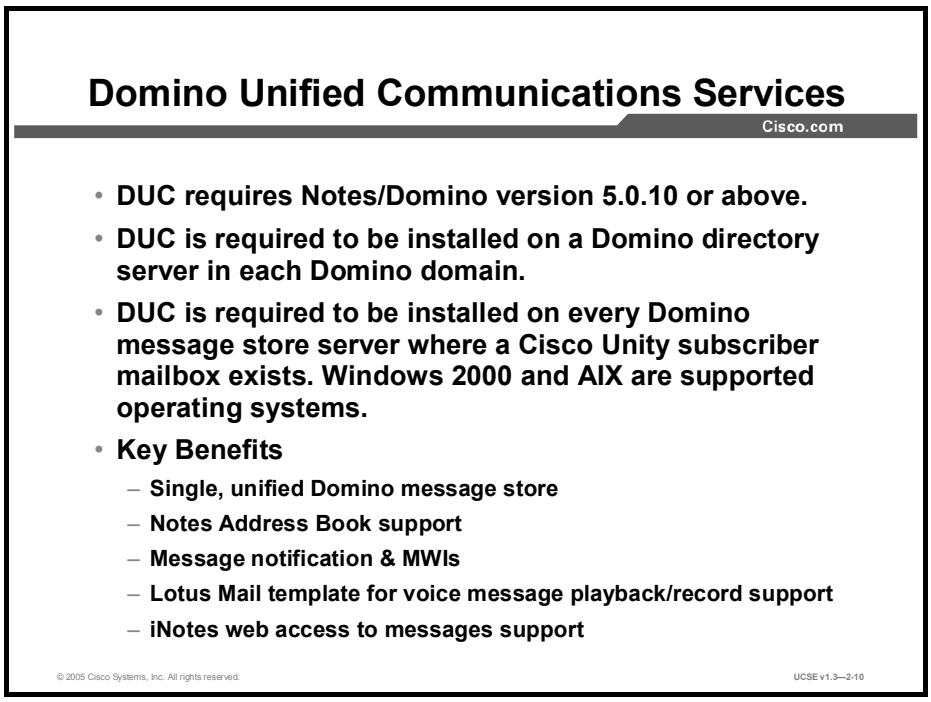
This topic describes the system software components used in a Cisco Unity for Domino installation.



Cisco Unity for Domino shares most of the same software components for a successful installation as Cisco Unity for Exchange. The major difference is the message store.

Domino Unified Communications Services

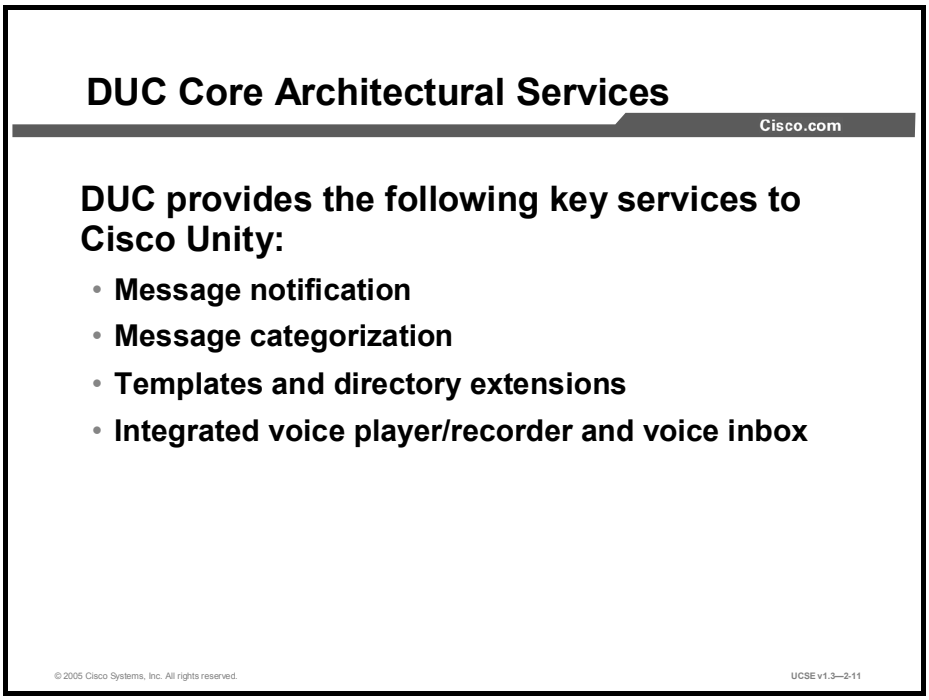
This topic describes the architectural services provided by DUC.



Any Domino server housing a message store for a Cisco Unity subscriber will require Windows 2000 or advanced interface executive (AIX) as its operating system.

Lotus Notes provides a client for mail, calendaring, and scheduling, similar to Microsoft Outlook. Cisco Unity will work with Notes 5.0.10, 5.0.11, 5.0.12, 6.0.x, and 6.5.x. IBM Lotus provides both Domino and Notes. Domino is the server software and Notes is the client.

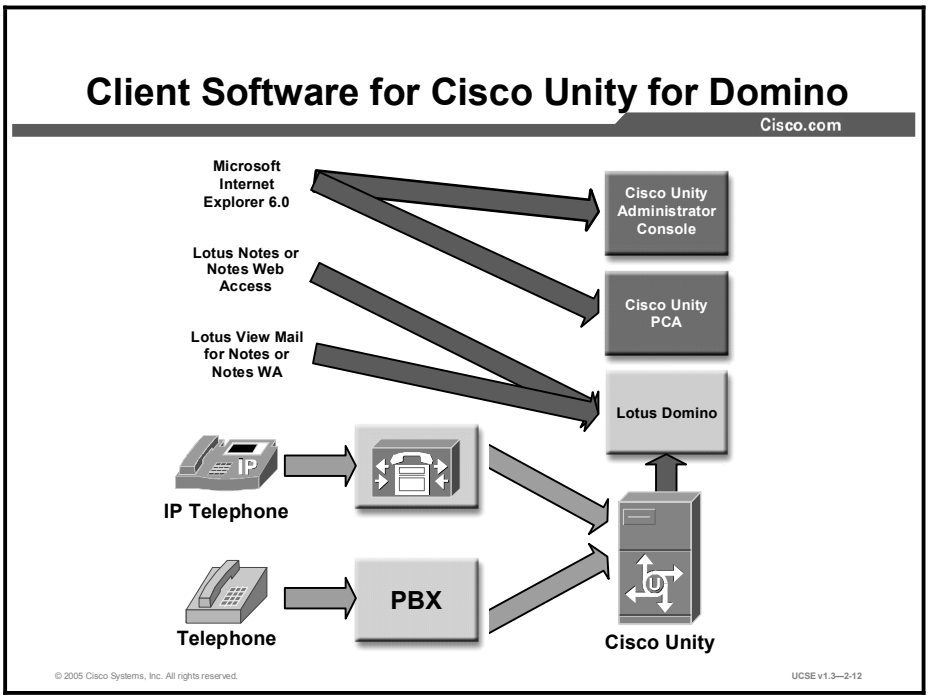
Cisco Unity for Domino is only supported in a unified messaging configuration, with Lotus Domino being installed off-box.



Lotus DUC provides the platform and key services upon which Cisco has built a Cisco Unity solution that uses Domino as the unified message store. Specifically, DUC provides message notification, message categorization, templates and directory extensions, and integrated voice player/recorder and voice inbox services for Cisco Unity in the Lotus Domino environment.

Client Software for Cisco Unity for Domino

This topic describes the client software components used in a Cisco Unity for Domino installation, including the Lotus ViewMail for Notes.



The client software supported on the Cisco Unity for Domino configuration is very similar to the client software for the Exchange configuration. In the case of Cisco Unity for Domino, the supported Domino Notes clients are installed rather than Outlook.

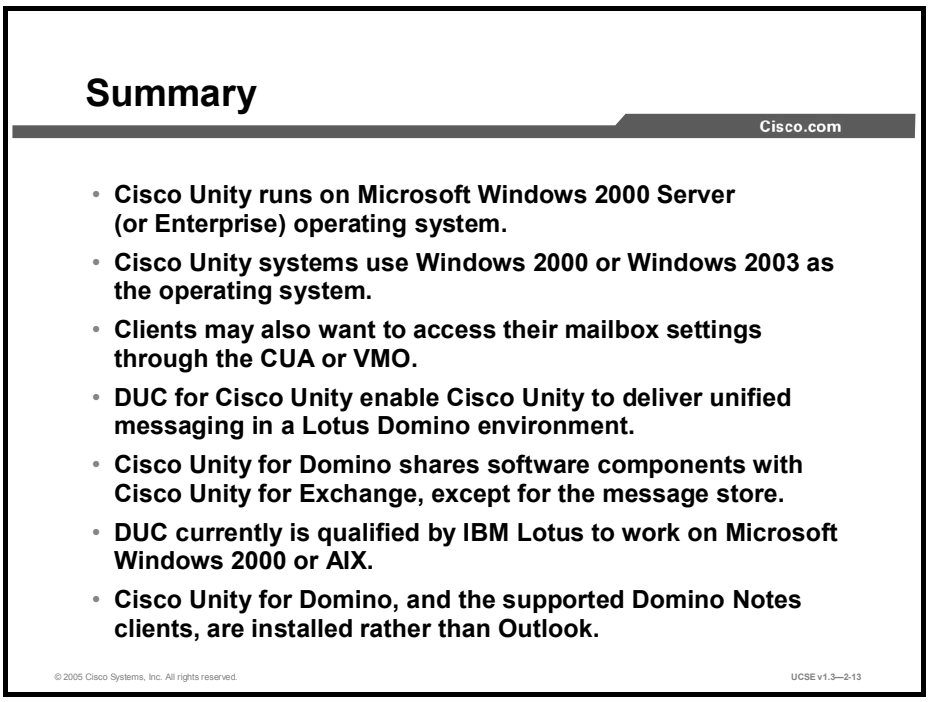
As with ViewMail for Outlook, Lotus ViewMail for Notes gives the end user an easy graphical interface from which to check their voice mail and e-mail, and to send, reply, or forward messages. The Lotus ViewMail for Notes client software is a Notes Mail form built and supported by IBM Lotus.

Class of service controls access to CPCA features and the Cisco Unity Administration screens and require Internet Explorer 6.0 or above to function.

Note	The client software for Cisco Unity in a Domino environment is applicable for unified messaging implementations only. For voice-mail-only implementations, Microsoft Exchange is required.

Summary

This topic summarizes the key points discussed in this lesson.



Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) SQL is installed on the Cisco Unity server for which of the following configurations?

A) Always in a failover configuration
B) Always in a Unified messaging configuration
C) More than 1000 subscribers
D) 36 ports or more

Q2) ViewMail for Outlook (VMO) can be used with which mail clients? (Choose three.)

A) Outlook 98
B) Outlook 2000
C) Outlook Express
D) Outlook XP
E) Outlook web access

Q3) DUC must be installed where?

A) a Domino directory server in every domain, and on each Domino messaging server where a Unity subscriber mailbox exists
B) a Domino directory server in every domain only
C) each Domino message server where a Unity subscriber mailbox exists
D) Cisco CallManager
E) the same server where Lotus Notes is installed

Q4) What is the major difference between a Cisco Unity for Exchange and a Cisco Unity for Domino software installation?

A) the version of Windows installed
B) the version of Internet Explorer required
C) the version of Cisco Unity installed
D) MSXML3 and MSXML3 SP2
E) the message store

Q5) The key benefits of Domino Unified Communications service include: (Choose all that apply.)

A) iNotes web access to messages
B) Single, unified Domino message store
C) Message notification & MWIs
D) Native Notes Address Book support
E) Native Lotus Mail template for voice message playback/record

Q6) Which internet browser(s) is required for Cisco Unity 4.0(5) to access the Cisco Unity Admin screens in a Cisco Unity Domino installation?

A) Either Internet Explorer 6.0 or Netscape 7.0
B) Internet Explorer 6.0 only
C) Internet Explorer versions 5.5 or later
D) Netscape 6.0 or later.

Quiz Answer Key

Q1) A,D

Relates to: Cisco Unity for Exchange Architecture

Q2) A, B, and D

Relates to: Client Software for Cisco Unity for Exchange

Q3) A

Relates to: Cisco Unity for Domino Architecture

Q4) E

Relates to: System Software for Cisco Unity for Domino

Q5) A, B, C, D, and E

Relates to: Domino Unified Communications Services

Q6) B

Relates to: Client Software for Cisco Unity for Domino

Lesson 2

Installing Cisco Unified Communications Software

Overview

This lesson describes the installation of the Cisco Unity software in its various forms, including the installation of the Cisco Unity software for Exchange and Domino.

Relevance

Understanding the installation process of the software leads to a successful installation of the Cisco Unity system. This is particularly important because the installation process for Cisco Unity 4.0 differs from previous versions.

Objectives

Upon completing this lesson, you will be able to list the recommended sequence for installing Cisco unified messaging software and verify its operation.

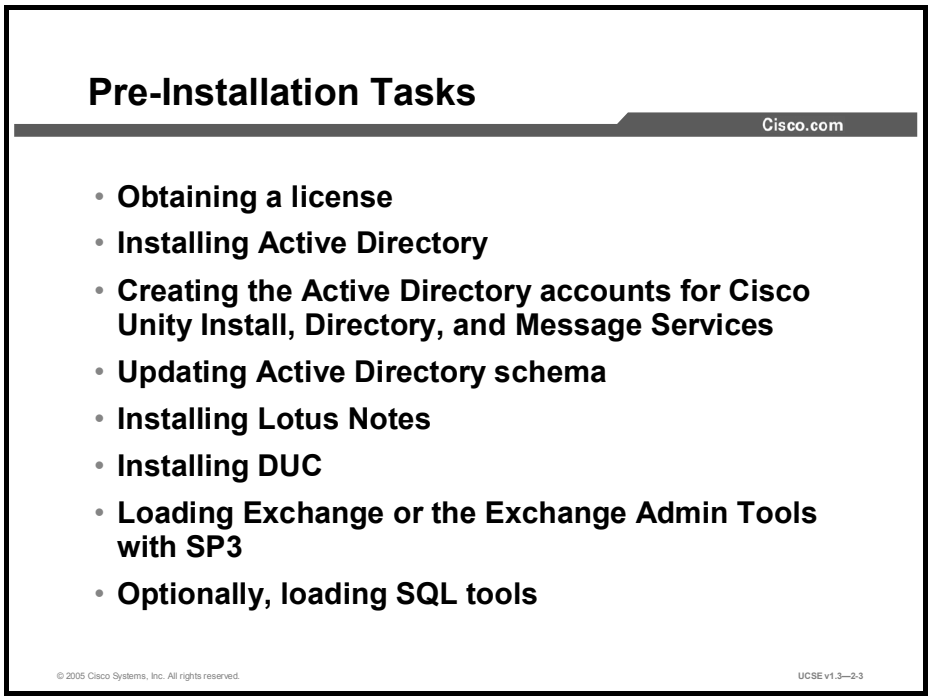
This ability includes being able to meet these objectives:

- Describe the tasks that must be performed before the installation, and the tasks that are not performed by the install disk or the platform configuration disk
- Describe how the Cisco Unity System Preparation Assistant assists in the preparation of a Cisco Unity system
- Describe how the Cisco Unity Installation and Configuration Assistant assists in the Cisco Unity installation process
- Describe the functions performed by the Permissions Wizard
- Describe the information needed for the Cisco Unity System Setup and the tasks performed
- Describe the tasks performed by the Install License File Wizard
- Describe the three Cisco Unity services configured by the Service Configuration Wizard
- Describe the choices for message store that must be made using the Message Store Configuration wizard

- Describe the Password Hardening wizard
- Describe how the Cisco Unity Telephony Integration Manager integrates Cisco Unity with your telephone system
- Describe the Authentication SSL process
- Describe the additional resources needed for a Cisco Unity installation

Pre-Installation Tasks

This topic describes the tasks that must be performed before the installation, as well as the tasks that are not performed by the installation disk or the platform configuration disk.

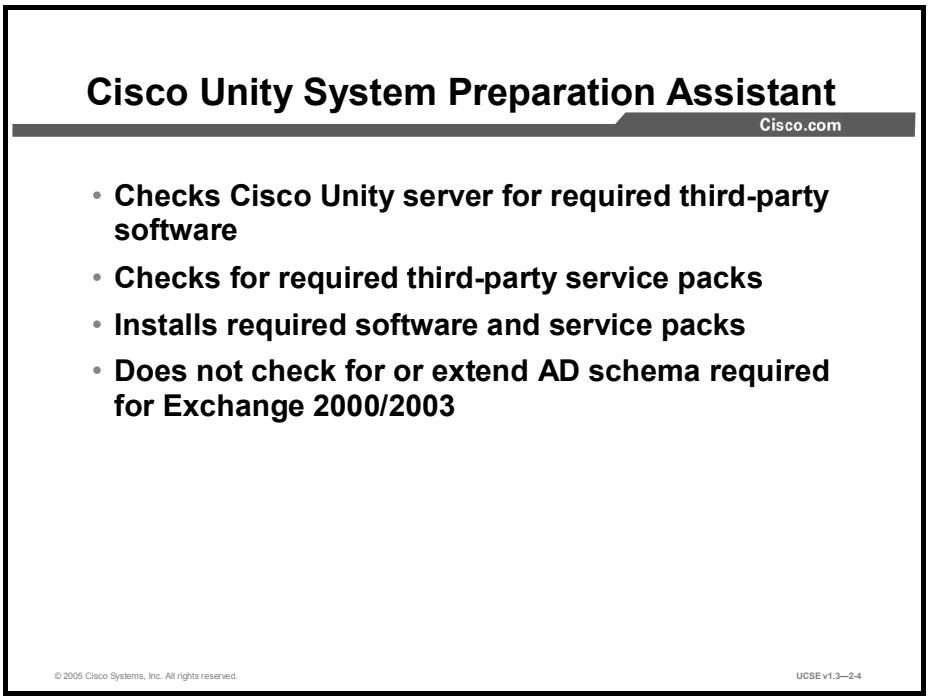


When installing either a voice-mail-only system or integrating Cisco Unity into an existing Exchange system, there are some tasks that have to be performed outside of the Cisco Unity System Preparation Assistant (CUSPA) and Cisco Unity Installation and Configuration Assistant (CUICA) wizards. Please note that some of these tasks are specific for Cisco Unity for Exchange or Cisco Unity for Domino. The tasks are as follows:

- Identifying the Active Directory that Cisco Unity will use, or installing a new Active Directory forest and domain
- Confirming that the Active Directory account that will act as the Cisco Unity Installer account (and default administrator), and the accounts that the directory and message services will log on as, are created
- Updating the Active Directory schema, to include the schema extensions that Cisco Unity requires
- Identifying the Exchange or Domino server that will be the partner server; and, if Exchange, ensuring that it has SP3 loaded
- If a Domino installation, confirm that Lotus Notes and Domino Unified Communication services (DUC) have been installed
- If the Exchange server is off-box, loading the Exchange Admin Tools on the Cisco Unity Server with SP3
- Optionally, loading the SQL tools for viewing and working with the SQL databases

Cisco Unity System Preparation Assistant

This topic describes how the Cisco Unity System Preparation Assistant assists in the preparation of a Cisco Unity system.

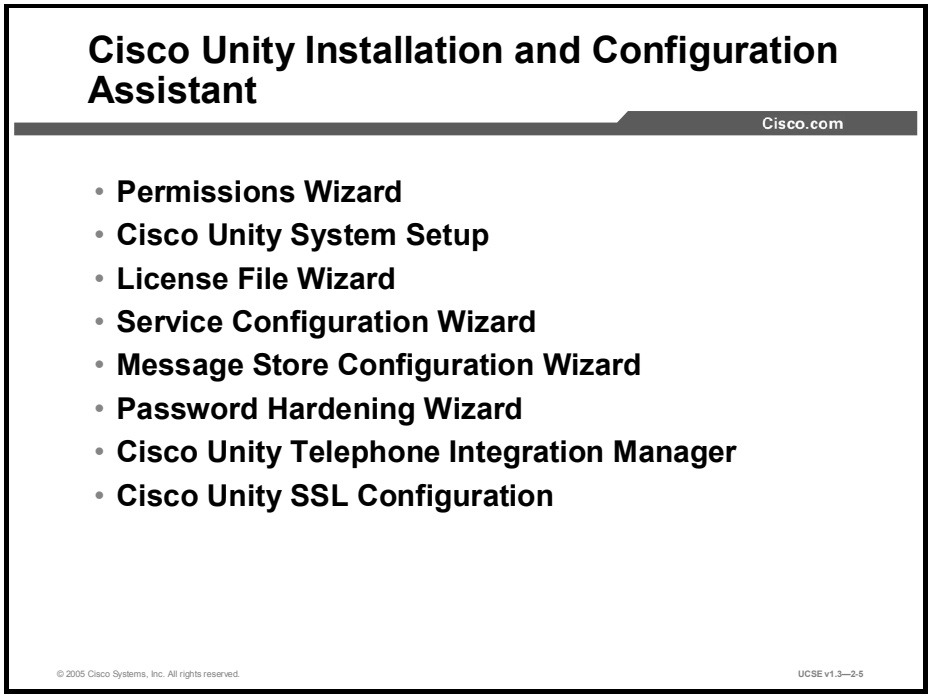


CUSPA is a tool to assist you in the preparation of a Cisco Unity system. This tool, located on the Service Pack disk, will check the Cisco Unity server for the required software and service packs. CUSPA will ask for your Cisco Unity server characteristics, such as unified messaging (UM) or voice mail (VM), failover, and number of Cisco Unity ports.

The Preparation Assistant will check for the proper levels of SQL, Microsoft extensible markup language (MSXML), Windows, Network News Transfer Protocol (NNTP), and Internet Explorer (IE). CUSPA does not check to make sure that the AD schema has been extended for an Exchange 2000 or 2003 installation. Extending the AD schema is required before beginning the Cisco Unity installation in an AD and Exchange 2000 or 2003 environment.

Cisco Unity Installation and Configuration Assistant

This topic describes how the Cisco Unity Installation and Configuration Assistant (CUICA) assists in the Cisco Unity installation process.



The Cisco Unity Installation and Configuration Assistant (CUICA) replaces the two-part Cisco Unity installation introduced in Version 3. The CUICA guides you through the entire setup process, including setting up the correct required permissions, installing Cisco Unity, and integrating Cisco Unity with the telephone system.

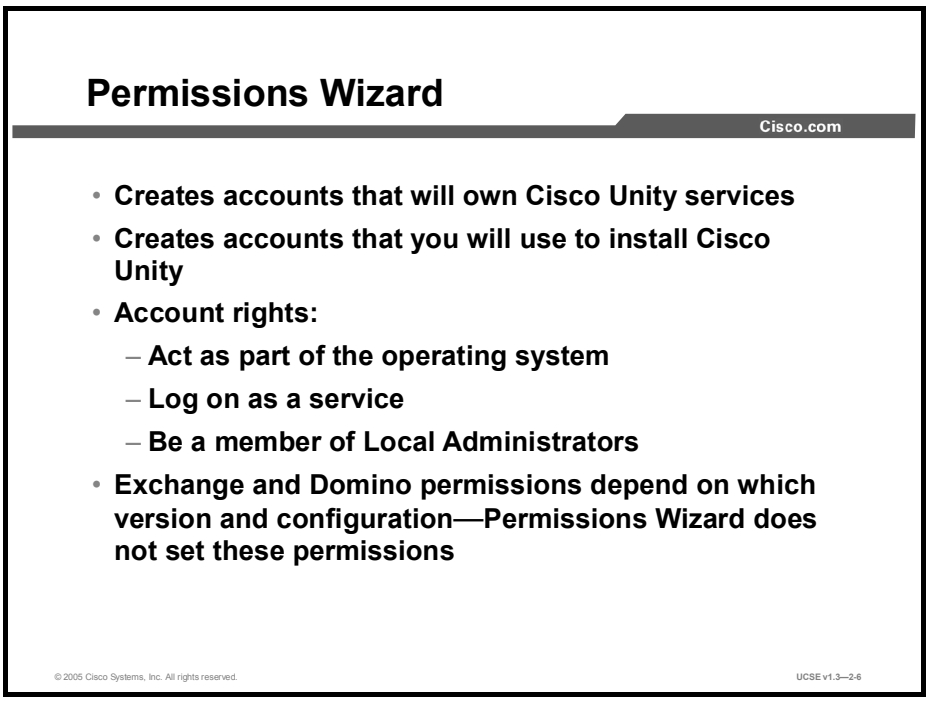
CUICA is actually seven separate wizard utilities combined with the Cisco Unity Setup Program. The seven wizard utilities are as follows:

- Permissions Wizard
- System setup
- License File Wizard
- Service Configuration Wizard
- Message Store Configuration Wizard
- Password Hardening Wizard
- Cisco Unity Telephone Integration Manager (UTIM)
- Cisco Unity Secure Socket Layer (SSL) configuration

All but the Message Store Configuration Wizard and the Password Hardening Wizard can be run individually after Cisco Unity is installed, by accessing the Tools Depot of Cisco Unity. The Message Store Configuration Wizard is located under the Commserver directory in the Configuration Setup folder.

Permissions Wizard

This topic describes the functions performed by the Permissions Wizard utility.



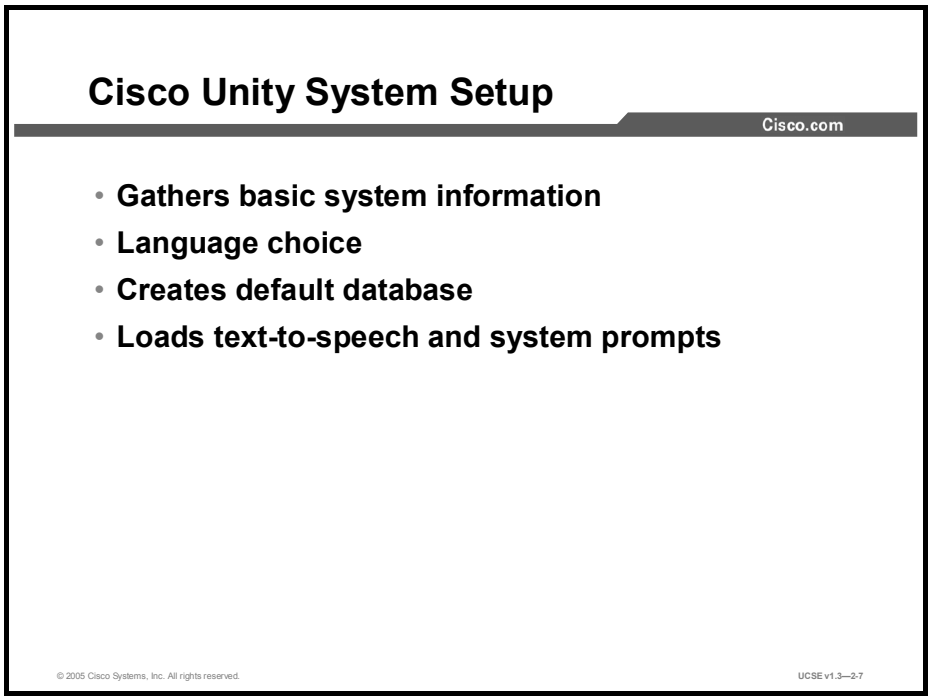
The Permissions Wizard utility sets the permissions needed to install Cisco Unity and for the Cisco Unity services to log on and run properly. This utility must be run before the Cisco Unity installation. Setting the correct permissions through the wizard will avoid complications as the Cisco Unity installation proceeds.

Before the wizard can set the correct permissions, it needs to know which message store you are using: Exchange 2000/2003, Exchange 5.5, or Domino. Depending on your configuration, the wizard will ask different questions. In general, you will be asked which account should be given permission to install and configure Cisco Unity, the account that Cisco Unity directory services will log on with, and the account to use to log on to Message Store.

After the Permissions Wizard finishes, there is a link to a document that explains the permissions required in an Exchange or Domino environment for Cisco Unity to be installed and function properly.

Cisco Unity System Setup

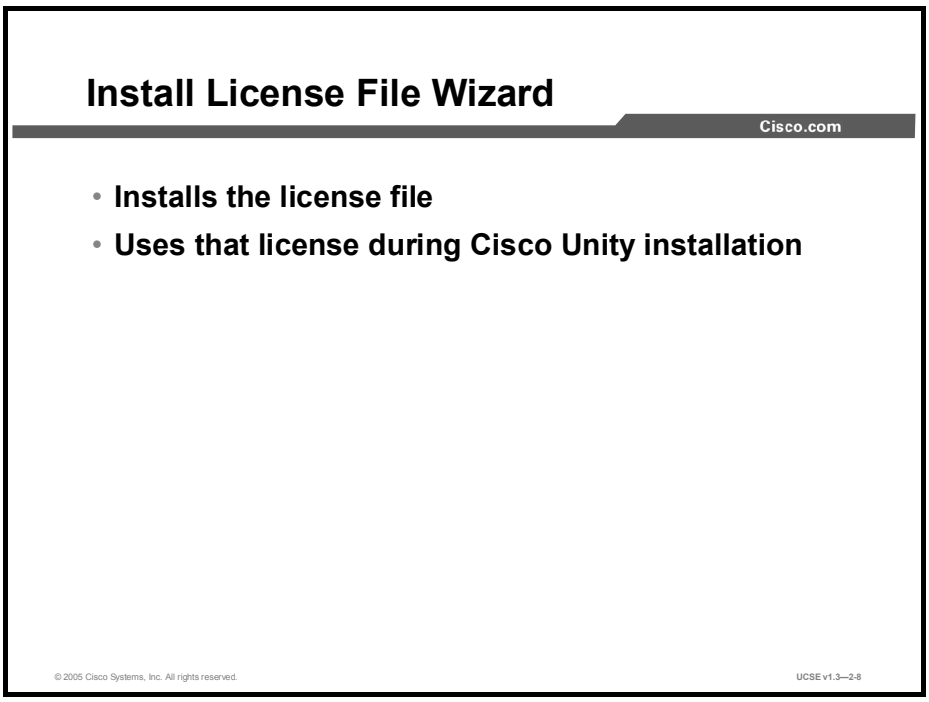
This topic describes the information needed for the Cisco Unity System Setup and the tasks performed.



This part of the installation process gathers general system information for the installation process. The setup process needs this information to install the correct languages on the system and the correct text-to-speech language, and to install Cisco Unity in the correct partition and folder on the hard drive. It loads the default database consisting of the Cisco Unity Installer account, the Example Administrator account, the Example Subscriber account, the default call handlers, and the other default objects.

Install License File Wizard

This topic describes the tasks performed by the Install License File Wizard.



At least 24 hours before your installation of Cisco Unity, you need to contact Cisco Systems to register and obtain your Cisco Unity license file. You will need to have the MAC address (physical address) for the network interface card (NIC) in the Cisco Unity computer and the Product Authorization Key (PAK), which is listed in the *Cisco Unity Software Keys* booklet that is shipped with the software disks. With that information, you access the license file generator site at http://www.cisco.com/go/license.

It is not enough to simply copy license files onto the file system of the Cisco Unity server. You need to run and complete the Install License File Wizard in order for Cisco Unity to use the information in the files. Specify the names of each of your license files in the wizard. You should specify all the files that you want Cisco Unity to use from that point forward, even if some of the files were installed previously. The wizard extracts the information from the files and checks the data for errors. If no errors are found, you may complete the wizard. Once you complete the wizard, Cisco Unity will begin using the license information from the files. If the wizard detects errors in the files, it will tell you what the problems are and will not permit you to proceed to the completion page. If you encounter problems, you should contact the Cisco Technical Assistance Center (TAC).

Unity Licensing Requirements

Licensing for Cisco Unity requires that you install Microsoft SQL 2000 Desktop Engine (MSDE) on systems with 32 ports or fewer. If you installed Microsoft SQL 2000 Standard Edition on a system with 32 ports or fewer, you need to downgrade to MSDE 2000 before Cisco TAC will provide support for the system. This does not apply to a Cisco Unity system set up for failover, for which you always install SQL Server 2000, regardless of the number of ports.

CPCA Licensing

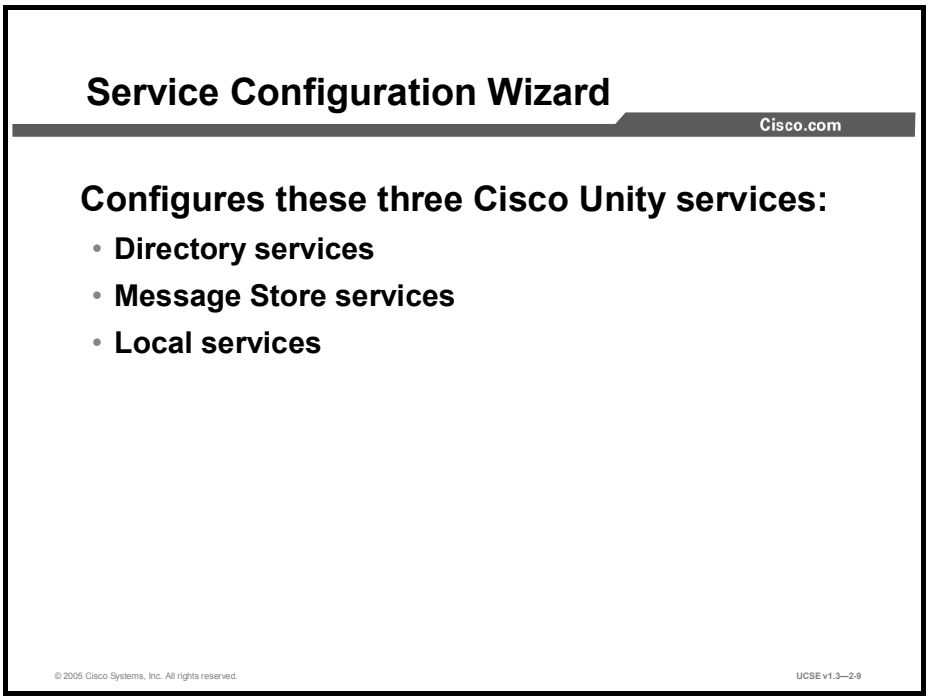
Both Active Assistant and Visual Messaging Interface (VMI) have been renamed for Cisco Unity Version 4.0 as part of the Cisco Personal Communications Assistant (CPCA).

Active Assistant has been renamed the Cisco Unity Assistant. Cisco Unity Assistant will continue to provide the same functionality, to enable end users to manage more of their own accounts, saving time and decentralizing routine administration. Cisco Unity Assistant is available to all users on a system at no additional cost.

VMI has been renamed the Cisco Unity Inbox, and continues to be the Cisco Unity message access console (supported on Internet Explorer 6.0 or higher) that provides a dedicated voice-mail inbox to deliver unified messaging functionality to non-Exchange network environments, such as Novell GroupWise. Cisco Unity Inbox is not available with Cisco Unity for Domino. Please note that Cisco Unity Inbox will continue to be licensed on a per-user basis.

Service Configuration Wizard

This topic describes the three Cisco Unity services configured by the Service Configuration Wizard.



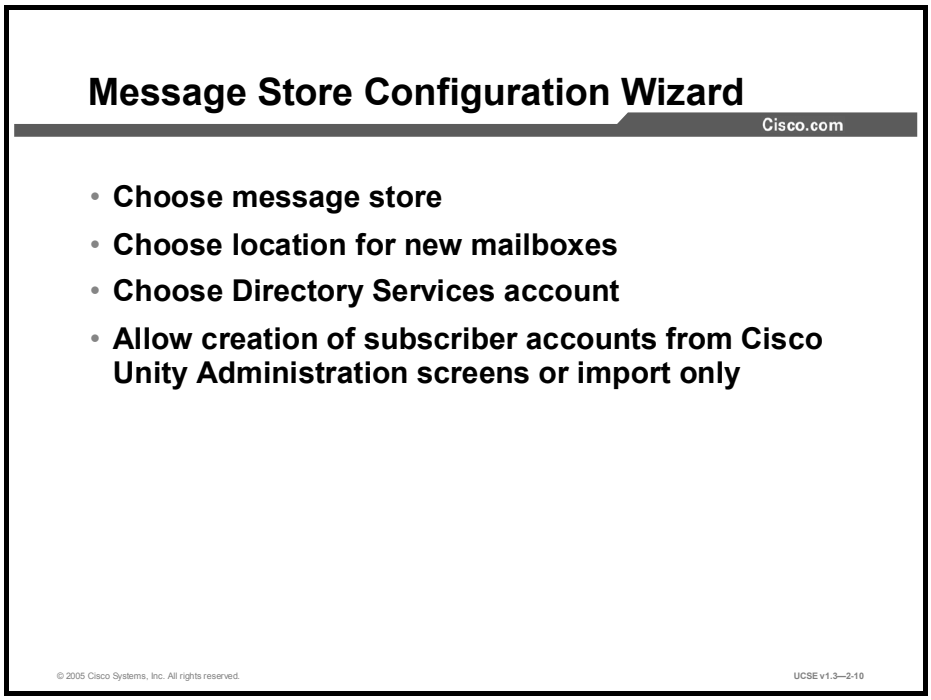
The Service Configuration Wizard helps you configure three groups of Cisco Unity services installed by your system. The wizard uses the selections you made during the Permissions Wizard as default accounts for the services. Since these are the accounts that have the correct permissions associated with them, it is best to accept the defaults. If you are not changing the account, you just have to put in the password for the accounts when asked. If, however, you change the accounts to use, make sure the accounts have the proper permissions.

You will be asked to confirm whether you are configured for Exchange 5.5, Exchange 2000/2003, or Lotus Domino R5/R6. Each of these systems requires a different setup version.

The Directory services sets the Cisco Unity account it will use to access the Microsoft Active Directory or the Lotus Domino Database. The Message Store services need to run under an account that is allowed access to Exchange 2000/2003 mailboxes or the Lotus Domino mailboxes. The Local Unity services, in an Exchange or Domino configuration, run under an account that allows them access to registry files, the file system, and the SQL server.

Message Store Configuration Wizard

This topic describes the choices for message store that must be made using the Message Store Configuration Wizard.

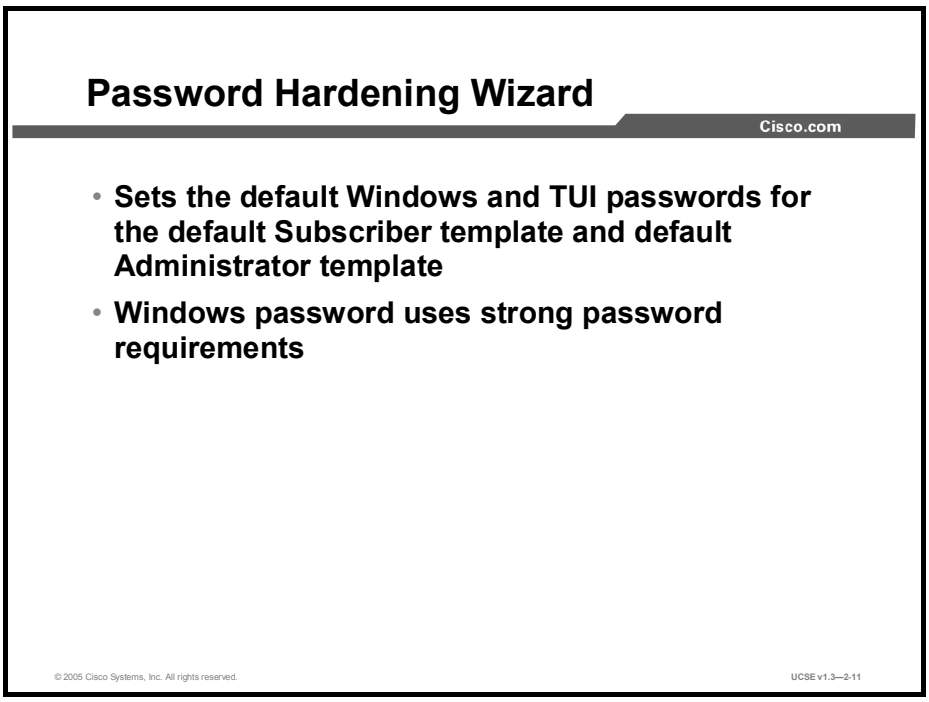


The Message Store Configuration Wizard section of the CUICA is where you choose between Exchange 5.5, Exchange 2000/2003, or Lotus Domino R5/R6/R6.5 as your message store. You need to decide where to home new mailboxes in your message store when they are added through the Cisco Unity System Administration screens. The Directory Service account would be the same account you chose in the Cisco Service Configuration Wizard as the account that will run the Cisco Unity Directory Service, which passes information back and forth between Cisco Unity and the message store.

The Message Configuration Wizard is also where you decide whether to allow a Cisco Unity administrator to create subscriber accounts along with the required Exchange-enabled Active Directory account, or to allow the administrator to "import only" existing Exchange-enabled Active Directory accounts to create Cisco Unity subscribers. This option is useful if there are different administrators for Cisco Unity, Active Directory, and Exchange. Some network administrators may feel uneasy with Cisco Unity creating Active Directory accounts. By choosing to "import only," you can ease their concern.

Password Hardening Wizard

This topic describes the Password Hardening Wizard.

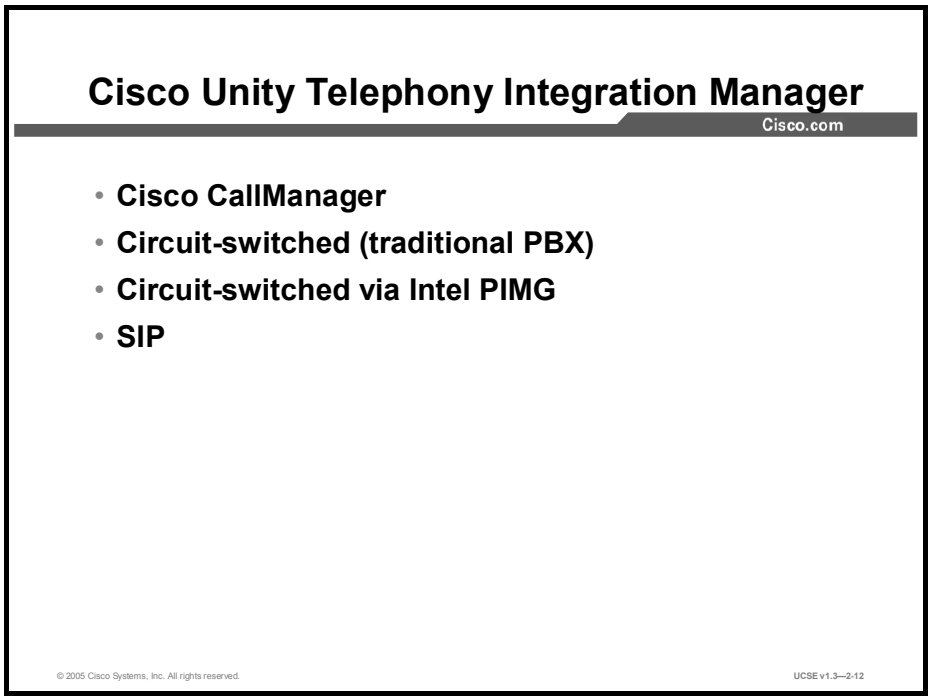


The Password Hardening Wizard section of the CUICA is where you select the default passwords for new subscribers in Cisco Unity. There are two default subscriber templates built into Cisco Unity, default Administrator and default Subscriber. As with all subscribers in Cisco Unity, subscribers created under either of the templates will need a default Telephone User Interface (TUI) password the first time they call into Cisco Unity. This will allow them access to the first-time enrollment dialogue, in which they will be prompted to set their own TUI password.

In addition, the Password Hardening Wizard will prompt you to create a Windows logon password for both of the default templates. This will be the logon password subscribers will use to log on to their Windows accounts if Cisco Unity creates those Active Directory accounts. If the Cisco Unity administrator imports new subscriber information from Active Directory, the Windows logon password created in the wizard will not be used.

Cisco Unity Telephony Integration Manager

This topic describes how the Cisco Unity Telephony Integration Manager integrates Cisco Unity with your telephone system.



The Cisco Unity Telephony Integration Manager (UTIM) steps you through integrating Cisco Unity with your telephone system. Cisco Unity will support integrations for IP telephony (Cisco CallManager), circuit-switched PBXs, and session initiation protocol (SIP).

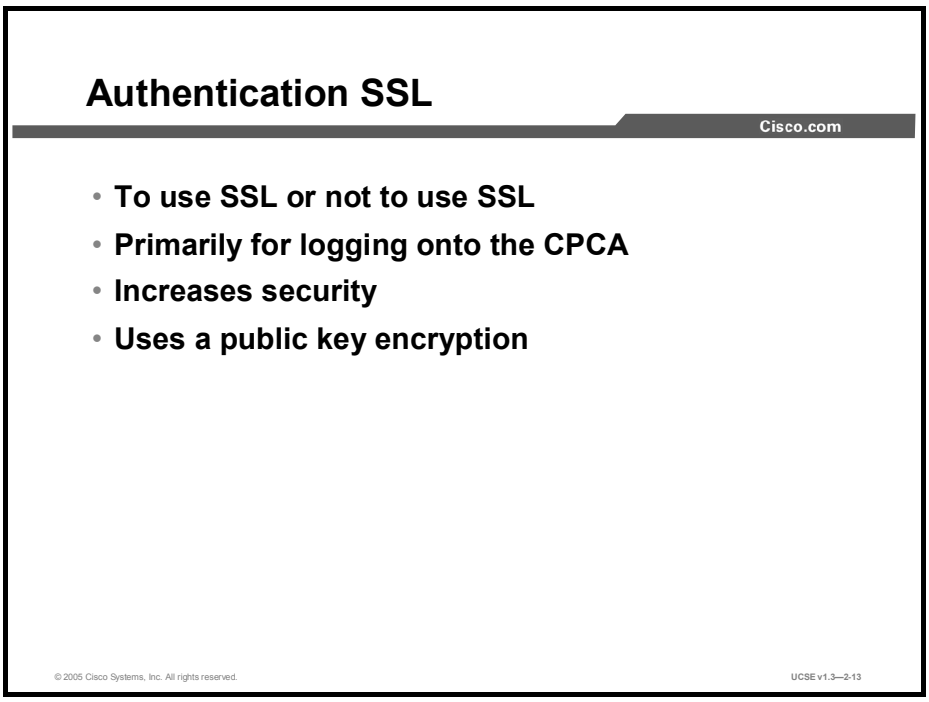
If you choose Telephony Service Provider (TSP) for Cisco Call Manager integration, you will need to have configured your Cisco CallManager to integrate with Cisco Unity before running UTIM. UTIM will ask for the Cisco CallManager IP address, the Display Name for the voice-mail ports created, and the Message Waiting On and Message Waiting Off dialed numbers (DNs). At the end of the process, you can run a test to ensure that the integration process was successful. Instructions on setting up Cisco CallManager to integrate with Cisco Unity can be found in the *Cisco CallManager Integration Guide*.

The PBX IP Media Gateway (PIMG) is an interface that allows for digital integration between Cisco Unity and a circuit-switched PBX, eliminating the need for voice boards.

SIP is an emerging Internet protocol designed to easily build up and tear down IP sessions. A number of vendors are embracing SIP as the next big Internet protocol for voice over IP. Currently, the Cisco Unity SIP integration will support interactions with Cisco SIP Proxy Server, as well as Cisco SIP-enabled 7960 IP Phones, Pingtel Expressa phones, and MSN Messenger.

Authentication SSL

This topic describes the Authentication Secure Socket Layer (SSL) process.



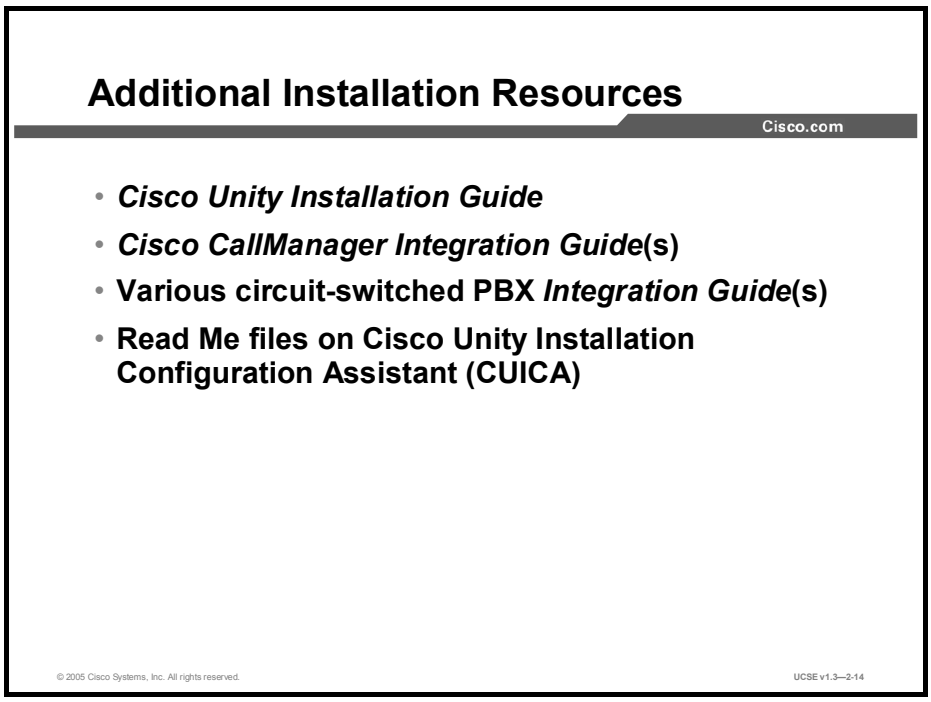
When subscribers log on to the CPCA, the default behavior is to send their credentials across the network to Cisco Unity in clear text. The same is true if you configure the Cisco Unity Administrator and the Status Monitor to use the anonymous authentication method. In addition, the information that subscribers enter on the pages of the CPCA and of the Cisco Unity Administrator (regardless of which authentication method it uses) is not encrypted.

For increased security, you should set up Cisco Unity to use the SSL protocol. SSL uses public-key encryption to provide a secure connection between servers and clients, and uses digital certificates to authenticate servers or servers and clients. (A digital certificate is a file that contains encrypted data that attests to the identity of an organization or entity, such as a computer.) Using the SSL protocol ensures that all subscriber credentials—as well as the information that a subscriber enters on any page of the Cisco Unity Administrator or the CPCA—are encrypted when the data is sent across the network. In addition, when you set up Cisco Unity to use SSL, each time that a subscriber tries to access any Cisco Unity web application, the browser will confirm that it is connected with the real Cisco Unity server, and not an entity falsely posing as such, before allowing the subscriber to log on.

To set up a web server such as Cisco Unity to use SSL, you can either obtain a digital certificate from a certification authority (CA) or use Microsoft Certificate Services available with Windows to issue your own certificate. A CA is a trusted organization or entity that issues and manages certificates at the request of another organization or entity. Cost, certificate features, ease of setup and maintenance, and the security policies practiced by the organization are some of the issues to consider when determining whether you should purchase a certificate from a CA or issue your own.

Additional Installation Resources

This topic describes the additional resources for a Cisco Unity installation.



A copy of the *Cisco Unity Installation Guide* is shipped with each Cisco Unity system. The installation manual contains information on installing the Cisco Unity system as a baseline (server purchased from Cisco), and as a component system (server supplied by the customer). In addition, there are instructions for upgrading earlier versions of Cisco Unity to Version 4.0.

If you are integrating Cisco Unity with Cisco CallManager, the *CallManager Integration Guides* are extremely helpful. There are different versions of the guides depending on your version of Cisco CallManager. Included are instructions for setting up your Cisco CallManager to integrate with Cisco Unity, as well as instructions for setting up a dual-switch integration.

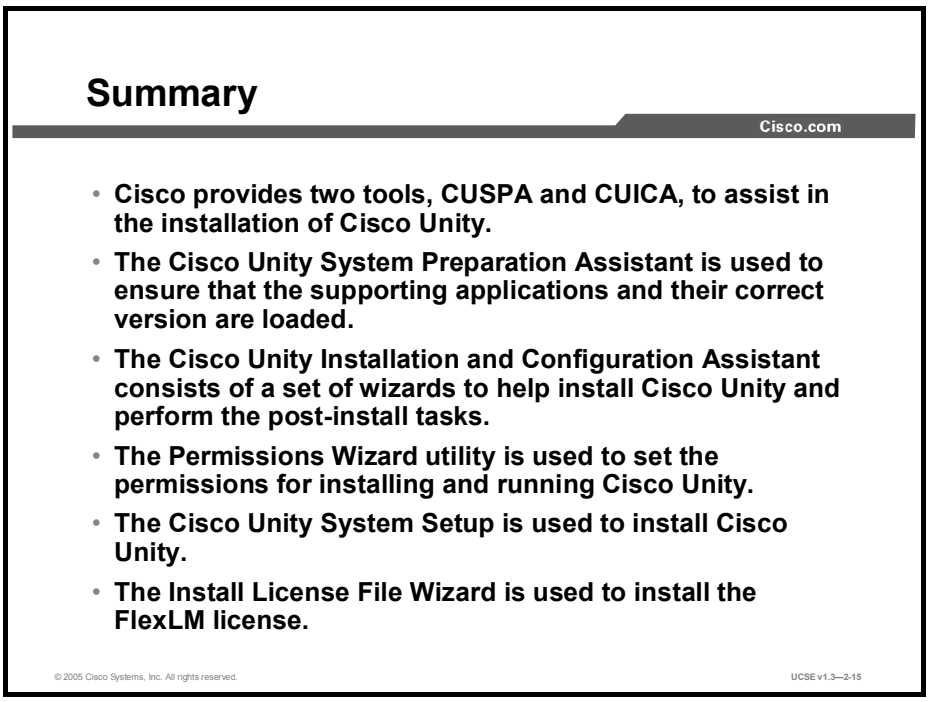
There are also various Integration Guides for supported circuit-switched telephone systems. These cover the programming on the circuit-based telephone systems necessary to integrate to Cisco Unity.

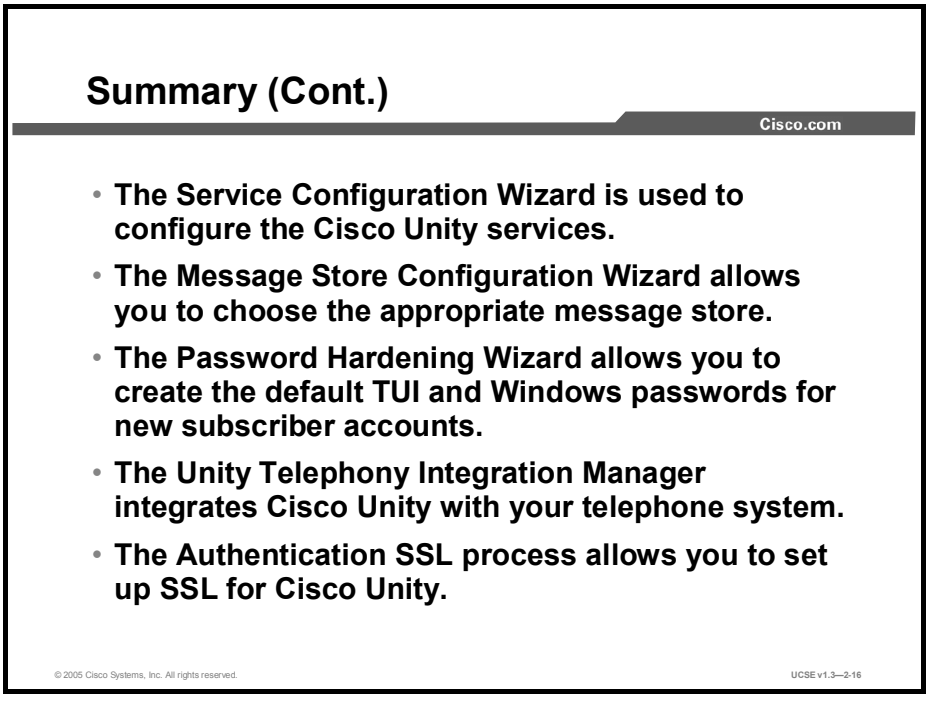
These documents are available at
http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/index.htm

The CUICA contains Read Me files to help guide you through the installation.

Summary

This topic summarizes the key points discussed in this lesson.





Next Steps

For the associated lab exercises, refer to the following sections of the course Lab Guide:

- Lab 2-1: Installing Cisco Unified Communications Software (Exchange)
- Lab 2-2: Installing Cisco Unified Communications Software (Domino)

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) The Cisco Unity System Preparation Assistant will check for which of the following? (Choose all that apply.)

A) SQL
B) Active Directory schema extensions
C) Active Directory
D) Microsoft Exchange
E) Internet Explorer

Q2) Choose the wizard utilities that combine with the Cisco Unity Setup Program in the Cisco Unity Installation and Configuration Assistant.

A) Authentication SSL wizard
B) Password Hardening wizard
C) Cisco Unity Server Preparation Assistant
D) Unity Telephony Integration Manager
E) Service Configuration wizard
F) Message Store wizard
G) Permissions wizard
H) Install License File wizard
I) Configure Voice Board Wizard

Q3) The Permissions Wizard sets permissions for which accounts?

A) Installer
B) Example Administrator
C) Messaging services
D) Example Subscriber
E) Directory service

Q4) The setup process of the CUICA configures which of the following? (Choose all that apply.)

A) the language choice
B) the number of users to be installed
C) codec
D) Cisco Unity folder and partition on the hard drive
E) the operating system

Q5) To register your copy of Cisco Unity and obtain your Cisco Unity license file, you will need to have the _____ and _____.

A) Purchase order number
B) MAC address of the NIC in the Cisco Unity server
C) Serial number on the Cisco Unity software media
D) Product authorization key
E) Serial number of the Cisco Unity server

Q6) The Service Configuration Wizard configures which Cisco Unity Services? (Choose three.)

A) directory services
B) access services
C) message store services
D) exchange services
E) local services

Q7) The Cisco Unity Telephony Integration Manager allows which of the following integrations? (Choose two.)

A) Cisco SIP Proxy Server
B) Cisco CUE
C) Direct Digital
D) Circuit-switched PBX
E) VPIM

Q8) Authentication SSL uses _____ encryption.

A) Private key
B) Public key
C) PGP security key
D) Cisco Security Agent key

Q9) In a Microsoft Exchange installation, which of the following tasks *must* be performed prior to installation? (Choose all that apply.)

A) obtain license
B) install Lotus Notes
C) load DUC
D) update Active Directory schema
E) load the SQL tools for viewing and working with the SQL databases

Quiz Answer Key

Q1) A, E

Relates to: Cisco Unity System Preparation Assistant

Q2) A, B, D, E, F, G, H

Relates to: Cisco Unity Installation and Configuration Assistant.

Q3) A, C, E

Relates to: Permissions Wizard.

Q4) A, C, D

Relates to: Cisco Unity System Setup

Q5) B, D

Relates to: Install License File Wizard

Q6) A, C, E

Relates to: Service Configuration Wizard

Q7) A, D

Relates to: Unity Telephony Integration Manager.

Q8) B

Relates to: Authentication SSL

Q9) A, D

Relates to: Additional Installation Resources

Lesson 3

Upgrading Cisco Unified Communications Software

Overview

This lesson describes the available upgrade paths and the steps involved in upgrading a previous version of Cisco Unity to Cisco Unity 4.0.

Relevance

Understanding the supported upgrades and the upgrade process will aid in the successful completion of a Cisco Unity upgrade. Some upgrades are complex, and not all upgrades from previous versions of Cisco Unity to Cisco Unity 4.0 are supported. Understanding this will avoid possible misunderstandings with your customer, and issues arising during the upgrade process.

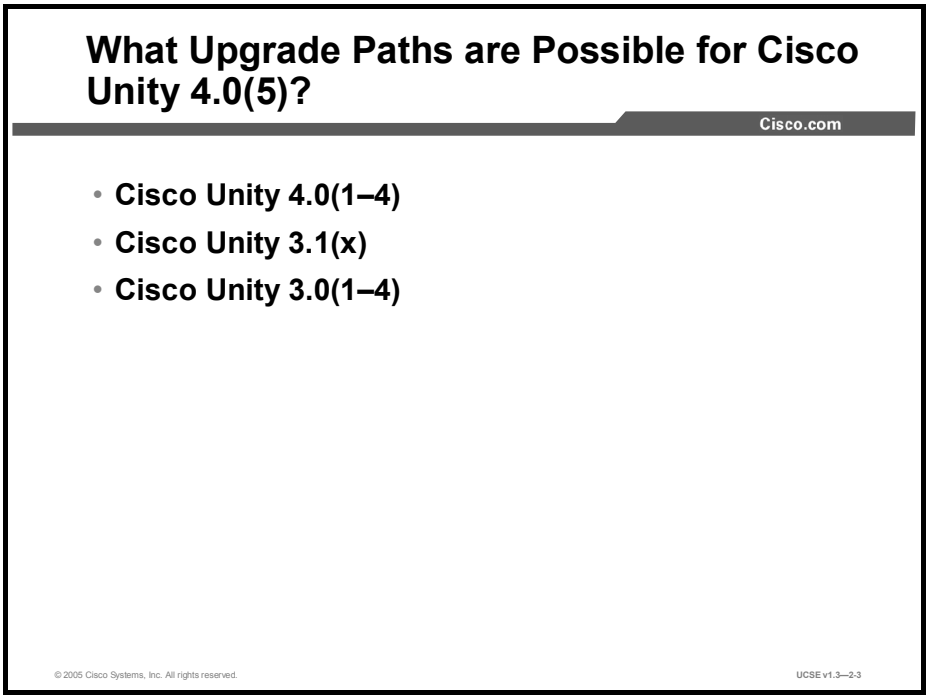
Objectives

Upon completing this lesson, you will be able to describe the steps necessary to perform an upgrade to Cisco Unity 4.0, and correctly perform an upgrade. This ability includes being able to meet these objectives:

- Identify the possible upgrade paths to Cisco Unity 4.0(5)
- Describe the steps required to upgrade from Cisco Unity 3.x to Cisco Unity 4.0(5) for Exchange
- Describe the steps required to upgrade from Cisco Unity 3.x for Exchange to Cisco Unity 4.0(5) for Domino

What Upgrade Paths Are Possible to Cisco Unity 4.0(5)?

This topic describes the possible upgrade paths to Cisco Unity 4.0(5).



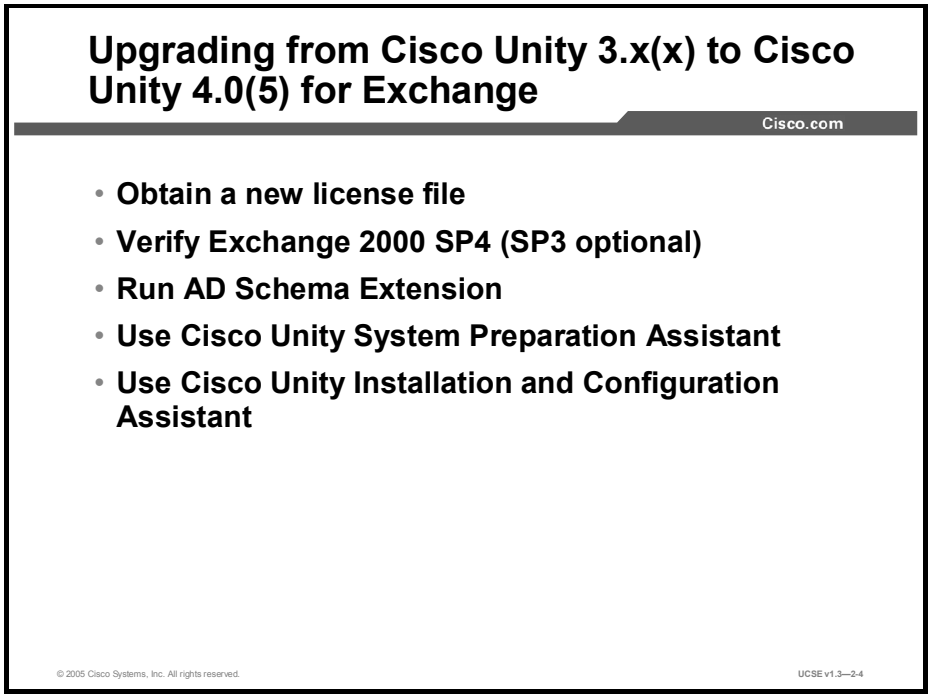
The upgrade to Cisco Unity 4.0(5) will be supported from the following previous versions of Cisco Unity:

- Cisco Unity 4.0(1–4)
- Cisco Unity 3.1(x)
- Cisco Unity 3.0(1–4)

However, versions of Cisco Unity prior to 3.0 will require a reinstallation of Cisco Unity, including a reentering of the database. Versions prior to Cisco Unity 3.0 stored database attributes in Exchange custom attributes 12 through 15, because the Exchange Directory Service was not extensible. With the release of Cisco Unity 3.0, Microsoft Structured Query Language (SQL) or Microsoft SQL 2000 Desktop Engine (MSDE) became the main database store. It is not possible to move the attributes from Exchange to SQL without reinstalling the database.

Upgrading from Cisco Unity 3.x to Cisco Unity 4.0(5) for Exchange

This topic describes the steps that are required to upgrade from Cisco Unity 3.x to Cisco Unity 4.0(5) for Exchange.

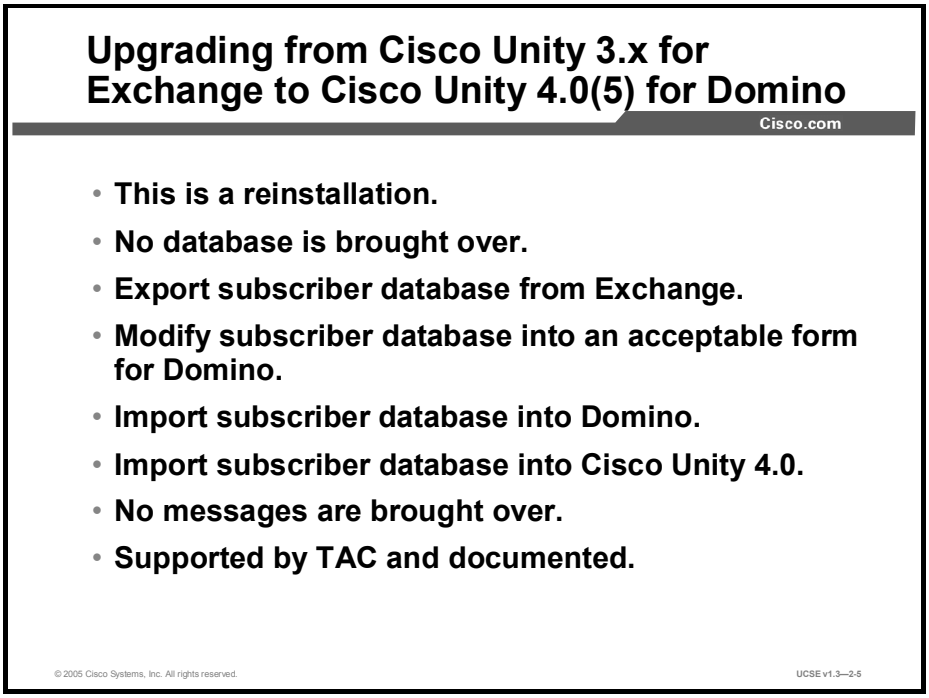


The upgrade procedure from Cisco Unity 3.x to Cisco Unity 4.0 for Exchange includes these points:

- You must obtain a new license file from Cisco, because the upgrade procedure itself will not upgrade the license file as it has in the past.
- You should ensure that Exchange 2000 SP3 or SP4 has been installed.
- There have been changes to the Active Directory (AD) Schema Extension utility that is run on the domain controller to extend the Active Directory schema for Cisco Unity. There is a new option in the AD Schema Extension utility for extending the schema for the Voice Profile for Internet Mail (VPIM) option, and the AD Schema Extension utility will need to be run for that option to function properly.
- The Cisco Unity System Preparation Assistant does not check for the Exchange version; however, the Cisco Unity Installation and Configuration Assistant will check for the Exchange version, and the Cisco Unity installation will fail if it does not find the correct version.
- The Cisco Unity Installation and Configuration Assistant will need to be run to load the new Cisco Unity 4.0 files. During this process there will be no database loss.

Upgrading from Cisco Unity 3.x for Exchange to Cisco Unity 4.0(5) for Domino

This topic describes the steps that are required to upgrade from Cisco Unity 3.x for Exchange to Cisco Unity 4.0(5) for Domino.

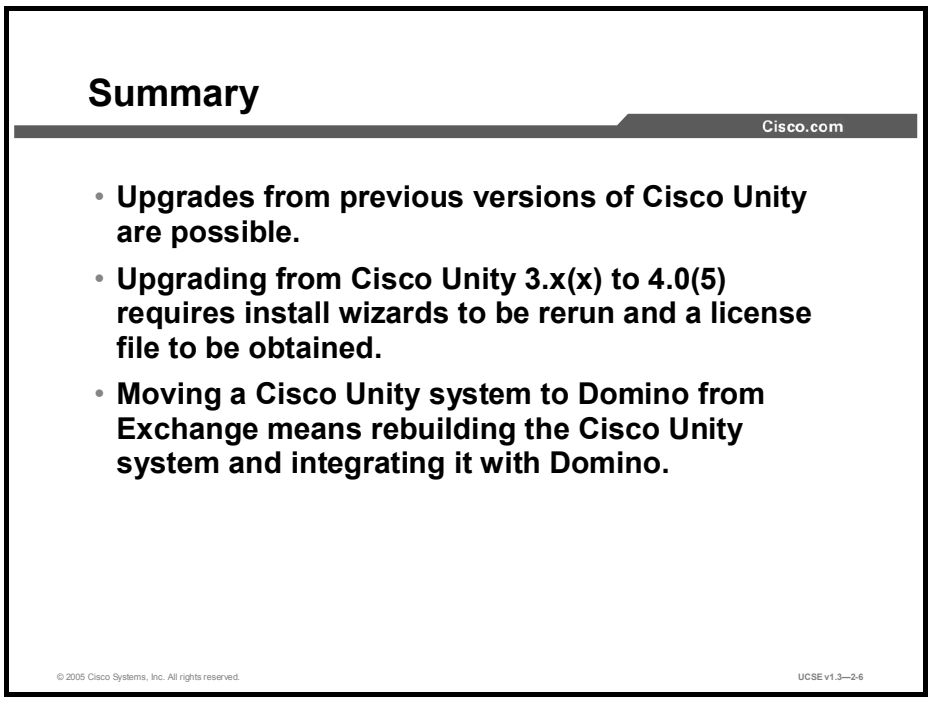


There may be circumstances when you will need to upgrade from Cisco Unity for Exchange to Cisco Unity for Domino. Customers in a Domino environment may have purchased Cisco Unity in a voice-mail-only configuration, awaiting the Cisco Unity Domino release so that they could gain the full benefits of unified messaging. A Cisco Unity voice-mail-only configuration is only supported in an Exchange environment.

Although the upgrade procedure for Cisco Unity 4.0 for Domino from Cisco 3.x for Exchange is supported and documented, you must keep in mind that this is basically a reinstallation. There is no way to carry over the database from one system to the other, because you have two completely different messaging systems. If you would like to save the subscriber database, you must export the subscriber database from Exchange, modify the subscriber database to a form acceptable to Domino, import it into Domino, and then import the subscribers from the Domino server into Cisco Unity 4.0. The information that will be exportable includes the subscriber names and extensions, but not the spoken name recordings, greetings, and so forth. Subscriber messages will not be brought over. Cisco does not offer a utility to accomplish this. Also, other Cisco Unity database information, such as call handlers, call routing tables, and restriction tables, are not brought over.

Summary

This topic summarizes the key points discussed in this lesson.



References

For additional information, refer to these resources:

- *Cisco Unity Installation Guide (with Lotus Domino)*, Release 4.0(5)
- *Cisco Unity Installation Guide (with Microsoft Exchange)*, Release 4.0(5)

Next Steps

For the associated lab exercises, refer to the following sections of the course Lab Guide:

- Lab Exercise 1: Installing Cisco Unified Communications Software (Exchange)
- Lab Exercise 2: Installing Cisco Unified Communications Software (Domino)

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) Which task must be performed before upgrading from Unity 3.0 to Unity 4.0(5)?

A) uninstall Cisco Unity 3.0
B) uninstall Exchange Message Store
C) uninstall AD schema updates
D) install Exchange 2003 Message Store
E) install AD schema updates

Q2) List tasks in order for upgrading from Cisco Unity 3.x(x) to Cisco Unity 4.0(4) for Exchange.

A)	Use the Cisco Unity System Preparation Assistant	1. _____
B)	Run AD Schema Extension on DC	2. _____
C)	Obtain a new license file	3. _____
D)	Use the Cisco Unity Installation and Configuration Assistant	4. _____
E)	Verify Exchange 2000 SP3 or SP4	5. _____

Q3) Which of the following items is carried over when moving a system from Cisco Unity for Exchange to Cisco Unity Domino?

A) Active Directory database
B) SQL database
C) Nothing
D) Messages

Quiz Answer Key

Q1) E

Relates to: What Upgrade Paths Are Possible to Cisco Unity 4.0(5)?

Q2) C, E, B, A, D

Relates to: Upgrading from Cisco Unity 3.x(x) to Cisco Unity 4.0(5) for Exchange

Q3) C

Relates to: Upgrading from Cisco Unity 3.x for Exchange to Cisco Unity 4.0(5) for Domino

Module Self-Check

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

Q1) The physical connection for the Cisco CallManager integration is a connection to which one of the following?

A) physical voice cards installed on the Cisco Unity server
B) connection to the LAN or WAN of the site
C) circuit-based telephone system
D) Cisco Unity Message Repository (UMR)
E) Cisco Unity Administration Active Server Pages (ASPs)

Q2) The Microsoft Active Directory will need to be installed on the Cisco Unity server if it will be in which configuration? (Choose one.)

A) if installed with Microsoft Exchange
B) if in VM-only configuration
C) when integrating Cisco Unity to a Cisco CallManager
D) when connecting to a circuit-switched telephone network
E) none of the above

Q3) The Cisco Unity for Domino configuration will only be supported in a(n) _____.

A) environment where Lotus Notes is not installed
B) VM-only environment
C) UM environment with Lotus Domino services installed *off* the Cisco Unity platform
D) UM environment with Lotus Domino services installed *on* the Cisco Unity platform
E) conjunction with Lotus Notes

Q4) When installing Cisco Unity for Domino, which of the following DUC need to be used on the Notes clients?

A) Install DUC 1.2.0 on Notes-enabled clients
B) Install DUC 1.2.1 on Notes-enabled clients
C) Install DUC 1.2.2 on Notes-enabled clients
D) Domino Notes Client 6.x only
E) Domino Notes Client 5.0.8 or higher

Q5) As of Cisco Unity 4.0(5), the DUC software is available through which channel?

A) IBM only
B) Cisco Systems
C) Microsoft
D) Novell

Q6) CUSPA does not check to make sure that the _____ has been extended for an Exchange 2000 install.

A) Exchange Server
B) Active Directory Schema
C) DHCP Scope
D) DNS Names Structure

Q7) All of the CUICA Wizard utilities except Message Store Configuration Wizard can be run individually after Cisco Unity is installed by accessing _____.

A) Unity Enterprise Tools
B) Tools Depot
C) System restart menu
D) Tools System menu

Q8) Using the Permissions Wizard, the System Engineer will be asked which of the following: (Choose all that apply.)

A) Which version of the message store will be used?
B) Which account should be given permissions to install and configure Cisco Unity?
C) Which account should Cisco Unity directory services log on with?
D) Which account should be used to log on to message store?
E) Which version of Internet Explorer is being used?

Q9) The purpose of the Cisco Unity System Setup of the installation process is _____.

A) to gather information for the Cisco Unity installation
B) to gather information for inputting subscribers
C) to gather information for creating call handlers
D) to gather information for building routing rules

Q10) In order to properly install and register your copy of Cisco Unity, you must do which of the following? (Choose two.)

A) Copy the license file on to the Cisco Unity server.
B) Run Cisco Unity Permissions Wizard.
C) Run the Install License File Wizard.
D) Obtain your Cisco Unity License File.
E) Submit the IP address of your Internet router to the TAC.

Q11) The Service Configuration Wizard uses the selections you made during the _____ as default accounts for the services.

A) Data Store setup
B) Permission Wizard
C) Message Store setup
D) Integration Wizard setup

Q12) In the Message Store Configuration Wizard, if you limit the creation of subscriber mailboxes to "import only," which of the following sources are allowed?

A) Active Directory
B) CSV file
C) Domino names.nsf
D) exported Exchange database file
E) Notes names.nsf

Q13) UTIM supports which kind of integrations with the phone system? (Choose three.)

A) IP Telephony (Cisco CallManager)
B) DNIS
C) circuit-switched PBXs
D) digital SMDS
E) SIP
F) analog MFT

Q14) When subscribers log on to the Cisco Personal Communications Assistant (CPCA) and SSL is not used, their credentials are sent across the network _____ to Cisco Unity.

A) with basic encryption
B) in plain text
C) credentials are not propagated to the end point
D) through a VPN tunnel

Q15) The Read Me files that are helpful in guiding system engineers through the Cisco Unity installation are located with the _____ utility.

A) CUICE
B) CUSPA
C) CUICA
D) CUCCA

Q16) Installing a voice-mail-only system or integrating Cisco Unity into an existing Exchange system requires that the following tasks be completed outside of the CUSPA and CUICA wizards: (Choose three.)

A) Identify the Active Directory that Cisco Unity will use or install a new Active Directory forest and domain.
B) Run the CUICA Wizard.
C) Update the Active Directory schema to include the Cisco Unity extensions.
D) Run the Exchange Update utility.
E) Join the schema admins group.

Q17) Which versions of Cisco Unity may be upgraded to version 4.0(5) without a reinstallation of Cisco Unity? (Choose three.)

A) Cisco Unity 2.0
B) Cisco Unity 2.4(5–6)
C) Cisco Unity 3.0(1–3)
D) Cisco Unity 3.1(x)
E) Cisco Unity 4.0(1–4)

Q18) When upgrading to Cisco Unity 4.0(5) from versions prior to Cisco Unity 3.0, you must obtain _____.

A) a new license file
B) an updated security key
C) the SQL update
D) new Exchange licenses

Q19) In upgrading to Cisco Unity 4.0(4) for Domino from Cisco Unity 3.x for Exchange, which items of information are exportable? (Choose two.)

A) subscriber extensions from Exchange
B) spoken name recordings from Cisco Unity
C) greetings from Cisco Unity
D) subscriber messages from Cisco Unity
E) subscriber names from Exchange

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent or better.

Module Self-Check Answer Key

Q1) B

Q2) B

Q3) C

Q4) B

Q5) B

Q6) B, Active Directory Schema

Q7) B, The Tools Depot of Cisco Unity

Q8) A, B, C, D

Q9) A, to gather general system information for the installation process

Q10) C, D

Q11) B, Permissions Wizard

Q12) A, C

Q13) A, C, E

Q14) B, in clear text

Q15) C, Cisco Installation Configuration Assistant (CUICA)

Q16) A, C

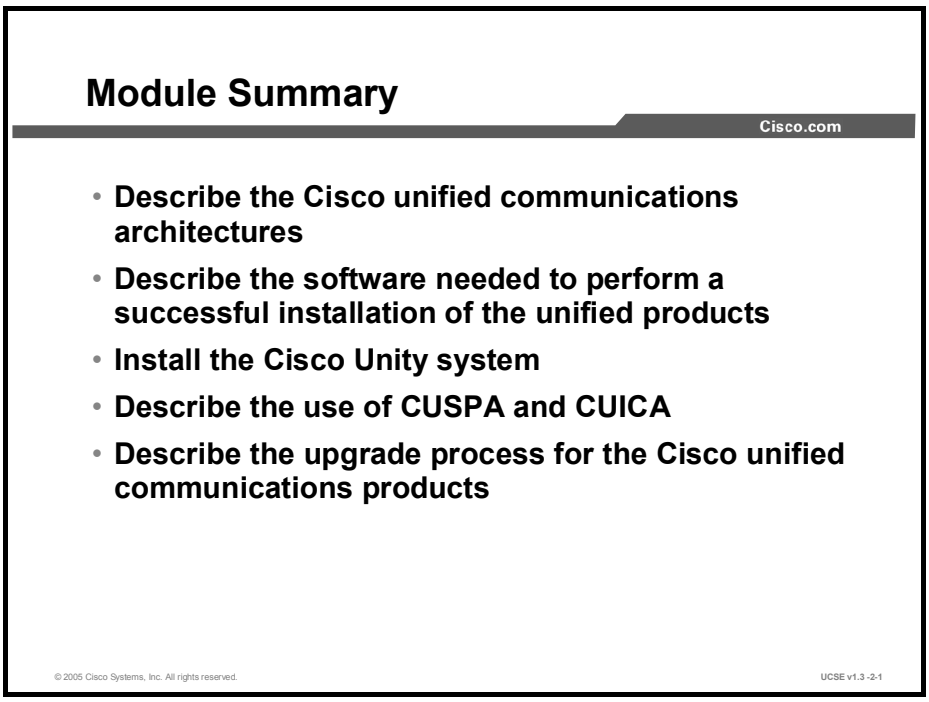
Q17) C, D, E

Q18) A

Q19) A, E

Module Summary

This topic summarizes the key points discussed in this module.



In this module, you learned about the underlying architecture and software required to install a Cisco Unity for Exchange and Cisco Unity for Domino server. The module described the steps necessary to perform such installations, as well as what is needed to upgrade to the latest Cisco Unity software version.

References

For additional information, refer to these resources:

- *Cisco Unity Installation Guide*

Module 3

Integrating Cisco Unified Communications Systems

Overview

This module describes the communication between a Cisco unified communications server and a telephone system. It describes the integration between Cisco Unity, Cisco CallManager, and circuit-switched PBXs.

Module Objectives

Upon completing this module, you will be able to choose the correct integration type, describe the steps needed to complete the integration, and describe the integration of Cisco unified communications systems with particular telephone switches. This ability includes being able to meet these objectives:

- Given a list of the possible types of integration available for a Cisco Unity system, choose the correct type for a given telephone switch
- Given a Cisco Unity system with Cisco CallManager, describe the programming and configuration setup necessary to integrate Cisco CallManager with Cisco Unity
- Define the attributes of unified communications integration

Lesson 1

Choosing Available Unified Communications Integrations

Overview

This lesson describes the attributes of unified communications integrations. You will learn the attributes of a communications integration between Cisco Unity and a telephone system.

Relevance

Understanding the attributes of a communications integration aids a technician during the installation process and while analyzing integration issues that may arise. In many instances, technicians troubleshoot the Cisco Unity server when in fact the issue may lie with the telephone system. The knowledge gained from this lesson can save valuable time when troubleshooting integration issues.

Objectives

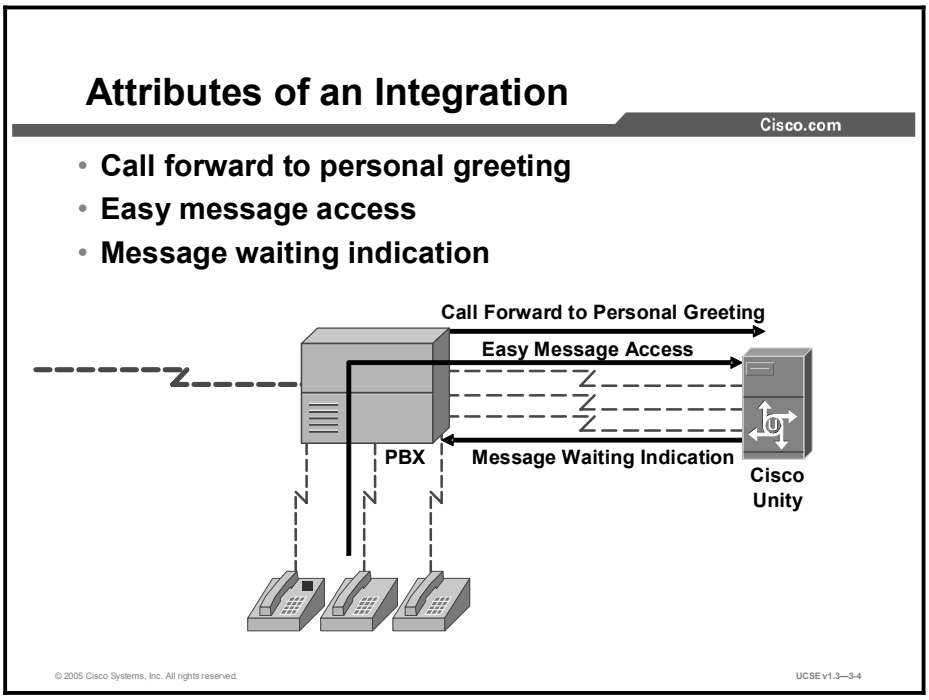
Upon completing this lesson, you will be able to describe the attributes of unified communications integrations. This ability includes being able to meet these objectives:

- Describe the three essential attributes of a communication integration between Cisco Unity and a telephone system
- Describe how Cisco Unity messaging systems integrate with Cisco CallManager using the Cisco Unity-Cisco CallManager TSP
- Describe how Cisco Unity messaging systems integrate with a telephone system using DTMF
- Describe how Cisco Unity messaging systems integrate with a telephone system using SMDI
- Describe how Cisco Unity messaging systems integrate with a telephone system using a PBXLink box
- Describe how Cisco Unity messaging systems integrate with a telephone system using a PIMG
- Describe how Cisco Unity messaging systems integrate with a telephone system using SIP

- Describe how the Cisco Unity messaging system can perform dual integration with a traditional circuit-switched PBX as well as Cisco CallManager
- List the supported telephone systems for Cisco Unity
- Define a messaging port and describe how it communicates between the telephone system and Cisco Unity
- Describe the five settings that can be used to configure a messaging port
- Describe the guidelines for configuring the Cisco Unity ports

Attributes of an Integration

This topic describes the three essential attributes of a communication integration between Cisco Unity and a telephone system.



A telephone switch and a voice processing system communicate with each other via an integration. An integration between Cisco Unity and a PBX takes place when the following three essential features are present:

- Call forward to personal greeting
- Easy message access
- Message waiting indication

These features are present when the PBX and the voice messaging system are exchanging information with each other in an agreed-upon manner. How the information is transferred between the two systems varies from integration to integration.

The basic integration types are as follows:

- IP-based, in-band dual tone multifrequency (DTMF)
- Simplified Message Desk Interface (SMDI)
- PBXLink
- PBX IP Media Gateway (PIMG)
- Session initiation protocol (SIP)

Cisco messaging systems currently integrate with telephone systems that make up approximately 70 percent of the business telephone market. Once an integration is made, the PBX and the voice-mail system work together, sharing information regarding call routing and message notification.

Call Forward to Personal Greeting

The Call Forward to Personal Greeting feature is essential to the working of voice mail. Call Forward to Personal Greeting is the way that the telephone system tells Cisco Unity what greeting to play. For a call to be routed to the correct greeting, information must be sent from the PBX along with the call to instruct Cisco Unity about what to do with the call. The integration packages enable information regarding station identification to be sent to Cisco Unity, which then plays the appropriate greeting.

The different integrations perform in various ways, as follows:

- An IP integration passes call information over the IP network using Skinny Station Control Protocol (SSCP) or PIMG.
- DTMF integration passes call information using DTMF tones.
- SMDI integrations pass call information along in a small packet of data sent via a serial cable or over a combination of modems and phone lines such as Centrex.
- PBXLink integrations must have special digital lines installed that will transmit information.
- SIP integrations send all call setup, control, and breakdown information as text-based packets on the network cabling connecting the devices at each end of the session.

With each call, the following call information is typically passed between the phone system and Cisco Unity:

- **Dialed number identification service (DNIS):** The extension of the called party.
- **Automatic number identification (ANI):** The extension of the calling party (for internal calls) or the phone number of the calling party (if it is an external call and the phone system supports Caller ID).
- **The reason for the forward:** The extension is busy, does not answer, or is set to forward all calls.
- **Redirected Dialed Number Identification Service (RDNIS):** The redirected extension of the called party.

Easy message access

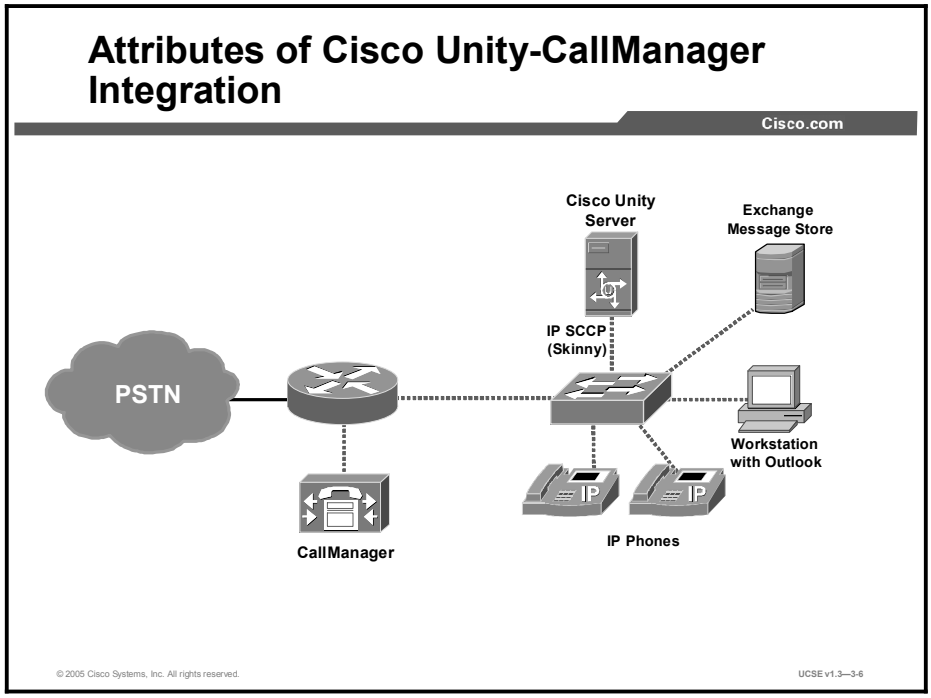
Cisco Unity recognizes a subscriber when they enter a one- or two-button code on their extension, without the subscriber needing to enter their personal ID. In any integration, the recognition is accomplished because the telephone system has been programmed to download the digits of a subscriber personal ID in response to that particular key sequence. You press one or two keys at your extension, for example “72,” or you may press a button labeled “VM” or “Messages” on your telephone, and the telephone switch transfers the call to the hunt group for the voice mail and sends along the digits for a Personal ID, such as “*1408.” The next thing you hear in the conversation is either a request for your password or the beginning of the subscriber conversation. With this feature present, subscribers should password-protect their voice mailboxes.

Message waiting indicators

The third feature that defines an integration is the ability of Cisco Unity to send codes to the PBX to activate and deactivate Message Waiting Indicator (MWI). That integration will take different forms, depending on the telephone switch and the telephone sets attached to it. The indicator can be a steadily lit or flashing light, a word on an LCD panel, or a special tone heard when the handset is picked up.

Attributes of Cisco Unity-Cisco CallManager Integration

This topic describes the attributes of communication integration between Cisco Unity and Cisco CallManager.



With the introduction of computer-based telephone switches that communicate via an Ethernet connection, voice-mail systems are challenged to integrate using a new method. Most IP-based telephone switches use Telephony Application Programming Interface (TAPI) to communicate with third-party devices, such as voice-mail systems. In designing Cisco Unity, Cisco decided to use TAPI as the communications protocol between all voice boards and itself. As a result, integration of the IP-based switch from Cisco is a straightforward matter. Because the switch and voice mail are on separate servers, each server must know the other's IP address so they can communicate across the network.

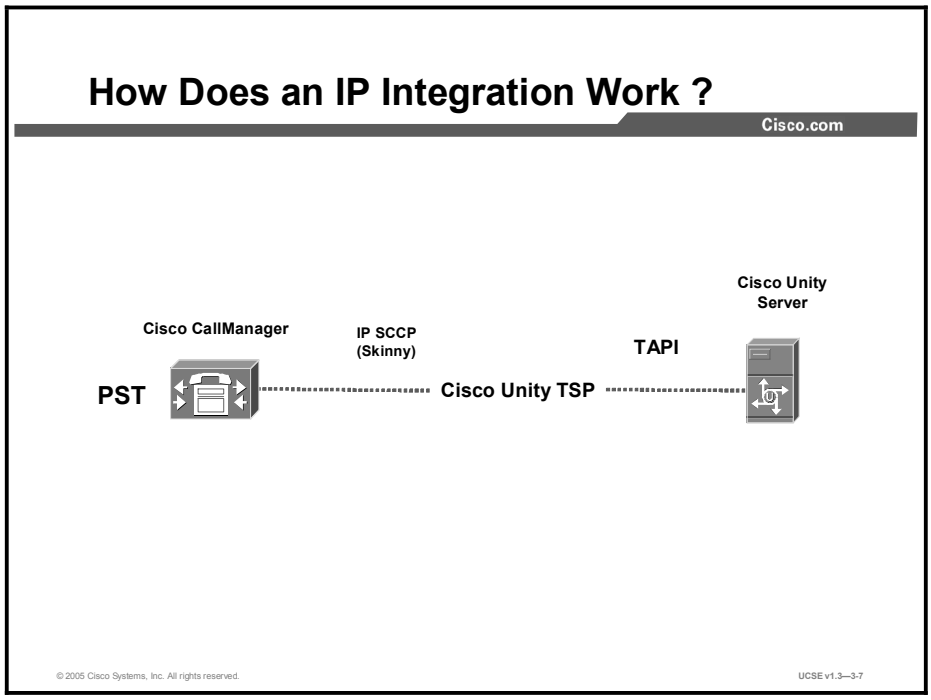
There are many ways in which Cisco CallManager and Cisco Unity can be configured, depending on the customer requirements and the existing network topology of the site.

The issues involved are mostly focused around WAN deployments. Most LAN deployments are very flexible, since there are fewer bandwidth constraints. It is important to understand how all the components interact in order to determine what works best for the customer.

When planning for an IP integration, both quality of service (QoS) and bandwidth requirements have to be considered throughout the entire network. In the LAN, although bandwidth may not be an initial issue, bottlenecks, aggregation points, and speed mismatches can all cause voice to be dropped if the queues overflow. In the WAN, there are major obstacles in serialization, propagation, and limited bandwidth. When planning for bandwidth, if you are using G.711 you need to plan for 80 kbps per call per port. In a system that has 32 ports, 32 x 80 = 2560 kbps is required for just the voice traffic going to the Cisco Unity system. If G.729 is used, 32 x 24 = 768 Kbps is required for voice traffic going to the Cisco Unity system. If ten simultaneous users use voice mail over a WAN, then, if G.711 is used, 10 x 80 = 800 kbps of bandwidth is needed just for voice traffic in the WAN. For more information on designing a Cisco Unity system, see the *Unity Design Guide*.

How Does an IP Integration Work?

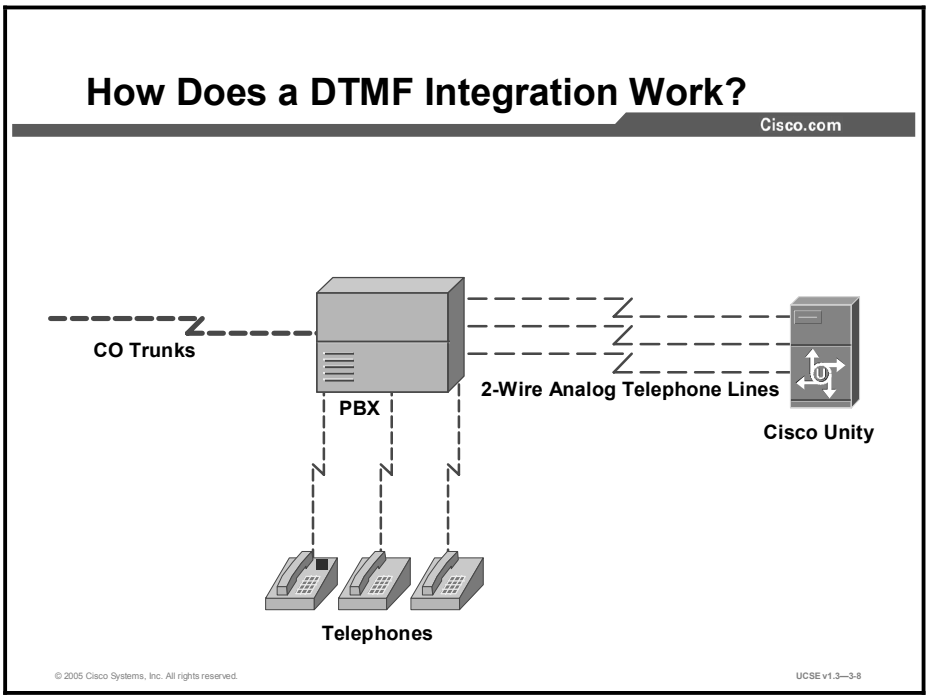
This topic describes how Cisco Unity messaging systems integrate with Cisco CallManager using the Cisco Unity-CallManager Telephony Service Provider (TSP).



Cisco CallManager communicates with all telephones using SSCP. Because Cisco Unity appears as a collection of single-line extensions to all PBXs, it must present its communication to and from Cisco CallManager in that form. The TSP is basically a translator that will take the Skinny Protocol messages and convert them to TAPI and take the TAPI messages and convert them to Skinny. Cisco Unity just sees the lines as TAPI lines, and does not really care about the underlying integration.

How Does a DTMF Integration Work?

This topic describes how Cisco Unity messaging systems integrate with a telephone system using DTMF.

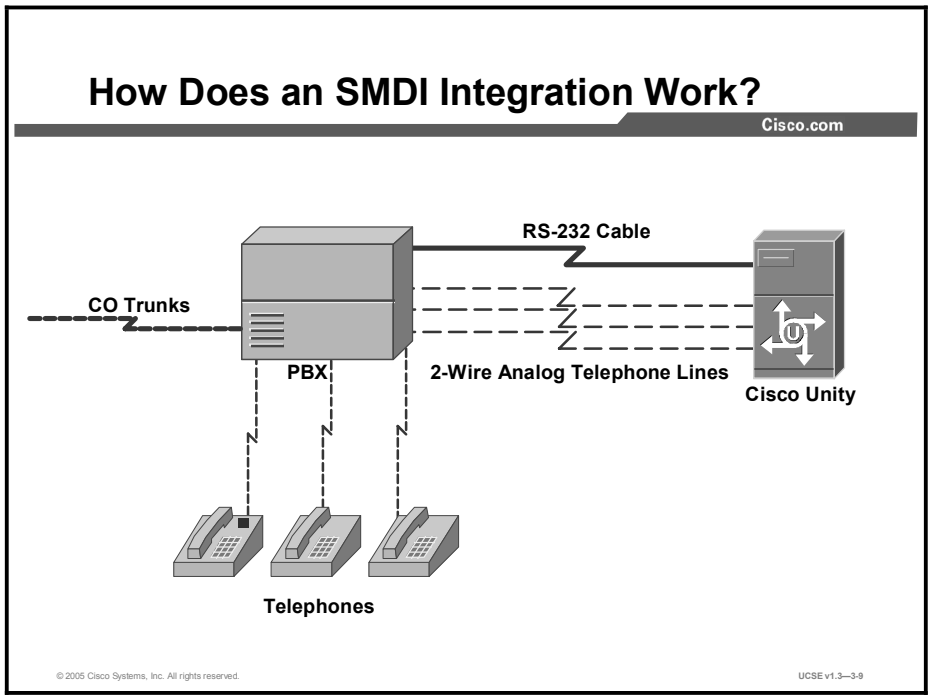


A telephone switch (PBX) using a DTMF integration sends a series of DTMF tones to the voice processing system that communicates information needed for Call Forward to Personal Greeting and Easy Message Access. The voice processing system in turn sends DTMF tones to the telephone switch to tell it to turn MWI on or off.

When a call initially comes in to Cisco Unity and the caller enters an extension, the system puts the caller on hold and dials the extension listed in the subscriber page for the extension ID listed. Once the caller is on hold, Cisco Unity outpulses the extension and then either waits on the line listening for ringing (Supervise Transfer) or releases the call (Release to Switch). If the call goes unanswered for the specified number of rings (either in Cisco Unity or the PBX programming, depending on the transfer type used), the call comes back to Cisco Unity. In the case of a supervised transfer, Cisco Unity still has control of the call, so it sends the call directly to the personal greeting. In the case of a release transfer, Cisco Unity answers as if it is a new incoming call, and the PBX pulses out in DTMF tones the call forwarding digits needed by Cisco Unity to play the correct subscriber personal greeting.

How Does an SMDI Integration Work?

This topic describes how Cisco Unity messaging systems integrate with a telephone system using SMDI.



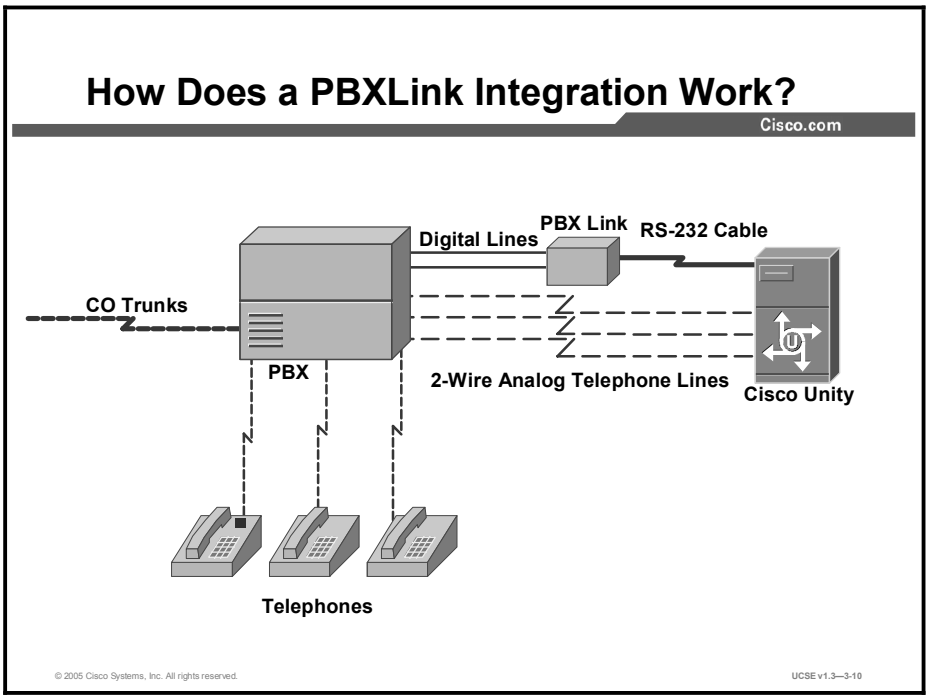
An SMDI integration usually uses an RS-232 cable to connect the voice-mail and telephone switch. The serial cable plugs into the voice processing system on one end and the telephone switch on the other end. This is also known as out-of-band signaling because the information about the call is carried on a different channel than the voice traffic. In contrast, an in-band DTMF solution carries the information about the call on the same port that carries the voice traffic.

SMDI integrations using a serial cable have a 100-foot connection limit determined by the technical specifications of the RS-232 standard. If you are using Centrex lines, in which the central office serves, in effect, as an offsite PBX, a dedicated line connected by modems at each end allows you to bypass the 100-foot limit. The serial packets sent are sometimes referred to as SMDI packets. This is the standard protocol used by Centrex, but also used by the NEC 2000 and the NEC 2400, among others.

A serial integration is more difficult to configure because of the variables involved: switch programming, cable configurations, and COM port configurations. Once it has been set up, a serial integration is both extremely reliable and quicker than a DTMF integration, particularly in the area of servicing MWI requests.

How Does a PBXLink Integration Work?

This topic describes how Cisco Unity messaging systems integrate with a telephone system using a PBXLink box.

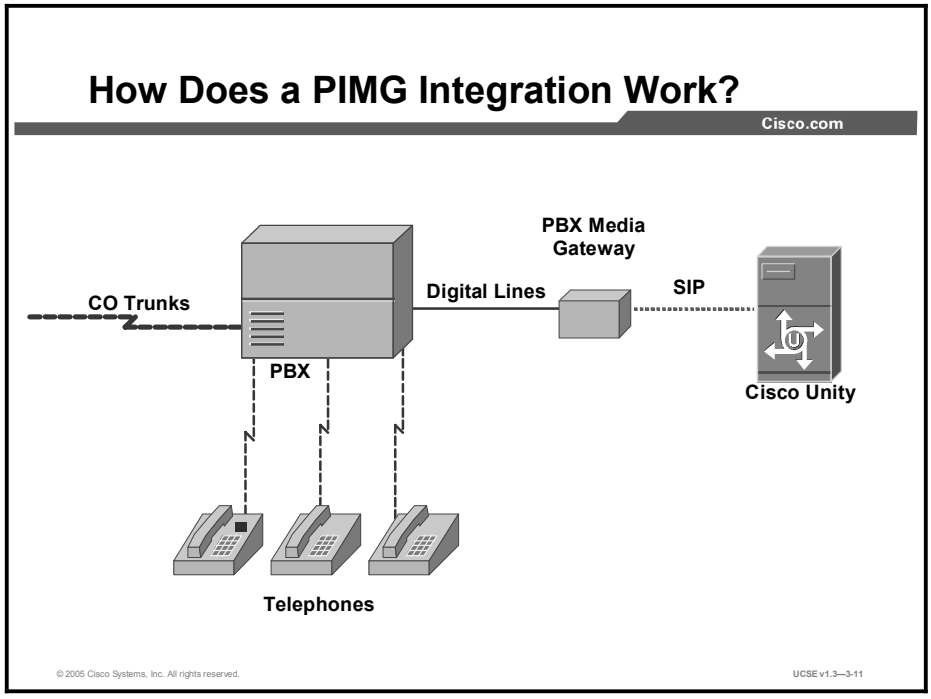


The PBXLink box provides an integration solution for several telephone switches, among them the Avaya Definity Gx and the Nortel Meridian-1. The PBXLink box works in conjunction with the voice boards inside Cisco Unity. The voice boards used in the integration are the standard boards available for Cisco Unity systems. Which boards are used will be determined by the configuration that makes the most efficient use of slots in the server.

The PBXLink is attached to the PBX via digital lines and programmed through feature set keys on the corresponding digital stations. The PBXLink uses the busy indicators to determine which analog lines between the PBX and the voice mail are busy, and when calls arrive at the voice-mail system, the PBXLink gathers the call information from the display of the digital set. The PBXLink reads the digital information about the call (called party extension, reason for the forward, and calling party extension on internal calls), translates that into SMDI packets, and sends the information through the RS-232 cable to the voice mail. The PBXLink box sends the information about the call (for example, which personal greeting to play when a call is forwarded to voice mail on a Ring No Answer) across the RS-232 cable. The PBX sends the call to the voice messaging system through the analog lines connecting the voice boards and the switch.

How Does the PIMG Integration Work?

This topic describes how Cisco Unity integrates with a telephone system using the PIMG.



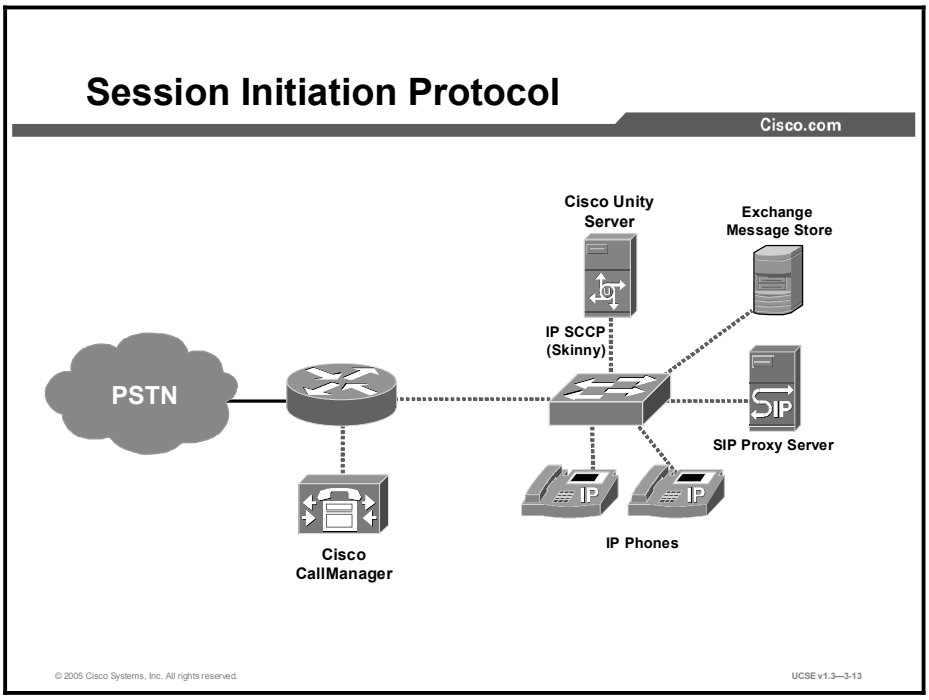
The PIMG is an interface allowing Cisco Unity to connect to circuit-switched PBXs through digital phone lines. The PIMG box converts the digital information coming from the PBX to SIP which is passed to Cisco Unity. Although it seems very similar to a PBXLink integration, the main distinguishing factor is the ability to use the IP network to communicate with Cisco Unity, thereby eliminating the need for voice boards in the Cisco Unity.

Eliminating the requirement for voice boards in Cisco Unity can result in a real cost savings to the customer. Many customers have digital cards in their PBXs to support their digital phone sets, but they are unlikely to have analog cards that are needed to supply analog lines in the PBX. Circuit-switched PBXs communicate with Cisco Unity through the analog lines and Intel Dialog voice boards. In many cases, such as with the PBXLink integration, the customer would have to invest in analog cards for their PBX in order to support analog lines for Cisco Unity. The PIMG integration eliminates that cost.

The PIMG integration is supported on the Siemens Hicom 300 and the Avaya G3 PBX.

Session Initiation Protocol

This topic describes how Cisco Unity messaging systems integrate with a telephone system using session initiation protocol (SIP).



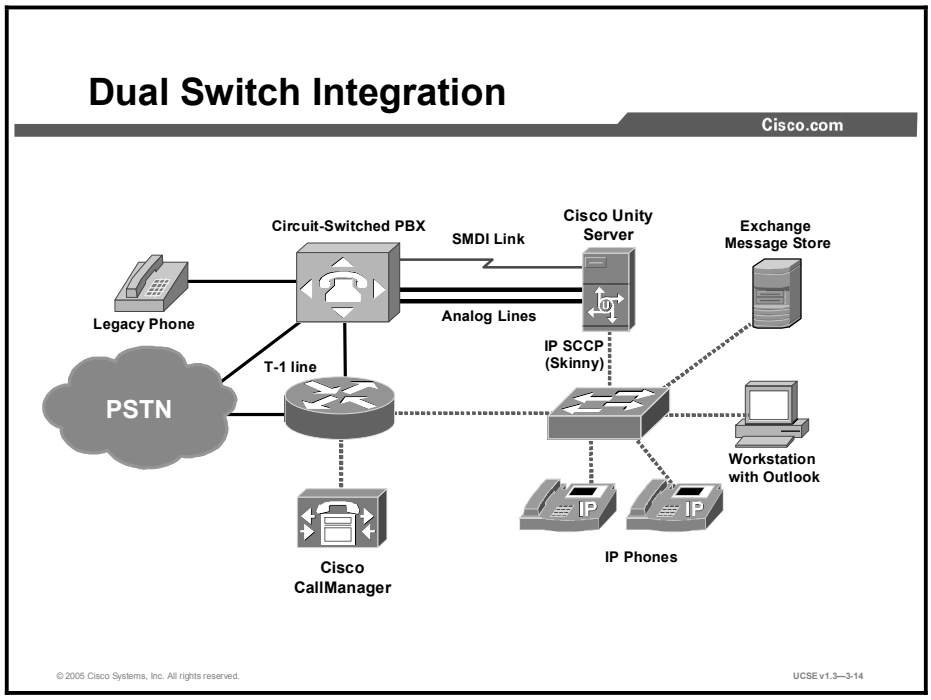
The SIP integration uses a Cisco SIP proxy server to set up communication between the voice messaging ports on the Cisco Unity server and the appropriate endpoint (for example, a SIP-enabled phone). The communications occur through an IP network (LAN, WAN, or Internet) to all SIP-enabled devices connected to it.

The proxy server sends the following information with the calls forwarded in the SIP message:

- The extension of the called party
- The reason for the forwarding call
- The extension of the calling party, for internal calls, or the SIP URL of the calling party if it is an external call and the system uses Caller ID

Dual Switch Integration

This topic describes how the Cisco Unity messaging system can integrate with a traditional circuit-switched PBX and Cisco CallManager simultaneously.



Compatibility between voice or unified messaging systems, the existing PBX equipment, and IP telephony solutions is a primary concern for most enterprises. Users must experience uninterrupted service and be offered a familiar interface in order to ensure a smooth migration from a traditional PBX system to an IP telephony environment.

Dual switch integration provides a superlative integration for customers who currently have a traditional circuit-switched PBX and would like to migrate to Cisco CallManager. This integration preserves a customer's investment in their circuit-switched infrastructure while simultaneously allowing for migration to packet-switched technology at any pace the customer chooses. This allows enterprises to operate in a hybrid environment while maintaining consistent voice messaging service across the organization.

Cisco Unity solutions are designed to provide connectivity with Cisco CallManager and existing PBX equipment at the same time. In addition to connectivity, Cisco Unity solutions also support complete voice-mail integration between both systems simultaneously.

Dual switch integration is also available in connecting Cisco Unity CallManager and a Cisco SIP proxy server.

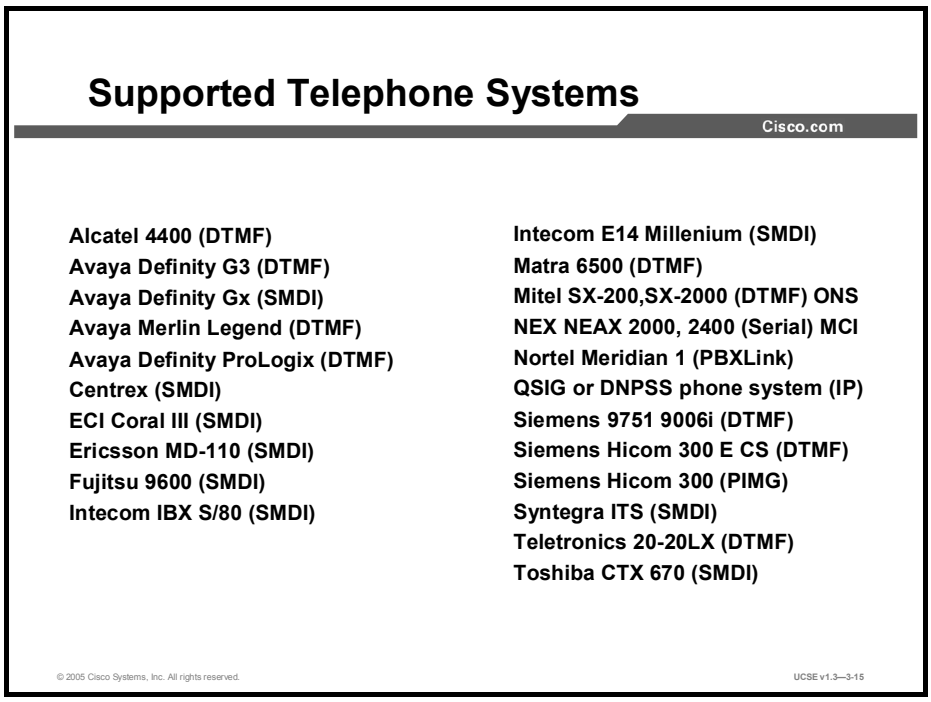
The best source for information about the Cisco Unity-Cisco CallManager integration in a dual switch environment is one of the integration guides in the *Cisco CallManager Integration Guide* series. You can find this information on the Cisco website at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/integuid/index.htm

Requirements for the telephone systems, settings for the Cisco Unity Administrator, switch settings in Cisco CallManager, and other topics are covered in the guides.

Supported Telephone Systems

This topic lists the supported telephone systems for Cisco Unity.



The figure lists the currently supported telephone systems for Cisco Unity 4.0.

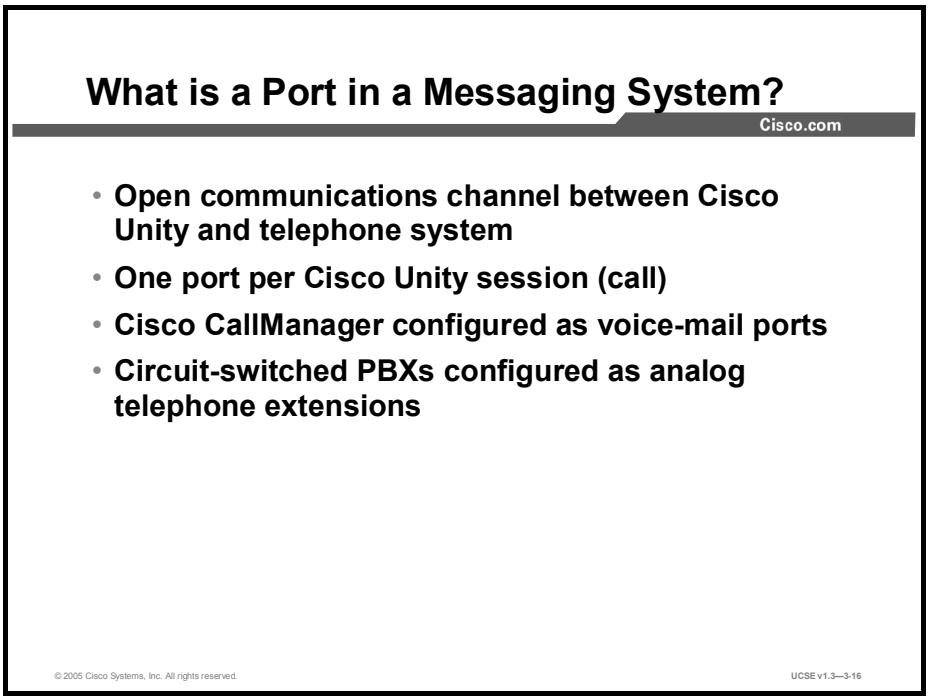
Cisco conducts extensive testing before qualifying a telephone system for use with Cisco Unity. Telephone systems are tested under many different call scenarios, and troubleshooting information is created. Cisco Technical Assistance Center (TAC) will not support systems not appearing on the list. If you do decide to install Cisco Unity on a nonsupported telephone system, you will be responsible for all integration issues on that system.

The complete list of supported telephone systems may be found on the Cisco website at the following URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_pre_installation_guide09186a0080117617.html#31803

What Is a Port in a Messaging System?

This topic defines a messaging port and describes how it provides communication between the telephone system and Cisco Unity.



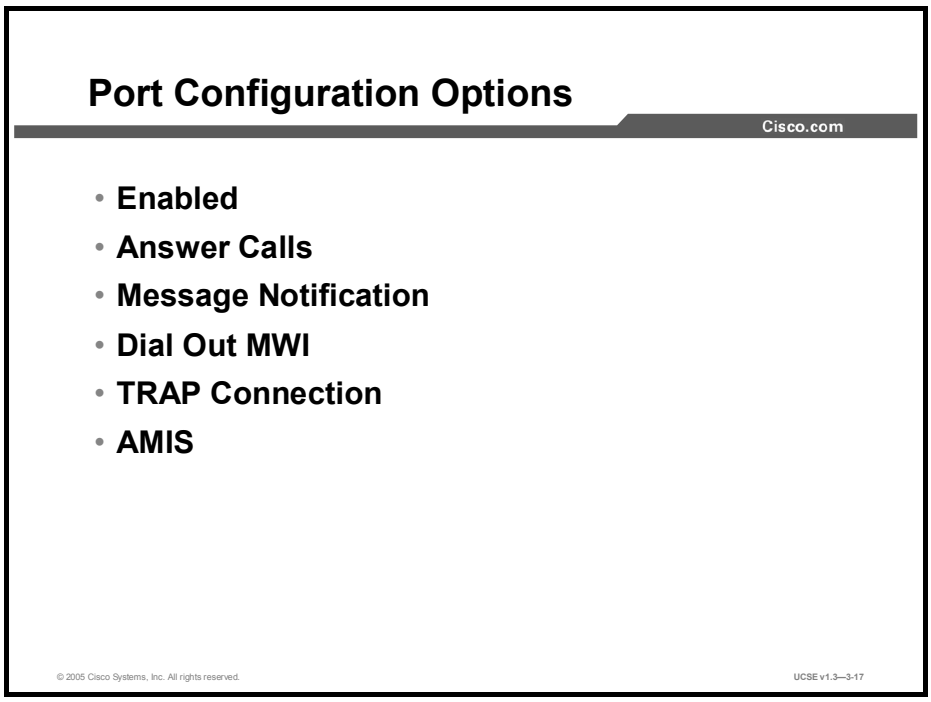
The Cisco Unity voice-mail ports are important parts of the general setup. Ports are also referred to in many of the Cisco Unity documents as sessions. The term “port” is a telephony term, originating when a physical connection was made between voice mail and the telephone switch. The term “session” is used in the IP telephony world.

A messaging port is an open communications channel between the telephone system and Cisco Unity. When Cisco Unity answers a public switched telephone network (PSTN) call or a call from a user checking messages, it uses a port. Cisco Unity requires one port for every simultaneous telephone call. Determining how many ports you require depends on the corporate messaging needs of your customer. Such features as Auto Attendant, Audiotext, Message Notification, and whether it is a DTMF integration can affect the number of ports required.

In Cisco CallManager, each Cisco Unity messaging port is configured as a voice-mail port. In circuit-based PBX integrations, the Cisco Unity messaging ports are analog extensions, with one extension used per port.

Port Configuration Options

This topic describes the settings that can be used to configure messaging ports.



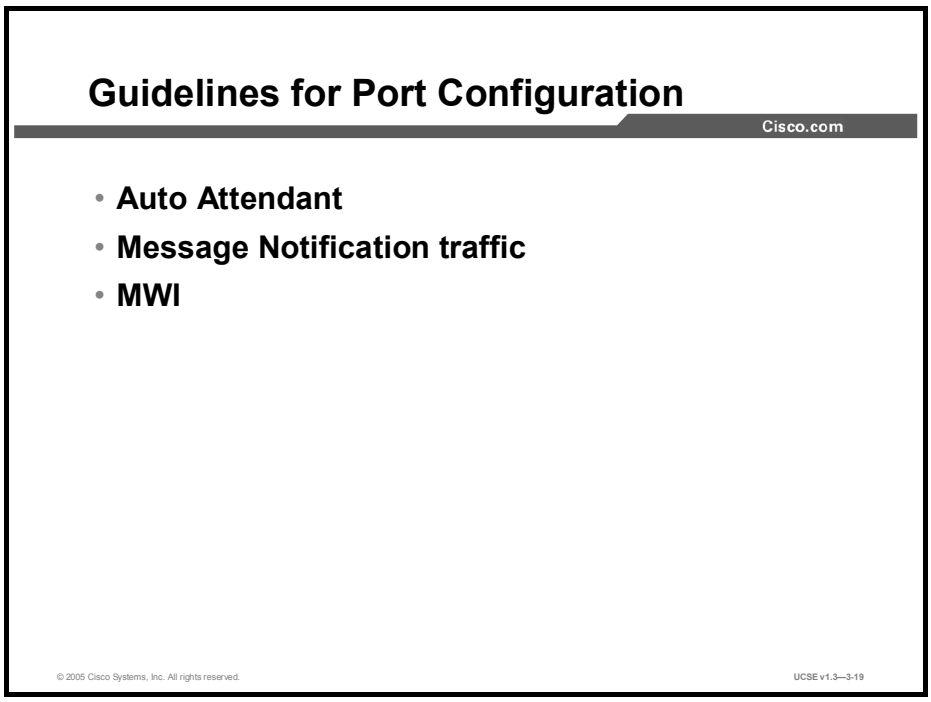
How the individual ports on your Cisco Unity server are configured will depend on your corporate messaging needs. Each Cisco Unity messaging port can be configured to one of the following five settings:

- **Enabled:** This setting means that the port is in service. If this setting is unchecked, the port is out of service, and the caller who reaches that port will receive ringing tones but the call will not be answered. You can uncheck this setting if you are having issues with that particular port or extension from the telephone system and you do not want callers to access that port. If you uncheck the setting, you should remove that port from the hunt group you created to prevent callers from accessing that port.
- **Answer Calls:** This setting means that Cisco Unity will answer a call received on this port. This can be either a call coming in from the PSTN or an internal call coming from the office extension number of a subscriber. Unchecking this setting means that Cisco Unity will not accept an incoming call on this port.
- **Message Notification:** This setting allows the Cisco Unity port to dial out calls for message notification, such as to a pager, a mobile phone, a text pager, and so on. Dialouts are subject to Restriction Table settings as discussed in the UCSA course.
- **Dial Out MWI:** The Message Waiting Indicator is the message light on the telephone. This setting allows the Cisco Unity port to dial out the message lamp on and off codes associated with telephone systems.

- **TRAP Connection:** The Telephone Record and Playback Connection (TRAP) is used during telephone recording and playback of greetings through the Media Master in Cisco Unity. The Media Master is used when recording or playing greetings using the Cisco Personal Communications Assistant (CPCA) or through system administration screens. Unchecking this setting for all ports would require users to use the microphone connected to their PC multimedia device for record and playback.
- **AMIS:** Calls between Cisco Unity and another voice mail system supporting the AMIS protocol use a port on the Cisco Unity system. Depending on the amount of AMIS traffic that you anticipate, you may need to configure more than one port for AMIS traffic.

Guidelines for Port Configuration

This topic describes the guidelines for configuring the Cisco Unity ports.



The configuration of your Cisco Unity ports is determined by your corporate messaging needs. Cisco Unity is feature-rich, and your use of the features directly impacts how the ports will be configured.

The Auto Attendant feature can affect the port configuration by requiring the Answer Calls setting to be used on all ports. To ensure that callers do not receive a busy signal when calling, you should set as many ports as possible to answer those calls.

The Message Notification feature of Cisco Unity can greatly increase the dial-out usage of the ports. Every subscriber has the option of having up to 13 different message notification devices configured to notify them when they have messages in their mailbox. If a port is not available, the message notification will be queued, and user notification may be delayed. The length of the delay will depend on how many message notifications are queued.

If the Dial-Out MWI setting is not selected on a sufficient number of Cisco Unity ports, there will be a delay in the lighting and extinguishing of message-waiting lamps on the user telephone. This may result in complaints of delayed messages, lamps not being lit, or the lamp not going out. These scenarios can occur on those installations using DTMF or (to a much lesser extent) on IP integrations. Serial and PBXLink integrations do not use Cisco Unity messaging ports to light message-waiting lamps.

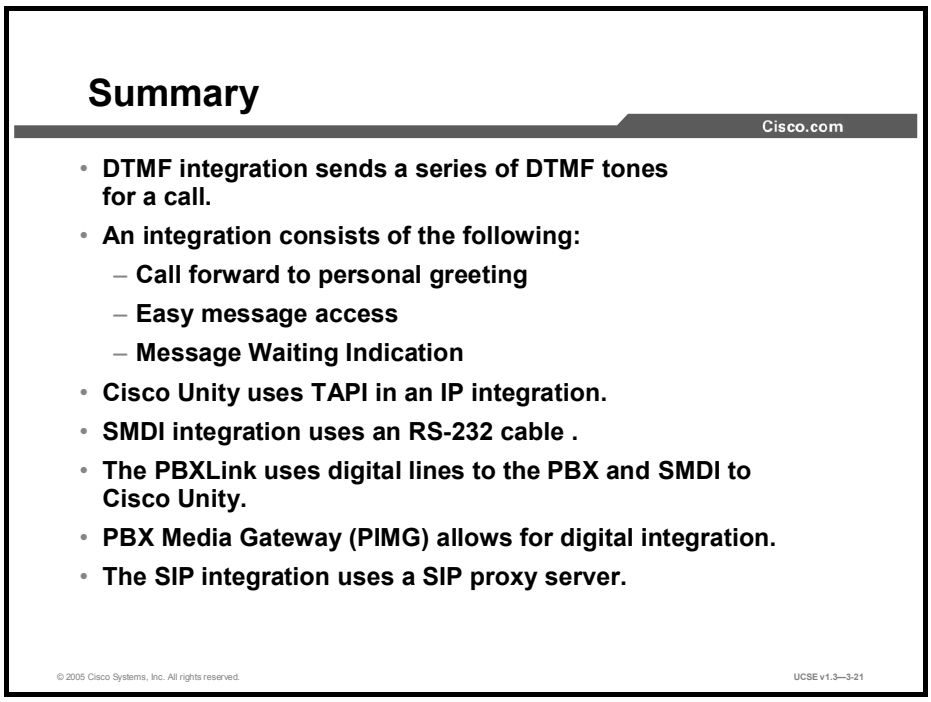
As a guide, you should initially set 25 percent of the Cisco Unity ports, on DTMF integrations, for Dial Out MWI. The port settings can be adjusted later if issues arise.

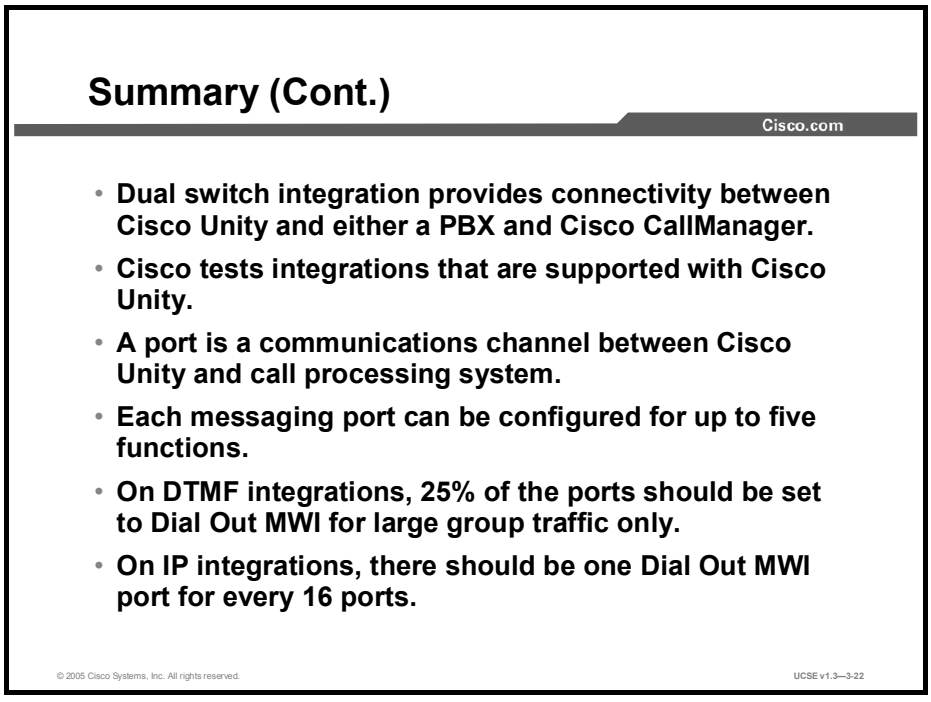
On IP integrations, it is required that one Dial Out MWI port be configured for every 16 ports on the Cisco Unity system. Although the Cisco Unity port does not send out touchtones to light lamps on an IP integration, the channel still needs to be open.

TRAP can also have an effect on ports. If not enough ports are configured for TRAP, some users will receive the error message “Unknown problems are preventing the completion of this call.” Those users must then use their PC multimedia microphone to record greetings during that session or initiate the call again, hoping for a free port.

Summary

This topic summarizes the key points discussed in this lesson.





Reference

For additional information, refer to these resources:

- *Cisco CallManager Integration Guide*
- Various PBX Integration Guides

Integration Guides may be found at:

- http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/integuid/index.htm

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) Which of the following are attributes of an integration? (Choose two.)

A) easy message access
B) analog connectivity
C) digital connectivity
D) call forward to personal greeting

Q2) CallManager uses which protocol to talk to Cisco Unity?

A) SMTP
B) PBXLink
C) DTMF
D) SCCP
E) SMDI

Q3) Which item is used to convert the SCCP protocol to TAPI?

A) WAV drivers
B) SMDI
C) TSP
D) DSP

Q4) In a DTMF integration, the call control signals are passed where?

A) in-band
B) out-of-band
C) side band
D) control band

Q5) Which integration methods use an RS-232 interface to pass control traffic?

A) DTMF
B) in-band
C) Skinny
D) PBXLink
E) SMDI

Q6) How does the PBXLink box connect to the Cisco Unity server?

A) RS-232
B) DTMF
C) fiber
D) Ethernet
E) analog lines
F) digital Lines

Q7) SIP communicates to Cisco Unity over a(n) _____ network.

A) SMDI
B) IP network
C) DTMF network
D) Octel network

Q8) How many different types of PBX or call processing systems can Cisco Unity integrate with simultaneously?

A) 1
B) 2
C) 3
D) 4

Q9) Cisco CallManager uses which kind of port when communicating with Cisco Unity?

A) physical
B) virtual
C) mapped physical drive
D) virtual port mapped to a physical port

Q10) If a port is used only for recorded greetings, which port configuration options need to be enabled? (Choose two.)

A) Enabled
B) Answer Calls
C) Message Notification
D) Dial Out MWI
E) TRAP Connection

Q11) PIMG eliminates the need for what in the Cisco Unity server ?

A) SIP
B) SQL
C) Intel Dialogic voice boards
D) Integration Protocol

Quiz Answer Key

Q1) A, D

Relates to: Attributes of an integration

Q2) D

Relates to: Attributes of Cisco Unity-Cisco CallManager Integration

Q3) C

Relates to: How Does an IP Integration Work?

Q4) A

Relates to: How Does a DTMF Integration Work?

Q5) E

Relates to: How Does an SMDI Integration Work?

Q6) A

Relates to: How Does a PBXLink Integration Work?

Q7) B

Relates to: Session Initiation Protocol (SIP)

Q8) B

Relates to: Dual Switch Integration

Q9) B

Relates to: What is a Port in a Messaging System?

Q10) A, E

Relates to: Port Configuration Options

Q11) C

Relates to: How Does the PIMG Integration Work?

Lesson 2

Integrating Cisco Unity with Cisco CallManager

Overview

Cisco CallManager is one of the primary call control systems being sold with Cisco Unity. This lesson describes the process of integrating Cisco Unity into a Cisco CallManager environment. Although this lesson is specific to Cisco CallManager, you have to follow similar procedures when integrating Cisco Unity with a circuit-switched PBX—Message Waiting Indicator (MWI) parameters have to be established, the voice ports have to be set up, and the voice-mail profile needs to be applied to the phones that will use the Cisco Unity system.

Relevance

Cisco Unity parameters must map to the Cisco CallManager voice-mail parameters in order to enable the phones to communicate with Cisco Unity through Cisco CallManager. This mapping is accomplished via the Cisco Unity Installer. Understanding the Cisco Unity Installer and the integration between Cisco Unity and Cisco CallManager is essential for successfully using Cisco Unity and Cisco CallManager together.

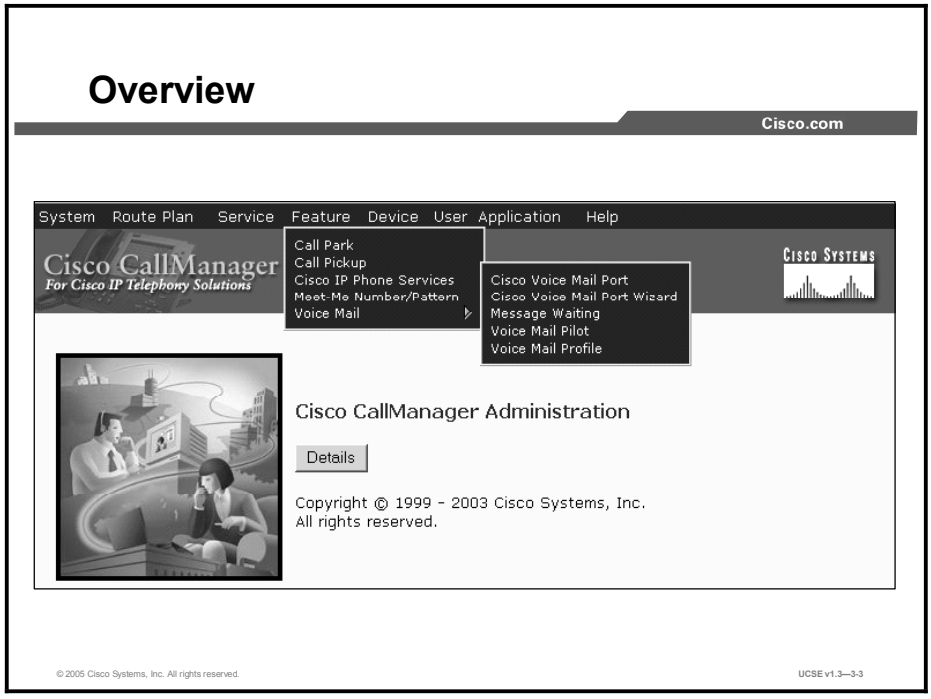
Objectives

Upon completing this lesson, you will be able to describe the programming and configuration setup necessary to integrate Cisco CallManager with Cisco Unity. This ability includes being able to meet these objectives:

- Describe the functions of the MWI directory numbers
- Describe the functions of the voice-mail pilot
- Describe the functions of the voice-mail profiles and how to set them
- Describe the functions of the voice-mail ports
- Describe the functions of line groups
- Describe the guidelines used in integrating Cisco Unity with Cisco CallManager

Setting Up Voice-Mail Connectivity

This topic describes the process for setting up voice-mail connectivity.



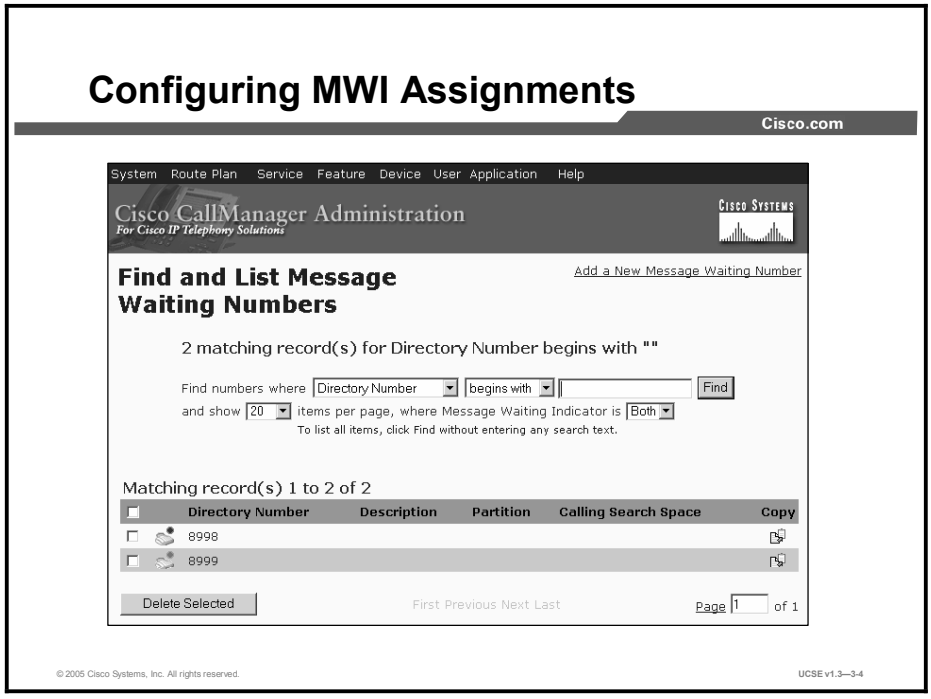
In order to support the activities of an integration—call forward to personal greeting, easy message access, and MWI activity—you need to configure components within Cisco CallManager. The voice-mail configuration is found under the Feature > Voice Mail options. The following six items have to be completed to configure the voice-mail ports for use with Cisco Unity:

- **Configure the voice mail ports:** Although Cisco Unity does not have directory numbers directly assigned to it, it will use the Telephony Service Provider (TSP) to build a connection between itself and Cisco CallManager. The TSP will use a voice-mail port name prefix that has to match the voice-mail port name in the Cisco CallManager voice-mail port. Cisco Unity needs one voice-mail port built in Cisco CallManager for each Cisco Unity port.
- **Configure the MWI directory numbers:** The directory numbers match the MWI On and Off numbers within Cisco Unity, so that when an MWI notification is sent, Cisco CallManager knows to either turn the light on or off.
- **Configure the pilot number:** Although Cisco Unity is not configured with the pilot number directly, the pilot number is used to represent the initial number of a hunt group for finding a free port to Cisco Unity. This is the number users would dial to get their messages, and the number associated with the messages button on their telephone.
- **Configure the line groups:** Line groups allow you to designate the order in which directory numbers are chosen. In Cisco Unity, the line group is the mechanism that allows Cisco CallManager to find the first available Cisco Unity port.

- **Configure the voice-mail profile:** The voice-mail profile allows you to assign the pilot number that will be the default number used when a user presses the message button, thus facilitating easy message access.
- **Configure the directory number to use the appropriate voice-mail profile:** When configuring the directory number, you are telling it which profile to use so that when the message button is pushed, it is directed to the appropriate voice-mail system.

Configuring MWI Assignments

This topic describes the functions of the MWI directory numbers.



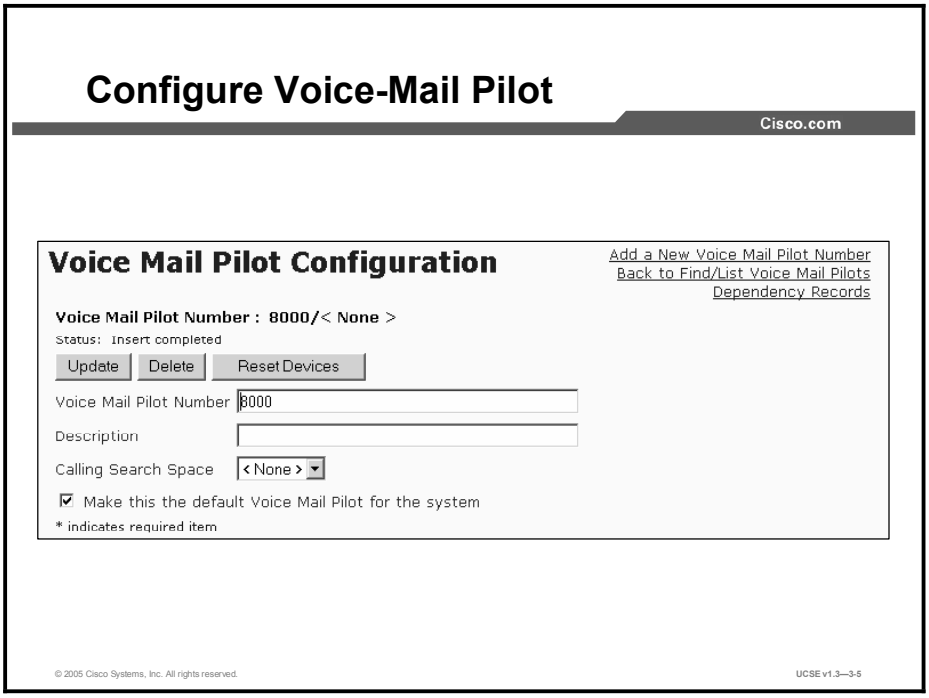
To configure the MWI lights to turn on and off, MWI directory numbers have to be assigned to MWI On and Off parameters. There could be multiple On and Off parameters, depending on how many Cisco Unity systems are working with this system. These directory numbers have to match in both Cisco CallManager and the Cisco Unity TSP.

Each Cisco Unity system may use the same or a separate set of MWI numbers. For example, in a lab scenario that has six Cisco Unity servers and one Cisco CallManager, each system can be set up with its own set of numbers in order to give the students the ability to build a full integration between Cisco Unity and Cisco CallManager.

In another example, there may be a legacy voice-mail system that is currently in place and Cisco Unity is to augment, then replace, the older system. To keep the two systems logically separate, a different set of MWI numbers can be used.

Configuring Voice-Mail Pilot

This topic describes the functions of the voice-mail pilot.

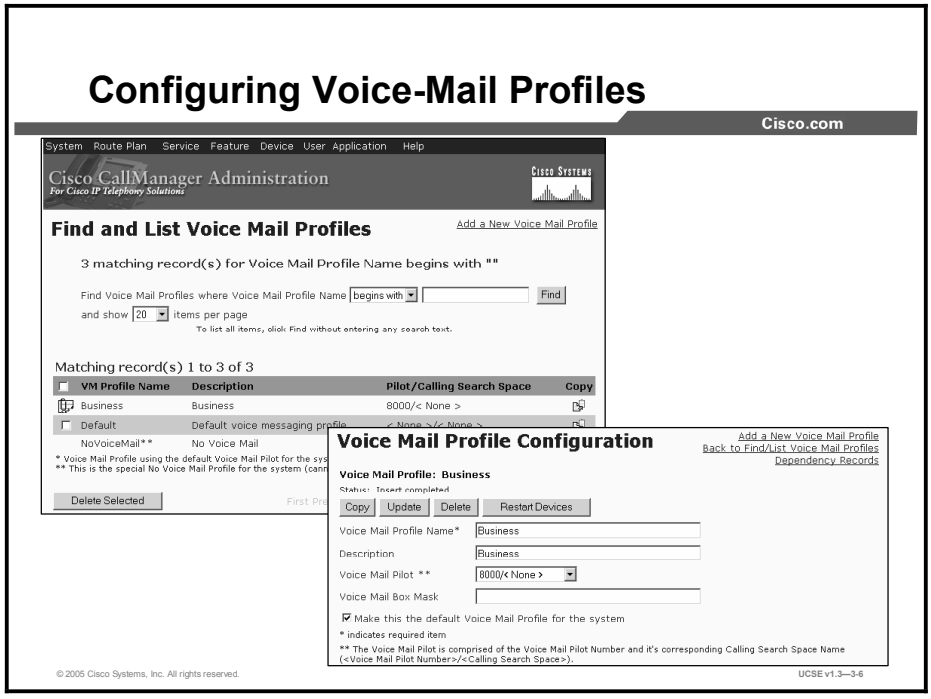


The voice-mail pilot number designates the directory number that you dial to access your voice messages. Cisco CallManager automatically dials the voice-messaging number when you press the Messages button on your phone. Each pilot number can belong to a different voice-mail messaging system. The voice-mail pilot number is typically the same number as the first voice-mail port. The voice-mail pilot will point to the voice-mail port that is assigned to the voice-mail pilot number. Generally it is the first voice-mail port. When you set up the voice-mail ports, you set them so that each is called in turn, but a user only has to dial the first one. After that, Cisco CallManager will find the next available port.

In older versions of Cisco CallManager, only one pilot number was allowed. In this case, in order to point phones to different voice-mail systems, you use Cisco CallManager features such as partitions, calling search spaces, and translation patterns to direct users to their designated voice-mail system.

Configuring Voice-Mail Profiles

This topic describes the functions of the voice-mail profiles and how to set them.



Voice-mail profiles allow you to define any line-related voice-mail information that is associated with a directory number, not a device. The voice-mail profile contains the following information:

- Voice Mail Profile Name
- Description
- Voice Mail Pilot Number
- Voice Mail Box Mask
- Default (checked if this particular profile is the default profile)

Different lines on a device can have different voice-mail profiles. For example, the phone of an administrative assistant can have a second line for the manager, which routes to the voice-messaging system of the manager. The administrative assistant line routes to its own voice-messaging system.

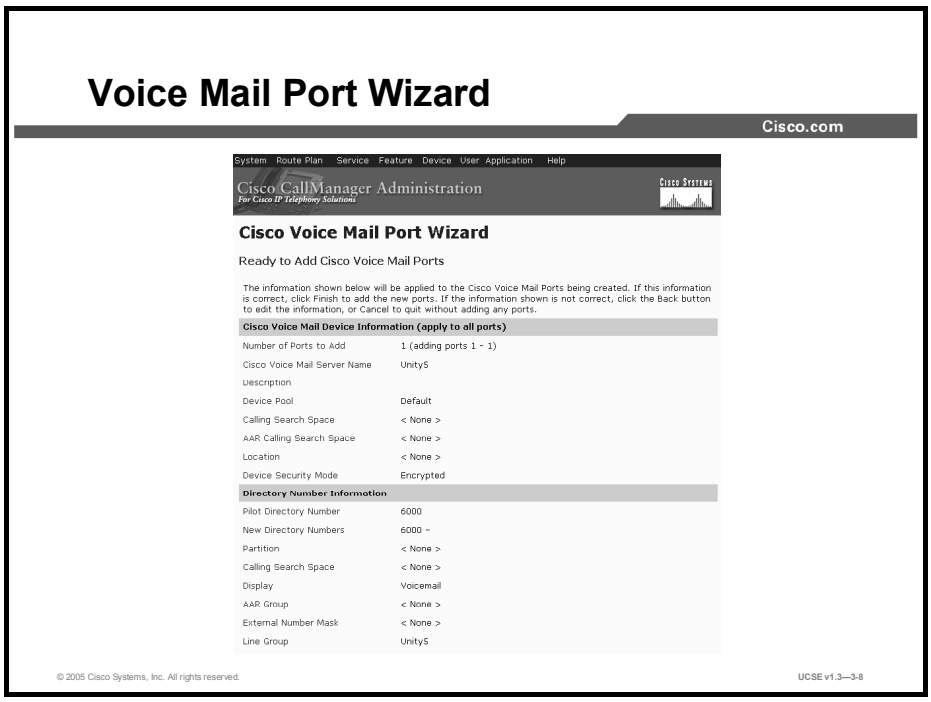
A predefined default voice-mail profile gets automatically assigned when you add a line. When you search for voice-mail profiles, “default” appears beside the profile name within the list.

A voice-mail profile takes precedence over other settings when calls are routed to a voice messaging system.

The directory numbers of a phone will use the voice-mail profile to make the association between a name and the voice-mail pilot number. The directory number picks up the base voice-mail pilot number as the primary number to pass calls over to voice mail on.

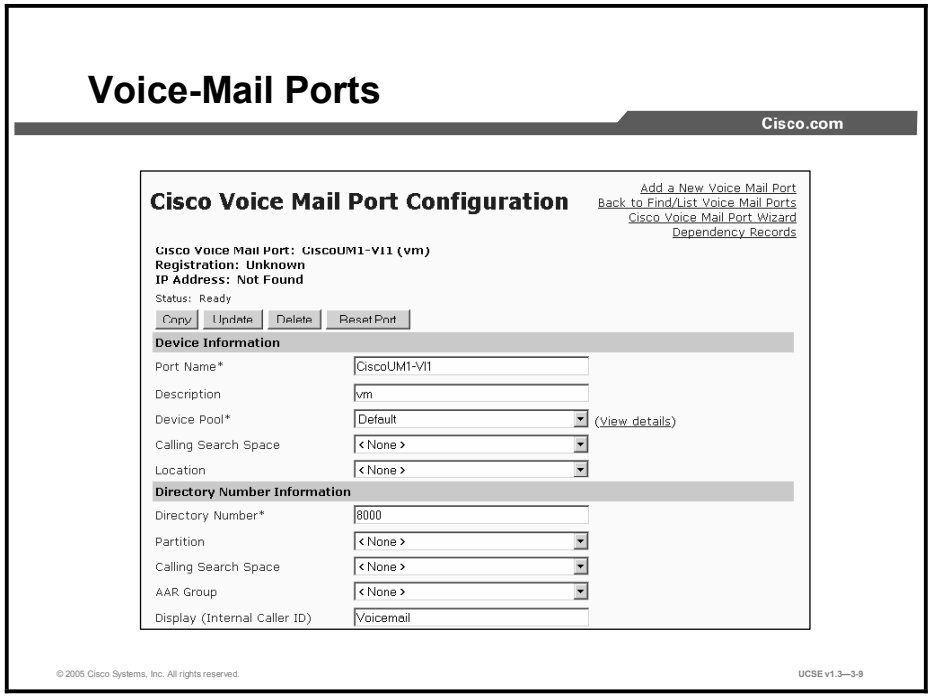
Configuring Voice-Mail Ports

This topic describes the functions and configuration of the voice-mail ports.



There are two ways to create the voice-mail ports. One is to use the Voice Mail Port Wizard. The other is to manually create each voice-mail port. The Voice Mail Port Wizard will direct you through the process of creating voice-mail ports by prompting for required information such as Calling Search Space of the ports, device name, Device Security Mode, and Line Group to which these ports are associated.

When creating voice-mail ports in Cisco CallManager, do not create more ports than Cisco Unity is licensed for. Remember the voice-mail port names you choose in Cisco CallManager, because this information will have to be entered in the Cisco Unity TSP configuration in the Cisco Unity Telephone Integration Manager. Choose a set of directory numbers that are discrete from the rest of the Cisco CallManager dial plan. You may also want to avoid assigning directory numbers that are a subset of your dial plan numbers, such as a voice-mail port of 100 when you have a Cisco CallManager directory number of 1000 also in the system.



A voice-mail port is the logical definition of a port that will be used to communicate with a voice-mail system. The voice-mail port is used to define the characteristics of the integration. The port name has to match what is configured on the Cisco Unity system. For example, the default port name is CiscoUM1-VI1. This port name matches the default settings in Cisco Unity. The voice-mail port configuration includes the following device parameters:

- **Port Name:** Enter a name to identify the Cisco voice-mail port. You must add a device for each port on Cisco voice mail. If 24 ports exist, you must define 24 devices.
- **Description:** Enter the purpose of the device.
- **Device Pool:** Choose the default value **Default**.
- **Calling Search Space:** Choose the appropriate calling search space. A calling search space comprises a collection of partitions that are searched for numbers called from a device.
- **Location:** Choose the default value **None**. The location specifies the total bandwidth that is available for calls to and from this device. A location setting of None means that the locations feature does not keep track of the bandwidth that is consumed by this device.

The voice-mail port configuration also includes the following parameters for Directory Number Information:

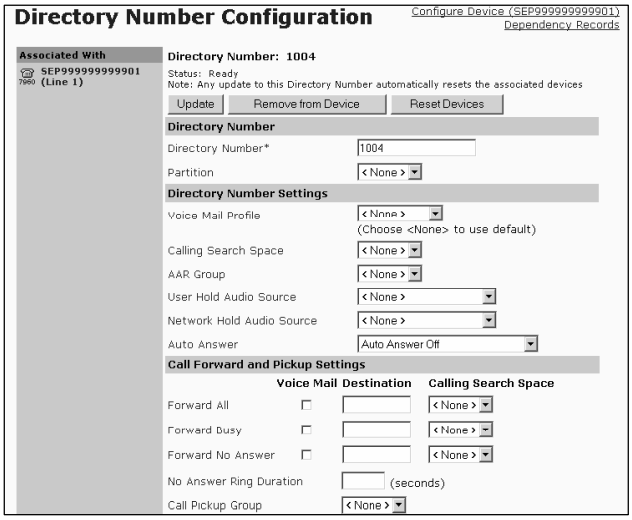
- **Directory Number:** Enter the number that is associated with this voice-mail port. Make sure that this field is unique in combination with the Partition field.
- **Partition:** Choose the partition to which the directory number belongs. Choose **None** if partitions are not used. If you choose a partition, you must choose a calling search space that includes that partition.

  If more than 250 partitions exist, the ellipsis (...) button displays next to the drop-down list box. Click the **...** button to display the Select Partition window. Enter a partial partition name in the List, in the Name field. Click the desired partition name in the list of partitions that displays in the Select item to use box, and click **OK**.

- **Calling Search Space:** Choose the appropriate calling search space. A calling search space comprises a collection of partitions that are searched for numbers that are called from a directory number. If you choose a partition, you must choose a calling search space that includes that partition.
- **Display:** This field indicates text that appears on the called party phone when a call is placed from this line.
- **AAR Group:** Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.
- **External Number Mask:** Specify the mask used to format caller ID information for external (outbound) calls. The mask can contain up to 50 characters. Enter the literal digits that you want to appear in the caller ID information and use “X” to represent the directory number of the device.

Voice-Mail Assignment

Cisco.com

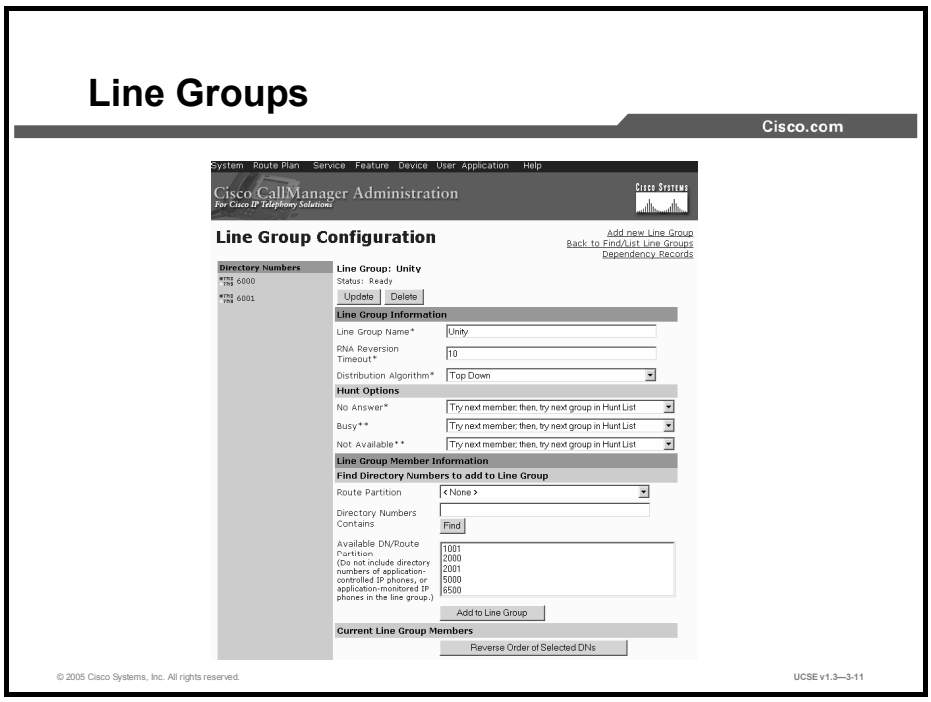


UCSE v1.3—3-10

Once the voice-mail port parameters are completed, you can then assign them to a directory number. Voice-mail profiles are associated with individual directory numbers, not phones. The voice-mail profile will then point to a voice-mail port or translation pattern so that when the user presses the message button, it will direct them to their voice-mail system. If a voice-mail profile is not selected, the default voice-mail profile will be used. If you want to automatically forward calls based on no answer or busy, you can select the check boxes, or put the pilot number in the blanks next to those options to forward the calls to voice-mail.

Line Groups

This topic describes the use of Line Groups with Cisco CallManager.



Line Groups enable you to indicate the order in which the Cisco Unity ports will answer calls. Formerly, this function was configured for you through the Voice Mail Port Wizard. You can configure line groups to follow distribution algorithms, such as top down, circular (also known as uniform distribution), longest idle time, or broadcast. In a Cisco Unity environment, you should select the “top down” distribution algorithm, which will select the first available Cisco Unity port, always beginning with the first Cisco Unity port, the Cisco Unity pilot number.

Line groups now have the responsibility for providing the call forward no answer and busy destinations. These should be configured to the line group’s “Try next member” option.

Since line groups are sending calls to Cisco Unity ports to answer calls, directory numbers for voice-mail ports that are set for dial out only, such as MWI and Message Notification, must not be included in the line group.

The line group created will be associated with the voice-mail ports during the Voice Mail Port Wizard configuration.

Line groups first appeared in Cisco CallManager 4.0. In Cisco CallManager versions previous to 4.0, the following items may need to be configured:

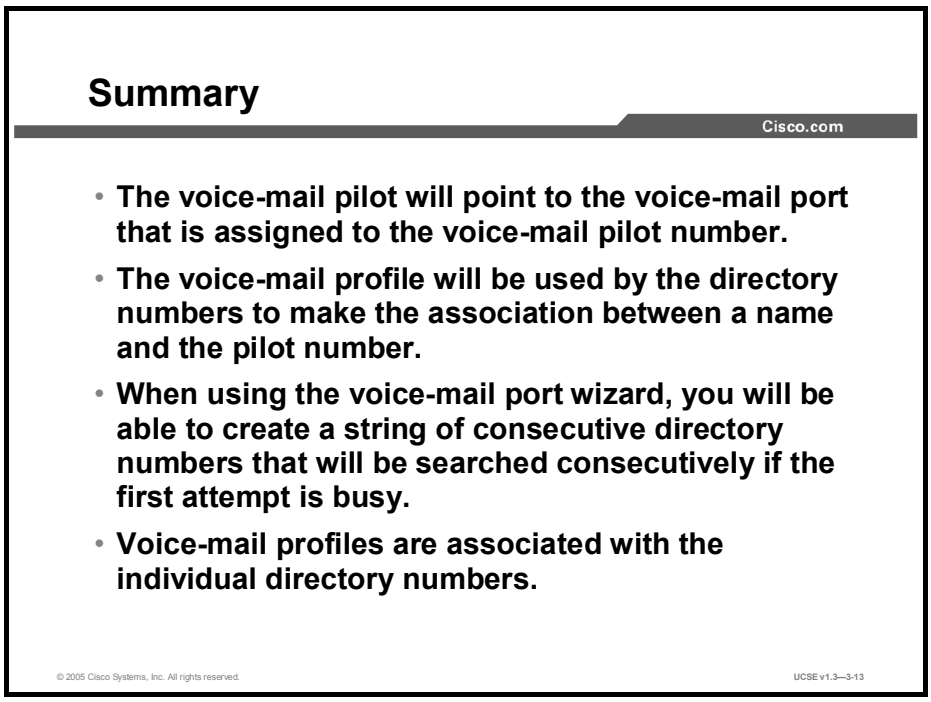
- **Voice Mail Maximum Hop Count:** Users may experience a busy signal when the Voice Mail Maximum Hop Count is set for a value less than the number of voice-mail ports. This parameter identifies how many ports to attempt to send a voice-mail call to. It starts with the first voice-mail port, and if the port is busy or rings no answer, it tries the next port, and so on, until the limit has been reached. When the limit has been reached, the caller will get a busy signal even if there are still more ports available that were not included in the limit value. This value should be equal to the number of voice ports that you have in use.

- **Advanced Call Forward Hop Flag:** If the Advanced Call Forward Hop Flag is set to True, Cisco CallManager call forwarding skips the busy or unregistered voice-mail port when choosing the next voice-mail port. The call is extended to an available voice-mail port; therefore, the voice-mail ports are chosen more efficiently. If the Advanced Call Forward Hop Flag is set to False, Cisco CallManager call forwarding does not skip the busy or unregistered voice-mail port; instead, the call extends to the busy or unregistered voice-mail port and waits until the busy or unregistered voice-mail port rejects the call, and the call is then forwarded to the next voice-mail port. It is better to turn on the Advanced Call Forward Hop Flag.

  Also, the Cisco Unity status monitor may show the port as free while users are getting busy signals when trying to access the voice-mail. If you are experiencing this symptom, you should forward the last port back to the first port and then increase the Voice Mail Maximum Hop Count to double the number of ports. This configuration results in Cisco CallManager checking the ports twice to determine if they are available, and by the second time around the ports are usually available through the status table.

Summary

This topic summarizes the key points discussed in this lesson.



References

For additional information, refer to these resources:

- *Cisco CallManager Administration Guide*, Release 4.1
- Cisco CallManager Integration Guides

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) Where in Cisco Unity must the MWI directory numbers also be entered?

A) system administration Integration page
B) cisco.ini file
C) Cisco Unity TSP
D) Interface Monitor

Q2) Which statement describes the relationship of the voice-mail pilot number to the voice-mail ports?

A) It should match the MWI On number.
B) It should match the first call park number.
C) It should match the first voice port number.
D) It should match the first voice profile number.

Q3) The voice-mail profile is associated with the _____.

A) MWI On number
B) MWI Off number
C) first voice-mail port DN
D) pilot DN

Q4) How many voice-mail ports should be created when using the Voice Mail Port Wizard?

A) the number of Cisco Unity ports.
B) twice the number of Cisco Unity ports.
C) 50 percent more for redundancy.
D) The Wizard will poll Cisco Unity for that information.

Q5) When configuring a Cisco Unity-Cisco CallManager integration, which items must match on both Cisco Unity and Cisco CallManager?

A) MWI numbers and device name prefix
B) MWI numbers and the pilot number
C) the pilot number and voice port names
D) voice-mail profile and voice port names

Q6) Line groups should choose which distribution algorithm?

A) circular
B) longest idle time
C) UCD
D) top down

Quiz Answer Key

Q1) C

Relates to: Configuring MWI Assignments

Q2) C

Relates to: Configuring Voice-Mail Pilot

Q3) D

Relates to: Configuring Voice-Mail Profiles

Q4) A

Relates to: Configuring Voice-Mail Ports

Q5) A

Relates to: Configuring MWI Assignments

Q6) D

Relates to: Line Groups

Module Self-Check

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

Q1) Which three essential features are required for a Cisco Unity integration? (Choose one.)

A) easy message access, time-of-day server, voice boards
B) easy message access, call forward to personal greeting, and MWI
C) MWI, call forward to personal greeting, and DTMF support
D) DTMF, time-of-day server, and voice boards

Q2) Cisco CallManager communicates with Cisco Unity over which media?

A) analog
B) SMDI
C) T1 Voice
D) IP network

Q3) The Cisco Unity TSP converts which two components?

A) RTCP to MAPI
B) SCCP to MIMEI
C) Skinny to TAPI
D) RTP to Windows MCI

Q4) How does an in-band integration send MWI information to the PBX?

A) SMDI packets
B) PBXLink data objects
C) DTMF tones
D) Skinny packets

Q5) The distance limitation on an SMDI connection with no line extension equipment is _____.

A) 10 feet
B) 100 feet
C) 500 feet
D) 1000 feet

Q6) How does the PBXLink box connect to a circuit-switched PBX?

A) RS-232
B) DTMF
C) fiber
D) Ethernet
E) analog lines
F) digital lines

Q7) Cisco Unity SIP integration uses a(n) _____ to set up communication between the voice messaging ports on the Cisco Unity server and the appropriate endpoint.

A) SIP distribution server
B) SIP name server
C) SIP redirect server
D) SIP proxy server

Q8) When implementing dual integration, which item differentiates the different switch types from each other?

A) One may use voice cards, the other uses IP.
B) Both integrations can use voice cards.
C) Both integrations share the same ports.
D) Ports are split evenly, every other one, between the two systems.

Q9) Which circuit-switched PBX systems support DTMF integration? (Choose two.)

A) Centrex
B) Matra 5400
C) Toshiba CTX 670
D) Nortel Meridian 1
E) Alcatel 4400

Q10) How many sessions can a single port terminate?

A) One
B) Two
C) Three
D) Four

Q11) If you want to use a port just for sending out MWI information, which port configuration options need to be set up? (Choose two.)

A) Enabled
B) Answer Calls
C) Message Notification
D) Dial Out MWI
E) TRAP Connection

Q12) When determining the number of ports, which of the following should be taken into consideration? (Choose two.)

A) number of interview handlers
B) amount of Message Notification traffic
C) amount of Internet subscriber traffic
D) number of users using Outlook Express

Q13) Which statement is true about the MWI DNs?

A) The On and Off numbers need to match the call park range.
B) The On and Off numbers need to be discrete numbers within Cisco CallManager.
C) The On and Off numbers can be any arbitrary overlapping DN.
D) The On and Off numbers do not need to be specified, because Cisco Unity will send them to Cisco CallManager.

Q14) When Cisco CallManager is integrated with multiple Cisco Unity systems, the voice-mail pilot should _____.

A) be the same DN for all integrations
B) be a different DN for each integration
C) be the voice-mail profile DN for each integration
D) be a number within the call park range

Q15) The voice-mail profile is applied where within Cisco CallManager?

A) subscriber directory number
B) voice-mail ports
C) voice-mail pilot
D) MWI lights

Q16) Line groups provide which function?

A) Decide which Cisco Unity port should receive a call
B) Set outdial parameters
C) Connect callers to the PSTN
D) Always send the call to the next voice port

Q17) When choosing voice-mail port numbers, they should be _____.

A) the same as the call park numbers
B) discrete numbers in the system
C) overlapped with other DNs in the system
D) any number currently used in the system

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent or better.

Module Self-Check Answer Key

Q1) B

Q2) D

Q3) C

Q4) C

Q5) B

Q6) F

Q7) D

Q8) A

Q9) A, E

Q10) A

Q11) A, D

Q12) A,B

Q13) B

Q14) B

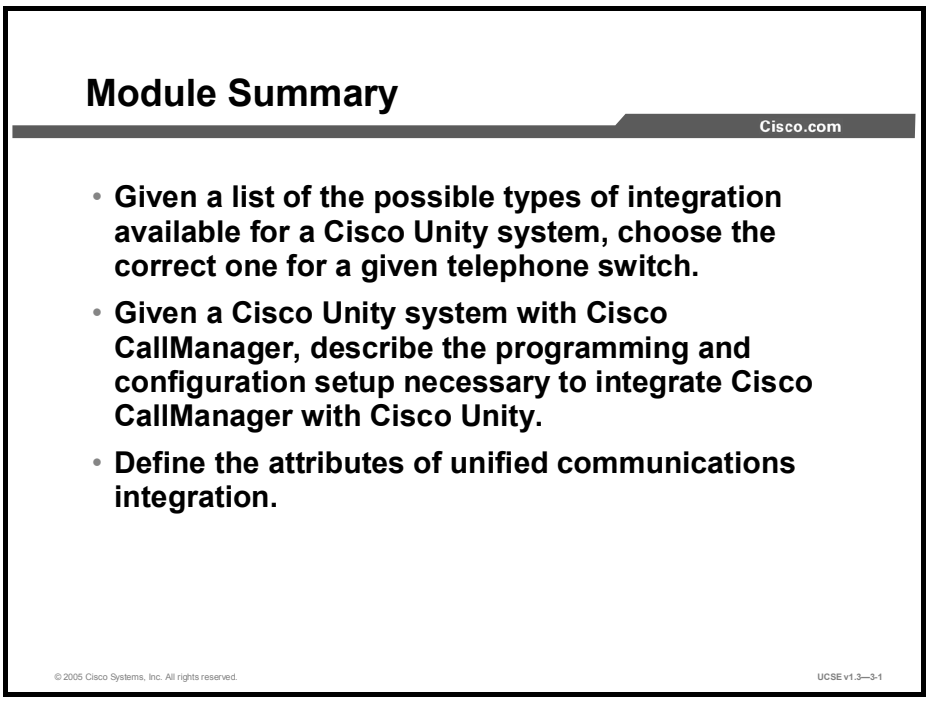
Q15) A

Q16) A

Q17) B

Module Summary

This topic summarizes the key points discussed in this module.



In this module, you learned about the different types of integrations that Cisco Unity supports and how to implement those integrations. The module specifically describes the Cisco Unity integration with Cisco CallManager.

References

For additional information, refer to these resources:

- *Cisco CallManager Integration Guide 4.1*
- *Cisco CallManager Administration Guide 4.1(2)*
- Various Telephone Integration Guides for Cisco Unity

Module 4

Networking Unified Communications Servers

Overview

Networking is one of the most powerful tools of Cisco Unity, allowing users to interact with both Cisco Unity and non-Cisco Unity recipients to send and receive e-mail, voice mail, and faxes. Companies and organizations must be able to communicate internally and externally, and networking is a tool that allows them to be connected. The module covers both basic and advanced topics of Cisco Unity, Exchange, and Domino networking.

Module Objectives

Upon completing this module, you will be able to select the appropriate type of Cisco Unity networking and subscriber account. This ability includes being able to meet these objectives:

- Given a particular server type, select the appropriate type of Cisco Unity networking to assure message delivery
- Given an Exchange 5.5 and Exchange 2000 environment, describe how messages are exchanged and how the active directory is replicated to all other domain controllers in the forest
- Given a list of user characteristics, be able to select and describe the appropriate type of subscriber for each user in a Cisco Unity networking solution
- Given an environment with multiple Cisco Unity servers, be able to describe how messages can be exchanged between them using digital networking
- Given SMTP networking in Cisco Unity, describe the requirements for interoperability and the basic steps needed to configure SMTP networking
- Describe how Cisco Unity uses VPIM networking to deliver voice, fax, and text messages over the Internet
- Describe how Cisco Unity uses AMIS networking protocol to transfer voice messages between AMIS-compliant servers
- Describe how Cisco Unity uses Bridge networking to deliver messages between Cisco Unity and mail servers in an Octal network

Lesson 1

Understanding Cisco Unity Networking

Overview

This lesson introduces the concepts important to networking in Cisco Unity, such as message delivery and directory replication, location objects, dialing domains, and the various types of networking offered in Cisco Unity.

Relevance

In order to implement networking between Cisco Unity and other messaging systems (including other Cisco Unity servers), you must understand the basic concepts and terminology of Cisco Unity networking.

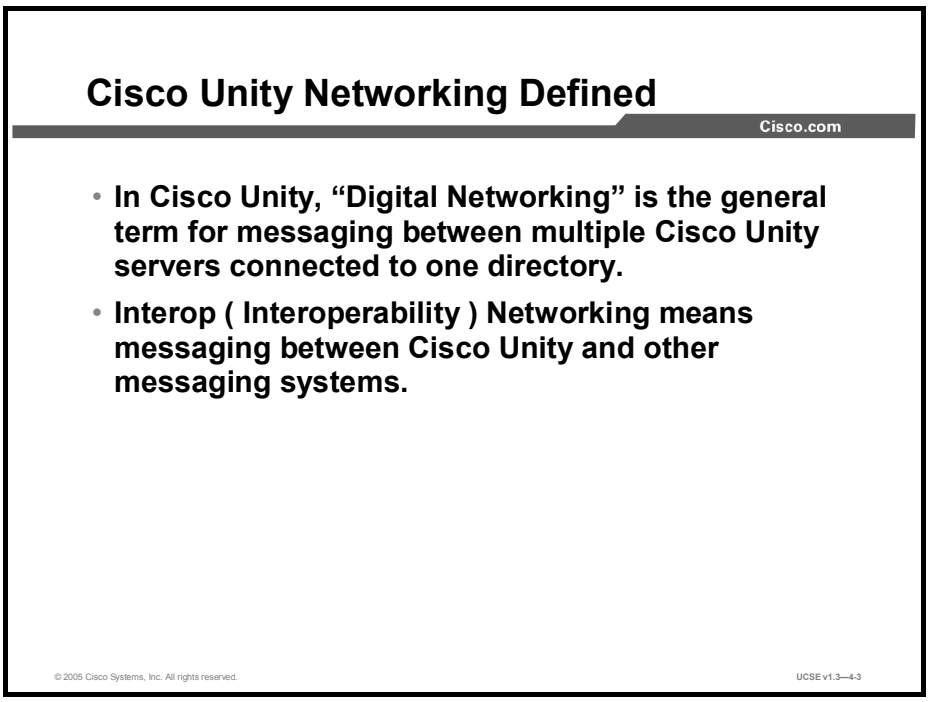
Objectives

Upon completing this lesson, you will be able to select the appropriate type of Cisco Unity networking to ensure message delivery. This ability includes being able to meet these objectives:

- Define networking in a Cisco Unity 4.0 environment
- Describe the five different types of networking that are available with Cisco Unity based on the target server
- Describe the networking options available for Cisco Unity 4.0
- Describe how the Interop Gateway for Domino allows messaging between different messaging systems
- Describe how the Voice Connector for Exchange allows messaging between different messaging systems

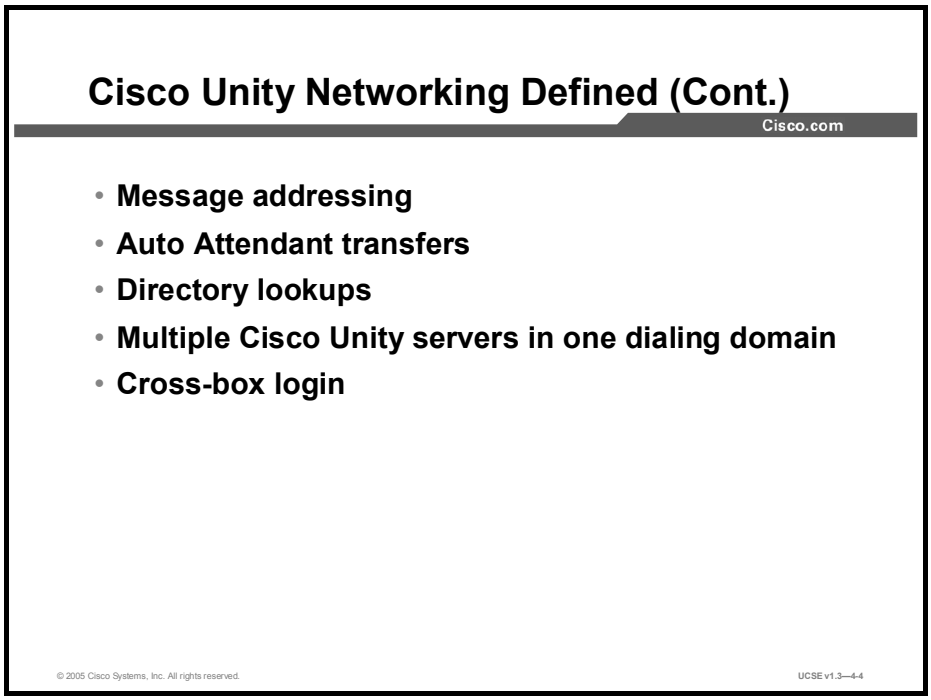
Cisco Unity Networking Defined

This topic describes networking in the Cisco Unity environment.



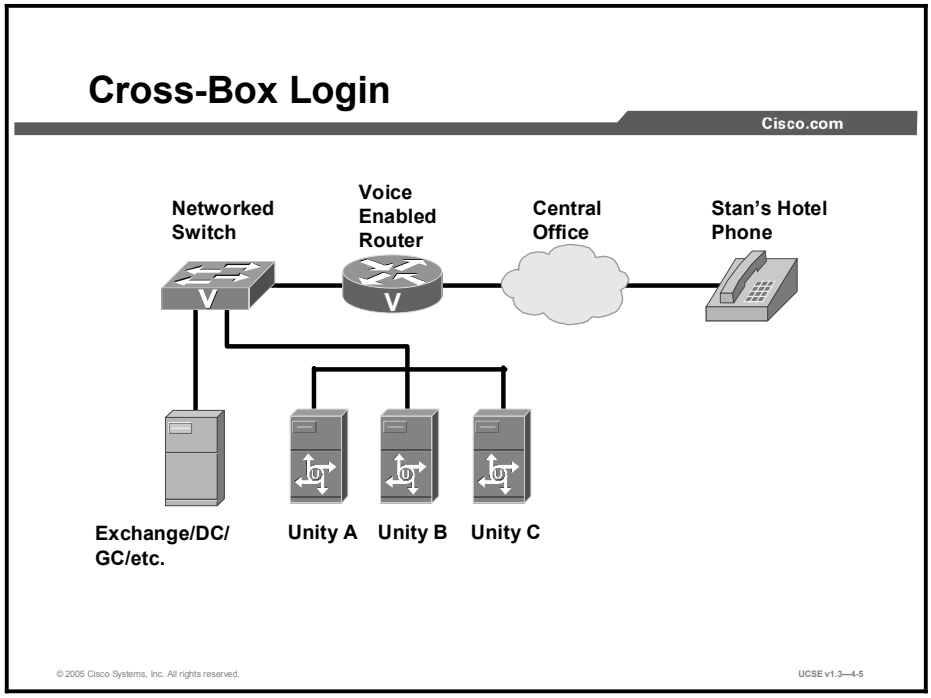
In Cisco Unity, “digital networking” is the general term for messaging between multiple Cisco Unity servers connected to one large directory. This configuration allows large-scale applications to be handled by Cisco Unity, so that a high call volume of traffic or a large number of users can be serviced by Cisco Unity.

Interop (Interoperability) is a function that allows a Cisco Unity user to address and send a message to someone on their e-mail server, on a voice-mail system on a separate directory, or, more commonly, on a voice messaging system made by another manufacturer.



In a networked Cisco Unity environment, any subscriber can message any other subscriber in the organization by name or extension. Callers can dial into any Cisco Unity server in the organization, and the Auto Attendant will transfer that call to the correct subscriber in the organization regardless of which Cisco Unity server that subscriber is associated with. Outside callers can dial into any Cisco Unity server in the organization, find any subscriber by name in the alphabetic directory and transfer to them, regardless of which Cisco Unity server that subscriber is homed on. Finally, any number of Cisco Unity servers can be bound together in a dialing domain so that subscribers can address messages and do Auto Attendant transfers dialing the same number they use to reach that person through the telephone system.

Cross-box login allows you to configure all Cisco Unity servers in a dialing domain so that subscribers can call into any Cisco Unity server in the domain and sign into their mailbox. A user puts in their ID, the messaging system locates the extension and transfers the call to the appropriate Cisco Unity server. The messaging system authenticates and transfers the caller to the assigned Cisco Unity server based on ID, extension, and Cisco Unity server assignments. An administration interface for defining the “hand off” numbers between different Cisco Unity servers within that dialing domain is provided.



The figure shows a very basic deployment model with three Cisco Unity servers set up behind a networked switch; but the switch could also be a large PBX or a Cisco CallManager cluster. The phone system being used is not relevant here, because this solution should work equally well with a legacy PBX, Cisco CallManager, session initiation protocol (SIP), or dual-switch integration. In this example, subscribers at the site are spread relatively evenly across the three Cisco Unity servers and the three boxes are configured to be in the same dialing domain.

Stan's Cisco Unity subscriber account is homed on Unity B, and he is calling from his hotel to check his messages. The administration staff for this site set up an 800 number for checking messages on the road. This number is configured to dump callers into the subscriber sign-in conversation on Unity A, and the following steps occur:

Step 1 Stan is asked to enter his ID, which he does.

Step 2 The subscriber sign-in conversation finds Stan's Cisco Unity account in the global subscriber table and determines that Stan is homed on Unity B.

Step 3 The sign-in conversation looks up the transfer number to get calls to the Unity B box.

Step 4 Once the sign-in conversation finds the number, it checks to see if the system is configured to play a "transition" prompt, to cover any potential delay, before handing the call off. If it is, a simple "one moment" prompt is played; if not, it skips to the next step.

Step 5 Unity A does a supervised transfer to Unity B using the dial string retrieved above, and once the call is answered, it dials a special series of dual tone multifrequency (DTMF) tones, such as "##**##".

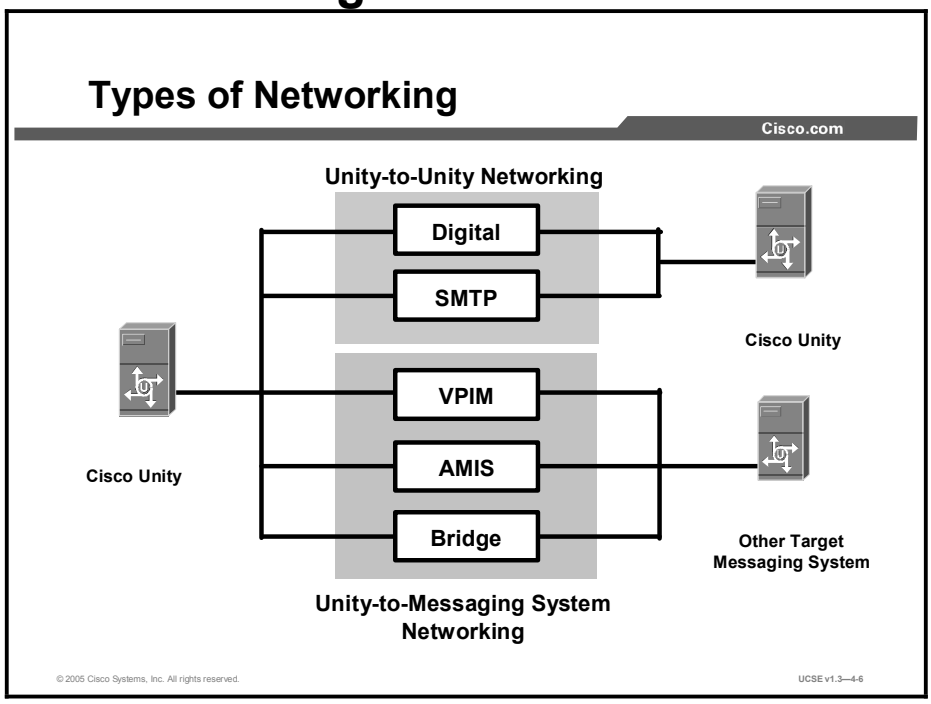
Step 6 The PHGreeting conversation on Unity B will notice this string of digits and realize that it means the incoming call is a subscriber sign in "hand off" from another Cisco Unity server, and responds with DTMF tones to let Unity A know it is ready to take the call.

Step 7 Unity B then launches a special conversation to handle the incoming call information.

Step 8 Unity A then sends Stan's user ID across to the special handoff sign-in conversation on Unity B and releases the call.

Step 9 The sign-in conversation on Unity B takes over as normal and asks Stan to provide his phone password.

Types of Networking



The main goal of networking in Cisco Unity is to deliver messages from a user on a Cisco Unity server to a target user on a different messaging server and from the target user on a different messaging server to a Cisco Unity user. A user experience is very simple: they leave a message for someone who is a subscriber on the system. They do not need to know what type of server the subscriber resides on and, if it is a server other than Cisco Unity, what communications protocols and software setup are used to make the message transfer. All of that is transparent, as it should be.

The type of networking used with Cisco Unity will depend on the target server(s) that you deliver subscriber messages to. The types of target servers, and the communication method used to reach them, are described as follows:

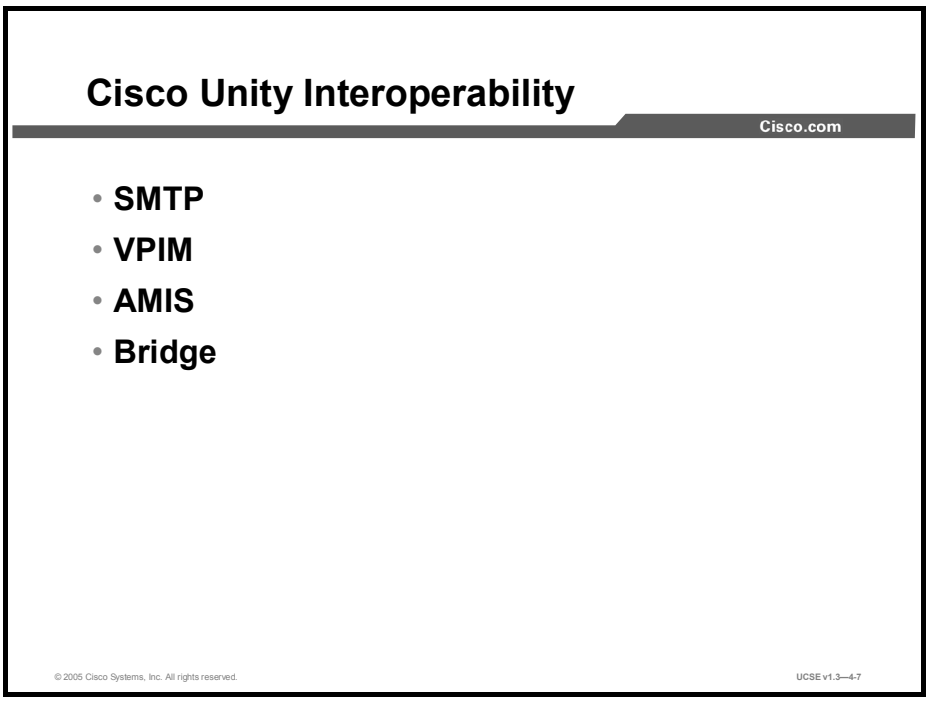
- **Digital:** If all of the servers are Cisco Unity servers and they all have access to the same global directory, digital networking is the method to implement.
- **Simple Mail Transfer Protocol (SMTP):** If a target server is a Cisco Unity server but does not have access to the same global directory, you should use SMTP networking. If the target server is any e-mail server capable of receiving SMTP mail, it is also a candidate for SMTP networking. The main difference between SMTP networking to a Cisco Unity server and to any other server is the appearance of the message when it arrives at the target server. At a Cisco Unity server, if a voice mail is sent, it retains all of its voice-mail attributes (that is, a subscriber can listen to it over the telephone). If the other target server is any other e-mail server, the voice message will arrive as an e-mail message with a WAV file attachment.
- **Audio Messaging Interchange Specification (AMIS):** If the target server is another voice-mail system, AMIS networking may be the best implementation. The target server must support the Audio Messaging Interchange Specification analog (AMIS-a) protocol.

- **Voice Profile for Internet Mail (VPIM):** If the target voice-mail system supports the VPIM protocol, VPIM is the preferable method for transferring messages between voice-mail servers. VPIM is a digital standard based on SMTP and the Multipurpose Internet Mail Extension (MIME) protocol. Voice, text, and fax messages may be transferred between target servers.
- **Bridge:** If the target voice-mail system is a supported Octel voice-mail system, Bridge would be the preferable method for transferring messages between voice-mail servers. Bridge uses VPIM, a digital standard based on SMTP and the MIME protocol with some proprietary extensions, to exchange messages with Cisco Unity, and uses the Octel analog messaging standard for communication with Octel servers. Voice, text, and fax messages may be transferred between target servers.

For more information on how these systems interoperate with Cisco Unity, refer to the following URL:
http://www.cisco.com/en/US/partner/products/sw/voicesw/ps2237/prod_configuration_guides_list.html

Cisco Unity Interoperability

This topic describes the types of networking available for Cisco Unity.

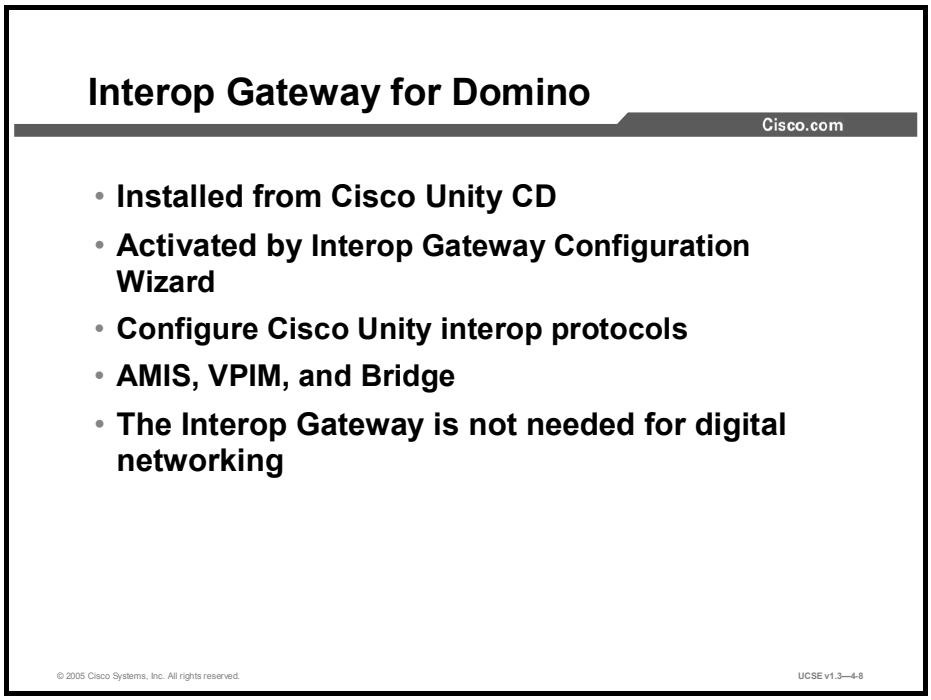


Cisco Unity 4.0(5) is capable of the full range of networking solutions. Users may send messages to subscribers residing on other Cisco Unity servers, SMTP servers, VPIM-compliant voice-mail servers, AMIS-a-compliant voice-mail servers, or Octel voice-mail servers using the Octel analog protocol.

If you are using Domino, you need to install and configure the Interop Gateway. If you are using Exchange, you need to install and configure the Voice Connector. This additional networking component is the software that enables communication with a wide variety of servers other than Cisco Unity. If you are deploying digital networking and all the Cisco Unity servers are connected to one large directory, there is no need for the additional software.

Interop Gateway for Domino

This topic describes how the Interop Gateway for Domino allows messaging between a Domino Cisco Unity solution and other messaging systems.



The Interop Gateway for Domino is a Cisco Unity service that runs on a Windows server (called CsDomInteropGty). It enables messaging between Cisco Unity and other voice messaging systems. The Interop Gateway files are copied to the Cisco Unity server during setup; however, the Interop Gateway is not installed as a service until you run the Interop Gateway Configuration wizard when configuring Cisco Unity for SMTP, AMIS, Bridge, or VPIM Networking. The Interop Gateway Configuration wizard configures and starts the service.

In the Interop Gateway Configuration wizard, you specify a Domino foreign domain name (for example, “voicemail.domain.com”) and mail file name.

Cisco Unity addresses outbound AMIS, Bridge, and VPIM messages to the specified foreign domain, and incoming Bridge and VPIM messages are addressed to the specified foreign domain. Messages addressed to the foreign domain are routed to the mail file specified in the foreign domain document by the Domino router.

The Interop Gateway monitors the mail file for messages, and performs the following functions:

- **AMIS networking:** The Interop Gateway routes voice messages to the applicable UAmis_<Servername> mailbox for outgoing analog delivery. Incoming AMIS voice messages received by the Cisco Unity AMIS bridgehead are routed to the Interop Gateway mail file for processing.

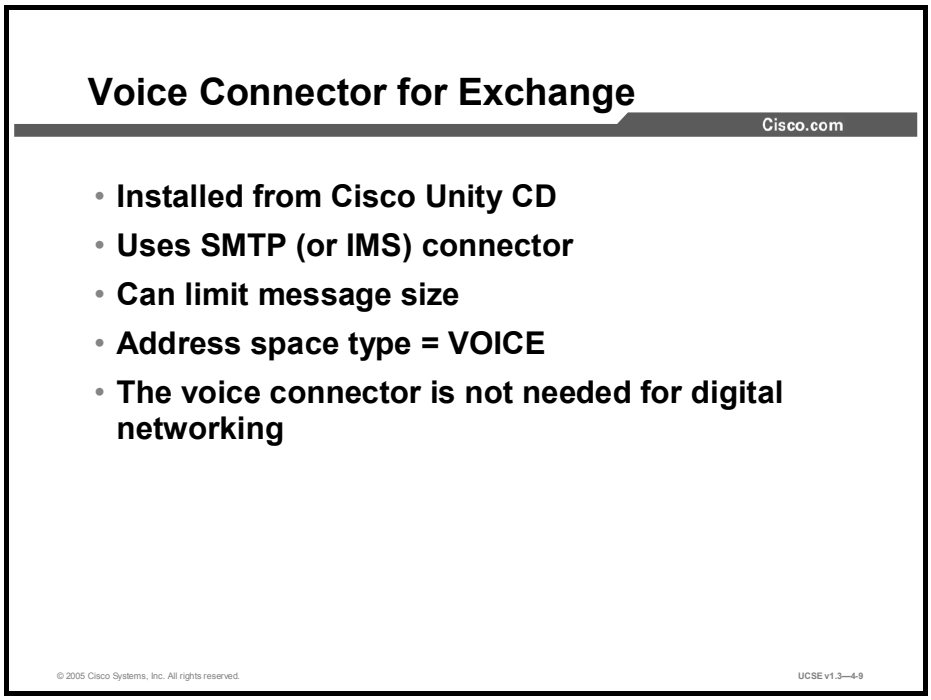
- **Bridge networking:** The Interop Gateway performs the message conversion and address translation that allows Cisco Unity to exchange messages with the Cisco Unity Bridge server.
- **VPIM networking:** The Interop Gateway performs the message conversion and address translation that allows Cisco Unity to exchange messages with other voice messaging systems by using the VPIM protocol. VPIM networking also provides the following messaging:
  - Between Cisco Unity servers, where the Domino servers are in different Domino domains and cannot be configured for digital networking
  - Between Cisco Unity with Domino systems and Cisco Unity with Exchange systems
  - Between Cisco Unity and Cisco Unity Express

Note that the Interop Gateway is not needed with digital networking because the Cisco Unity servers access the same directory.

You can find these instructions in the *Networking in Cisco Unity Guide (With Domino)*.

Voice Connector for Exchange

This topic describes how the Voice Connecter allows an Exchange Cisco Unity solution to send and receive messages from other messaging systems.



The Voice Connector allows two Cisco Unity servers to send and receive voice messages as SMTP mail while preserving the Cisco Unity attributes within the message. It also allows Cisco Unity to communicate with SMTP servers, Octel voice-mail servers, VPIM-compliant voice-mail servers, and AMIS-a-compliant voice-mail servers.

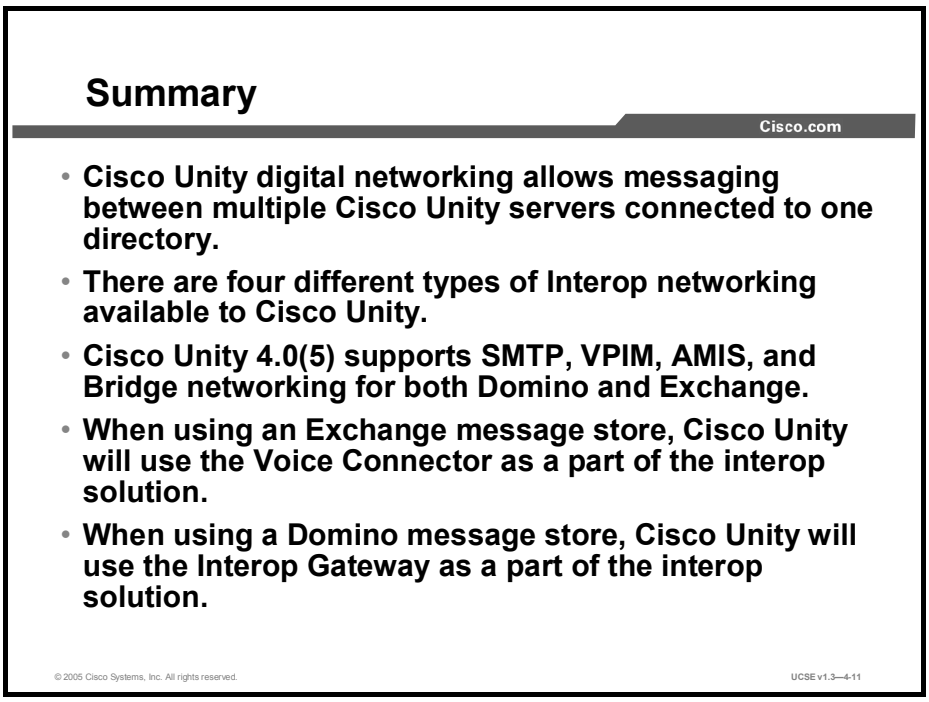
Destination type is one of the data objects defined within the location object. Whenever you specify another Cisco Unity server as the destination type, the SMTP message is packaged with a binary code that identifies the mail to the receiving machine (another Cisco Unity system) as a Cisco Unity voice-mail message. The result is that the message may be played over the telephone as well as played and managed by ViewMail for Outlook, and does not appear as an attached WAV file.

The Voice Connector is a separate installation from Cisco Unity and is found on the Cisco Unity Installation CD. Once the connector is installed, it appears as an Exchange connector object similar to the Internet Mail Service (IMS) (Exchange 5.5) or SMTP Connector (Exchange 2000), and therefore an entry is created in the Exchange Gateway Address Routing Table for a message type of VOICE. Because the Voice Connector uses SMTP, it requires the IMS connector to function properly in Exchange 5.5.

The current version of the Voice Connector is 11.x. If you are upgrading to Cisco Unity 4.0, you should use the latest connector. It is important that you have only one connector installed. Instructions for removing earlier versions of the connector are very dependent upon the version installed. These instructions are found in the *Networking in Cisco Unity Guide (With Microsoft Exchange)*.

Summary

This topic summarizes the key points discussed in this lesson.



References

For additional information, refer to these resources:

- *Networking in Cisco Unity Guide (With Microsoft Exchange)*
- *Networking in Cisco Unity Guide (With IBM Lotus Domino)*
- *Cisco Unity Bridge Networking Guide*

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) In Cisco Unity, Interop is the general term for _____.

A) messaging between messaging systems
B) messaging to an Octel voice-mail system
C) messaging to a VPIM endpoint
D) messaging between PBXs

Q2) Which of the following is a type of Cisco Unity networking? (Choose three.)

A) Bridge
B) DTMF
C) VPIM
D) AMIS
E) SMDI
F) serial

Q3) Cisco Unity for Domino requires which connecter for VPIM messaging?

A) Voice Connecter
B) Interop Gateway
C) Bridge Server
D) AMIS Bridge

Q4) How many networking options are available with Cisco Unity 4.0?

A) 3
B) 5
C) 7
D) 9

Q5) The Voice Connector allows Cisco Unity to send voice messages to an e-mail server with which protocol?

A) analog
B) Dialogic
C) SMTP
D) SMDI

Quiz Answer Key

Q1) A

Relates to: Cisco Unity Networking Defined

Q2) A, C, D

Relates to: Types of Networking

Q3) B

Relates to: Interop Gateway for Domino

Q4) B

Relates to: Voice Connector for Exchange

Q5) C

Relates to: Voice Connector for Exchange

Lesson 2

Understanding Message Transfer and Directory Replication

Overview

This lesson describes the message transfer and directory replication process in general, and then specifically addresses Cisco Unity interactions with Active Directory in Windows 2000.

Relevance

Understanding how messages are exchanged and how Active Directory is replicated to all other domain controllers is an essential skill needed for the successful implementation of Cisco Unity and its integration with Microsoft Exchange.

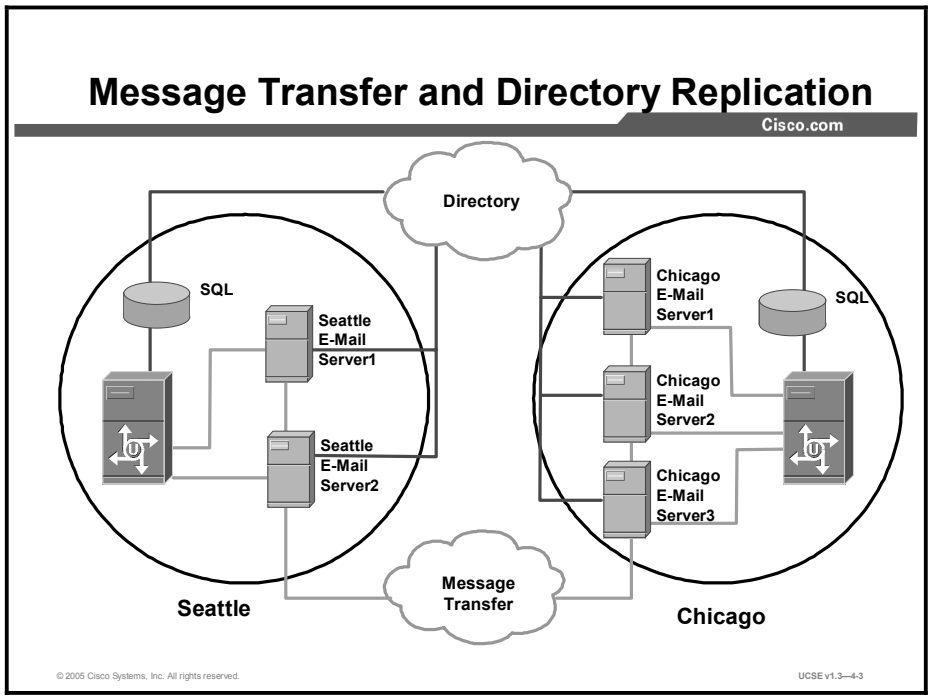
Objectives

Upon completing this lesson, you will be able to describe how messages are exchanged and how a Windows Active Directory is replicated to all other domain controllers in a forest. This ability includes being able to meet these objectives:

- Describe the message transfer and directory replication process, specifically addressing Cisco Unity interactions with Active Directory in Windows 2000
- Describe how intrasite messaging assures that messages are delivered to the correct server
- Describe how intersite messaging assures that messages are delivered to the correct server
- Describe how routing group message passing ensures that messages are delivered to the correct home server in a multiple routing group environment
- Describe how Active Directory replicates changes to all other domains in its forest
- Describe how SQL replication works in a Cisco Unity environment

Message Transfer and Directory Replication

This topic describes the message transfer and directory replication process, specifically addressing Cisco Unity interactions with Active Directory in Windows 2000.



The high-level, conceptual diagram in the figure illustrates the connection between two Cisco Unity servers installed on a corporate network. The specific e-mail backend servers are not an issue at this level. The Directory contains information about all the mail users in the company, and the mail store, or e-mail servers, allow users to gain access to their messages, monitor their mailbox, leave messages, and so on. As long as the company has a single directory for all of its employees, you can add as many sites to this diagram as you wish and the model remains the same. All of the data that Cisco Unity collects in the Directory—Cisco Unity objects, mail users, public distribution lists, and so on—are synchronized with the local Structured Query Language (SQL) database on each of the servers. Therefore, directory lookups for subscribers across the organization are fast.

Information written to the directory from SQL is a considerably smaller set of data than earlier versions of Cisco Unity. Only information needed to find subscribers, address messages to them, and transfer to their phone will be stored in the directory itself; everything else will be on the local SQL database. Here is a list of the subscriber data that is sent to the directory:

- First name
- Last name
- Display name
- Recorded voice name
- E-mail alias
- Fax ID (Used for integration with third-party fax servers for routing inbound faxes directly to the subscriber mailbox)

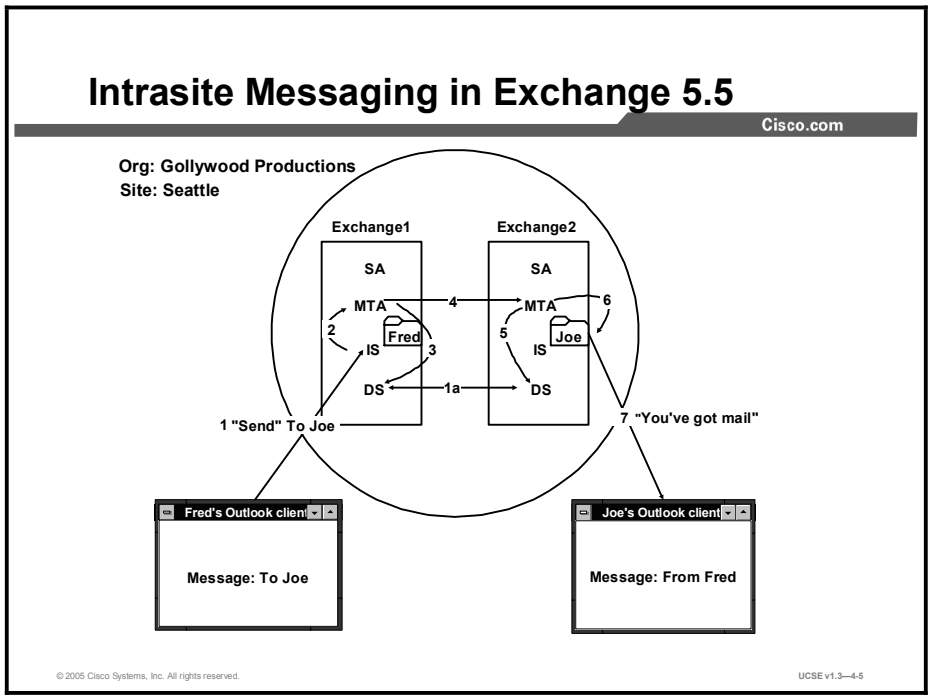
- Primary ID (Usually the work extension of the subscriber. This is the ID that the subscriber uses to log on to the voice-mail system.)
- Up to nine alternate IDs
- Location object assignment
- System ID (This identifies the Cisco Unity server that the subscriber is associated with.)
- Transfer string (The specific digits necessary to ring the subscriber phone. This can include trunk access codes, pauses, and DTMF digits. There can only be one string per subscriber.)

In the example in the figure, all of the information known about a subscriber is first entered into the local SQL database in Seattle when you add a subscriber there. On its regular replication schedule, the SQL database pushes the items listed above to the directory. From there the changes are picked up by the other SQL database(s). In this way, a subscriber in Chicago could look up that Seattle subscriber by either name or extension and hear their voice name back as confirmation when addressing a message.

The direct message connections are limited to the servers in the local site. Any subscriber can send messages to users outside the site by using the message transfer cloud (the Mail Transfer Agent [MTA] in Exchange 5.5, or SMTP in Exchange 2000), but you can only log in and access messages on a server in your site. The same sorts of limitations apply to Exchange 2000 and Domino. Only the names of the defined boundaries will change.

Intrasite Messaging in Exchange 5.5

This topic describes how intrasite messaging assures that messages are delivered to the correct home server.



The following steps describe the process of intrasite messaging in Exchange 5.5. The numbers of the steps correspond to those in the drawing.

Step 1 Fred composes a message, addresses it to Joe, and sends it.

Step 2 The Exchange1 Information Store (IS) sends a message to the MTA for delivery to a remote Exchange server.

Step 3 The Exchange1 MTA performs a directory lookup in the Directory Service (DS) and finds the name of the remote server MTA.

Step 4 The Exchange1 MTA opens an association (connection) with the Exchange2 MTA and delivers the message.

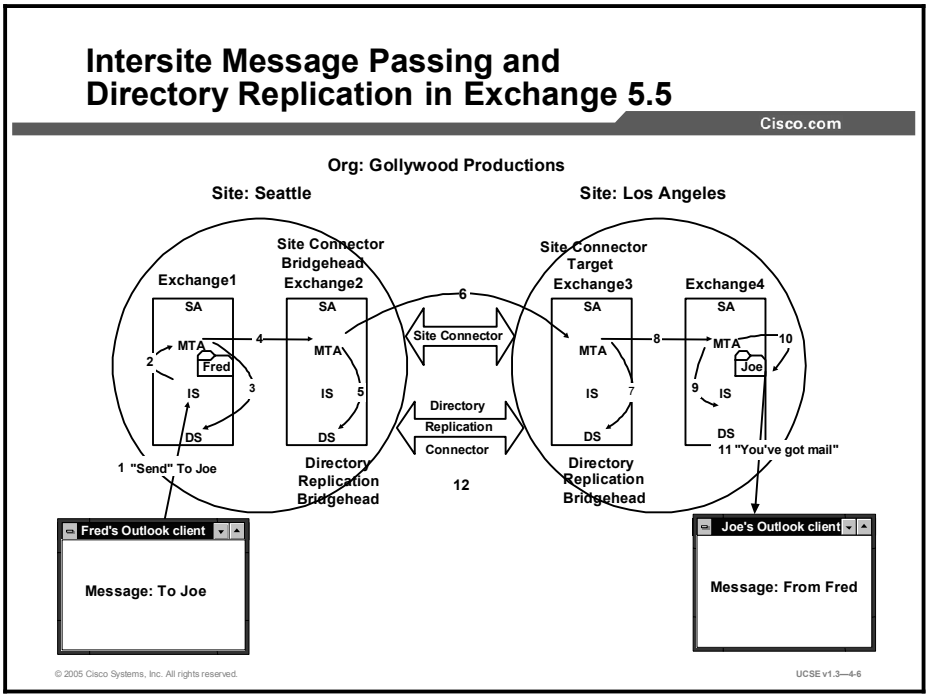
Step 5 The Exchange2 MTA performs a directory lookup in the DS and finds that Joe's mailbox is homed locally.

Step 6 The Exchange2 MTA delivers the message to the IS.

Step 7 Joe sees a new message from Fred show up in his mailbox.

Intersite Message Passing and Directory Replication in Exchange 5.5

This topic describes how intersite messaging assures that messages are delivered to the correct server.



Replication

Within sites, all directory services communicate with each other directly, about five minutes after a change, to keep the Exchange directory up to date. Connecting multiple servers in multiple sites is very similar to a single site, but with a few exceptions. As the Exchange administrator, you must manually set up messaging connectors and directory replication connectors between sites. Messaging connectors include site connectors, X.400 connectors, Internet Mail Service (IMS) connectors, and Dynamic Remote Access Service connectors. You should carefully choose which messaging connector you use, because each connector provides a different set of features, such as connector on/off scheduling and user and message size restrictions.

After you set up your messaging connector(s), you set up the appropriate directory replication connectors based on your organization topology. Since the directory replication connector relies on a messaging connector to send its directory replication messages, it can only be set up after a messaging connector is installed. Directory replication between sites is scheduled to occur every three hours by default, but may be accelerated. Upon initial installation of the directory replication connector, directory replication occurs within a few minutes and typically does not need to be accelerated. After the initial replication, only *changes* are sent on subsequent updates of the directory. Once directory replication has completed, subscribers can address messages to anyone in the organization by accessing either the Cisco Unity telephone directory conversation or the Exchange-based global address list (GAL).

The figure illustrates how messages are passed within an Exchange 5.5 organization with multiple sites and servers. The numbers of the following steps correspond to those in the drawing:

Step 1 Fred composes a message, addresses it to Joe, and sends it.

Step 2 The Exchange1 IS sends a message to the MTA for delivery to a remote Exchange server.

Step 3 The Exchange1 MTA performs a directory lookup in the DS and finds the name of the remote server MTA.

Step 4 The Exchange1 MTA notices that Joe's home server is in the remote site Los Angeles and chooses the Site Connector. The Exchange1 MTA sees that it must send all mail using the Site Connector to the Site Connector Bridgehead, Exchange2.

Step 5 The Exchange2 MTA performs a directory lookup in the DS, realizes that it must pass this message to the remote site Los Angeles, and uses the Site Connector.

Step 6 Because Exchange2 is the Site Connector Bridgehead, its MTA makes a connection to the Los Angeles site connector target server, Exchange3, and delivers the message.

Step 7 The Exchange3 MTA performs a directory lookup and sees that Joe's home server is Exchange4.

Step 8 The Exchange3 MTA passes the message to the Exchange4 MTA.

Step 9 The Exchange4 MTA performs a lookup and sees that Joe is homed on Exchange4.

Step 10 The Exchange4 MTA passes the message to the IS.

Step 11 Joe sees a new message appear in his inbox.

Directory Replication Between Sites

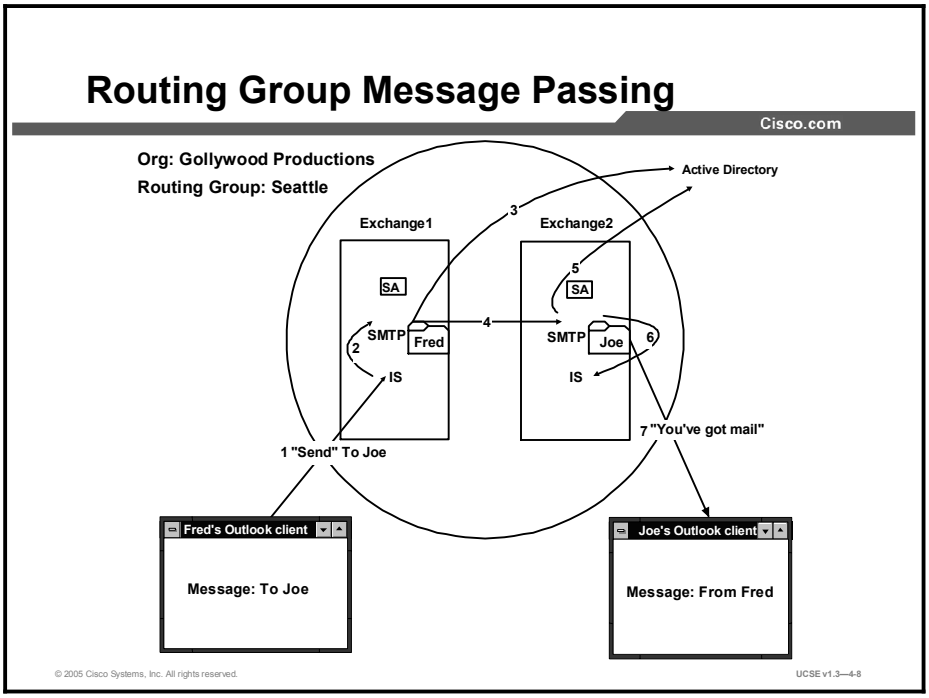
In order for directory replication to occur between sites, you must install the Directory Replication Connector after you install a Site Connector. As part of the installation process, you must define a bridgehead server in each site. Replication between these bridgehead servers occurs once every three hours by default. This number may be changed in the connector property pages. All Domain Server changes are sent between bridgeheads as mail messages. The local MTAs are responsible for delivery.

Intra-Routing Group Message Passing and Directory Replication

Exchange 2000 uses routing groups to perform functions similar to sites in Exchange 5.5. If a server in a routing group is the only server in that group, all messages and directory information reside on that server. However, if two or more servers exist in a routing group, messages must be delivered to the correct home server and directories must be accessed. To accomplish delivery of messages, Exchange 2000 relies on Active Directory to provide information about where the recipient is homed. The home server for a recipient is specified when the recipient is created, but may be modified by an administrator at any time and is the server where the mail of the recipient is physically kept on disk for retrieval. Once a server is added to a site, directory information is shared automatically so that each server in the site knows the list of recipients on every other server in that site. Directory information is available to all servers that are members of the same forest.

Routing Group Message Passing and Active Directory Replication

This topic describes how routing group message passing assures that messages are delivered to the correct home server in a multiple routing group environment.



The following steps describe the process of routing group message passing. The numbers of the steps correspond to those in the figure.

Step 1 Fred composes a message, addresses it to Joe, and sends it.

Step 2 The Exchange1 IS sends a message to the SMTP for delivery to a remote Exchange server.

Step 3 The Exchange1 SMTP performs a directory lookup in the Active Directory and finds the name of the remote server SMTP.

Step 4 The Exchange1 SMTP opens an SMTP connection with the Exchange2 SMTP and delivers the message.

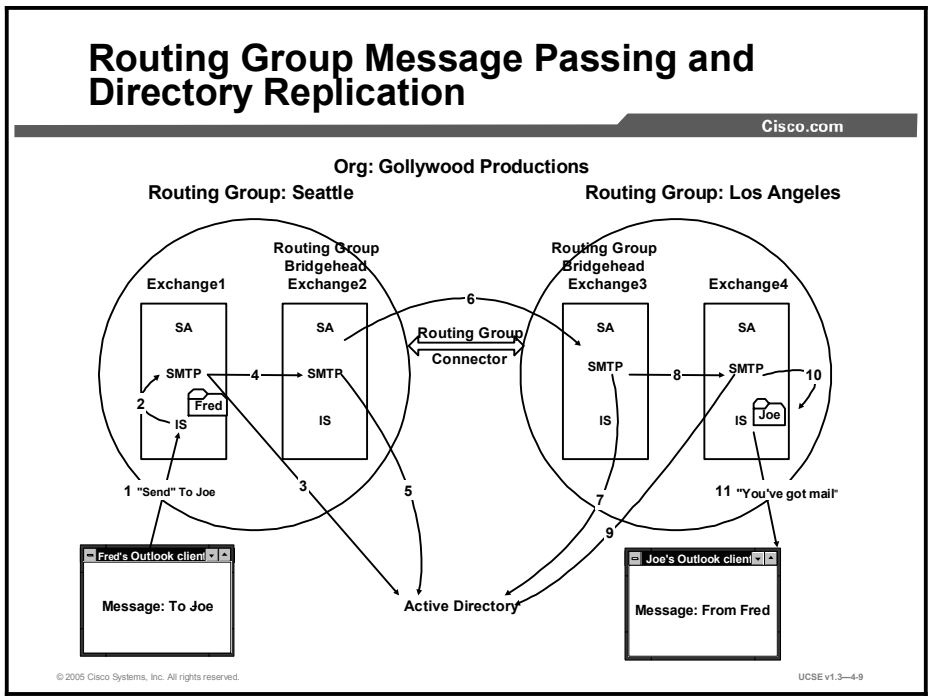
Step 5 The Exchange2 SMTP performs a directory lookup in the Active Directory and finds that Joe's mailbox is homed locally.

Step 6 The Exchange2 SMTP delivers the message to the IS.

Step 7 Joe sees a new message from Fred show up in his mailbox.

Replication

Active Directory handles all directory services within a Windows 2000 forest, which maintains a one-to-one correspondence with the Exchange organization. The time it takes to replicate information will vary depending on what Windows 2000 knows about the links between servers and groups. Inside a routing group, all servers should be on fast, permanent LAN links, so replication of updated attributes of directory objects takes place every five minutes.



Connecting multiple servers in multiple routing groups is very similar to a single routing group, but with a few exceptions. As the Exchange Administrator, you must manually set up routing group connectors between groups. You do this by establishing bridgehead servers in both routing groups and setting a cost for each route. If you have multiple routing groups configured with alternate paths, it is possible for Exchange 2000 to deliver messages even if the primary link between two routing groups is down.

The figure illustrates how messages are passed within an Exchange 2000 organization with multiple routing groups and servers. The numbers of the following steps correspond to those in the drawing:

Step 1 Fred composes a message, addresses it to Joe, and sends it.

Step 2 The Exchange1 IS sends a message to the SMTP for delivery to a remote Exchange server.

Step 3 The Exchange1 SMTP performs a directory lookup in the Active Directory and finds the name of the remote server SMTP.

Step 4 The Exchange1 SMTP notices that Joe's home server is in a different routing group, Los Angeles, and, after consulting its internal link-state table, chooses the least-cost routing group connector. The Exchange1 SMTP sees that it must send all mail using the routing group connector to the group bridgehead, Exchange2.

Step 5 The Exchange2 SMTP performs a directory lookup in the Active Directory (AD), realizes that it must pass this message to the routing group Los Angeles, and uses the connector.

Step 6 Because Exchange2 is the connector bridgehead, its SMTP makes a connection to the Los Angeles connector target server, Exchange3, and delivers the message.

Step 7 The Exchange3 SMTP performs a directory lookup and sees that Joe's home server is Exchange4.

Step 8 The Exchange3 SMTP passes the message to the Exchange4 SMTP.

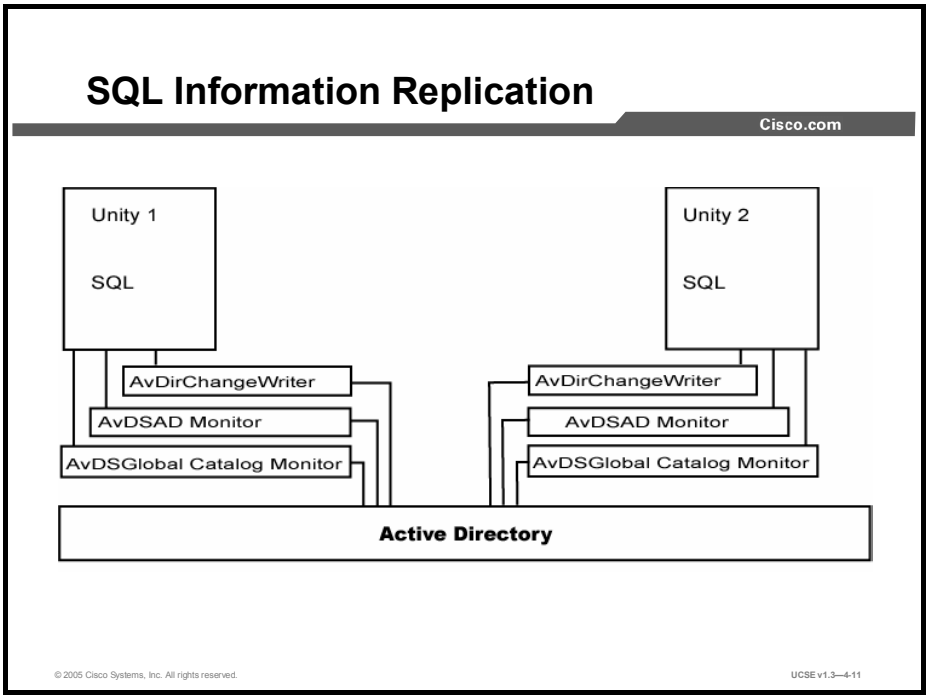
Step 9 The Exchange4 SMTP performs a lookup and sees that Joe is homed on Exchange4.

Step 10 The Exchange4 SMTP passes the message to the IS.

Step 11 Joe sees a new message appear in his inbox.

SQL Information Replication

This topic describes how SQL replication works in a Cisco Unity environment.

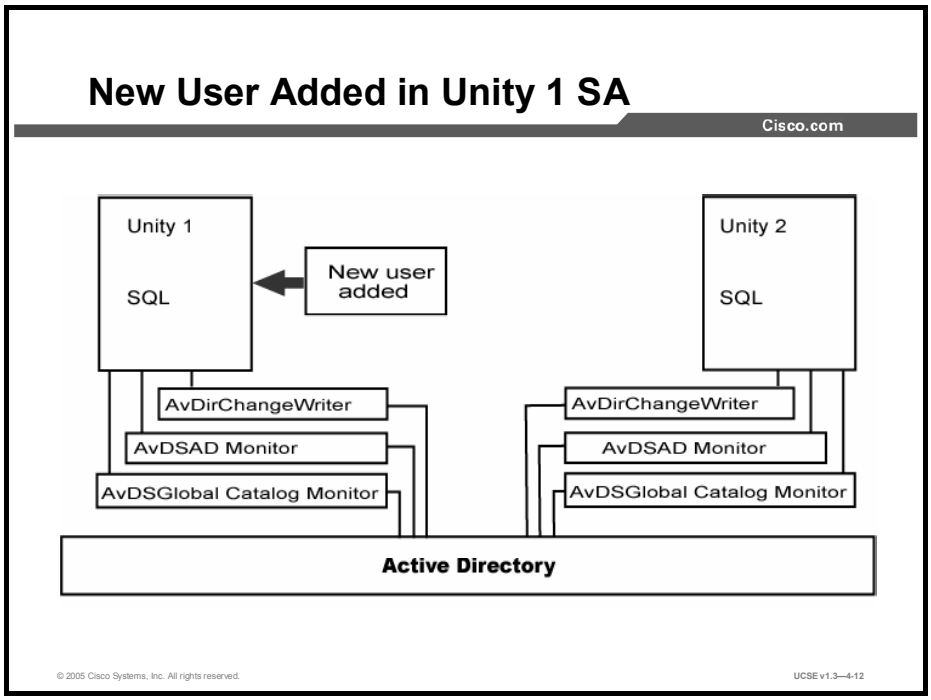


Active Directory Replication

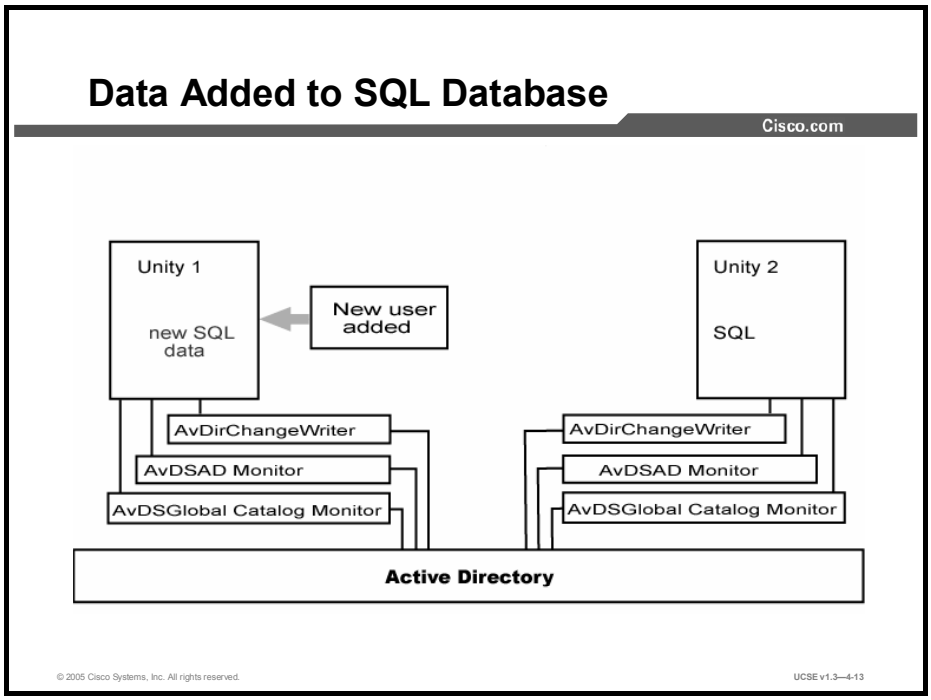
Active Directory, a directory service built using Internet-standard technologies, is fully integrated with Exchange 2000. All Exchange directory information is stored within AD, which stores data for a large and customizable set of objects. Cisco Unity takes advantage of the ability of AD to be customized when it extends the AD schema. All domain controllers in a forest contain a copy of the same AD database. Once the initial directory is built, AD replicates changed or updated attributes of an object to all other domain controllers in its forest. Once directory replication has completed, subscribers can address messages to anyone in the organization by accessing either the Cisco Unity telephone directory conversation or the Exchange-based GAL.

Following is a detailed look at the way Cisco Unity interacts with the Active Directory. Start with two Cisco Unity systems installed in the same Active Directory forest.

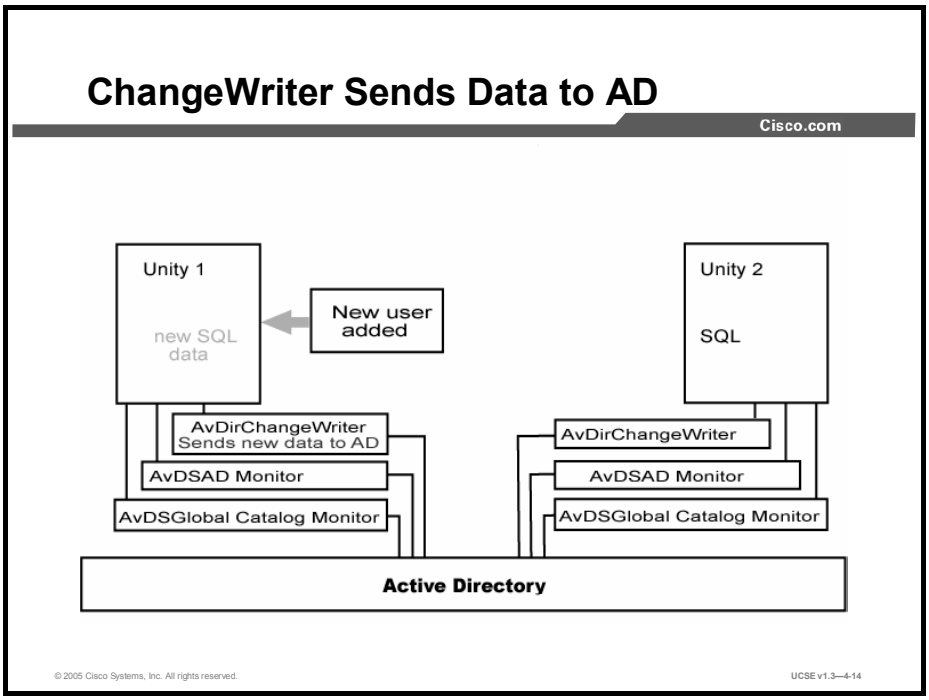
A typical administrative action might be the addition of a new subscriber using the Cisco Unity HTML administration tool.



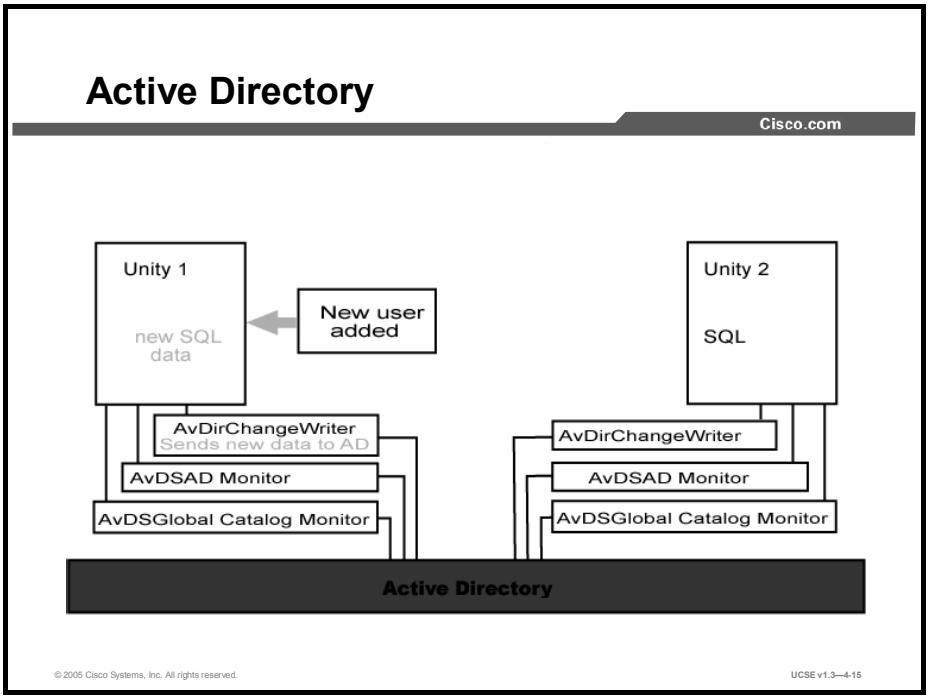
Once the administrator saves the data, it is written to the Unity 1 local SQL database.



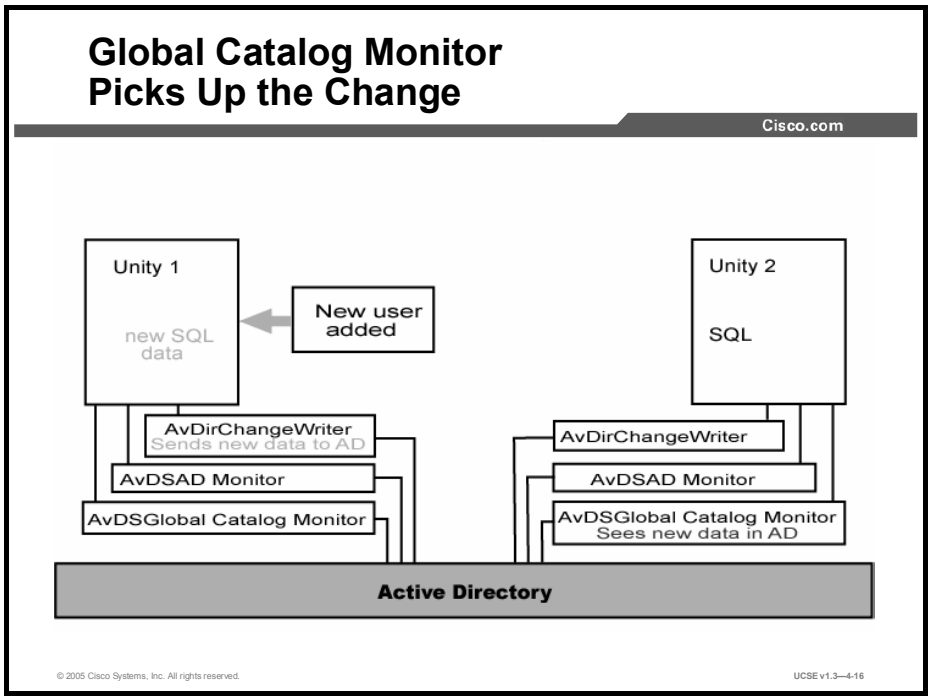
The Unity 1 Directory Change Writer (AvDirChangeWriter) sees the data and sends the relevant pieces of it to Active Directory.



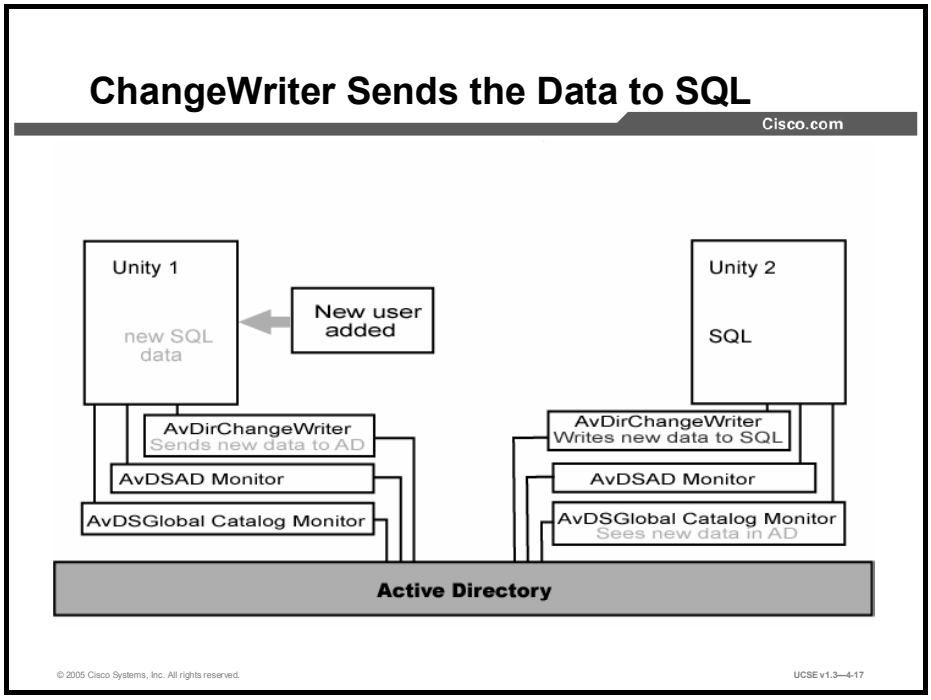
Now that the data is located in Active Directory, it is replicated through the forest on its already-established schedule.



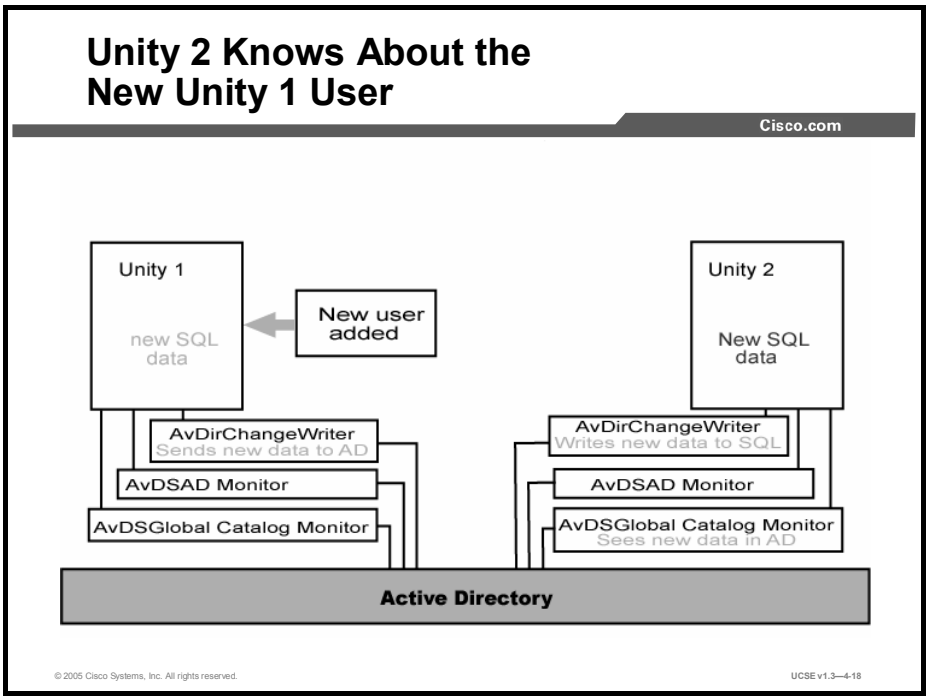
The Unity 2 server Global Catalog Monitor (AvDSGlobalCatalogMonitor), a service that continuously monitors the Active Directory, notices the change.



The Global Catalog Monitor passes a message to the ChangeWriter to send the changes to the local SQL database in Unity 2.



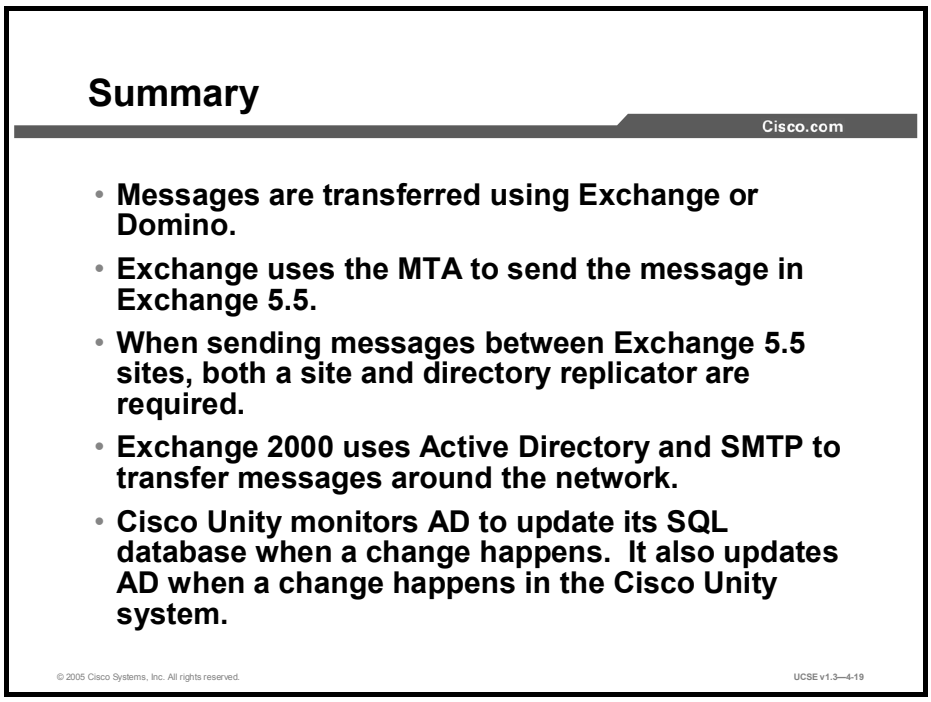
Any subscriber or outside caller reaching Unity 2 can now address and send messages to the new subscriber on Unity 1.



At this point, new SQL data has been replicated and is available on Unity 1 and Unity 2.

Summary

This topic summarizes the key points discussed in this lesson.



Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) Exchange 5.5 uses an (the) _____ to transfer messages.

A) SA
B) SID
C) MTA
D) DID

Q2) With intersite message passing, all sites are a member of the same _____.

A) site connector
B) organization in Exchange
C) site in Exchange
D) MTA

Q3) What are the connectors between different logical parts of the same organization using Exchange 2000 called?

A) site connectors
B) organizational connectors
C) routing group connectors
D) directory replication connectors

Q4) Cisco Unity uses which services to monitor AD for changes?

A) AVDirChangeWriter
B) AVDSAD Monitor
C) AVCVS Catalog Monitor
D) AVGaen Monitor

Quiz Answer Key

Q1) C

Relates to: Message Transfer and Directory Replication

Q2) B

Relates to: Routing Group Message Passing and Active Directory Replication

Q3) C

Relates to: SQL Information Replication

Q4) A,B

Relates to: SQL Information Replication

Lesson 3

Networking Subscribers

Overview

This lesson describes the options available for adding subscribers and presents a decision tree for choosing the most appropriate type of subscribers.

Relevance

In order to implement networking between Cisco Unity and other messaging systems, you must understand the basic concepts and terminology. This lesson defines the building-block concepts for understanding particular implementations of networking.

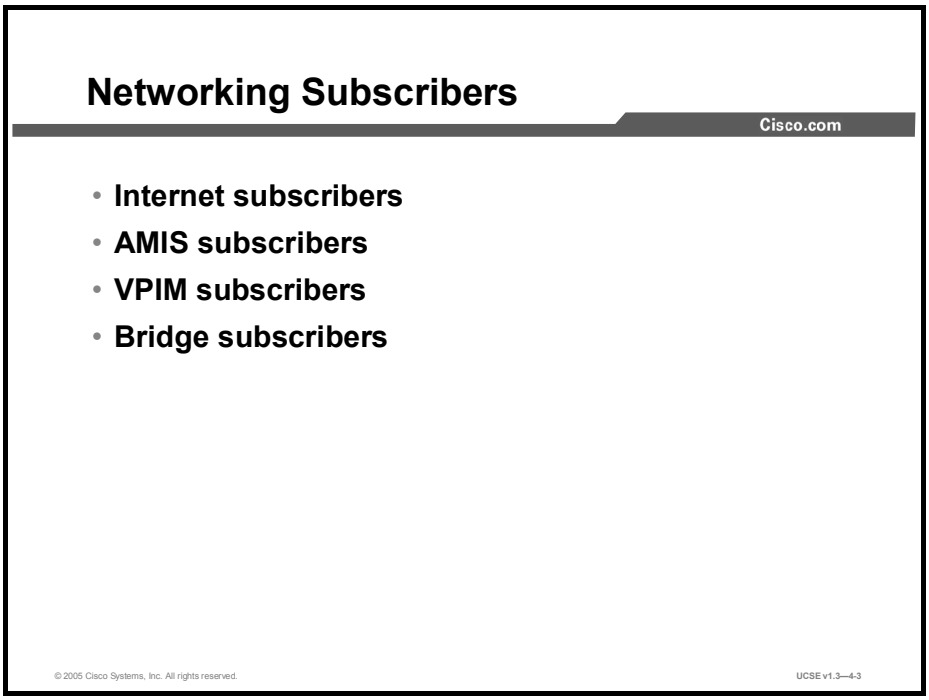
Objectives

Upon completing this lesson, you will be able to select and describe the appropriate type of subscription for each user in a Cisco Unity networking solution. This ability includes being able to meet these objectives:

- Describe the options available for the different types of subscribers and present a decision tree for choosing the most appropriate type of subscribers
- Describe the characteristics of an Internet subscriber
- Describe the characteristics of an AMIS subscriber
- Describe the characteristics of a VPIM subscriber
- Describe the characteristics of a Bridge subscriber
- Describe the choices to be made when using Internet, AMIS, VPIM, and Bridge subscribers or blind addressing

Networking Subscribers

This topic describes the different types of subscriber options available and presents a decision tree for choosing the most appropriate type of subscribers.

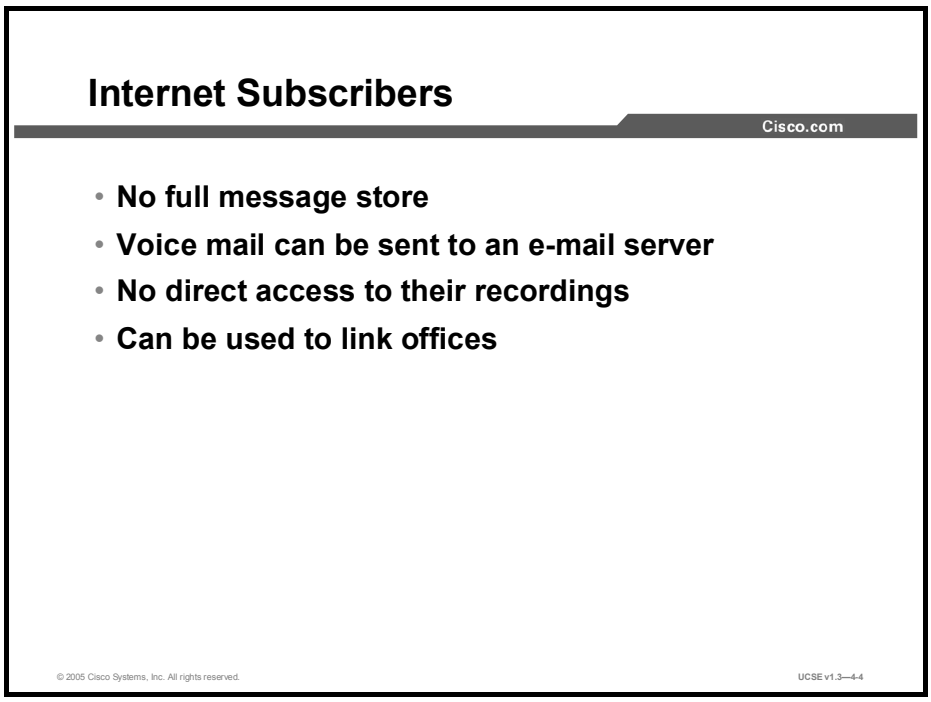


Internet, Audio Messaging Interchange Specification (AMIS), Voice Profile for Internet Mail (VPIM), and Bridge subscribers share most features with regular Cisco Unity subscribers. You can give them an off-campus telephone number, and calls will be transferred there if the numbers are compatible with the Cisco Unity call restriction tables or the call restriction tables of the PBX that Cisco Unity is associated with. Outside callers may look up Internet, AMIS, VPIM, or Bridge subscribers in the directory (unless you have restricted this access) and leave voice mail for them. The subscribers can be members of distribution lists. The main purpose of the recipients is to allow them to address messages to them by name or by extension so that they receive messages in a transparent manner.

Blind addressing allows Cisco Unity to address messages without having specific information about the recipients on the remote voice messaging system. One of the steps in setting up blind addressing is to change the Blind Addressing setting on the Primary Location > Addressing Options page to something other than None. You also create a delivery location that corresponds to each voice messaging system with which Cisco Unity communicates. When blind addressing a message, subscribers dial a number that is made up of the delivery location Dial ID and the mailbox number of the recipient. Before addressing the message, Cisco Unity parses the number that the subscriber entered and searches for a matching delivery location. If Cisco Unity does not find a matching location, it reports the error to the sender and does not address the message. If a matching delivery location is found, Cisco Unity addresses the message without verifying that the remote mailbox number exists. Cisco Unity does provide voice name confirmation that the delivery location exists before addressing the message (assuming a voice name was recorded for the delivery location).

Internet Subscribers

This topic describes the characteristics of an Internet subscriber.



Internet subscribers are special types of Cisco Unity voice-mail users specifically used for networking and Simple Mail Transfer Protocol (SMTP) mail delivery. When you add a new subscriber in the Cisco Unity Administrator, a radio button option allows you to create an Internet subscriber (mailbox) and specify an SMTP address for that user. This is similar to an Exchange custom recipient in Exchange 5.5 or a contact in Windows 2000/Exchange 2000; the Internet subscriber is actually a mailbox that has no local message store.

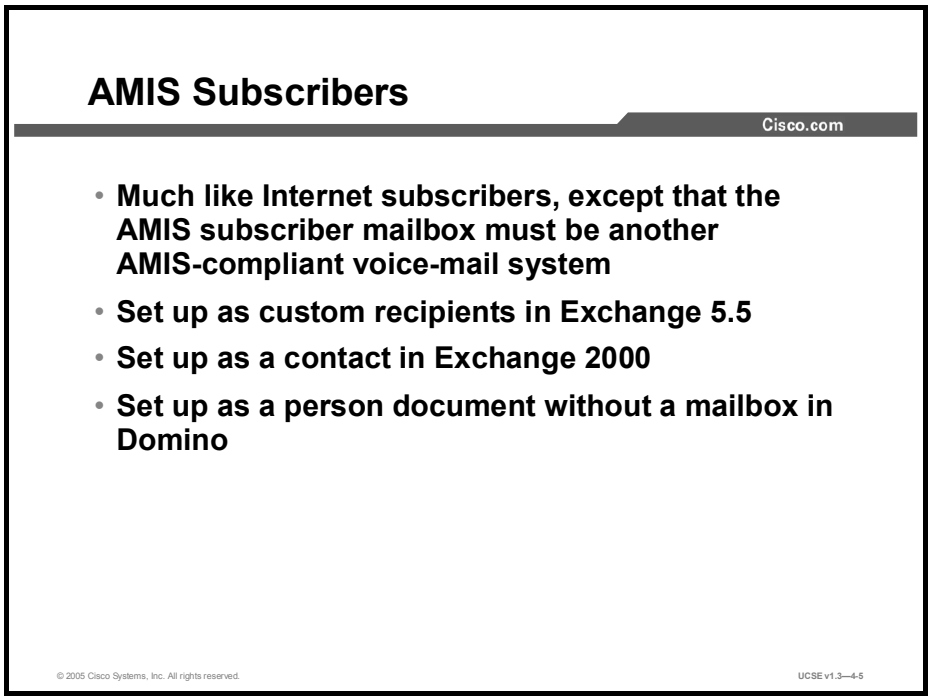
When creating an Internet subscriber, setup options relating to the local message store are not available. These options include phone password, private lists, conversation, and message notification. In other words, the mailbox acts as a pointer to the SMTP address you specify when you create the Internet subscriber account. Both outside and internal callers benefit from the ability to address messages to the subscriber over the telephone, in most cases, and internal users also have an option to address them using the global address list (GAL). The Internet subscriber has a recorded voice name and greeting just like any other Cisco Unity subscriber. The main difference between a regular Cisco Unity subscriber and an Internet subscriber is that when mail is left for Internet subscribers, the mail is delivered out the SMTP gateway (Internet Mail Service [IMS]) to its Internet destination as specified within their account. The end location could be any other mail server or even another voice-mail system, and therefore allows an offsite users (such as a field technician or outside sales person) to look and feel to the sender as if that recipient were actually on site.

Additionally, you can use Internet subscribers to link offices without the need to set up messaging connectors and directory replication connectors between sites. However, you must manually and individually set up Internet subscribers for each destination location. This may be unacceptable where a large number of users exist in remote offices. For organizations with many users in various locations, blind addressing is typically a better choice than Internet subscribers.

Internet subscribers can be used for delivering Cisco Unity voice messages to other non-directory-replicating Cisco Unity subscribers. With the Voice Connector, the message gets to the Cisco Unity subscriber as a voice-mail type message; the light on the phone comes on and the pager goes off and it is a standard voice message, not an attachment.

AMIS Subscribers

This topic describes the characteristics of an Audio Messaging Interchange Specification (AMIS) subscriber.

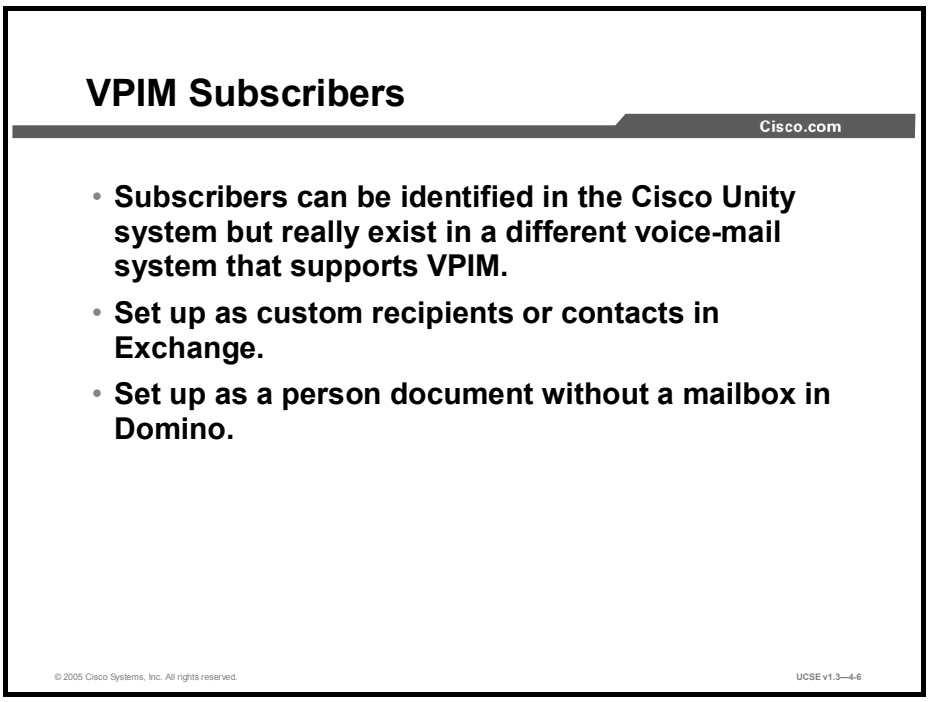


Cisco Unity 4.0 offers users the ability to interface with third-party voice-mail systems using the Audio Messaging Interchange Specification analog (AMIS-a) protocol. AMIS subscribers are much like Internet subscribers, with one important difference. While the off-box storage of an Internet subscriber is generally another e-mail system, the off-box storage of an AMIS subscriber is going to be a different voice-mail system. The AMIS subscriber off-box storage appears as custom recipients in Exchange 5.5 or contacts in Active Directory.

As with Internet subscribers, options relating to the local message store are unavailable. This means that AMIS subscribers cannot log on to Cisco Unity to check or send messages, log on to Cisco Unity via the telephone, or use Active Assistant to change personal settings, own private lists, set up or receive message notification, or receive message waiting indication via Cisco Unity. Messages sent to an AMIS subscriber are transferred to the target voice-mail system through telephone calls placed from one server to the other, and messages played over the analog phone lines.

VPIM Subscribers

This topic describes the characteristics of a VPIM subscriber.

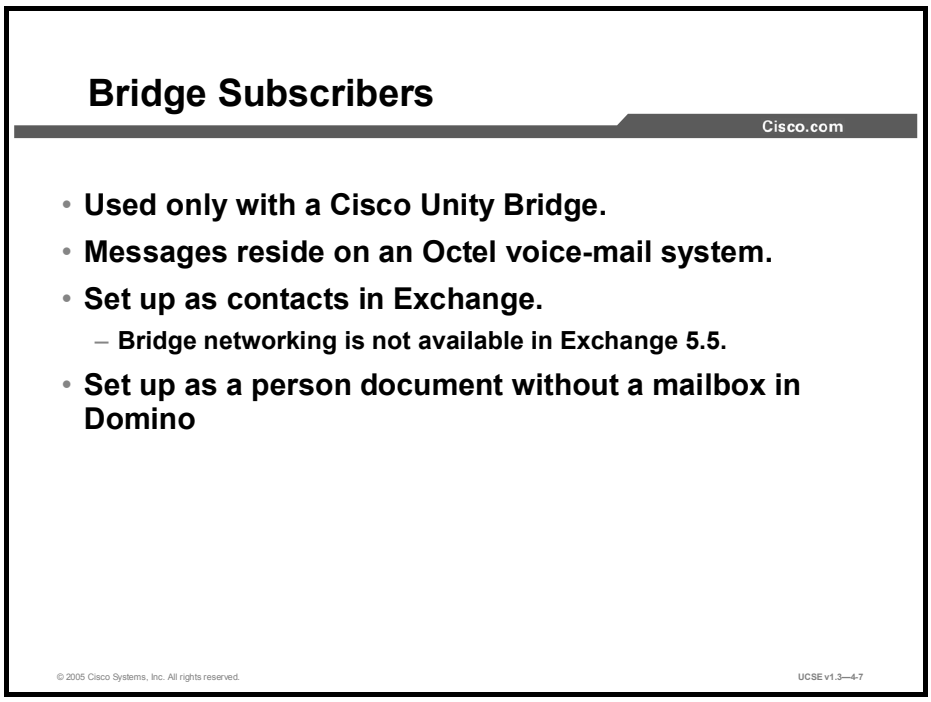


Cisco Unity Version 4.0 offers users the ability to interface with third-party voice-mail systems using VPIM. The main advantage of using VPIM over AMIS is that VPIM messages are transferred digitally, while AMIS messages are transmitted over analog lines. This results in messages being sent more quickly via VPIM. As with AMIS, the off-box storage of a VPIM subscriber is going to be a different voice-mail system. VPIM subscribers appear as contacts in Active Directory. The main difference is that the messages are transmitted via SMTP rather than as an analog message over the PSTN.

As with Internet subscribers, any options relating to the local message store are unavailable. This means that VPIM subscribers cannot log in to Cisco Unity to check or send messages, log in to Cisco Unity via the telephone, or use Cisco Unity Assistant to change personal settings, own private lists, set up or receive message notification, or receive message waiting indication via Cisco Unity.

Bridge Subscribers

This topic describes the characteristics of a Bridge subscriber.

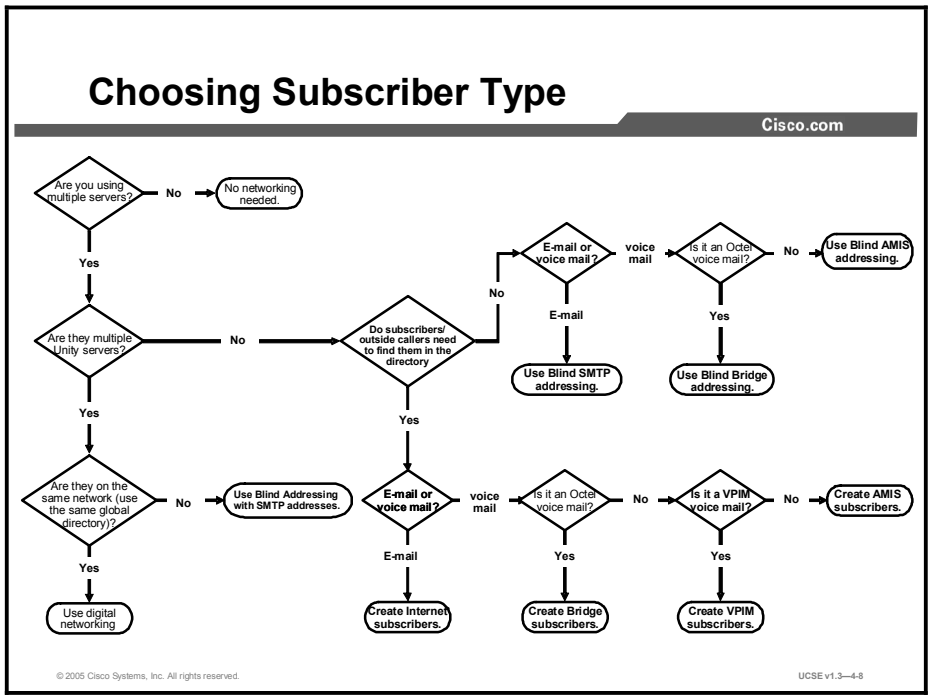


Bridge subscribers are created in Cisco Unity to enable Cisco Unity subscribers to find them in the directory and to send messages as they would to any other subscriber. Bridge subscribers are associated with a delivery location and are stored as contacts in Active Directory. Mailbox greetings and voice names can be individually recorded for each Bridge subscriber. Messages sent to a Bridge subscriber are sent through the Cisco Unity Bridge server to the applicable mailbox on the Avaya Octel system. Bridge subscribers do not have messages stored locally. Their messages are stored on the Octel messaging system.

Bridge subscribers are automatically created when the Bridge creates usage-based directory entries for Octel users (in support of NameNet). You can also create Bridge subscribers manually in Cisco Unity or create permanent directory entries on the Bridge server, which results in the automatic creation of Bridge subscribers. Bridge subscribers that are automatically created are referred to as “auto-created Bridge subscribers.”

Choosing Subscriber Type

This topic describes the choices to be made when using Internet, AMIS, VPIM, and Bridge subscribers or blind addressing.



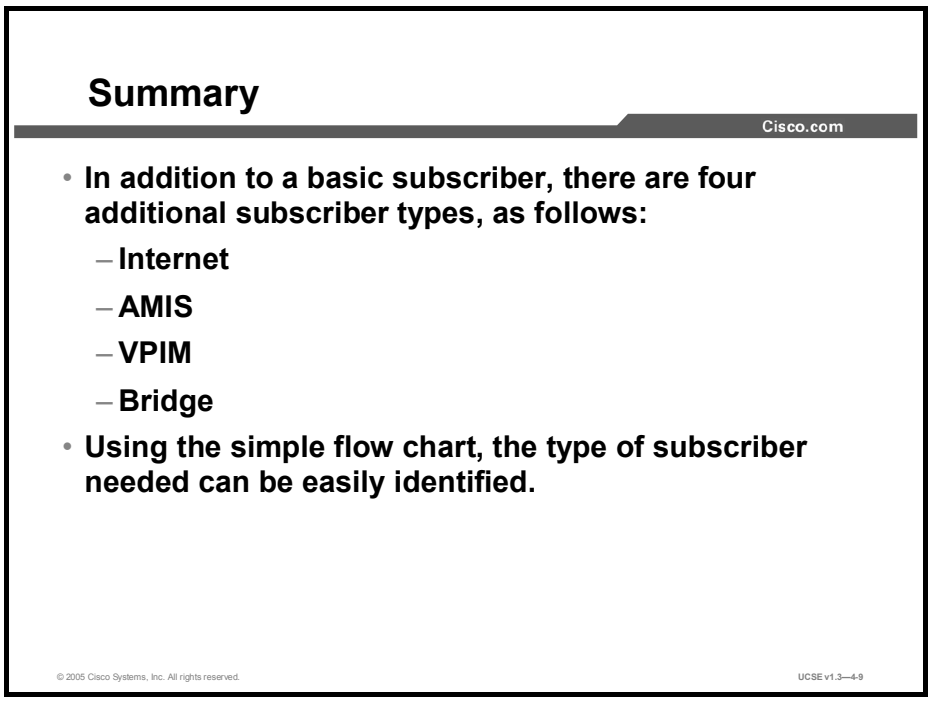
The flowchart in the figure represents a decision tree for choosing which types of subscribers to create on a Cisco Unity server. The choices are not mutually exclusive. It is possible, because of multiple message targets, to need several of the subscriber addressing options.

After asking a series of three or four questions, you can determine which type of target server and which type of addressing to use. First, find out whether all of the target servers are Cisco Unity servers; and if they are, whether they all use the same global directory. If they do, then implementing digital networking is the best choice. If not, blind SMTP addressing will work best.

If you know that the servers are not Cisco Unity servers, but you want callers to be able to find these subscribers in the directory, then you will implement them as AMIS, VPIM, Internet, or Bridge subscribers. Which type you choose is dependent on the target server. If the target servers are not Cisco Unity servers and you do not wish to have the subscribers listed in the directory, blind addressing will work best.

Summary

This topic summarizes the key points discussed in this lesson.



Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) Which of the following are network subscribers? (Choose two.)

A) AMIS
B) Domino
C) Exchange
D) Internet
E) SNMP

Q2) Match the following subscribers with their attribute:

A) message destination is e-mail
B) uses analog voice delivery
C) uses IP networking for voice delivery
D) only used with Octel analog systems

_____ 1. Bridge subscriber

_____ 2. Internet subscriber

_____ 3. AMIS subscriber

_____ 4. VPIM subscriber

Quiz Answer Key

Q1) A, D

Relates to: Networking Subscribers

Q2) A-2

B-3

C-4

D-1

Relates to: Networking Subscribers

Lesson 4

Applying Digital Networking in Cisco Unity

Overview

In organizations with multiple Cisco Unity servers, digital networking is the feature that allows subscribers to exchange voice messages with other Cisco Unity subscribers who are homed on separate Cisco Unity servers. Digital networking also allows for outside caller access to all users from any Cisco Unity server in a transparent manner. This lesson describes the components of digital networking and how to implement them.

Relevance

Digital networking is enabled on every Cisco Unity server as a standard feature. Understanding the basic concepts of digital networking and the details of how to implement them will enable you to provide digital networking in a seamless and efficient manner.

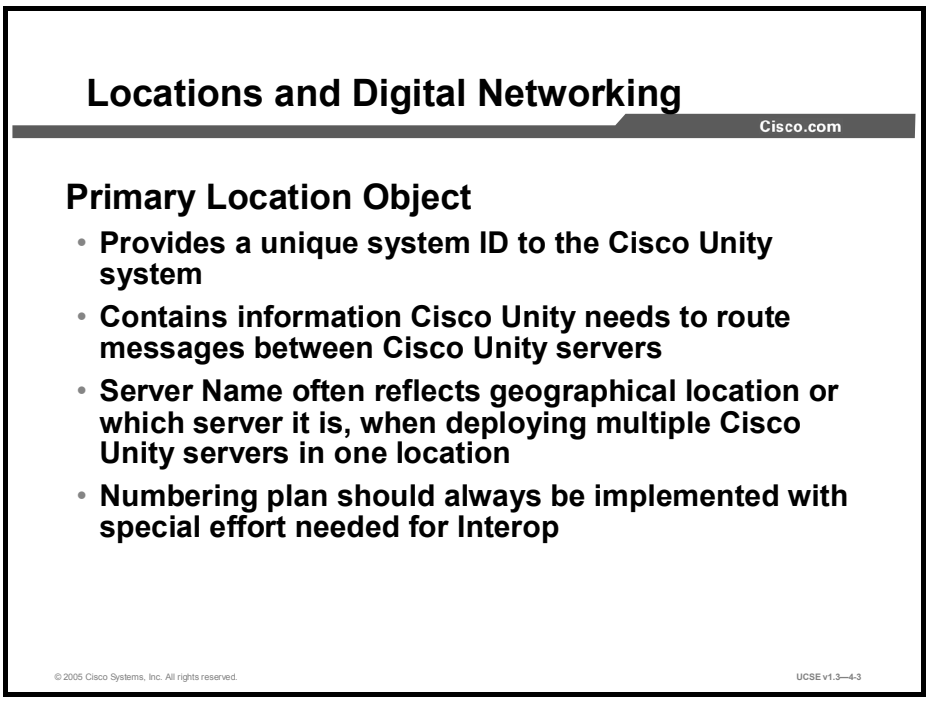
Objectives

Upon completing this lesson, you will be able to describe how messages can be exchanged between Cisco Unity servers using digital networking. This ability includes being able to meet these objectives:

- Describe the purpose and function of location objects in digital networking
- Describe the requirements for setting up digital networking
- Describe the steps needed to set up digital networking
- Describe the parameters that determine how extensive a search will be
- Define the concept of dialing domains in Cisco Unity

Locations and Digital Networking

This topic describes the purpose and function of location objects in digital networking.



Location objects are key items in digital networking. When you install Cisco Unity, a single default location, known as the primary location object, is created. As subscribers are added to Cisco Unity, they become members of this default location. The Cisco Unity Administrator allows you to create additional location objects that represent other messaging servers, including Cisco Unity. If you are in the same Active Directory forest, there is no need to create additional locations, because location objects will be available as delivery locations. Each Cisco Unity server will see the other Cisco Unity servers that are connected to the main directory as delivery locations. It is important to set up the primary location object to define and provide server information to the rest of the Cisco Unity servers connected to the single directory. It is also critical to set up the primary location object with a proper numbering plan if there will be any interop connections. The system location objects can be tied together using a property called the dialing domain ID. The dialing domain ID allows you to create a meta-location that spans multiple Cisco Unity servers by assigning them all the same dialing domain ID, which allows you to easily span sites or other networking boundaries, and to provide transparent dialing capabilities to customers that have networked telephone switches.

Recorded object data for the location object includes the following:

- A voice name for addressing
- A display name for the administrative console
- Three dual tone multifrequency (DTMF) names (one for each keypad mapping)
- A DTMF ID for addressing
- An SMTP address for blind addressing
- A destination type
- A send blind flag
- Information about the keypad mapping used at that location

In Cisco Unity, subscribers and system objects can only be associated with the primary location object created by the setup program. All other location objects are used solely for addressing purposes.

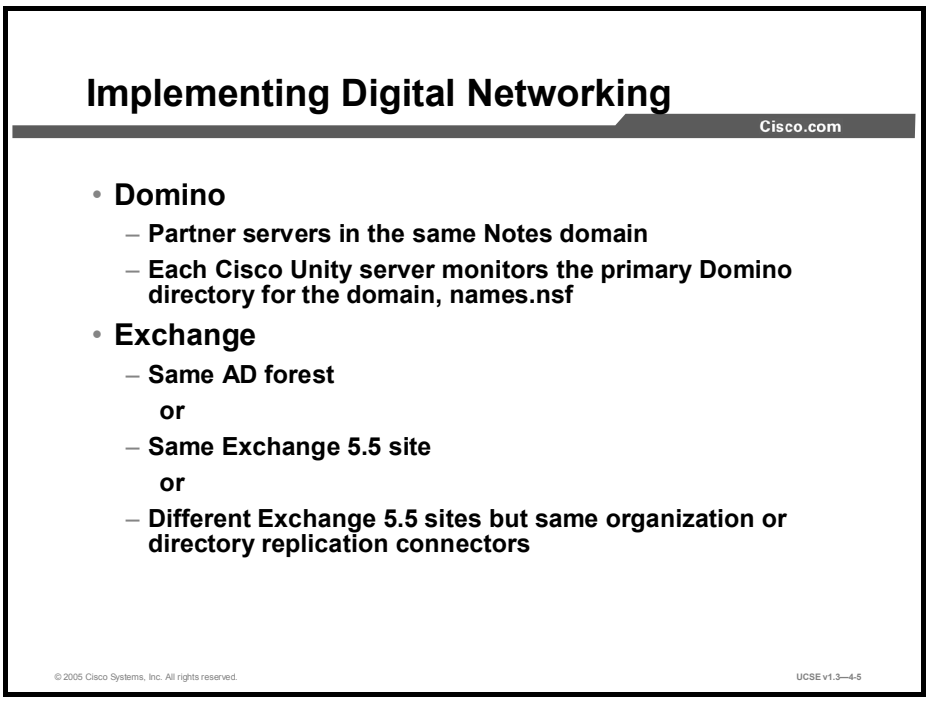
When outside callers use the Cisco Unity directory, they are presented with a list of names that includes members of the primary location object. Directory search options can be configured so that all other administrator-created locations are available to all callers. Users associated with any location object other than the default object may be added to public and private distribution lists or added to message address lists by subscribers only.

When defining the primary location object, you give it a Dial ID. Creating a dial plan for your organization that will result in callers reaching subscribers correctly and efficiently is very important. The Dial IDs that you create are an important part of that dial plan. Be sure that they do not conflict with previously assigned IDs.

In the Cisco Unity Administrator, all location objects will be visible, but administrators will only be able to edit or delete location objects created on their Cisco Unity system. Location objects that replicate from other sites will be read-only. The original location object that is installed with the system (the primary location object) can be edited but not deleted from the system.

Implementing Digital Networking

This topic describes the requirements for implementing digital networking.

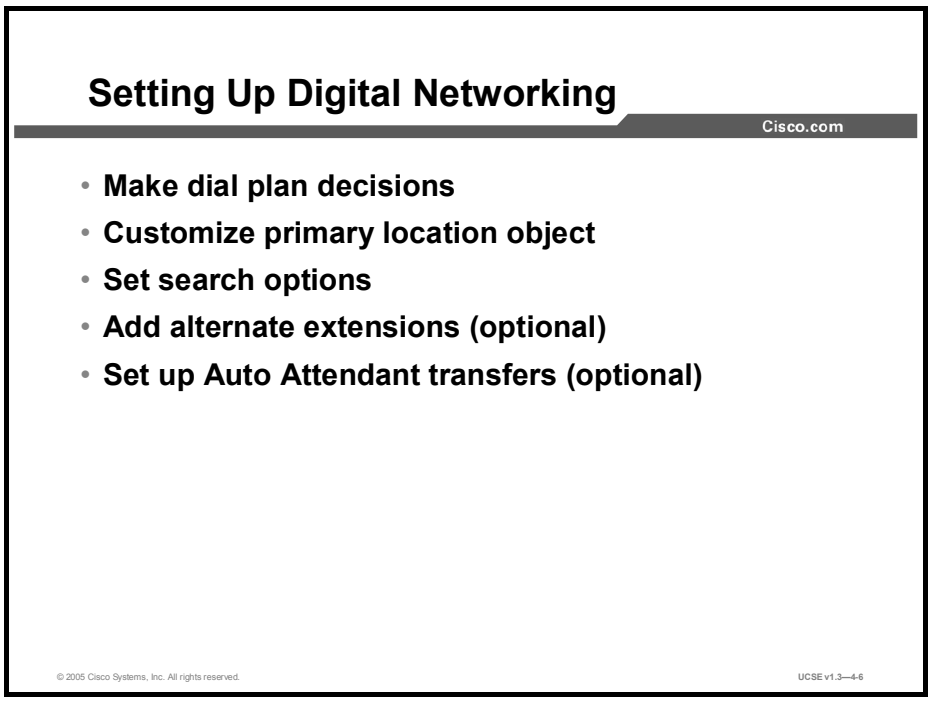


Implementing digital networking in Cisco Unity is easily accomplished once you understand the requirements. All subscribers who expect to send messages using the digital networking feature must be able to see each other's address. This means that, in a Domino environment, all of the partner servers must be in the same Notes domain, and each Cisco Unity server must monitor the Domino directory for the domain: names.nsf. In an Exchange environment, all servers must be members of the same Active Directory forest, or be members of the same Exchange 5.5 site, or be members of sites in an Exchange 5.5 organization that are connected for directory replication.

With these conditions met, all subscribers will be able to see all locations and all subscribers at those locations. The ultimate factor is directory replication. Any site, location, or administrative group that has access to the directory can be digitally networked. Conversely, if an entity cannot see the directory, it cannot participate in digital networking.

Setting up Digital Networking

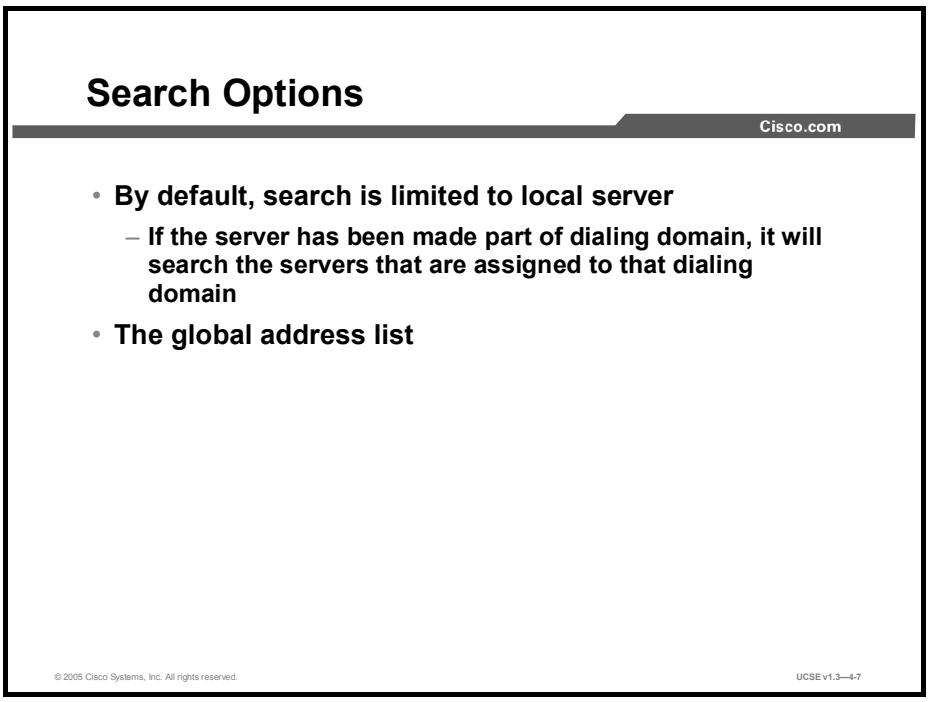
This topic describes the steps needed to set up digital networking.



Setting up digital networking is very simple. Once you make dial plan decisions, you can customize primary location objects on all Cisco Unity servers. Alternate extensions provide two benefits: the ability to provide easy message access (automatic sign-in to a subscriber account) from telephones other than the subscriber primary extension, and an extension address that matches the one that other subscribers use to reach a subscriber on a networked telephone system. If the Cisco Unity servers are attached to a networked telephone system, you should also set up Auto Attendant transfers. If each Cisco Unity server is integrated with a separate phone system, this step is not necessary.

Search Options

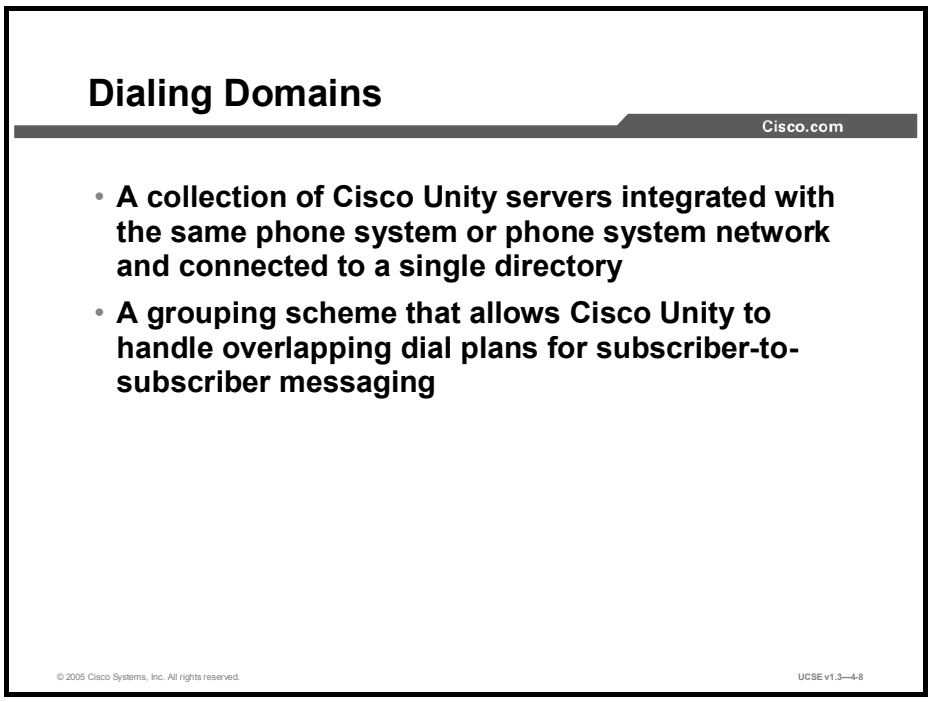
This topic describes the parameters that determine how extensive a search will be.



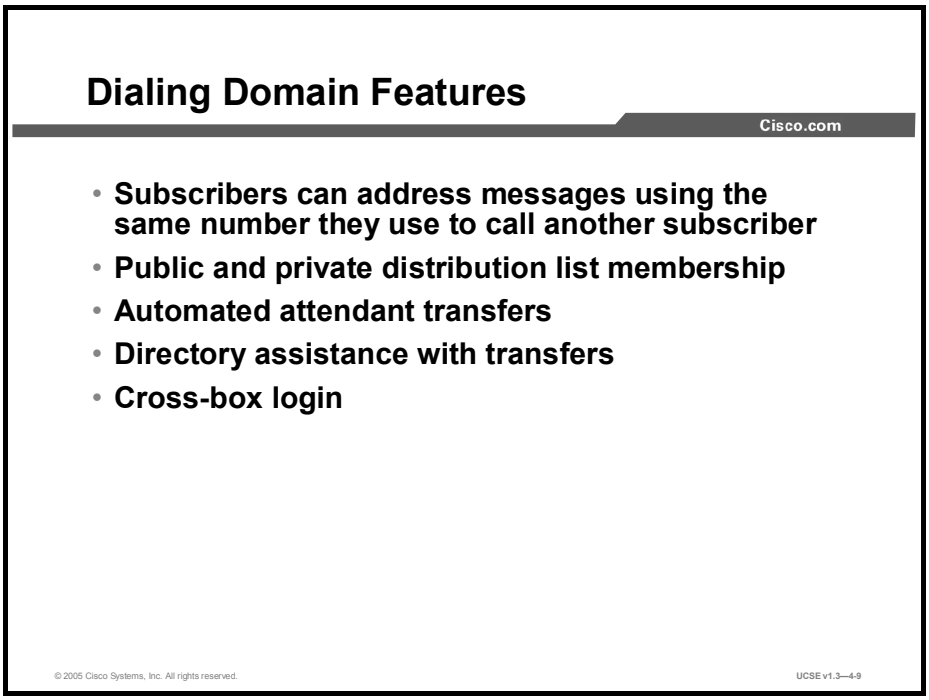
You define searches in Cisco Unity in order to put parameters on how extensive your search will be. Searches are needed at various times: when a subscriber is addressing a message, when subscribers are being added to public or private distribution lists, when callers reach the opening greeting for your company, or when an outside caller is looking for a subscriber in the directory. By default, Cisco Unity limits searches to the local server that a call originates on. If your servers are attached to a networked phone system, you will probably identify the primary location object of each server as being part of a dialing domain. If you limit searches to the dialing domain, an outside caller or subscriber will be able to find subscribers in the domain, no matter which server they are on. A caller can then be transferred to the extension of the subscriber regardless of which Cisco Unity server initially took the call. The widest possible scope is to allow people to search the entire global address list (GAL). There may be good reasons for allowing searches of your global address list—the needs of your customers will guide you.

Dialing Domains

This topic defines the concept of dialing domains in Cisco Unity.



In a networked phone system, subscribers can dial each other without having to use a trunk access code or standard prefix (total of seven digits). Within a networked phone system, all extensions must be unique. If a company has several Cisco Unity servers with some attached to a networked phone system and others attached to separate phone systems, the networked phone systems and the separate systems may have an overlapping dial plan with no ill effects, with the exception of how the users address messages. Dialing domains in Cisco Unity working with a networked phone system allow for several dialing domain features to be simultaneously implemented.

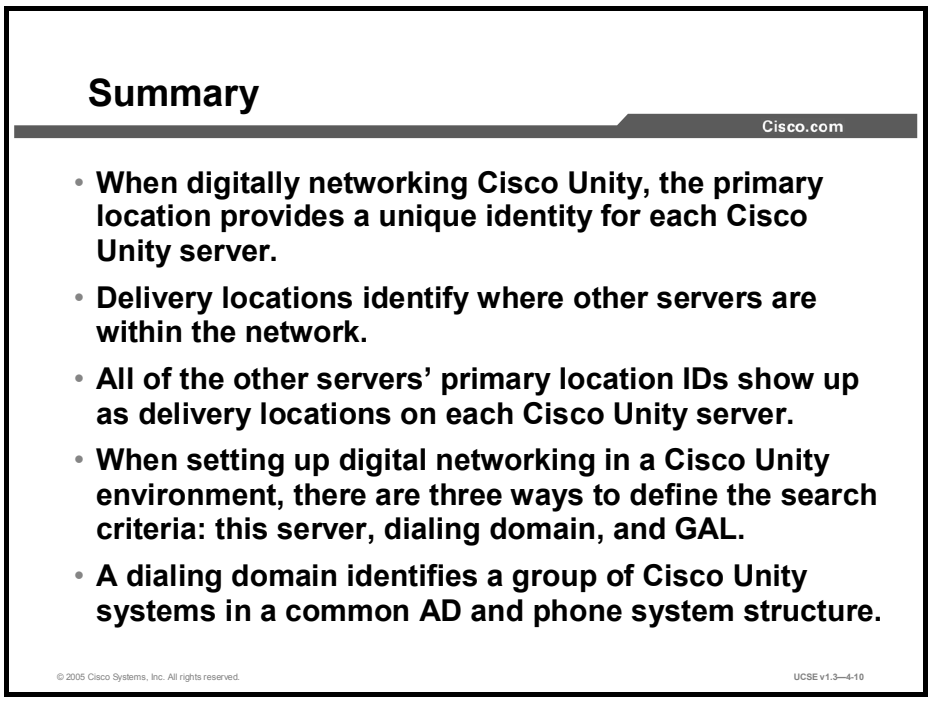


Subscribers can address messages directly to subscribers residing on other Cisco Unity systems. If alternate extensions are implemented, the alternate extension number may be the same number they use to reach the subscriber directly by telephone. Subscribers on any Cisco Unity server within the dialing domain can be added to public or private distribution lists. Outside callers dialing in to any Cisco Unity server in the dialing domain can look up any subscriber in the directory and be transferred to that subscriber, assuming that the search scope has been expanded to include the dialing domain.

Identified subscriber messaging will not work across dialing domains. If a subscriber calls another subscriber on a networked phone system and the call is passed to Cisco Unity by the phone system, the calling subscriber extension ID is not forwarded, and the call is treated as one from an outside caller.

Summary

This topic summarizes the key points in this lesson.



References

For additional information, refer to these resources:

- *Networking In Cisco Unity Guide (With IBM Lotus Domino)*
- *Networking In Cisco Unity Guide (With Microsoft Exchange)*

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) What is the primary location used for?

A) to identify the remote endpoint Cisco Unity server
B) to identify both the remote and local Cisco Unity server endpoints
C) to identify the path between the Cisco Unity server endpoints
D) to identify the local Cisco Unity server endpoint

Q2) When implementing digital networking in an Exchange 5.5 environment, which is a true statement? (Choose two.)

A) All Exchange servers have to be in the same site.
B) All Exchange servers have to be in the same organization.
C) All Exchange servers must run a directory connector.
D) All Exchange servers must run a directory replication connector.

Q3) Which steps are first and second when setting up digital networking. (Choose two.)

A) Make dial plan decisions.
B) Customize primary location object.
C) Set search options.
D) Add alternate extensions (optional).
E) Set up automated attendant transfers (optional).

Q4) The widest possible search scope is to allow people to search the entire _____.

A) server dialing domain
B) local server
C) global address list
D) Active Directory domain

Q5) Which item explains what a Cisco Unity dialing domain is?

A) a set of Exchange servers
B) all servers in a domain
C) a grouping scheme of Cisco Unity servers
D) a collection of Cisco CallManager and Cisco Unity servers

Quiz Answer Key

Q1) D

Relates to: Locations and Digital Networking

Q2) A, B

Relates to: Implementing Digital Networking

Q3) A, B

Relates to: Setting Up Digital Networking

Q4) C

Relates to: Search Options

Q5) C

Relates to: Dialing Domains

Lesson 5

Using SMTP Networking for Interoperability

Overview

With Simple Mail Transfer Protocol (SMTP) networking in Cisco Unity, subscribers on a local server can send voice messages to people who do not have mailboxes on the local Exchange network. These could be Cisco Unity subscribers who access a different directory on the messaging system, or individuals who have a messaging account on a computer connected to the Internet.

Relevance

Cisco Unity subscriber messaging needs extend beyond the range of subscribers on the local system. SMTP networking allows you to extend the reach of subscriber voice messaging to any messaging system available on the Internet. A system engineer must understand SMTP networking in order to integrate Cisco Unity subscribers who access a different messaging system directory or who access their messaging account via the Internet.

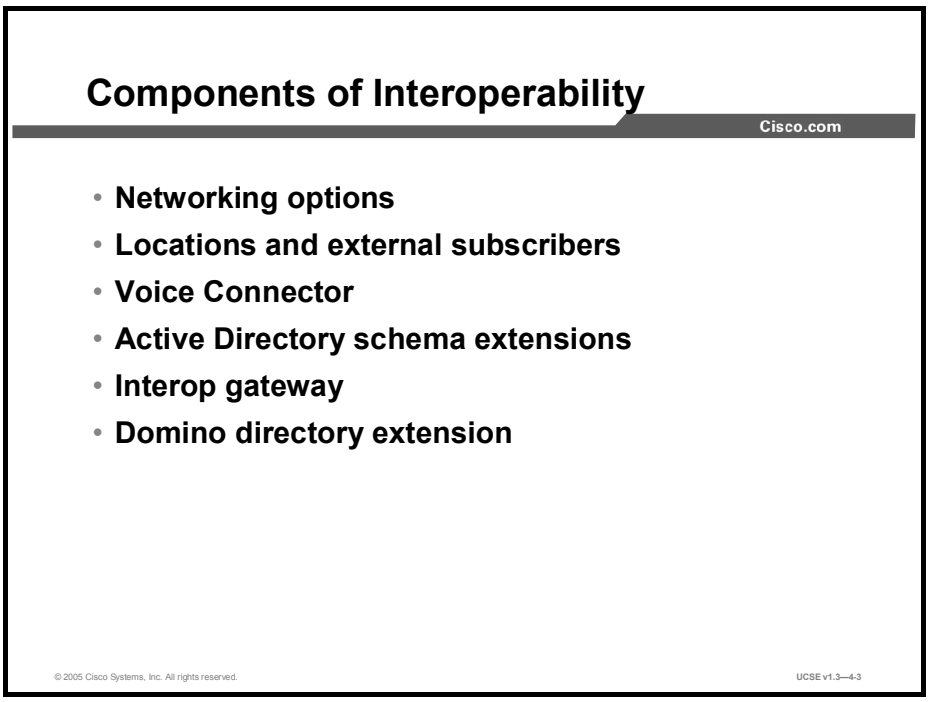
Objectives

Upon completing this lesson, you will be able to describe the requirements for interoperability and the basic steps needed to configure SMTP networking. This ability includes being able to meet these objectives:

- Describe the four components of interoperability needed to set up networking
- Describe how Cisco Unity uses SMTP networking to deliver messages
- Describe the general procedural steps for setting up SMTP networking
- Describe the use of primary and delivery locations in SMTP networking
- Describe how the Cisco Unity Voice Connector works in SMTP networking
- Describe how messages are transferred in an SMTP network
- Describe options available and setup procedures for SMTP subscribers

Components of Interoperability

This topic describes the four components of interoperability needed to set up networking.



To set up networking in Cisco Unity, you must consider the following components of interoperability:

- **Networking options:** The main goal of networking in Cisco Unity is to deliver messages from a Cisco Unity server to a target, and from the target to Cisco Unity. The networking options available in Cisco Unity are defined according to a combination of the message transport mechanism and the target server. Regardless of which networking option you choose, the setup process is similar.

  For each networking option, you customize the settings for the primary location. Each Cisco Unity server has a default or primary location, which is created during installation and which cannot be deleted. The primary location contains information that identifies the Cisco Unity server to other messaging systems—which may or may not be Cisco Unity systems.

  For all networking options except digital networking, you create delivery locations. A delivery location contains the network information that Cisco Unity needs to send messages to other messaging servers—which may or may not be Cisco Unity servers. You create a delivery location for each voice messaging server with which the local Cisco Unity server will communicate.

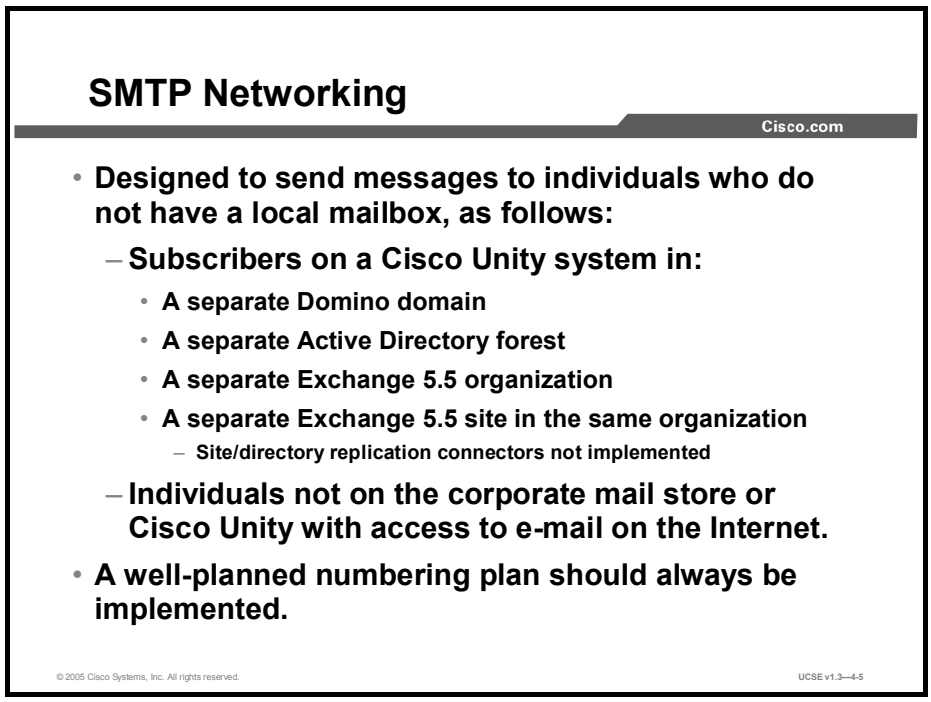
- **Locations and external subscribers:** For all networking options except digital networking, you may need to create external subscribers (that is, Internet, Audio Messaging Interchange Specification [AMIS], Bridge, or Voice Profile for Internet Mail [VPIM] subscribers). The messages for external subscribers are stored externally to the Cisco Unity voice message store. When creating external subscribers, you supply addressing information so that Cisco Unity can send messages to them. For example, when creating an Internet subscriber, you supply the subscriber e-mail address; messages are sent to that e-mail address instead of to an Exchange mailbox on the local network.
- **Voice Connector:** The Cisco Unity Voice Connector for Exchange is a Cisco Unity networking component that enables messaging between the following:
  - Cisco Unity servers that access separate directories (referred to as SMTP networking)
  - Cisco Unity servers and other voice messaging systems

  There are two voice connectors, as follows:
  - **Voice Connector for Exchange 5.5:** When your network consists only of Exchange 5.5 servers, use the Voice Connector for Exchange 5.5.
  - **Voice Connector for Exchange 2000:** When your network consists only of Exchange 2000 or Exchange 2003 servers, or a mixture of Exchange 2000 or Exchange 2003 servers and Exchange 5.5 servers, use Voice Connector for Exchange 2000.
- **Active Directory schema extensions:** When Cisco Unity is installed in a network that consists only of Exchange 2000 or Exchange 2003 servers or in a mixed-mode environment with both Exchange 2000 or Exchange 2003 servers and Exchange 5.5 servers, a small subset of Cisco Unity data is stored in Active Directory. Therefore, before installing Cisco Unity, the Active Directory schema must be extended. In addition to the schema extensions required before installing Cisco Unity, the Active Directory schema must be extended before setting up Bridge networking and VPIM networking.

  The schema extensions needed to support digital networking and AMIS networking are part of the general set of schema extensions for Cisco Unity.
- **Interop Gateway:** The Cisco Unity Interop Gateway is a Cisco Unity networking component that enables messaging between the following:
  - Cisco Unity servers that access separate directories (referred to as SMTP networking)
  - Cisco Unity servers and other messaging systems
- **Domino Names.nsf file modification:** When Cisco Unity is installed in a network that consists of Domino mail stores, a small subset of Cisco Unity data is stored in the Domino database, commonly referred to as the Names.nsf file. Therefore, before installing Cisco Unity, the Domino Names.nsf file must be modified with software from IBM that includes an application called CSServer. Running this software application on the all Domino servers that will have unified messaging users homed on them will create the fields for the Cisco Unity data.

SMTP Networking

This topic describes how Cisco Unity uses SMTP networking to deliver messages.



SMTP is designed to send mail to receiving servers that are always on line. Because it is not convenient (and possibly not affordable) to be connected to the network at all times, Post Office Protocol Version 3 (POP3) and Internet Message Access Protocol (IMAP) were developed. POP3 allows users to dial up and collect their mail from a point of presence, typically an Internet service provider (ISP). IMAP allows for the same dial-up collection of mail, but is even more conservative of bandwidth, only initially downloading the headers of messages. In simpler terms, SMTP is used to send, and POP3 and IMAP are used to receive. However, if the sender and receiver are always on line, they only need SMTP.

In Exchange 5.5, the Internet Mail Service (IMS) connector provides Internet mail services using the SMTP, IMAP4, and POP3 protocols. The IMS connector is installed and configured through the Exchange Administrator and requires a Domain Name System (DNS) server in order to properly perform name resolution of fully qualified domain names (FQDNs) for delivery of messages. An FQDN is a name that follows the pattern of recipient@domain.com. When an Exchange user is created, an SMTP address is automatically generated using the Exchange alias of the recipient followed by *site.organization.com*, where *site* and *organization* correspond to the site and organization names of the Exchange server. Most administrators use the Exchange Administrator tool to modify the site addressing to *organization.com* (removing the site name) to allow for easier addressing when sending SMTP mail. Additionally, you may modify the *.com* extension as necessary, based on your particular naming requirements. Common examples include *.edu*, *.org*, and *.gov*.

The IMS (or gateway) allows you to send electronic mail to users on both Exchange and non-Exchange mail servers. The IMS queries the DNS server to determine the name of the server responsible for accepting mail for the recipient domain, connects to that server, and delivers the mail.

Exchange 2000/2003 uses SMTP explicitly. When Windows Internet Information Services (IIS) is installed, SMTP is one of the services that is installed with it. Exchange 2000 uses SMTP as its message transport mechanism. Even if it is not configured in Exchange, it is still used for the transfer of mail. The SMTP connector in Exchange adds functionality and manageability to SMTP. You can define routes for SMTP traffic, relay messages to specific domains, and configure inbound and outbound security.

DNS is critical to the correct functioning of Active Directory and Exchange. You must have a well-designed, reliable DNS implementation if you want to have a reliable and efficient Windows or Exchange messaging system.

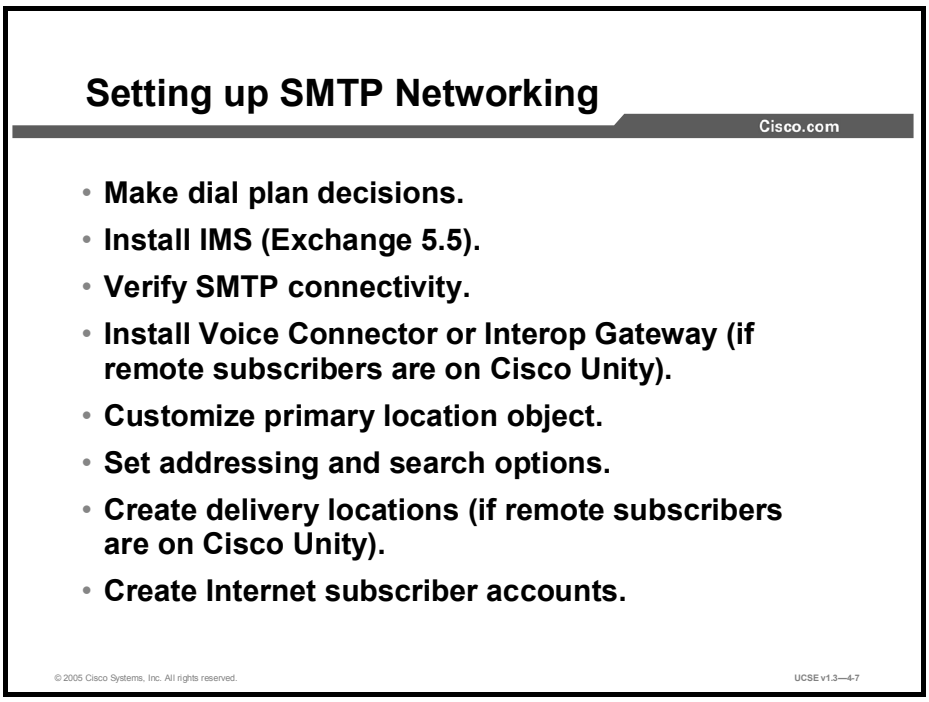
Cisco Unity uses the standard SMTP connector in Microsoft Exchange 2000/2003 (the IMS in Exchange 5.5) to provide messaging among Cisco Unity servers that are not on the same directory and to individuals who are not using Cisco Unity as their messaging server. The SMTP connector provides the ability to send and receive messages through the Internet to computers supporting SMTP. This means that both Exchange and non-Exchange servers can receive messages from Cisco Unity.

While SMTP provides distinct advantages for sending electronic mail over the Internet, it does have several possible disadvantages. Voice mail will lose its Cisco Unity-specific attributes when traveling to a non-Cisco Unity system and will appear as regular e-mail with an attached WAV file. Additionally, message recipients not in your Exchange organization require special procedures to be entered in the Exchange directory. Specifically, they must be created manually as either custom recipients on the Exchange server or as address book entries in the personal address books on local e-mail clients such as Outlook. Fortunately, Cisco Unity has several methods for addressing these SMTP concerns.

If SMTP networking is used in conjunction with the Voice Connector, the Cisco Unity-specific attributes of a voice mail will be retained as that message is prepared for transmission across the Internet. The Voice Connector registers with Exchange to handle messages of type VOICE. When a VOICE message is sent, Exchange hands it off to the Voice Connector, which packages the message as a Multipurpose Internet Mail Extension (MIME) message that contains all of the information within it to be restored as a voice message at the receiving system. If the receiving system is another Cisco Unity system with a Voice Connector installed, the message is handed off to the Voice Connector. The message is delivered to the target subscriber with the voice message qualities intact: a Message Waiting Indicator (MWI) lamp is lit, and the message is ready for pickup over the phone or at the desktop. If no Voice Connector is available, the message is treated as an e-mail with a WAV file attachment.

Setting up SMTP Networking

This topic describes the general procedural steps for setting up SMTP networking.



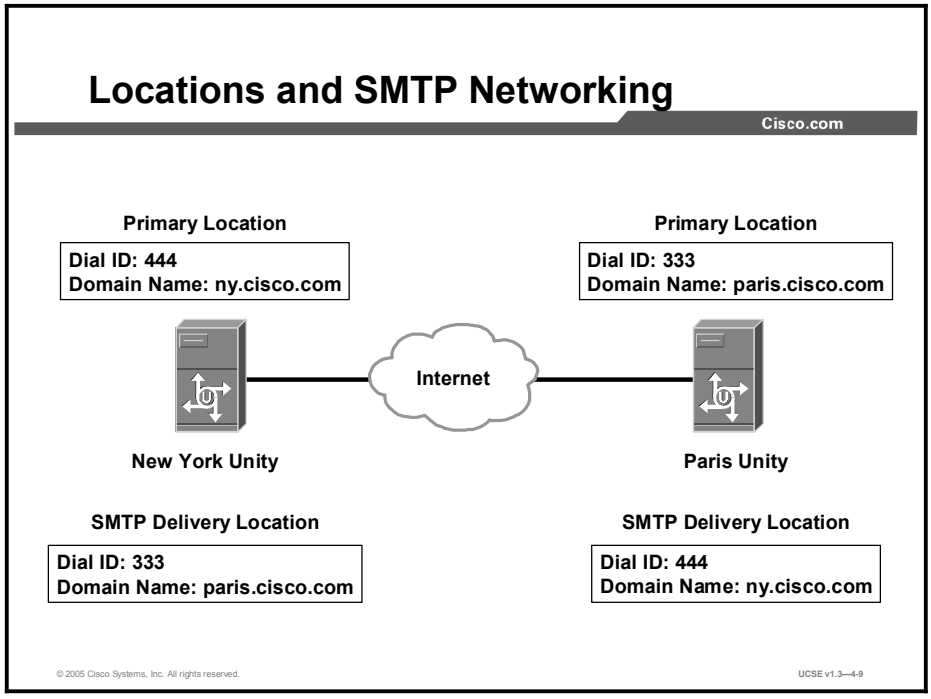
Many of the steps necessary for SMTP networking are similar to the steps for digital networking, with the addition of the installation of the Voice Connector. To set up SMTP networking between remote Cisco Unity servers, the following steps must be implemented on both systems:

- **Make dial plan decisions:** Making dial plan decisions before implementing the system will result in an installation that has no conflicting IDs to confuse those searching for subscriber addresses.
- **Install IMS:** If you are implementing SMTP networking in an Exchange 5.5 environment, you will have to explicitly install the IMS, because this is not done by default.
- **Verify SMTP connectivity:** In Exchange 2000, SMTP is the default message transport mechanism, so there is no need to install it there.
- **Install the Interop Gateway:** Once you have verified connectivity, you can install the Interop Gateway, if some or all of the remote sites are using Cisco Unity. You should have only one installation of the Interop Gateway in a Domino domain.
- **Install Voice Connector:** Once you have verified connectivity, you can install the Voice Connector if some or all of the remote sites are using Cisco Unity. You should have only one installation of the Voice Connector in an Exchange 5.5 site or AD forest. If a previous version was installed, you must uninstall it before continuing.

- **Customize primary location object:** After installation of the current Voice Connector, you customize the primary location object on the Cisco Unity server by entering a meaningful name, giving it a Dial ID, recording a voice name, and, if appropriate, making it a member of a dialing domain. If you are a part of the dialing domain, the name for the domain only needs to be entered on one server. After replication, any server in the domain can pick the dialing domain name from a drop-down list. Next, enter the SMTP domain name. If multiple Cisco Unity servers are using digital networking, the primary location on all servers, particularly the SMTP domain name, must be configured. Otherwise, SMTP networking will not work for the subscribers on other Cisco Unity servers.
- **Set addressing and search options:** Setting addressing and search options involves the same set of considerations as in digital networking.
- **Create delivery locations:** If some or all of the remote messaging recipients are on Cisco Unity servers, you should create delivery locations for each of those servers. When you have multiple Cisco Unity servers networked together, it is only necessary to create those delivery locations on one server in the network. The directory holds the location data, and it will be available to all who can access the directory.
- **Create Internet subscriber accounts:** Creating Internet subscribers is the last task necessary for setting up SMTP networking.

Locations and SMTP Networking

This topic describes the use of primary and delivery locations in SMTP networking.



Location objects are key items in digital networking. When you install Cisco Unity, a single default location referred to as the primary location object is created. As subscribers are added to Cisco Unity, they become members of this default location. The Cisco Unity Administrator allows you to create additional location objects that represent other messaging servers, including Cisco Unity. If you are in the same Active Directory forest, there is no need to create additional locations, because location objects will be available as default objects on their home system. Location objects can be tied together using a property called the dialing domain ID, which allows you to create a meta-location that spans multiple Cisco Unity servers by assigning them all the same dialing domain ID. The dialing domain ID allows you to easily span sites or other networking boundaries, and to provide transparent dialing capabilities to customers that have networked telephone switches.

In the previous figure, the location objects are not in the same Active Directory forest. The location object for each Cisco Unity server identifies it to other servers as they exchange voice mails back and forth across the internet.

Recorded object data for the location object includes the following:

- A voice name for addressing
- A display name for the administrative console
- Three dual tone multifrequency (DTMF) names (one for each keypad mapping)
- A DTMF ID for addressing
- An SMTP address for blind addressing
- A destination type

- A send blind flag
- Information about the keypad mapping used at that location.

In Cisco Unity, subscribers and any other system objects can only be associated with the primary location object created by the setup program. All other location objects are used solely for addressing purposes.

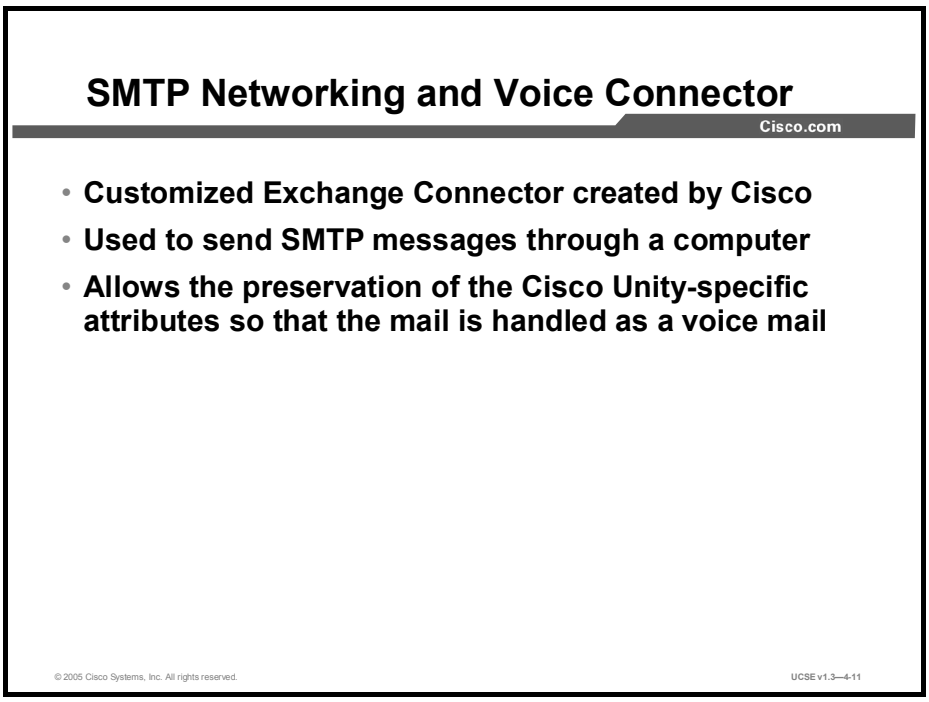
When outside callers use the Cisco Unity directory, they are presented with a list of names that includes members of the primary location object. Directory search options can be configured so that all other administrator-created locations are available to all callers. Users associated with any location object other than the default object may be added to public and private distribution lists or added to message address lists by subscribers only.

When defining the primary location object, you give it a Dial ID. Creating a dial plan for your organization that will result in callers reaching subscribers correctly and efficiently is very important. The Dial IDs that you create are an important part of that dial plan. Be sure that they do not conflict with previously assigned IDs.

In the Cisco Unity Administrator, all location objects will be visible, but administrators will only be able to edit or delete location objects created on their Cisco Unity system. Location objects that replicate from other sites will be read-only. The original location object that is installed with the system (the primary location object) can be edited but not deleted from the system.

SMTP Networking and the Voice Connector

This topic describes how the Cisco Unity Voice Connector works in SMTP networking.



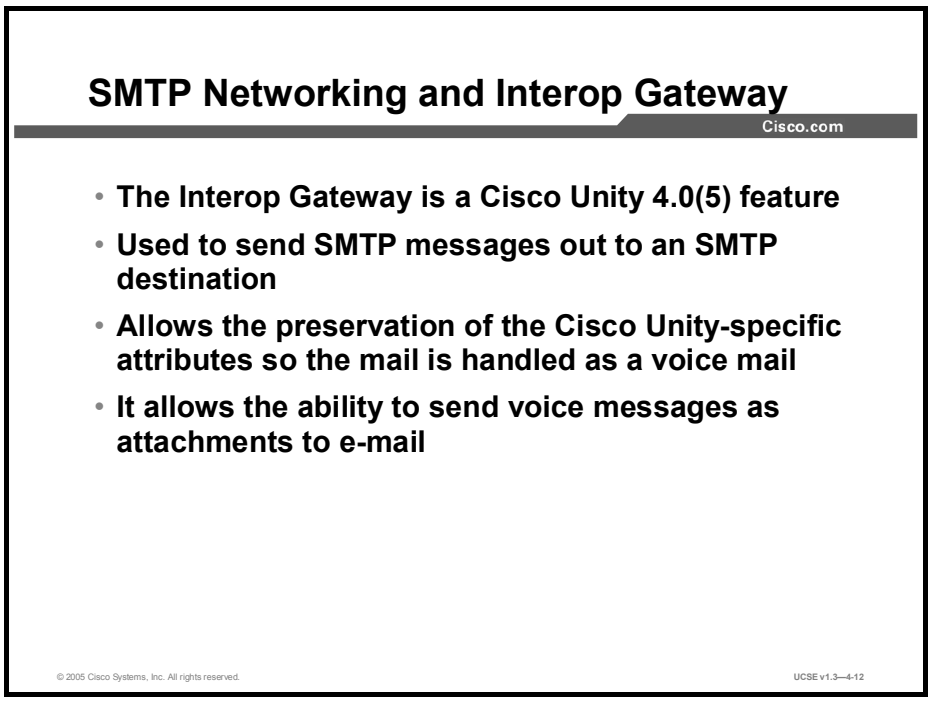
Cisco Unity makes use of the standard Exchange SMTP Connector to provide messaging among Cisco Unity servers that access separate directories, and to individuals who do not use Cisco Unity. In Exchange 5.5, the SMTP Connector is called the Internet Mail Service.

The SMTP Connector provides the ability to send and receive messages through the Internet to computers that support SMTP, which means that messages can be sent to both Exchange and non-Exchange mail servers. The Cisco Unity Voice Connector allows Cisco Unity systems to send and receive SMTP mail while preserving the Cisco Unity-specific attributes in the voice messages. These attributes allow Cisco Unity to handle messages as voice messages.

The Voice Connector is registered with Exchange to handle messages with the VOICE address type, so all messages to remote recipients must have VOICE in the address. When a subscriber sends a voice message to someone at another location, the Voice Connector converts the voice message to Multipurpose Internet Mail Extension (MIME) format. The Exchange SMTP Connector can then send the message with all associated information. On the receiving Cisco Unity server, because the message address type is VOICE, Exchange gives the message to the Voice Connector to handle. The Voice Connector converts the MIME message back to a voice message. When the message is delivered to the recipient Exchange mailbox, it is identified as a voice message, and Cisco Unity lights the MWI lamp on the recipient phone. The recipient can access the message just like any other voice message, by using the phone, ViewMail for Microsoft Outlook, or the Cisco Unity Inbox.

SMTP Networking and the Interop Gateway

This topic describes how the Cisco Unity Interop Gateway works in SMTP networking.



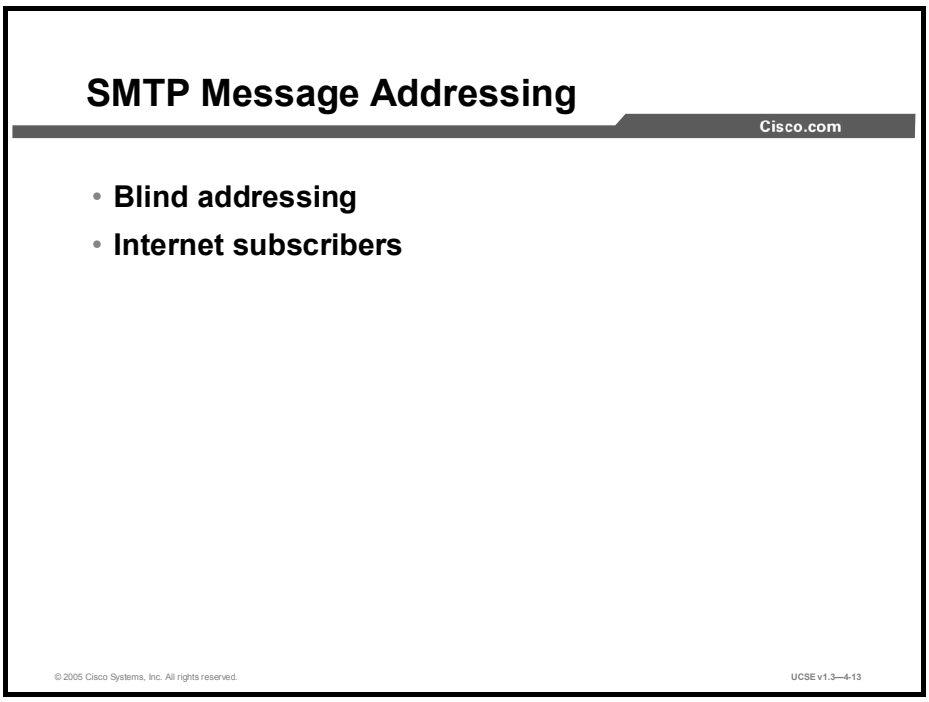
Cisco Unity makes use of the standard Domino SMTP Connector to provide messaging among Cisco Unity servers that are in different Domino domains, and to individuals who do not use Cisco Unity. In Domino, there will be connection documents in place that will control how SMTP messages are sent and received.

The Interop Gateway provides the ability to send and receive messages through the Internet to computers that support SMTP, which means that messages can be sent to both Domino and non-Domino mail servers. The Cisco Unity Voice Connector allows Cisco Unity systems to send and receive SMTP mail while preserving the Cisco Unity-specific attributes in the voice messages. These attributes allow Cisco Unity to handle messages as voice messages.

The Interop Gateway is a service that runs on the Cisco Unity server. When a subscriber sends a voice message to someone at another location, the Interop Gateway converts the voice message to MIME format. The Domino SMTP Connector can then send the message with all associated information. On the receiving Cisco Unity server, the process is done in reverse so that the MIME message being received over the SMTP Connecter is converted back to the voice message format that Cisco Unity will see as a new voice mail, and Cisco Unity will light the lamp on the recipient phone. The recipient can access the message just like any other voice message by using the phone, ViewMail for Notes, or the Cisco Unity Inbox.

SMTP Message Addressing

This topic describes how messages are transferred in an SMTP network.

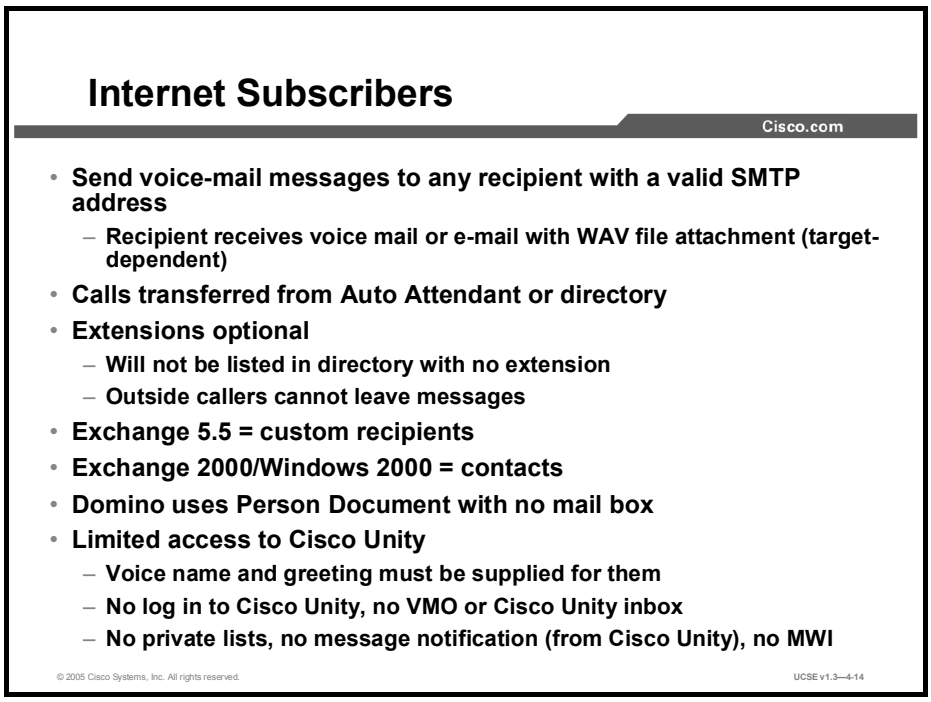


Cisco Unity provides the following two methods for addressing messages to subscribers and to others who do not have mailboxes on the local Exchange network:

- **Blind addressing:** Allows subscribers on the local Cisco Unity server to send messages to subscribers on a remote Cisco Unity server, even though the recipient extension, name, and recorded name are not in the directory. Even though Cisco Unity cannot provide voice name confirmation (thus the term “blind addressing”), the message is addressed and sent. The subscribers on the remote Cisco Unity server receive voice messages.
- **Internet subscribers:** Allows messaging to recipients on computers that may or may not be using Cisco Unity. Subscribers on the local Cisco Unity server address messages to Internet subscribers the same way that they address messages to regular subscribers—by extension or spelled name.

Internet Subscribers

This topic describes options available and setup procedures for Internet subscribers.



Internet subscribers are special types of Cisco Unity voice-mail users who do not have a local message store but instead send and receive messages by using an Internet Mail Service (SMTP gateway). When you add a new subscriber in the Cisco Unity Administrator, a radio button option allows you to create an Internet Subscriber (Mailbox) and specify an SMTP address for that user. In Exchange 5.5, a new subscriber is called an Exchange custom recipient, and in Windows 2000/Exchange 2000, a new subscriber is called a mail-enabled contact. In Domino, the Internet subscriber is a person document without a mailbox. The SMTP subscriber is actually a pointer to a mailbox, but there is no local mail box or message store.

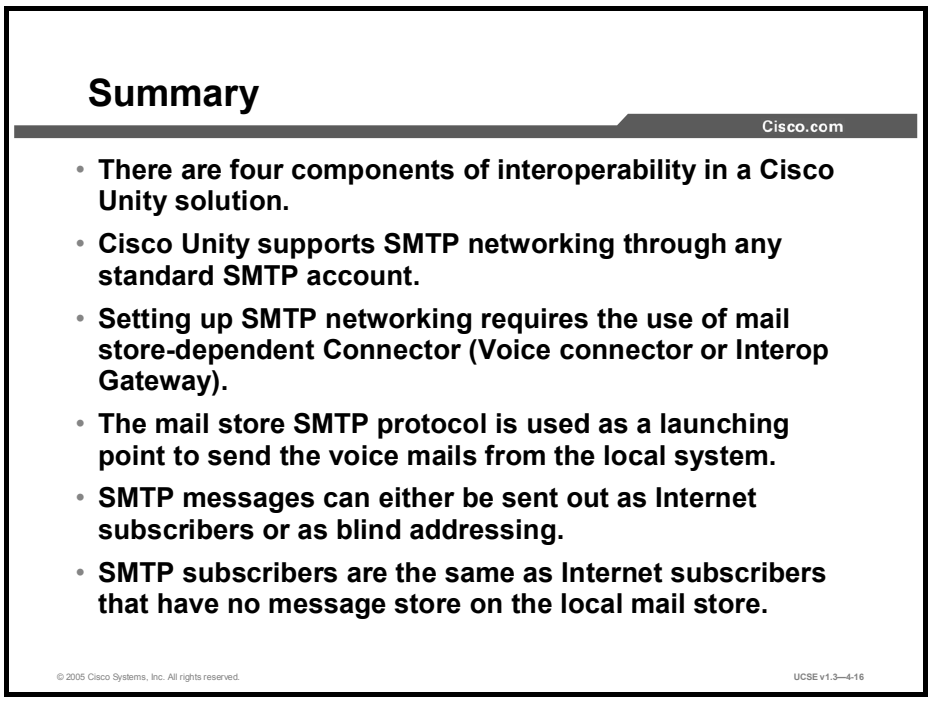
When creating an SMTP subscriber, setup options relating to the local message store, such as phone password, private lists, conversation, and message notification, are not available. In other words, the mailbox acts as a pointer to the SMTP address you specify when you create the SMTP subscriber account. Both outside and internal callers benefit from the ability to address messages to the subscriber over the telephone in most cases, and internal users also have an option to address to them using the global address list (GAL) or Names & Address Book (NAB). The SMTP subscriber has a recorded voice name and greeting just like any other Cisco Unity subscriber; the difference is that the administrator must record the name and greeting, as SMTP subscribers do not have access to Cisco Unity via the Telephone User Interface (TUI) or Cisco Personal Communications Assistant (CPCA). The main difference between a regular Cisco Unity subscriber and an SMTP subscriber is that when mail is left for SMTP subscribers, the mail is delivered out the SMTP gateway (IMS) to its Internet destination as specified within their account. The end location could be any other mail server or even another voice-mail system, and therefore allows offsite users (such as field technicians or outside sales personnel) to look and feel to the sender as if that recipient was actually on site.

Additionally, you can use SMTP subscribers to link offices without the need to set up messaging connectors and directory replication connectors between sites. However, the administrator must manually and individually set up SMTP subscribers for each destination location. This may be unacceptable where a large number of users exist in remote offices. For organizations with many users in various locations, blind addressing is typically a better choice than SMTP subscribers.

If remote subscribers are not on a Cisco Unity system, a voice-mail message sent to them will appear as an e-mail with a WAV file attachment.

Summary

This topic summarizes the key points discussed in this lesson.



References

For additional information, refer to these resources:

- *Networking in Cisco Unity Guide (With Microsoft Exchange)*
- *Networking in Cisco Unity Guide (With IBM Domino)*

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) Which item is a goal of Cisco networking?

A) to deliver messages
B) to extend the network
C) to remove subscribers
D) to add call handlers

Q2) The three types of Voice Connector are for which mail stores? (Choose two.)

A) IBM Domino
B) Exchange 2000
C) Cisco Unity
D) IBM Voice net

Q3) Most administrators use which program to create a user?

A) Cisco Unity
B) Linux
C) Exchange
D) Cisco CallManager
E) ADUC

Q4) The IMS service is also known as a _____.

A) device pool
B) CCS
C) gateway
D) route point

Q5) How many Voice Connecters can you have for Interop per Active Directory?

A) 1
B) 2
C) 3
D) 4

Q6) If a domain name is not configured, which item will not work?

A) Cisco CallManager on the same Cisco Unity server
B) Cisco CallManager on a different Cisco Unity server
C) redundant Cisco CallManagers on the same Cisco Unity server
D) receiving messages from remote redundant Cisco CallManagers
E) redundant Cisco CallManagers on a different Cisco Unity server

Q7) Location objects in Cisco Unity are used for which purpose?

A) addressing purposes
B) spares
C) Cisco CallManager use
D) Cisco Unity use

Q8) Who can edit or delete the location objects that are created by Cisco Unity?

A) administrators
B) administrators who created location
C) any local administrator
D) no one

Q9) What is the SMTP connector called in Exchange 5.5?

A) Internet Mail Service
B) IVS
C) SMPT Connector
D) Voice Connector

Q10) When a message is addressed to a remote Cisco Unity subscriber, the message will pass through which program?

A) Voice Exchange
B) Voice Connector
C) Exchange
D) Cisco Unity server

Q11) How many methods of addressing messages to subscribers does Cisco Unity have?

A) 1
B) 2
C) 3
D) 4

Q12) What are the two main differences between a regular Cisco Unity subscriber and an Internet subscriber? (Choose two.)

A) Mail is left for Internet subscribers.
B) The mail is delivered out the SMTP gateway (IMS) to its Internet destination as specified within an Internet subscriber account.
C) Mail is left on the Cisco Unity server.
D) Mail is deleted.

Q13) For organizations with many users in various non-replicating locations, which addressing works best?

A) blind addressing
B) Internet subscribers
C) Cisco Unity users
D) Bridge users

Quiz Answer Key

Q1) A

Relates to: Components of Interoperability

Q2) A, B

Relates to: Components of Interoperability

Q3) C

Relates to: SMTP Networking

Q4) C

Relates to: Components of Interoperability

Q5) A

Relates to: SMTP Networking and the Voice Connector

Q6) D

Relates to: Locations and SMTP Networking

Q7) A

Relates to: Locations and SMTP Networking

Q8) A

Relates to: Locations and SMTP Networking

Q9) A

Relates to: SMTP Networking and the Voice Connector

Q10) B

Relates to: SMTP Networking

Q11) B

Relates to: Setting up SMTP Networking

Q12) A, B

Relates to: Internet Subscribers

Q13) A

Relates to: SMTP Message Addressing

Lesson 6

Using VPIM Networking

Overview

Voice Profile for Internet Mail (VPIM) networking in Cisco Unity allows different voice messaging systems to exchange voice, fax, and text messages over the Internet or any TCP/IP network. This lesson describes the concepts and procedures involved with VPIM networking.

Relevance

If the messaging target of any of your Cisco Unity subscribers resides on a VPIM-compliant voice-mail server, it is important that you know how to set up VPIM networking to allow that messaging to take place in a transparent (to the caller) manner.

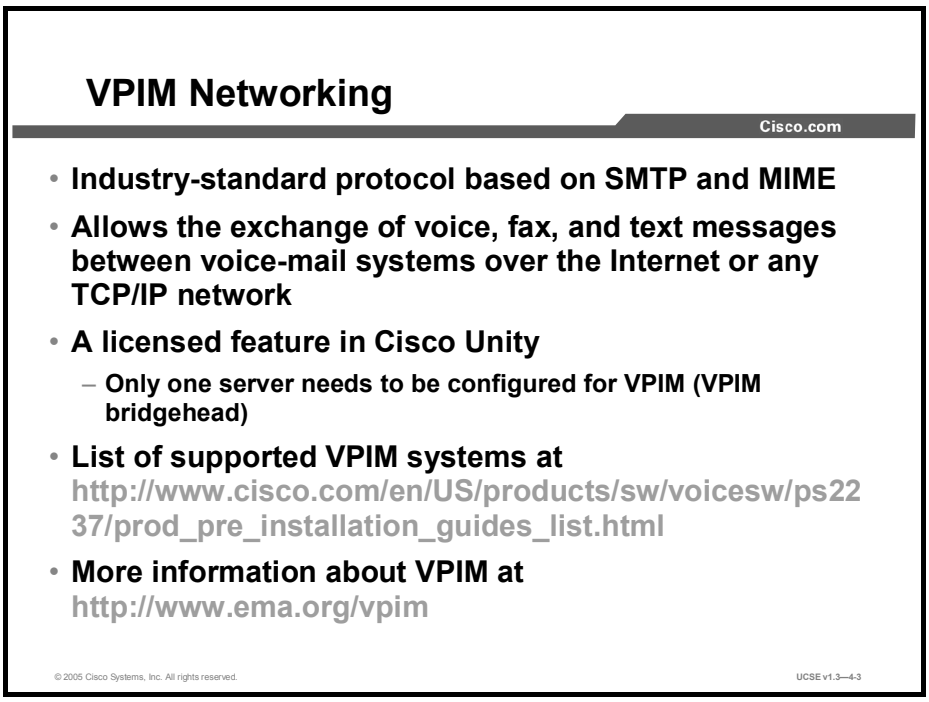
Objectives

Upon completing this lesson, you will be able to describe how Cisco Unity uses VPIM networking to deliver voice, fax, and text messages over the Internet. This ability includes being able to meet these objectives:

- Describe how Cisco Unity uses VPIM networking to deliver messages
- Describe the general procedural steps for setting up VPIM networking
- Describe the use of primary and delivery locations in VPIM networking
- Describe how the Cisco Unity Voice Connector works in VPIM networking
- Describe how messages are transferred in a VPIM network
- Describe options available and setup procedures for VPIM subscribers

VPIM Networking

This topic describes how Cisco Unity uses VPIM networking to deliver messages.



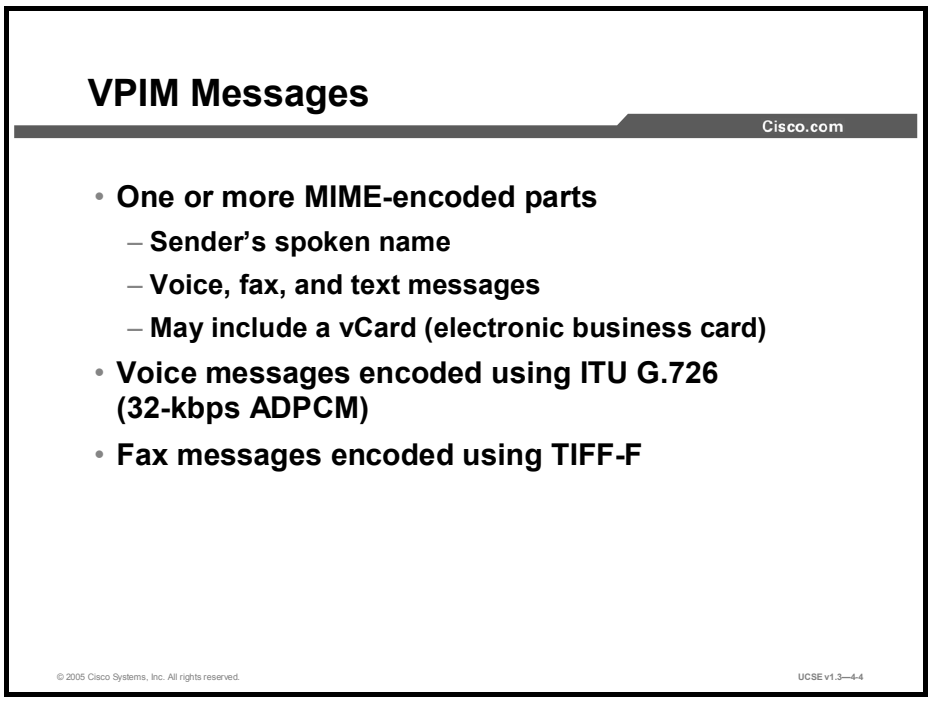
VPIM is a digital standard based on Simple Mail Transfer Protocol (SMTP) and the Multipurpose Internet Mail Extension (MIME) protocol. Voice, text, and fax messages are transferred digitally between target servers. VPIM networking may allow organizations to save long-distance toll charges on messages between target servers, because those messages are traveling over a TCP/IP network rather than more costly public switched telephone network (PSTN) lines. The VPIM specification defines the format of messages and message addresses as well as the protocol for message exchange between servers. VPIM does not specify which client applications can be used or how those client applications work with their individual servers, thereby allowing many different types of systems to support VPIM. More information about the VPIM standard is available at these websites:

- http://www.ema.org/vpim
- http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_pre_installation_guides_list.html

VPIM networking is a licensed feature of Cisco Unity. As such, only one server in an Exchange organization of multiple Cisco Unity systems (the VPIM bridgehead) needs to be licensed for use.

VPIM Messages

This topic describes the components and characteristics of VPIM messages.



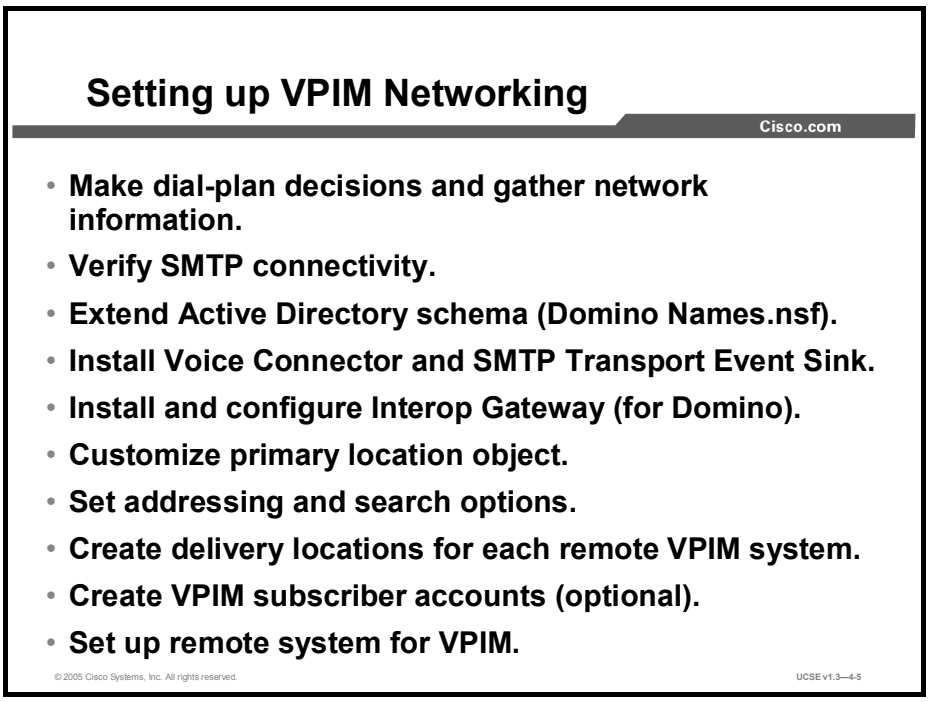
VPIM messages are made up of one or more MIME-encoded parts. These parts, in addition to the voice, fax, or text message, can include the spoken name of the sender and possibly a vCard, or electronic business card. In Cisco Unity, you can choose whether or not the spoken name and vCard are included in an outgoing message. If a spoken name is included in an incoming message, it is included as part of the message. If a vCard is included in an incoming message, it can be viewed in ViewMail for Outlook.

VPIM voice messages are encoded using the ITU G.726 adaptive differential pulse code modulation (ADPCM) standard, and fax messages are encoded using the TIFF-F standard.

When VPIM messages are addressed, they use information from the VPIM delivery location page to format the To: address, and from the VPIM location page and the primary location object page to format the From: address.

Setting up VPIM Networking

This topic describes the general procedural steps for setting up VPIM networking.



Many of the steps necessary for setting up VPIM networking are similar to the steps for setting up digital and SMTP networking, including the installation of the Voice Connector for Exchange or the Interop Gateway for Domino. The steps are as follows:

Step 1 Make dial-plan decisions before implementing the system, which will result in an installation that has no conflicting IDs to confuse those searching for subscriber addresses.

Step 2 Verify that there is SMTP connectivity between the target systems. Because VPIM uses SMTP and MIME to accomplish its tasks, SMTP connectivity is a foundation requirement.

Step 3 Extend the Active Directory schema to enable VPIM networking. The schema changes made are additions to the Cisco Unity location object class. A full description of the schema changes is listed in the file vpimgateway.ldf, located in the Schema\LdifScripts directory on Cisco Unity Disc 1.

Step 4 Install the Voice Connector on an Exchange 2000 server or the Interop Gateway for Domino on a Cisco Unity server. You should have only one installation of the Voice Connector in an Active Directory (AD) forest. If a previous version was installed, it must be uninstalled before continuing.

Step 5 While you are installing the Voice Connector, you will have the opportunity to install the SMTP Transport Event Sink. These should both be installed on the server that will receive incoming VPIM messages. If there is only one server in the organization that will be receiving VPIM messages, this will only need to be done once. Otherwise, install it on every server that accepts incoming VPIM messages.

Step 6 After installation of the current Voice Connector or Interop Gateway, customize the primary location object on the Cisco Unity server by entering a meaningful name, giving it a Dial ID, recording a voice name, entering the SMTP domain name, and, if appropriate, making it a member of a dialing domain. If you are a part of the dialing domain, the name for the domain only needs to be entered on one server. After replication, any server in the domain can pick the dialing domain name from a drop-down list.

Step 7 Enter the SMTP domain name. If multiple Cisco Unity servers are using digital networking, the primary location on all servers, particularly the SMTP domain name, must be configured. Otherwise SMTP networking will not work for the subscribers on other Cisco Unity servers.

Step 8 Set addressing and search options, using the same set of considerations as in digital networking.

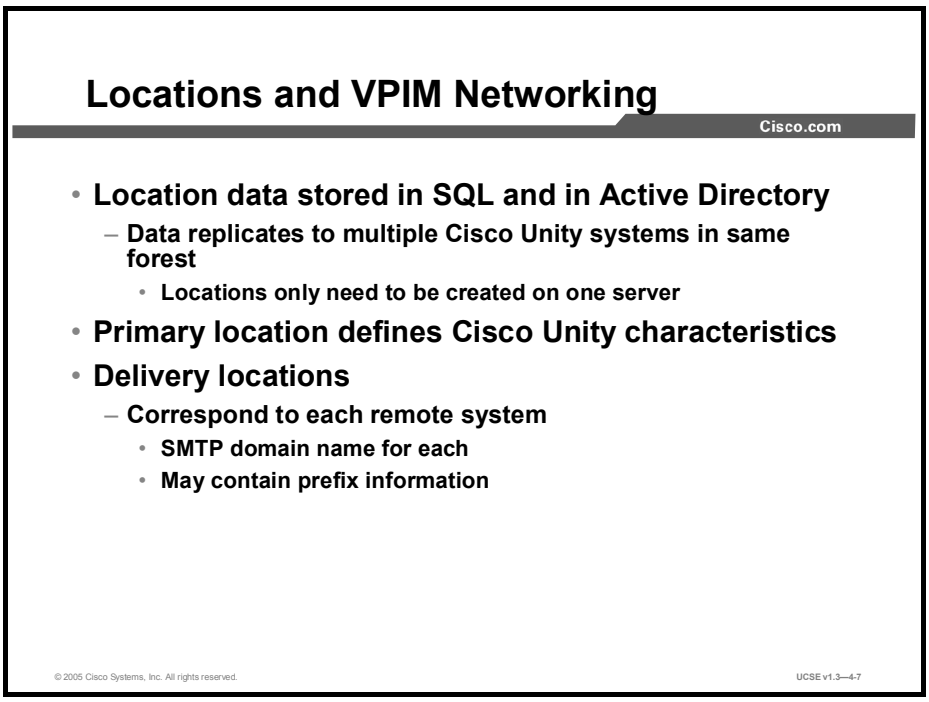
Step 9 Create a VPIM delivery location for each remote voice-messaging server to which subscribers send messages. When you have multiple Cisco Unity servers networked together, it is only necessary to create those delivery locations on one server in the network. The directory holds the location data, and it will be available to all who can access the directory.

Step 10 Create VPIM subscriber accounts for those persons you wish to be found from the corporate directory.

Step 11 Configure the remote system for VPIM.

Locations and VPIM Networking

This topic describes the use of primary and delivery locations in VPIM networking.



Location objects play a central role in VPIM networking. When you install Cisco Unity, a single default location, referred to as the primary location object (the default location object when Cisco Unity is first installed), is created. As subscribers are added to Cisco Unity, they become members of this location. The Cisco Unity Administrator allows you to create additional location objects that represent additional Cisco Unity servers. If you are in the same Active Directory forest, there is no need to create additional locations, as they will be available within minutes of their creation as a default object on their home system. Location objects can be tied together using a property called a dialing domain ID, which allows you to create a meta-location that spans multiple Cisco Unity servers by assigning them all the same dialing domain ID. This meta-location lets you easily span sites or other networking boundaries and provide transparent dialing capabilities to customers that have networked telephone switches.

Recorded object data for the location object includes the following:

- A voice name for addressing
- A display name for the administrative console
- Three dual tone multifrequency (DTMF) names (one for each keypad mapping)
- A DTMF ID for addressing
- An SMTP address for blind addressing
- A destination type
- A send blind flag
- Information about the keypad mapping used at that location.

In Cisco Unity, subscribers and any other system objects can only be associated with the primary location object created by the setup program. All delivery location objects are used solely for addressing purposes. An administrator creates delivery location objects for each remote messaging system that Cisco Unity will communicate with. Delivery location objects usually contain the SMTP domain name of the server and may contain other information.

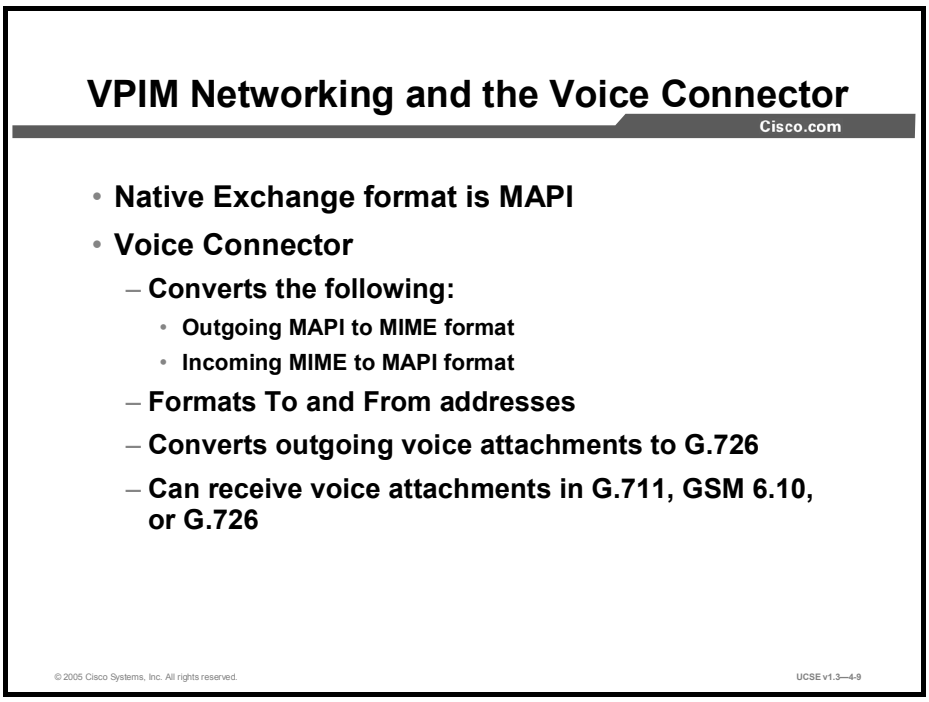
When outside callers use the Cisco Unity directory, they are presented with a list of names that includes members of the primary location object. Directory search options can be configured so that all other administrator-created delivery locations are available to all callers. Users associated with any location object other than the default object may be added to public and private distribution lists or added to message address lists by subscribers only.

When defining the primary location object, you give it a Dial ID. Creating a dial plan for your organization that will result in callers reaching subscribers correctly and efficiently is very important. The Dial IDs that you create are an important part of that dial plan. Be sure that they do not conflict with previously assigned IDs.

In the Cisco Unity Administrator, all location objects will be visible, but administrators will only be able to edit or delete location objects that were created on their Cisco Unity system. Location objects that replicate from other sites will be read-only. The original location object that is installed with the system (the primary location object) can be edited but not deleted from the system.

VPIM Networking and the Voice Connector

This topic describes how the Cisco Unity Voice Connector works in VPIM networking.

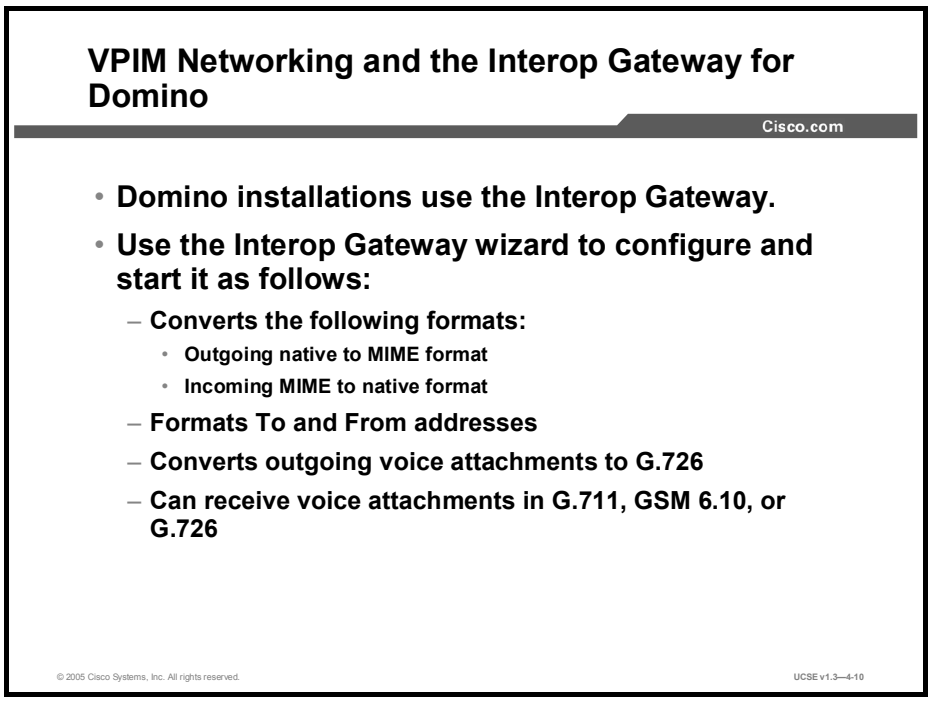


Cisco Unity uses Exchange 2000, a VPIM-compliant messaging system, to provide message transport between itself and other VPIM-compliant voice messaging systems. When a message bound for a VPIM recipient is passed to the Voice Connector (because it is registered with Exchange 2000 to handle VPIM messages), it first converts the message from the Exchange native Messaging Application Programming Interface (MAPI) format to MIME. It then formats the To: field with the domain name and prefix specified on the correct VPIM delivery location page. It formats the From: field with a prefix from the correct delivery location page and the domain name of the primary location page. Outgoing voice messages are converted to G.726 format and then a recorded voice name and vCard, if specified, are attached. The message is then put in the SMTP pickup folder for delivery.

Incoming messages are first noticed by the event sink and readdressed to the Voice Connector by the event sink. Once the Voice Connector receives the message, it first verifies that the message has come from a known VPIM delivery location. If no match is made, the message is rejected and a non-delivery receipt (NDR) is sent to the originator of the message. If a matching delivery location is found, the Voice Connector removes the prefixes in the To: and From: addresses, validates the recipient(s) of the message, formats the addresses, and converts the message from MIME to MAPI. Any voice attachments are converted into the audio format specified on the delivery location page, and the message is handed back to Exchange for delivery to the subscriber mailbox.

VPIM Networking and the Interop Gateway

This topic describes how the Cisco Unity Interop Gateway works in VPIM networking.

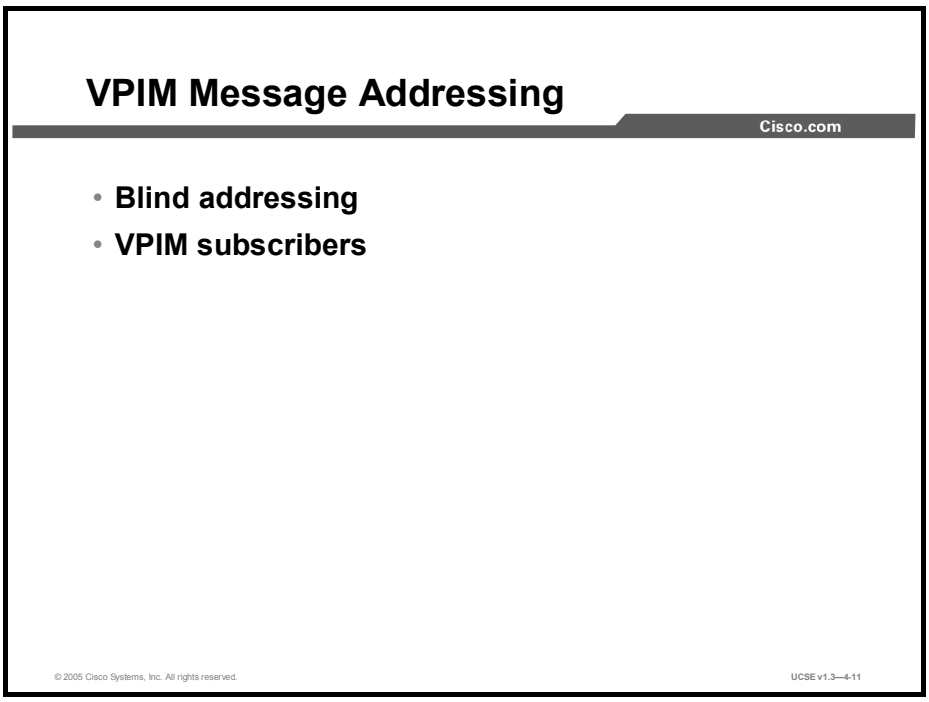


Cisco Unity Interop Gateway provides a way for Domino solutions to become VPIM-compliant, to provide message transport between itself and other VPIM-compliant voice messaging systems. When a message bound for a VPIM recipient is passed to the Interop Gateway, it converts the message from the Domino native format to MIME. It then formats the To: field with the domain name and prefix specified on the correct VPIM delivery location page. It formats the From: field with a prefix from the correct delivery location page and the domain name of the primary location page. Outgoing voice messages are converted to G.726 format and then a recorded voice name and vCard, if specified, are attached. The message is then put in the SMTP pickup folder for delivery.

Incoming messages are first noticed by the event sink and readdressed to the Interop Gateway. Once the Interop Gateway receives the message, it first verifies that the message has come from a known VPIM delivery location. If no match is made, the message is rejected and an NDR is sent to the originator of the message. If a matching delivery location is found, the Interop Gateway removes the prefixes in the To: and From: addresses, validates the recipient(s) of the message, and formats the addresses and converts the message from MIME to native Domino format. Any voice attachments are converted into the audio format specified on the delivery location page, and the message is handed back to Domino for delivery to the subscriber mailbox.

VPIM Message Addressing

This topic describes how messages are addressed in a VPIM network.



Cisco Unity provides the following ways to address messages to individuals by using a VPIM-compliant voice messaging system:

- **Blind addressing:** Blind addressing allows Cisco Unity to send messages without having specific information about the recipients on the remote voice messaging system (such as their names and mailbox numbers). It is one of the methods that Cisco Unity provides for addressing VPIM messages to users of another voice messaging system. To address a message to someone on another voice messaging system, subscribers enter the delivery location Dial ID and the remote mailbox number of the recipient.

  One of the steps to setting up blind addressing is to change the Blind Addressing setting on the Primary Location > Addressing Options page to something other than None. You also create a VPIM delivery location that corresponds to each voice messaging system with which Cisco Unity communicates. You provide the following key information for each delivery location:

  — **Dial ID:** A unique number that identifies the location to Cisco Unity. This is the number that subscribers dial when blind addressing messages to individuals who use the remote voice messaging system.

  — **SMTP domain name:** The Internet-addressable SMTP domain name that is used to construct addresses for individuals who use the voice messaging system that corresponds to the delivery location.

When blind addressing a message, subscribers dial a number that is made up of the delivery location Dial ID and the mailbox number of the recipient. Before addressing the message, Cisco Unity parses the number that the subscriber entered and searches for a matching delivery location. If Cisco Unity does not find a matching location, it reports the error to the sender and does not address the message. If a matching delivery location is found, Cisco Unity addresses the message without verifying that the remote mailbox number exists. Cisco Unity provides voice name confirmation that the delivery location exists before addressing the message (assuming that a voice name was recorded for the delivery location).

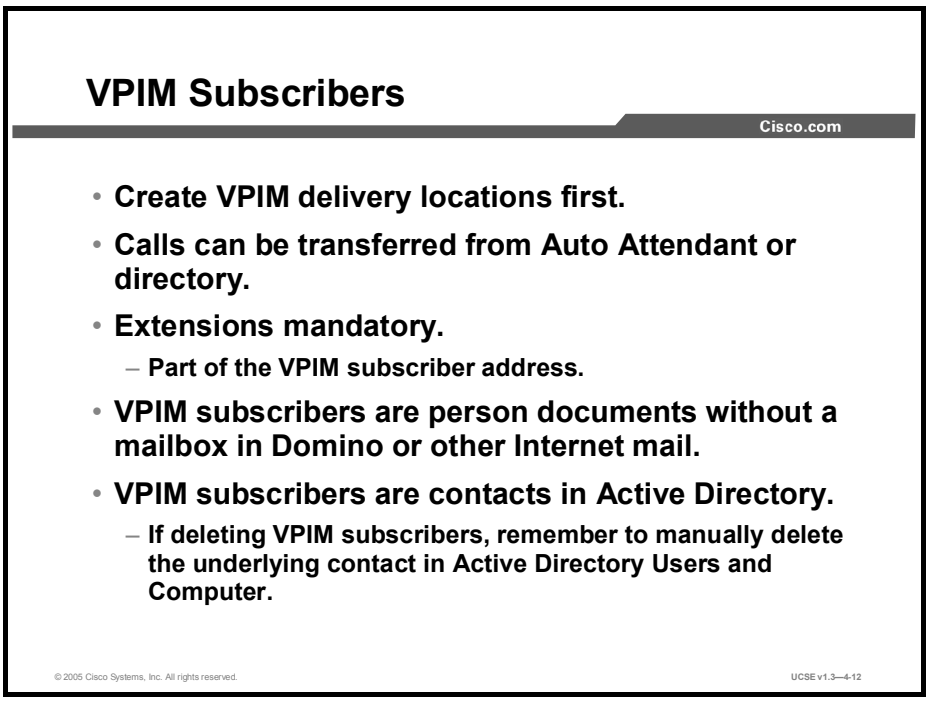
- **VPIM Subscribers:** VPIM subscribers are represented in Cisco Unity as individuals who use another voice messaging system. VPIM subscribers are created in Cisco Unity to enable Cisco Unity subscribers to find them in the directory and send them messages as they would with any other subscriber. Voice messages addressed to VPIM subscribers are sent to the voice messaging system that they use.

  To set up VPIM subscribers, you first create a VPIM delivery location that corresponds to each remote voice messaging system with which Cisco Unity communicates. After creating the delivery locations, you create a VPIM subscriber for each remote user. When creating each VPIM subscriber, you specify the user mailbox number on the other voice messaging system, and select a VPIM delivery location with which to associate the subscriber. The Voice Connector uses the information on the associated delivery location when delivering a message to the VPIM subscriber. Note that VPIM subscribers can be created only on the VPIM bridgehead server on which the associated VPIM delivery location has been created.

  You create and manage VPIM subscriber accounts in much the same way that you do regular subscriber accounts. You can use the Cisco Unity Administrator to create, modify, and delete VPIM subscriber accounts one at a time, and you can use the Cisco Unity Bulk Import wizard to create and modify multiple VPIM subscriber accounts.

VPIM Subscribers

This topic describes options available and setup procedures for VPIM subscribers.

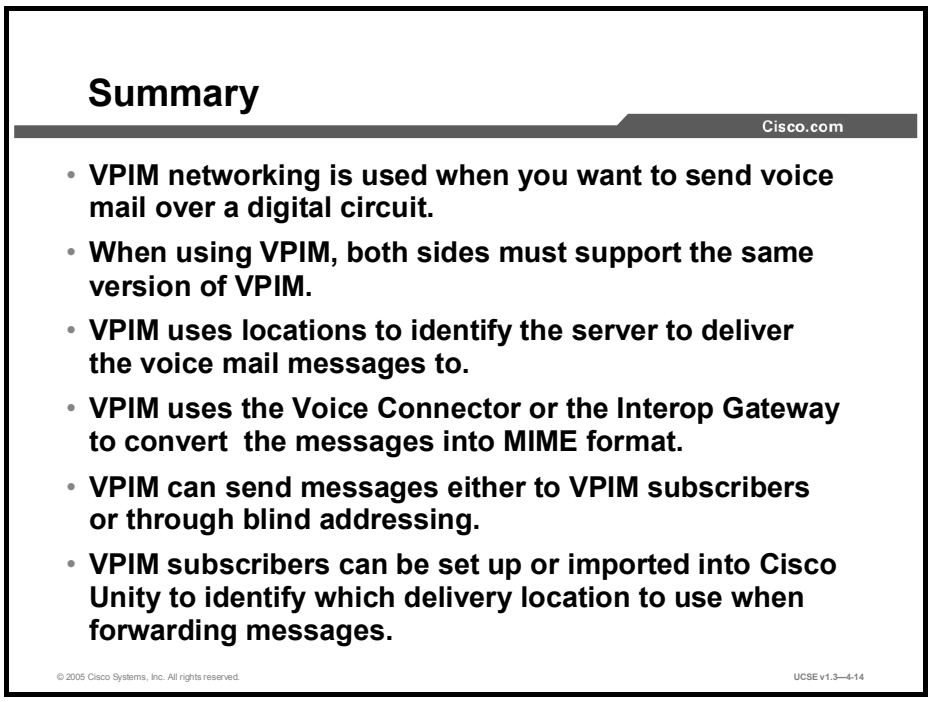


VPIM subscribers, like Internet subscribers, are Cisco Unity subscribers with no mailbox storage on the Exchange mail store. Before creating any VPIM subscribers, you must first create the VPIM delivery locations corresponding to the server on which their mailbox resides. When you create VPIM subscribers, you must specify the user mailbox number on the delivery system and the delivery location that the subscribers are associated with. You must include an extension for each VPIM subscriber, although this extension does not have to match the delivery location mailbox number. VPIM subscribers are represented as contacts in Active Directory. When you delete VPIM subscribers, either by deleting individual accounts or by deleting the delivery location that accounts are associated with, remember to go into Active Directory and delete the underlying contact information, because the Cisco Unity Administrator program will not do this.

As with Internet subscribers, any options relating to the local message store are unavailable. This means that VPIM subscribers cannot log onto Cisco Unity to check or send messages, log onto Cisco Unity via the telephone, or use Cisco Unity Assistant to change personal settings, own private lists, set up or receive message notification, or receive message waiting indication via Cisco Unity.

Summary

This topic summarizes the key points discussed in this lesson.



References

For additional information, refer to this resource:

- *Networking in Cisco Unity Guide (With Microsoft Exchange)*

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) VPIM is an industry-standard protocol based on which two protocols? (Choose two.)

A) SMTP
B) SMDI
C) NNTP
D) MIME
E) IMAP

Q2) Which two of the following are MIME-encoded parts of a VPIM message? (Choose two.)

A) video stream
B) text message
C) sender's x.400 address
D) vCard (electronic business card)

Q3) In the following list, identify the first two setup steps for a VPIM with Exchange solution.

A) ____Extend Active Directory schema.
B) ____Make dial-plan decisions and gather network information.
C) ____Create VPIM subscriber accounts.
D) ____Install Voice Connector and SMTP Transport Event Sink.
E) ____Verify SMTP connectivity.
F) ____Set addressing and search options.
G) ____Create delivery locations for each remote VPIM system.
H) ____Customize primary location object.
I) ____Set up remote system for VPIM.

Q4) What is the minimum number of VPIM servers needed in a network?

A) 1
B) 2
C) 3
D) 4

Q5) Which of the following is the first step in setting up a VPIM connection?

A) Extend Active Directory schema
B) Make dial-plan decisions and gather network information
C) Create VPIM subscriber accounts
D) Install Voice Connector and SMTP Transport Event Sink
E) Verify SMTP connectivity

Q6) Which of the following is a way to address messages with VPIM?

A) blind addressing
B) network addressing
C) default addressing
D) mixed addressing

Quiz Answer Key

Q1) A, D

Relates to: VPIM Networking

Q2) B, D

Relates to: VPIM Messages

Q3) E-1, A-2

Relates to: Setting up VPIM Networking

Q4) A

Relates to: Locations and VPIM Networking

Q5) E

Relates to: VPIM Networking and the Voice Connector

Q6) A

Relates to: VPIM Message Addressing

Lesson 7

Using AMIS Networking

Overview

Cisco Unity supports the Audio Messaging Interchange Specification analog (AMIS-a) protocol for the transfer of voice-mail messages between AMIS-compliant servers. This lesson describes the concepts underlying AMIS networking and the procedures necessary for implementing AMIS in a Cisco Unity environment.

Relevance

If your Cisco Unity networking plans call for delivery of voice messages to remote voice-mail servers that support the AMIS-a protocol, it is important for you to understand how to implement AMIS networking reliably and efficiently.

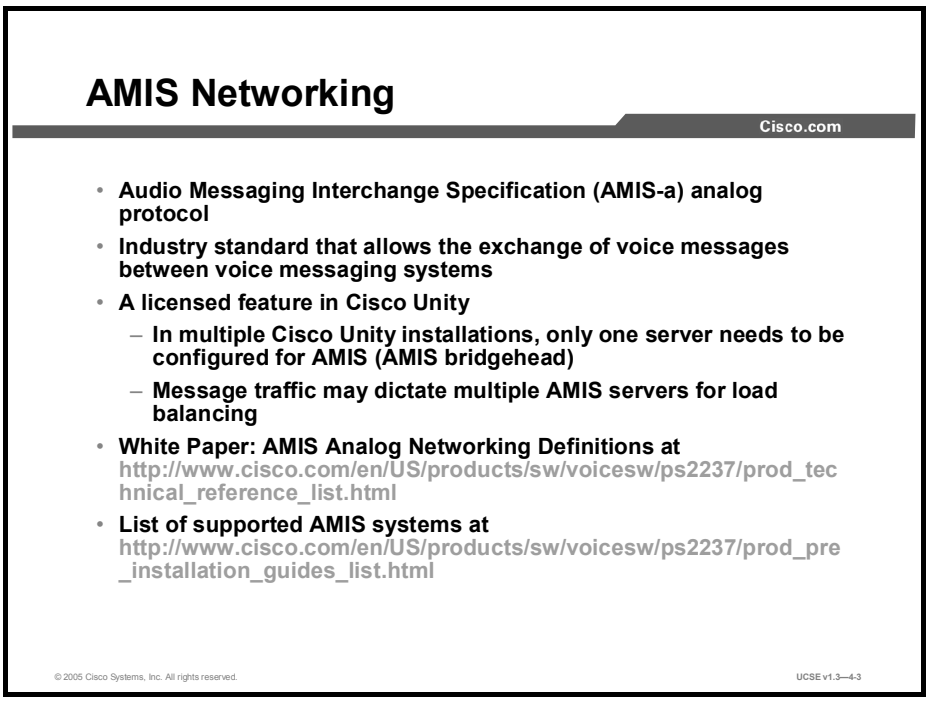
Objectives

Upon completing this lesson, you will be able to describe how Cisco Unity uses the AMIS networking protocol to transfer voice messages between AMIS-compliant servers. This ability includes being able to meet these objectives:

- Describe how Cisco Unity uses AMIS networking to deliver messages
- Describe the general procedural steps for setting up AMIS networking
- Describe the use of primary and delivery locations in AMIS networking
- Describe how the Voice Connector works in AMIS networking
- Describe how messages are transferred in an AMIS network
- Describe options available and setup procedures for AMIS subscribers

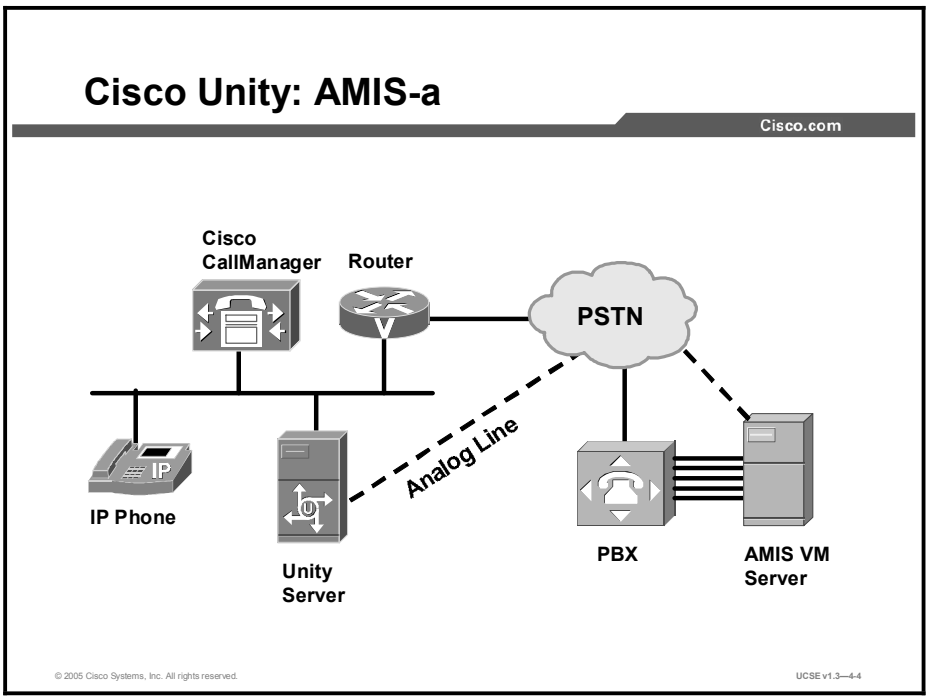
AMIS Networking

This topic describes how Unity uses AMIS networking to deliver messages.



The AMIS-a protocol is an industry standard that allows the exchange of voice messages between voice messaging systems over the public switched telephone network (PSTN) using standard analog telephone lines. In AMIS terms, Cisco Unity and all of the AMIS target servers that it communicates with are nodes in an AMIS network. Each node has a unique ID, its Node ID. In an AMIS message exchange, the originating node places a call to the destination node. When the destination node answers, the originating node transmits its Node ID by using a sequence of dual tone multifrequency (DTMF) tones (touchtones). If the destination node recognizes the Node ID and accepts the call, the originating node then transmits another series of touchtones that identify which subscriber the message is for. The destination node opens a new message, the originating node plays the message, and then a series of touchtones confirming the call are exchanged. For more information on the touchtones transmitted during a call, read the white paper located at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_white_paper09186a00800875e3.shtml

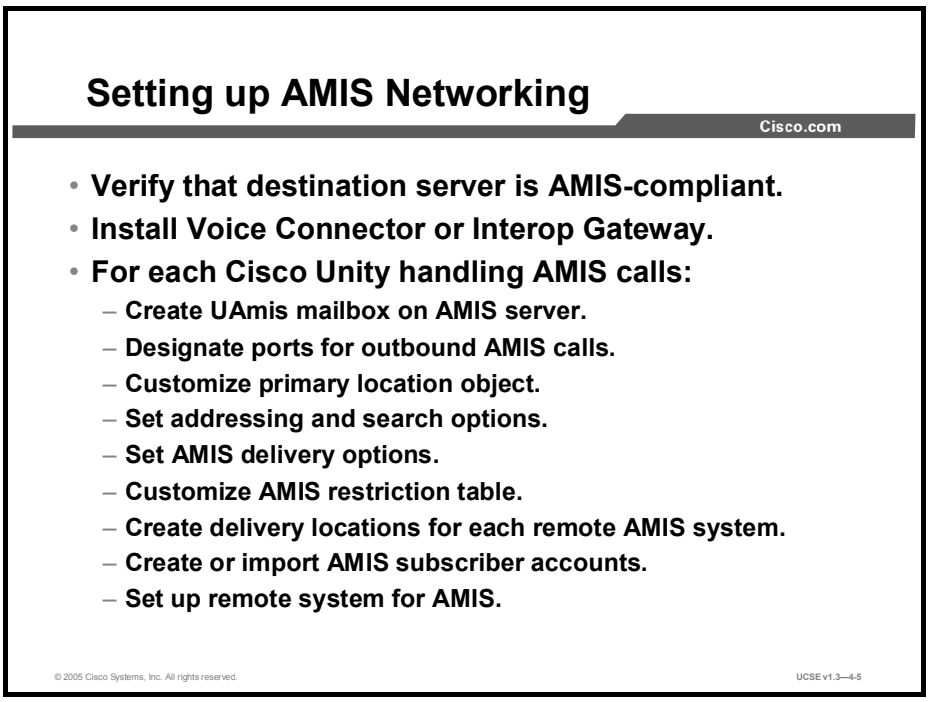
AMIS networking is a licensed feature of Cisco Unity. If you have multiple Cisco Unity servers in your organization, only one server needs to be licensed and designated as the AMIS server. If message traffic warrants, more AMIS servers can be added to balance the load.



In the figure, Cisco Unity supports subscribers on its own message store, as well as on a remote AMIS-compliant mail system. Through the PSTN and the analog lines that connect the circuit-switched PBX and voice mail, Cisco Unity can send and receive voice mail messages using the AMIS-a protocol.

Setting up AMIS Networking

This topic describes the general procedural steps for setting up AMIS networking.



Many of the steps necessary for AMIS networking are similar to the steps for digital, Simple Mail Transfer Protocol (SMTP), and Voice Profile for Internet Mail (VPIM) networking, including the installation of the Voice Connector. Because AMIS makes use of analog telephone lines for communication, there are some very important setup differences.

Before any other steps are taken, verify that the destination server is AMIS-compliant. A list of supported AMIS servers is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_data_sheet0900aecd800fe15f.html

One of the first steps is to install the Voice Collector on an Exchange server. You should have only one installation of the Voice Collector in an Active Directory (AD) forest, Exchange site, or multisite organization. If a previous version was installed, you must uninstall it before continuing.

After installation of the current Voice Connector, there are still a number of tasks to perform. If you are installing AMIS on multiple servers to handle a large volume of traffic, the following tasks must be completed on each server:

Step 1 Create the UAmis mailbox on the AMIS server and designate which ports will be used for outbound AMIS calls.

Step 2 Customize the primary location object on the Cisco Unity server by entering a meaningful name, giving it a Dial ID, recording a voice name, entering the Node ID, and, if appropriate, making it a member of a dialing domain. If you are a part of the dialing domain, the name for the domain needs to be entered on only one server.

Step 3 Set addressing and search options, which involves the same set of considerations as in digital, SMTP, or VPIM networking.

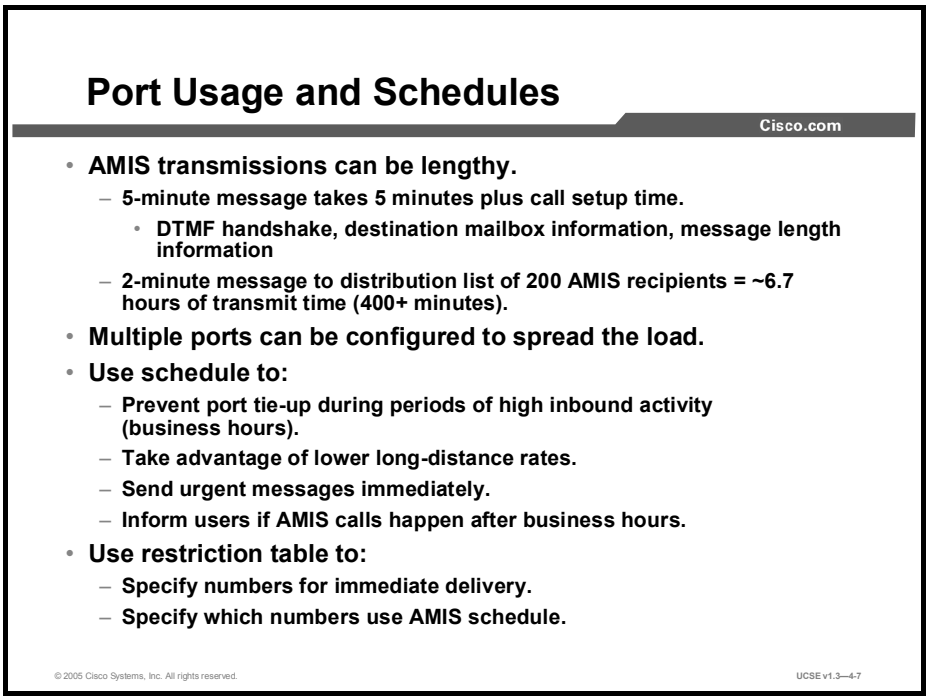
Step 4 Set AMIS delivery options for each Cisco Unity server which will deliver AMIS messages.

Step 5 Customize the AMIS restriction table. The combination of the AMIS schedule and the AMIS restriction table will determine both when and where AMIS calls will be delivered.

Step 6 Create a delivery location for each remote voice-messaging server to which subscribers send messages. When you have multiple Cisco Unity servers networked together, it is only necessary to create those delivery locations on one server in the network. The directory holds the location data, and it will be available to all who can access the directory.

Step 7 Create AMIS subscriber accounts for those persons you wish to be found from the corporate directory.

Step 8 Configure the remote system for AMIS.

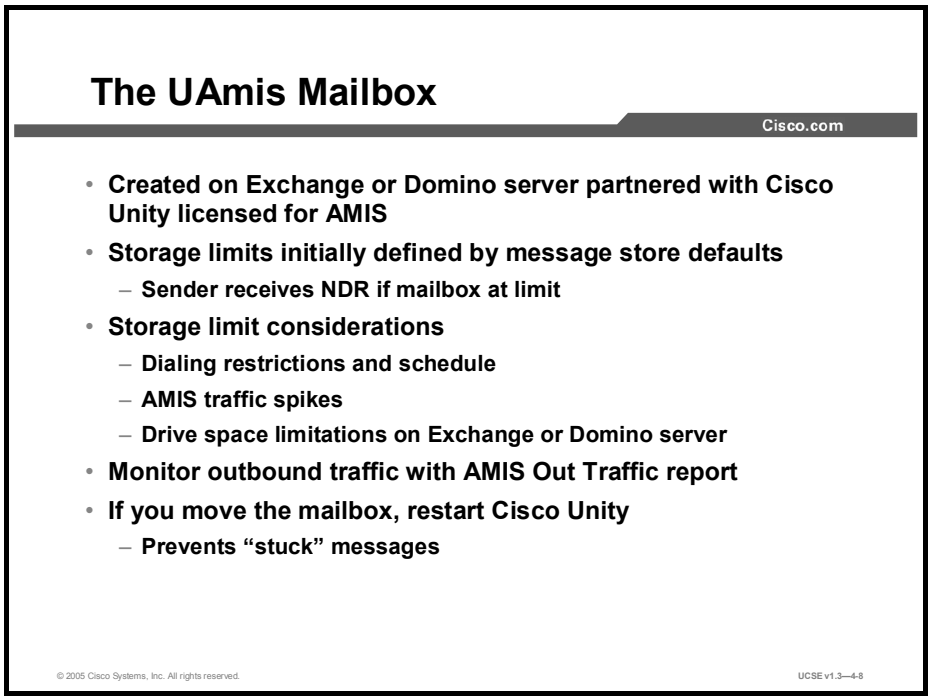


You must designate which ports will be used for outgoing AMIS calls on a Cisco Unity system used for calls. All ports that are set to answer calls are used for inbound AMIS calls. By their nature, AMIS calls can be lengthy; a five-minute message sent to a target AMIS server takes five minutes to transmit the message plus the time needed for the two servers to set up the transfer. Some of this overhead takes place with every call. A two-minute message sent to a distribution list of 200 AMIS recipients is sent individually to each recipient. That message will take at least six hours and 40 minutes to successfully transmit.

Specifying multiple ports to handle outbound AMIS calls will spread the load out. If there are multiple messages to a single destination, the messages are grouped in batches of nine, and each batch will be sent on a different port. If multiple destinations are involved, calls will go out on separate ports to each destination.

Because AMIS transmissions can be lengthy, you can set the AMIS schedule to transmit during periods of lower system activity, generally after standard business hours. In this way, you can also benefit from lower long-distance rates. AMIS messages marked as urgent can be sent immediately if you have configured the AMIS schedule appropriately. If you do configure the schedule to send messages after business hours, be sure to inform users. They may choose to send an e-mail instead of a voice mail if the matter requires a quicker response.

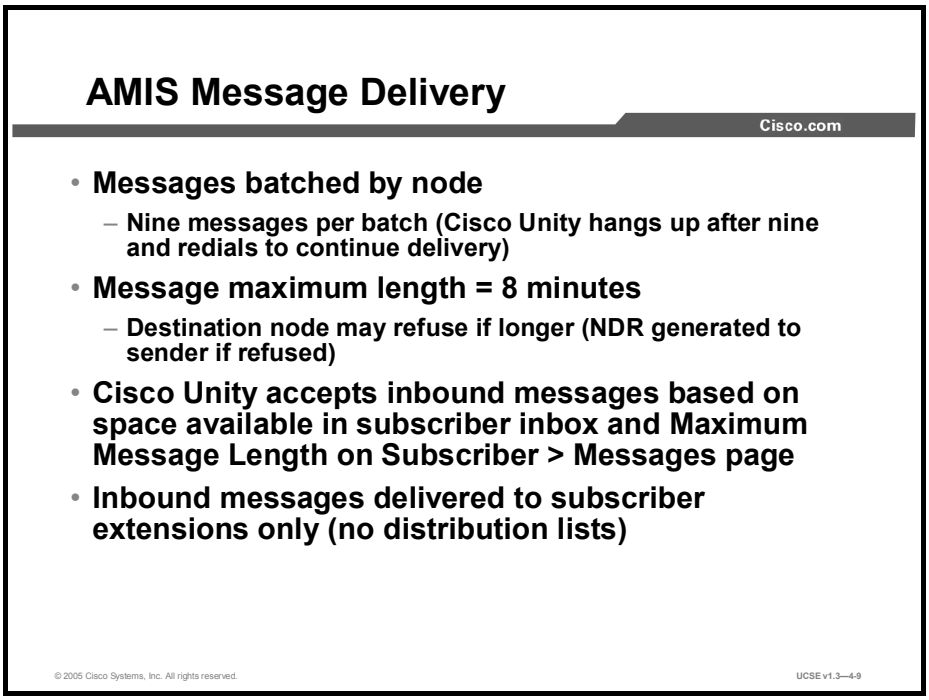
The AMIS restriction table can be used to specify which delivery locations will be delivered immediately and which will use the standard AMIS schedule.



Outgoing AMIS messages are placed in the UAmis mailbox for delivery. This mailbox is created on the Exchange server associated with Cisco Unity, licensed for AMIS. Because lengthy AMIS transmissions can occupy a great deal of space, the storage limits placed on the UAmis mailbox are important. Initially, any mailbox created on an Exchange system uses the storage defaults established by the system administrator. You can change those limits on a mailbox-by-mailbox basis, and you should do so for the UAmis mailbox. Items to consider include any dialing and scheduling restrictions placed on AMIS, times of day when AMIS traffic spikes occur, and drive space limits on the Exchange server.

It is a good idea to monitor outbound AMIS traffic with the AMIS Out Traffic report available on the Cisco Unity Administrator. You should do this before setting limits on the UAmis mailbox.

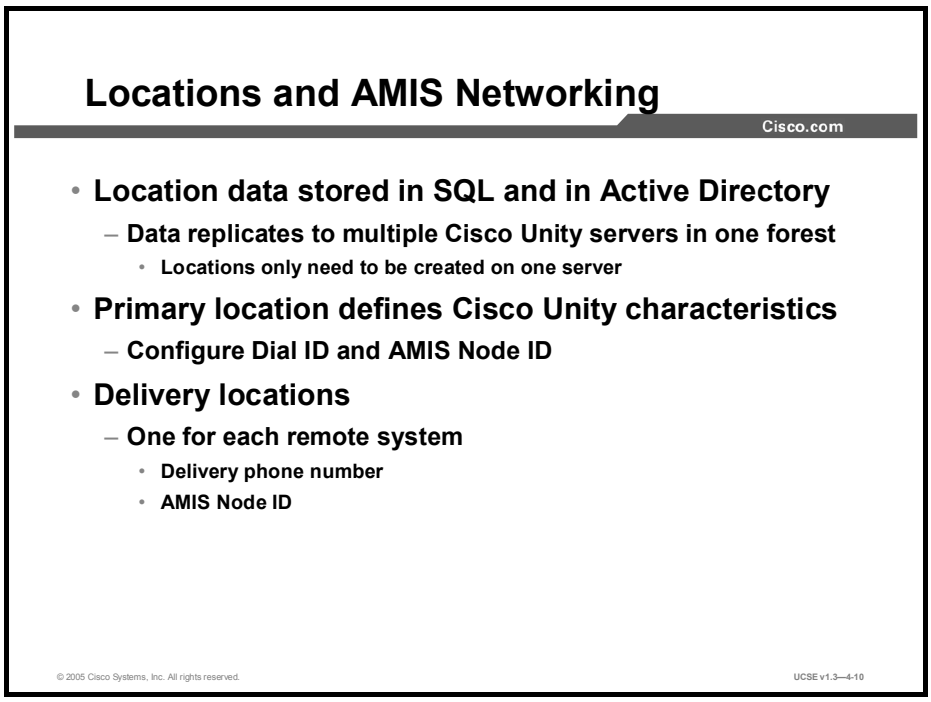
You can move the UAmis mailbox, just as you can move any other Exchange mailbox. If you do move the mailbox, restart the Cisco Unity system so that it reestablishes connection with the mailbox in its new location. Otherwise, messages sent to the mailbox may be stuck there, and not transmitted during the regularly scheduled time.



Outgoing messages are batched by node and then sent in batches of no more than nine messages per batch. If there are more than nine messages to a particular destination, Cisco Unity hangs up after nine are delivered, waits a short period of time, then redials and continues delivery. AMIS messages can be no longer than eight minutes. During transmission, the originating node sends the destination node the length of the message. If it exceeds the maximum allowed message length, the destination node may refuse it. Cisco Unity will accept inbound AMIS messages longer than eight minutes as long as the subscriber Messages page allows it and the subscriber mailbox has enough free space. Incoming AMIS messages are only delivered to subscribers and not to public distribution lists.

Locations and AMIS Networking

This topic describes the use of primary and delivery locations in AMIS networking.



Location objects play a central role in AMIS networking. A primary location object is created when you install Cisco Unity. As subscribers are added to Cisco Unity, they become members of this location. The Cisco Unity Administrator allows you to create additional location objects that represent additional Cisco Unity servers. If you are in the same Active Directory forest, there is no need to create additional locations, because they will be available within minutes of their creation as default objects on their home system. Location objects can be tied together using a property called a dialing domain ID. This allows you to create a meta-location that spans multiple Cisco Unity servers by assigning them all the same dialing domain ID. This meta-location lets you easily span sites or other networking boundaries and provide transparent dialing capabilities to customers that have networked telephone switches.

Recorded object data for the location object includes the following:

- A voice name for addressing
- A display name for the administrative console
- Three DTMF names (one for each keypad mapping)
- A DTMF ID (for addressing)
- A Node ID
- A destination type
- A send blind flag
- Information about the keypad mapping used at that location.

In Cisco Unity, subscribers and any other system objects can only be associated with the primary location object created by the setup program. All delivery location objects are used solely for addressing purposes.

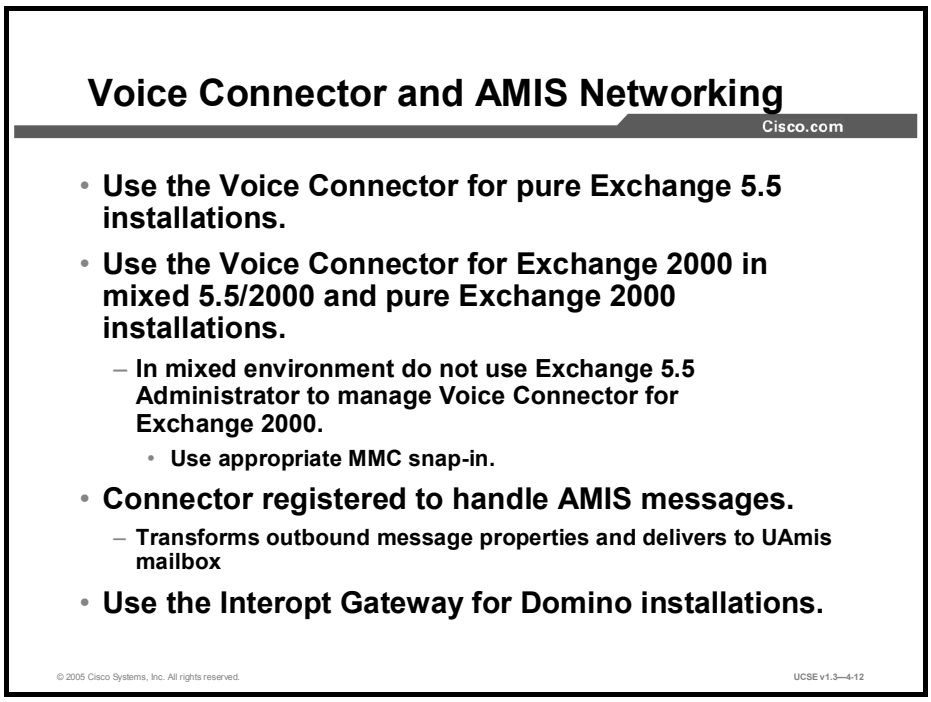
When defining the primary location object, you give it a Dial ID. Creating a dial plan for your organization that will result in callers reaching subscribers correctly and efficiently is very important. The Dial IDs that you create are an important part of that dial plan. Be sure that they do not conflict with previously assigned IDs.

In the Cisco Unity Administrator, all location objects will be visible, but administrators will only be able to edit or delete location objects that were created on their Cisco Unity system. Location objects that replicate from other sites will be read-only. The original location object that is installed with the system (the primary location object) can be edited but not deleted from the system.

You must set up a delivery location for every AMIS node that Cisco Unity will exchange messages with. The delivery locations contain the delivery phone number and Node ID that Cisco Unity needs to deliver messages correctly. Delivery locations only need to be created on one Cisco Unity server. After replication, the locations will be available to all servers accessing the same directory.

Voice Connector and AMIS Networking

This topic describes how the Voice Connector works in AMIS networking.

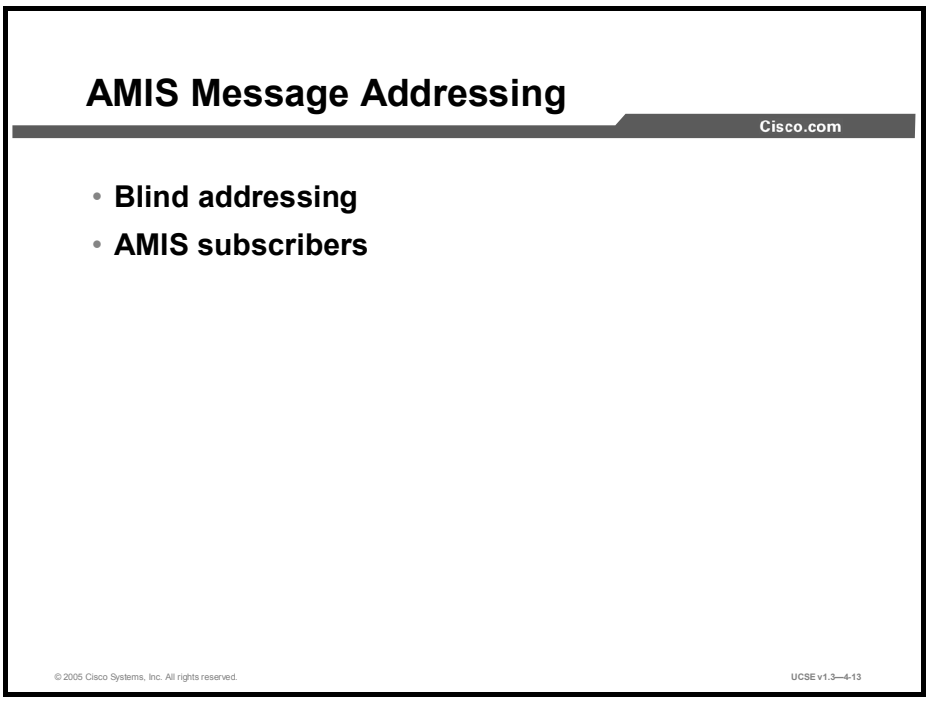


The Voice Connector allows Cisco Unity to send and receive AMIS messages. When a message bound for an AMIS recipient is passed to the Voice Connector (because the Voice Connector is registered with Exchange to handle AMIS messages), the Voice Connector formats the To: and From: address fields, then puts the message in the UAmis mailbox for delivery.

If you are using Cisco Unity in a pure Exchange 5.5 installation, use the Voice Connector for Exchange 5.5. If your installation has a mix of Exchange 5.5 and Exchange 2000 servers, or is a pure Exchange 2000 installation, then use the Voice Connector for Exchange 2000. In a mixed environment, do not use the Exchange 5.5 Administrator program to manage the Voice Connector for Exchange 2000; use the appropriate Microsoft Management Console (MMC) snap-in.

AMIS Message Addressing

This topic describes how messages are addressed in an AMIS network.



Cisco Unity provides the following message addressing options in an AMIS network:

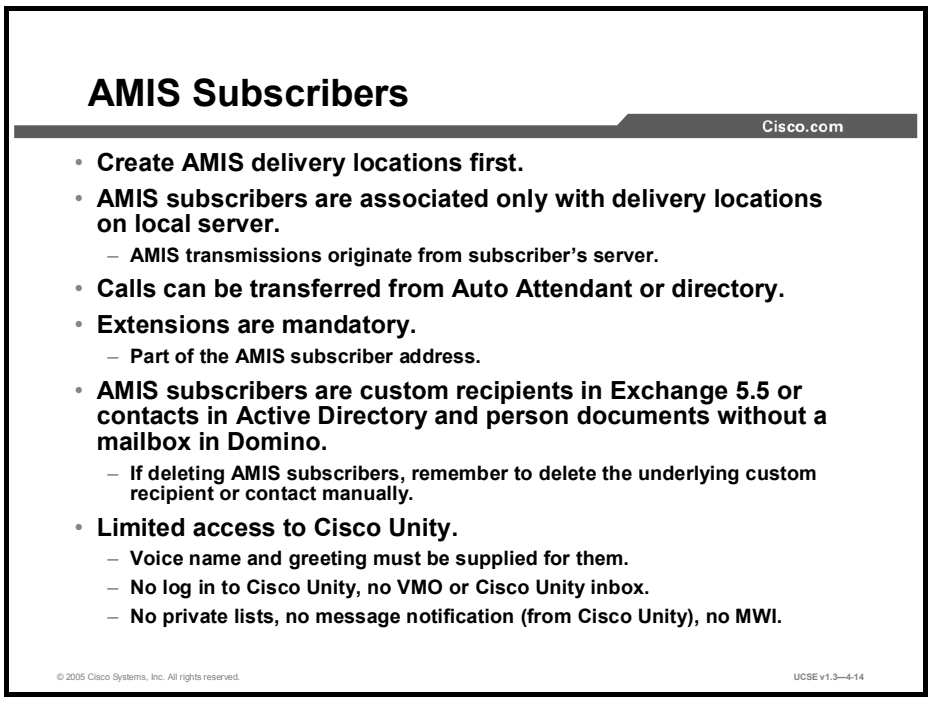
- **Blind addressing:** Allows Cisco Unity subscribers to send messages to subscribers on the remote voice messaging system, even though the recipient mailbox number, name, and recorded name are not in the directory. Although Cisco Unity cannot provide voice name confirmation (therefore the term “blind addressing”), the message is addressed and sent.
- **AMIS subscribers:** Allow Cisco Unity subscribers to get voice name confirmation when addressing messages to subscribers on the remote voice messaging system. AMIS subscribers are a representation in Cisco Unity of the subscribers on the remote messaging system. AMIS subscribers are created in Cisco Unity to enable Cisco Unity subscribers to find them in the directory and send them messages as they would with any other subscriber.

Subscribers can use the Cisco Unity phone conversation, also known as the Telephone User Interface (TUI), ViewMail for Microsoft Outlook, or the Cisco Unity Inbox to reply to and forward AMIS messages, just as they do with regular voice messages. However, when sending or retrieving AMIS messages, subscribers will encounter the following limitations:

- AMIS messages marked urgent when they are sent are not marked urgent when they are retrieved by the recipient.
- AMIS messages marked private when they are sent are not marked private when they are retrieved by the recipient.
- Requests for return receipts on AMIS messages are not honored.
- E-mail messages cannot be sent to AMIS recipients even though ViewMail allows subscribers to address them. Instead of being delivered, e-mail messages sent to AMIS recipients are returned to the sender as non-delivery receipts (NDRs).

AMIS Subscribers

This topic describes options available and setup procedures for AMIS subscribers.

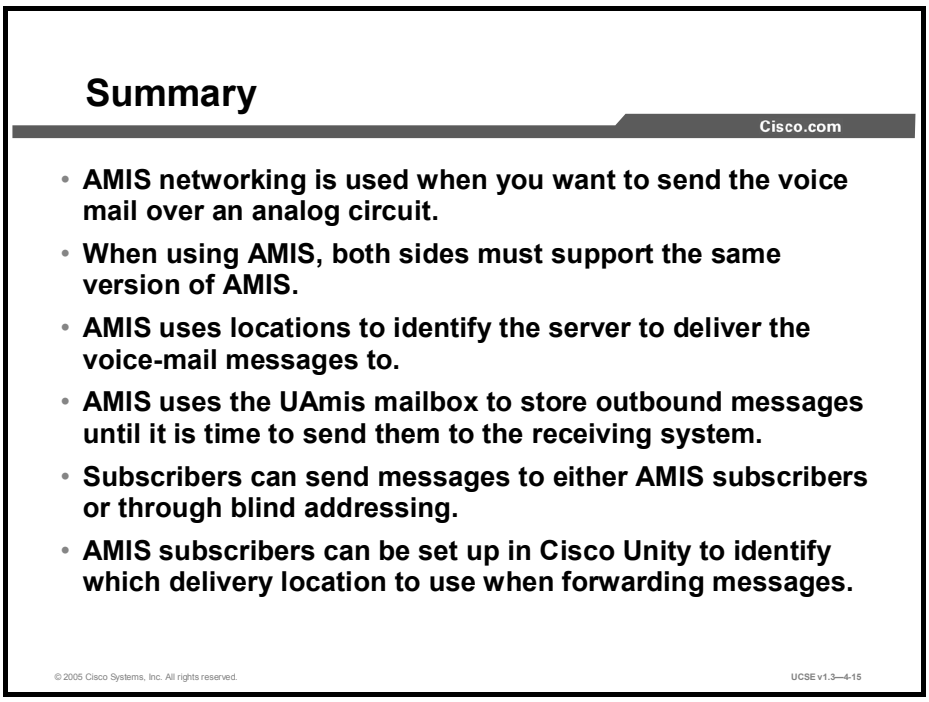


AMIS subscribers, like Internet and VPIM subscribers, are Cisco Unity subscribers with no mailbox storage on the Exchange mail store. Before creating any AMIS subscribers, you must first create the AMIS delivery locations corresponding to the server on which their mailbox resides. When you create AMIS subscribers, you must specify the user mailbox number on the delivery system and the delivery location the subscribers are associated with. You must include an extension for each AMIS subscriber, although this extension does not have to match the delivery location mailbox number. AMIS subscribers are represented as contacts in Active Directory or as custom recipients in Exchange 5.5. When you delete AMIS subscribers, either by deleting individual accounts or by deleting the delivery location that accounts are associated with, remember to go into Active Directory or the Exchange 5.5 Administrator and delete the underlying contact information, because the Cisco Unity Administrator program will not do this.

As with Internet and VPIM subscribers, any options relating to the local message store are unavailable. This means that AMIS subscribers cannot log into Cisco Unity to check or send messages, log into Cisco Unity via the telephone, or use Cisco Unity Assistant to change personal settings, own private lists, set up or receive message notification, or receive message waiting indication via Cisco Unity.

Summary

This topic summarizes the key points in this lesson.



References

For additional information, refer to this resource:

- *Networking in Cisco Unity Guide (With Microsoft Exchange)*

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) How many servers need to be licensed for AMIS?

A) 1
B) 3
C) 2
D) 5

Q2) Which media does AMIS use to transmit its messages?

A) video stream
B) analog
C) sender's x.400 address
D) digital

Q3) Put the following setup steps in order according to Cisco Unity training documentation.

A) ____Create UAmis mailbox on AMIS server.
B) ____Designate ports for outbound AMIS calls.
C) ____Customize primary location object.
D) ____Set addressing and search options.
E) ____Set AMIS delivery options.
F) ____Customize AMIS restriction table.
G) ____Create delivery locations for each remote AMIS system.
H) ____Create AMIS subscriber accounts.
I) ____Set up remote system for AMIS.

Q4) Which of the following are true about AMIS subscribers? (Choose two.)

A) They cannot log in to Cisco Unity to check or send messages.
B) They can log in to Cisco Unity via the telephone.
C) They cannot use Cisco Unity Assistant to change personal settings.
D) They can own private lists.
E) They can set up or receive message notification.
F) They cannot receive message waiting indication via Cisco Unity.
G) They cannot receive messages.

Q5) Which mailbox is used to store the AMIS messages for outbound delivery?

A) UOMNI
B) UAmis
C) UMNST
D) POP3

Q6) Of the following, which is a way to address messages with AMIS?

A) blind addressing
B) network addressing
C) default addressing

Q7) Before you create an AMIS subscriber, you must create a(n) _____. (Choose one.)

A) attendant console
B) operator handle
C) delivery location
D) search scope

Quiz Answer Key

Q1) A

Relates to: AMIS Networking

Q2) B

Relates to: AMIS Networking

Q3) A-7, B-1, C-6, D-2, E-3, F-5, G-8, H-4, I-9

Relates to: Setting Up AMIS Networking

Q4) A, C

Relates to: Locations and AMIS Networking

Q5) B

Relates to: Voice Connector and AMIS Networking

Q6) A

Relates to: AMIS Message Addressing

Q7) C

Relates to: AMIS Subscribers

Lesson 8

Using Cisco Unity Bridge Networking

Overview

Networking with the Cisco Unity Bridge provides communication between Cisco Unity and Octel voice-mail servers in an Octel analog network.

Relevance

If you are implementing Cisco Unity in an enterprise that currently uses Octel voice-mail servers, you must understand the concepts underlying Bridge networking and be familiar with the procedures necessary to implement Bridge networking.

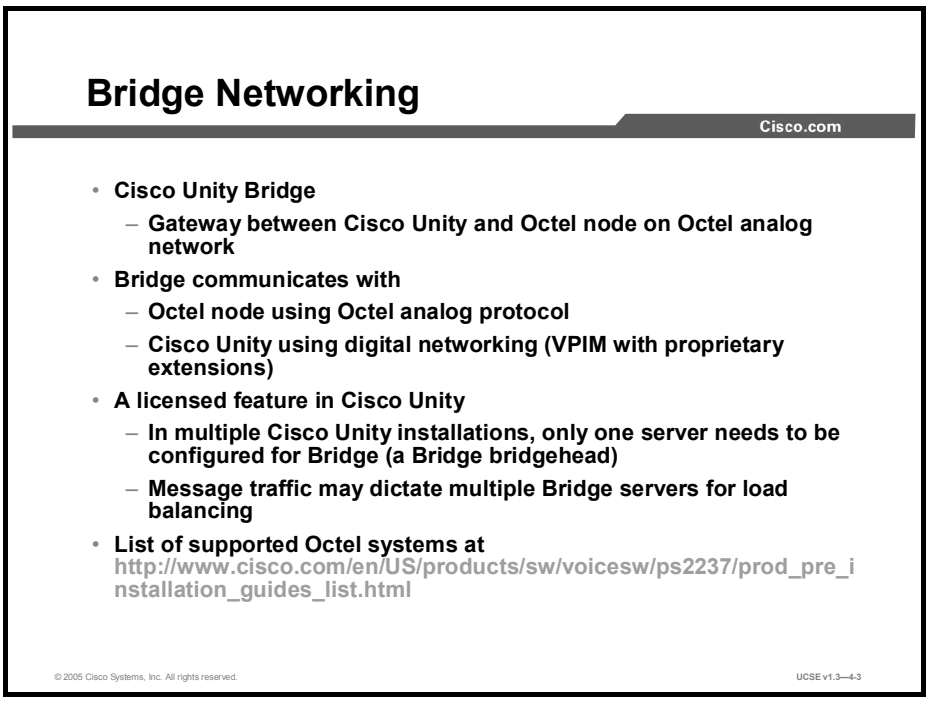
Objectives

Upon completing this lesson, you will be able to describe how Cisco Unity uses Bridge networking to deliver messages between Cisco Unity and mail servers in an Octel network. This includes being able to meet these objectives:

- Describe how Cisco Unity uses Bridge networking to deliver messages
- Describe the general procedural steps for setting up Bridge networking
- Describe the use of primary and delivery locations in Bridge networking
- Describe how the Cisco Unity Voice Connector works in Bridge networking
- Describe how messages are transferred in a Bridge network
- Describe options available and setup procedures for Bridge subscribers

Bridge Networking

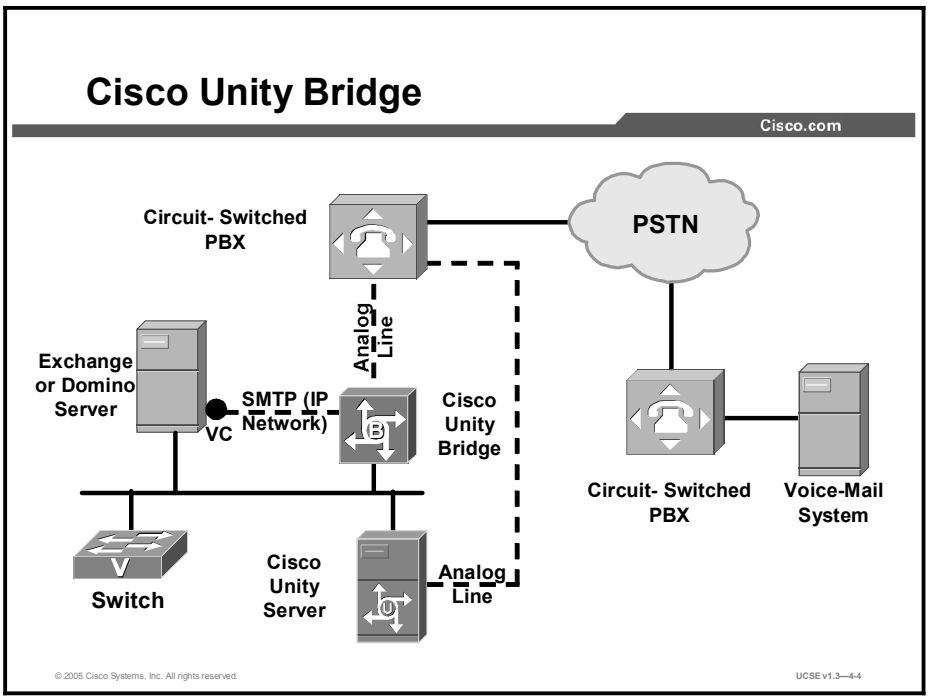
This topic describes how Cisco Unity uses Bridge networking to deliver messages.



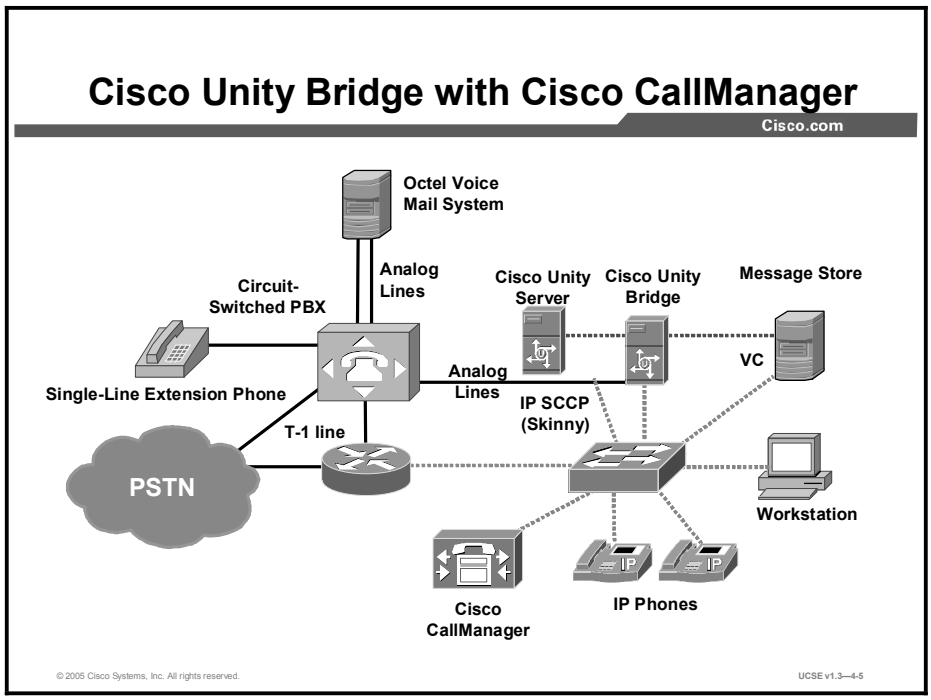
Cisco Unity Bridge acts as a gateway between Cisco Unity and an Octel node on an Octel analog network. To the rest of the Octel analog network, the Bridge appears as just another node, in much the same manner as Cisco Unity using Audio Messaging Interchange Specification (AMIS) appears as another node on an AMIS network. As a gateway, the Bridge translates messages between two different protocols. It communicates with an Octel node by placing a phone call and then using the Octel analog protocol; it communicates with Cisco Unity using the digital networking protocol, which is based on Voice Profile for Internet Mail (VPIM) with some proprietary extensions for added functionality. Messaging between Cisco Unity and the Bridge is done over the Internet or any TCP/IP network using Simple Message Transfer Protocol (SMTP).

Bridge networking is a licensed feature of Cisco Unity. In addition to the separate Bridge server, you must also license Cisco Unity to communicate with Bridge. If you have multiple Cisco Unity servers in your organization, only one server needs to be licensed for and designated as the Bridge server. If message traffic warrants, more Bridge servers can be added to balance the load. Bridge servers exist in a one-to-one relationship with Cisco Unity servers.

A list of supported Octel systems is available at http://www.cisco.com/en/US/partner/products/sw/voicesw/ps2237/prod_system_requirements_hardware09186a00801b91cc.html.



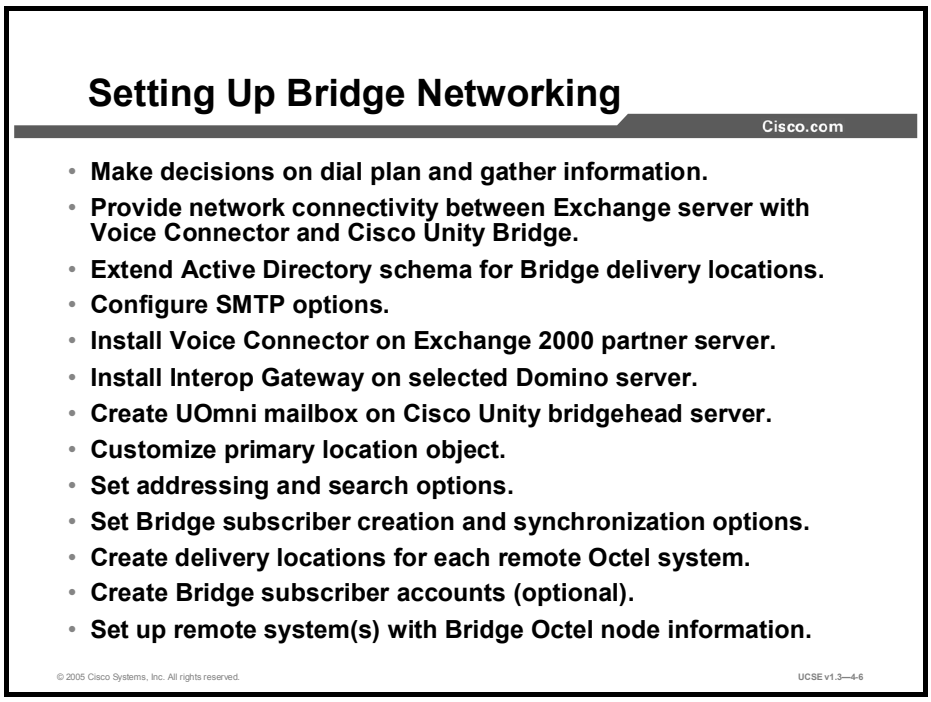
Cisco Unity coupled with Cisco Unity Bridge is a messaging server combination capable of helping an organization manage the transition from older telephone equipment to a converged IP network. Cisco Unity is integrated with two switches: a circuit-switched (legacy) PBX and a Cisco CallManager, and can manage voice-mail accounts for subscribers with either IP telephones or standard single-line extensions attached to the circuit-switched PBX. In addition, through the analog lines that connect the legacy PBX and voice mail, Cisco Unity Bridge can send and receive voice-mail messages using the Octel analog messaging protocol. In this way, an enterprise may maximize its return on its investment in older telephone equipment while migrating subscribers to an IP telephone network at its own pace.



In this design, Cisco Unity provides messaging services to subscribers being served by Cisco CallManager and a circuit-switched PBX is providing voice-mail service to subscribers on an Octel system. Cisco Unity Bridge is helping the organization manage the transition from older telephone equipment to a converged IP network. Through the analog lines that connect the legacy PBX and voice mail, Cisco Unity can use the Cisco Unity Bridge to send and receive voice-mail messages using the Octel analog messaging protocol.

Setting up Bridge Networking

This topic describes the steps for setting up Bridge networking.



Many of the steps necessary for Bridge networking are similar to the steps required for digital, SMTP, VPIM, and AMIS networking, including the installation of the Voice Connector. Because Bridge makes use of analog telephone lines for communication, there are some very important setup differences.

Before any other steps are taken, be sure the server meets the requirements in the Cisco Unity Bridge System Requirements, and Supported Hardware and Software, available at the following URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_pre_installation_guides_list.html

The steps for setting up Bridge networking are as follows:

Step 1 Make dial-plan decisions before implementing the system, in order to avoid an installation that has conflicting IDs that will confuse those searching for subscriber addresses.

Step 2 Provide network connectivity between the Exchange server that will have the Voice Connector installed on it and the Cisco Unity Bridge.

Step 3 Extend the Active Directory schema to enable Bridge networking. The schema changes made are additions to the Bridge delivery location object class. A full description of the schema changes is listed in the file vpimgateway.ldf, located in the Schema\LdifScripts directory on Cisco Unity Disc 1.

Step 4 Grant permissions to the Bridge server to relay e-mail through the Exchange SMTP virtual server, and configure an SMTP connector to route messages to the Bridge.

Step 5 Install the Voice Connector on an Exchange 2000 server. You should have only one installation of the Voice Connector in an Active Directory forest. If a previous version was installed, it must be uninstalled before continuing.

Step 6 If you are installing in a Domino environment, install the Interop Gateway on the selected Domino server.

Step 7 Create the UOmni mailbox on the Cisco Unity bridgehead server.

Step 8 Customize the primary location object on the Cisco Unity server by entering a meaningful name, giving it a Dial ID, recording a voice name, entering the Node ID (this Node ID must match the serial number on the Cisco Unity nodes page in the Bridge Administrator), entering the fully qualified domain name of the Bridge server, and, if appropriate, making it a member of a dialing domain. If you are a part of the dialing domain, the name for the domain only needs to be entered on one server.

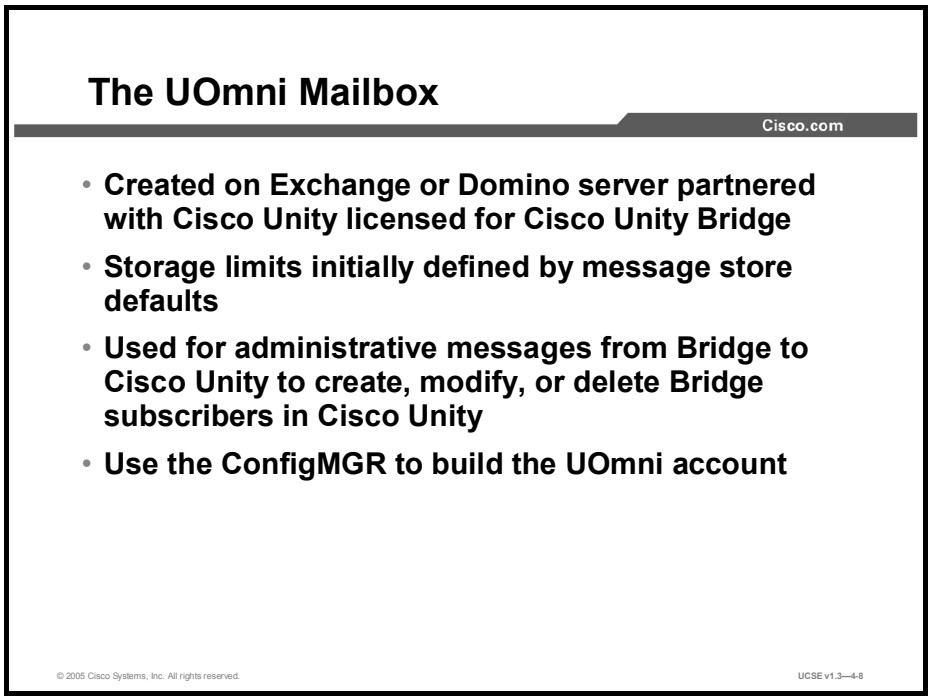
Step 9 Set addressing and search options, which involves the same set of considerations as in digital, SMTP, VPIM, or AMIS networking.

Step 10 Set Bridge subscriber creation and synchronization options.

Step 11 Create a delivery location for each remote Octel system to which subscribers send messages. Optionally, you can change the standard messaging menu conversation or the default display name-parsing rule.

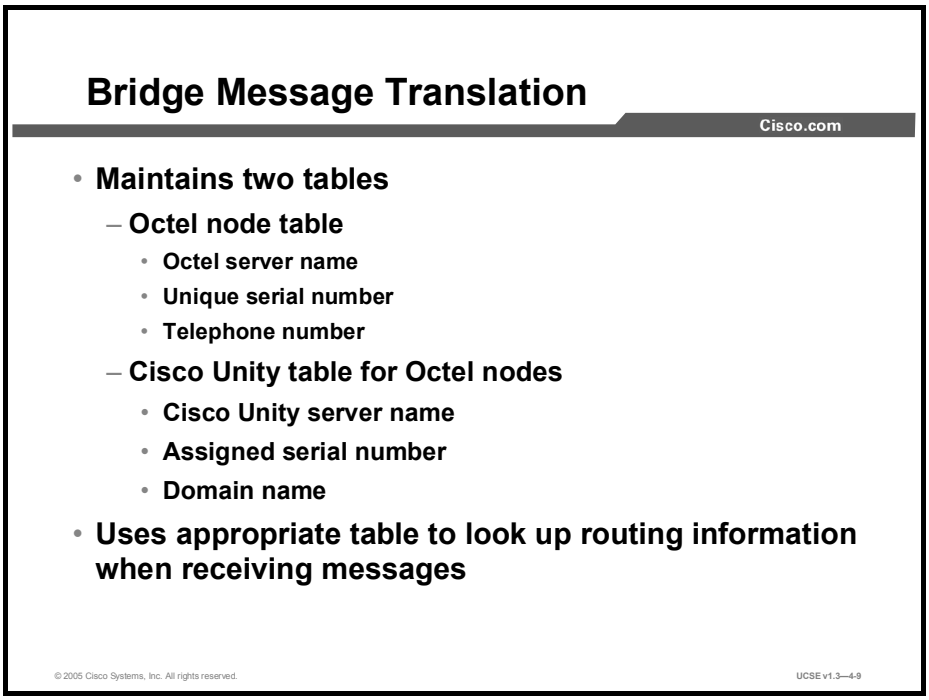
Step 12 Optionally, you can create Bridge subscriber accounts for those persons you wish to be found from the corporate directory on a permanent basis.

Step 13 If the Bridge will be joining an Octel network as a new node, configure the remote Octel systems to recognize the new node.



The UOmni mailbox is created on the Exchange server partnered with the Cisco Unity system that is licensed for Cisco Unity Bridge. The mailbox will initially take whatever message storage limits are defined in the Exchange system. It is likely that these limits will be acceptable, because the function of the UOmni mailbox is to accept administrative messages from the Bridge to Cisco Unity. These messages concern the automatic creation, modification, or deletion of Bridge subscribers in Cisco Unity that happen as a result of Octel NameNet emulation. Octel NameNet is the feature that allows nodes to obtain new entries from directories on other nodes. When a message is sent to a node by a new subscriber, the node will request display name and recorded name information and will then add that information to its directory. Cisco Unity Bridge emulates that behavior and then passes the messages on to Cisco Unity via the UOmni mailbox.

If you do move the UOmni mailbox after it has been created, be sure to stop and restart Cisco Unity so it will be aware of the new location of UOmni. Otherwise, messages may get stuck in the mailbox.



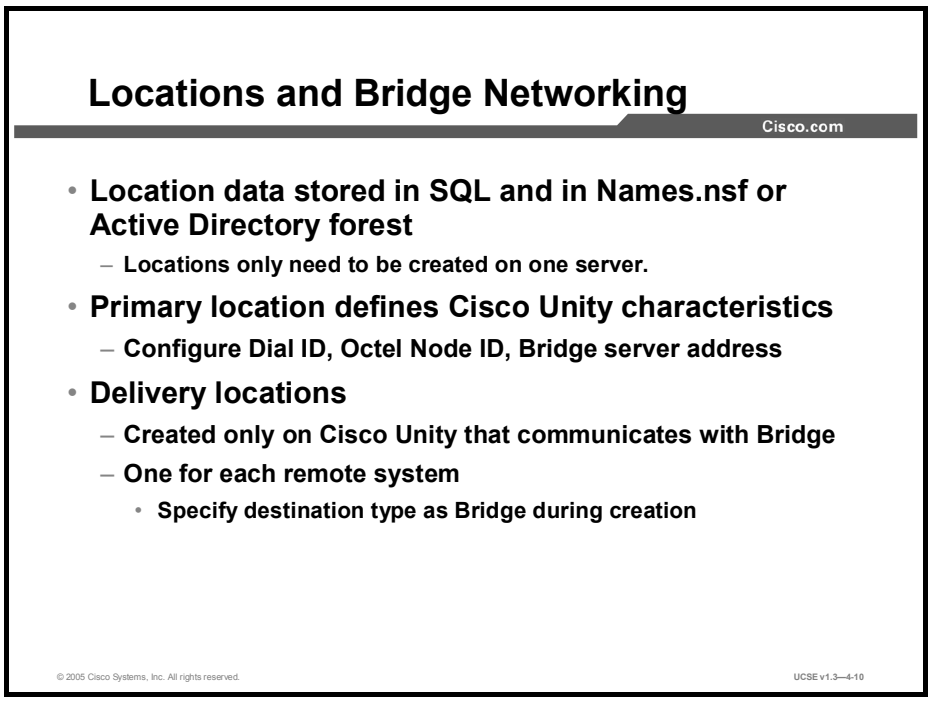
The Cisco Unity Bridge delivers fax and voice messages between servers that use differing protocols. As a result, the Bridge must translate the messages coming to it into the form the receiving server expects to see. To do this, the Bridge maintains the following two tables:

- **The Octel node table:** Contains the server name, unique Octel serial number, and the telephone number of each Octel node it communicates with
- **A Cisco Unity table:** Contains the Cisco Unity server name, assigned serial number, and its domain name.

Using these two tables, the Bridge can receive a message from either type of node, Octel or Cisco Unity, look up the address, reformat the information into the desired form, and then send the message to its destination.

Locations and Bridge Networking

This topic describes the use of primary and delivery locations in Bridge networking.



Location objects play a central role in Bridge networking as they do in all of the other forms of networking. Cisco Unity Administrator allows you to create additional location objects called delivery locations that represent additional target servers. If you are in the same Active Directory forest, there is no need to create additional locations, because they will be available within minutes of their creation as default objects on their home system. Location objects can be tied together using a property called a dialing domain ID. A dialing domain ID allows you to create a meta-location that spans multiple Cisco Unity servers by assigning them all the same dialing domain ID. This meta-location lets you easily span sites or other networking boundaries and provide transparent dialing capabilities to customers that have networked telephone switches.

The important object data for the primary location object on a Cisco Unity server used in Bridge networking includes the following:

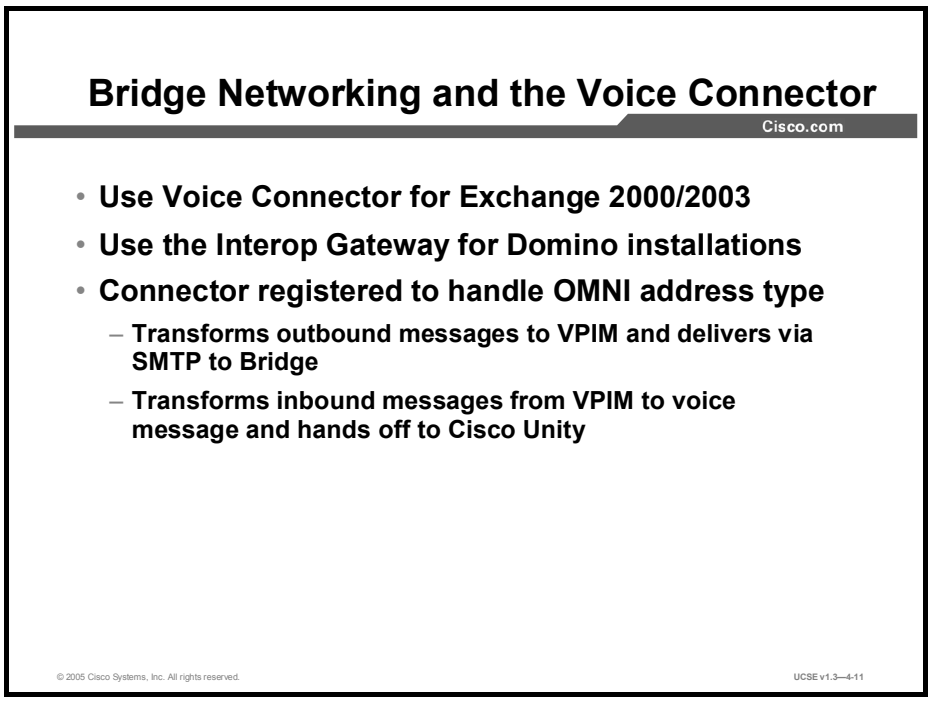
- **Node ID:** This Cisco Unity server ID on the Octel analog network
- **Dial ID:** Identifies this location to Cisco Unity
- **Server Address:** The fully qualified domain name of the Bridge server with which Cisco Unity is associated.

When defining the primary location object, you give it a Dial ID. Creating a dial plan for your organization that will result in callers reaching subscribers correctly and efficiently is very important. The Dial IDs that you create are an important part of that dial plan. Be sure that they do not conflict with previously assigned IDs.

Delivery locations in Bridge networking are created for each Octel system to which subscribers will send messages. You select Bridge as the destination type during creation, record a voice name for the location, and enter the Octel Node ID. This number must match the number on the Octel node and must match the one recorded in the Bridge Administrator.

Bridge Networking and the Voice Connector

This topic describes how the Cisco Unity Voice Connector works in Bridge networking.

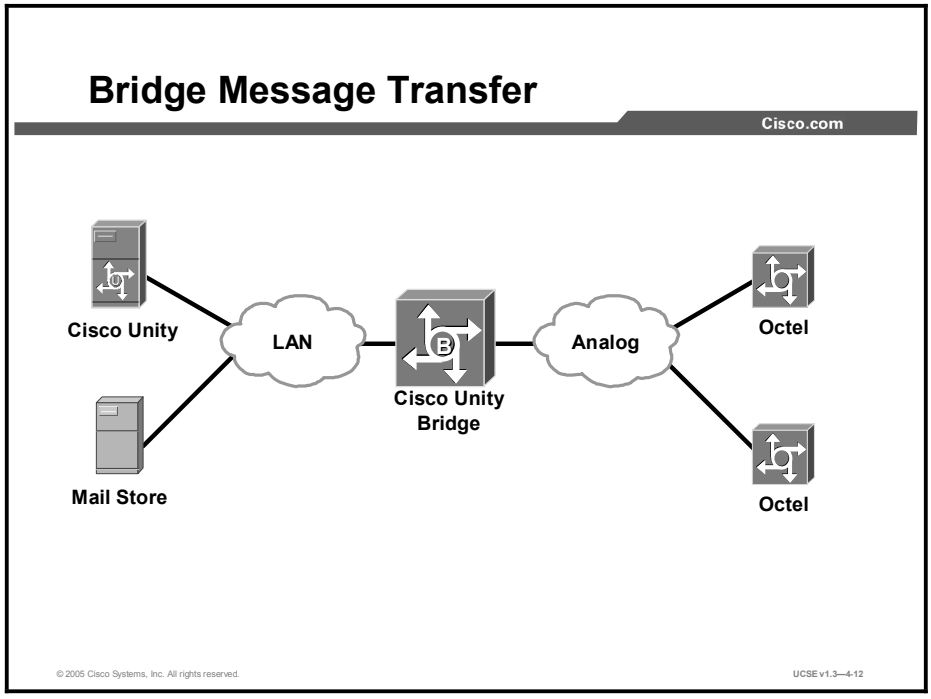


The Voice Connector allows Cisco Unity to send messages to, and receive messages from, the Bridge. When a message bound for a Bridge recipient is passed to the Voice Connector, because it is registered with Exchange to handle OMNI address type messages, it transforms the message into the proprietary VPIM format and delivers it to the Bridge via SMTP. Incoming messages are transformed from the VPIM format into voice messages and handed off to Exchange for delivery.

The Voice Connector for Exchange 2000 is the only voice connector supported for use with Unity Bridge. If your installation has a mix of Exchange 5.5 and Exchange 2000 servers, or is a pure Exchange 2000 installation, use the Voice Connector for Exchange 2000. In a mixed environment, do not use the Exchange 5.5 Administrator program to manage the Voice Connector for Exchange 2000. Use the appropriate Microsoft Management Console (MMC) snap-in.

Bridge Message Transfer

This topic describes how messages are transferred in a Bridge network.



Messaging Between the Bridge and Cisco Unity

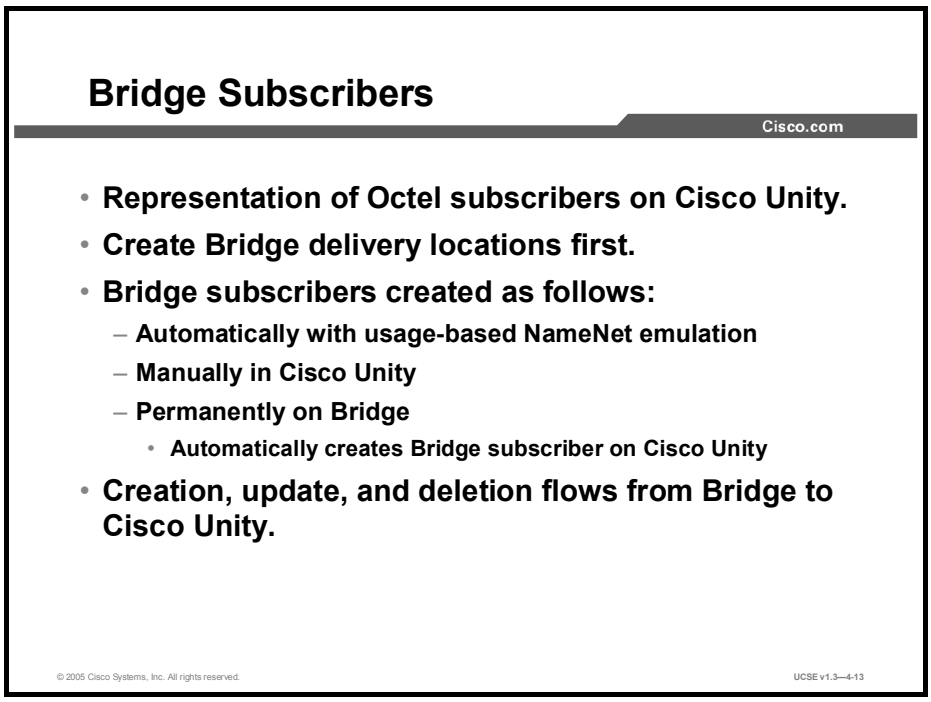
Messaging between the Bridge and Cisco Unity is done over the Internet or any TCP/IP network by using SMTP. The Bridge sends messages to an SMTP server that you specify when configuring the Bridge server. The SMTP server then routes messages to Exchange, which delivers messages to recipient mailboxes.

Messaging Between the Bridge and Octel

Messaging between the Bridge and the Octel servers is done via Octel analog networking. The Bridge masquerades as one or more nodes on the Octel analog network. Voice messages are transmitted between nodes by using ordinary phone connections. When one node calls another by dialing a specified phone number, the originating node transmits a sequence of DTMF tones to identify itself as an Octel node. The destination node then transmits DTMF tones in reply. If the destination node accepts the call, the originating node transmits each voice message by using analog playback, and the destination node records each message and delivers it. To the Octel servers, the Bridge behaves like any other Octel node on the Octel analog network.

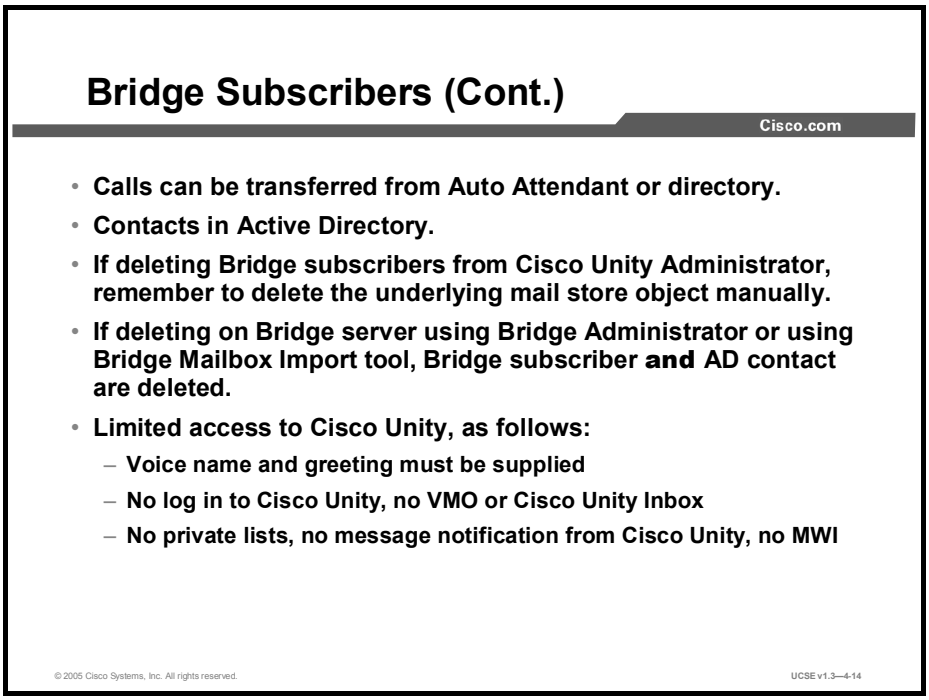
Bridge Subscribers

This topic describes options available and setup procedures for Bridge subscribers.



Bridge subscribers, like Internet, AMIS, and VPIM subscribers, are Cisco Unity subscribers with no mailbox storage on the Exchange mail store. They are a representation on the Cisco Unity system of subscribers on the Octel system. Before creating any Bridge subscribers, you must first create the Bridge delivery locations corresponding to the Octel node on which their mailbox resides.

Bridge subscribers can be created in a number of ways. They can be created automatically through usage-based NameNet emulation, permanently on the Unity Bridge, or manually in Cisco Unity. When entries are created, updated, or deleted via NameNet emulation or permanently at the Bridge, that information flows from the Bridge to Cisco Unity.



Bridge subscribers can receive calls that are transferred either directly from the Auto Attendant or from within the directory. Calls could even be transferred off premises if Cisco Unity and the telephone switch allow it. All Bridge subscribers are represented as Contacts within Active Directory. Other than receiving messages, Bridge subscribers do not have access to other Cisco Unity features, and some sections of the Cisco Unity Administrator are disabled for Bridge subscribers. Bridge subscribers face the following limitations:

- They cannot log in to Cisco Unity by phone to check or send messages.
- They cannot log in to Cisco Unity by phone—nor use the Cisco Unity Assistant—to adjust personal settings.
- They cannot own private lists.
- They cannot set up or receive message notifications.
- They cannot receive message waiting indications.

Before creating a Bridge subscriber, you must first create a Bridge delivery location that corresponds to each Octel node with which Cisco Unity communicates.

Bridge subscribers are automatically created when the Bridge creates usage-based directory entries for the Octel users. You can also create Bridge subscribers manually in Cisco Unity, or create permanent directory entries on the Bridge server, which results in the automatic creation of Bridge subscribers.

There are two ways to delete Bridge subscribers. If you are deleting them from the Cisco Unity Administrator, you must remember to manually delete the underlying mail store object. If you use the Bridge Administrator or the Bridge Mailbox Import tool, the Bridge subscriber account in Cisco Unity and the Active Directory contact information are deleted at the same time.

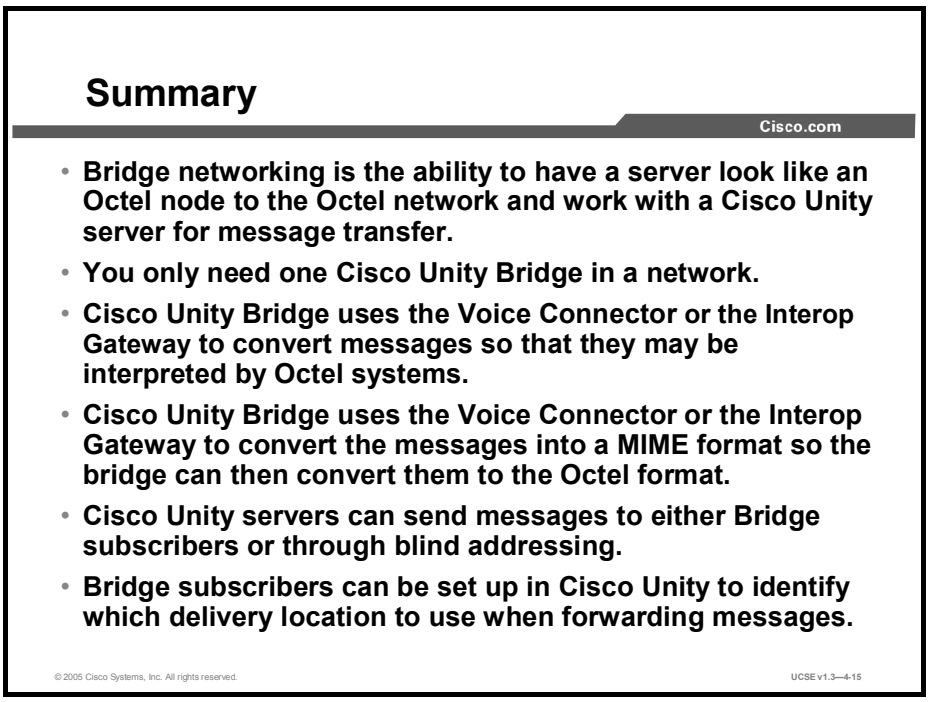
Note that information for creating, updating, and deleting Bridge subscribers is pushed from the Bridge server to Cisco Unity, never the reverse.

If you decide that you want to control the creation of Bridge subscriber accounts, use one of the following approaches:

- Create Bridge subscribers in Cisco Unity by using the Cisco Unity Administrator or the Cisco Unity Bulk Import wizard.
- Create permanent directory entries on the Bridge server by using the Bridge Administrator or the Cisco Unity Bridge Mailbox Import Tool.
- First create the Bridge subscribers in Cisco Unity, and then create corresponding permanent directory entries on the Bridge.

Summary

This topic summarizes the key points discussed in this lesson.



References

For additional information, refer to this resource:

- *Cisco Unity Bridge Networking Guide*

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) How many Cisco Unity servers need to be licensed to use the Cisco Unity Bridge?

A) 0
B) 1
C) 2
D) 3

Q2) The Bridge receives messages from Cisco Unity over which transport?

A) video stream
B) analog
C) senders' x.400 address
D) IP

Q3) Which of the following steps should be done first when creating a Bridge connection?

A) Provide network connectivity between Exchange server with Voice Connector and Cisco Unity Bridge.
B) Extend Active Directory schema for Bridge delivery locations.
C) Install Voice Connector on an Exchange 2000 server.
D) Create UOmni mailbox on Cisco Unity bridgehead server.
E) Customize primary location object.
F) Set addressing and search options.

Q4) What is the minimum number of Bridge servers needed in a network?

A) 1
B) 2
C) 3
D) 4

Q5) Which mailbox is used to process the Bridge messages?

A) UOmni
B) UAmis
C) UMNST
D) POP3

Q6) Which of the following is a way to address messages using an extension with the subscriber and with the Bridge?

A) blind addressing
B) network addressing
C) default addressing
D) mixed addressing

Q7) Before you create a bridge subscriber, you must create a _____.

A) attendant console
B) operator handle
C) delivery location
D) search scope

Quiz Answer Key

Q1) B

Relates to: Bridge Networking

Q2) D

Relates to: Setting Up Bridge Networking

Q3) C

Relates to: Setting up Bridge Networking

Q4) A

Relates to: Locations and Bridge Networking

Q5) A

Relates to: Bridge Networking and the Voice Connector

Q6) A

Relates to: Bridge Message Transfer

Q7) C

Relates to: Bridge Subscribers

Module Self-Check

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

Q1) In a digital networked Cisco Unity dialing domain, any subscriber can message any other subscriber in the organization by _____ and _____.

A) name, location
B) location, extension
C) location, name
D) extension, name

Q2) To connect to an Octel system, which kind of networking is supported between Cisco Unity and the Octel systems?

A) Bridge
B) VPIM
C) SMTP
D) AMIS
E) digital

Q3) Which of the following can be used with Domino networking?

A) VPIM
B) AMIS
C) digital
D) SMTP

Q4) Cisco Unity for Exchange uses which type of networking for Internet subscribers?

A) SMTP
B) VPIM
C) AMIS
D) Bridge

Q5) The Voice Connector is used with which mail store?

A) Domino
B) digital networking
C) Exchange
D) Groupwise

Q6) Multiple sites in the same domain must share _____ to do Cisco Unity digital networking.

A) a single Exchange server
B) a single Cisco Unity server
C) a single SQL server
D) a single directory

Q7) In Exchange 5.5, which component sends the message to the MTA?

A) DIA
B) IS
C) DIID
D) MTA

Q8) When connecting two different Exchange 5.5 sites, which connectors are required? (Choose two.)

A) group connector
B) interchange connector
C) network connector
D) directory replication connector
E) site connector

Q9) Exchange 2000/2003 uses which directory structure to store user names and attributes?

A) DC directory
B) Exchange MTA
C) Active Directory
D) IPlanet Directory

Q10) When a user is added to Cisco Unity, which process does Cisco Unity use to notify Active Directory of the change?

A) AvDSGlobal Catalog Server
B) AVDSAD Monitor
C) AVGaen
D) AVDIRChangeWriter

Q11) Which statement is true about Internet subscribers?

A) Internet subscribers have a local information store.
B) Internet subscribers use digital networking to find the message recipient.
C) Internet subscribers have no local information store.
D) Internet subscribers can control their own greetings.

Q12) The Internet subscriber's voice mail is sent where?

A) to an e-mail server
B) to an AMIS voice-mail server
C) to a Local Exchange server
D) to a VPIM voice-mail server

Q13) The AMIS subscriber's voice mail is sent where?

A) to an e-mail server
B) to another voice-mail server
C) to a Local Exchange server
D) to a VPIM voice-mail server

Q14) Which types of subscribers only use the IP network for message delivery to the destination? (Choose two.)

A) AMIS
B) VPIM
C) Internet
D) Bridge

Q15) Which subscriber has a voice-mail box on an Octel voice-mail system?

A) AMIS
B) VPIM
C) Internet
D) Bridge

Q16) When choosing the subscriber type, which of the following is one of the primary concerns?

A) destination mailbox type
B) local licensing options
C) endpoint networking capabilities
D) analog connectivity
E) digital connectivity

Q17) How many primary location objects can there be?

A) 1
B) 2
C) 3
D) 4

Q18) Which is a requirement for implementing digital networking in a Domino environment?

A) same Exchange site
B) same routing group
C) same AD forest
D) same Notes domain

Q19) Which are optional steps when setting up digital networking? (Choose two.)

A) make dial plan decisions
B) customize primary location object
C) set search options
D) add alternate extensions
E) set up automated attendant transfers

Q20) Which is the correct search option when looking for subscribers that are local to a Cisco Unity server?

A) Active Directory
B) this server
C) all servers
D) managed server list

Q21) A collection of Cisco Unity servers integrated with the same phone system or phone system network can take advantage of which product feature?

A) dialing scope
B) dialing network
C) dialing digits
D) dialing domain

Q22) Which networking options do not use delivery location?

A) digital networking
B) analog networking
C) AMIS
D) servers

Q23) You have to extend the Active Directory schema to set up which Cisco Unity features? (Choose two.)

A) Bridge networking
B) VPIM networking
C) AMIS
D) Cisco Unity

Q24) Which environment is the IMS connector designed to work in?

A) Domino R6
B) Domino R5
C) Exchange 2000
D) Exchange 5.5

Q25) To run DNS, which of the following is needed?

A) Exchange messaging system
B) Window program
C) Exchange program
D) Active Directory

Q26) Which is the first step for setting up an SMTP network between remote Cisco Unity servers?

A) create delivery locations
B) check SMPT connectivity
C) build subscribers
D) extend AD scheme

Q27) Which step can be preformed last when setting up SMPT networking?

A) creating IVS
B) creating Internet subscribers
C) creating dialing domains
D) creating Internet publishers

Q28) How many primary default location(s) are configured when you install Cisco Unity?

A) 1
B) 2
C) 3
D) 4

Q29) Can all the primary locations be deleted with digital networking?

A) no, none can
B) yes, all of them can
C) all but one, the default
D) only the default

Q30) When a message is sent via VPIM, the Voice Connector converts the voice message to which format?

A) MINE
B) MIME
C) DIME
D) TTS

Q31) A voice-mail-only user can pick up messages in which of the following? (Choose two.)

A) by Microsoft Outlook
B) by the Cisco Unity inbox
C) by their cell phone
D) in the mail

Q32) Do both outside and inside callers using the Auto Attendant benefit from the ability to address messages to a subscriber over the telephone?

A) yes
B) no
C) sometimes
D) most of the time

Q33) If remote subscribers receive their messages at an e-mail server, a voice-mail message sent to them will appear as an e-mail with which type of file attachment?

A) WAV
B) MP3
C) audio
D) no file is attached

Q34) Which of the following types of messages can be transferred by VPIM? (Choose three.)

A) video
B) voice
C) text
D) fax

Q35) Which encoding scheme is used by VPIM?

A) G.711
B) G.729
C) G.726
D) G.723

Q36) When installing VPIM, which of the following has to be done?

A) add Bridge subscribers
B) define call handlers
C) enable message caching
D) verify IP connectivity

Q37) To implement VPIM networking, locations should be created on which server?

A) all servers need locations created
B) only on one server
C) only on Bridge server
D) none of the servers need locations defined

Q38) The VPIM Voice Connector converts incoming packets from _____?

A) MAPI to MIME
B) MAPI to SMTP
C) SMTP to MAPI
D) MIME to MAPI

Q39) Which of the following can be used to address a message to a VPIM destination without building a VPIM subscriber?

A) name
B) location ID plus extension
C) extension plus location ID
D) telephone number

Q40) VPIM subscribers show up as which kind of data in Active Directory?

A) users
B) groups
C) contacts
D) containers

Q41) Which types of messages can be transferred by AMIS?

A) video
B) voice
C) text
D) fax

Q42) AMIS voice messages are encoded using which codec?

A) G.711
B) G.729
C) G.726
D) G.723

Q43) When installing AMIS, which of the following has to be done?

A) add Bridge subscribers
B) define call handlers
C) enable message caching
D) verify analog connectivity

Q44) For AMIS networking, locations should be created on which server?

A) All servers need all locations created.
B) Only on one server.
C) Only on bridge server.
D) None of the servers need locations defined.

Q45) Which message stores support AMIS networking? (Choose two.)

A) Exchange 4.7
B) Domino
C) Groupwise
D) Exchange 2000

Q46) How many ways are there to address messages to individuals by using an AMIS-compliant voice messaging system?

A) 1
B) 2
C) 3
D) 4

Q47) AMIS subscribers show up as which kind of data in Domino Names.nsf Notes Address Book (NAB)?

A) users
B) contacts
C) person documents
D) NSF containers

Q48) Which types of messages can be transferred by a Cisco Unity Bridge?

A) video
B) voice
C) text
D) fax

Q49) The Cisco Unity Bridge connects to the PBX via _____ lines.

A) digital
B) serial
C) analog
D) MAN

Q50) When installing the Bridge, which of the following has to be done?

A) install UOmni mailbox
B) define call handlers
C) enable message caching
D) install the event sync server

Q51) For Bridge networking, delivery locations should be created on which server?

A) all servers need all locations created
B) only on bridgehead Cisco Unity server
C) only on one server
D) none of the servers need locations defined

Q52) Which Octel systems are supported by Bridge networking? (Choose two.)

A) Octel 250
B) Octel 2547
C) Octel 300
D) Octel R532

Q53) Bridge subscribers show up as which type of data in Active Directory?

A) users
B) groups
C) contacts
D) containers

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent or better.

Module Self-Check Answer Key

Q1) D

Q2) A

Q3) A, B, C, D

Q4) A

Q5) C

Q6) D

Q7) B

Q8) D, E

Q9) C

Q10) D

Q11) C

Q12) A

Q13) B

Q14) B, C

Q15) D

Q16) A

Q17) A

Q18) D

Q19) D, E

Q20) B

Q21) D

Q22) A

Q23) A, B

Q24) D

Q25) D

Q26) B

Q27) B

Q28) A

Q29) A

Q30) B

Q31) B, C

Q32) A

Q33) A

Q34) B, C, D

Q35) C

Q36) D

Q37) B

Q38) D

Q39) B

Q40) C

Q41) B

Q42) A

Q43) D

Q44) B

Q45) B, D

Q46) B

Q47) C

Q48) B

Q49) C

Q50) A

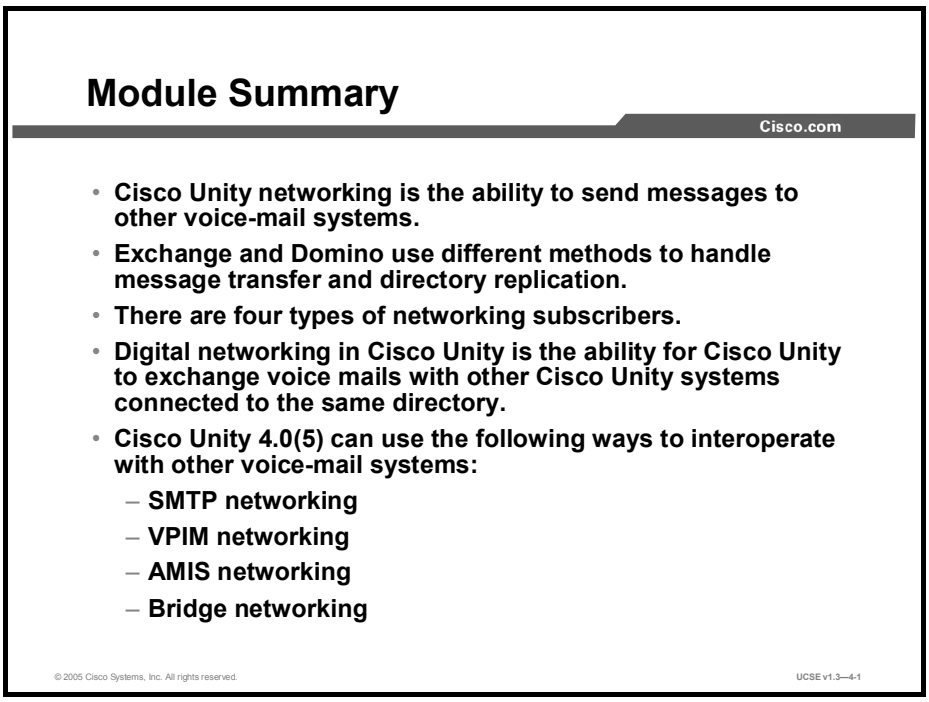
Q51) B

Q52) A, C

Q53) C

Module Summary

This topic summarizes the key points discussed in this module.



Module 5

Using Unified Communications Maintenance and Utilities

Overview

This module describes suggested maintenance procedures and system utilities used to service an efficiently running Cisco Unity system. Troubleshooting procedures to help diagnose any issues with the Cisco Unity system are also described.

Module Objectives

Upon completing this module, you will be able to describe and be able to use the tools for system maintenance, diagnostics, and troubleshooting. This ability includes being able to meet these objectives:

- Describe the recommended maintenance procedures for Cisco Unity
- Describe the utilities and their functions in Cisco Unity
- Describe troubleshooting procedures for Cisco Unity

Lesson 1

Using Cisco Unity Administration Tools

Overview

This lesson describes the administration tools located in the Tools Depot of Cisco Unity. The administration tools are used in importing different types of users into the system, upgrading the system, disaster recovery, and changing many registry settings.

Relevance

Cisco Unity administration tools are important for maintaining and, at times, troubleshooting a Cisco Unity system. Familiarity with these tools makes it easier for you to maintain the Cisco Unity system.

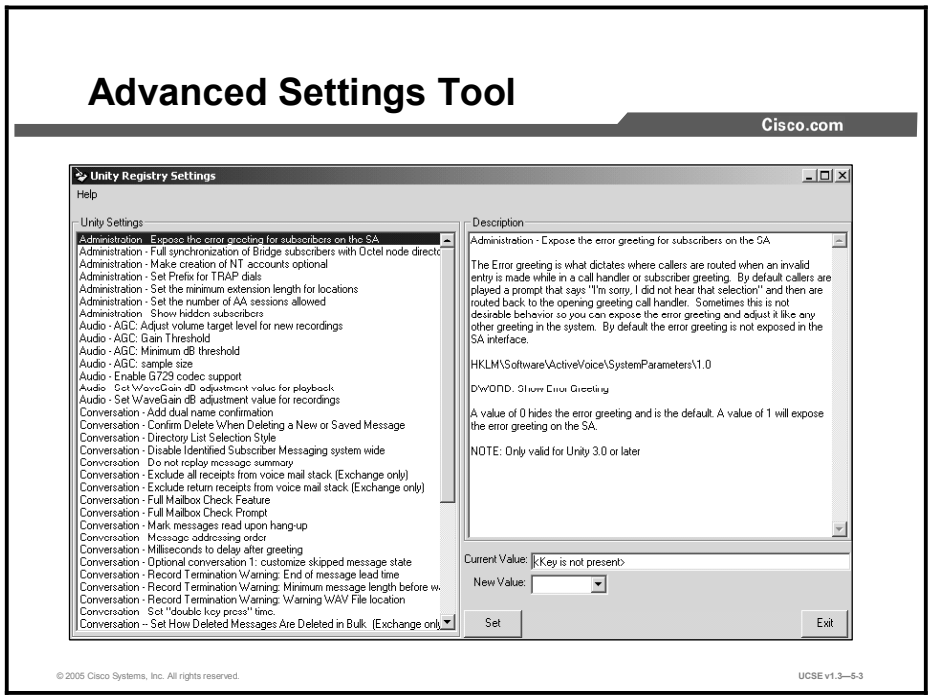
Objectives

Upon completing this lesson, you will be able to describe and use the appropriate tool to import users, upgrade the system, perform disaster recovery, and change registry settings. This ability includes being able to meet these objectives:

- Describe and be able to use the Advanced Settings tool
- Describe and be able to use the Migrate Subscriber Data utility
- Describe the Custom Keypad Map utility
- Describe the Bulk Subscriber Delete utility
- Describe and be able to use the License Viewer utility
- Describe how to uninstall Cisco Unity 3.x and 4.x
- Describe and be able to use the Status Monitor

Advanced Settings Tool

This topic describes the use of the Advanced Setting Tool found in the Cisco Unity Tools Depot.



This is a simple tool that allows users to safely edit many of the hidden registry settings that commonly need to be modified in the field. These are items that are not on the System Administrator interface, and that require users to add or edit keys to the registry.

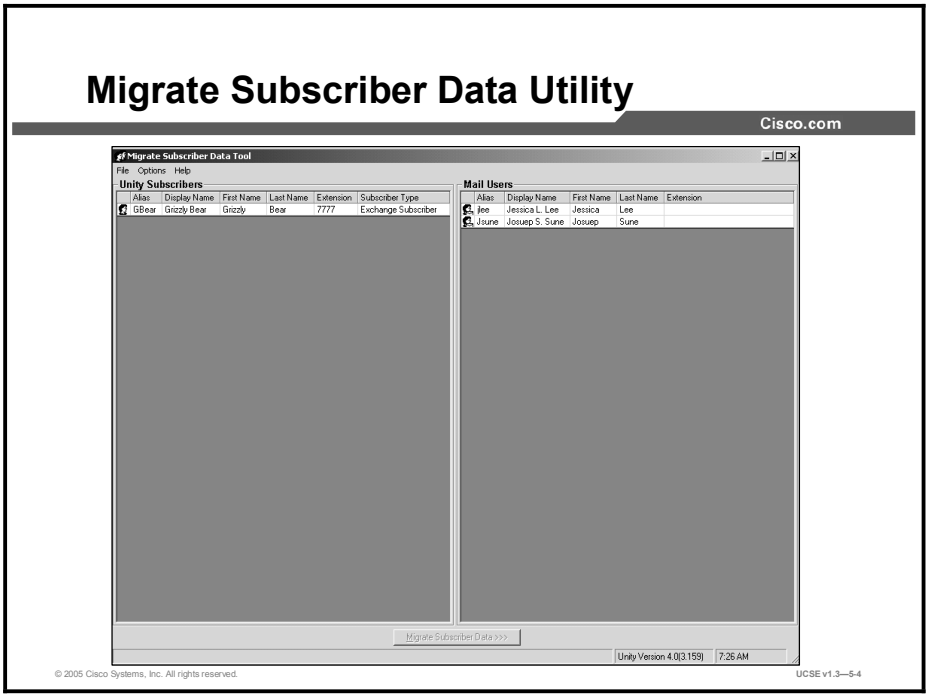
The Advanced Settings Tool prevents potential accidents by forcing specific value ranges, and making sure edits are not applied to Cisco Unity versions that can not handle them. There are only a few settings that are string values that need to be edited free-form. The rest of the settings are limited to a drop-down list of values, or are “key only” values, in which the presence of the key in the registry is sufficient and no value needs to be added.

Other factors about the Advanced Settings Tool are as follows:

- It runs with Cisco Unity version 2.4.6 or later.
- Keys are visible only for those values that are valid to adjust on the locally running system.
- You can add you own keys, but the keys will be overwritten if you update the tool to a later version.

Migrate Subscriber Data Utility

This topic describes the Migrate Subscriber Data utility.



The Migrate Subscriber Data utility allows the Cisco Unity administrator to move subscriber settings from a Cisco Unity subscriber account to a mail user account. Use of this tool allows you to preserve all of the subscriber settings, such as voice name, greetings, private distribution lists, and so on, because these Cisco Unity-specific attributes are added to the mail user account attributes. The tool is useful for moving from a voice-mail-only installation to unified messaging, or for migrating users from another voice-mail system to Cisco Unity (for example, migrating Octel users who have been set up as Bridge subscribers).

For example, imagine you have created two directory accounts for each employee. One of John's accounts is used for voice-mail messages (vJSmith) and the other is used for e-mail (JSmith), and now it is time to move John's voice-mail account. You bring up the Migrate Subscriber Data utility and select John's voice-mail subscriber account and his e-mail account, and click the Migrate Subscriber Data button. The result is that John's subscriber record is modified; his e-mail account directory ID is copied over his voice-mail directory ID. His alias, display name, and first and last name are also transferred from his e-mail account to his subscriber record. His primary call handler alias is modified to match his alias. These modifications take place within the Cisco Unity database, not the directory. His previous subscriber directory account is modified to remove the subscriber-specific settings, but the directory account is not deleted. When you exit the utility, the Cisco Unity database is synchronized with the directory. When the directory synchronization is complete, any new voice-mail messages John receives will be delivered to his e-mail account.

ExMerge

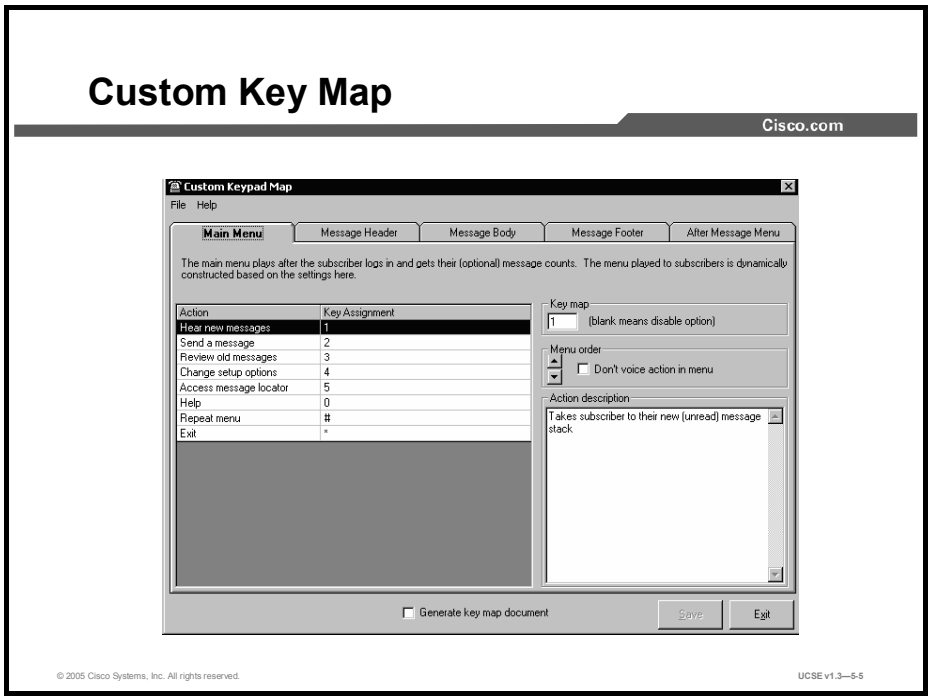
You may use the ExMerge program to extract data from mailboxes on a Microsoft Exchange server and then merge this data into mailboxes on another Microsoft Exchange server using ExMerge. The program copies data from the source server into personal folders (.pst files) and then merges the data, in the personal folders, into mailboxes on the destination server. The ability to merge data to and from an Exchange server makes this program an invaluable tool with a variety of uses, especially during disaster recovery. The program can also replace existing data instead of merging new data if specified by the Administrator. ExMerge has some limitations. Please read the tools documentation before using this program.

You need to keep the following in mind as you use ExMerge:

- Messages are not automatically removed from the System Attendant mailbox. You must do that manually.
- If the original message was forwarded with a different subject, the ExMerge utility cannot delete the message based on the original message subject line, or MTS-ID.
- If the Item Retention option is turned on, the message may be available for recovery on the Outlook client.

Custom Keypad Map

This topic describes the Custom Keypad Map utility.

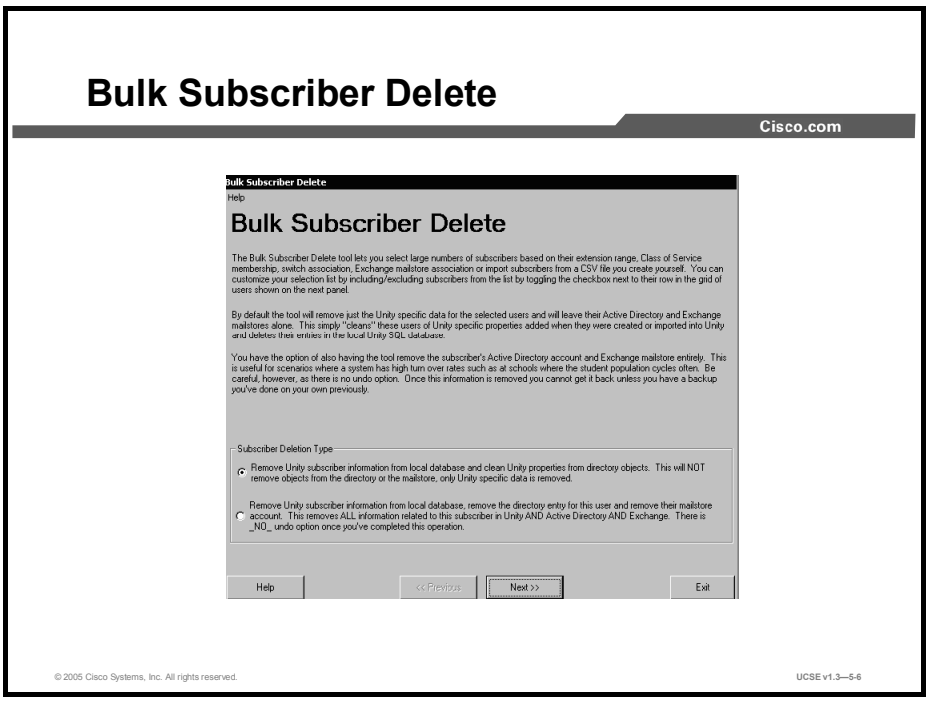


The Custom Key Map tool allows you to edit the key mappings associated with the “Custom Keypad Mapping“ conversation which can be assigned to subscribers in the conversation page in the Cisco Unity System Admin screens. It is important to remember that this tool will not replace, nor affect, any of the default key mappings that exist on the conversation page. The new key maps generated by using this utility will be in addition to the default mappings.

This tool allows for either a single- or two-digit key press. It may be helpful to some customers who do not wish to totally change the user message retrieval experience when replacing a third-party voice-mail product with Cisco Unity.

Bulk Subscriber Delete

This topic describes the Bulk Subscriber Delete utility.



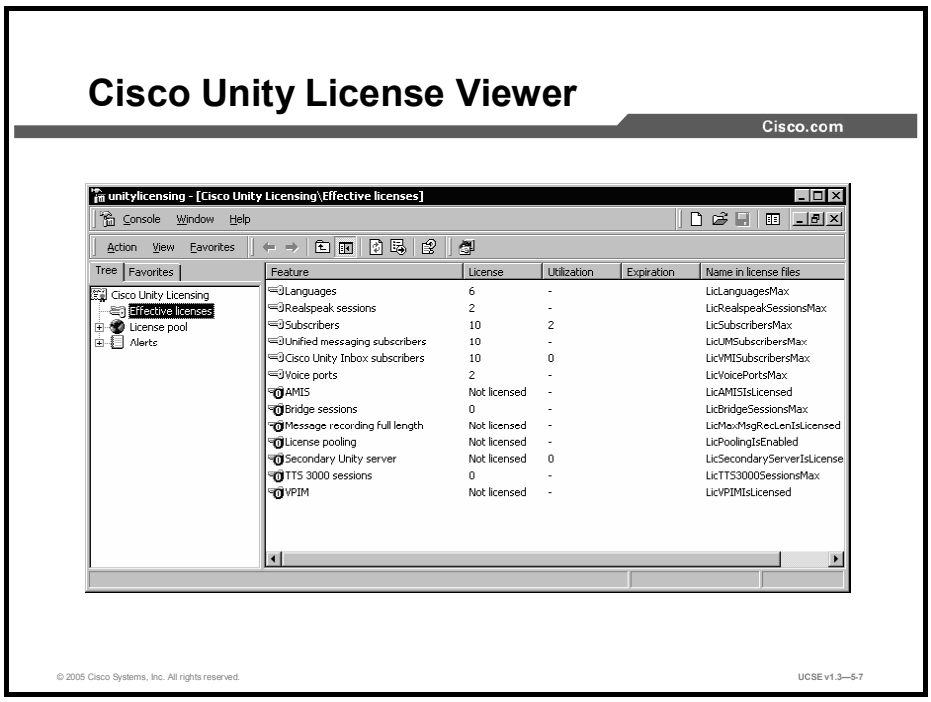
The Bulk Subscriber Delete utility replaces the Remove Subscriber Properties tool which was designed to allow administrators to remove Cisco Unity subscriber properties from Active Directory accounts. In addition to allowing administrators to remove the Cisco Unity subscriber properties from Active Directory, the utility can also be used to entirely remove the subscriber account from Cisco Unity, including the subscriber Active Directory and Exchange accounts. This is useful for scenarios in which a system has high turnover, such as universities where the student population cycles frequently.

The Bulk Subscriber Delete utility must be run on the Cisco Unity server and functions only with Cisco Unity versions 4.0(3) or later. The utility will work only with Exchange 5.5, 2000, and 2003. Domino is not supported.

When you select to remove the directory and mail store information associated with an Exchange 5.5 installation, only the Exchange 5.5 mailbox will be removed. It will still be necessary to access Active Directory to remove the associated Active Directory account.

Cisco Unity License Viewer

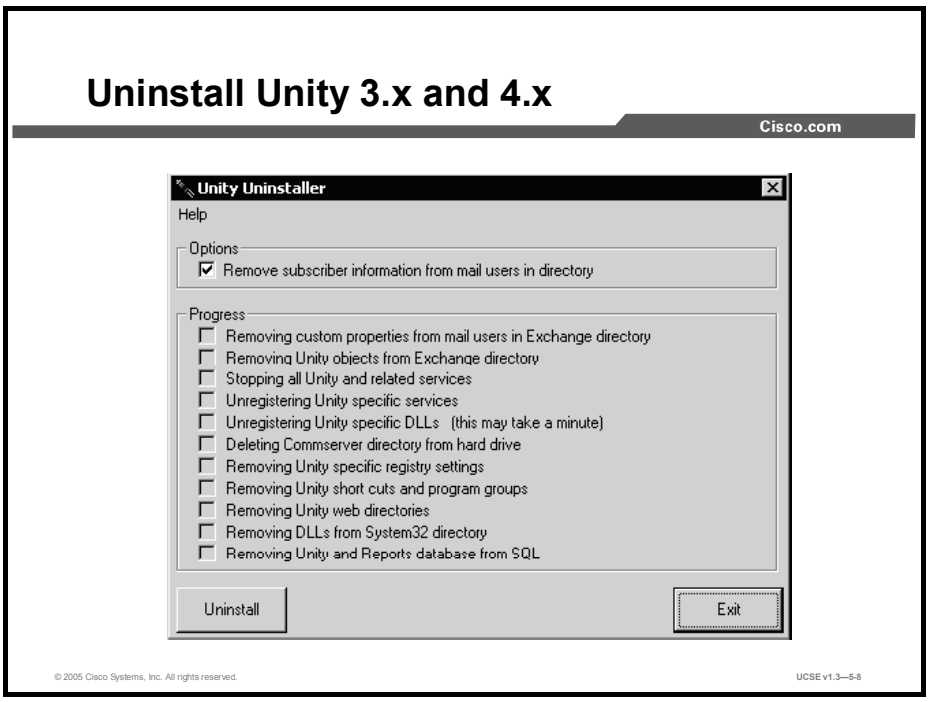
This topic describes the Cisco Unity License Viewer utility.



The License Viewer utility is a handy way to see the current licenses for your Cisco Unity system. FLEXlm licensing controls many aspects of your Cisco Unity configuration, such as how many languages you are allowed, voice ports, text-to-speech sessions, and so on. If you try to install a new feature or add another language and the system does not allow you, it may be because you are not licensed for it. In this case, you would need to purchase additional licenses. When you receive the new license file, you would run the License wizard and then as a check, look at the License Viewer to confirm that your new licenses are active.

Uninstall Cisco Unity 3.x and 4.x

This topic describes how to uninstall Cisco Unity 3.x and 4.x.



The Unity Uninstaller utility will remove all Cisco Unity-related files, registry settings, and most directory items in Exchange and Active Directory from your system. You will need to manually remove three accounts (Example Administrator, Example Subscriber, Installer) and three distribution lists (System Event Messages, All Subscribers, and Unaddressed Messages) from your system after uninstalling. After that, you should be able to install a clean version of Cisco Unity, after rebooting your server.

This version of Uninstaller works only with Cisco Unity 3.0(1) and later. There is a separate version for the 2.x uninstall.

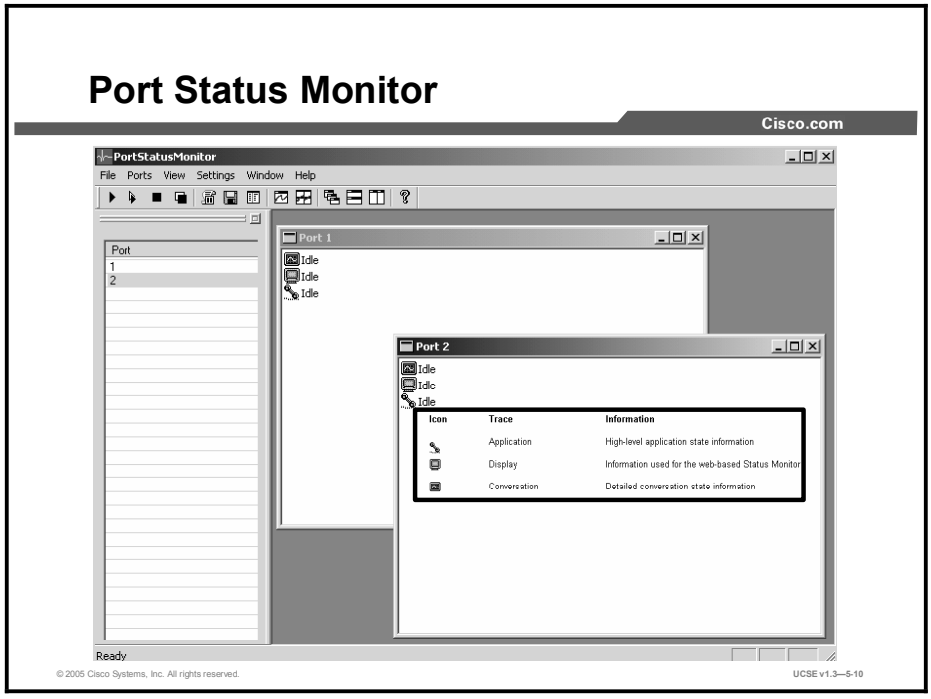
This tool does *not* remove Dialogic, network management system (NMS), Cisco Telephony Service Providers (TSPs), or WAV drivers. Before running the Cisco Unity Uninstall utility, you should manually remove these items. The Unity Uninstaller also does not remove Active Fax.

Running the Uninstaller utility causes the following actions:

- Cisco Unity-specific data is removed from all Cisco Unity subscribers on the server. This does not have any affect on the normal mail-user properties for subscribers in Exchange—only the Cisco Unity-specific extensions are removed. High-level items that are not Cisco Unity-specific, such as the recorded voice name, are left intact. Only subscribers associated with the local Cisco Unity server will have their Cisco Unity-specific properties removed. As a result, if you have multiple Cisco Unity servers installed into the same Exchange site, the uninstall should not affect users associated with the other systems.
- All location objects associated with the local Cisco Unity server are removed from the directory entirely.
- The Cisco Unity database information is removed from Structured Query Language (SQL). This includes all call handlers, class of service (CoS) definitions, interview handlers, restriction tables, and so on.
- All Cisco Unity-specific services are stopped and then removed from the Service Control Manager.
- All Cisco Unity-related registry settings are removed.
- The Commserver directory and all its subdirectories are removed from the hard drive.
- The Cisco Unity program group is removed.
- The links to the system administrator, Status Monitor, and the “part 2 setup” are removed from the desktop.
- The Tray Status application is removed from the startup group.
- All the Cisco Unity-specific web information for the system administrator, Auto Attendant (AA), and Status Monitor sites is removed from the wwwroot directory.
- Several Cisco Unity-specific dynamic link library (DLL) files are removed from the WinNT\System32 directory.

Port Status Monitor

This topic describes the use of the Port Status Monitor.



The Cisco Unity Port Status Monitor allows you to view activity, in the form of port activity messages, on one or more Cisco Unity voice ports in real time.

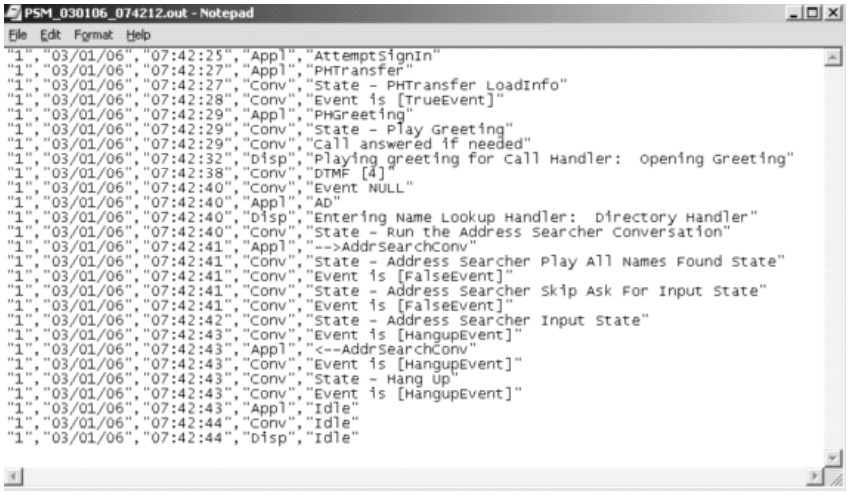
Activity on each port is displayed in a separate window. Each window can display any or all of three different traces:

- **Application trace:** High-level application state information
- **Display trace:** Information used for the web-based Status Monitor
- **Conversation trace:** Detailed conversation state information

Traces are displayed in status monitor windows in the order in which they are received from Cisco Unity. Port Status Monitor is a great tool to use to verify that Cisco Unity is dialing out Message Waiting Indicator (MWI) requests and pager notifications, as well as when you need to monitor larger port applications.

Port Status Monitor Log

Cisco.com

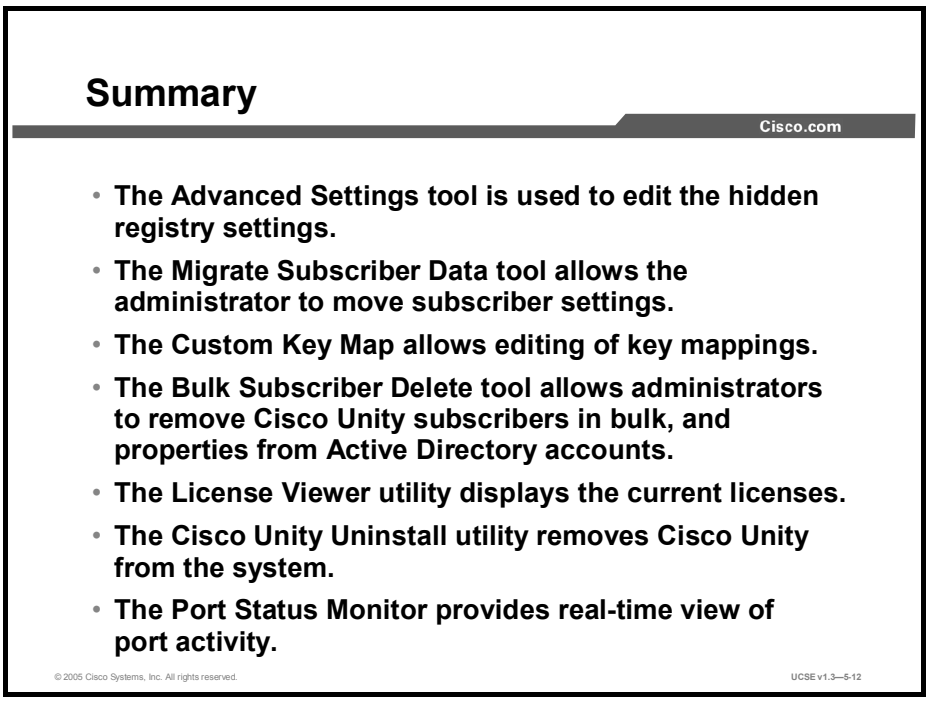


The figure provides an example of a port status monitor log. The columns in the log output file are:

- **Port:** The voice port being logged
- **Date:** The date the trace was received
- **Time:** The time the trace was received
- **Trace:** The trace received—application, display, or conversation
- **Info:** The actual text of the trace received

Summary

This topic summarizes the key points discussed in this lesson.



References

For additional information, refer to these resources:

- *Cisco Unity Troubleshooting Guide*
- *Cisco Unity System Administration Guide*

Next Steps

After completing this lesson, go to:

- Cisco Unity Audio Management Tools

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) Match the description of the maintenance and utility tool with the name of the tool.

A) Edits many of the hidden registry settings
B) Preserves all of the subscriber settings
C) Removes subscriber properties from Active Directory accounts
D) View current Cisco Unity licenses
E) Removes all Cisco Unity-related files, registry settings, and most directory items

_____ 1. Migrate Subscriber Data utility

_____ 2. License View utility

_____ 3. Advanced Settings tool

_____ 4. Bulk Subscriber Delete

_____ 5. Uninstall Cisco Unity 3.x and 4.x

Q2) The Advanced Settings tool is used to edit _____.

A) registry keys
B) user accounts
C) e-mail settings
D) voice-mail settings

Q3) The Migrate Data Subscriber utility allows the administrator to _____.

A) see the current licenses for your Cisco Unity system
B) remove Cisco Unity subscriber properties from Active Directory accounts
C) move subscriber settings from a Cisco Unity subscriber account to a mail-user account
D) safely edit many of the hidden registry settings

Q4) The Bulk Subscriber Delete tool is needed to remove users when _____.

A) users need to be removed
B) the Cisco Unity server was removed without a proper uninstall
C) users have violated their privileges
D) employees change departments

Q5) The Cisco Unity License Viewer is a handy way to _____.

A) see the current licenses for your Cisco Unity system
B) remove Cisco Unity subscriber properties from Active Directory accounts
C) move subscriber settings from a Cisco Unity subscriber account to a mail user account
D) safely edit many of the hidden registry settings

Q6) The Cisco Unity Uninstaller utility is useful for _____.

A) uninstalling SQL
B) removing users
C) removing user groups
D) uninstalling Cisco Unity

Q7) The Cisco Unity Status Monitor _____.

A) displays license information for the server
B) is used to test call handler applications
C) is used to display user activity

Q8) The Custom Key Map _____.

A) changes the order in which messages are played
B) can be used to edit Cisco Unity prompts
C) can be used to change keystrokes that subscribers use during message retrieval
D) can be used on Cisco Unity 4.0(1) or later

Quiz Answer Key

Q1) A-3, B-1, C-4, D-2, E-5

Relates to: Unity Administration Tools

Q2) A

Relates to: Advanced Settings Tools

Q3) C

Relates to: Migrate Subscriber Data Utility

Q4) B

Relates to: Bulk Subscriber Delete

Q5) A

Relates to: Cisco Unity License Viewer

Q6) D

Relates to: Uninstall Unity 3.x and 4.x

Q7) C

Relates to: Status Monitor

Q8) C

Relates to: Custom Key Map

Lesson 2

Using Cisco Unity Audio Management Tools

Overview

This lesson describes various audio management tools available through the Tools Depot utility. The audio management tools are necessary for modifying audio levels and quality of Cisco Unity prompts and greetings. This is also where you can change the codec (G.711 or G.729 Annex A) in which Cisco Unity stores messages.

Relevance

There may be times when you have to change the codec on an existing system. After an upgrade there may be a need to change the audio levels. Understanding the audio management tools will give you the ability to make these and other changes.

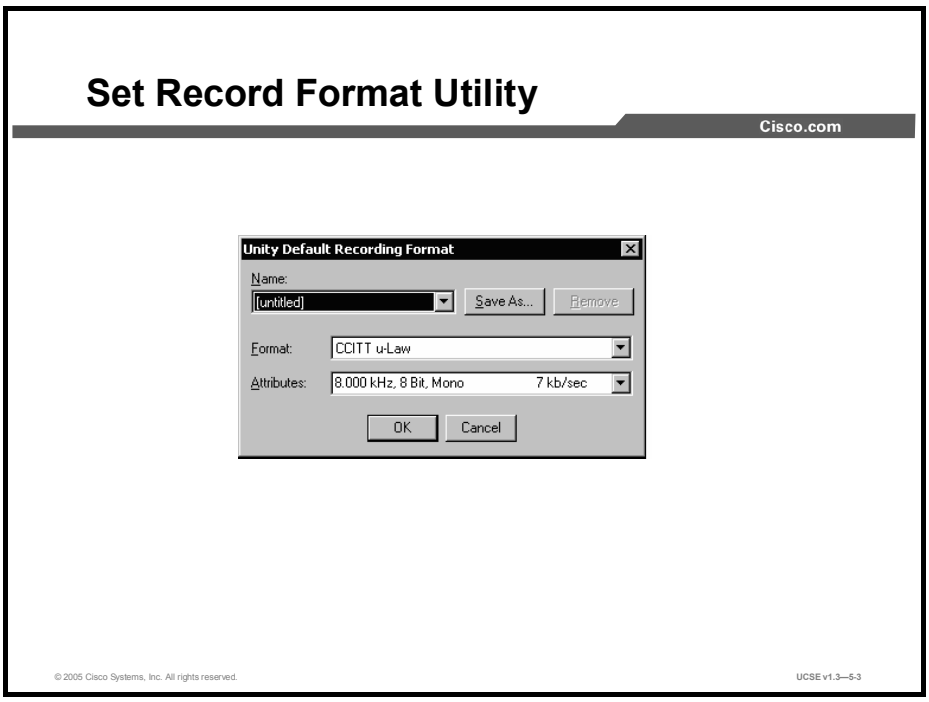
Objectives

Upon completing this lesson, you will be able to select and describe the appropriate tool for modifying audio levels, quality of prompts, and changing the codec. This ability includes being able to meet these objectives:

- Describe and be able to use the Set Record Format utility
- Describe and be able to use the Set Wave Format utility
- Describe and be able to use the Wave Gain utility
- Describe and be able to use the Codec Checker
- Describe and be able to use the Set Prompt Speed utility

Set Record Format Utility

This topic describes how to use the Set Record Format utility.

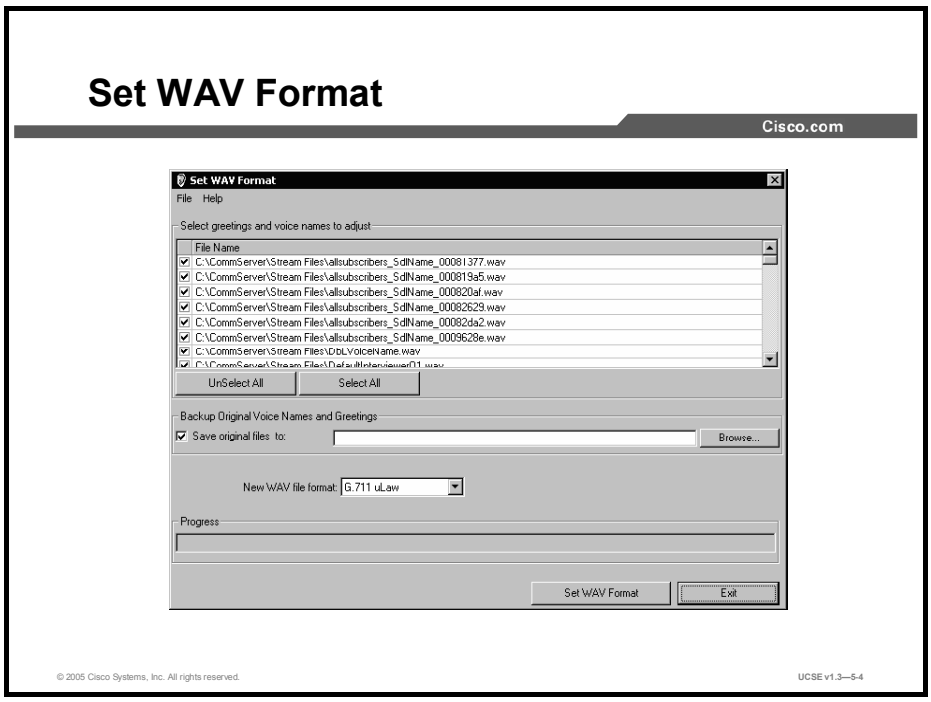


The Set Record Format utility allows you to choose any sound codec installed on the Cisco Unity server as a default recording format that Cisco Unity uses for all recordings. By default, the record format is set to 8 KB mu-law (codec G.711). G.711 or G.729 can be selected and sample rates can be adjusted. Remember that this affects all recordings on Cisco Unity. It is not possible to select specific formats for individual users, ports, WAV file types, and so on. It will be necessary to restart Cisco Unity before the recording format changes take effect.

Be sure to select a codec that will work for all clients. The audio quality of the G.711 codec is noticeably different than the G.729 codec. If you send a voice mail to a user who will be accessing that message via their desktop messaging client, they will need the same codec installed on their local system to play it.

Set WAV Format

This topic describes the Set WAV Format utility.



The Set WAV Format tool allows you to convert all the standing greetings and voice names on a Cisco Unity server to a selected WAV codec. You can choose from G.711 U-law, G.711 a-law, or G.729 Annex A.

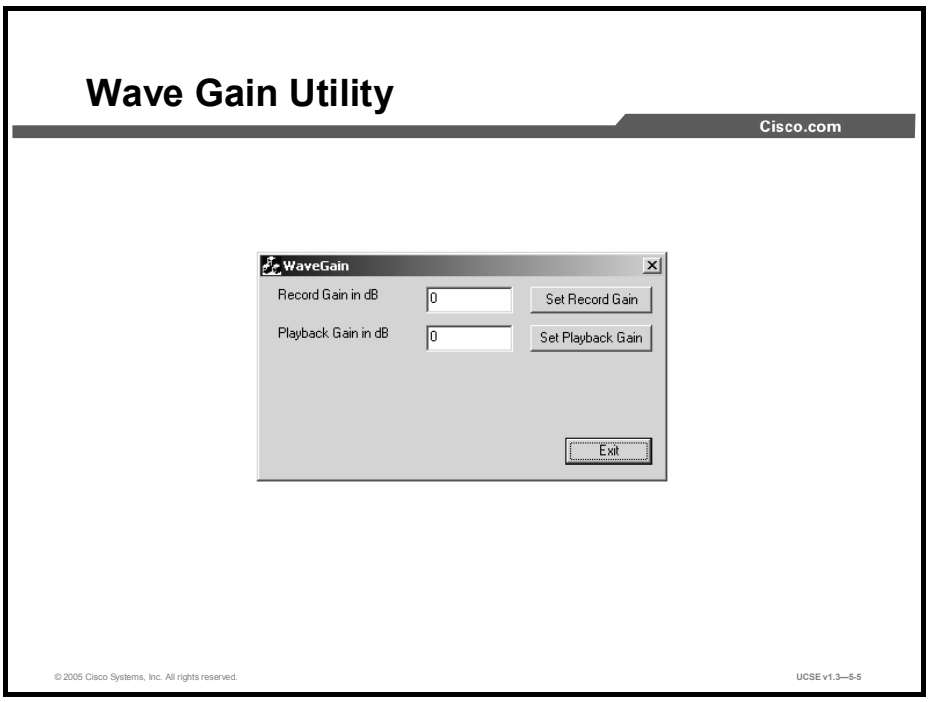
If a site has selected to change recording formats from G.711 (default) to G.729 Annex A, for example, you may want to use this tool to convert all standing greetings and voice names into G.729 Annex A. While Cisco Unity will convert from G.711 to G.729 Annex A (and vice versa) on the fly using software, this is CPU-intensive and it is often desirable to have all WAV files in the same format to prevent this.

Converting WAV files from G.711 to G.729 and back to G.711 will degrade sound quality, because the formats are compressed differently and you lose a certain amount of information during the conversion. You should back up your greetings and voice names before changing their format. If the WAV files are damaged or do not sound good, you can recover some or all of them. The Set WAV Format tool has a built-in backup and restore mechanism for all greetings and voice names. Simply select a directory to copy greetings to using the **Browse** button and check the **Save original files to** option. Before modifying the WAV files, the tool will copy all greetings and voice names to the target directory. To restore these greetings, select the **Restore backed up greetings and voice names** option from the File menu.

This tool does *not* convert standing messages in subscriber mailboxes.

Wave Gain Utility

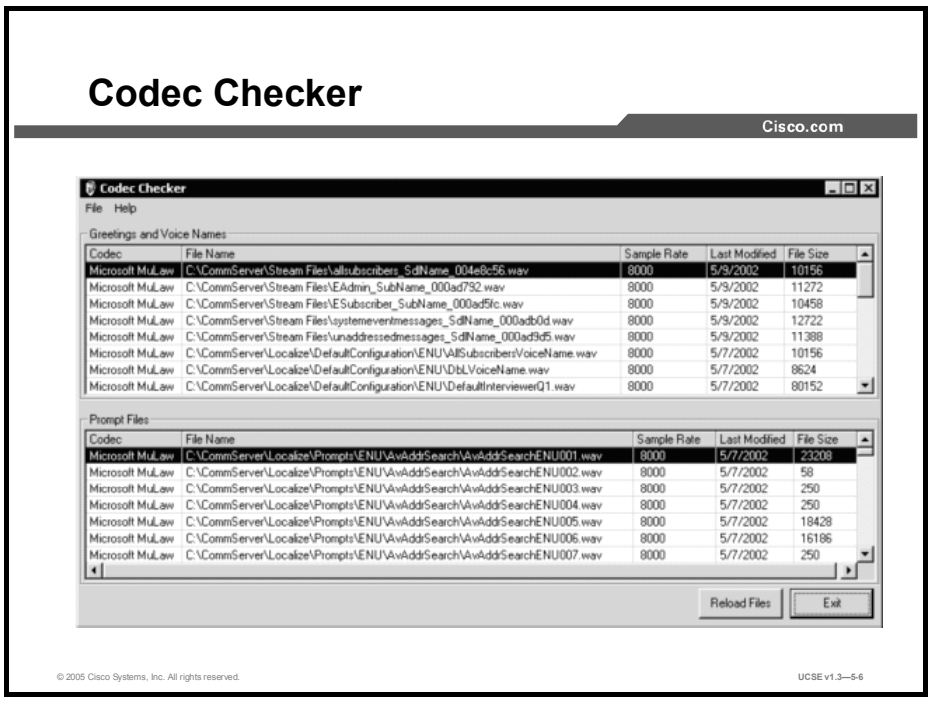
This topic describes the Wave Gain utility.



The Wave Gain utility allows you to adjust the overall volume adjustment for new recordings or for playbacks when using Cisco Call Manager. You enter the increase (positive numbers) or decrease (negative numbers) in decibels. The changes take place immediately while Cisco Unity is running, so you can quickly adjust the playback and record levels until you are satisfied with them. Once you have found the values you want, you need to write those into the registry manually or use the Advanced Settings Tool to do this for you. You must edit the registry for the values to be in effect the next time you restart your system, otherwise Cisco Unity will return to its preset defaults on a restart.

Codec Checker

This topic describes the Codec Checker application.



Cisco Unity supports recording prompts and voice names in various codecs and ships the standard prompt set in G.711 and G.729 Annex A formats. After successive upgrades, prompt set applications, codec changes, and so on, it can be useful to get a full accounting of which WAV files are recorded in which format.

The Codec Checker application provides a full list of all greetings, voice names, and system prompts and indicates which codec they are recorded in, their sample rate, and file size. If multiple languages are installed, all prompt files for all languages will be shown. With many greetings and multiple languages installed, it can take a few minutes to process all the files at startup time.

Once the file information is loaded, you can sort the columns to find what you are interested in, or you can export the information to CSV files for further review. The prompt file information, and greetings and voice name information, are exported separately. These options are found under the File menu.

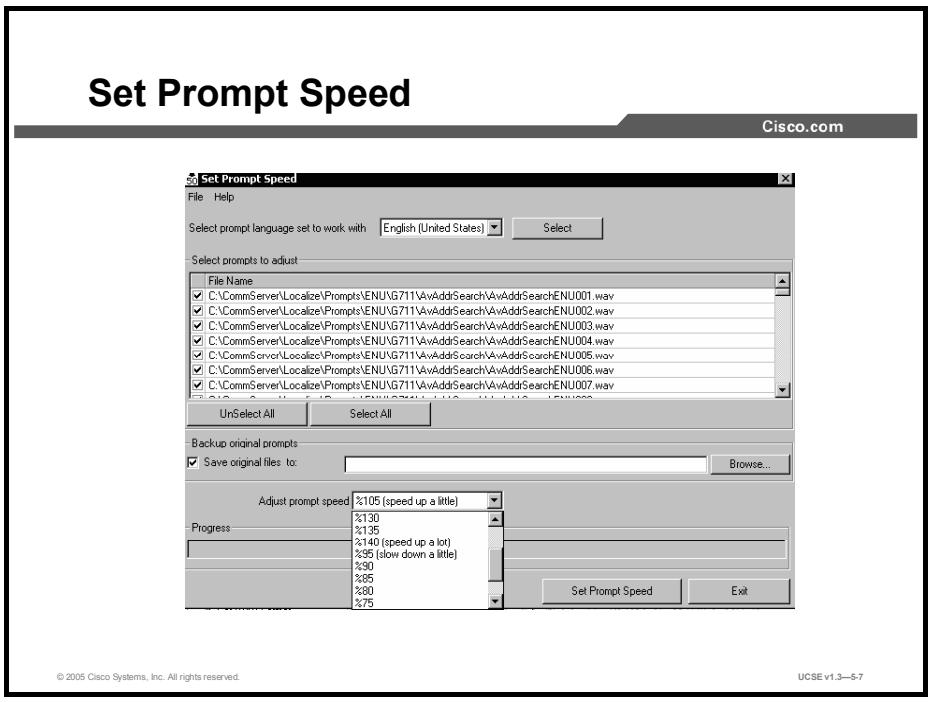
If a codec is encountered that the tool does not recognize, it will be reported as “Unknown Codec=xx,” where xx is the ID pulled from the RIFF header of the WAV file. If you run into this in the field, report the ID to Cisco and it can be added to the list of codec names the tool will recognize. All supported codecs as of Cisco Unity 3.1(3) are included in the tool.

In the sample screen shown in the figure, note the following:

- The Sample Rate column is shown in bytes/sec. The mu-law codec is sampling at 8 KB/sec.
- The Last Modified column is the date the file was last updated. This can be used specifically for spotting customer recorded prompts in the field.
- The File Size column is in bytes.

Set Prompt Speed

This topic describes how to change the Cisco Unity prompt play speed.

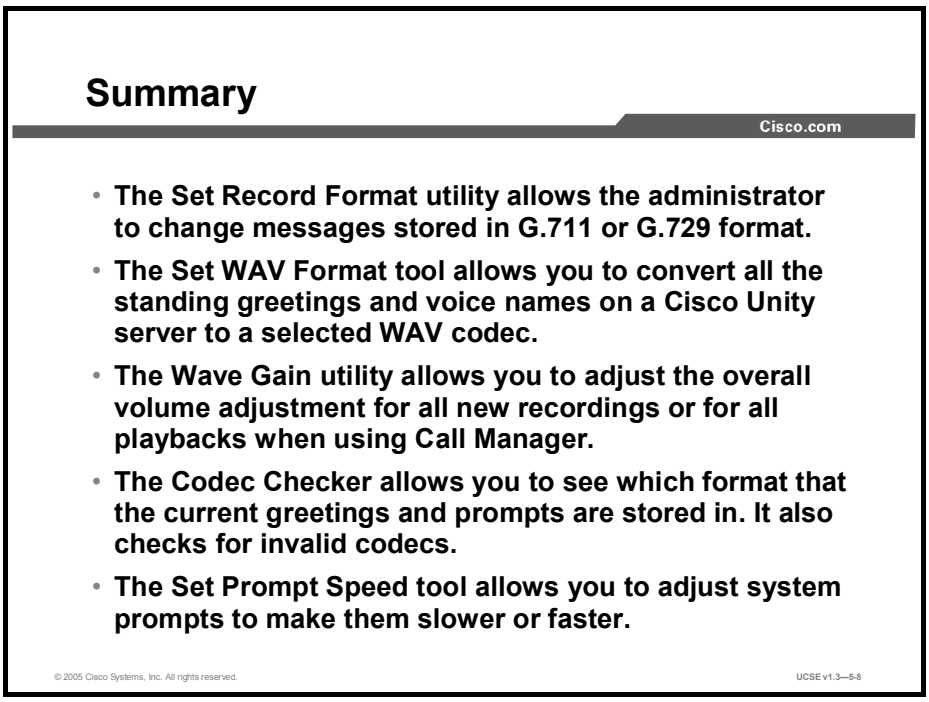


The Set Prompt Speed utility is used to adjust the system prompts to make them play either slower or faster, depending on site preference. This is useful in those situations in which the customer feels that the Cisco Unity system is too slow. Speed can be increased up to 140 percent of default speed, or slowed down to 60 percent of default speed. As a precaution, the tool will prompt you for a location to back up the existing prompts.

The Set Prompt Speed utility can only be on the Cisco Unity server and not through Windows Terminal Services. The Cisco Unity system must be off line as well. Because this is a prompt tool, it does not change or affect recorded greetings and voice names. It will only adjust prompts recorded in the G.711 codec.

Summary

This topic summarizes the key points discussed in this lesson.



References

For additional information, refer to these resources:

- *Cisco Unity Troubleshooting Guide*
- *Cisco Unity Administration Guide*

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) The Wave Gain utility _____.

A) displays the codec for WAV files
B) sets overall volume for WAV files
C) converts voice name codecs
D) defines default codecs

Q2) The Set Record Format utility _____.

A) displays the codec for WAV files
B) sets overall volume for WAV files
C) converts voice name codecs
D) defines default codecs

Q3) The Codec Checker application _____.

A) displays the codec for WAV files
B) sets overall volume for WAV files
C) converts voice name codecs
D) defines default codecs

Q4) The Set Wave Format utility _____.

A) displays the codec for WAV files
B) sets overall volume for WAV files
C) converts voice name codecs
D) defines default codecs

Q5) The Set Prompt Speed tool _____.

A) changes the playback speed of recorded voice names
B) changes the playback speed of recorded greetings
C) changes the playback speed of prompts recorded in G.729 Annex A codec
D) changes the playback speed of prompts recorded in G.711 codec

Quiz Answer Key

Q1) B, Sets overall volume for WAV files.

Relates to: Wave Gain Utility

Q2) D, Defines default codecs.

Relates to: Migrate Subscriber Data Utility

Q3) A, Displays the codec for WAV files.

Relates to: Codec Checker Application

Q4) C, Converts voice name codecs.

Relates to: Set Wave Format

Q5) D

Relates to: Set Prompt Speed

Lesson 3

Using Cisco Unity Diagnostic Tools

Overview

This lesson describes the Cisco Unity diagnostic tools available in the Cisco Unity product. Diagnostic tools help in setting traces and logging debug information for resolving Cisco Unity problems.

Relevance

The diagnostic tools assist in maintaining a properly running Cisco Unity system. The Database Walker utility, for example, checks the integrity of your database, and the diagnostic traces will log additional information to help Cisco Technical Assistance Center (TAC) to troubleshoot any issues with your system.

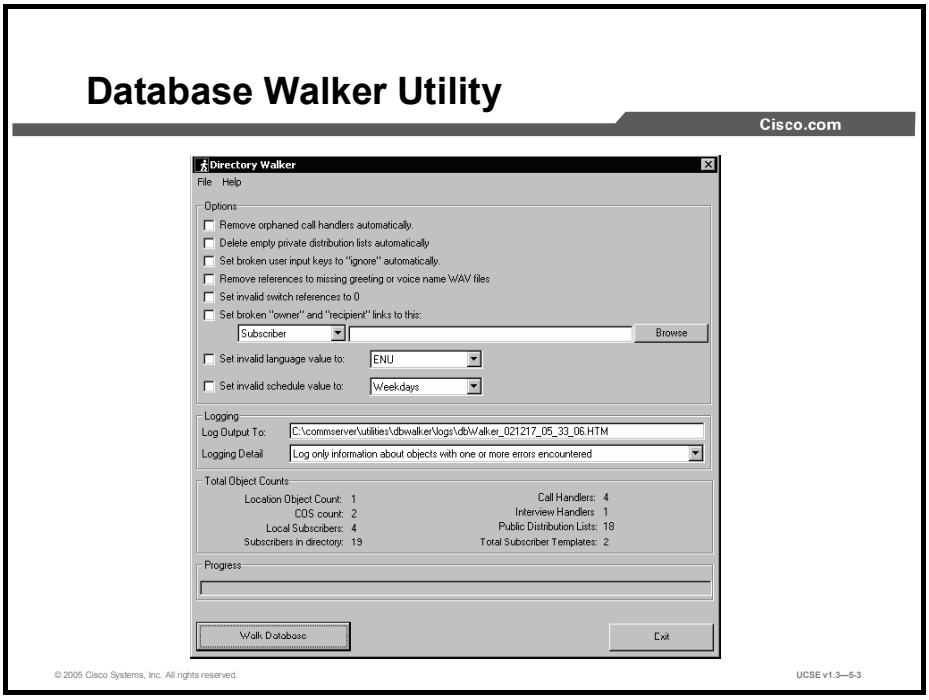
Objectives

Upon completing this lesson, you will be able to select and describe the appropriate tool for setting traces and logging debug information. This ability includes being able to meet these objectives:

- Describe and be able to use the Database Walker utility
- Describe and be able to use the diagnostic traces available
- Describe and be able to use the SysCheck utility
- Describe and be able to use CUPID
- Describe and be able to use the Directory Access Diagnostics
- Describe and be able to use the Cisco Unity Diagnostic Viewer

Database Walker Utility

This topic describes the Database Walker utility.



The Database Walker (DbWalker) utility “walks” the Cisco Unity database and makes a series of checks on all call handler, subscriber, subscriber template, interview handler, locations, and directory handler objects in the database. If there is a problem, the string “error” will appear in red in the output HTML. Warning strings in yellow that start with “warning” are also logged for items that you should check on but are not necessarily problems. If an item is automatically fixed, a string that starts with “fixed” will be in green directly under the error to indicate what was done. When the utility is complete, a dialog box will pop up letting you know it is finished and telling you how many errors and warnings were encountered in the process. You can search the output file for the string “error” or “warning” and you will be taken to each problem in the log. Brief explanations of the problems encountered will usually appear in the log. Be sure to read them in their entirety to determine what you should do about them, if anything.

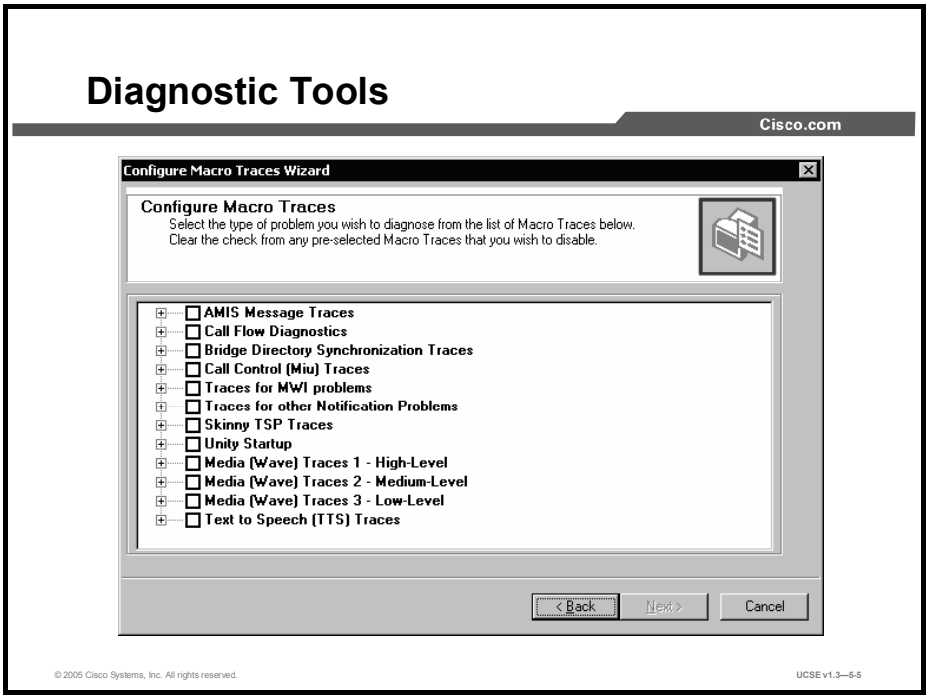
If you are running the Database Walker utility for the first time, you should set the utility to make no automatic fixes the first time you run it. Once it has completed, read through the log to see what errors, if any, have been found. Once you understand what is in the log, you can run the utility again, turning on the options necessary to fix things automatically.

Some problems are logged as errors and fixed automatically (for example, if the standard contact rule or greeting rule has been disabled, it will be enabled again). Some problems are fixed optionally if you indicate **OK** (for example, orphaned call handlers are removed if you check the option to do so at the top of the form). Other problems cannot be fixed automatically and you will need to intervene manually.

The Logging Detail drop-down list box can be set to show information about all objects checked during the database walk, or you can choose to limit the output to only those objects that encounter one or more errors (default). Each time you press the **Walk Database** button, a new output file is generated and stored in the /logs directory where you installed DbWalker. To quickly view the /logs directory, select **File > View Log Directory** from the menu. When DbWalker runs, it will automatically delete any logs in this directory older than ten days.

Diagnostic Tools

This topic describes the diagnostic traces available.



The Cisco Unity diagnostic tool allows the creation and viewing of diagnostic log files in order to troubleshoot problems. It allows the system administrator or TAC staff to selectively run diagnostic traces at the following two levels:

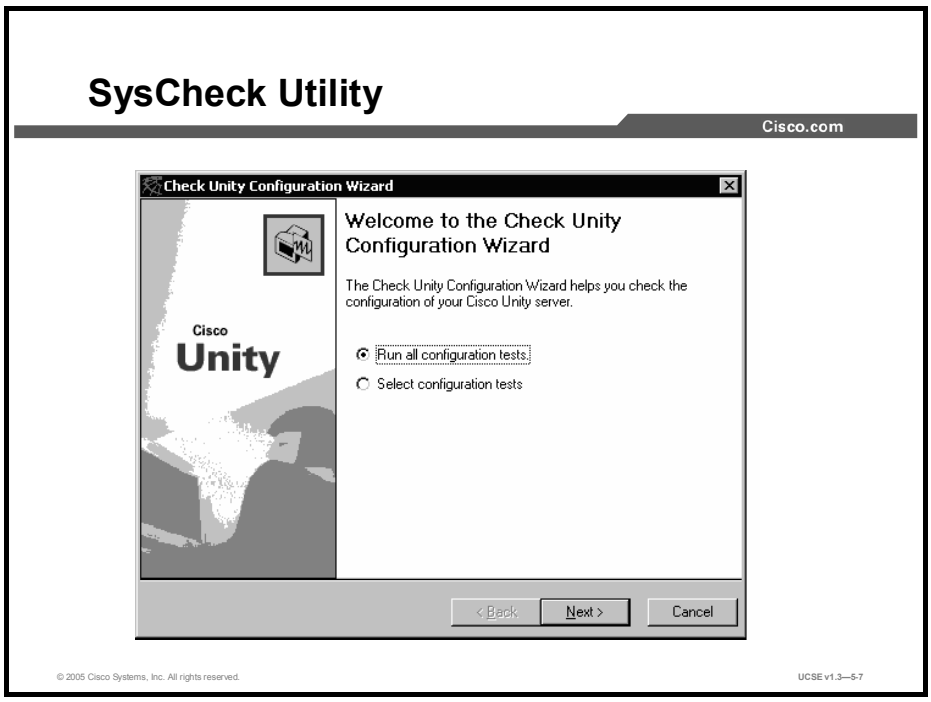
- **Macro Traces:** These are collections of component traces that help diagnose problems such as message waiting indicator and system problems.
- **Micro Traces:** These are the individual component traces. Each component has up to 32 traces that can be individually selected.

The Cisco Unity diagnostic tool also allows you to perform the following tasks:

- **Create new log files on demand**. This makes troubleshooting problems easier. When a problem can be reproduced reliably, you can close all existing log files and create new log files prior to reproducing the problem. This eliminates many unnecessary and unrelated items from the logs.
- **Configure log settings**. You can adjust the maximum disk space allowed for all diagnostic log files. The default setting is 400 MB. The Logging Properties screen also allows the system administrator to disable all diagnostic output by clearing the Diagnostic Output check box. You can also change the location of the log files.
- **Gather standard logs**. This option provides the ability to quickly gather all or selected Microsoft Windows and Cisco Unity logs.
- **Disable all traces**. This is a quick way to return diagnostic logs to their default settings after troubleshooting efforts are complete.
- **View the Event Log**. The Event Log files for either the local computer or another computer can be viewed and exported.

SysCheck Utility

This topic describes the SysCheck utility.



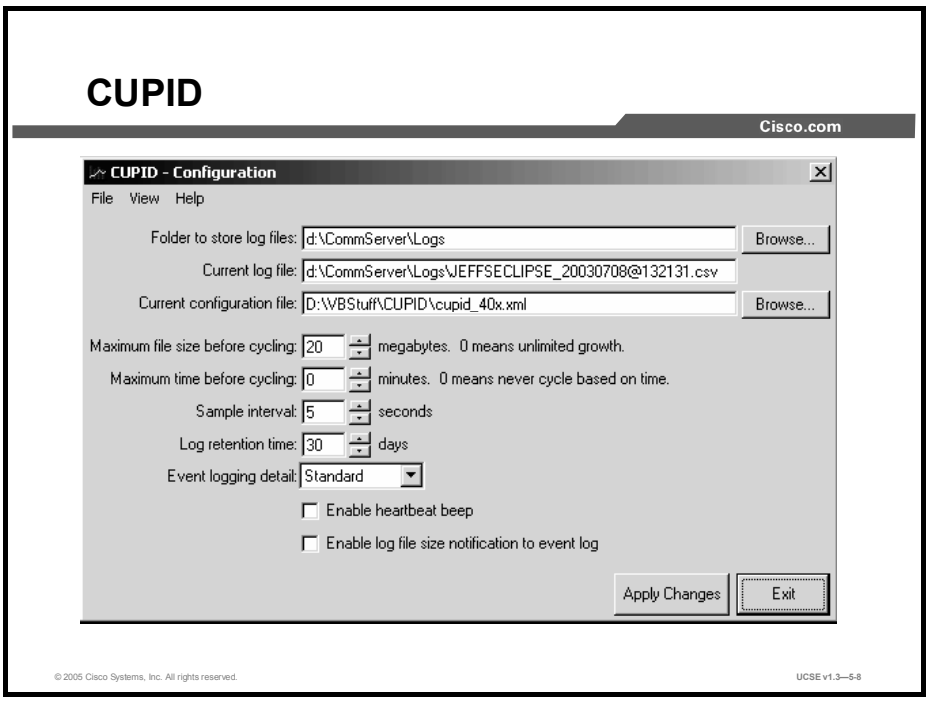
The SysCheck tool is used to help troubleshoot difficulties when the Cisco Unity installation program is not able to complete due to missing rights and permissions. This is the same tool used by the setup application itself to determine if the account running Cisco Unity setup has all the rights necessary to complete the task. Running SysCheck directly will give more detailed information about the source of the failure and can assist in resolving the problem.

The SysCheck tool can be run prior to installation, directly from the Cisco Unity installation CDs, or after installation to check if rights and permissions have been removed from the Cisco Unity service account, and also to check for basic database configuration issues.

To check for database inconsistencies, however, you should use the DbWalker tool. SysCheck is primarily a rights-checking application.

CUPID

This topic describes the Cisco Unity Performance Information and Diagnostics (CUPID) tool.



CUPID is a performance and diagnostic information collection utility for Windows 2000. At its core, CUPID is an NT service that communicates to the performance subsystem of the Windows operating system, and collects data based on the counters specified in an extensible markup language (XML) configuration file. CUPID is available in Tools Depot for Cisco Unity version 4.0(3) and later.

A configuration document used for CUPID consists of an XML document that implements a single CounterSet element with several Counter child elements that define the counters to collect. The configuration files included with the CUPID installation represent the latest recommended performance counters to collect when running a performance test. By default, CUPID will look for a default configuration file at: C:\%SYSTEMROOT%\System32\Cupid_default.xml. If this file is not available, another configuration file will need to be specified. Review the configuration document for the specific needs of the system under test. For example, additional counters may be needed to monitor a third-party backup or antivirus solution, in addition to normal messaging activity.

Menu Options

File

You can select from the following options under the File drop-down list:

- **Install Service:** This option will install the CUPID service and start it running. By default, the service is set to automatically start when the server is started. You can set it to manual start in the Service Control Manager applet. This option will be disabled if the service is already installed.
- **Remove Service:** This will remove the CUPID service and all its corresponding registry settings. When you remove the service, most of the options on the user interface will be disabled until you install the service again.
- **Start Service:** This will force the CUPID service to start. If the service is already started, this menu option will still be available to you—the interface does not know if the service is currently running, only if it is installed.
- **Stop Service:** This will force the CUPID service to stop. This option is always available if the service is installed, regardless of its current running state.
- **Cycle Log:** This option will immediately cycle the current log and start a fresh log.

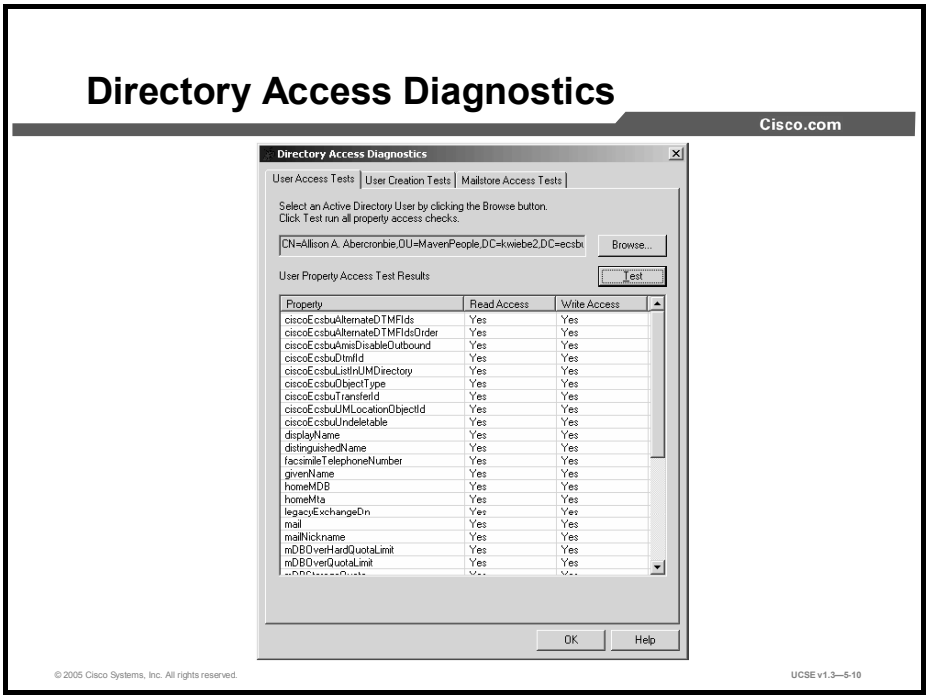
View

You can select from the following options under the View drop-down list:

- **Log Directory:** This will open File Explorer to the current directory selected for CUPID to write log files to.
- **Current Log File:** This will open a grid view of the Comma-Separated Values (CSV) file currently being used by the CUPID service. All columns and rows are shown. If the file is very large, it may take a minute to open.
- **Selected Log File:** This option lets you browse for CSV files, starting in the log output directory. Once you select a CSV file, the file is displayed in a grid view.
- **Refresh:** This forces a reread of the data in the registry, including, most notably, the current log file.

Directory Access Diagnostics

This topic describes the Directory Access Diagnostics tool.



The Cisco Unity Directory Access Diagnostics (DAD) tool checks the Cisco Unity directory service account permissions to import, manage, or create a single Active Directory user object.

DAD also checks the Cisco Unity message store service account permissions on Microsoft Exchange 2000 and Exchange 2003 mail stores.

DAD provides three basic tests:

- User access test
- User creation test
- Mailstore access test

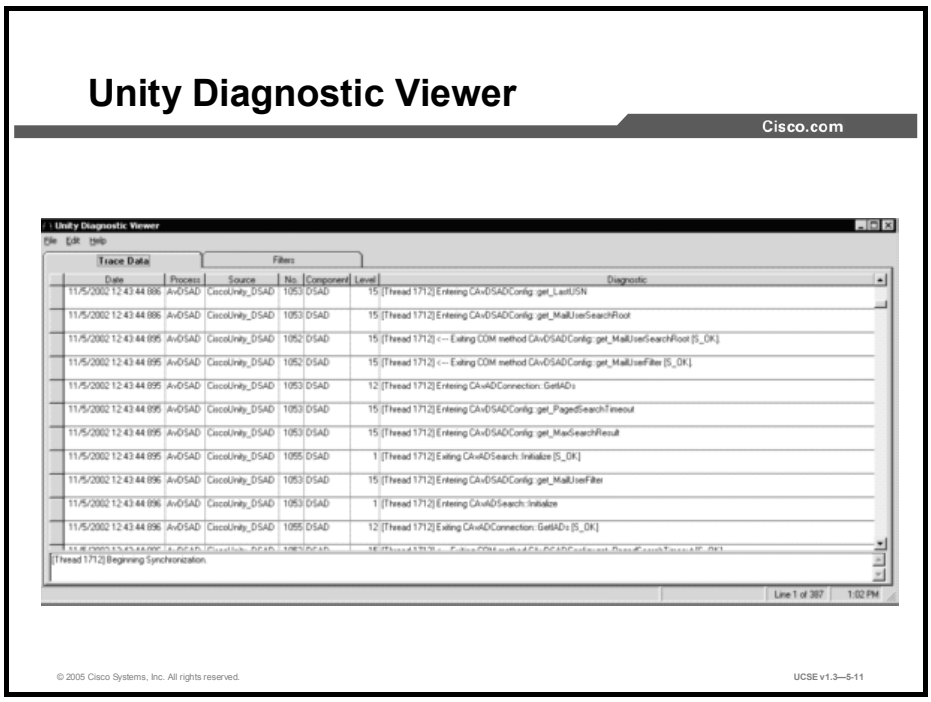
DAD is for use with Cisco Unity deployed in a Microsoft Exchange 2000 or Exchange 2003 environment only.

DAD must be run on the Cisco Unity server and is designed for use with Cisco Unity 3.1 and later.

To use DAD, you must log in to the Cisco Unity server as the account configured as the logon account for either the Cisco Unity AvDSAD or administrator. DAD will not run if you are logged in as any other user.

Cisco Unity Diagnostic Viewer

This topic describes the Cisco Unity Diagnostic Viewer.

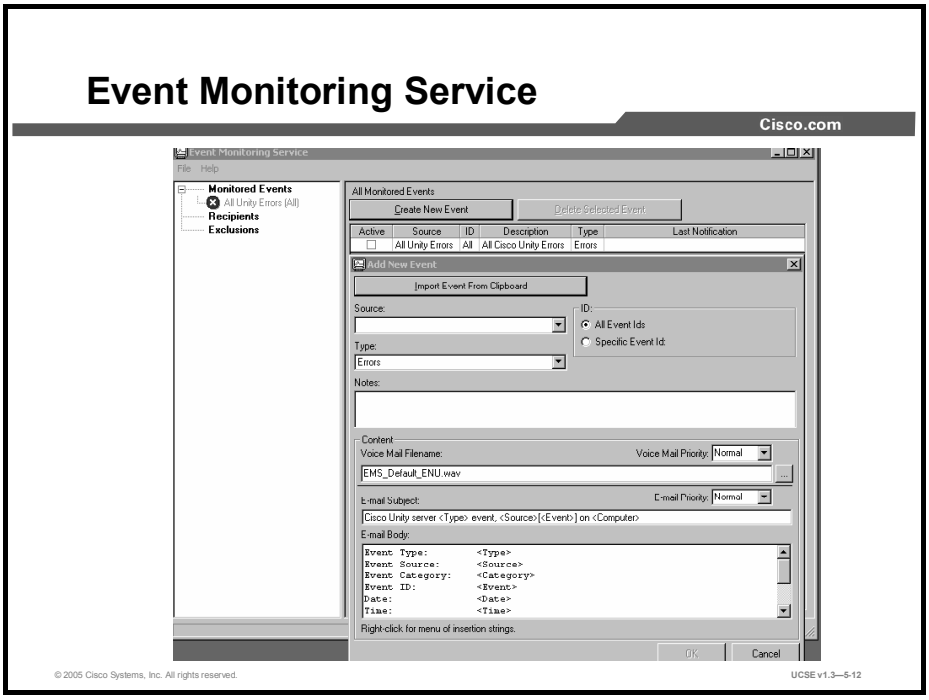


The Cisco Unity Diagnostic Viewer (UDV) is a utility for viewing the output from Cisco Unity diagnostics. This tool allows you to filter out extraneous diagnostics that may not be relevant to the problem being investigated. The UDV works in conjunction with the Gather Logs wizard in the Cisco Unity Diagnostic Tool. A new option in the Unity Diagnostic Tools in Cisco Unity 4.0 is to gather all of the logs over a specified time range.

You can launch the UDV directly from the Gather Logs wizard in the UDT, by selecting **Open Logs in Viewer** on the final page of the wizard. Selecting this option brings up the new UDV with the diagnostics gathered by the Cisco Unity Diagnostic Tool. Alternately, you can launch the UDV from Tools Depot and open any CSV file generated by the UDV Gather Logs wizard.

Event Monitoring Service

This topic describes the Event Monitoring Service.



The Event Monitoring Service (EMS) provides basic notification capabilities when specific events are written to the event logs. You can use this tool to watch for errors on the Cisco Unity server and receive notifications via voice mail or e-mail. Configuration of the EMS involves defining the events to monitor for and creating the recipients that will receive notification of events. The EMS comes with only one predefined monitoring event: All Unity Errors. If this event is enabled, this will provide notification for all Cisco Unity generated event log errors.

There are three components to the EMS, as follows:

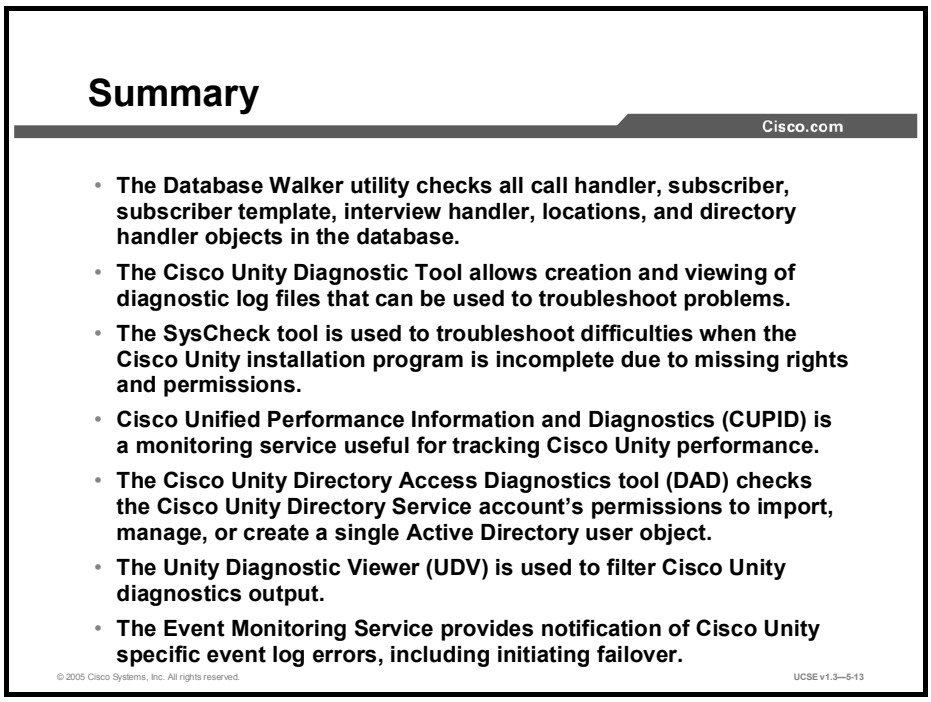
- CsEmsSvc.exe: The Windows service that monitors the event logs and generates notifications
- EMSAdmin.exe: The administration tool
- EMSDB.MDB: The database that contains all of the configuration settings and monitored event information

EMS can also be used with the Cisco Unity failover option. One of the recipients of an error event can be failover. If you select failover as a recipient of an error event, you are telling the EMS you want it to initiate a failover on that event. Obviously you should use this type of notification with extreme caution and create a unique failover recipient notification that is only used for very specific Cisco Unity error events.

The EMS requires Cisco Unity 3.0(1) or later and must be run on the Cisco Unity server.

Summary

This topic summarizes the key points discussed in this lesson.



References

For additional information, refer to these resources:

- *Cisco Unity Troubleshooting Guide*
- *Cisco Unity System Administration Guide*

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) Database Walker has the ability to automatically fix errors that it finds. Which are some of the errors it can fix? (Choose two.)

A) delete unused distribution lists
B) delete empty private lists
C) set valid language
D) set all schedules
E) reset invalid switch references

Q2) Which types of traces can be captured by Cisco Unity?

A) macro and micro
B) macro traces only
C) micro traces only
D) Skinny traces only

Q3) Which tool can help in troubleshooting installation problems?

A) Call Viewer
B) DbWalker
C) SysCheck
D) ATM
E) CUDL

Q4) Match the description of the Unity Diagnostic tool with the name of the tool.

A) used to determine if the account running Cisco Unity setup has all the rights necessary to complete the task
B) monitoring service useful for tracking Cisco Unity performance
C) replaces the diagnostic log functionality in Maestro Tools
D) checks the Cisco Unity Directory Service account's permissions to import, manage, or create a single Active Directory user object
E) checks on all call handler, subscriber, subscriber template, interview handler, location, and directory handler objects in the Cisco Unity database
F) allows the user to filter out extraneous diagnostics when viewing logs

_____ 1. Database Walker utility

_____ 2. SysCheck utility

_____ 3. Directory Access Diagnostics

_____ 4. CUPID

_____ 5. Diagnostic Tools

_____ 6. Cisco Unity Diagnostic Viewer

Quiz Answer Key

Q1) AE

Relates to: Database Walker Utility

Q2) A

Relates to: Diagnostic Tools

Q3) C

Relates to: SysCheck Utility

Q4) A-2, B-4, C-5, D-3, E-1, F-6

Relates to: Diagnostic Tools

Lesson 4

Using Cisco Unity Switch Integration Tools

Overview

This lesson discusses the available switch integration tools located in the Tools Depot of Cisco Unity.

Relevance

The importance of the switch integration tools cannot be overstated. The tools greatly aid in the troubleshooting of the integration of Cisco Unity with a telephone system. If the integration is not set up correctly, Cisco Unity may not function properly—callers cannot leave messages and users cannot retrieve messages.

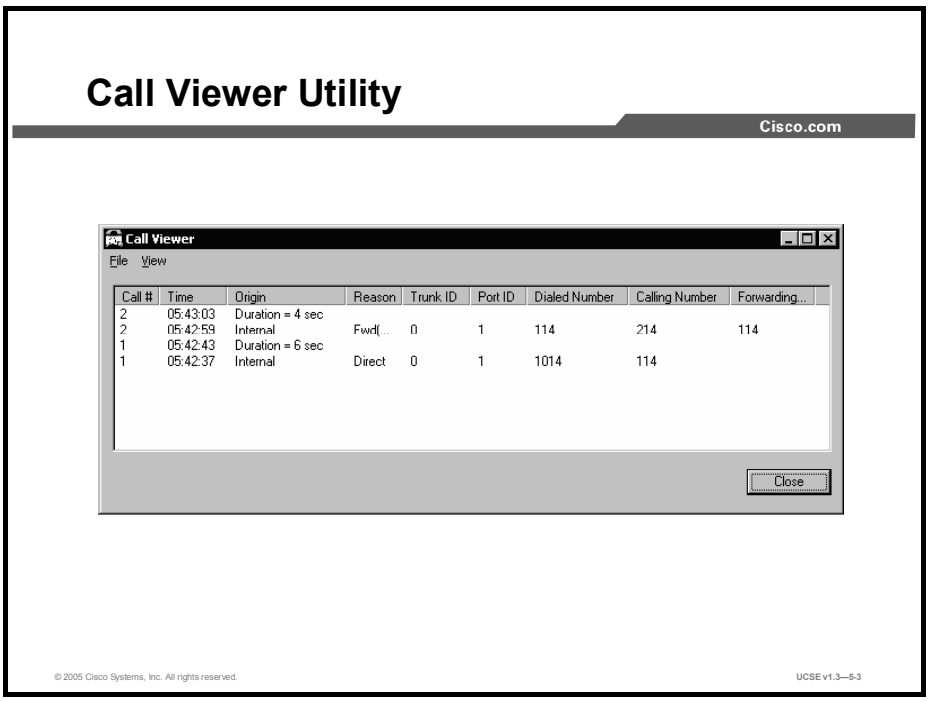
Objectives

Upon completing this lesson, you will be able to select and describe the appropriate tool for troubleshooting the integration of Cisco Unity with a telephone system. This ability includes being able to meet these objectives:

- Describe and be able to use the Call Viewer utility
- Describe and be able to use the Edit Switch utility
- Describe and be able to use the Integration Monitor

Call Viewer Utility

This topic describes the Call Viewer utility.



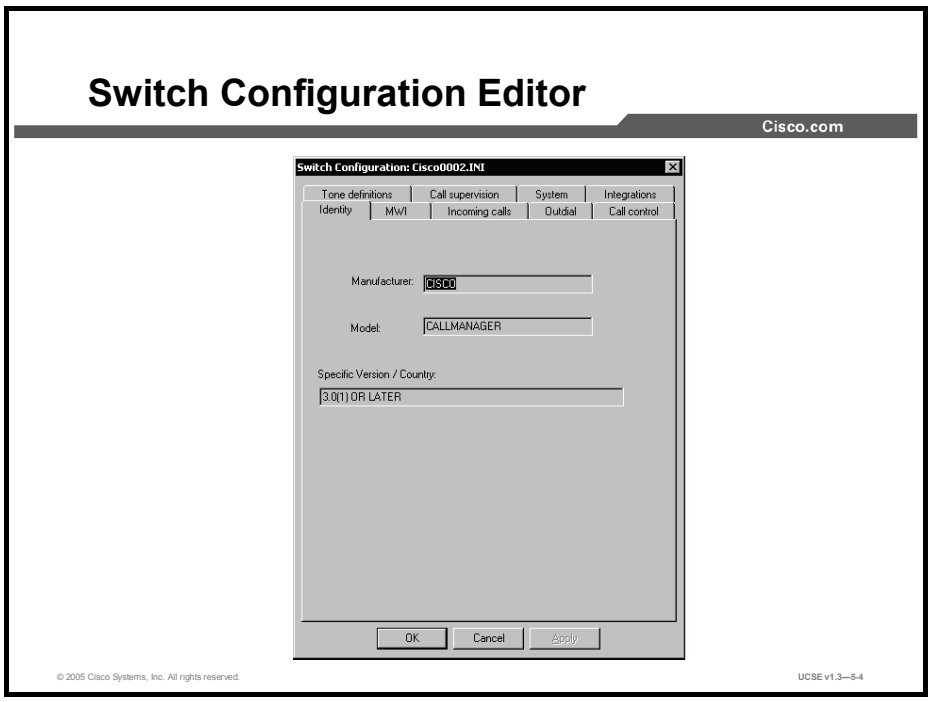
The Call Viewer application shows basic call information for incoming calls on an IP integration. The incoming call information displayed can be used to troubleshoot call routing rules you have generated in Cisco Unity. Any information not displayed in Call Viewer is not being received from the switch integration for that call.

There is an “always on top” option on the View menu that is especially handy when editing and testing new call-routing rules in the System Administrator. You can have the Call Viewer visible while testing your new rule values.

You can also save the information to a log file if, for example, Cisco Technical Assistance Center (TAC) wants to review the call data.

Switch Configuration Editor

This topic describes the Switch Configuration Editor.



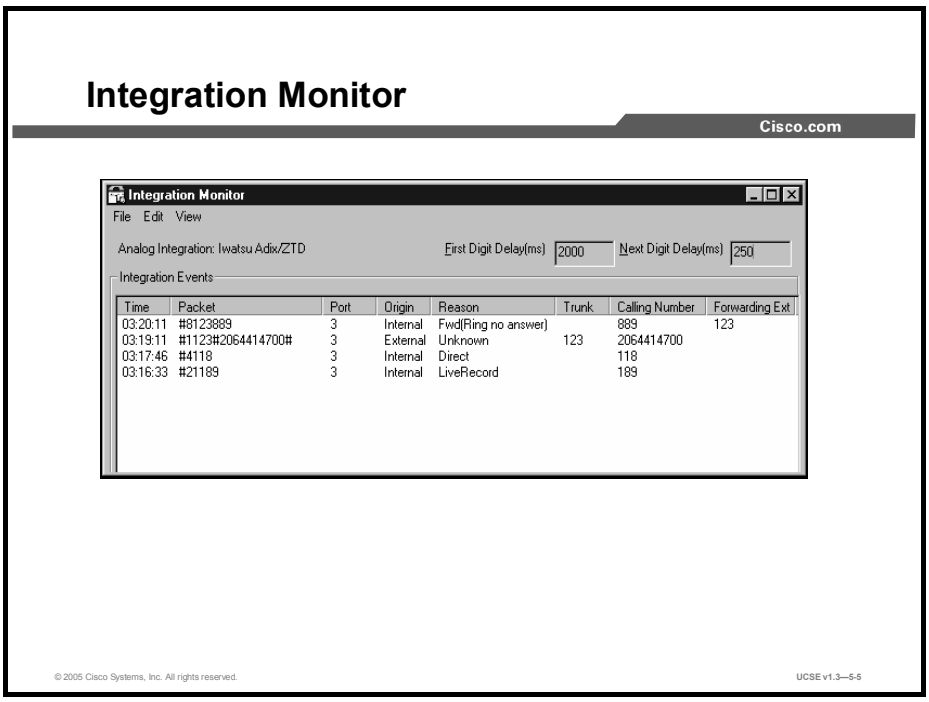
The Switch Configuration Editor allows you to edit specific integration information on the Cisco Unity server for the switch that the server is connected to. You can set data such as Message Waiting Indicator (MWI) on-off codes, the number of rings before Cisco Unity will answer an incoming call, delays or access codes needed for outdialing, and so forth.

A field technician or support person with knowledge of the switch integration features uses this tool. You can break your integration with the phone system if you do not use this tool carefully. Using this tool is analogous to changing Registry settings, or changing the protocol (language) one of the devices speaks. If the change is incorrect, the two devices will not understand each other.

This tool should *not* be used when making switch-related changes to Cisco CallManager. For those purposes, use the Cisco Unity Telephony Integration Manager tool found at Start > Settings > Control Panel > Phone and Modem Options on the Advanced tab. This is where you can gain access to the Telephony Service Provider (TSP) used by Cisco Unity and Cisco CallManager.

Integration Monitor

This topic describes the Integration Monitor.

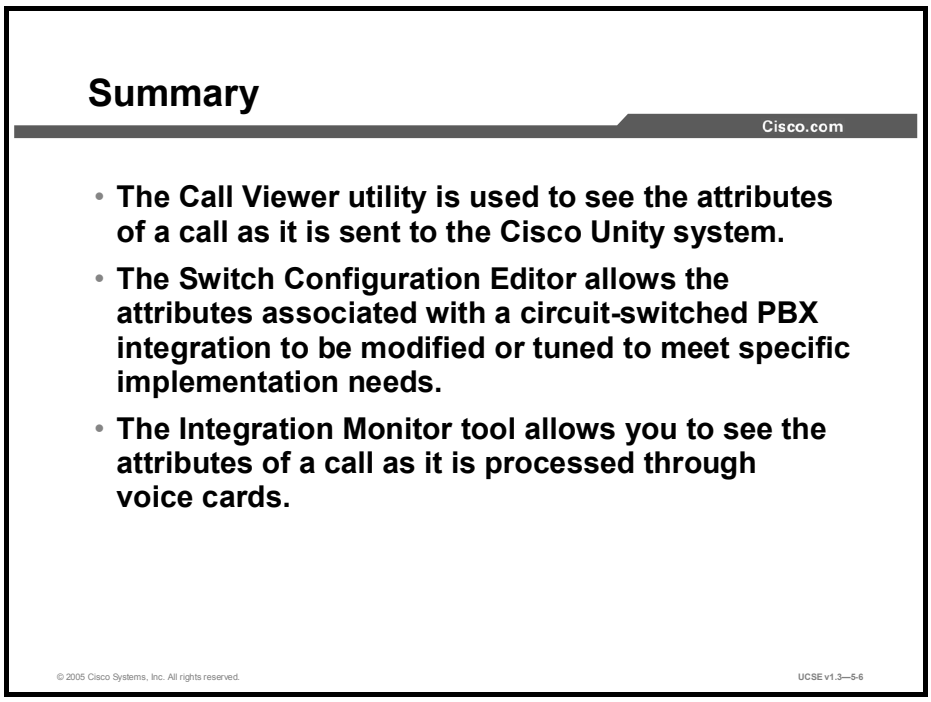


The Integration Monitor shows detailed information about each call on a circuit-switched phone system. This shows much of the same information that the Call Viewer application shows, in addition to raw packet information and the ability to see outbound call information. The Integration Monitor will parse the raw packets and display the information in a more readable format.

This tool does not work with Cisco CallManager as the switch. It should only be used for analog or Simplified Message Desk Interface (SMDI) circuit-switched PBX integrations.

Summary

This topic summarizes the key points discussed in this lesson.



References

For additional information, refer to these resources:

- *Cisco Unity Troubleshooting Guide*
- *Cisco Unity System Administration Guide*

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) The _____ shows basic call information for incoming calls on an IP integration.

A) Integration Monitor
B) Switch Configuration Editor
C) Edit Caller utility
D) Call Viewer utility

Q2) The Switch Configuration Editor is used to _____.

A) see the current licenses for your Cisco Unity system
B) edit specific integration parameters for a switch
C) edit user account information
D) safely edit many of the hidden registry settings

Q3) Which tool is used to view call information for circuit-switched PBX integration?

A) Integration Monitor
B) Switch Configuration Editor
C) Edit Caller utility
D) Call Viewer utility

Q4) The Call Viewer utility works with _____.

A) IP telephony integration
B) circuit-switched PBX integration
C) both A) and B)
D) neither A) nor B)

Q5) Which tool displays raw packet information?

A) Integration Monitor
B) Switch Configuration Editor
C) Edit Caller utility
D) Call Viewer utility

Quiz Answer Key

Q1) D, Call Viewer Utility.

Relates to: Call Viewer Utility

Q2) B, Edit specific integration parameters for a switch.

Relates to: Switch Configuration Editor

Q3) A, Integration Monitor.

Relates to: Integration Monitor

Q4) A, IP telephony integration.

Relates to: Call Viewer Utility.

Q5) A, Integration Monitor

Relates to: Integration Monitor

Lesson 5

Understanding Disaster Recovery and Cisco Unity

Overview

This lesson discusses the use of the Disaster Recovery Backup and Disaster Recovery Restore tools (DiRT) in Cisco Unity.

Relevance

Understanding the process of performing a disaster recovery backup and restore, to restore a server to a fully operational mode as quickly as possible in the event of a catastrophic failure, is essential to maintaining a Cisco Unity system.

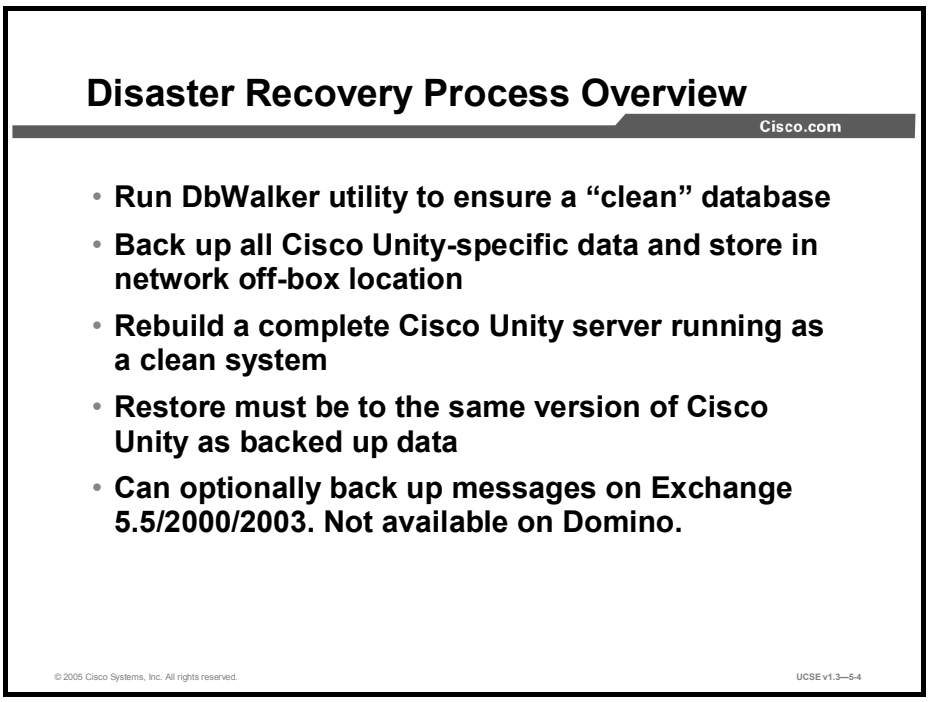
Objectives

Upon completing this lesson, you will be able to describe the function of the Disaster Recovery Backup and Restore tools. This ability includes being able to meet these objectives:

- Describe the disaster recovery process
- Describe the supported disaster recovery scenarios
- Describe which data is saved during the backup process
- Describe which data is not saved during the backup process
- Describe the Disaster Recovery Backup procedure
- Describe the two-hop SQL backup method
- Describe how to schedule backups using the tool
- Describe the overall restore procedure
- Describe when and how to use remap subscriber alias strings during the restore process
- Describe the important considerations during an Exchange-based restore
- Describe the important considerations during a Domino-based restore

Disaster Recovery Process Overview

This topic describes an overview of the disaster recovery process.



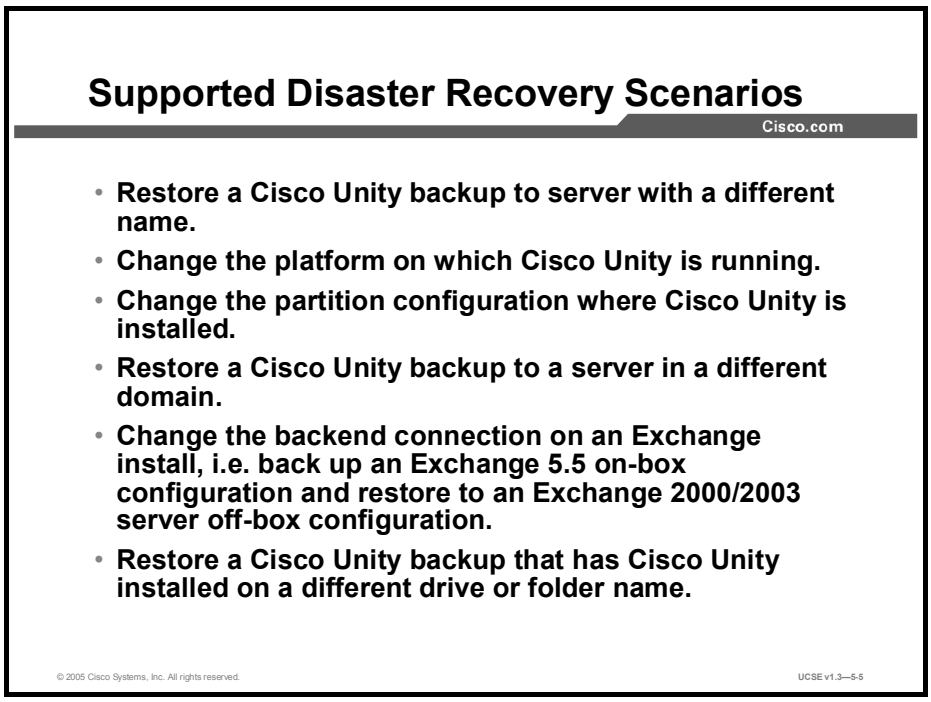
The disaster recovery tools provide a way to back up all Cisco Unity data on a server and store it on a network drive in an off-box location. The data saved includes all Cisco Unity objects and data—greetings, voice names, routing rules, switch information, and so on. Optionally, in an Exchange environment, you can back up messages.

In the event of a catastrophic failure of a Cisco Unity server, you must build up a new server to the point where Cisco Unity is running a “clean” operating system of the same version that was backed up. You must also configure integration to Cisco CallManager. After this, you can begin a restore.

The disaster recovery tool is ideal for sites that have installed Cisco Unity in a unified messaging configuration and users are homed off-box. In such a configuration, the site will already have Exchange or Domino backup procedures in place and can use the DiRT tool to back up and restore the Cisco Unity data.

Supported Disaster Recovery Scenarios

This topic describes the supported disaster recovery scenarios.

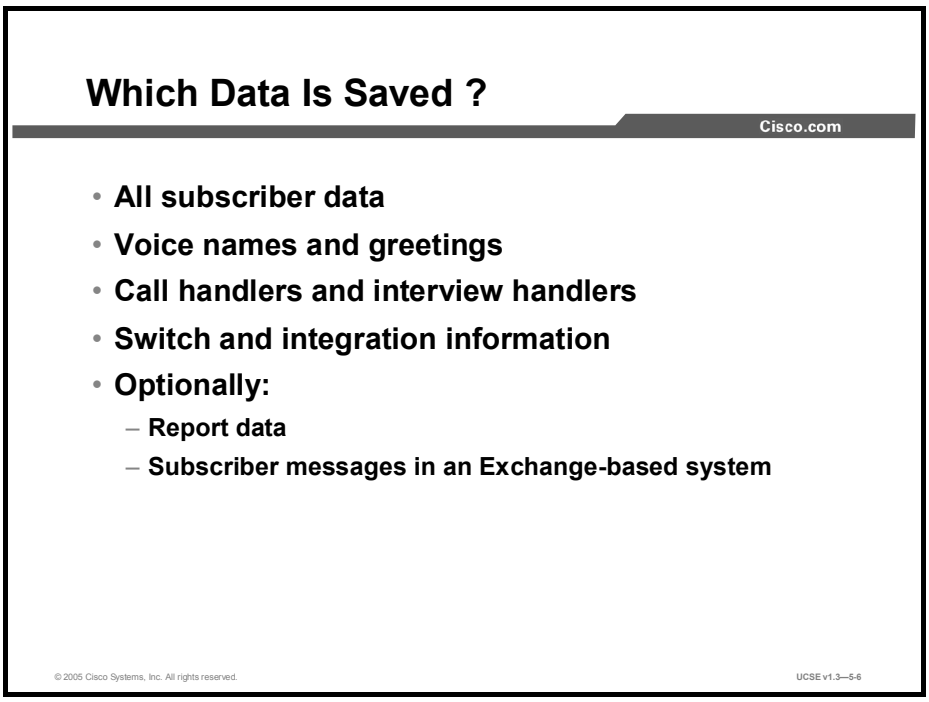


In addition to disaster recovery, the DiRT utility can be useful for other issues that arise. The tool can be used to restore Cisco Unity to a server with a different name if you decide that the name on the present Cisco Unity server needs to change. You can restore the DiRT backup to a Cisco Unity server in a different domain if necessary. A restore can be done if your new server has Cisco Unity installed on a different drive or folder name; for example, if your backup is on C:\CommServer and you want to restore it to E:\Unity.

With Exchange as the back end, you can also restore to a changed version of the back end. For example, you could be changing from an Exchange 5.5 on-box Cisco Unity to an Exchange 2000/2003 off-box installation. The DiRT utility will make the changes in the database and registry, or references, to make the transitions work.

Which Data Is Saved?

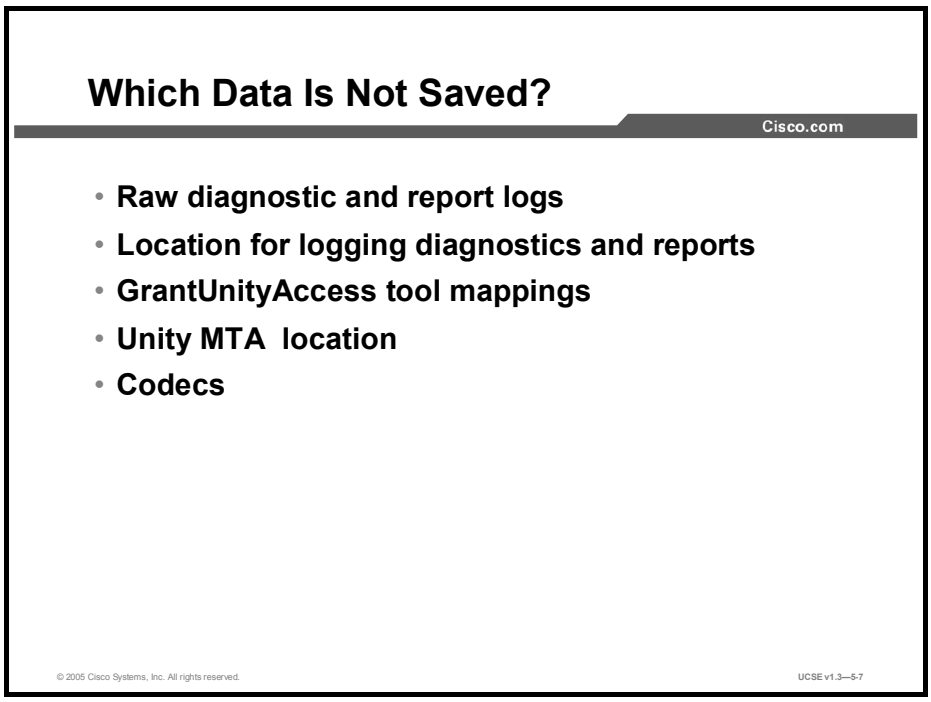
This topic describes which data is saved in a Disaster Recovery Backup.



Almost all Cisco Unity data is saved during the backup process. This would include all subscriber data, call handlers, interview handlers, directory handlers, voice names, greetings, passwords, switch configuration information, and so on. In addition, if desired, report information and, in the case of an Exchange-based system, subscriber messages will be saved. You will be given these options during the backup configuration process.

Which Data Is Not Saved?

This topic describes which data is not backed up during the Disaster Recovery Backup process.



There is some Cisco Unity information that is not saved during the Disaster Recovery Backup process. The report logs and the raw diagnostic logs will not be included in the backup. This includes information gathered by initiating micro or macro diagnostic traces used to resolve issues with Cisco Unity.

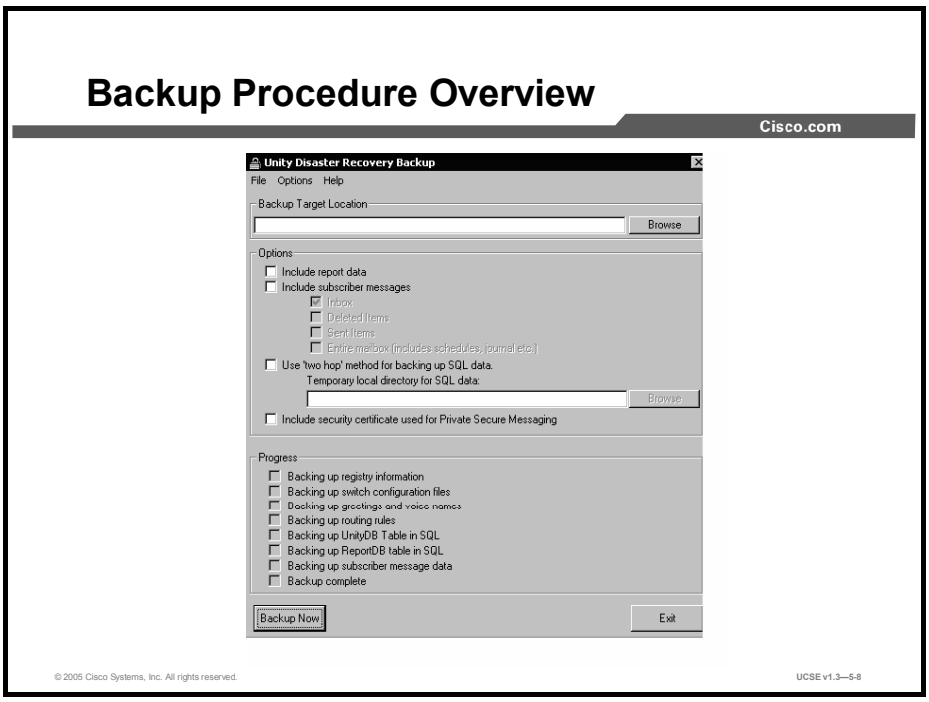
If you made any mappings to administer other Cisco Unity servers for the GrantUnityAccess utility, these mappings will also be lost and will have to be reset.

The location of the Cisco Unity Mail Transfer Agent (MTA) folder, as well as the system logs folder, can be changed during the installation process. These changes are not held during the backup process.

If you changed the codec on the backup system to something other than G.711, you will need to configure the codec again, using the SetRecordFormat tool.

Backup Procedure Overview

This topic describes the backup procedure.



Before running the Disaster Recovery Backup, you must decide the backup target location. The target location should be off-box, because leaving it on-box defeats the purpose of performing the backup. You must enter the full path, such as e:\sea-lab\unitybackup.

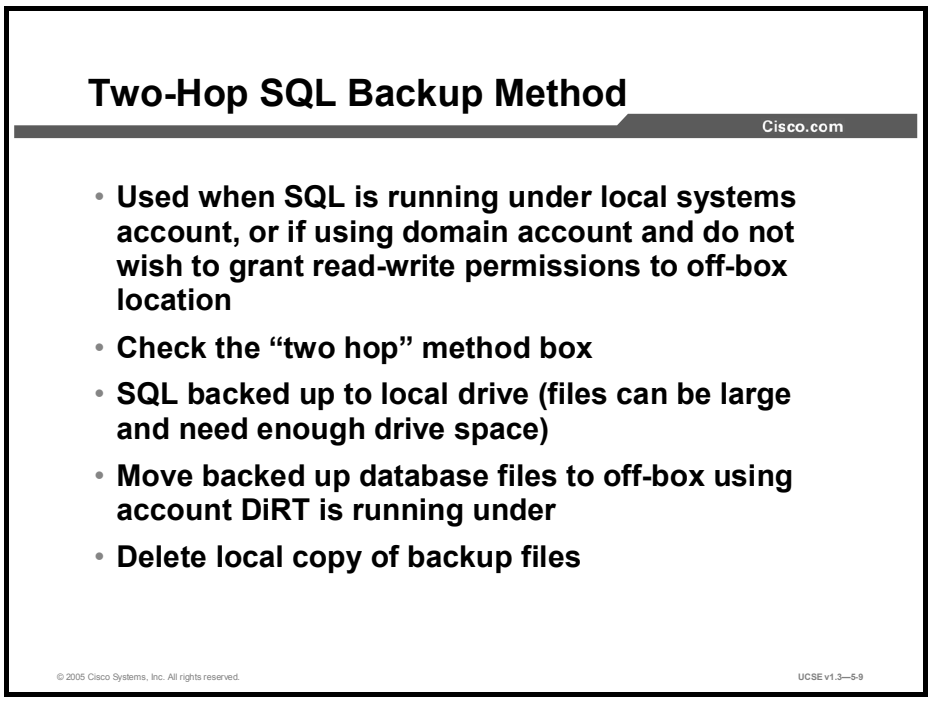
You must allocate enough space in the target location to accommodate the backup files. Keep in mind that the backup will, at a minimum, include voice name and greetings files, which can be large. You can check the size of the \CommServer\StreamFiles directory to learn about how much space is needed for the voice files. Then add some space for the Cisco Unity Structured Query Language (SQL) table. Look at the \CommServer\UnityDB.BAK file to learn how large that table will be. You might also decide to back up subscriber messages. There is no easy way to estimate how much space will be needed for subscriber messages.

You must run the Disaster Recovery Backup tool under an account that has the necessary administration rights to SQL, and to Exchange if you decide to back up messages.

The progress of the backup will be indicated by the checkboxes next to each task. When the backup is complete, you will be given an error count and will be able to review the log file.

Two-Hop SQL Backup Method

This topic describes how to use the two-hop SQL backup method.



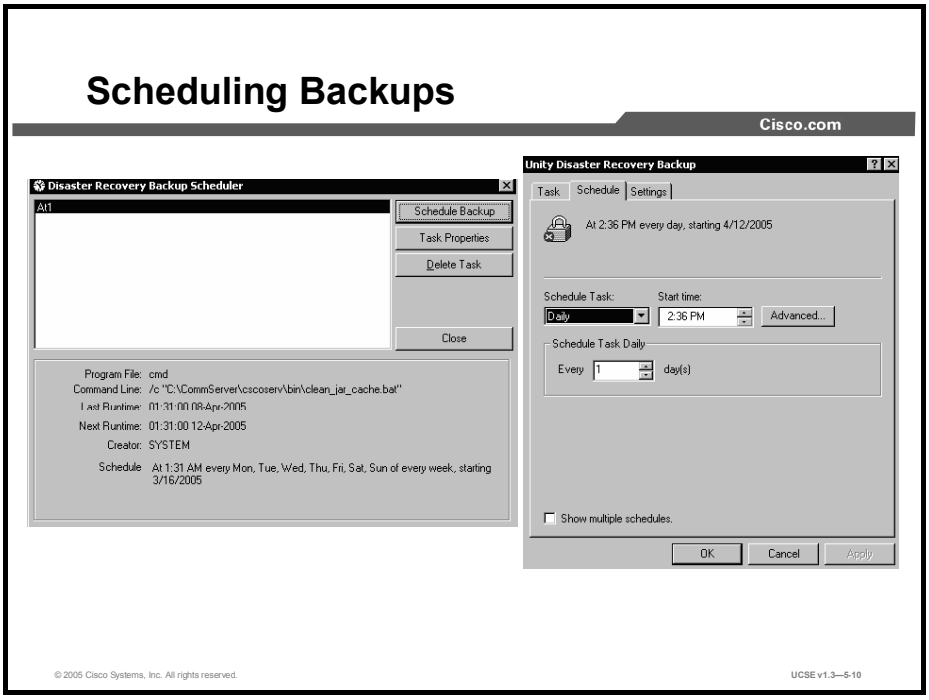
The two-hop method for backing up the SQL database allows you to write files to an off-box location in order to supersede limitations of using the SQL account. Customers will often have the SQL services running under the local system account. When SQL attempts to write the backed-up data to the off-box location, it will fail. If you are using a domain account for the SQL services but do not want to grant read-write permissions to the off-box location, the SQL backup portion will fail as well.

The method is termed two-hop because the data will take two hops to be backed up. First, you perform an SQL backup to a local drive, and then move the files to an off-box target using the account that DiRT is running under. Then you delete the local copy of the backup-up files.

To use the two-hop method, check the appropriate box on the Disaster Recovery Backup screen and provide a local target to use. Be sure there is enough room to accommodate the backed-up files.

Scheduling Backups

This topic describes how to schedule backups.



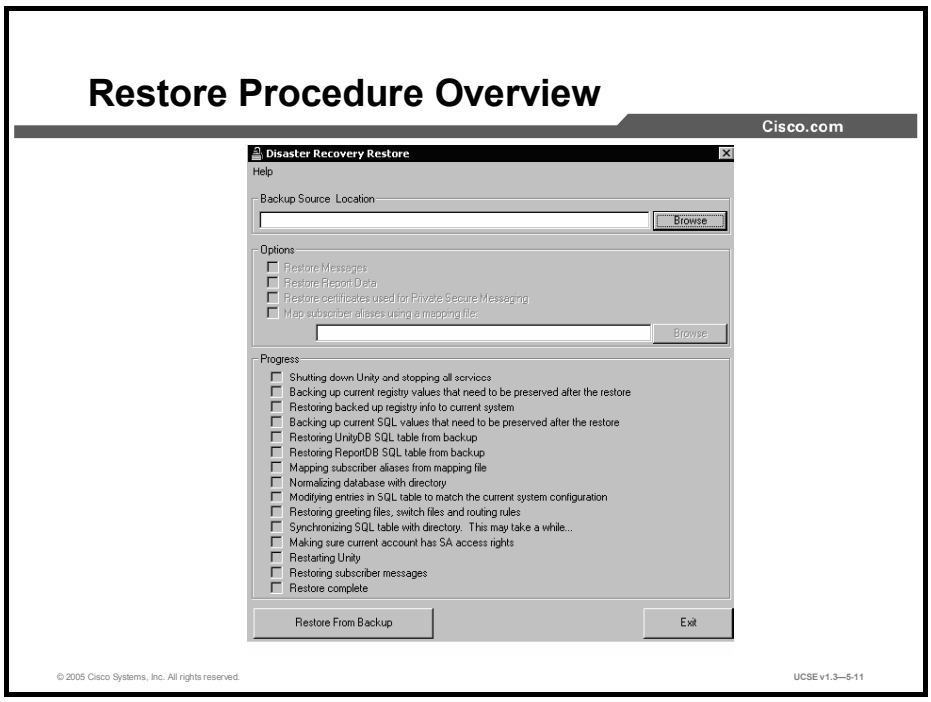
The Disaster Recovery Backup tool has a built-in scheduler that uses the Windows scheduling service. Before using the scheduler, make sure that you have completed a successful backup in regular interactive (manual) mode. This will ensure that the account in which you are logged in has the correct rights and that the location you are writing to is configured properly.

To schedule a backup, select the **Schedule Regular Backup** item in the Options menu of the Disaster Recovery Backup tool. This will open the schedule dialog which interfaces with the Windows scheduler. You may see other scheduled tasks in this list that have nothing to do with the Disaster Recovery Backup—just add your schedule in addition to those already there. To add the schedule, click **Schedule Backup**. You will provide a name for the schedule and then set the Task Properties for the backup. Do not adjust the path or the command-line options, because those are set automatically. Check the **Enabled** box under the Task tab, and set the schedule times and frequency under the Schedule tab. After you click **OK**, you will be asked to provide the login name and password of the account that you would like the task to run under. You should use the same account that you used to perform the manual backup. In this way, you can be sure that the account has the correct rights and permissions.

As with running a backup manually, a log is generated with the backup in case there are errors.

Restore Procedure Overview

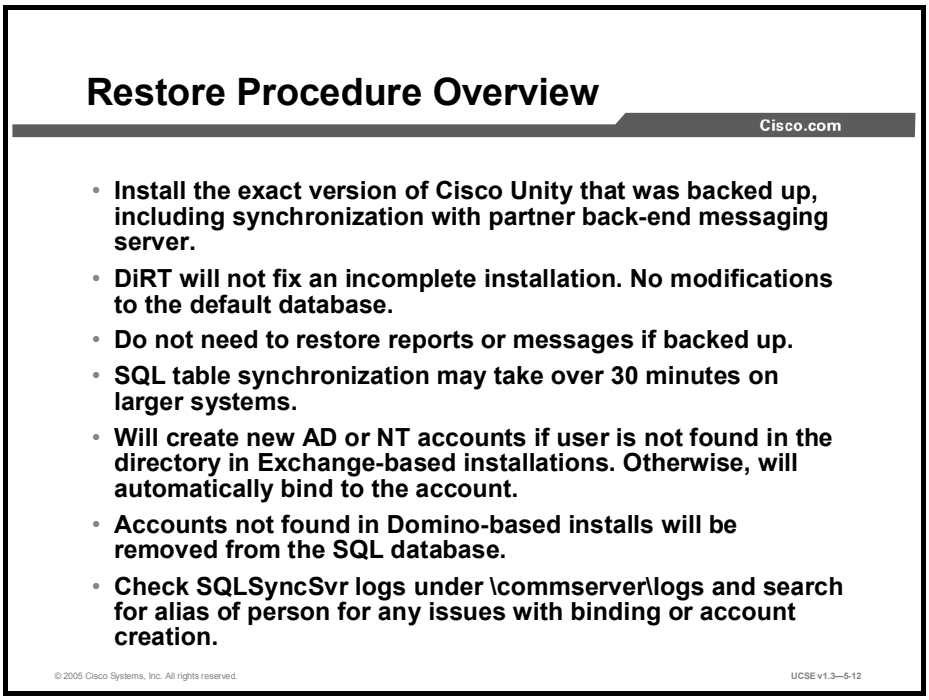
This topic gives an overview of the restore procedure.



Before restoring from a backup, you must install the same version of Cisco Unity that you backed up from. The Cisco Unity installation must be “clean” and running before a restore can be run. The restore will not fix an incomplete Cisco Unity installation. If the restore program detects any problems with the Cisco Unity installation, it will abort. You should test Cisco Unity; that is, make sure that it answers calls and that the System Administration is functioning properly, before starting the restore.

You also need to have the Cisco Unity partner messaging server, Exchange or Domino, up and integrated with Cisco Unity. The messaging servers do not need to be the same version from which you backed up.

To begin the restore, use the **Browse** button to point to the backed up files location. The restore tool then checks to see if all the necessary files it needs for restore are there and checks to make sure that the backed-up version of Cisco Unity is installed on the local server. The Disaster Recovery Restore tool also confirms that the local Cisco Unity server is a clean install, with no new subscribers, call handlers, or directory handlers added or modified. If the system is not clean, or if the Cisco Unity version does not match, or an essential file is missing, then the restore will abort and an error dialog will appear.



If you backed up report data or messages, those check boxes will be available, but you do not need to restore either report data or messages, even though you backed them up. Also, you can restore messages for single subscribers only if you choose.

During the disaster recovery restore, the “Synchronizing SQL table with directory” task could take 30 minutes or longer to complete on large directories. Do not interrupt the process. If there is an error, the program will terminate itself and log an error.

Once the SQL synchronization is complete, Cisco Unity will restart and the process of restoring messages (if selected) will begin. Cisco Unity can be up and running during this process.

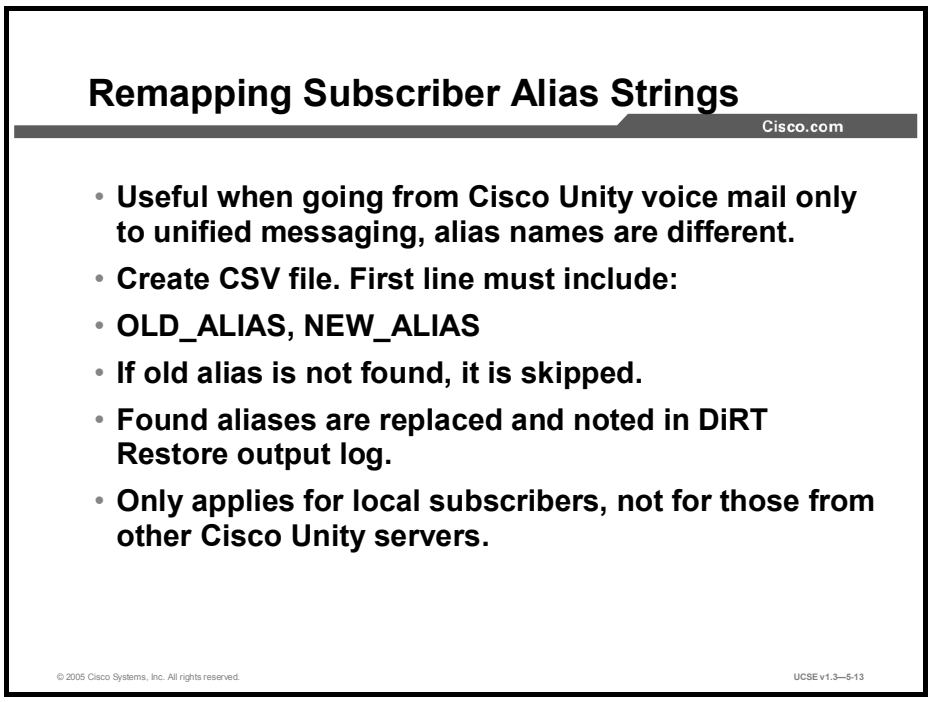
At the end of the restore process, an error and warning log will appear and you can review the log.

When a restore is run on Exchange systems, users that are missing in the directory will be re-created by the Disaster Recovery Restore tool in the container selected during the Cisco Unity setup process. Users that are in the directory will “bind” automatically.

When a restore is run on a Domino system, the Disaster Recovery Restore tool has no ability to create the missing directory accounts. Instead you will be given an opportunity to address the issue in Domino or the Disaster Recovery Restore tool will remove these missing accounts from the SQL database.

Remapping Subscriber Alias Strings

This topic describes the remapping of subscriber alias strings.



Remapping subscriber aliases is typically done in situations in which you have backed up Cisco Unity data from a voice-mail-only deployment and are moving it into a unified messaging configuration in which the alias naming convention is different.

The process for remapping aliases is very simple. You create a CSV file that contains the old alias string to be found in the Cisco Unity backup and the new alias sting you would like to use in the restored system. You check the “Map subscriber aliases using a mapping file” box on the Disaster Recovery Restore screen and provide the path of where to find the CSV file. During the restore, DiRT will search for all the old aliases and, if found, replace them. This will be completed before the directory synchronization, so that Cisco Unity will automatically “bind” to users with the new aliases.

The CSV must be properly formatted. The first line must be as follows:

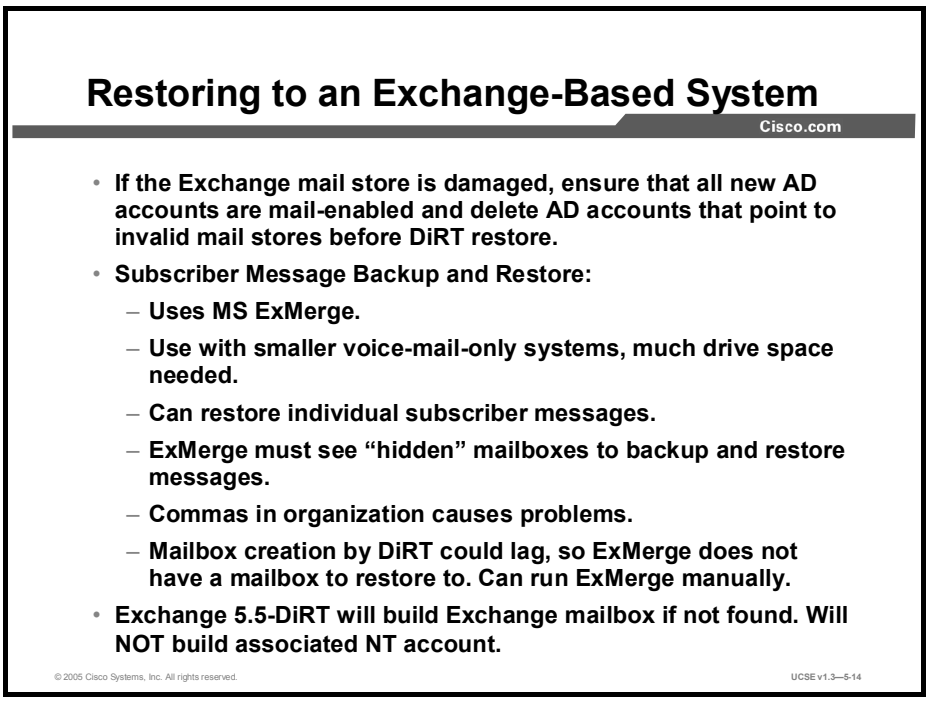
OLD_ALIAS, NEW_ALIAS

If the restore does not see the first line as shown, it will not accept the file.

If the old alias is not found in the restored database, it is noted in the log file and skipped. All aliases that are found and replaced in the local system are noted in the DiRT restore output log. Only aliases for local subscribers on the server are searched for and replaced. Subscribers from other Cisco Unity servers are not searched for.

Restoring to an Exchange-Based System

This topic describes issues to consider when restoring to an Exchange-based system.



When restoring to an Exchange-based system, there are a few issues to remember concerning account creation and restoring of messages.

In the event of a disaster where an Exchange mail store is destroyed or damaged, you can have Active Directory accounts that are configured as mail-enabled but that point to a mail store that no longer exists. The DiRT restore utility is not capable of telling whether the mail store is valid or not—it will only see an Active Directory account and assume that the mail store is there. The restore process will update the account to be a Cisco Unity subscriber. Of course, without the associated mail store for the subscriber, the restore for this subscriber in essence will fail.

To avoid a failure of the restore, you can do one of the following:

- Mail-enable the Active Directory accounts prior to running the DiRT restore tool. DiRT will bind to this account during the restore.
- Delete the Active Directory accounts that point to invalid mail stores. DiRT will re-create both the Active Directory and mail store for these users and update them to be Cisco Unity subscribers during the restore process.

As mentioned previously, DiRT has the ability to back up and then restore subscriber messages on an Exchange-based system. This feature is intended for use with smaller voice-mail-only systems and is not a replacement for proper backup protection for Exchange. DiRT will work in any configuration of Exchange, but the drive space required to back up the messages can be very large.

The Disaster Recovery Restore tool leverages the Microsoft ExMerge utility to back up and restore messages. This enables DiRT to be able to restore a single subscriber's messages. ExMerge backs up each individual subscriber's messages into its own PST file. You can find the PST files in the target backup directory under the Messages folder. To restore an individual subscriber's messages, you can use Outlook to import the PST file into their mailbox. If Outlook is unavailable, you can use ExMerge directly, which can be found under Program Files\Exchsrvr\Bin. ExMerge has a GUI interface that will guide you through the restore process.

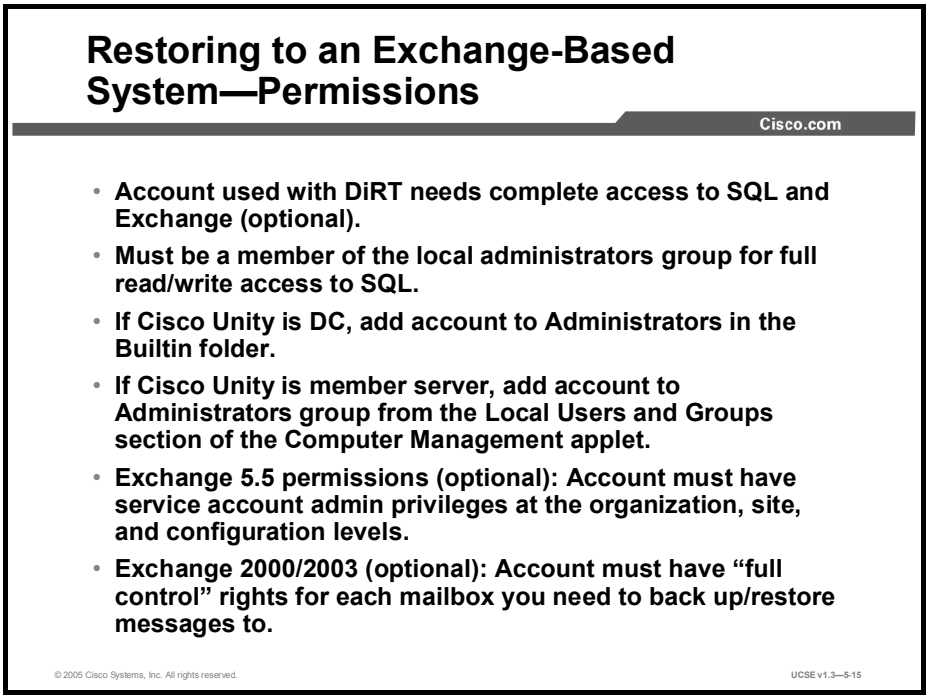
You can also restore individual greetings and voice name files for subscribers and call handlers. These are WAV files and can be found in the \CommServer\StreamFiles directory. Each file is named with the alias of the object with which it is associated, so finding the WAV file you need is easy.

One object ExMerge does not handle well is hidden mailboxes in Exchange 2000. If you are backing up or restoring messages on an Exchange 2000 system that has hidden mailboxes, you will need to unhide them during the restore and then hide them again. This is an Exchange ExMerge issue that DiRT can not fix.

ExMerge also does not like commas in an organization name (for example, "Cisco Systems, Inc."), and the backing up and restoring of messages will likely fail. This, however, is only an Exchange 5.5 issue, because in Exchange 2000 and 2003, commas in organization names are not allowed.

Restoring to an Exchange-Based System—Permissions

This topic describes the permissions needed when restoring to an Exchange-based system.



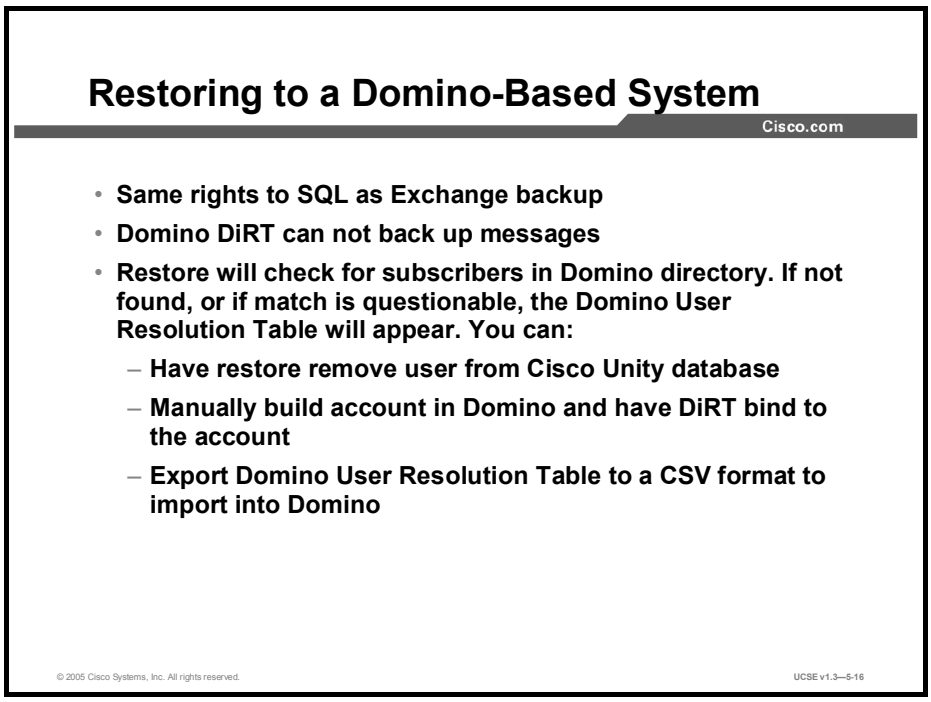
The account that you run DiRT under must have complete access to SQL in all cases, and must have access to mailboxes in Exchange if you wish to back up and restore subscriber messages. This account must be a member of the local administrators group to gain full read/write access to SQL. DiRT will not function without access to SQL. If the Cisco Unity system is also its own domain controller, add the account to the Administrators group in the Builtin folder. If Cisco Unity is a member server, you will need to pass the account to the Administrators group from the Local Users and Groups section in the Computer Management applet.

To back up and restore messages on an Exchange 5.5 system, the account must have Service Account Admin privileges at the organization, site, and configuration levels in Exchange.

In Exchange 2000, the account needs to have "full control" rights for each mailbox for which you want to back up messages. This is difficult to accomplish in Exchange 2000 due to the Active Directory security model. For more information, reference the README file that comes with the Disaster Recovery Backup utility. You can also reference Microsoft Knowledgebase article Q262054 which is titled, "How to get 'service account' access to all mailboxes in Exchange 2000".

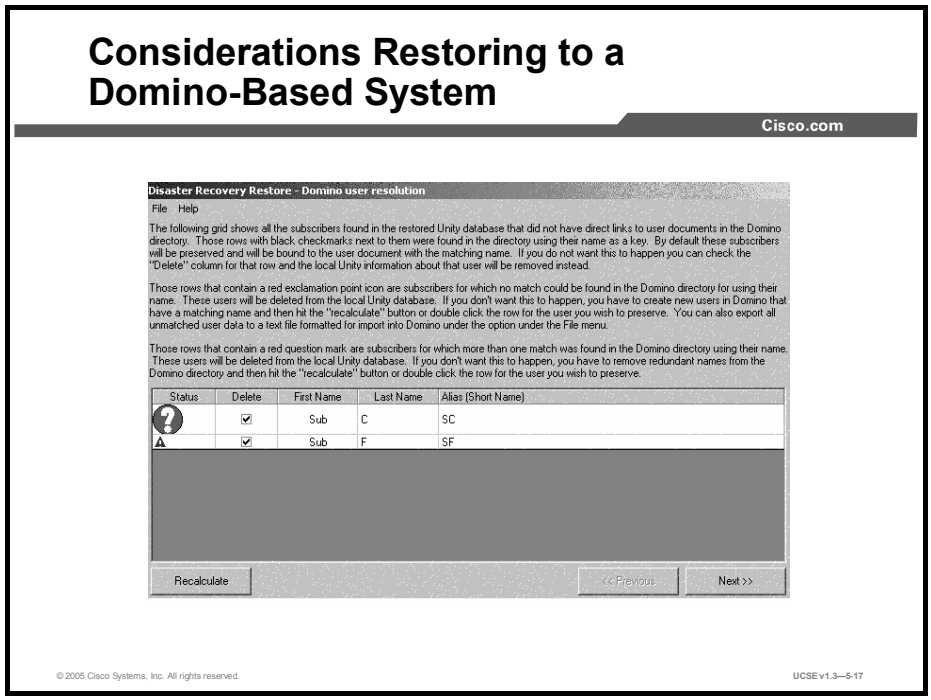
Restoring to a Domino-Based System

This topic describes issues to consider when restoring to a Domino-based system.



The restore process for Domino is identical to an Exchange restore except for a few items. Unlike in the Exchange environment, Cisco Unity, and therefore DiRT, can not create accounts in the Domino directory, because the Domino Unified Communication services (DUC) does not allow creation of accounts. Therefore, all Cisco Unity subscribers must have accounts in the Domino directory that the DiRT restore process can bind to, or those users must be removed from the Cisco Unity backup.

After DiRT has restored the SQL tables, it checks to see that each subscriber in the table has an associated entry in the Domino directory. If the user is not found, they will be listed in a Domino user resolution table, which shows subscribers found in the restored Cisco Unity database that did not have direct links to user documents in the Domino directory.



Following are three types of users that may appear in the Domino user resolution table:

- If the users can be found by their short or full names, they are shown as a potential match that you can confirm in the table. Short names are not necessarily unique, therefore you must confirm the mapping that is used. The icon for this type of user is a black checkmark. By default, these users will be bound unless you select not to bind them.
- If users can not be found by their short or full names, they are listed with a red exclamation mark. These users will be deleted in SQL unless you create a user to match them in the directory.
- If a user is found by their short name in the directory but there is more than one user that matches, they are shown in the table with a green question mark.

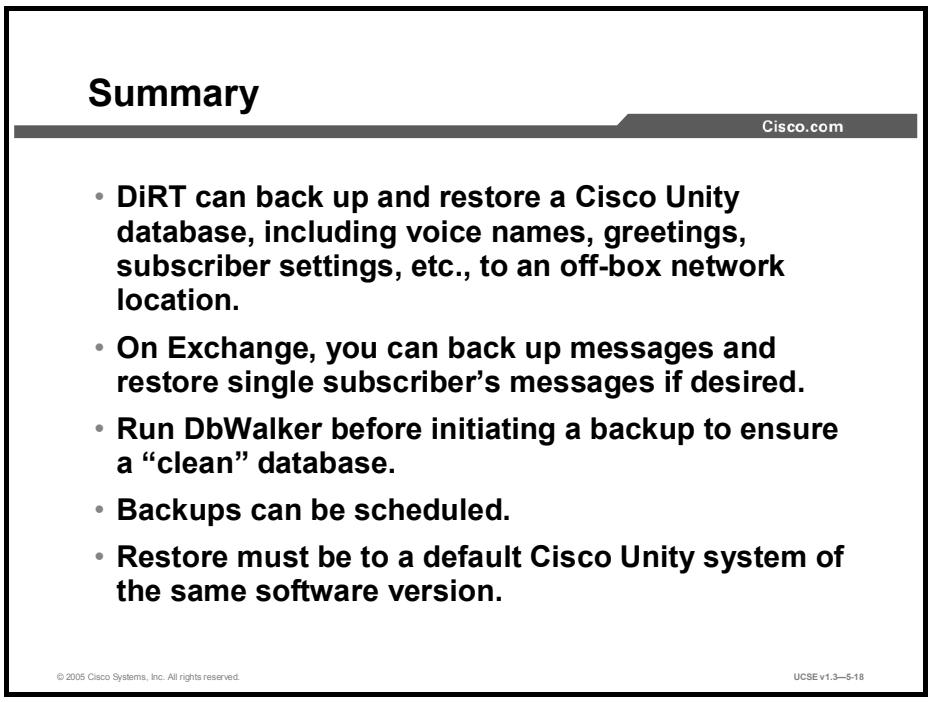
You review the entries presented in the table and decide what to do with them. You can simply let the restore remove the users from the Cisco Unity database, or create accounts for these users in Domino and have DiRT bind to them during the restore process. You can also export the table to a CSV format that can be used to import into Domino.

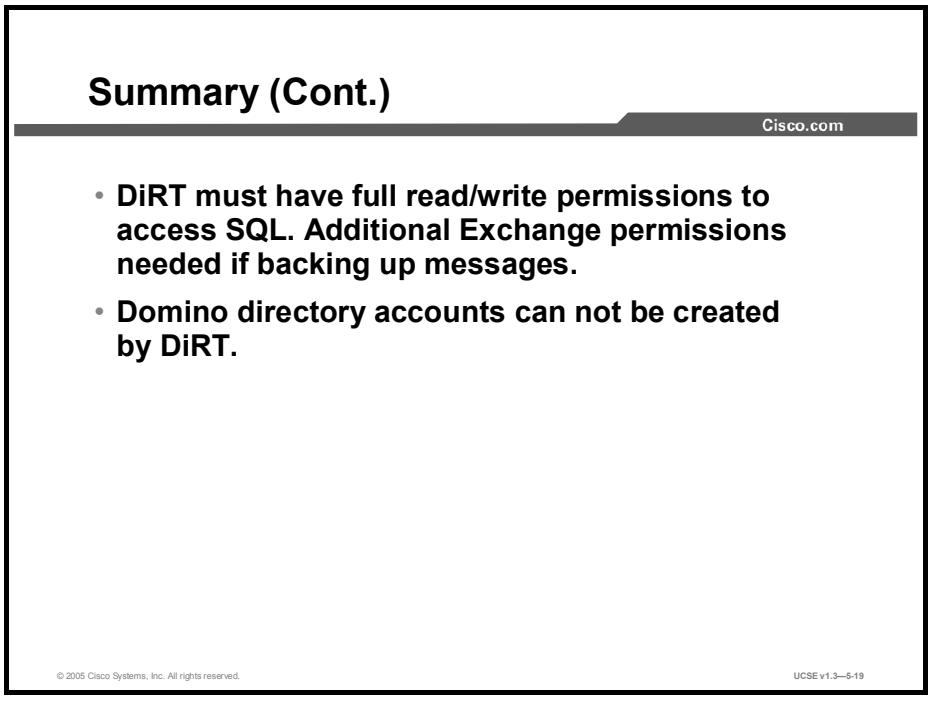
If you have made a decision to delete subscribers from the Cisco Unity database backup, you will be asked to provide replacements for the links these users may represent. This prevents the Cisco Unity database from being corrupted in the process of removing the users.

Because you can not back up messages in a Domino environment, no other permissions are required.

Summary

This topic summarizes the key points discussed in this lesson.





References

For additional information, refer to these resources:

- ReadMe file associated with the Disaster Recovery Backup Utility

Lesson 6

Providing Redundancy: Implementing Failover in Cisco Unity

Overview

Failover is a Cisco Unity feature that provides simple redundancy, allowing voice messaging functions to continue if the Cisco Unity server fails or when you need to perform maintenance. To set up failover, you install and configure Cisco Unity on two servers, a primary server and a secondary server.

Relevance

Voice messaging usually serves a crucial function in the way businesses work. It is important that the voice messaging system always be available. Failover, an optional Cisco Unity feature, provides a method to ensure availability, by providing a redundant system that can take over responsibility for answering calls, recording messages, delivering message notification, and turning Message Waiting Indicator (MWIs) on and off.

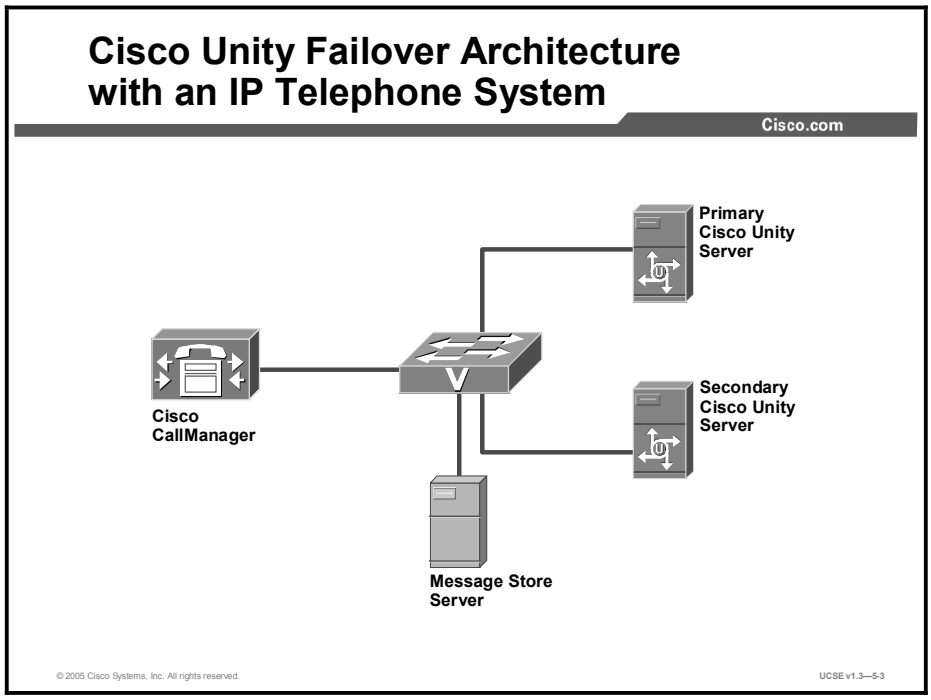
Objectives

Upon completing this lesson, you will be able to describe and implement Cisco Unity failover. This ability includes being able to meet these objectives:

- Describe Cisco Unity failover architecture
- Describe how failover works in Cisco Unity
- Implement failover on a Cisco Unity system
- Configure failover on a Cisco Unity system
- Describe the procedures to back up and restore Cisco Unity systems configured for failover

Cisco Unity Failover Architecture

This topic describes how Cisco Unity servers are arranged to provide failover support in the most commonly occurring configurations.



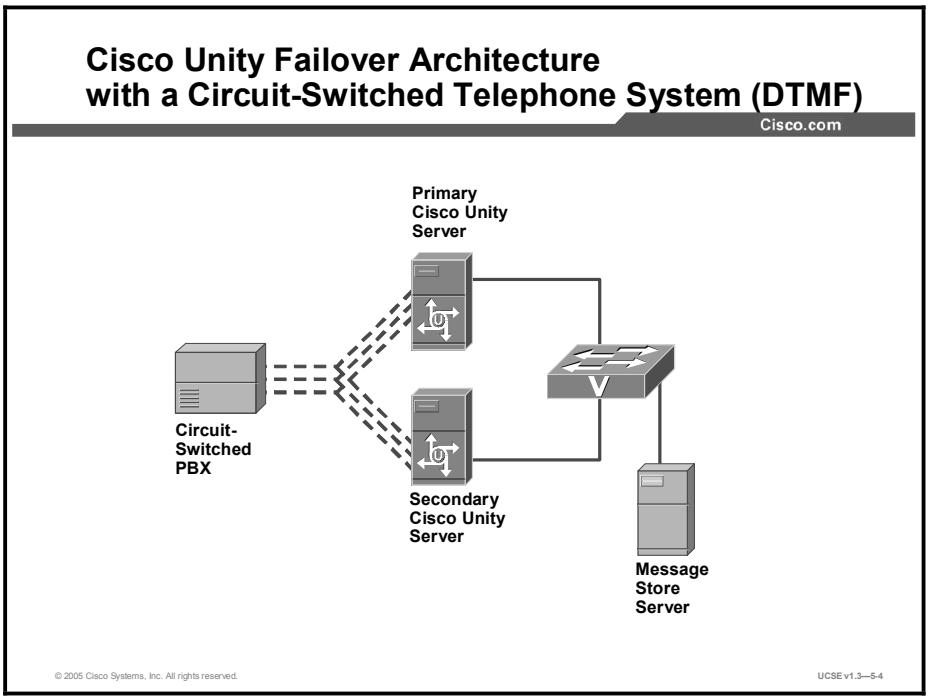
Under normal circumstances, the primary server is active—Cisco Unity answers calls and takes messages, sends message notifications, and turns MWIs on and off. The secondary server is inactive—Cisco Unity is running, but it does not perform any voice messaging functions until called upon to do so.

If the primary server fails or if the Cisco Unity service on the primary server stops, the secondary Cisco Unity server automatically becomes active and starts performing standard Cisco Unity tasks. This shift from primary to secondary servers is called failover. If you want to stop the primary Cisco Unity server for maintenance, you can initiate failover manually.

In every failover architecture, all messages must be stored off-box on a separate message store server. Storing messages on the Cisco Unity server would call for far too much replication traffic between servers.

Failover Configuration for a Circuit-Switched Telephone System (DTMF)

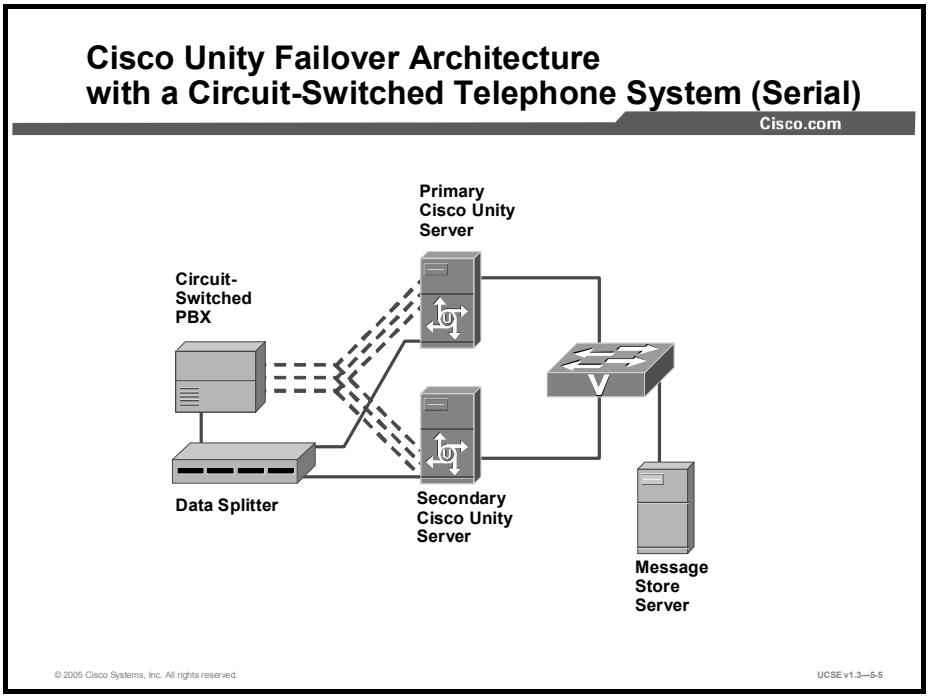
This figure shows how a circuit-switched telephone system, using dual tone multifrequency (DTMF), would be connected to both the primary and secondary Cisco Unity servers in a failover configuration.



Each of the lines coming from the single line extension cards on the PBX would have to be split so that the call and its integration information arrives at both the primary and secondary server.

Failover Configuration for a Circuit-Switched Telephone System (Serial)

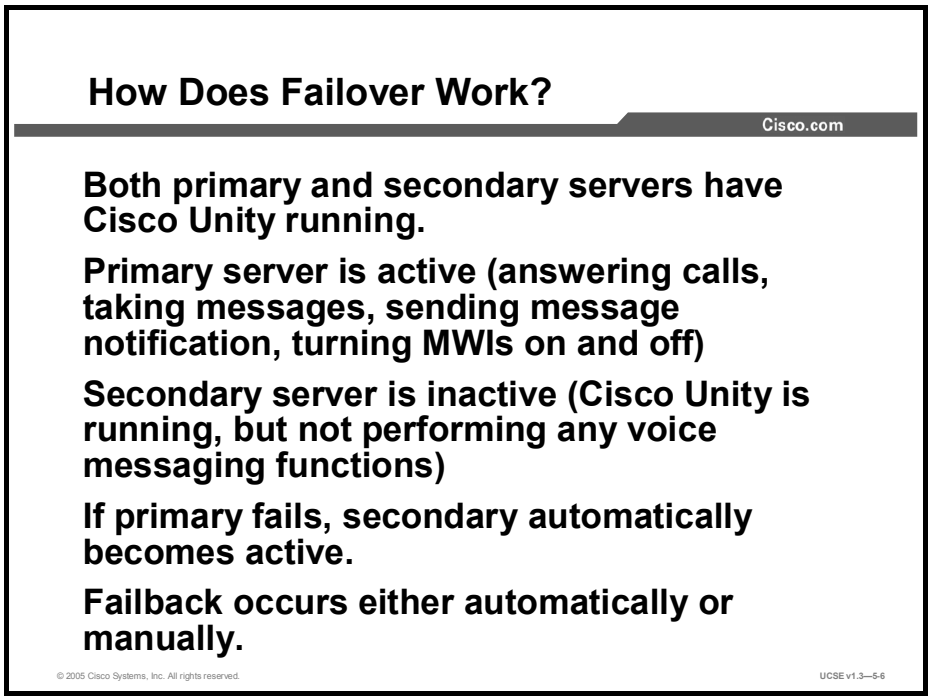
This slide shows a circuit-switched telephone system using a serial integration connected to both the primary and secondary Cisco Unity servers in a failover configuration.



Notice that in this case another piece of equipment is needed to split the serial data stream so that it arrives at both the primary and secondary servers. The call itself travels over the analog telephone lines, but the integration information about the call is carried on the serial cable. All of the normal specifications for RS-232 devices still apply.

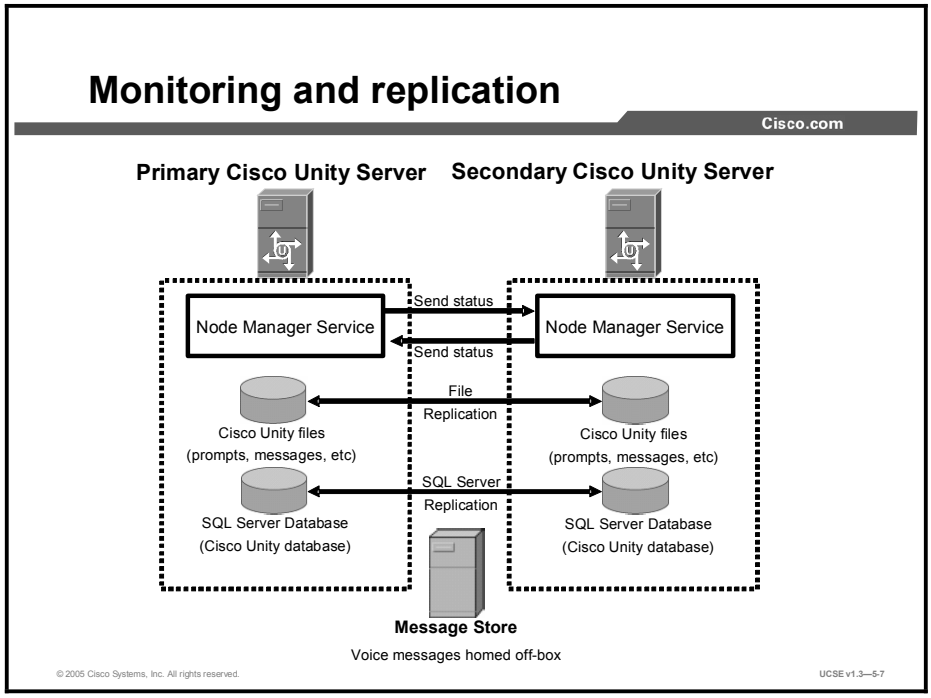
How Does Failover Work?

This topic describes how Cisco Unity servers share information and monitor each other so that failover can happen smoothly.



Failover works through a combination of keep-alive status events and file and database replication. Failover occurs when one of the following events occurs:

- The Node Manager service on the secondary server does not receive a status update in the required time period (for example, when the primary server crashes or network connectivity is lost).
- The Cisco Unity service on the primary server is stopped. The Node Manager service on the primary server reports the stoppage to the Node Manager service on the secondary server.
- A port on the secondary server receives a call when the Force Failover If Call Arrives on Inactive Secondary check box is checked in the Failover Monitor.



Both the primary and secondary servers run the Node Manager service (AvCsNodeMgr in the Services window) as a way of sharing their status. Each Node Manager monitors the Cisco Unity service (AvCsMgr) on its respective server and sends a keep-alive signal to the other at an installer-configured interval. The default interval is 1 second. On each server, the installer also configures how many keep-alive events can be missed before failover is initiated. The default is 30 keep-alive events. Increasing the interval will cut down on network traffic, but will also increase the amount of time before the secondary server begins answering calls if needed.

In addition, the Node Manager service monitors and replicates the files in the directories Localize\DefaultConfiguration, Localize\Prompts, Snapshot, StreamFiles, Support, and UnityMTA (which contains the Unity Message Repository [UMR]) on the Cisco Unity server. Node Manager creates a snapshot in the Snapshot directory of the files in the replicated directories during each replication cycle. In subsequent cycles, the Node Manager service compares the current snapshot with the previous one to determine which files should be replicated. The default file replication interval is 10 minutes, but is configurable. Increasing the interval will decrease network traffic, but will increase the possibility of losing data in the event of a failover event.

If changed files have not been replicated to the secondary server when the AvCsMgr service is stopped or the Cisco Unity server crashes, the changes may be lost. Under those circumstances, the new information will not be on the secondary server and may be lost or corrupt on the primary server. If the Node Manager service is set to manual, file replication is disabled.

Structured Query Language (SQL) server database replication occurs every minute if there are changes to the database. The database on the primary server is configured as the publisher and distributor; the database on the secondary server is configured as the subscriber. The database publication is called UnityDbPublication. Two-way replication is enabled so that the primary server can receive database changes when it is online and inactive.

Voice messages are not replicated because failover requires a separate message store. Subscribers will be able to access their messages no matter which server is active. Voice messages saved in the UMR of the active server when the message store is off-line are replicated to the inactive server with other Cisco Unity files.

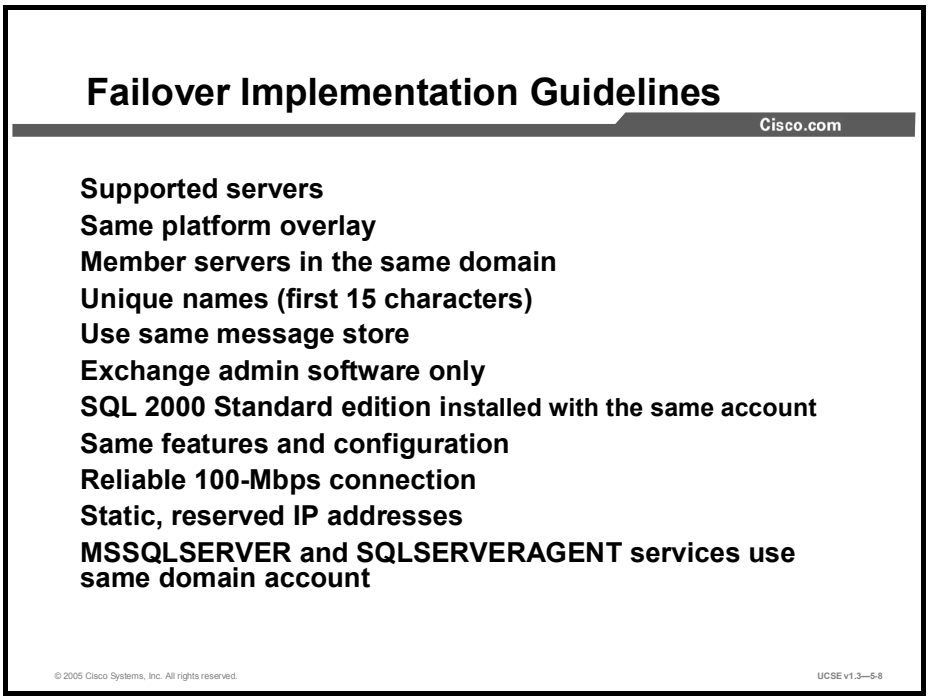
There are some Cisco Unity settings that are not replicated between servers. If you make changes to them on one server, then you must do so manually on the other server. The following settings are not replicated:

- Registry settings
- Recording settings
- Phone Language settings
- GUI Language settings
- Port settings
- Integration settings
- Media Master server name settings
- In Cisco Unity 4.0(1) through 4.0(3): AMIS restriction table selection. In Cisco Unity 4.0(4) and later, the AMIS restriction table selection is replicated.

Once one of the three conditions for failover occurs, the Node Manager on the secondary server assumes that the Cisco Unity service on the primary server is stopped and activates the Cisco Unity service on its server. If the secondary server receives a call, the Node Manager service on the secondary server instructs the Node Manager service on the primary server to initiate the failover. The secondary server begins answering calls, sending message notifications, and turning MWIs on and off. The Node Manager service on the secondary server writes a warning into the Event Log.

Failover Implementation Guidelines

This topic describes the guidelines that must be used in implementing a Cisco Unity failover solution.



In order to implement Cisco Unity failover, there are a number of requirements that must be met. Both servers must be qualified for use with Cisco Unity and they must be at the same platform overlay level. Both servers must be member servers in the same domain; neither of them can be a domain controller nor have any part of Active Directory installed on them. Server names can be longer than 15 characters, but they must be unique within the first 15 characters.

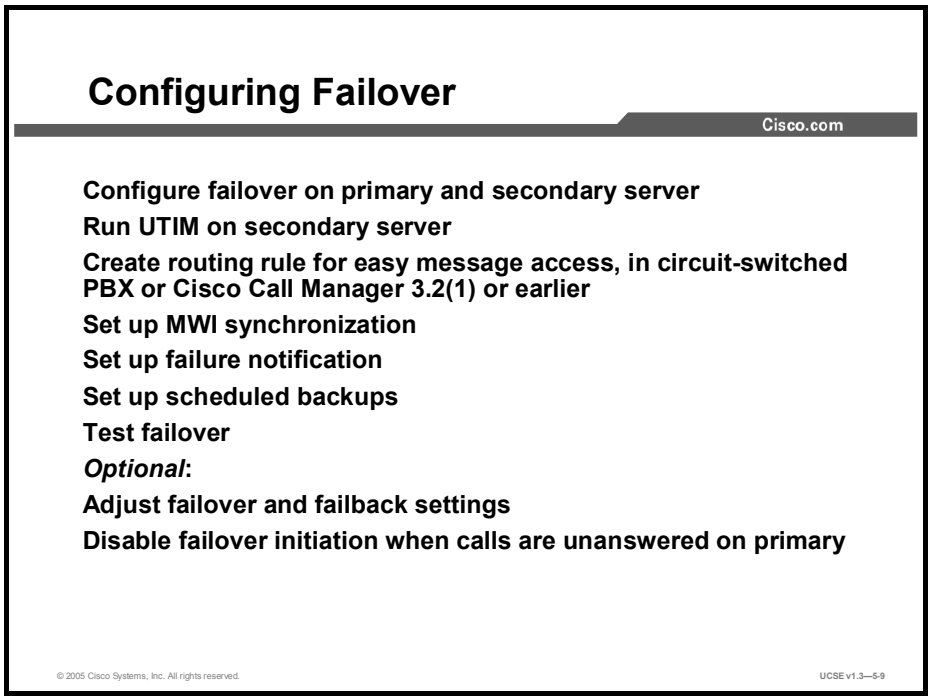
Both servers must be connected to the same Exchange message store. The only Exchange software that can be installed on either server is the administration software. Having all other Exchange software and services on another server will ensure that both servers have access to all messages no matter which one is active. Install SQL Server 2000 Standard edition on both servers using the same domain account to install each instance of SQL.

One server must be designated as the primary server and the other as the secondary server. Each server must have the same enabled features and configuration. Both servers must have a reliable 100-Mbps connection to the network. Failover will work in any supported Cisco Unity configuration except one that has no network connection. IP addresses for the Cisco Unity servers must not change in an uncontrolled fashion. Either configure each server with a static IP address, or if you are using Dynamic Host Configuration Protocol (DHCP) with a short lease duration, use DHCP reservations. If you are using DHCP with long leases, you can allow DHCP to assign IP addresses.

MSSQLSERVER and SQLSERVERAGENT services on both servers must be configured to use the same domain account that is a member of the Local Administrators group. These services cannot be configured to run as Local System. SQLSERVERAGENT on the primary server must be able to log in to the SQL server on the secondary server by using Windows NT authentication.

Configuring Failover

This topic describes the process of configuring failover on the primary and secondary Cisco Unity servers.



Configuration of the failover feature takes place after Cisco Unity has been installed on both the primary and secondary servers and after you have programmed the phone system and configured Cisco Unity to work with that phone system.

When you configure the primary and secondary servers, you are establishing their separate roles and providing the name of the other server. The IP address of the server is filled in automatically by FailoverConfig.exe. You also identify the account that owns the failover service. This account must be the same for both servers. The account must have the right to act as a part of the operating system, to log on as a service, and must be a member of the Local Administrators group. The only thing you do differently, when configuring the secondary server, is to set the date and time to exactly match the values shown on the primary server. Otherwise, the procedure is identical.

Once basic configuration is completed, you configure the voice ports on the secondary server by running the Cisco Unity Telephony Integration Manager (UTIM). These port settings should match those on the primary server. On the secondary server you need to create a routing rule that allows subscribers to log in to the secondary server after failover occurs. If Cisco Unity is integrated with Cisco CallManager 3.2(2) or later, or with a SIP proxy server, this is not necessary because the phone systems automatically forward calls to the secondary server when the secondary server becomes active.

Cisco recommends that you set the primary and secondary servers to resynchronize MWIs daily when network traffic is at its lowest. Cisco also recommends that you set up the Event Monitoring Service (EMS) to notify system administrators when failover occurs. The EMS monitors the Windows Event Logs and can send notification when the secondary server becomes active. It can send a prerecorded voice message, an e-mail, a Simple Mail Transport Protocol (SMTP) message, a Simple Network Management Protocol (SNMP) trap, or a write to syslog. Cisco also recommends that you prevent the loss of data due to a hardware failure by implementing a process of regular backups of both the primary and secondary servers using an approved third-party backup and restore application of the Cisco Unity Disaster Recovery Backup and Restore tool (DiRT).

Once this is accomplished, test Cisco Unity failover. To do this, create a new subscriber on the primary server, including a recorded name, and confirm that the data is replicated to the secondary server. Initiate a failover, then test the integration of the PBX with the secondary server. Record a message for the new subscriber and watch for the MWI to go on. Call in as the new subscriber, listen to the message, and watch for the MWI to go off. Once this is done, you can delete the test subscriber account.

Optional Configuration Steps

You can customize the default settings for failover and failback given to the primary and secondary servers by the failover configuration wizard. You can specify how often the primary and secondary servers send keep-alive events. The default is to send them once every second and to wait for 30 missed keep-alive events before initiating failover. If the active server is not receiving keep-alive events from the inactive server, failover or failback will not occur. You can also specify the frequency of file replication. The default value is every 10 minutes. Increasing the value will increase the possibility of data loss during a failure, but will decrease the amount of network traffic generated. You can also customize whether the secondary server will automatically initiate a failback at a specified time during the day. The default is to failback manually. You customize these settings on either the primary or secondary server. The values are then replicated to the other server.

The other setting you can customize is whether failover is initiated when a call is answered by a port on the secondary server. This event can happen for a number of reasons: one or more ports on the primary server locks up and fails to respond to calls; there is too much traffic for the primary server to handle; the primary server is experiencing high CPU utilization; or, in a Cisco CallManager integration, the voice messaging ports on the primary server unregister with the Cisco CallManager server.

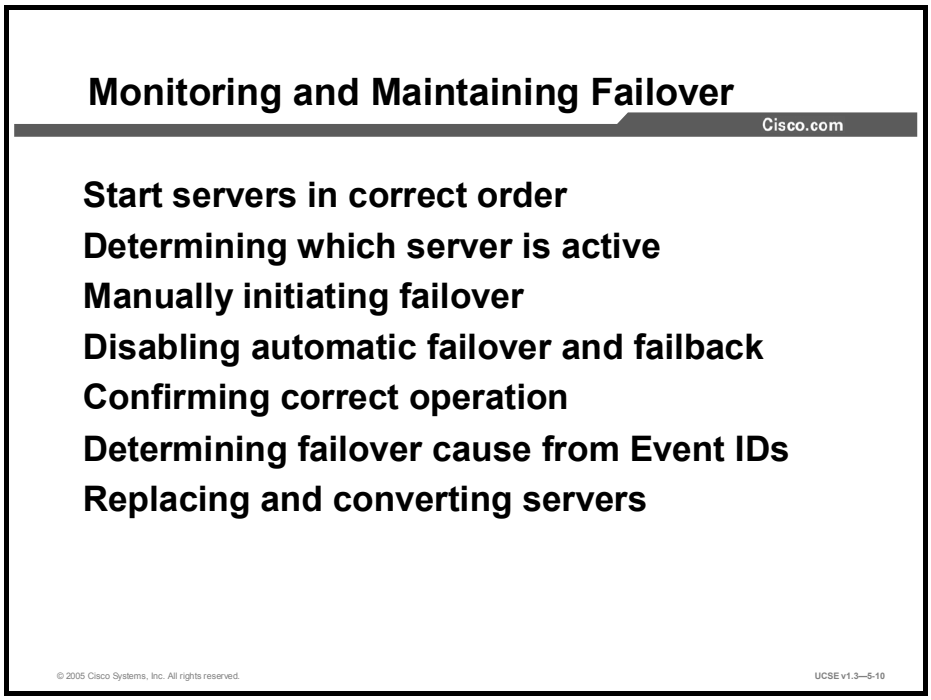
When a call arrives at the secondary server while it is inactive, the server writes an entry in the Event Log and the secondary server answers the call. The first action may trigger an alert to the system administrator. The second action initiates the failover process.

You may want the secondary server to become active when a voice messaging port on the primary server fails. However, customers who install Cisco Unity servers with large numbers of ports often do not want the failover to occur just because one port locks up.

You configure this option by checking the Force Failover If Call Arrives on Inactive Secondary box in the Failover Monitor.

Monitoring and Maintaining Failover

This topic describes tasks that must be done to monitor and maintain the Cisco Unity failover feature effectively.



In order for the primary server to be active, it must be started first. If the secondary server is started first, it becomes the active server by default. By looking at the Failover Monitor on either server, you can determine which is active. There are two fields in the Status section, Local Status and Remote Status. One of them will read “Running; Active”; the other will read “Running; Inactive”. If you are reading this from the primary server and Local Status is “Running; Inactive” and Remote Status is “Running; Active”, that means that the secondary server is currently the active one.

Before you manually initiate a failover, it is a good idea to confirm that any recent changes to the Cisco Unity database have been replicated to the inactive server. Once you have done this, you start the Failover Monitor on the primary server and click **Failover**. To initiate a failback from the secondary server, you start the Failover Monitor on the secondary server and click **Failback**.

The only reason you would ever disable automatic failover and failback would be during a troubleshooting process. When you disable the feature, file replication is also disabled. In addition, if you restart the primary and secondary servers while automatic failover is disabled, both servers come up as inactive.

To confirm that the failover servers operate correctly, place a text file in the primary server's CommServer\StreamFiles directory, and confirm that the file replicates to the secondary server within the specified replication interval, and then change a subscriber's extension and confirm that this change is replicated immediately. Manually initiate a failover and confirm that the secondary server becomes active. Call the system and confirm that the secondary server answers the call. Delete the test file from the secondary server's CommServer\StreamFiles directory and confirm that the deletion is replicated to the primary server. Manually initiate the failback and confirm that the primary server now answers calls.

When a failover event occurs, a note is made of it in the Event Log in the Application Log. The *Cisco Unity Failover Configuration and Administration Guide (With Microsoft Exchange)* contains a table that explains the causes of failover or failback based on the Event ID.

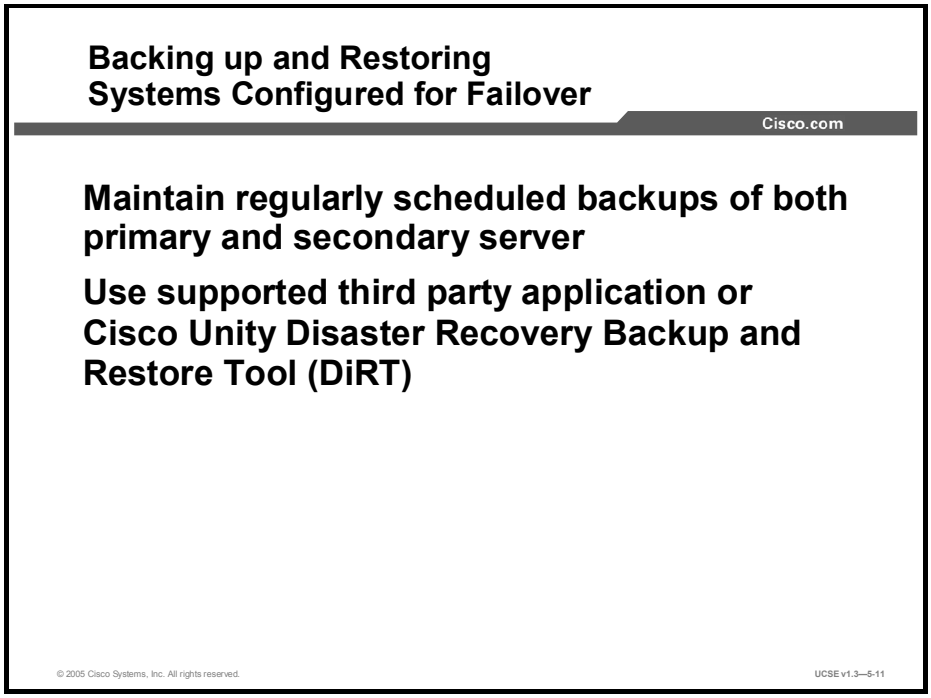
There are a number of scenarios for replacement or conversion of failover servers, as follows:

- Replacing the primary server
- Replacing the secondary server
- Replacing both servers
- Converting the secondary server to a permanent regular Cisco Unity server
- Converting the primary server to a permanent regular Cisco Unity server.

Each of these scenarios is covered in the *Cisco Unity Reconfiguration and Upgrade Guide (With Microsoft Exchange)*.

Backing Up and Restoring Systems Configured for Failover

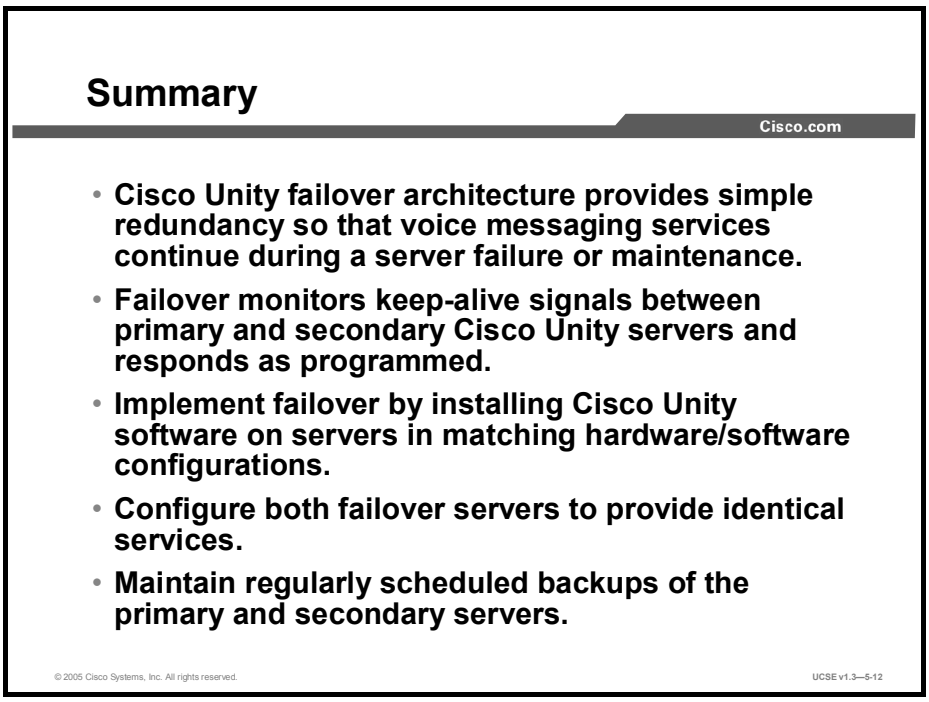
This topic describes the procedures for backup and restoration of systems configured for failover.



To prevent the loss of data caused by the failure of hardware components, it is important that you set up regular, scheduled backups of both the primary and secondary servers in a failover configuration. You can schedule backups using one of the supported third-party backup and restore applications, or the Cisco Unity Disaster Recovery Backup and Restore tool (DiRT). The procedure for backing up the primary and secondary servers is the same as for any other Cisco Unity system. Information on backing up any Cisco Unity system can be found in the *Cisco Unity Maintenance Guide* in the "Backing Up and Restoring a Cisco Unity System" chapter.

Summary

This topic summarizes the key points discussed in this lesson.



References

For additional information, refer to these resources:

- *Cisco Unity Failover Configuration and Administration Guide (With Microsoft Exchange)*
- *Cisco Unity Reconfiguration and Upgrade Guide (With Microsoft Exchange)*
- *Cisco Unity Maintenance Guide*

Lesson 7

Troubleshooting Common Problems

Overview

This lesson describes the most common problems facing a Cisco Unity system engineer. The lesson describes each problem, its symptoms, and its solutions.

Relevance

The Cisco Unity system engineer must be able to quickly diagnose common problems using available tools, and use recovery procedures that will minimize any disruption to Cisco Unity subscribers.

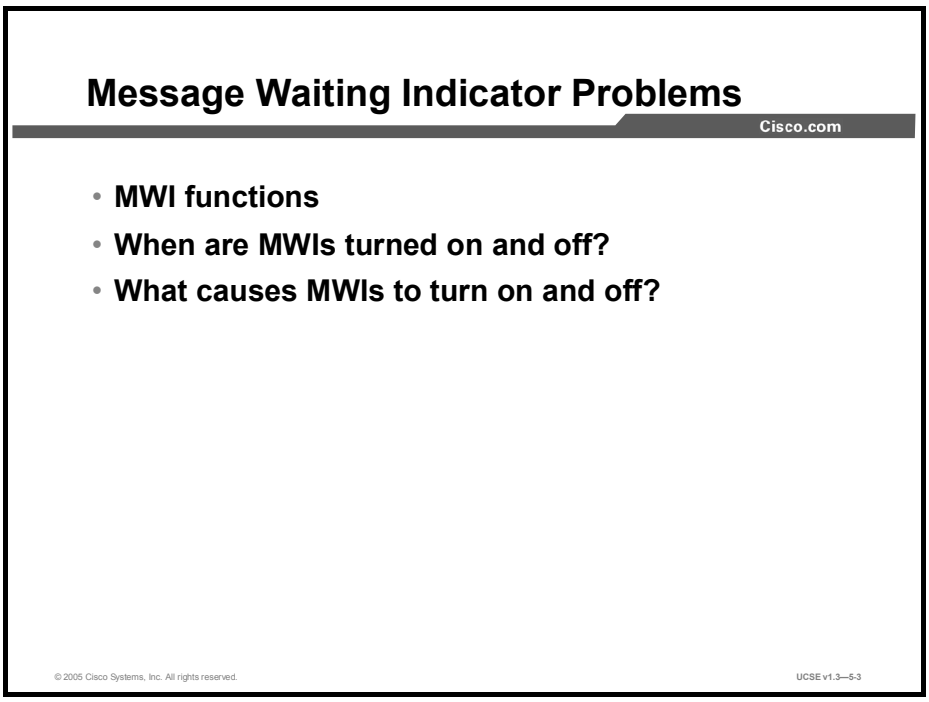
Objectives

Upon completing this lesson, you will be able to select and describe the best diagnostic tool to use to identify and correct each problem. This ability includes being able to meet these objectives:

- Describe how to troubleshoot problems with the MWI
- Describe how to troubleshoot call transfer problems
- Describe how to troubleshoot reorder tone problems
- Describe how to troubleshoot delayed, disappearing, or nondelivered message problems
- Describe how to troubleshoot subscriber and administrator access problems
- Describe how to troubleshoot Message Notification call problems
- Describe how to troubleshoot CPCA problems

Message Waiting Indicator Problems

This topic describes how to troubleshoot problems with Message Waiting Indicators (MWIs).



An MWI is a lamp, a flashing liquid crystal display (LCD) panel, or a special dial tone on subscriber phones that lets subscribers know a voice message is waiting. The type of indicator depends on the phone system and the phones that subscribers use. An MWI is not the same as a message notification, which is the feature that notifies a subscriber of new voice messages by calling a phone or pager, or by sending an e-mail message.

When Are MWIs Turned On and Off?

Following are the two principal events that cause Cisco Unity to activate and deactivate MWIs:

- When a caller leaves a new voice message for a subscriber, Cisco Unity notifies the phone system to activate the MWI on the phone for that subscriber.
- When the subscriber listens to the last new voice message, Cisco Unity notifies the phone system to deactivate the MWI on the phone.

Following are three additional events that cause Cisco Unity to activate and deactivate MWIs:

- When the subscriber saves a listened-to voice message as a new message, Cisco Unity notifies the phone system to activate the MWI on the phone for that subscriber.
- When a subscriber deletes a new voice message without listening to it, or moves it to another folder in Outlook, Cisco Unity notifies the phone system to deactivate the MWI on the phone.
- When MWIs are manually resynchronized—for example, by clicking **Resynchronize Now** on the Properties tab in the Cisco Unity Telephony Integration Manager (UTIM)—Cisco Unity queries the Data Object Hierarchy (DOH) to determine the MWI status of all phones and resets all MWIs as necessary.

An MWI remains activated under the following conditions when a subscriber listens to a new message:

- More messages are waiting to be heard. When all new messages are listened to, the MWI will be turned off.
- A new message arrives while the subscriber is listening to the original message. When all new messages are listened to, the MWI will be turned off.
- The subscriber listens on the phone to only part of the message and time stamp, then either hangs up or skips to the next message before hearing the entire message and time stamp.
- The server with the message store is offline and the message is stored in the Unity Message Repository (UMR).
- In the Inbox, the subscriber marks a listened-to message as unread (unified messaging only).
- The subscriber uses the Inbox in offline mode to listen to messages (unified messaging only).

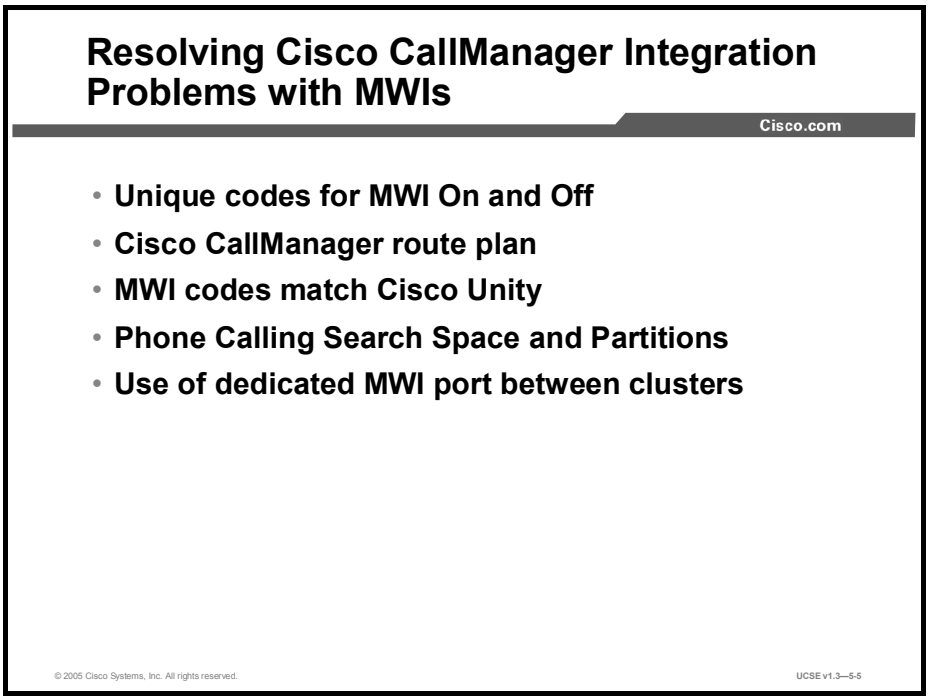
In the following situations, MWIs are not activated:

- E-mail messages arrive. Cisco Unity monitors only voice messages (unified messaging only).
- Fax messages arrive. Cisco Unity monitors only voice messages (unified messaging only).
- Return receipts arrive. Cisco Unity monitors only voice messages (unified messaging only).
- An Inbox rule automatically moves voice messages to another folder. Cisco Unity monitors only the Inbox (unified messaging only).
- The server with the message store is offline and the message is stored in the UMR.

What Causes MWIs to Turn On and Off?

Phone systems are generally set up with one code to turn MWIs on and a second code to turn MWIs off. Cisco Unity sends the code to the phone system to turn the MWI on or off. The MWI on and off codes are established at the PBX, whether Cisco CallManager or a circuit-switched PBX.

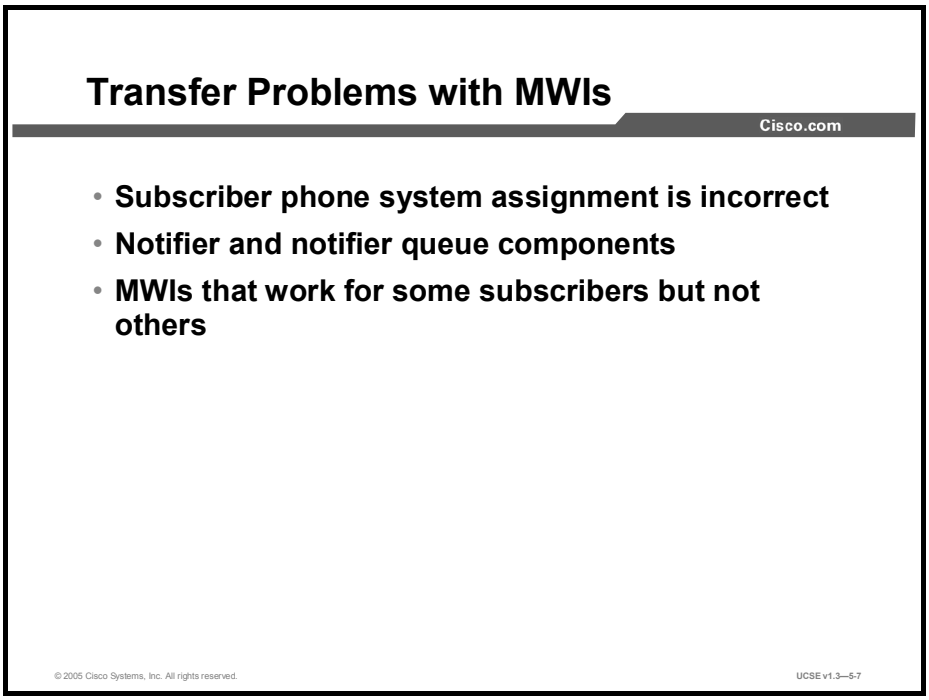
If you are using Cisco CallManager at the PBX, you enter these codes for Cisco Unity in the UTIM. Click **Programs > Cisco Unity > Unity Telephony Integration Manager** to access UTIM.



The following problems might occur if Cisco CallManager is integrated with Cisco Unity:

- The unique directory numbers for turning MWIs on and off may not have been entered in the Cisco CallManager server. For instructions on setting these directory numbers, refer to the applicable Cisco CallManager integration guide.
- A Cisco CallManager route plan may include the unique directory numbers for turning MWIs on and off. For example, a route plan could send all numbers starting with 9 to a gateway, while the extension that turns MWIs on is 99991. Revise the route plan so that it does not include the MWI directory numbers, or alter the directory numbers. For instructions on setting up route plans, refer to the applicable *Cisco CallManager Administration Guide* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm.
- The unique directory numbers for turning MWIs on and off may not have been entered in the MWI On Extension and MWI Off Extension fields in UTIM, or Cisco Unity may not have been restarted to enable these values. Enter the applicable values in UTIM. For instructions on setting these values in UTIM, refer to the applicable Cisco CallManager integration guide.
- The IP Phone may not be in the same calling search space and partition as the Cisco Unity voice messaging ports. From a phone, dial the directory number that turns on MWIs. If you hear the reorder tone, the directory number for turning MWIs on is not assigned the correct calling search space and partition in Cisco CallManager. If you do not hear the reorder tone but the MWI is not activated or deactivated, a route plan may be causing the problem.
- The unique directory numbers for turning MWIs on and off in Cisco CallManager may not be identical to the values entered in the MWI On Extension and MWI Off Extension fields in UTIM. Confirm the values and restart the Cisco CallManager servers and Cisco Unity server. For instructions on setting these values, refer to the applicable Cisco CallManager integration guide.

- If Cisco Unity integrates with multiple Cisco CallManager clusters, you need to dedicate at least one voice messaging port to set MWIs for each cluster. For example, in a two-cluster environment, there must be at least two ports dedicated to setting MWIs, one sending MWI requests for the first cluster and another sending MWI requests to the second cluster. Confirm that at least one voice messaging port is dedicated to each cluster and that the port is set to Dialout MWI. For instructions on configuring ports, refer to the applicable Cisco CallManager integration guide.

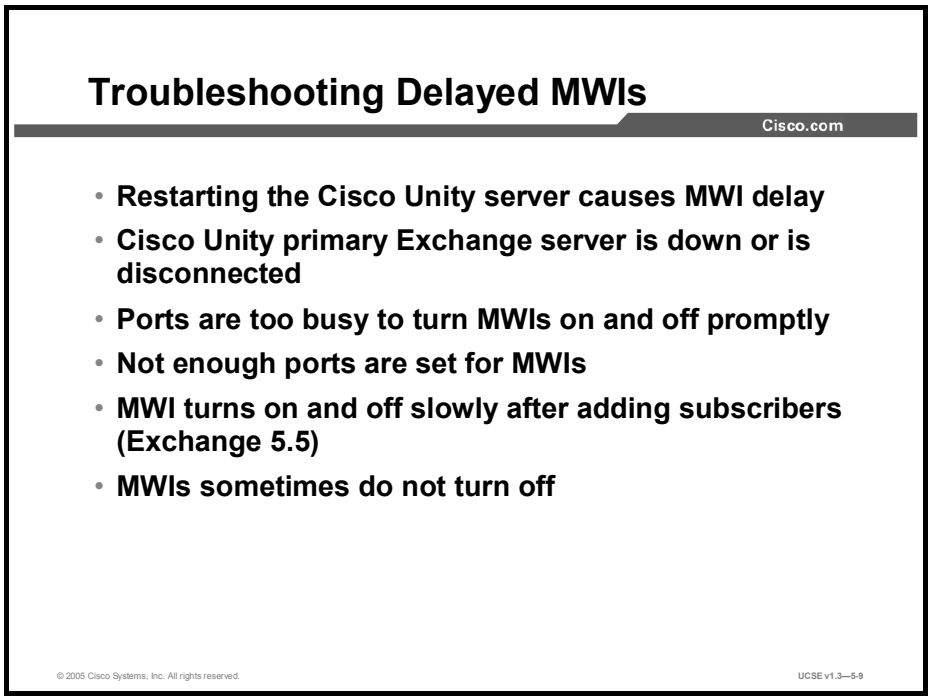


If the subscriber is assigned to the wrong phone system, confirm the subscriber phone system assignment (dual-phone system or former dual-phone system integration), as follows:

Step 1 In the Cisco Unity Administrator, go to the Subscribers > Subscribers > Profile page.

Step 2 In the Subscriber Information section, confirm that the correct phone system has been selected for the subscriber. Correct if necessary.

Step 3 If you made a change, click **Save**, then shut down and restart Cisco Unity.



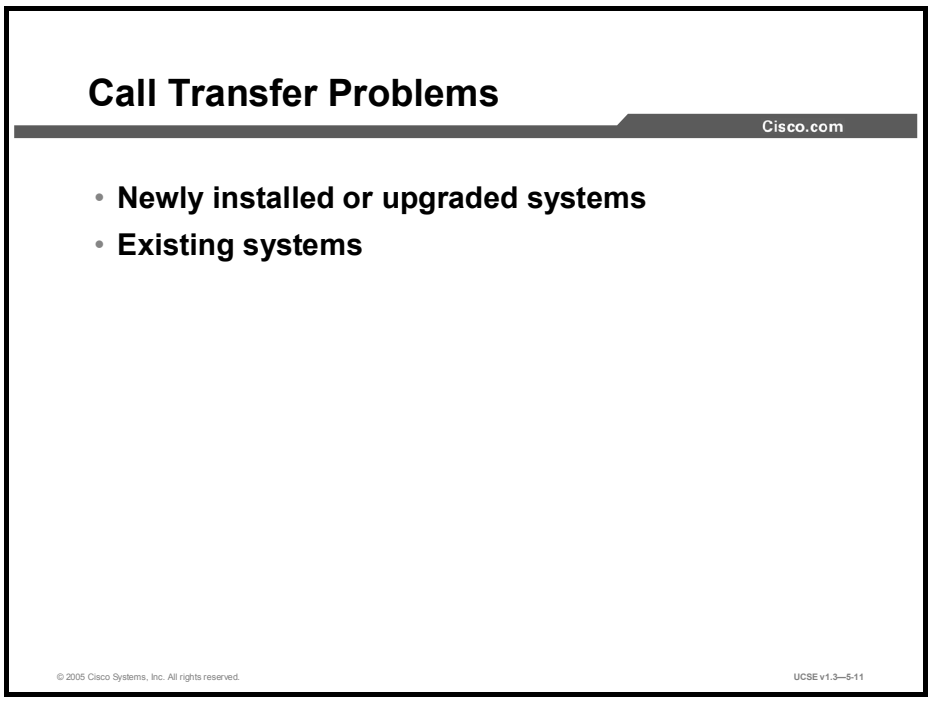
Some of the most common causes of MWI issues are as follows:

- Restarting the Cisco Unity servers sometimes causes MWI delay.
- Cisco Unity primary Exchange server is down or is disconnected.
- Ports are too busy to turn MWI on and off promptly.
- When Cisco Unity takes many messages, the ports assigned to turn MWIs on and off may not always be able to dial out promptly. A single port set to dial out only for message waiting indication with an IP Phone system integration can change approximately 240 to 360 MWIs per hour, depending on the phone system. An analog integration can take up to seven seconds per MWI change.
- There may not be enough ports set for MWIs. One way to check whether there are enough MWI ports set is to run a port usage report for just the MWI ports. If the percentage of ports used does not exceed 40 percent usage during peak periods, the number of message waiting indication ports is adequate. If the percentage of ports used exceeds 40 percent usage during peak periods, review the existing port configuration and determine if one or more additional ports can be set only to Dialout MWI.
- MWIs can turn on and off too slowly in an Exchange 5.5 server. The cause is often the creation or moving of many subscribers. When the new subscribers are created or imported, Cisco Unity creates a primary call handler on the Cisco Unity server. However, Exchange 5.5 needs to allocate additional threads to service MWIs for the new subscribers. The solution is to run Exchange 5.5 Optimizer, which allocates additional threads in Exchange. If there are other Exchange servers in the site, you do not need to run the Exchange Optimizer on the other Exchange servers.

- MWIs sometimes do not turn off. One possible reason for MWIs not turning off as expected is because the MWIs have lost synchronization. MWIs may lose synchronization if, for example, the phone system is off-line when an MWI status changes. There are two ways to resynchronize the MWIs. The first is to resynchronize the MWIs for all subscribers, and the second is to synchronize the MWI light for an individual subscriber. If the phone system has been off-line, you should resynchronize all subscribers. If an individual is having a problem, then resynchronizing their individual account will be a less processor-intensive activity.

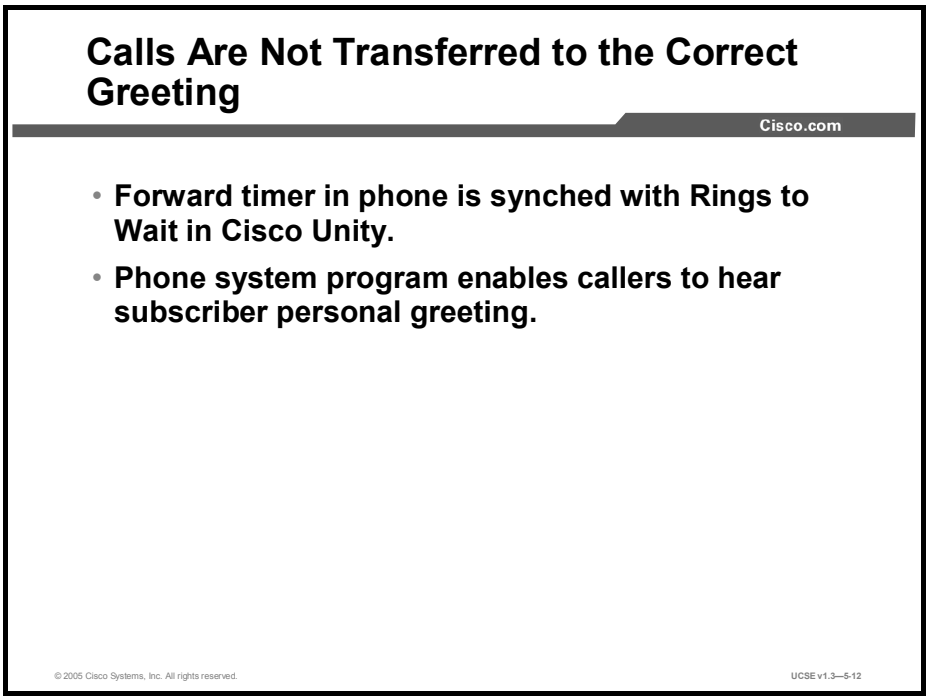
Call Transfer Problems

This topic describes how to troubleshoot call transfer problems.



Call transfer problems fall into two categories:

- **Problems on a newly installed or upgraded system:** For call transfer problems that occur on newly installed systems or on systems that have just been upgraded, the following items should be checked:
  - Check that the integration is complete.
  - Check that you can reach the opening greeting.
  - Check the call transfer rules.
  - Refer to the Cisco Unity integration guide for your system.
- **Problems on existing systems:** Call transfer problems that occur on existing systems include:
  - Calls are not transferred to the correct greeting.
  - The Forward Timer in the phone system is not synchronized with the Rings to Wait setting in Cisco Unity.
  - The phone system programming does not enable callers to hear the subscriber personal greeting.
  - The subscriber hears a reorder tone when answering a call from Cisco Unity.



When troubleshooting call transfers to the wrong greeting, the following tasks should be performed:

- Confirm that the forward timer in the phone system is synchronized with the Rings To Wait setting in Cisco Unity.
- Confirm that the phone system programming enables callers to hear the subscriber personal greeting.

For supervised transfers, the number of rings that Cisco Unity waits before routing a call to a subscriber personal greeting (or to another extension) can be reconfigured. If the phone system is programmed to forward calls, confirm that the phone system waits longer to forward a call than Cisco Unity waits before taking a message.

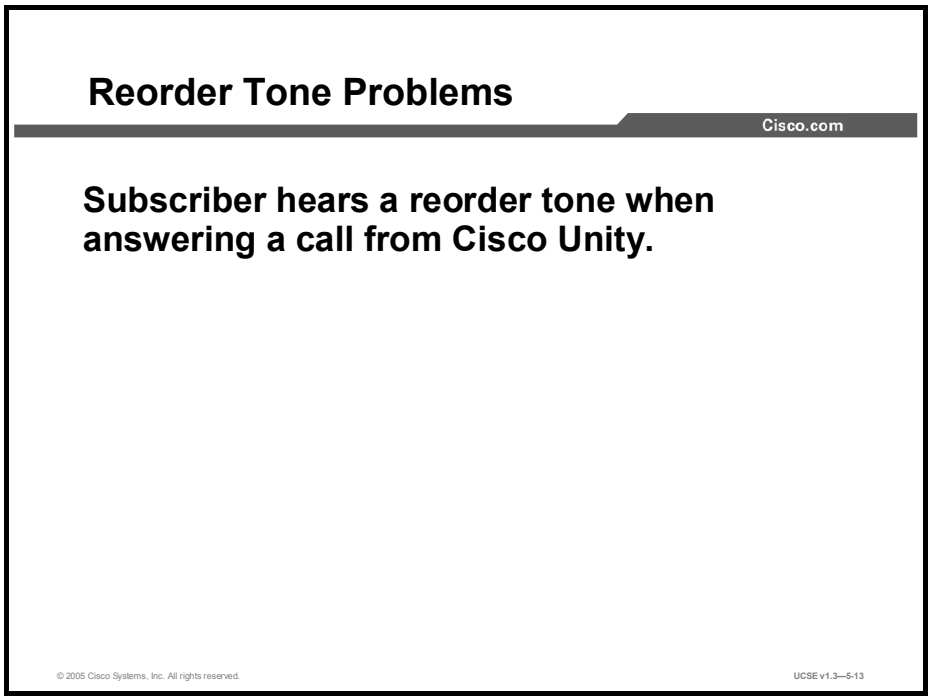
If the phone system is forwarding the call to another extension before Cisco Unity can take a message, the following may occur:

- The caller does not hear the beginning of the subscriber personal greeting. (For example, the subscriber's greeting is "Hi, this is Maria Ramirez. Please leave a message after the tone." But the caller hears only "...message after the tone.")
- The call is forwarded to another phone (for example, the operator) rather than to the subscriber's personal greeting.
- The call is forwarded to the opening greeting.
- The caller hears only ringing.

When callers hear the opening greeting instead of a subscriber's personal greeting after ringing that subscriber's extension, confirm that the integration is enabled and that the phone system settings are correct. If the settings are incorrect, call forward to personal greeting and easy message access will not be enabled.

Reorder Tone Problems

Reorder tone is also known as “fast busy” or “idiot” tone. It is the tone that generally plays if you leave a telephone off hook too long without dialing a number. This topic describes how to troubleshoot reorder tone problems.

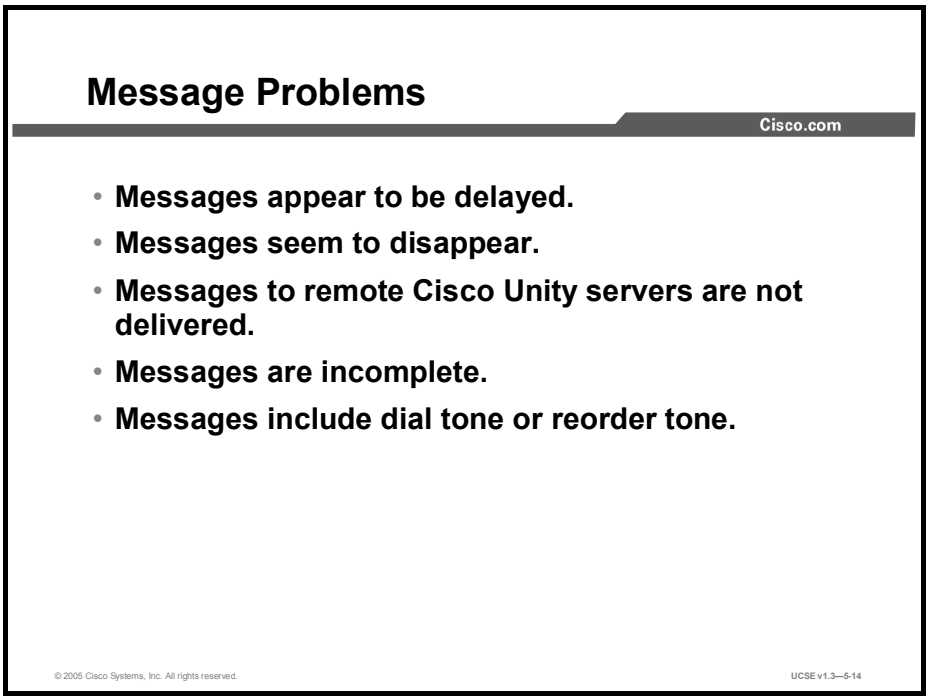


A possible cause for the problem of a subscriber hearing a reorder tone when answering a call from Cisco Unity is that the Rings to Wait settings are incorrect.

Cisco Unity requires a minimum setting of three rings to wait to properly transfer a call. If the number of rings to wait is set to fewer than three, a subscriber may hear the reorder tone instead of the Cisco Unity conversation.

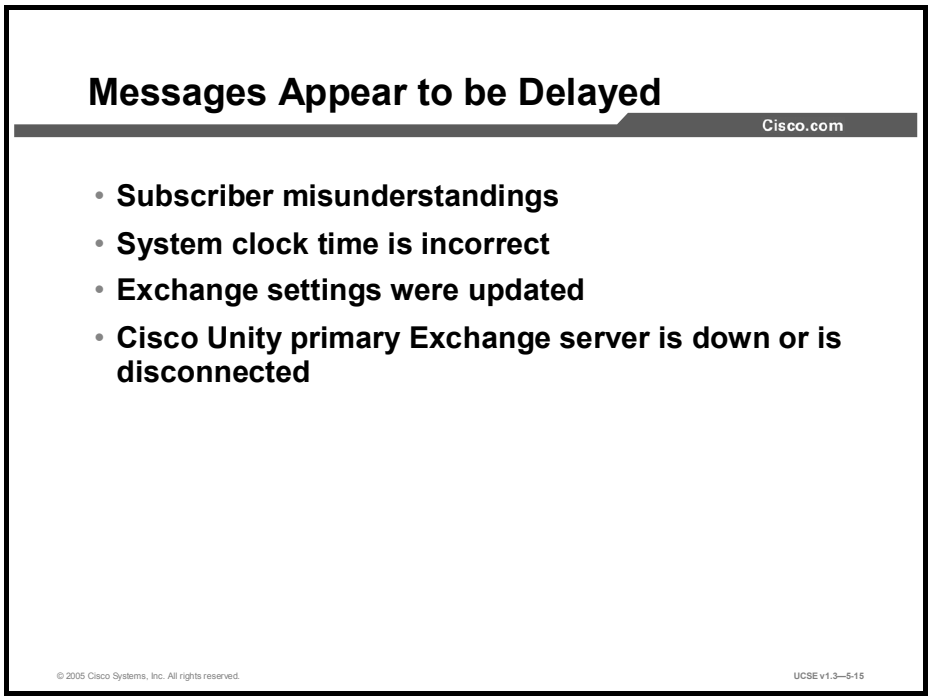
Message Problems

This topic describes how to troubleshoot delayed, disappearing, or nondelivered message problems.



Following are some of the common problems for messages:

- Messages appear to be delayed.
- Messages seem to disappear.
- Messages to remote Cisco Unity servers are not delivered.
- Messages are incomplete.
- Messages include dial tone or reorder tone.



Problem: Subscriber Misunderstandings

A subscriber who is using Optional Conversation 1 may misunderstand the effect of pressing the # key twice during message playback. When a subscriber presses the # key twice while listening to a message, Cisco Unity saves the message as a new message and skips to the next message. Later, the subscriber checks messages again, hears the same message, and believes the message arrived after a delay.

Solution: Explain to the subscriber that pressing the # key twice while a message plays saves it as a new message.

Problem: System Clock Time Is Incorrect

When the system clock is slow or when a desk clock is fast, the subscriber may believe messages were delayed.

Solution: Confirm that the system clock on the Cisco Unity server is reporting the correct time and that any clocks that the subscriber uses are accurate.

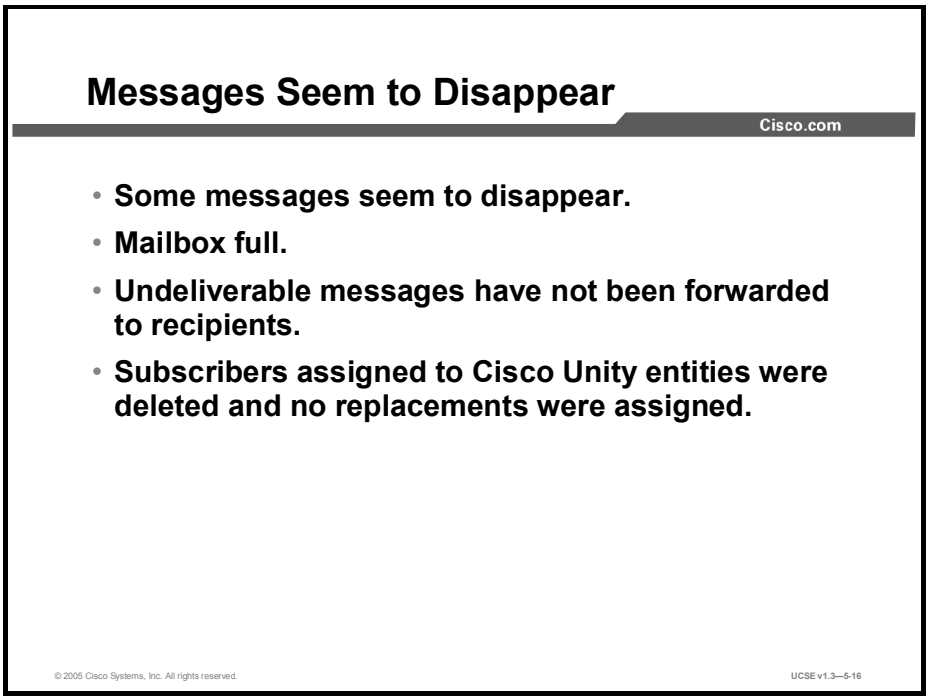
Problem: Exchange Settings Were Updated

When settings are changed for a subscriber in Exchange, the new values may not be reflected immediately in Cisco Unity.

Solution: Explain to the subscriber that the settings may take a few minutes to synchronize, causing a delay in receipt of messages.

Problem: Cisco Unity Primary Exchange Server Is Down Or Is Disconnected

Messages recorded while the primary Exchange server is down or disconnected are stored in the UMR until the server is brought back up. The delay experienced between the time a message is recorded and its delivery is dependent on the amount of time that the primary Exchange server was down or disconnected.



Problem: Some Messages Seem to Disappear

If the network or the home Exchange server is down, messages are being delayed. This applies only if there are multiple Exchange servers. Increasing the Max Open Retries value and decreasing the Open Interval value will increase the number of tries and decrease the wait time that Exchange uses when it tries to deliver a message after the network or server comes back up.

Solution: Change these Mail Transfer Agent (MTA) site configuration values, if needed, in the Exchange Administrator.

Problem: A Mailbox Is Full

By default, Cisco Unity does not check whether a subscriber mailbox has exceeded the Prohibit Send and Receive limit before allowing a caller to leave a message, although Cisco Unity does check before sending the message to the subscriber mailbox. If the subscriber mailbox is no longer allowed to receive messages, Cisco Unity handles the message in one of two ways:

- If the message was left by an unidentified caller—an outside caller or a caller from inside the organization calling from a phone that is not associated with a subscriber account (such as a conference room)—Cisco Unity sends the message to the Unaddressed Messages distribution list, which should be monitored by the Cisco Unity system administrator or another subscriber.
- If the message was left by another subscriber, Cisco Unity sends a non-delivery receipt (NDR) message to the subscriber who left the message.

Problem: Undeliverable Messages Have Not Been Forwarded to Recipients

Messages returned to the Cisco Unity Messaging System mailbox are forwarded automatically to subscribers whose names appear on the Unaddressed Messages public distribution list. The messages then must be forwarded to the intended recipients.

Solution: Explain to subscribers on the Unaddressed Messages public distribution list the importance of regularly checking for and forwarding undeliverable messages.

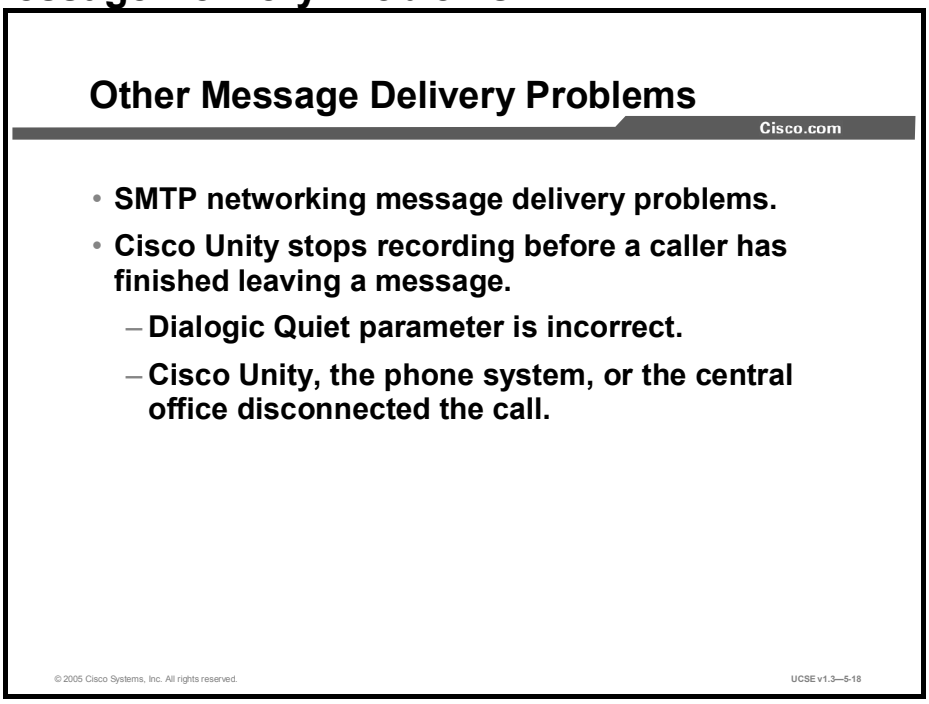
Problem: Subscribers Assigned to Cisco Unity Entities Were Deleted and No Replacements Were Assigned

Messages may be lost if you do not assign another subscriber or a public distribution list to replace a deleted subscriber who was assigned to review messages sent to any of the following Cisco Unity entities:

- Unaddressed Messages distribution list
- System Event Messages distribution list (by default, the Example Administrator is the only member of this distribution list)
- Operator call handler (by default, the Example Administrator is the only member of this distribution list)
- Opening Greeting call handler
- Goodbye call handler
- Example Interview call handler

Solution: To identify call handlers that are associated with improperly deleted accounts, run the Unresolved References report. Then you can fix any “stranded” call handlers that you find by running the DbWalker utility.

Other Message Delivery Problems



Troubleshooting SMTP Networking Message Delivery Problems

By understanding the path of a voice message as it is routed via Simple Mail Transfer Protocol (SMTP) networking to a remote Cisco Unity server, you can use applicable tools to troubleshoot message delivery problems.

The path of a voice message is similar, whether the subscriber who sent the message used blind addressing, or addressed the message to an Internet subscriber on the local server that corresponds to a subscriber on a remote Cisco Unity server. The path is as follows:

1. On the phone, a subscriber addresses a message to a subscriber on another Cisco Unity server.
2. Cisco Unity searches for a matching extension or delivery location.
   - If a matching extension is found, voice confirmation is provided, and Cisco Unity obtains the SMTP address from the Internet subscriber account and addresses the message.
   - If a matching delivery location is found, the number that the subscriber entered is used for the address.
   - In both cases, Cisco Unity forms an address in the following format and gives the message to Exchange:
     VOICE: <Delivery Location Dial ID>_<Extension>
3. Because the message has the VOICE address type, Exchange hands off the message to the Voice Connector.
4. The Voice Connector obtains the domain name from the delivery location and constructs the To address in the following format:
   SMTP: IMCEAVOICE <Delivery Location Dial ID>_<Extension>@<Domain Name>

5. The Voice Connector obtains information from the primary location and constructs the From address in the following format:
   SMTP: IMCEAVOICE<Primary Location Dial ID>_<Extension>@<Domain Name>. If the message is from an unidentified caller to an Internet subscriber, the From message is constructed in the following format:
   SMTP: IMCEAVOICE-<Primary Location Dial ID>_unknown@<Domain Name>
6. The Voice Connector converts the message to Multipurpose Internet Mail Extension (MIME) and then hands the message back to Exchange to be sent through the Exchange SMTP gateway.
7. On the receiving side, because of the IMCEAVOICE address type, Exchange hands the message over to the Voice Connector for processing, if the receiving server is a Cisco Unity server or is an Exchange server within a Cisco Unity installation.
8. The Voice Connector parses the To address and looks for a matching primary location and a matching subscriber extension at that location to obtain the e-mail address for the recipient. If a match is found, the Voice Connector addresses the message appropriately so that it can be delivered by Exchange. If a match is not found, an NDR is returned to the sender.
9. The Voice Connector parses the From address and looks for a matching Internet subscriber. If a match is found, the Voice Connector changes the From address so that the sender is identified when the recipient listens to the message.
10. The Voice Connector converts the MIME message back to a voice message.
11. The Voice Connector sends the message back to Exchange to be delivered to the subscriber.

Cisco Unity Stops Recording Before a Caller Has Finished Leaving a Message

Dialogic Quiet Parameter Is Incorrect

A caller may report hearing a prompt and being prevented from completing a message, or a subscriber may report this problem after noticing that a recording ends before the caller finished leaving a message. This can happen when the Dialogic Quiet parameter is not set to recognize low voice volume. It can also happen when a changed Dialogic Quiet parameter is not retained after a Cisco Unity upgrade. Another possibility is that the caller has reached the end of the maximum recording time. In that case, the message will be exactly 300 seconds long (or whatever the value is for that subscriber).

Cisco Unity, The Phone System, or the Central Office Disconnected the Call

If a caller reports being cut off while leaving a message and if the caller did not hear a prompt prior to the disconnect, Cisco Unity, the phone system, or the central office may have disconnected the call.

To determine why the call was disconnected, perform the following steps:

Step 1 On the Windows Start menu, click **Programs > Administrative Tools > Event Viewer**.

Step 2 On the Log menu, click **System**.

Step 3 In the System Event log, look for an error that occurred at the time of the reported disconnected call.

If an error appears, double-click the error and skip to Step 6.

If no error appears for the date and time of the disconnected call, continue with Step 4.

Step 4 On the Log menu, click **Application**.

Step 5 In the Application Event log, look for an error that occurred at the time of the reported disconnected call. Double-click the error.

Step 6 In the Event Detail dialog box, review the contents of the Description box.

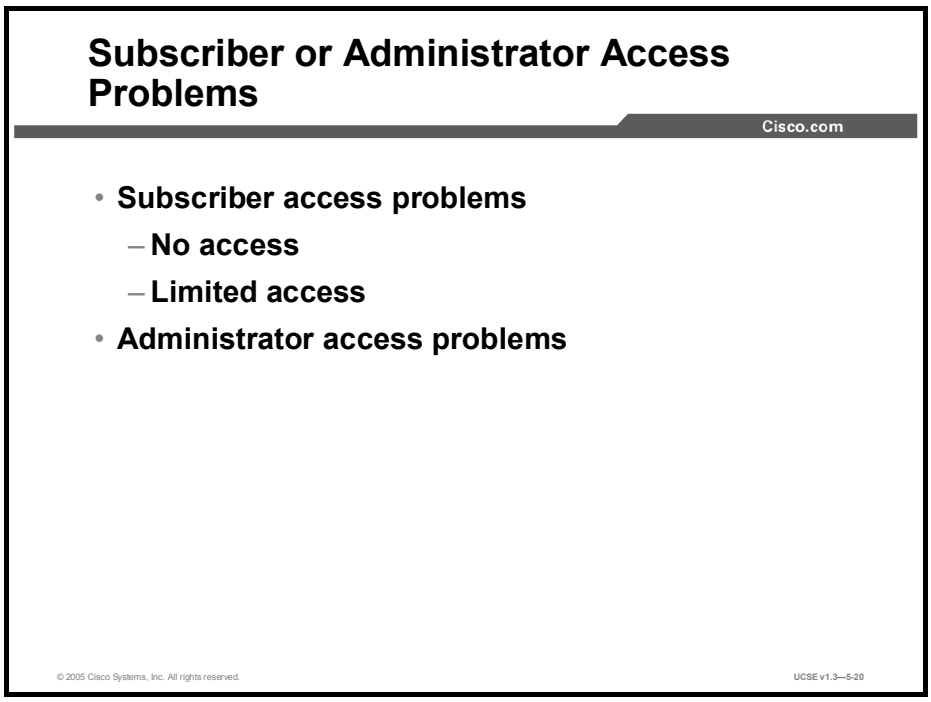
If you need assistance interpreting or resolving the error, or if no error appears in the Application Event log that matches the date and time of the reported disconnected call, contact Cisco Technical Assistance Center (TAC).

Dial Tone or Reorder Tone Is Present at the End of a Message

A possible cause may be that the switch disconnect tone or the public switched telephone network (PSTN) disconnect tone is incorrect in the switch.ini file (for circuit-switched phone systems only). Running the Learn Tones utility will correct the switch.ini file so that Cisco Unity will recognize dial tone and reorder tone, preventing them from being recorded as part of a message.

Subscriber and Administrator Access Problems

This topic describes how to troubleshoot subscriber and administrator access problems.



Subscriber access problems are usually related to a problem with the phone system integration. The following problems that can be encountered prevent subscribers from using Cisco Unity:

- Subscribers logging on to Cisco Unity hear the opening greeting instead of the subscriber conversation.

  Solution: Confirm that the integration is enabled and that the phone system settings are correct.

  To verify the phone system settings in the Cisco Unity Administrator:

  Step 1 On the Windows Start menu on the Cisco Unity server, click **Programs > Cisco Unity > Manage Integrations**. The Cisco Unity Telephony Integration Manager (UTIM) appears.

  Step 2 Confirm that the settings match those indicated in the integration guide for your phone system.

  Step 3 Correct any incorrect values for the phone system.

  Step 4 If you changed values in Step 3, click **Save**.

  Step 5 If prompted, restart the Cisco Unity server.

  Step 6 If you have confirmed that the integration is enabled and that the phone system settings are correct, and subscribers still hear the opening greeting instead of the subscriber conversation, contact Cisco TAC.

- Cisco Unity does not respond to touch tones.
  - (Cisco CallManager only) Confirm that DTMF relay is enabled through VoIP dial-peer gateways.
  - (Circuit-switched phone systems only) Confirm that the DTMF signal is being sent.
  - (Circuit-switched phone systems only) Confirm that the DTMF values are consistent with Cisco Unity and the phone system.

The following problems that can be encountered prevent subscribers from fully using the features of Cisco Unity and the phone system:

- Subscribers cannot use ViewMail for Outlook.
- Cisco Personal Communications Assistant pages cannot be opened or have been defaced.
- Subscribers cannot access Cisco Personal Communications Assistant (CPCA) pages.
- Subscribers cannot access the Cisco Unity Assistant or Cisco Unity Inbox from the Cisco PCA.
- Subscribers cannot save changes on pages in the Cisco Unity Assistant or the Cisco Unity Inbox.
- No sounds play on the multimedia system after installing the Cisco CallManager software.
- Subscribers cannot be located in a new or updated directory handler.

The following administrator access problems can be encountered:

- Cisco Unity Administrator or Status Monitor pages cannot be opened or have been defaced.
- Cisco Unity Administrator page cannot be accessed after an upgrade.

The following error message may appear after a Cisco Unity upgrade, or application of a Microsoft service pack:

```
Error Message   Access Denied. Your browser must have cookies
enabled to access the Unity web pages.
```

This error can occur if cookies are not enabled, or if the Cisco Unity server name contains unsupported Domain Name System (DNS) characters.

Recommended Action: Do the following procedure, to enable cookies on the Cisco Unity server and confirm the server name:

Step 1 In Internet Explorer, click **Tools > Internet Options**.

Step 2 On the Privacy tab, under the Security options for Intranet, confirm that the Settings slide bar is not set to Block All Cookies.

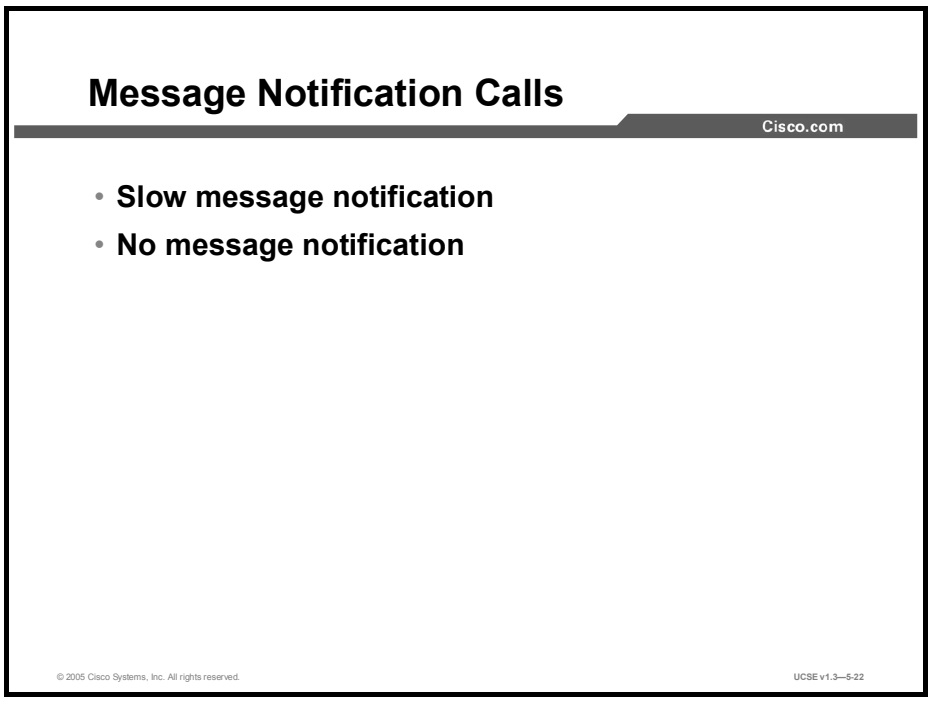
Step 3 In Internet Explorer, click **Help > About Internet Explorer**. Confirm that the version is 6.0 and that SP1 is installed. With SP1, all ASP cookies are blocked if the server name contains non-DNS supported characters, such as an underscore.

Step 4 On the desktop, right-click **My Computer**, then click **Properties**.

Step 5 On the Network Identification tab, confirm that the computer name contains only DNS-supported characters. Note that DNS-supported characters include A through Z, a through z, and 0 through 9. The underscore is not supported. If your server name contains non-DNS-supported characters, change the server name to use only DNS-supported characters.

Message Notification Problems

This topic describes how to troubleshoot message notification problems.



When multiple subscribers report that message notification is slow, or communication problems between Exchange and Cisco Unity delay messages, a port setup problem is the likely cause. You need to ensure that Network Time Protocol (NTP) is running and both the Exchange system and Cisco Unity system share the same NTP reference. If the time is off, it could cause delays of up to a day. Isolated complaints about slow message notification are likely related to a subscriber's message notification settings. The following items need to be checked:

- Confirm that the Exchange server is not down or disconnected.
- Confirm that ports are not too busy to handle message notification.
- Confirm that there are enough ports assigned to message notification.
- Confirm that the phone system sends calls to ports that are set to answer calls.

To troubleshoot slow message notifications for multiple subscribers, perform the following actions:

- Confirm that the Exchange server is not down or disconnected.
- Confirm that there are enough ports assigned to message notification.
- Confirm that the phone system sends calls to ports that are set to answer calls.
- Confirm that ports are not too busy to handle message notification.

Some system problems can prevent Cisco Unity from making any notification calls. When a subscriber sets up message notification incorrectly, it can prevent Cisco Unity from making any notification calls to that subscriber.

To troubleshoot nonfunctional message notifications for a subscriber, perform the following actions:

- Confirm that message notification is enabled for the correct types of messages.
- Confirm that the message notification phone number includes the access code for an external line if notification is to an external phone.
- Confirm that the notification device is enabled.
- (Dual phone system integrations only) Confirm that the notification device is assigned to the correct phone system.

Unity Restriction Tables

When a subscriber uses the Cisco Unity Assistant or the Cisco Unity conversation to attempt to change a phone number that will be used for message notification, fax delivery, or call transfer, Cisco Unity applies the appropriate restriction table to verify that the phone number entered is allowed. The same thing happens when you use the Cisco Unity Administrator to attempt to change a phone number that will be used for message notification, fax delivery, or call transfer. In each case, the restriction table used is the one associated with the subscriber or administrator who is changing the number.

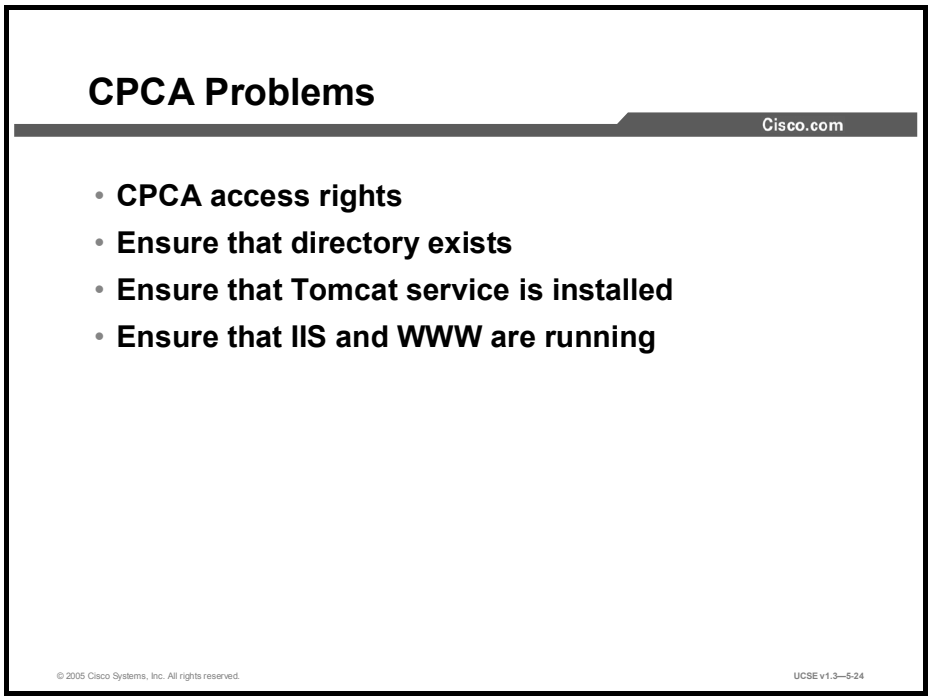
For example, if a subscriber uses the Cisco Unity Assistant to enter a phone number on the Message Notification page, and then saves the page, Cisco Unity applies the restriction table associated with class of service of that subscriber, and displays an error message if the phone number is not allowed. But when an administrator changes a message notification number for a subscriber by using the Cisco Unity Administrator, Cisco Unity applies the restriction table associated with the administrator class of service, not the class of service of the subscriber. Therefore, an administrator can, when necessary, override the limitations of the class of service of a particular subscriber.

Each row of a restriction table is made up of a dial string. Each dial string consists of a call pattern and a setting that specifies whether numbers matching the call pattern are permitted for use. The restriction table is applied when a subscriber or an administrator attempts to change a number controlled by a restriction table, not when Cisco Unity tries to complete a transfer or delivery. (Note, however, that the Audio Messaging Interchange Specification (AMIS) restriction table is applied every time a message is sent to an AMIS subscriber or an AMIS location.)

When a restriction table is applied to a number, such as a pager number for a message notification, Cisco Unity compares the number with the call pattern of the first dial string in the restriction table. If the number does not match the call pattern, Cisco Unity then compares the number with the call pattern in the second dial string, and so on, until it finds a match. When Cisco Unity finds a match, it either permits or restricts the use of this number as specified in the dial string.

CPCA Problems

This topic describes how to troubleshoot Cisco Personal Communications Assistant (CPCA) problems.



When the CPCA fails to operate properly, follow these steps:

Step 1 If there is an error message associated with the problem, review the "CPCA Error Messages."

Step 2 Confirm that the CommServer\Cscoserv directory exists on the Cisco Unity server, and that it contains Java2SDK, Tomcat, bin, and ciscopca directories.

Step 3 Check that the Tomcat service is installed and that the service has started.

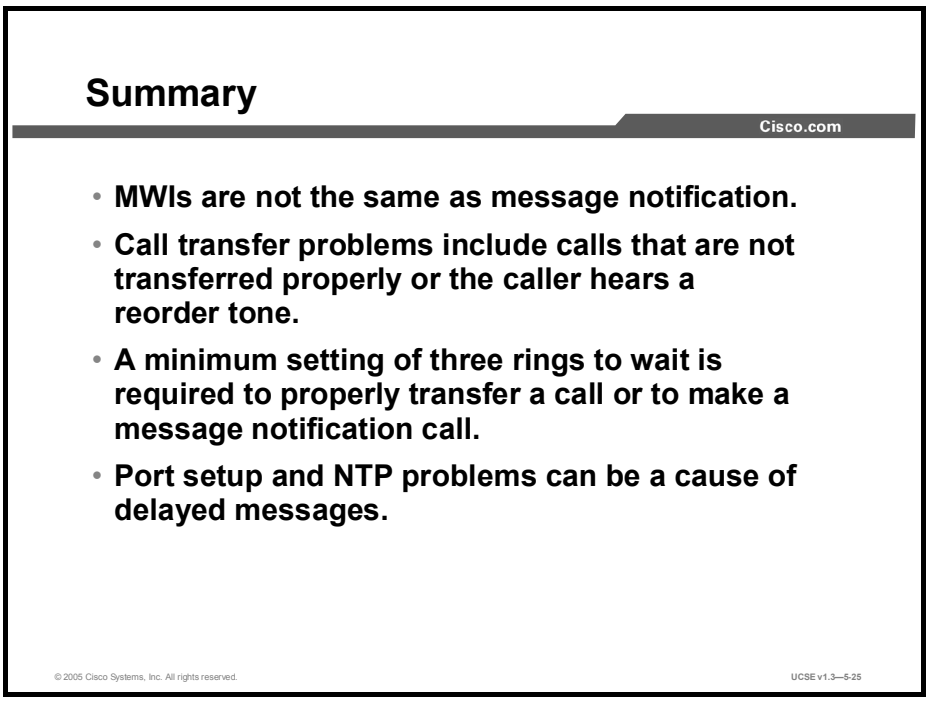
Step 4 Check that the World Wide Web Publishing Service is installed and that the service has started.

Step 5 Check that Internet Information Services (IIS) and the CPCA components are configured correctly.

Step 6 Check that the IIS and Tomcat integration is configured correctly.

Summary

This topic summarizes the key points discussed in this lesson.



Next Steps

For the associated lab exercises, refer to the following sections of the course Lab Guide:

- Lab 5-1: Troubleshooting Delayed Message Notification Problems
- Lab 5-2: Troubleshooting Message Waiting Indicator Problems
- Lab 5-3: Troubleshooting Delayed Message Problems
- Lab 5-4: Troubleshooting CPCA Problems

Quiz

Use the practice items here to review what you learned in this lesson. The correct answers are found in the Quiz Answer Key.

Q1) What is the purpose of MWI?

A) to let the administrator know there is a new message
B) to let Cisco Unity know there is a new message
C) to let the subscriber know there is a new message
D) to let the Exchange server know a new message has arrived

Q2) Which of the following is a common problem with call transfers?

A) Calls are being sent to Cisco CallManager.
B) Calls are not transferred to the correct greeting.
C) Calls are not sent to the subscriber telephone.
D) Calls are not directed to the operator.

Q3) Which of the following is a possible cause for hearing reorder tone?

A) Rings to Wait settings are incorrect.
B) Cisco Unity requires a minimum of 2 rings to wait to transfer a call.
C) Cisco Unity requires a minimum of 2 rings to wait for message notification.
D) Subscriber hangs up before the call is answered.

Q4) If Exchange is not running, messages may _____.

A) appear to never be taken
B) appear to never be delivered
C) appear to be delayed
D) appear to be deleted
E) appear to be repeated

Q5) Subscriber login problems can generally be related to which types of problems? (Choose two.)

A) Cisco Unity server is down
B) access rights
C) Exchange server is down
D) administrator password not set correctly

Q6) Which port property has to be enabled to send message notifications?

A) TRAP
B) MWI
C) message notification
D) disabled
E) answer mode

Q7) CPCA requires which service to be running?

A) AVGain
B) CPCA login
C) IIW and WWS
D) Tomcat
E) Catman

Quiz Answer Key

Q1) C

Relates to: Message Waiting Indicator Problems

Q2) B

Relates to: Call Transfer Problems

Q3) A

Relates to: Reorder Tone Problems

Q4) C

Relates to: Message Problems

Q5) A, B

Relates to: Subscriber and Administrator Access Problems

Q6) C

Relates to: Message Notification Problems

Q7) D

Relates to: CPCA Problems

Module Self-Check

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

Q1) The Advanced Setting tool is used to _____.

A) see the current licenses for your Cisco Unity system
B) remove Cisco Unity subscriber properties from Active Directory accounts
C) move subscriber settings from a Cisco Unity subscriber account to a mail user account
D) safely edit many of the hidden registry settings

Q2) The Migrate Data Subscriber utility is used to _____.

A) copy user information from voice-mail accounts to e-mail accounts
B) copy user information from e-mail accounts to voice-mail accounts
C) upgrade to a newer version of Cisco Unity
D) remove Cisco Unity subscriber properties from Active Directory accounts

Q3) The Remove Subscriber Properties tool may be valuable when you need to _____.

A) see the current licenses for your Cisco Unity system
B) remove Cisco Unity subscriber properties from Active Directory accounts
C) move subscriber settings from a Cisco Unity subscriber account to a mail-user account
D) safely edit many of the hidden registry settings

Q4) The Cisco Unity License Viewer may be helpful if you _____.

A) need to move users from one system to another
B) are not permitted to install a new feature
C) need to uninstall Cisco Unity 2.0
D) need to test a specific call handler

Q5) Which of the following is *not* removed by the Cisco Unity Uninstaller utility?

A) Cisco Unity-related registry settings
B) Cisco Unity-related directories
C) Cisco Unity-related WAV drivers
D) Cisco Unity-related files

Q6) How many different versions of the Status Monitor are there?

A) one
B) two
C) three
D) four

Q7) The greeting codecs can be converted with which tool or utility?

A) Set Record Format
B) Set Wave Format
C) Wave Gain
D) Codec Checker

Q8) The Set Volume tool:

A) sets overall volume
B) adjusts volume on already recorded WAV files
C) sets playback volume
D) sets record volume

Q9) Which utility is used to define the recording codec?

A) Set Record Format
B) Set Wave Format
C) Wave Gain
D) Codec Checker

Q10) The overall volume for new recordings can be set with _____.

A) Set Record Format
B) Set Wave Format
C) Wave Gain
D) Codec Checker

Q11) Which tool or utility can be used to display the codec for a given WAV file?

A) Set Record Format
B) Set Wave Format
C) Wave Gain
D) Codec Checker

Q12) "Warnings" in the Database Walker utility are _____.

A) red
B) yellow
C) green
D) blue

Q13) _____ is a monitoring service that's useful for tracking Cisco Unity performance.

A) SysCheck utility
B) Directory Access Diagnostics
C) Database Walker utility
D) CUPID

Q14) The Unity Diagnostics Viewer works in conjunction with the _____.

A) Database Walker
B) CUPID
C) Directory Access Diagnostics
D) Unity Diagnostic tool

Q15) With diagnostic micro traces, each component has up to _____ individual traces.

A) 4
B) 8
C) 16
D) 32

Q16) Which tool checks the Cisco Unity Directory Service account permissions to manage single-user objects?

A) SysCheck utility
B) Directory Access Diagnostics
C) Database Walker utility
D) CUPID

Q17) SysCheck is primarily a _____-checking application.

A) rights
B) database
C) log
D) subscriber

Q18) Which tool is used to set the number of rings before Cisco Unity will answer a call?

A) Integration Monitor
B) Edit Switch utility
C) Edit Caller utility
D) Call Viewer utility

Q19) Raw packet information can be viewed with the _____.

A) Integration Monitor
B) Edit Switch utility
C) Edit Caller utility
D) Call Viewer utility

Q20) The Call Viewer Application shows _____.

A) raw packet information for incoming calls on an IP integration
B) raw packet information from a circuit-switched PBX
C) basic call information for incoming calls on an IP integration
D) basic call information from a circuit-switched PBX

Q21) The Integration Monitor works with _____.

A) circuit-switched PBX integration
B) IP telephony integration
C) both
D) neither

Q22) Which tool is most likely to "break" the integration if not used properly?

A) Integration Monitor
B) Edit Switch utility
C) Edit Caller utility
D) Call Viewer utility

Q23) If Cisco Unity stops recording a message before a call is finished, the problem could *not* be that _____.

A) Cisco Unity disconnected the call
B) the central office disconnected the call
C) Tomcat services are not installed
D) the Dialogic Quiet parameter is incorrect

Q24) Tomcat is integral to the function of the _____.

A) CPCA
B) Call handlers
C) Mailboxes
D) System clock

Q25) Administrator access problems to the server could result if _____.

A) a mailbox is full
B) the SMTP address is incorrect
C) cookies are not enabled
D) the system clock is incorrect

Q26) When troubleshooting call transfer problems, it is important to confirm that the _____.

A) forward timer in the phone system is synchronized with the Rings To Wait setting in Cisco Unity
B) phone system programming enables callers to hear the subscriber personal greeting
C) forward timer in the phone system is synchronous with the Rings to Wait setting in Cisco Unity
D) all of the above

Q27) With Dual Phone System Integration, you *must* _____.

A) confirm that message notification is enabled for the correct types of messages
B) confirm that the message notification phone number includes the access code for an external line if notification is to an external phone
C) confirm that the notification device is enabled
D) confirm that the notification device is assigned to the correct phone system

Q28) MWIs will *not* be activated by _____.

A) faxes
B) new voice mails
C) saved voice mails
D) additional voice mails in queue

Q29) Cisco Unity requires a minimum setting of _____ ring(s) to wait to properly transfer a call.

A) one
B) two
C) three
D) four

Module Self-Check Answer Key

Q1) D, safely edit many of the “hidden” registry settings.

Q2) A, copy user information from voice-mail accounts to e-mail accounts.

Q3) B, remove Unity subscriber properties from Active Directory accounts.

Q4) B**,** are not permitted to install a new feature.

Q5) C, Unity related WAV drivers

Q6) B, two

Q7) B, Set Wave Format

Q8) B, adjusts volume on already recorded WAV files

Q9) A, Set Record Format

Q10) C, Wave Gain

Q11) D, Codec Checker

Q12) B, yellow

Q13) D, CUPID

Q14) D, Unity Diagnostic Tool

Q15) D, 32

Q16) B, Directory Access Diagnostics

Q17) A, rights

Q18) B, Edit Switch utility

Q19) A, Integration Monitor

Q20) C, basic call information for incoming calls on an IP integration

Q21) A, circuit-switched PBX integration

Q22) B, Edit Switch utility

Q23) C, Tomcat services are not installed

Q24) A, CPCA.

Q25) C, cookies are not enabled.

Q26) D, All of the above.

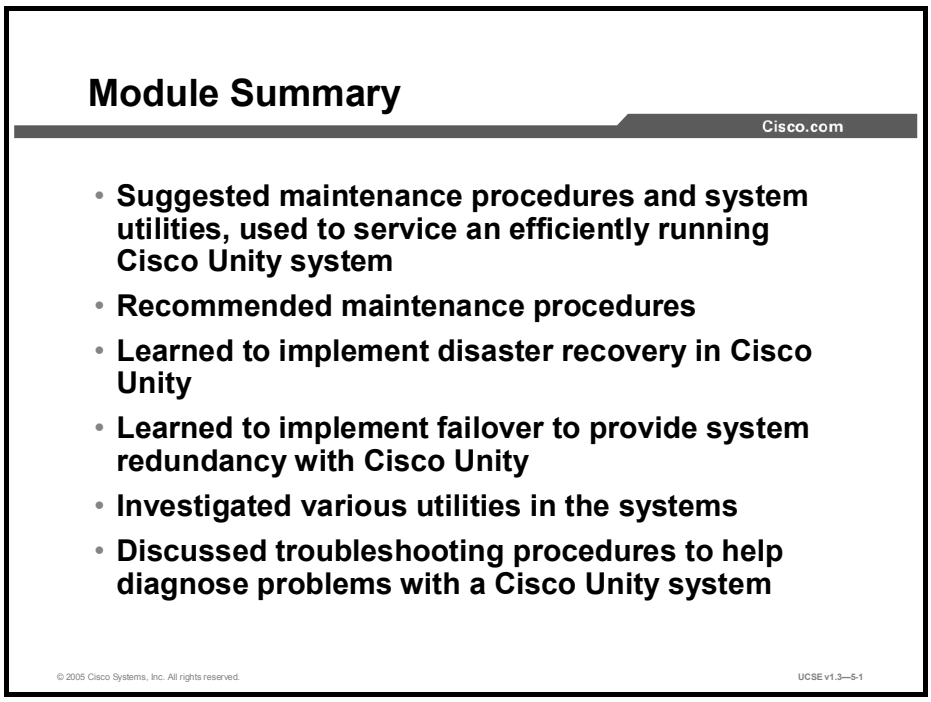
Q27) D, confirm that the notification device is assigned to the correct phone system.

Q28) A, faxes.

Q29) C, 3

Module Summary

This topic summarizes the key points discussed in this module.



Having completed this module, you should now be able to:

- Describe the recommended maintenance procedures for Cisco Unity
- Describe and be able to implement disaster recovery in Cisco Unity
- Describe and be able to implement failover in Cisco Unity
- Describe the utilities and their functions in Cisco Unity
- Describe troubleshooting procedures for Cisco Unity

UCSE

Cisco Unified Communications System Engineer

Version 1.3

Lab Guide

CLS Production Services: 06.29.05

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

UCSE

Lab Guide

Overview

This guide presents the instructions and other information concerning the activities for this course. You can find the solutions in the activity Answer Key.

Outline

This guide includes these activities:

- Lab 2-1: Installing Cisco Unified Communications Software (Exchange)
- Lab 2-2: Installing Cisco Unified Communications Software (Domino)
- Lab 3-1: Digital Networking in Cisco Unity
- Lab 5-1: Troubleshooting Delayed Message Notification Problems
- Lab 5-2: Troubleshooting Message Waiting Indicator Problems
- Lab 5-3: Troubleshooting Delayed Message Problems
- Lab 5-4: Troubleshooting CPCA Problems

Lab 2-1: Installing Cisco Unified Communications Software (Exchange)

Complete this lab activity to practice what you learned in the related module.

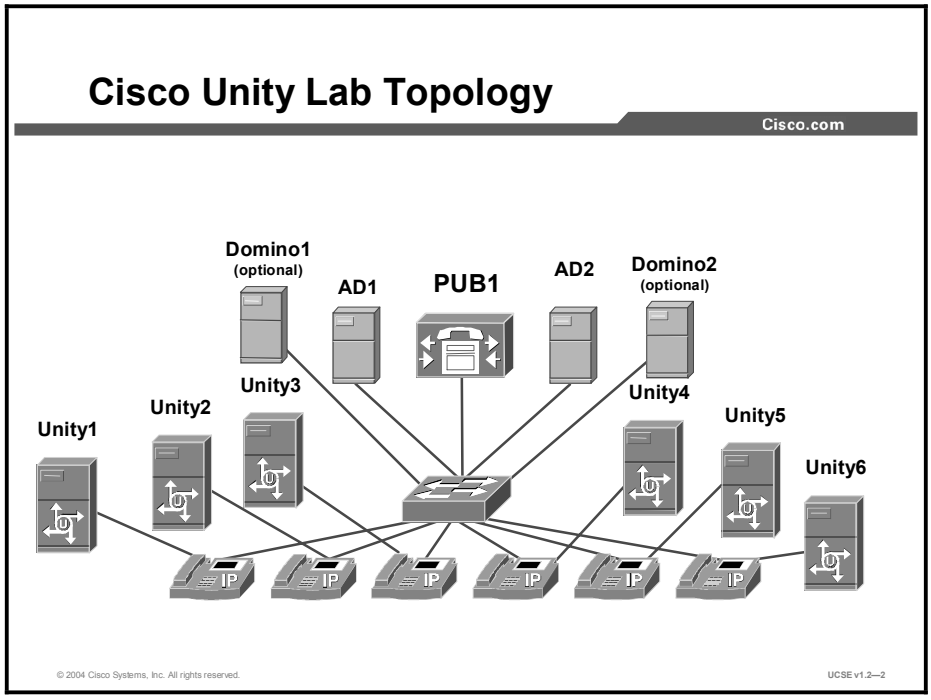
Activity Objective

In this activity, you will install the Cisco Unity software. After completing this activity, you will be able to meet these objectives:

- Use the Cisco Unity Installation and Configuration Assistant
- Use the Permissions Wizard
- Use the License Wizard
- Use the Cisco Unity Setup
- Use the Services Configuration Wizard
- Use the Message Store Wizard
- Use the Password Hardening Wizard
- Use the Cisco Unity Telephone Integration Monitor
- Set up Cisco Personal Communications Assistant to use SSL

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment required to complete this activity:

- Cisco Unity server

Task 1: Using the Permissions Wizard

During this task, you will be setting permissions for the Cisco Unity installation. This assumes that the system has already been preloaded with Exchange and AD, the AD schema has been updated, and the CUSPA utility has been completed.

Activity Procedure

Complete these steps:

Step 1 On your Cisco Unity server, access the D:**Unity** drive.

Step 2 Select the **CD1** folder.

Step 3 Double-click on the **SETUP.EXE** icon

Step 4 The Cisco Unity Configuration and Installation Assistant will launch. After reading the instructions, click **Continue**.

Step 5 On the Pre-Installation Requirements page, read the steps. On Step 4, click the link **Run the Permissions Wizard**.

Step 6 On the Welcome screen, choose **Microsoft Exchange 2000** and click **Next**.

Step 7 On the Choose Windows Account to Install Cisco Unity, confirm or type: *your Domain\your Server#* (for example: **classroom1\server1**), and click **Next**.

Step 8 On the Account to own Cisco Unity Directory Services screen, click **Change** and find your service account (for example: Server1=Server1），and click **OK**. Click **Next**.

Step 9 On the Account to own Cisco Unity Message Store Services screen, click **Change** and find the UnityAdmin Server#, (for example: Server1=UnityAdmin1). Click **OK**. Click **Next**.

Step 10 On the Select Active Directory Container for New Objects screen, under Users, click **Modify** and select the Org number that corresponds with your Server number (for example: Server1=Org1).

Step 11 Repeat the same steps for Groups. Click **Next**.

Step 12 On the Select Which Objects Cisco Unity Administrator Can Create screen, confirm that all the boxes are checked and click **Next**.

Step 13 On the Active Directory Container for Location Objects screen, click **Modify** and choose the Org that corresponds with your Server number. Click **Yes** to replace and then click **Next**.

Step 14 On the Active Directory Containers for Import screen, click **Add**, expand the domain and choose your Org. Click **OK.** Click **Yes** to replace and then click **Next**.

Step 15 On Choose Mailstores, click the **Choose Mailstores** box. Click on **First Administrative Group** box. This deselects (unchecks) all boxes. Now check the box to the left of your server name. Three checks should appear. Click **OK** and then **NEXT**.

Step 16 On the Verify Permissions screen, read it to make sure the correct selections were made, and click **Next**. The system will take a few minutes while it sets the permissions.

Step 17 After the permissions are granted, click **Finish**. You should be taken to a Read Me file that contains information on setting the necessary Exchange 5.5, Exchange 2000, or Domino permissions for the Cisco Unity installation. These permissions have already been set by your instructor, so close the screen.

Activity Verification

You have completed this activity when you attain this result:

- You are at the Install Unity screen.

Task 2: Using Cisco Unity Setup

During this task, you will be running the Cisco Unity Setup Wizard.

Activity Procedure

Complete these steps:

Step 1 On the Install Cisco Unity screen, under Step 2, click the **Run the Cisco Unity Setup Program** link.

Step 2 A language selection box will appear. Double-click the **Double-click to continue in English** option**.**

Step 3 On the Welcome screen, click **Next.**

Step 4 The setup program takes a few minutes while it examines your server. You will be prompted to disable all virus scanning services. There are none in our environment, so click **OK**.

Step 5 On the User Information screen, accept the defaults and click **Next**.

Step 6 On the Enter Installation Locations screen, accept the defaults and click **Next**.

Step 7 On the Select Features page, make sure **Install Unity** and **Enable TTS** are checked. Do not check the option to install voice hardware cards. Click **Next**.

Step 8 On the Choose the System Prompt Set page, select **G.711**. Click **Next**.

Step 9 On the Unity Languages page, select the **English (United States)** box. Click **Next**.

Step 10 On the Select Default Languages page, keep the English (United States) defaults and click **Next**.

Step 11 On the Select Keypad Map page, keep the default. Click **Next,** and again click **Next**.

Step 12 The program now has enough information to continue the install, so click **Next**.

Step 13 If installing from the DVD, there may be a pause before the system responds. If you are installing from CDs, the system will prompt for CD2. When prompted for CD2, click **Browse.** In the window that appears, expand **My Computer,** select **D:Unity, CD2.** Click **OK**, and then **OK** again. The system will load files and then ask you for CD1 again. Perform these same steps to access CD1.

Step 14 The system now installs the system default configuration. This could take up to 40 minutes. When you receive the Setup Complete message page, click **Finish** to reboot the server.

Activity Verification

You have completed this activity when you attain this result:

- You are at the Install the License File Wizard.

Task 3: Install the Cisco Unity License File

During this task, you will install the license file for Cisco Unity.

Activity Procedure

Complete these steps:

Step 1 On the Install Cisco Unity License File page, select the link in Step 2 **Run the Cisco Unity License File Wizard**.

Step 2 On the Welcome screen, click **Next**.

Step 3 On the License Files page, click **Add**.

Step 4 On the Add page, select **CiscoUnity4.0.lic** and click **Open**.

Step 5 The file will appear in the License Files page. Click **Next**.

Step 6 The Licenses page shows you the licenses allowed on your system. Review them and click **Next**.

Step 7 On the Completing the Install License File Wizard page, click **Finish**.

Activity Verification

You have completed this activity when you attain this result:

- You are at the Configure Cisco Unity Services screen.

Task 4: Configure the Cisco Unity Services

During this task you will configure the services for Cisco Unity.

Activity Procedure

Complete these steps:

Step 1 On the Configure the Cisco Unity Services screen, select the link in Step 2: **Run the Cisco Unity Services Configuration Wizard**.

Step 2 On the Welcome to the Cisco Unity Configuration Wizard screen, click **Next**.

Step 3 On the Message store type, select **Microsoft Exchange 2000**, then click **Next**.

Step 4 On the Select Directory Services Account page, confirm that the Server# account is in the Account field.

Step 5 In the Password field, type **password**. Click **Next**.

Step 6 On the Select Message Store Account page, confirm that the Unity Admin Server# account is in the Account field.

Step 7 In the Password field, type **password**. Click **Next.**

Step 8 On the Select Local Services Account page**,** click **Account**, and click **Browse,** and find your server account (for example: Server1@classsroom1.com), and click **OK**.

Step 9 The password field is filled in for you. Click **Next**.

Step 10 Click **Next** to confirm changes, and the wizard configures the services. Click **Next** to continue and then click **Finish** to complete the wizard**.**

Activity Verification

You have completed this activity when you attain this result:

- You are at the Configure Cisco Unity Message Store screen.

Task 5: Configure the Cisco Unity Message Store

During this task, you will configure the message store for Cisco Unity.

Activity Procedure

Complete these steps:

Step 1 On the Configure the Cisco Unity Message Store screen, select the link in Step 3 **Run the Cisco Unity Message Store Configuration Wizard**.

Step 2 On the Welcome screen, click **Next.**

Step 3 On the Select Installation account, check that the User name is your server# account, and under **password**, type **password**. Click **Next**.

Step 4 The Select Unity Administration account will be the one you selected earlier, so click **Next**.

Step 5 On Select Partner Message Store, select **Microsoft Exchange 2000** and click **Next**.

Step 6 On Select Mailbox Location, select **your server#** under Exchange Server. Click **Next**.

Step 7 On the Select Active Directory container for new objects, confirm that users, distribution lists, and locations are set for your Org. Click **Next**.

Step 8 Click **OK** to stop Cisco Unity services.

Step 9 Decide how subscribers will be created. Select **Create new accounts** and **import existing accounts**. Click **Next**.

Step 10 The Directory Services account will be the same account you selected earlier. Click **Next**, and then click **Finish** to complete the wizard.

Activity Verification

You have completed this activity when you attain this result:

- You are at the Password Hardening Wizard.

Task 6: Password Hardening

During this task, you will set default passwords on the Administrator and Subscriber templates for both Windows 2000 authentication (if Cisco Unity creates the Active Directory account) and Cisco Unity access using the telephone (TUI).

Activity Procedure

Complete these steps:

Step 1 On the Set New Default Password screen, select the link on Step 2: **Run the Password Hardening Wizard.**

Step 2 On the Welcome Screen, click **Next.**

Step 3 On the Password for the Default Administrator Template screen, type **Administrator!**. (Be careful: the "A" should be upper-case while all other letters should be lower-case. These passwords are case-sensitive.) Click **Next**.

Step 4 On the Telephone Password for the Default Administrator Template screen, enter **206256** as the password. Click **Next**.

Step 5 On the Password for the Default Subscriber Template screen, type **Subscriber!** (Again, be careful about the lower and upper cases). Click **Next**.

Step 6 On the Telephone Password for the Default Subscriber template, enter **206256**. Click **Next.**

Step 7 Click **Next** to confirm the changes and then **Finish.**

Activity Verification

You have completed this activity when you attain this result:

- You are at the Cisco Unity Telephone Integration Manager.

Task 7: Integrate the Phone System with Cisco Unity

During this task, you will use the Cisco Unity Telephone Integration Manager to configure a Cisco Unity/Cisco CallManager integration.

Activity Procedure

Complete these steps:

Step 1 On the Integrate the Phone System with Cisco Unity page, select the link in Step 1: **Run the Cisco Unity Telephone Integration Manager**.

Step 2 On the Manage Integrations page, select **Create Integration**.

Step 3 On the Welcome to the Telephony Integration Setup Wizard, select **Cisco CallManager** and click **Next**.

Step 4 Accept the defaults on the name of Cisco CallManager and the Cluster. Click **Next**.

Step 5 Enter the IP address designated by your instructor, and accept the default TCP port of 2000. Click **Next**.

Step 6 Click **Next** to bypass the secondary server for failover setup.

Step 7 Under the MWI extensions, enter `7001` for MWI on extension and `7002` for MWI off extension. Click **Next**.

Step 8 Change the number of voice-mail ports to **2**. Change the default CallManager Device Name Prefix to `Cisco UM(your Server#)-VI` (for example: Server1=CiscoUM1-VI). Click **Next**.

Step 9 Click **Next** to bypass the Enter Trunk Access Code setup, and then click **Finish** to complete the Integration Wizard.

Step 10 Select **OK** after Cisco Unity tells you the services have restarted. If the services cannot be restarted, the system will produce an error stating that the services cannot be started and you will have to reboot the computer. Follow the on-screen instructions.

Step 11 Close the Manage Integration screen. Click **Close** to close and complete the Cisco Unity Installation and Configuration Assistant.

Activity Verification

You have completed this activity when you attain this result:

- You are at the Set Up the Cisco Personal Communications Assistant to Use SSL screen.

Task 8: Set up the Cisco Personal Communications Assistant to use SSL

During this task, you will set up the CPCA to use SSL.

Activity Procedure

Complete these steps:

Step 1 In the options, select the **Do Not Set Up Cisco PCA to use SSL**, or **Set Up SSL Manually** radio button.

Step 2 Read the caution note. Click **Continue**.

Step 3 Click **Close**.

Activity Verification

You have completed this activity when you attain this result:

- You are able to dial into your Cisco Unity server and hear the Opening Greeting.

Lab 2-2: Installing Cisco Unified Communications Software (Domino)

Complete this lab activity to practice what you learned in the related module.

Activity Objective

In this activity, you will install the Cisco Unity software. After completing this activity, you will be able to meet these objectives:

- Use the Cisco Unity Installation and Configuration Assistant
- Use the Permissions Wizard
- Use the License Wizard
- Use the Cisco Unity Setup
- Use the Services Configuration Wizard
- Use the Message Store Wizard
- Use the Unity Telephone Integration Monitor

Required Resources

These are the resources and equipment required to complete this activity:

- Cisco Unity server

Task 1: Using the Permissions Wizard

During this task, you will be setting permissions for the Cisco Unity installation.

Activity Procedure

Complete these steps:

Step 1 On your Cisco Unity server, access the D: drive and select the **Unity 4.0** folder.

Step 2 Select the **CD1** folder.

Step 3 Double-click the **SETUP.EXE** icon.

Step 4 The Cisco Unity Configuration and Installation Assistant will launch. After reading the instructions, click **Continue**.

Step 5 On the Pre-Installation Requirements page, read the steps. On Step 4, click the link **Run the Permissions Wizard**.

Step 6 On the Welcome screen, choose **Lotus Domino** and click **Next**.

Step 7 On Choose Windows Account to Install Cisco Unity, your installation account is filled in. Confirm that it is your classroom domain\Server# (for example: `classroom1\server1`), and click **Next**.

Step 8 On the Account to Own Cisco Unity Services screen, click **Change**, find your service account (for example: Server1=User Server1), and click **OK**. Click **Next**.

Step 9 On the Verify Permissions screen, read it to make sure the correct selections were made and click **Next**. The system will take a few minutes to set the permissions.

Step 10 After the permissions are granted, click **Finish**. You should be taken to a Read Me file that contains information on setting the necessary Exchange 5.5, Exchange 2000, or Domino permissions for the Cisco Unity installation. These permissions have already been set by your instructor, so close the screen.

Activity Verification

You have completed this activity when you attain this result:

- You are at the Install Unity screen.

Task 2: Using Cisco Unity Setup

During this task, you will be running the Cisco Unity Setup wizard.

Activity Procedure

Complete these steps:

Step 1 On the Install Cisco Unity screen under Step 3, click the link: **Run the Cisco Unity Setup Program**.

Step 2 A language selection box will appear. Double-click the **Double-click to continue in English** option**.**

Step 3 On the Welcome screen, click **Next.**

Step 4 The setup program takes a few minutes while it examines your server.

Step 5 On the User Information screen, accept the defaults and click **Next**.

Step 6 On the Enter Installation Locations screen, accept the defaults and click **Next**.

Step 7 On the Select Features page, make sure Install Unity and Enable TTS are checked. Uncheck the **Install Voice Card software** box. Click **Next**.

Step 8 On the Choose the System Prompt Set page, select **G.711**. Click **Next**.

Step 9 On the Unity Languages page, select the **English (United States)** box. Click **Next**.

Step 10 On the Select Default Languages page, keep the English (United States) defaults and click **Next**.

Step 11 On the Select Keypad Map page, keep the default. Click **Next,** and again click **Next**.

Step 12 The program now has enough information to continue the install, so click **Next**.

Step 13 The system now installs the system default configuration. This could take up to 20 minutes. When you receive the Setup Complete message page, click **Finish** to reboot the server.

Activity Verification

You have completed this activity when you attain this result:

- You are at the Install the License File Wizard screen.

Task 3: Install the Cisco Unity License File

During this task, you will install the license file for Cisco Unity.

Activity Procedure

Complete these steps:

Step 1 On the Install Cisco Unity License File page, select the link in Step 2: **Run the Cisco Unity License File Wizard**.

Step 2 On the Welcome screen, click **Next**.

Step 3 On the License Files page, click **Add**.

Step 4 On the Add page, select **CiscoUnity4.0.lic** and click **Open**.

Step 5 The file will appear in the License Files page. Click **Next**.

Step 6 The Licenses page shows you the licenses allowed on your system. Review them and click **Next**.

Step 7 On the Completing the Install License File Wizard page, click **Finish**.

Activity Verification

You have completed this activity when you attain this result:

- You are at the Configure Cisco Unity Services screen.

Task 4: Configure the Cisco Unity Services

During this task, you will configure the services for Cisco Unity.

Activity Procedure

Complete these steps:

Step 1 On the Configure the Cisco Unity Services screen, select the link in Step 2: **Run the Cisco Unity Services Configuration Wizard**.

Step 2 On the Welcome to the Cisco Unity Configuration Wizard screen, click **Next**.

Step 3 On the message store type, select **Lotus Domino R5**, and then click **Next**.

Step 4 On the Select Directory Services and Message Store Account page, confirm that the Server# account is in the Account field.

Step 5 In the Password field, type **password**. Click **Next**.

Step 6 On the Select Local Services Account page**,** click **Account**, and click **Browse,** and find your server account (for example: Server1@classsroom1.com), and click **OK**.

Step 7 The password field is filled in for you. Click **Next**.

Step 8 Click **Next** to confirm changes, and the wizard loads the changes. Click **Next** to continue and then click **Finish** to complete the wizard**.**

Activity Verification

You have completed this activity when you attain this result:

- You are at the Configure Cisco Unity Message Store screen.

Task 5: Configure the Cisco Unity Message Store

During this task, you will configure the message store for Cisco Unity.

Activity Procedure

Complete these steps:

Step 1 On the Configure the Cisco Unity Message Store screen, select the link in Step 3: **Run the Cisco Unity Message Store Configuration Wizard**.

Step 2 On the Welcome screen, click **Next.**

Step 3 On Select Installation Account, check that the User name is your server# account and under Password, type: **password**. Click **Next**.

Step 4 The Select Unity System Administration account will be the one you selected earlier, so click **Next**.

Step 5 On Select Message Store, select **Lotus Domino R5** and click **Next**.

Step 6 On Select Directory Services Account, confirm that the User name is your server account. Click **Next**.

Step 7 On Confirm Domino User ID password, type: **password**. Click **Next** (If you receive an error of "wrong password", leave the password field blank).

Step 8 On Collect Address Book Information, enter the following information: Server type: `Domino1` or `Domino2` depending on which domain you are in; Address Book: `Names.nsf`; Display Name: `Domino User List`. Click the `>>` button to add the information and then click **Next**.

Step 9 Click **OK** to stop the Cisco Unity services.

Step 10 Click **Finish** to complete the wizard.

Activity Verification

You have completed this activity when you attain this result:

- You are at the Integrate the Phone System with Cisco Unity screen.

Task 6: Integrate the Phone System with Cisco Unity

During this task, you will use the Cisco Unity Telephone Integration Manager to configure a Cisco Unity/Cisco CallManager integration.

Activity Procedure

Complete these steps:

Step 1 On the Integrate the Phone System with Cisco Unity page, select the link in Step 1: **Run the Cisco Unity Telephone Integration Manager**.

Step 2 On the Manage Integrations page, select **Create Integration**.

Step 3 On the Welcome to the Telephony Integration Setup Wizard, select **Cisco CallManager** and click **Next**.

Step 4 Accept the defaults on the name of Cisco CallManager and the Cluster. Click **Next**.

Step 5 Enter the IP address designated by your instructor, and accept the default TCP port of 2000. Click **Next**.

Step 6 Click **Next** to bypass the Secondary server for failover setup.

Step 7 Under the MWI extensions, enter `7001` for MWI on extension and `7002` for MWI off extension. Click **Next**.

Step 8 Change the number of VoiceMail ports to **2**. Change the default CallManager Device Name Prefix to `Cisco UM(your Server#)-VI` (for example: Server1=CiscoUM1-VI). Click **Next**.

Note The character after the "V" is the letter "I", not the numeral "1".

Step 9 Click **Next** to bypass the Enter Trunk Access Code setup, and then click **Finish** to complete the Integration Wizard.

Step 10 Select **OK** after Cisco Unity tells you the services have restarted.

Step 11 Close the Manage Integration Screen. Click **Close** to close and complete the Cisco Unity Installation and Configuration Assistant.

Activity Verification

You have completed this activity when you attain this result:

- You are able to dial your Cisco Unity system and listen to the opening greeting.

Task 7: Installing DUC

During this task, you will install DUC, which gives you ViewMail for Notes capability.

Activity Procedure

Complete these steps:

Step 1 On the desktop, navigate to My Computer > Unity (D:) > DUC 1.11 > csClient. Double-click **Setup**.

Step 2 Click **Accept** to accept the License Agreement.

Step 3 Click **Next** on the Welcome page. Accept the default location by clicking **Next**.

Step 4 Check the Update mail file box. Confirm that **Office** (Network) is highlighted and click **Next**.

Step 5 If the install asks for a password, type: **password** and click **OK**.

Step 6 Click **Next** to copy files.

Step 7 Uncheck the Readme file box and then click **Finish**.

Step 8 When asked to install the 729a driver, click **OK**. You may be told that the file already exists, and asked if you want to overwrite. If so, click **No**. Click **Yes** to restart the computer.

Step 9 After the computer restarts, log in and click **Start > Search > For files and folders**, and search for the Notes.ini file on C: drive.

Step 10 Open the file and find the following line: EXTMgR_Addins=ucclient

Step 11 Edit the line by adding a comma then: **CsNotesPwdSvr**. So the end result should be EXTMgr=ucclient,CsNotesPwdSvr.

Step 12 Click **File**, and then **Save**. Close the file and restart the server.

Activity Verification

You have completed this activity when you attain this result:

- You are able to open Lotus Notes and see the option for Voice Message.

Lab 3-1: Digital Networking in Cisco Unity

Complete this lab activity to practice what you learned in the related module.

Activity Objective

In this activity, you will configure digital networking for Cisco Unity. After completing this activity, you will be able to meet these objectives:

- Configure the default location object correctly
- Implement digital networking
- Configure dialing domains
- Configure search scopes

Required Resources

These are the resources and equipment required to complete this activity:

- Cisco Unity server

Task 1: Add an Active Directory Account and then Import the Account into Cisco Unity

During this task, you will be adding an Active Directory account and importing the account as a Cisco Unity subscriber.

Activity Procedure

Complete these steps:

Step 1 Click **Start > Programs > Microsoft Exchange > Active Directory Users and Computers**.

Step 2 In the left side panel, expand the domain and right-click your Org. Click **New**, and click **User**.

Step 3 Create a user by filling in the name. For User Logon, enter *first name*, *initial*, and *last name*. Click **Next .**

Step 4 You can create a password or leave the password blank. Confirm that the rest of the fields are unchecked. Click **Next**.

Step 5 Confirm that Create an Exchange Mailbox is checked. Under Server, select your server #. Click **Next** and then click **Finish**.

Step 6 On the right side panel, find your new user and double click. Click **Member of**, click **Add**, select **Domain Admins**, and click **Add**. Click **OK**, click **OK**. Close the Active Directory Users and Computer window.

Step 7 Double-click the Unity System Administration shortcut on the desktop.

Step 8 Click **Subscribers**, and click the **Add** icon.

Step 9 Select **Import Existing Exchange User**, and click **Select**. Confirm that the option selected under Exchange is the Mail system type, and click **Find**.

Step 10 Scroll until you find the new user you created in Active Directory and click the **first name** link.

Step 11 Choose the **Default Administrator** subscriber template.

Step 12 Enter your telephone extension as the Extension and click **Add**.

Step 13 On the Profile page record the user's name. Uncheck **Set subscriber for self-enrollment at next login**.

Step 14 On the Phone Password page, uncheck **User Must Change Password at Next Logon**.

Step 15 Click **Greetings,** and under Source, select **Recording**, and record a personal greeting for the user.

Step 16 Click **Call Transfer**, select **Yes**, ring subscriber's extension. Click the **Save** icon.

Activity Verification

You have completed this activity when you attain this result:

- You are able to call in to Cisco Unity from your telephone extension and are prompted to enter your password (12345).

Task 2: Configuring the Primary Location Object and Dialing Domains

In this task, you configure the Primary Location object for your Cisco Unity server and set a dialing domain.

Activity Procedure

Complete these steps:

Step 1 From the System Admin screen, click **Primary Location**.

Step 2 Under Display Name, type: *your Server#* (for example: **Server1**). Under Dial ID, type: 90Server# (for example:**Server1=901**). Record your display name.

Step 3 For Dialing Domain, select the lower radio button and type in your domain name in lower case (dialing domain entries are case sensitive). Under SMTP, also type in your domain name.

Step 4 On the Navigation bar, click **Addressing Options,** and set both the Subscriber Searches and Blind Addressing fields to **Global Directory**. Check **Include location in searches** box**.** Click the **Save** icon.

Step 5 Move to the main navigation bar using the **Back** (blue triangle) button.

Step 6 After a few minutes, click **Delivery Location**. Click the **Find** icon. You should see all the other servers within your domain listed. You need to wait until the other pods in the domain have completed this step for their systems to appear.

Activity Verification

You have completed this activity when you attain this result:

- When you can see the other servers within your domain listed under Delivery Locations.

Task 3: Messaging Within an Organization Using the TUI

In this task, you will leave a message for a subscriber on another Cisco Unity server within your organization using the telephone.

Activity Procedure

Step 1 From the primary extension on your telephone, dial into Cisco Unity and access your mailbox. After entering your password, press **2** to send a message.

Step 2 Spell out the name of a subscriber on another Cisco Unity server within your organization and leave that person a message.

Step 3 Confirm that the person has received the message.

Activity Verification

You have completed this activity when you attain this result:

- The subscriber you left the telephone message for confirms they received it.

Task 4: Installing VMO and Creating an Outlook Profile

In this task, you will load the ViewMail for Outlook client and configure an Outlook profile for a subscriber.

Activity Procedure

Step 1 While logged on as the server account on your Cisco Unity server, click **My Computer**, and select the **D:** Drive. On the D: drive, click the **ViewMail** folder, and then click the **Setup** icon**.**

Step 2 On the ViewMail Installation Wizard screen, click **Next.** Choose the language you wish to hear the VMO prompts in and click **OK.**

Step 3 At the Welcome to ViewMail for Outlook screen, click **Next**. On the Select Directory screen, click **Next**. (If asked, click **OK** to build the directory). The install program loads the software. When completed, click **Finish.**

Step 4 Log off your server using the server account. Log back on using the subscriber account you created earlier.

Step 5 On the desktop, double-click the **Microsoft Outlook** icon. If the Install Outlook Millenium Edition begins to run, click **Cancel**. In the lower right of the screen, a User box will appear. Click **OK**.

Step 6 The Microsoft Outlook Wizard begins. Check **Microsoft Exchange Server**. Leave the Internet Email box unchecked. Click **Next**.

Step 7 In the Microsoft Exchange Server field, type: *your Server#* (for example: **Server1**). In the logon box, confirm that your logon name is entered. If not, type it in. Click **Next.**

Step 8 Confirm that **No** is selected in answer to the question, "Do you travel with this computer?" Click **Next.** Click **Finish.**

Step 9 Click **No** when asked if you would like Outlook to be your default manager.

Activity Verification

You have completed this activity when you attain this result:

- You double-click the Outlook icon on the desktop and your Outlook Inbox appears.

Task 5: Messaging Within your Organization Using VMO

In this task you will leave a message for a subscriber on another Cisco Unity server within your organization using the VMO.

Activity Procedure

Step 1 On the Outlook toolbar, click the **New Voice Message** icon located on the far right of the tool bar.

Step 2 The ViewMail for Outlook form opens. Click **To** and select a subscriber on another Cisco Unity server**.** Highlight the subscriber's name and double click. The name appears in the Message Recipients field. Click **OK**.

Step 3 On the Media Master bar. click the **down options** arrow, and select your playback and record device. Click the red button on the bar to record your message. In your message, ask the recipient to send a response.

Step 4 Click **Send**.

Step 5 To listen to the response, double-click on the message in the Outlook Inbox and click the **Play** button on the Media bar.

Activity Verification

You have completed this activity when you attain this result:

- You receive a response from the voice-mail message you sent using VMO.

Lab 5-1: Troubleshooting Delayed Message Notification Problems

Complete this lab activity to practice what you learned in the related module.

Activity Objective

In this activity, you will select and describe the best diagnostic tool to use to identify and correct a common delayed message notification problem. After completing this activity, you will be able to:

- Use the appropriate tools to troubleshoot why a message notification is being delayed

Required Resources

These are the resources and equipment required to complete this activity:

- A preconfigured Cisco Unity system with Instructor Hack
- Access to the Cisco Unity Server through Terminal Services or VNC
- The password and telephone information at each work station
- The steps in this activity

Command List

The table describes the commands used in this activity.

Table 1: Cisco Unity Access Commands

Command	Description
`http://ip_addr_of_Unity/SAWeb`	URL to access the Cisco Unity server
`C:\CommServer\Utilities\ToolsDepot\ToolsDepot.exe`	Path to access the Tools Depot
`http://unity404/WebSM/Default.htm`	URL to access Cisco Status Monitor

Task 1: Troubleshooting Message Notification

In this task, you will use proven problem isolation techniques to list the symptoms of problems with message notification and apply diagnostic tools to solve the following problem:

You have configured Message Notification on your Cisco Unity account, but you do not seem to be getting any notification when a new message is received. You have tested the notification process by leaving yourself a message to see if you would receive notification, but you did not receive notification.

Activity Procedure

Complete these steps:

Step 1 List the possible causes of the malfunction.

Step 2 List which tools you would use to evaluate each possible cause.

Step 3 Apply the diagnostic tools to locate the cause of the malfunction.

Step 4 When the source of the problem is identified, explain what was happening and what the solution is.

Step 5 Resolve the problem.

Activity Verification

You have completed this activity when you attain this result:

- You leave yourself a message and are notified that you have received a new message.

Lab 5-2: Troubleshooting Message Waiting Indicator Problems

Complete this lab activity to practice what you learned in the related module.

Activity Objective

In this activity, you will select and describe the best diagnostic tool to use to identify and correct a common Message Waiting Indicator problem. After completing this activity, you will be able to:

- Use the appropriate tools to troubleshoot why a message notification is being delayed.

Required Resources

These are the resources and equipment required to complete this activity:

- A preconfigured Cisco Unity system with Instructor Hack
- Access to the Cisco Unity server through Terminal Services or VNC
- The password and telephone information at each work station
- The steps in this activity

Command List

The table describes the commands used in this activity.

Table 1: Cisco Unity Access Commands

Command	Description
`http://ip_addr_of_Unity/SAWeb`	URL to access the Cisco Unity server
`C:\CommServer\Utilities\ToolsDepot\ToolsDepot.exe`	Path to access the Tools Depot
`http://unity404/Web/SM/Default.htm`	URL to access Cisco Status Monitor

Task 1: Troubleshooting Message Waiting Indicator Lamps

In this task, you will use proven problem isolation techniques to list the symptoms of problems with Message Waiting Indicator lamps and apply diagnostic tools to solve the following problem:

You are receiving new messages but the MWI light on the phone does not light up to indicate that there are new messages.

Activity Procedure

Complete these steps:

Step 1 List the possible causes of the malfunction.

Step 2 List which tools you would use to evaluate each possible cause.

Step 3 Apply the diagnostic tools to locate the cause of the malfunction.

Step 4 When the source of the problem is identified, explain what was happening and what the solution is.

Step 5 Resolve the problem.

Activity Verification

You have completed this activity when you attain this result:

- You leave yourself a message and the MWI light on the phone lights up to indicate you have received a new message.

Lab 5-3: Troubleshooting Delayed Message Problems

Complete this lab activity to practice what you learned in the related module.

Activity Objective

In this activity, you will select and describe the best diagnostic tool to use to identify and correct a common delayed message problem. After completing this activity, you will be able to:

- Use the appropriate tools to troubleshoot why a message is delayed in delivery.

Required Resources

These are the resources and equipment required to complete this activity:

- A preconfigured Cisco Unity system with Instructor Hack
- Access to the Unity Server through Terminal Services or VNC
- The password and telephone information at each work station
- The steps in this activity

Command List

The commands used in this activity are described in the table here.

Table 1: Cisco Unity Access Commands

Command	Description
`http://ip_addr_of_Unity/SAWeb`	URL to access the Cisco Unity server
`C:\CommServer\Utilities\ToolsDepot\ToolsDepot.exe`	Path to access the Tools Depot
`http://unity404/Web/SM/Default.htm`	URL to access Cisco Status Monitor

Task 1: Troubleshooting Delayed or Missing Messages

In this task, you will use proven problem isolation techniques to list the symptoms of problems with delayed or missing messages and apply diagnostic tools to solve the following problem:

You receive a call from your supervisor asking why you are not in the meeting. He tells you that he left you a message two hours ago stating the new time and place and asks that you hurry there now. While you are away in your meeting, your broker calls and leaves a message suggesting you sell certain stocks. Later he calls again and asks why you did not respond to his query. You realize you are not getting your messages.

Activity Procedure

Complete these steps:

Step 1 List the possible causes of the malfunction.

Step 2 List which tools you would use to evaluate each possible cause.

Step 3 Apply the diagnostic tools to locate the cause of the malfunction.

Step 4 When the source of the problem is identified, explain what was happening and what the solution is.

Step 5 Resolve the problem.

Activity Verification

You have completed this activity when you attain these results:

- You leave yourself a message and you receive it in your voice-mail box.
- You have someone from outside your Cisco Unity system leave you a message and you receive it.

Lab 5-4: Troubleshooting CPCA Problems

Complete this lab activity to practice what you learned in the related lesson.

Activity Objective

In this activity, you will select and describe the best diagnostic tool to use to identify and correct a common CPCA problem. After completing this activity, you will be able to:

- Use the appropriate tools to troubleshoot problems with CPCA.

Required Resources

These are the resources and equipment required to complete this activity:

- A preconfigured Cisco Unity system with Instructor Hack
- Access to the Unity Server through Terminal Services or VNC
- The password and telephone information at each work station
- The steps in this activity

Command List

The commands used in this activity are described in the table here.

Table 1: Cisco Unity Access Commands

Command	Description
`http://ip_addr_of_Unity/SAWeb`	URL to access the Cisco Unity server
`C:\CommServer\Utilities\ToolsDepot\ToolsDepot.exe`	Path to access the Tools Depot
`http://unity404/Web/SM/Default.htm`	URL to access Cisco Status Monitor

Task 1: Troubleshooting CPCA Problems

In this task, you will use proven problem isolation techniques to list the symptoms of problems with CPCA and apply diagnostic tools to solve the following problem:

You are out of the office and want to change your greeting through CPCA to let people know that you will not be in today. You have performed this often in the past, but for some reason you cannot bring up the CPCA site to make the changes.

Activity Procedure

Complete these steps:

Step 1 List the possible causes of the malfunction.

Step 2 List which tools you would use to evaluate each possible cause.

Step 3 Apply the diagnostic tools to locate the cause of the malfunction.

Step 4 When the source of the problem is identified, explain what was happening and what the solution is.

Step 5 Resolve the problem.

Activity Verification

You have completed this activity when you attain this result:

- You are able to bring up the CPCA and change your greeting.

