



## **Cisco Unity Failover Configuration and Administration Guide (With IBM Lotus Domino)**

Release 4.0(5) and Later  
Revised October 12, 2007

### **Corporate Headquarters**

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

Text Part Number: OL-7321-02



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

*Cisco Unity 4.0(5) and Later Failover Configuration and Administration Guide (With IBM Lotus Domino)*  
© 2007 Cisco Systems, Inc. All rights reserved.



## **Preface**   vii

Audience and Use	vii
Documentation Conventions	viii
Cisco Unity Documentation	viii
Obtaining Documentation	viii
Cisco.com	ix
Documentation DVD	ix
Ordering Documentation	ix
Documentation Feedback	ix
Cisco Product Security Overview	x
Reporting Security Problems in Cisco Products	x
Obtaining Technical Assistance	xi
Cisco Technical Support Website	xi
Submitting a Service Request	xi
Definitions of Service Request Severity	xii
Obtaining Additional Publications and Information	xii

---

## **CHAPTER 1**

### **Configuring Cisco Unity Failover**   1-1

Configuring Failover on the Primary and Secondary Servers	1-2
Configuring the Voice Messaging Ports on the Secondary Server	1-3
Creating a Routing Rule That Enables Subscriber Logon by Phone After Failover	1-4
Setting Up Automatic Daily Resynchronization of MWIs	1-5
Setting Up Notification of When Failover Occurs	1-5
Setting Up Scheduled Backups of Cisco Unity	1-9
Testing Cisco Unity Failover	1-9
Customizing Failover and Failback Settings for the Cisco Unity System (Optional)	1-12
Disabling Failover Initiation When Calls Are Unanswered on the Primary Server (Optional)	1-14

---

## **CHAPTER 2**

### **Tasks Required When Failover or Failback Occurs**   2-1

Notifying Subscribers of the Active Server and the URLs to Use for Accessing Cisco Unity Web Applications	2-1
Notifying Subscribers to Update the Server Name in the Media Master	2-1
Changing Media Master Settings for Recording and Playback After Failover or Failback	2-2

T1 Integration: Enabling the Phone System to Send Calls to the Active Server After Failover or Failback Occurs 2-2

**CHAPTER 3**

**Monitoring and Maintaining Cisco Unity Failover 3-1**

- Starting the Servers in the Correct Order 3-1
- Determining Which Server Is Active 3-1
- Manually Initiating Failover or Failback 3-2
- Disabling Automatic Failover and Failback for Troubleshooting 3-3
- Confirming That Failover and Failback Function Correctly 3-5
- Determining the Cause of Failover or Failback from an Event ID 3-7
- Changing the IP Address of the Primary Server 3-8
- Changing the IP Address of the Secondary Server 3-13
- About Uninstalling Failover on a Cisco Unity Server 3-18
- Replacing and Converting the Primary and Secondary Servers 3-18

**CHAPTER 4**

**About Cisco Unity Failover 4-1**

- How Failover Works in Cisco Unity 4-1
- Requirements for Cisco Unity Failover 4-4
- Effects of Using or Not Using the Force Failover Setting 4-5
- Effects of Failover and Failback on Calls in Progress 4-6
- Status Monitoring and File Replication 4-6
  - Data That Is Not Replicated 4-8
- Events When Failover Occurs 4-9
- Events When Failback Occurs 4-9
- Automatic and Manual Failback 4-10
- Causes of Failover and Failback 4-10
  - Failover Causes 4-10
  - Failback Causes 4-11
- Intervals for Failover and Failback 4-12
  - Failover Interval 4-12
  - Failback Interval 4-12
- Causes of Both Servers Becoming Active at the Same Time 4-14
- Effects of Shutting Down and Restarting the Primary and Secondary Servers 4-15
- Licensing Restrictions on Using a Secondary Server Without a Primary Server 4-15

**APPENDIX A**

**Exiting and Starting the Cisco Unity Software and Server A-1**

- Exiting the Cisco Unity Software A-1

Shutting Down or Restarting the Cisco Unity Server **A-2**

Starting the Cisco Unity Software **A-3**

---

**APPENDIX B**
**Line Connections Between the Phone System and the Cisco Unity Servers **B-1****

Analog Voice Line Connections for Failover **B-1**

Requirements **B-1**

Connections with D/41-Series Voice Cards **B-2**

Connections with D/120-Series Voice Cards **B-4**

Serial Data Cable Connections for Failover **B-6**

Requirements **B-6**

Pinouts for the Serial Data Cables **B-6**

Connections for the Serial Data Cables **B-8**

---

**APPENDIX C**
**Behavior of Cisco Unity Failover During Outages of Network Components **C-1****

Introduction **C-1**

Outage Scenarios for Networks of Windows 2000 and IBM Lotus Domino **C-1**

The Primary Server Is Disconnected from the Network, Then Reconnected **C-2**

The Secondary Server Is Disconnected from the Network, Then Reconnected **C-3**

The Primary and Secondary Servers Are Simultaneously Disconnected from the Network, Then the Primary Server Is Reconnected First **C-4**

The Primary and Secondary Servers Are Simultaneously Disconnected from the Network, Then the Secondary Server Is Reconnected First **C-5**

The Primary and Secondary Servers Are Simultaneously Disconnected from the Network, Then Both Servers Are Simultaneously Reconnected **C-6**

The Publisher Cisco CallManager Server Is Disconnected from the Network, Then Reconnected **C-7**

The Subscriber Cisco CallManager Server Is Disconnected from the Network, Then Reconnected **C-8**

The Cisco CallManager Cluster Is Disconnected from the Network, Then Reconnected **C-8**

The Primary Server Crashes **C-9**

The Secondary Server Crashes **C-10**

The Primary and Secondary Servers Crash Simultaneously **C-10**

The Primary Server Is Disconnected from the Network, Then the Domino Server Is Disconnected from the Network **C-11**

---

**INDEX**





## Preface

---

This preface contains the following sections:

- Audience and Use, page vii
- Documentation Conventions, page viii
- Cisco Unity Documentation, page viii
- Obtaining Documentation, page viii
- Documentation Feedback, page ix
- Cisco Product Security Overview, page x
- Obtaining Technical Assistance, page xi
- Obtaining Additional Publications and Information, page xii

## Audience and Use

The *Cisco Unity Failover Configuration and Administration Guide* is intended for installers, system administrators, and technicians who are installing and configuring, customizing, or administering Cisco Unity failover.

The guide contains instructions for configuring and using failover on a Cisco Unity system with IBM Lotus Domino, as well as information on how failover works. You configure Cisco Unity failover after both the primary and secondary servers have been installed according to instructions in the *Cisco Unity Installation Guide*.

For information on making changes to the current Cisco Unity system configuration, refer to the *Cisco Unity Reconfiguration and Upgrade Guide* at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/rug/dom/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/rug/dom/index.htm)

# Documentation Conventions

**Table 1** Cisco Unity Failover Guide Conventions

Convention	Description
boldfaced text	Boldfaced text is used for: <ul style="list-style-type: none"> <li>Key and button names. (Example: Click <b>OK</b>.)</li> <li>Information that you enter. (Example: Enter <b>Administrator</b> in the User Name box.)</li> </ul>
< > (angle brackets)	Angle brackets are used around parameters for which you supply a value. (Example: In the Command Prompt window, enter <b>ping &lt;IP address&gt;</b> .)
- (hyphen)	Hyphens separate keys that must be pressed simultaneously. (Example: Press <b>Ctrl-Alt-Delete</b> .)
> (right angle bracket)	A right angle bracket is used to separate selections that you make: <ul style="list-style-type: none"> <li>On menus. (Example: On the Windows Start menu, click <b>Settings &gt; Control Panel &gt; Phone and Modem Options</b>.)</li> <li>In the navigation bar of the Cisco Unity Administrator. (Example: Go to the <b>System &gt; Configuration &gt; Settings</b> page.)</li> </ul>

The *Cisco Unity Failover Guide* also uses the following conventions:



#### Note

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.



#### Caution

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

## Cisco Unity Documentation

For descriptions and URLs of Cisco Unity documentation on Cisco.com, refer to the *Cisco Unity Documentation Guide*. The document is shipped with Cisco Unity and is available at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/about/aboutdoc.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/about/aboutdoc.htm).

## Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

## Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

## Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

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

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpck/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm)

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:  
<http://www.cisco.com/en/US/partner/ordering/>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

## Documentation Feedback

You can send comments about technical documentation to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems  
Attn: Customer Document Ordering  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—[security-alert@cisco.com](mailto:security-alert@cisco.com)
- Nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)



### Tip

---

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

---

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

# Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

## Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



### Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

## Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

## Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

## Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- World-class networking training is available from Cisco. You can view current offerings at this URL:  
<http://www.cisco.com/en/US/learning/index.html>





# Configuring Cisco Unity Failover



## Caution

Configure Cisco Unity failover only after you have installed both the primary and secondary servers according to instructions in the *Cisco Unity Installation Guide*, and after you have programmed the phone system and configured Cisco Unity according to instructions in the applicable Cisco Unity integration guide.

In this chapter, you do the following tasks in the order listed to configure failover correctly:

1. Configure failover on the primary and secondary servers. See the [“Configuring Failover on the Primary and Secondary Servers”](#) section on page 1-2.
2. On the secondary server, run the Cisco Unity Telephony Integration Manager to configure the voice messaging ports. See the [“Configuring the Voice Messaging Ports on the Secondary Server”](#) section on page 1-3.
3. *If the Cisco Unity system is integrated with a circuit-switched phone system, or with Cisco CallManager 3.2(1) or earlier:* Create a new routing rule so that subscribers will have easy message access when failover occurs. See the [“Creating a Routing Rule That Enables Subscriber Logon by Phone After Failover”](#) section on page 1-4.
4. Set up automatic daily resynchronization of MWIs. See the [“Setting Up Automatic Daily Resynchronization of MWIs”](#) section on page 1-5.
5. Set up notification of when failover occurs. See the [“Setting Up Notification of When Failover Occurs”](#) section on page 1-5.
6. Set up scheduled backups of the Cisco Unity system. See the [“Setting Up Scheduled Backups of Cisco Unity”](#) section on page 1-9.
7. Test Cisco Unity failover. See the [“Testing Cisco Unity Failover”](#) section on page 1-9.
8. *Optional:* Adjust the failover and failback settings. See the [“Customizing Failover and Failback Settings for the Cisco Unity System \(Optional\)”](#) section on page 1-12.
9. *Optional:* Disable failover initiation when calls are unanswered on the primary server. See the [“Disabling Failover Initiation When Calls Are Unanswered on the Primary Server \(Optional\)”](#) section on page 1-14.

If you are installing a new system, return to the “Overview of Mandatory Tasks for Installing Cisco Unity” in the *Cisco Unity Installation Guide* when you are finished with the failover configuration tasks, to continue installing the system correctly.

**Note**

The task list contains tasks that reference instructions in Cisco Unity documentation other than the *Cisco Unity Installation Guide*, so if you do not use the list, the installation will not be successful.

## Configuring Failover on the Primary and Secondary Servers

The Configure Cisco Unity Failover wizard configures default settings for failover and failback on the Cisco Unity system. (For information on the default settings, see [Table 1-2 on page 1-13](#).) You can adjust the settings later in the configuration process—the *Cisco Unity Failover Configuration and Administration Guide* alerts you when to do the procedure.

**Caution**

The Computer Browser service for both primary and secondary servers must have the startup type set to Automatic and must be running. Otherwise, the Configure Cisco Unity Failover wizard cannot locate the other server in the failover pair.

Do the following two procedures in the order listed.

### To Configure Failover on the Primary Server

- Step 1** In Windows Explorer, browse to the **CommServer** directory.
- Step 2** Double-click **FailoverConfig.exe** to start the Configure Cisco Unity Failover wizard.
- Step 3** On the Welcome page, click **Next**.
- Step 4** On the Specify Server Role page, click **Primary Server**, and click **Next**.
- Step 5** On the Enter the Name of Your Server page, click **Browse**, select the name of the secondary server, and click **OK**. The IP address for the secondary server is filled in automatically.
- Step 6** Click **Next**.
- Step 7** On the Enter Failover Account Information page, click **Browse**, and double-click the name of the messaging account. This account will own the failover service.

The account you select must have the right to act as part of the operating system and to log on as a service, and must be a member of the Local Administrators group.

**Caution**

You must specify the same account on both the primary and secondary servers.

- Step 8** In the Password field, enter the password for the account that owns the failover service, and click **Next**.
- Step 9** On the Begin Configuring Your Server page, click **Configure**. The wizard verifies settings and configures failover on the primary server.  
If the wizard does not finish the configuration successfully, an error message explains why the wizard failed. Exit the wizard, correct the problem, and click **Configure** again.
- Step 10** On the Completing page, click **Finish**.

### To Configure Failover on the Secondary Server

---

- Step 1** On the Windows taskbar, double-click the system clock. The Date/Time Properties dialog box appears.
- Step 2** Set the time to the same hour and minute as shown on the primary server, and click **OK**.
- Step 3** In Windows Explorer, browse to the **CommServer** directory.
- Step 4** Double-click **FailoverConfig.exe** to start the Configure Cisco Unity Failover wizard.
- Step 5** On the Welcome page, click **Next**.
- Step 6** On the Specify Server Role page, click **Secondary Server**, and click **Next**.
- Step 7** On the Enter the Name of Your Server page, click **Browse**, select the name of the primary server, and click **OK**. The IP address for the primary server is filled in automatically.
- Step 8** Click **Next**.
- Step 9** On the Enter Failover Account Information page, click **Browse**, and double-click the name of the messaging account. This account will own the failover service.

The account you select must have the right to act as part of the operating system and to log on as a service, and must be a member of the Local Administrators group.



**Caution** You must specify the same account on the both the primary and secondary servers.

---

- Step 10** In the Password field, enter the password for the account that owns the failover service, and click **Next**.
- Step 11** On the Begin Configuring Your Server page, click **Configure**. The wizard verifies settings and configures failover on the secondary server.
- If the wizard does not finish the configuration successfully, an error message explains why the wizard failed. Exit the wizard, correct the problem, and click **Configure** again.
- Step 12** On the Completing page, click **Finish**.
- 

## Configuring the Voice Messaging Ports on the Secondary Server

After running the failover configuration wizard on the secondary server, you must enter settings for the voice messaging ports (for example, set the ports for Answer Calls, Dialout MWIs).

### To Configure the Voice Messaging Ports on the Secondary Server

---

- Step 1** After the secondary server restarts, on the Windows Start menu, click **Programs > Cisco Unity > Manage Integrations**. The Cisco Unity Telephony Integration Manager (UTIM) appears.
- Step 2** In the left pane of the UTIM window, click the phone system integration you are creating.
- Step 3** In the right pane of the UTIM window, click the **Ports** tab.

- Step 4** Enter the port settings. For details on the settings needed by the phone system, refer to the applicable Cisco Unity integration guide. (Integration guides are available at [http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html).)



**Caution** When programming the phone system, do not forward calls to voice messaging ports in Cisco Unity that cannot answer calls (voice messaging ports that are not set to Answer Calls). For example, if a voice messaging port is set only to Dialout MWI, do not forward calls to it.

- Step 5** Click **Save**.

- Step 6** Exit UTIM.

## Creating a Routing Rule That Enables Subscriber Logon by Phone After Failover



**Note** If the Cisco Unity system is integrated with a SIP proxy server or with Cisco CallManager version 3.2(2) or later, skip this section because the phone system automatically forwards calls to the secondary server when it becomes active.

The routing rule for failover allows subscribers to use the phone to log on to Cisco Unity on the secondary server after failover occurs. With the rule, when subscribers dial the internal Cisco Unity phone number that they normally use to access their messages, Cisco Unity automatically routes the call to the secondary server, and subscribers hear the subscriber logon conversation instead of the external caller greeting.

Create the routing rule only after you have run the failover configuration wizard on both the primary and secondary servers. Do the procedure in this section only on the primary server when it is active.

### To Create a Routing Rule That Enables Subscriber Logon by Phone After Failover

- Step 1** On the primary server, open the Cisco Unity Administrator.
- Step 2** Go to the **Call Management > Call Routing > Forwarded Calls** page.
- Step 3** Click the **Add** icon to add a new routing rule.
- Step 4** Enter a name for the rule, and click **Add**.
- Step 5** Enter the corresponding values in the following fields:

<b>Status</b>	Enabled
<b>Call Type</b>	Both

<b>Dialed Number (DNIS)</b>	<The pilot number for the voice messaging ports used by the primary server> Typically, the pilot number is the extension of the first voice messaging port. (For example, if the voice messaging ports are numbered from 7000 to 7047, the pilot number is 7000.)
<b>Send Call To</b>	Attempt Sign-in

- Step 6** Click the **Save** icon. Do not change the order of the rules.  
The new routing rule is stored in the SQL Server database and replicated to the secondary server.
- Step 7** Exit and restart the Cisco Unity software on the primary server, then on the secondary server. For more information, see [Appendix A, “Exiting and Starting the Cisco Unity Software and Server.”](#)
- Step 8** Confirm that the rule is in effect:
- Manually initiate failover. See [“Manually Initiating Failover or Failback” section on page 3-2.](#)
  - Press the messages button on a phone that is associated with a subscriber. Cisco Unity should play the subscriber logon conversation.
  - Press the messages button on a phone that is not associated with a subscriber. Cisco Unity should play the external caller greeting.

## Setting Up Automatic Daily Resynchronization of MWIs

We recommend that you set up the primary and secondary servers to resynchronize MWIs every day.

### To Set Up Automatic Daily Resynchronization of MWIs

- Step 1** On the primary server, on the Windows Start menu, click **Programs > Cisco Unity > Manage Integrations**.
- Step 2** In the left pane of the UTIM window, click the **Properties** node for the phone system integration.
- Step 3** Under MWI Synchronization, check the **Resynchronize** check box.
- Step 4** Select a time when network traffic is at its lowest.
- Step 5** Click **Save**.
- Step 6** Exit UTIM.
- Step 7** On the secondary server, repeat [Step 1](#) through [Step 6](#).

## Setting Up Notification of When Failover Occurs

We recommend 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. You choose the message type(s) that the EMS uses to notify system administrators.

[Table 1-1](#) describes the available message types; the procedure to set up notification follows the table.

**Table 1-1 Message Types Used by the Event Monitoring Service**

Message Type	Description
Voice message	<p>A recorded notification is sent to one or more subscribers or public distribution lists. With this option, you can use the default message, or you can record the message you want sent. The recording must be a WAV file and must be saved on the secondary server. You can use a recording and playback device on the active primary server to record the message.</p> <p>(For information on making recordings, refer to the “Using the Media Master to Record Greetings and Names” section in the “Cisco Unity Conversation” chapter of the <i>Cisco Unity System Administration Guide, Release 4.0(5)</i> at <a href="http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/sag/sag405/dom/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/sag/sag405/dom/index.htm</a>.)</p>
E-mail message	A text message is sent to one or more subscribers or public distribution lists.
SMTP message	A text message is sent by using the SMTP server included with Microsoft Internet Information Services (IIS). This capability is useful when you want to send notification over the Internet to an e-mail address at another location. Because this method does not depend on Cisco Unity for the notification, it can be used to monitor events that indicate catastrophic failure of Cisco Unity.
SNMP trap	<p>SNMP trap notification works with the Remote Serviceability Kit (RSK) to allow you to configure SNMP notifications for monitored Windows Event log entries. You configure the SNMP destinations by using the SNMP Service properties in the Services configuration manager in Windows.</p> <p>(For information on setting up SNMP on the Cisco Unity server, refer to the “Setting Up SNMP Notification” section in the “Configuring Cisco Unity for Maintenance Tasks” chapter of the <i>Cisco Unity Maintenance Guide, Release 4.0(5)</i> at <a href="http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/maint/maint405/dom/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/maint/maint405/dom/index.htm</a>.)</p>
Syslog	A Windows Event log entry is sent over the IP network to a syslog server.

### To Set Up Notification of When Failover Occurs

- Step 1** On the secondary server, click the **Cisco Unity Tools Depot** icon.
- Step 2** In the left pane of the Tools Depot window, expand **Diagnostic Tools**, and double-click **Event Monitoring Service**.
- Step 3** If you are not starting the EMS for the first time, skip to [Step 4](#).  
If you are starting the EMS for the first time, when prompted, enter the password for the account that the AvCsMgr service logs on as, and click **OK**.
- Step 4** On the File menu of the Event Monitoring Service window, click **New > Recipient**. The Create New Recipient dialog box appears.
- Step 5** In the Recipient Name field, enter a display name for the subscriber or distribution list that you want to receive notification.
- Step 6** If you do not want to add notification by voice message, skip to [Step 7](#).

To select the subscriber or list for notification by voice message:

- a. Click the **Voice Mail** tab.
- b. Click either **Subscriber** or **Distribution List**, depending on the recipient.
- c. Click **Select**.
- d. In the Search dialog box, click **Search**, click the name of the subscriber or list, and click **OK**.
- e. To add notification by another message type, continue with the applicable step:

<b>E-mail message</b>	<a href="#">Step 7</a>
<b>SMTP message</b>	<a href="#">Step 8</a>
<b>SNMP Trap</b>	<a href="#">Step 9</a>
<b>Syslog</b>	<a href="#">Step 10</a>

Otherwise, click **OK**, and skip to [Step 11](#).

**Step 7** If you do not want to add notification by e-mail, skip to [Step 8](#).

To select the subscriber or list for notification by e-mail:

- a. Click the **E-Mail** tab.
- b. Click either **Subscriber** or **Distribution List**, depending on the recipient.
- c. Click **Select**.
- d. In the list, click the name of the subscriber or list, and click **OK**.
- e. To add notification by another message type, continue with the applicable step:

<b>SMTP message</b>	<a href="#">Step 8</a>
<b>SNMP Trap</b>	<a href="#">Step 9</a>
<b>Syslog</b>	<a href="#">Step 10</a>

Otherwise, click **OK**, and skip to [Step 11](#).

**Step 8** If you do not want to add notification by SMTP, skip to [Step 9](#).

To select the subscriber or list for notification by SMTP:

- a. Click the **SMTP** tab.
- b. In the **New SMTP Address** field, enter a fully qualified SMTP address for the subscriber or distribution list.
- c. Click **>>** to add the SMTP address to the SMTP Addresses list.
- d. Repeat [Step 8b.](#) and [Step 8c.](#) for each additional SMTP address you want to enter for the subscriber or list.

- e. To add notification by another message type, continue with the applicable step:

<b>SNMP Trap</b>	<a href="#">Step 9</a>
<b>Syslog</b>	<a href="#">Step 10</a>

Otherwise, click **OK**, and skip to [Step 11](#).

- Step 9** If you do not want to add notification by SNMP, skip to [Step 10](#).  
To select an SNMP community name for notification:
- Click the **SNMP Trap** tab.
  - Check the **SNMP Trap Enabled** check box.
  - To add a syslog server for notification, continue with [Step 10](#).  
Otherwise, click **OK**, and skip to [Step 11](#).
- Step 10** If you do not want to add notification by syslog server, skip to [Step 11](#).  
To select a syslog server for notification:
- Click the **Syslog** tab.
  - Check the **Enabled** check box.
  - In the Server field, enter the IP address of the syslog server that you want to receive the Event log message.
  - Click **OK**.
- Step 11** Repeat [Step 4](#) through [Step 10](#) for each additional subscriber or distribution list that you want to receive notification.
- Step 12** On the File menu, click **New > Event**. The Add New Event dialog box appears.
- Step 13** In the Source list, click **CiscoUnity\_NodeMgr**.
- Step 14** Under ID, click **Specific Event ID**, and enter **1047**.
- Step 15** In the Type list, click **Errors**.
- Step 16** In the Notes field, enter **Failover** or another name to indicate what this event monitors.
- Step 17** If you did not add notification by voice message, skip to [Step 18](#).  
To configure the voice message for notification by voice message:
- To the right of the Voice Mail File Name field, click **...**, browse to the WAV file you want to use as the voice message, and click **OK**. The EMS will send this recording as a voice message.
  - In the Voice Mail Priority list, click **Urgent** or another priority that you want.
  - To configure notification by e-mail or by SMTP, continue with [Step 18](#).  
Otherwise, click **OK**, and skip to [Step 19](#).
- Step 18** If you did not add notification by e-mail or SMTP, skip to [Step 19](#).  
To configure e-mail or SMTP content for notification by e-mail or by SMTP:
- In the E-Mail Subject field, enter the subject line for the e-mail or SMTP notification that the EMS will send. You can enter text or right-click to see a menu of insertion strings that the service provides. (For example, you can enter Cisco Unity Failover Occurred.)

- b. In the E-Mail Priority field, click **Urgent** or another priority that you want.
- c. In the E-Mail Body field, accept the default body text or enter customized body text for the e-mail or SMTP notification that the EMS will send. You can enter text or right-click to see a menu of insertion strings that the EMS provides.

For example, you can enter the following:

Cisco Unity Failover Occurred.

Date: <Date>

Time: <Time>

Event ID: <Event>

Event source: <Source>

- d. Click **OK**.

- Step 19** In the right pane of the Event Monitoring Service window, under Recipients, click the **Add Recipients** icon.
- Step 20** In the Edit Recipients for Event dialog box, check the **Active** check box for all recipients you created in [Step 4](#) to receive failover notification, and click **OK**.
- Step 21** Near the top of the right pane, check the **Active** check box, and click **Apply**.
- Step 22** Close the Event Monitoring Service window and the Tools Depot window.
- 

## Setting Up Scheduled Backups of Cisco Unity

To prevent loss of Cisco Unity data caused by the failure of hardware components on the primary and secondary servers, we recommend that you set up scheduled backups of Cisco Unity by using a supported third-party backup and restore application.

For information on backing up Cisco Unity, refer to the “Backing Up a Cisco Unity System” chapter of the *Cisco Unity Maintenance Guide, Release 4.0(5)* at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/unity40/maint/maint405/dom/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/maint/maint405/dom/index.htm).

## Testing Cisco Unity Failover

To test whether Cisco Unity failover and the integration with the secondary server function correctly, do the seven procedures in this section in the order listed.

The testing procedures require that:

- Failover is configured on the primary and secondary servers.
- The primary server is active, and the secondary server is inactive.
- Both servers are integrated with the phone system.

### To Add a Test Subscriber with a Recorded Name

---

- Step 1** In the Cisco Unity Administrator on the primary server, go to the **Subscribers > Subscribers > Profile** page.
- Step 2** Click the **Add** icon.

- Step 3** Click **Notes**.
- Step 4** In the Address Book list, confirm that the address book listed is the one that contains the user data that you want to import.
- If the address book that you want to use is not listed, go to the **System > Configuration > Subscriber Address Books** page and add a different address book.
- Step 5** In the Find Domino Person By list, indicate whether to search by short name, first name, or last name.
- Step 6** Enter the applicable short name or name. You also can enter \* to display a list of all users, or enter one or more characters followed by \* to narrow your search.
- Step 7** Click **Find**.
- Step 8** In the list of matches, click the name of the user to import.
- Step 9** Enter the applicable information on the Add Subscriber page.
- Step 10** Click **Add**.
- Step 11** Record the subscriber name by using the Media Master control bar.
- Step 12** On the subscriber record, customize settings as applicable, then click the **Save** icon.
- 

#### To Confirm That the Data Replication to the Secondary Server Occurred

---

- Step 1** In the Cisco Unity Administrator on the secondary server, go to the **Subscribers > Subscribers > Profile** page for the test subscriber. Seeing the test subscriber on the secondary server indicates that failover replicates the UnityDb SQL database.
- Step 2** Confirm that the Media Master control bar shows that a recorded name exists (the length of the recording is greater than 0). Seeing the recorded name indicates that failover replicates recordings.
- 

#### To Make the Secondary Server Active

---

- Step 1** On the primary server, on the Windows Start menu, click **Programs > Cisco Unity > Failover Monitor**.
- Step 2** Click **Failover**.
- Step 3** Click **OK** to confirm that you want to initiate failover to the secondary server.
- 

#### To Set Up the Integration Test for the Secondary Server

---

- Step 1** Set up two test extensions (Phone 1 and Phone 2) on the same phone system that the Cisco Unity servers are integrated with.
- Step 2** Set Phone 1 to forward calls to the Cisco Unity pilot number when calls are not answered.
- Step 3** In the Cisco Unity Administrator, go to the **Subscribers > Subscribers > Profile** page for the test subscriber you created in the procedure [“To Add a Test Subscriber with a Recorded Name.”](#)
- Step 4** In the Extension field, enter the extension of Phone 1.
- Step 5** In the Active Schedule field, click **All Hours - All Days**.
- Step 6** Click the **Save** icon.

- Step 7** In the navigation bar, click **Call Transfer** to go to the Subscribers > Subscribers > Call Transfer page for the test subscriber.
  - Step 8** Under Transfer Incoming Calls, click **Yes, Ring Subscriber's Extension**, and confirm that the extension is for Phone 1.
  - Step 9** Under Transfer Type, click **Release to Switch**.
  - Step 10** Click the **Save** icon.
  - Step 11** In the navigation bar, click **Messages** to go to the Subscribers > Subscribers > Messages page for the test subscriber.
  - Step 12** Under Message Waiting Indicators (MWIs), check the **Use MWI for Message Notification** check box.
  - Step 13** In the Extension field, enter **x**.
  - Step 14** Click the **Save** icon.
- 

#### To Test Recording a Message and Activating the MWI

---

- Step 1** From Phone 2, dial the extension for Phone 1.
  - Step 2** Confirm that Phone 1 rings and that you hear a ringback tone on Phone 2. Do not answer Phone 1.
  - Step 3** Confirm that after the number of rings that the phone system is set to wait, the call is forwarded to Cisco Unity and that you hear the greeting for the test subscriber. Hearing the greeting means that the phone system forwarded the unanswered call and the call-forward information to Cisco Unity, which correctly interpreted the information.
  - Step 4** Leave a message for the test subscriber, and hang up Phone 2.
  - Step 5** Confirm that the MWI on Phone 1 is activated. The activated MWI means that the phone system and the secondary server are successfully integrated for activating MWIs.
- 

#### To Test Listening to a Message and Deactivating the MWI

---

- Step 1** From Phone 1, dial the internal pilot number for Cisco Unity.
  - Step 2** When asked for your password, enter the password for the test subscriber. Hearing the request for your password means that the phone system sent the necessary call information to Cisco Unity, which correctly interpreted the information.
  - Step 3** Confirm that you hear the recorded name for the test subscriber (if you did not record a name for the test subscriber, you will hear the extension for Phone 1). Hearing the recorded name means that Cisco Unity correctly identified the subscriber by the extension.
  - Step 4** When asked whether you want to listen to your messages, press **1**.
  - Step 5** After listening to the message, press **3** to delete the message.
  - Step 6** Confirm that the MWI on Phone 1 is deactivated. The deactivated MWI means that the phone system and Cisco Unity are successfully integrated for deactivating MWIs.
  - Step 7** Hang up Phone 1.
-

**To Delete the Test Subscriber**

- 
- Step 1** In the Cisco Unity Administrator, go to the **Subscribers > Subscribers > Profile page**.  
If the name of the test subscriber is not displayed, click the **Find** icon (the magnifying glass) in the title bar, then click **Find**, and click the name of the test subscriber in the list that appears.
- Step 2** In the title bar, click the **Delete Subscriber** icon (the X).
- Step 3** Click **Delete**.
- 

## Customizing Failover and Failback Settings for the Cisco Unity System (Optional)

You can customize the default settings for failover and failback that the failover configuration wizard gives the primary and secondary servers. (For example, you might want to increase the frequency of file replication.)

When you customize failover and failback, you can specify:

- The frequency with which the primary and secondary servers send keep-alive events (or “pings”) to one another, and the number of missed keep-alive events before the secondary server starts taking calls. The default setting is to send keep-alive events every second and to wait 30 keep-alive events before failing over.




---

**Note** When the primary server is active but not receiving keep-alive events from the secondary server, failover will not occur because the secondary server may not be able to take calls. Similarly, when the secondary server is active but not receiving keep-alive events from the primary server, failback will not occur because the primary server may not be able to take calls.

---

- The frequency of file replication. The default setting is to replicate changed files every 10 minutes.
- Whether the secondary server initiates failback to the primary server during a certain time range each day. The default setting is for manual failback.
- Whether failover is initiated when a call is answered by a port on the secondary server. The default setting is to enable failover initiation.

You customize failover and failback on only one server. Changes to failover configuration are replicated to the other server.

**To Customize Failover and Failback Settings**

- 
- Step 1** On either server (unless otherwise noted in [Table 1-2](#)), on the Windows Start menu, click **Programs > Cisco Unity > Failover Monitor**.
- Step 2** Click **Configure**.
- Step 3** Using [Table 1-2](#), change the applicable values in the Failover Configuration dialog box.

**Table 1-2** Failover and Failback Configuration Settings

Field	Value
Interval (ms)	Specify the amount of time that elapses between keep-alive events. <i>The default setting is 1,000 milliseconds (1 second).</i>  Increasing the interval between keep-alive events decreases network traffic. However, it also increases the amount of time before the secondary server begins answering calls if the primary server fails.
Missed Events Before Failover	Specify the number of keep-alive events from the primary server that the secondary server must miss before it becomes the active server. <i>The default is 30 keep-alive events.</i>  Decreasing the number of missed keep-alive events before failover may cause a network glitch or abnormally high traffic on the network to trigger an unnecessary failover. Increasing the number increases the amount of time before the secondary server begins answering calls if the primary server fails.  Note that failover can also be initiated under other circumstances. Some errors are detected immediately (for example, if the Cisco Unity service—AvCsMgr.exe—stops running), and failover is initiated when the error is detected.
File Replication Interval (In Minutes)	Specify the amount of time that elapses before the active server replicates changed files to the inactive server. <i>The default is 10 minutes.</i>  Increasing the file replication interval causes the active server to replicate files to the inactive server less often, which decreases network traffic.
Failback Type	<ul style="list-style-type: none"> <li>• If you do not want to schedule the secondary server to initiate failback to the primary server, click <b>Manual</b>. The secondary server fails back only when you manually initiate failback by using the Failover Monitor. <i>The default is the Manual failback type.</i></li> <li>• If you want to schedule when the secondary server initiates failback to the primary server, click <b>Scheduled</b>, and enter settings for the Scheduled Failback Start and Scheduled Failback End field. (You can manually initiate failback before the scheduled time in the Failover Monitor.)</li> </ul>
Scheduled Failback Start and Scheduled Failback End	If you chose Scheduled in the Failback Type field, enter the range of time in which the secondary server initiates failback. <i>The default is 3 a.m. to 6 a.m.</i>
Force Failover If Call Arrives on Inactive Secondary	Set this field only on the secondary server. The setting does not replicate between servers. <ul style="list-style-type: none"> <li>• Check the check box to enable failover initiation when a call is not answered by a voice messaging port on the primary server, is forwarded to the secondary server, and then is answered by a port on the secondary server. <i>The default is to enable failover initiation.</i></li> <li>• Uncheck the check box to disable failover initiation when a call is answered by a port on the secondary server.</li> </ul>

**Step 4** Click **OK** to close the Failover Configuration dialog box.

**Step 5** Close the Failover Monitor.

# Disabling Failover Initiation When Calls Are Unanswered on the Primary Server (Optional)

By default, failover is initiated when a call is not answered by a voice messaging port on the primary server, is forwarded to the secondary server, and then is answered by a port on the secondary server.

Do the following procedure if you want to disable the initiation of failover when calls are unanswered on the primary server.

## To Disable Failover Initiation When Calls Are Unanswered on the Primary Server

- 
- Step 1** On the secondary server, on the Windows Start menu, click **Programs > Cisco Unity > Failover Monitor**.
  - Step 2** Click **Configure**.
  - Step 3** Uncheck the **Force Failover If Call Arrives on Inactive Secondary** check box.
  - Step 4** Click **OK**.
-



## Tasks Required When Failover or Failback Occurs

---

This chapter contains the following sections:

- [Notifying Subscribers of the Active Server and the URLs to Use for Accessing Cisco Unity Web Applications, page 2-1](#)
- [Notifying Subscribers to Update the Server Name in the Media Master, page 2-1](#)
- [T1 Integration: Enabling the Phone System to Send Calls to the Active Server After Failover or Failback Occurs, page 2-2](#)

### Notifying Subscribers of the Active Server and the URLs to Use for Accessing Cisco Unity Web Applications

Notify subscribers when failover or failback occurs, and give them the correct URLs to use for accessing the following Cisco Unity web applications on the active server:

- Cisco Unity Administrator
- Status Monitor
- Cisco Personal Communications Assistant (Subscribers use the Cisco PCA to access the Cisco Unity Assistant and the Cisco Unity Inbox.)



**Note**

---

When subscribers access the Cisco Unity Administrator on the inactive server, they will not be allowed to save changes. When subscribers access the Cisco PCA on the inactive server, any changes they make in the Cisco Unity Assistant can be saved, but the changes are not replicated on the active server.

---

### Notifying Subscribers to Update the Server Name in the Media Master

The Media Master control bar appears on some Cisco Unity Administrator and Cisco Unity Assistant pages. By clicking the VCR-style controls, subscribers use it to make and play recordings. They specify whether it uses a phone or a computer microphone and speakers as recording and playback devices.

When failover or failback occurs, the phone does not work as a recording or playback device with the Media Master in the Cisco Unity Administrator unless subscribers manually update the Cisco Unity server name specified in the Media Master. (The server name updates automatically for the Media Master in the Cisco Unity Assistant.)

The next section contains a procedure for manually updating Media Master settings in the Cisco Unity Administrator.

**Note**

Subscribers who use a computer microphone and speakers as the Media Master recording and playback devices do not need to make changes after failover or failback.

## Changing Media Master Settings for Recording and Playback After Failover or Failback

After failover or failback, do the procedure in this section to change the server name setting for the Media Master control bar in the Cisco Unity Administrator, so you can continue to use the phone as the Media Master recording and playback device.

Note that updates to the Media Master settings in the Cisco Unity Administrator are saved per user, per computer. This means that:

- A subscriber who is logged on to the Cisco Unity Administrator can update the server name from any Media Master control bar Options menu.
- If a subscriber also uses another computer to access the Cisco Unity Administrator (for example, a computer at home), the server name specified in the Media Master needs to be updated on the second computer as well.
- If multiple subscribers share the same computer, the Media Master settings need to be updated for each subscriber who uses the computer.

### To Change Media Master Settings for Recording and Playback After Failover or Failback

- 
- Step 1** Log on to the Cisco Unity Administrator.
  - Step 2** Go to a Media Master control bar.
  - Step 3** On the Media Master control bar Options menu, click **Options**.
  - Step 4** In the Phone Record and Playback Settings dialog box, enter the name of the applicable server.
  - Step 5** Click **OK**.
  - Step 6** Repeat [Step 1](#) through [Step 5](#) on each computer that you use to access the applications.
- 

## T1 Integration: Enabling the Phone System to Send Calls to the Active Server After Failover or Failback Occurs

When Cisco Unity and the phone system use a T1 line for voice connections, the phone system cannot send calls to the secondary server when failover occurs. Similarly, after the secondary server is active and receiving calls and failback occurs, the phone system cannot send calls to the primary server.

This section contains two procedures. After failover occurs, do the first procedure, “[To Enable the Phone System to Send Calls to the Secondary Server After Failover Occurs](#),” to enable the phone system to send calls over a T1 line to the secondary server. (Alternatively, you can disconnect the T1 line that connects the primary server and the phone system.)

After failback occurs, do the second procedure, “[To Enable the Phone System to Send Calls to the Primary Server After Failback Occurs](#),” to enable the phone system to send calls over a T1 line to the primary server. (Alternatively, you can reconnect the T1 line that connects the primary server and the phone system.)

#### To Enable the Phone System to Send Calls to the Secondary Server After Failover Occurs

---

- Step 1** On the primary server, exit the Cisco Unity software. For more information, see the “[Exiting the Cisco Unity Software](#)” section on page A-1.
  - Step 2** On the Windows Start menu, click **Programs > Dialogic System Software > Dialogic Configuration Manager–DCM**.
  - Step 3** On the Service menu, click **Stop Service**. A second Dialogic Configuration Manager window appears.
  - Step 4** When the message “Success: Dialogic service stopped” appears, click **Close**.
- 

#### To Enable the Phone System to Send Calls to the Primary Server After Failback Occurs

---

- Step 1** On the primary server, on the Windows Start menu, click **Programs > Dialogic System Software > Dialogic Configuration Manager–DCM**.
  - Step 2** On the Service menu, click **Start Service**. A second Dialogic Configuration Manager window appears.
  - Step 3** When the message “Success: Dialogic service started” appears, click **Close**.
  - Step 4** Start the Cisco Unity software. For more information, see the “[Starting the Cisco Unity Software](#)” section on page A-3.
-

■ T1 Integration: Enabling the Phone System to Send Calls to the Active Server After Failover or Failback Occurs



# Monitoring and Maintaining Cisco Unity Failover

This chapter contains the following sections:

- [Starting the Servers in the Correct Order, page 3-1](#)
- [Determining Which Server Is Active, page 3-1](#)
- [Manually Initiating Failover or Failback, page 3-2](#)
- [Disabling Automatic Failover and Failback for Troubleshooting, page 3-3](#)
- [Confirming That Failover and Failback Function Correctly, page 3-5](#)
- [Determining the Cause of Failover or Failback from an Event ID, page 3-7](#)
- [Changing the IP Address of the Primary Server, page 3-8](#)
- [Changing the IP Address of the Secondary Server, page 3-13](#)
- [About Uninstalling Failover on a Cisco Unity Server, page 3-18](#)
- [Replacing and Converting the Primary and Secondary Servers, page 3-18](#)

## Starting the Servers in the Correct Order

Start the primary server first, then start the secondary server. If you start the secondary server first, it becomes the active server.

## Determining Which Server Is Active

You can determine which server is active by viewing information in the Failover Monitor on either server. In the Services section, Local Status indicates the status of the server on which you are viewing the Failover Monitor, and Remote Status indicates the status of the other server. [Table 3-1](#) lists the values and their meanings.

**Table 3-1** Meanings of Local Status and Remote Status Values

Value for Local Status or Remote Status	Meaning
Running; Active	The specified server is the active server.
Running; Inactive	The specified server is the inactive server.

Table 3-1 Meanings of Local Status and Remote Status Values (continued)

Value for Local Status or Remote Status	Meaning
Not running; Active	No server is currently active because a required service is not running. However, the specified server will be the active server when you restart the Cisco Unity software.
Not running; Inactive	The specified server is the inactive server. However, if the active server fails, the specified server will not start taking calls because a required service is not running.  If you restart the Cisco Unity software on the specified server, it will become the active server as long as you have not disabled automatic failover and failback, and the other server is not active.
Running Not running; Unknown	The Node Manager service (AvCsNodeMgr) is starting on the specified server.
Other	Failover or failback is occurring.

## Manually Initiating Failover or Failback

You can manually initiate failover from the primary server to the secondary server so that the secondary server takes calls while you perform maintenance on the primary server. When you want the primary server to start taking calls again, you manually initiate failback from the secondary server to the primary server.

Manual failover can also be initiated by the Event Monitoring Service (EMS) when a user-specified event occurs. For details, refer to EMS Help.



### Note

The failover feature cannot be used for continuing Cisco Unity service on one server while upgrading the Cisco Unity software on the other server. Both the primary and secondary servers must be out of service while the Cisco Unity software is upgraded. The secondary server cannot handle voice messaging while the primary server is being upgraded.

When you manually initiate failover or failback, the interaction of the primary and secondary servers is the same as for automatic failover and failback. However, we recommend that you confirm that any changes to the SQL Server database (UnityDb) on the active server have been replicated to the inactive server before initiating failover or failback. Do the first procedure, [“To Confirm That Changes to UnityDb Have Been Replicated to the Inactive Server.”](#)

The second and third procedures provide instructions for initiating failover and failback.

### To Confirm That Changes to UnityDb Have Been Replicated to the Inactive Server

- Step 1** On the primary server, on the Windows Start menu, click **Programs > Microsoft SQL Server > Enterprise Manger**.
- Step 2** In the left pane of the Console Root window, browse to the name of the primary server. Typically, this name is two levels under the Microsoft SQL Servers node.
- Step 3** Browse to the **Replication Monitor > Agents** node.

**Step 4** Check for errors in the **Snapshot Agent**, **Log Reader Agent**, **Distribution Agent**, and **Queue Reader Agent**. Ignore errors that do not apply to the time period when UnityDb changed.

Replication is complete when both primary and secondary servers are running, the agents are not active, and the status of the agents is Idle or Succeeded. Any other status for any agent indicates that replication is not complete.

---

#### To Manually Initiate Failover to the Secondary Server

---

**Step 1** On the primary server, on the Windows Start menu, click **Programs > Cisco Unity > Failover Monitor**.

**Step 2** Click **Failover**.

**Step 3** Click **OK** to confirm that you want to fail over to the secondary server.

**Step 4** See the following sections to do the applicable tasks:

- [“Notifying Subscribers of the Active Server and the URLs to Use for Accessing Cisco Unity Web Applications” section on page 2-1](#)
- [“Notifying Subscribers to Update the Server Name in the Media Master” section on page 2-1](#)
- [“T1 Integration: Enabling the Phone System to Send Calls to the Active Server After Failover or Failback Occurs” section on page 2-2](#)

---

#### To Manually Initiate Failback to the Primary Server

---

**Step 1** On the secondary server, on the Windows Start menu, click **Programs > Cisco Unity > Failover Monitor**.

**Step 2** Click **Failback**.

**Step 3** Click **OK** to confirm that you want to fail back to the primary server.

**Step 4** See the following sections to do the applicable tasks:

- [“Notifying Subscribers of the Active Server and the URLs to Use for Accessing Cisco Unity Web Applications” section on page 2-1](#)
- [“Notifying Subscribers to Update the Server Name in the Media Master” section on page 2-1](#)
- [“T1 Integration: Enabling the Phone System to Send Calls to the Active Server After Failover or Failback Occurs” section on page 2-2](#)

## Disabling Automatic Failover and Failback for Troubleshooting

Disable automatic failover and failback only during troubleshooting.

This section contains procedures for disabling automatic failover and failback, for manually initiating failover and failback while the automatic functions are disabled, and for re-enabling automatic failover and failback.

Note that when automatic failover and failback are disabled:

- File replication is also disabled.

- You must manually force a server to become active or inactive by using the Failover Monitor.
- If you restart the primary and secondary servers while automatic failover and failback are disabled, both servers start as inactive, so Cisco Unity is not able to take calls.

**Caution**

When you disable automatic failover and failback, the primary server never fails over to the secondary server even if the primary server stops taking calls. In addition, the secondary server never fails back to the primary server even if you have specified a schedule for automatic failback.

---

**To Disable Automatic Failover and Failback**

- Step 1** On the primary server, on the Windows Start menu, click **Programs > Cisco Unity > Failover Monitor**.
- Step 2** Click **Advanced**.
- Step 3** Check the **Disable Automatic Failover and Failback** check box.
- Step 4** Click **OK**.
- 

---

**To Manually Initiate Failover to the Secondary Server While Automatic Failover and Failback Are Disabled**

- Step 1** On the primary server, on the Windows Start menu, click **Programs > Cisco Unity > Failover Monitor**.
- Step 2** Click **Force Inactive**.
- Step 3** Click **OK** to confirm.
- Step 4** On the secondary server, on the Windows Start menu, click **Programs > Cisco Unity > Failover Monitor**.
- Step 5** Click **Force Active**.
- Step 6** Click **OK** to confirm.
- Step 7** See the following sections to do the applicable tasks:
- [“Notifying Subscribers of the Active Server and the URLs to Use for Accessing Cisco Unity Web Applications”](#) section on page 2-1
  - [“Notifying Subscribers to Update the Server Name in the Media Master”](#) section on page 2-1
  - [“T1 Integration: Enabling the Phone System to Send Calls to the Active Server After Failover or Failback Occurs”](#) section on page 2-2
- 

---

**To Manually Initiate Failback to the Primary Server While Automatic Failover and Failback Are Disabled**

- Step 1** On the secondary server, on the Windows Start menu, click **Programs > Cisco Unity > Failover Monitor**.
- Step 2** Click **Force Inactive**.
- Step 3** Click **OK** to confirm.
- Step 4** On the primary server, on the Windows Start menu, click **Programs > Cisco Unity > Failover Monitor**.
- Step 5** Click **Force Active**.

- Step 6** Click **OK** to confirm.
- Step 7** See the following sections to do the applicable tasks:
- “Notifying Subscribers of the Active Server and the URLs to Use for Accessing Cisco Unity Web Applications” section on page 2-1
  - “Notifying Subscribers to Update the Server Name in the Media Master” section on page 2-1
  - “T1 Integration: Enabling the Phone System to Send Calls to the Active Server After Failover or Failback Occurs” section on page 2-2
- 

Do the following procedure if you are not planning to run the failover configuration wizard. (Automatic failover and failback are re-enabled during the failover configuration wizard.)

#### To Re-enable Automatic Failover and Failback

---

- Step 1** On the primary server, on the Windows Start menu, click **Programs > Cisco Unity > Failover Monitor**.
- Step 2** Click **Advanced**.
- Step 3** Uncheck the **Disable Automatic Failover and Failback** check box.
- Step 4** Click **OK**.
- 

## Confirming That Failover and Failback Function Correctly

This section contains two procedures. Do the first procedure, “[To Check the Consistency of the Cisco Unity Database](#),” only if you have not already run the Cisco Unity Directory Walker (DbWalker) utility. DbWalker is used to check the consistency of and correct errors in the Cisco Unity database, ensuring that database replication to the secondary server will function correctly after the failover configuration wizard has been run.

During the second procedure, “[To Confirm That Failover and Failback Function Correctly](#),” you may need to run the failover configuration wizard, depending on test results.

#### To Check the Consistency of the Cisco Unity Database

---

- Step 1** On the primary server, install the latest version of the Cisco Unity Directory Walker (DbWalker) utility, available at [http://ciscounitytools.com/App\\_DirectoryWalker4.htm](http://ciscounitytools.com/App_DirectoryWalker4.htm).
- Step 2** Run DbWalker, and correct all errors that the utility finds. Refer to DbWalker Help for detailed instructions on running the utility and on correcting errors in the database. (The Help file, DbWalker.htm, is in the same directory as DbWalker.exe.)
-

If you must configure failover again or run the failover configuration wizard during the following procedure, see the “[Configuring Cisco Unity Failover](#)” chapter for instructions.

### To Confirm That Failover and Failback Function Correctly

- 
- Step 1** While the primary server is active, create a test file (for example, Test.txt) in the CommServer\Stream Files directory on the primary server.
- Step 2** Confirm that the file replicates to the secondary server within the time set in the File Replication Interval field in the Failover Monitor (the default is 10 minutes).
- If the file does not replicate, you must configure failover on both the primary and secondary servers, then do this procedure again.
- Step 3** On the primary server, modify the extension of a subscriber.
- Step 4** Confirm that the change replicates to the secondary server immediately. When you open the Cisco Unity Administrator on the secondary server, ignore the warnings that the secondary server is inactive.
- If the change does not replicate, you must configure failover on both the primary and secondary servers, then do this procedure again.
- Step 5** On the primary server, on the Windows Start menu, click **Programs > Microsoft SQL Server > Enterprise Manager**. The SQL Server Enterprise Manager window appears.
- Step 6** In the left pane, expand the **Microsoft SQL Servers** node.
- Step 7** Expand the **Replication Monitor** node.
- If the node does not exist, failover has not been configured. You must configure failover on both the primary and secondary servers, then do this procedure again.
- Step 8** If the Replication Monitor subnodes do not have red Xs on them in the left pane, UnityDb database replication for failover is functioning normally.
- If the Replication Monitor subnodes have red Xs on them, restore replication for failover:
- On the primary server, close the SQL Server Enterprise Manager window.
  - On the secondary server, run the failover configuration wizard.
- Step 9** Restore the original extension of the subscriber.
- Step 10** On the primary server, manually initiate failover.
- Step 11** Confirm that the primary server becomes inactive and that the secondary server becomes active.
- Step 12** Call in to Cisco Unity.
- Step 13** Confirm that the secondary server answers the call.
- If the secondary server does not answer the call, you must configure failover on both the primary and secondary servers, then do this procedure again.
- Step 14** On the secondary server, delete the test file from the CommServer\Stream Files directory.
- Step 15** Confirm that the file is deleted from the primary server within the time set in the File Replication Interval field in the Failover Monitor (the default is 10 minutes).
- Step 16** On the secondary server, manually initiate failback.
- Step 17** Confirm that the primary server becomes active and that the secondary server becomes inactive.

- Step 18** Call in to Cisco Unity.
- Step 19** Confirm that the primary server answers the call.

## Determining the Cause of Failover or Failback from an Event ID

This section describes how to determine the cause of failover and failback based on the event IDs that appear in the Event log.

### To Determine the Cause of Failover or Failback from an Event ID

- Step 1** On the primary server, on the Windows Start menu, click **Programs > Administrative Tools > Event Viewer**.
- Step 2** In the Tree pane on the left, click **Application Log**. The log appears in the right pane.
- Step 3** Locate the entries that show **CiscoUnity\_NodeMgr** in the Source column.
- Step 4** For the entries, note the event IDs that appear in the Event column.
- Step 5** On the secondary server, repeat [Step 1](#) through [Step 4](#).
- Step 6** Use [Table 3-2](#), which follows the procedure, to determine the cause of failover or failback.

**Table 3-2** Causes of Failover or Failback Based on Event ID

Server and Event ID	Cause
Primary: 1070 and 1048 Secondary: 1050 and 1047	Manual failover occurred, initiated by the system administrator using the Failover Monitor.
Primary: 1078 and 1048 Secondary: 1050 and 1047	Manual failover occurred, initiated by the Event Monitoring Service (EMS) when a user-specified event occurs.
Secondary: 1068 and 1048 Primary: 1049 and 1047	Manual failback occurred.
Secondary: 1069 and 1048 Primary: 1049 and 1047	Scheduled failback occurred.
Secondary: 1050 and 1047 1010 (possible) 1011 (possible)	The active primary server crashed.
Primary: 1049 and 1047 1010 (possible) 1011 (possible)	The active secondary server crashed.

**Table 3-2 Causes of Failover or Failback Based on Event ID (continued)**

Server and Event ID	Cause
Primary: 1010 (possible) 1011 (possible) Secondary: 1050 and 1047 1010 (possible) 1011 (possible)	The active primary server has network connectivity problems.
Secondary: 1010 (possible) 1011 (possible) Primary: 1049 and 1047 1010 (possible) 1011 (possible)	The active secondary server has network connectivity problems.
Primary: 1048 Secondary: 1050, 1047, and CiscoUnity_Miu 542	<p>The combination of event IDs will appear for any of the following causes:</p> <ul style="list-style-type: none"> <li>• The active primary server has a bad port that caused failover to occur.</li> <li>• A caller dialed the extension of a voice messaging port in the secondary server and the Force Failover If Call Arrives on Inactive Secondary check box is checked in the Failover Monitor, causing failover to occur.</li> <li>• <i>Circuit-switched phone systems:</i> For phone systems that use a linear hunt group (the hunt group starts searching always with the same voice messaging port), an unintended failover may have occurred if the Force Failover If Call Arrives on Inactive Secondary check box is checked in the Failover Monitor. With this configuration, when a call to Cisco Unity is terminated either before being answered or within a few seconds after being answered by the primary server, the phone system may route a second call immediately to the same port. This can cause the secondary server to count rings from both calls as a single call, thus triggering failover.</li> </ul> <p>The cause can be eliminated by setting up a guard timer on the phone system. The timer enforces a minimum interval between consecutive calls sent to a given port. Note that the timer may not be available on all phone systems.</p>

## Changing the IP Address of the Primary Server

When choosing an IP address for the primary Cisco Unity server, note the following considerations:

- Do not choose an address accessible from the Internet. Doing so can expose the Cisco Unity server to unwanted intrusion from the Internet, even when the server is hardened.
- Do not choose an address that puts the Cisco Unity server on the opposite side of a firewall from:
  - The Domino server to which Cisco Unity sends voice messages for delivery.
  - The Domino server that Cisco Unity monitors for changes to the directory.
  - Any Domino server that homes Cisco Unity subscriber mailboxes.

- The domain controller/global catalog server that Cisco Unity accesses.

Do the following nine procedures in the order listed.

#### To Disable Automatic Failover and Failback, and Stop File Replication

---

- Step 1** On the secondary server, on the Windows Start menu, click **Programs > Cisco Unity > Failover Monitor**.
  - Step 2** Click **Failover**.
  - Step 3** Click **OK** to confirm that you want to fail over to the secondary server.
  - Step 4** Click **Advanced**.
  - Step 5** Check the **Disable Automatic Failover and Failback** check box.
  - Step 6** Click **OK**.
  - Step 7** Click **Configure**.
  - Step 8** Uncheck the **Force Failover If Call Arrives on Inactive Secondary** check box.
  - Step 9** Click **OK**.
  - Step 10** Close the Failover Monitor.
- 

#### To Stop the Node Manager Service on the Primary and Secondary Servers

---

- Step 1** On the primary server, on the Windows Start menu, click **Programs > Administrative Tools > Services**.
  - Step 2** In the Services window, right-click **AvCsNodeMgr**, and click **Stop**.
  - Step 3** Close the Services window on the primary server.
  - Step 4** On the secondary server, on the Windows Start menu, click **Programs > Administrative Tools > Services**.
  - Step 5** In the Services window, right-click **AvCsNodeMgr**, and click **Stop**.
  - Step 6** Close the Services window on the secondary server.
- 

#### To Change the IP Address of the Primary Server

---

- Step 1** On the primary server, on the Windows Start menu, click **Settings > Control Panel > Network and Dial-Up Connections > Local Area Connection**.
- Step 2** Click **Properties**.
- Step 3** In the Components Checked Are Used by This Connection list, select **Internet Protocol (TCP/IP)**, but do not uncheck the check box.
- Step 4** Click **Properties**.

- Step 5** In the Internet Protocol (TCP/IP) Properties dialog box, change values as applicable. Refer to Windows Help for more information.
  - Step 6** Click **OK** to close the Internet Protocol TCP/IP Properties dialog box.
  - Step 7** Click **OK** to close the Local Area Connection Properties dialog box.
  - Step 8** Close the Local Area Connection Status window.
  - Step 9** If the IP address is in a different subnet, disconnect the network cable from the original subnet, and connect the cable from the target subnet to the Cisco Unity server.
  - Step 10** Confirm that the server name can be resolved to the new IP address.
- 

#### To Check the Consistency of the Cisco Unity Database

---

- Step 1** On the primary server, install the latest version of the Cisco Unity Directory Walker (DbWalker) utility, available at [http://ciscounitytools.com/App\\_DirectoryWalker4.htm](http://ciscounitytools.com/App_DirectoryWalker4.htm).
  - Step 2** Run DbWalker, and correct all errors that the utility finds. Refer to DbWalker Help for detailed instructions on running the utility and on correcting errors in the database. (The Help file, DbWalker.htm, is in the same directory as DbWalker.exe.)
- 

#### To Set the Registry of the Secondary Server by Reconfiguring Failover

---

- Step 1** On the Windows taskbar, double-click the system clock. The Date/Time Properties dialog box appears.
- Step 2** Set the time to the same hour and minute as shown on the primary server, and click **OK**.
- Step 3** In Windows Explorer, browse to the **CommServer** directory.
- Step 4** Double-click **FailoverConfig.exe** to start the Configure Cisco Unity Failover wizard.
- Step 5** On the Welcome page, click **Next**.
- Step 6** On the Specify Server Role page, click **Secondary Server**, and click **Next**.
- Step 7** On the Enter the Name of Your Server page, click **Browse**, select the name of the primary server, and click **OK**. The IP address for the primary server is filled in automatically.
- Step 8** Click **Next**.
- Step 9** On the Enter Failover Account Information page, click **Browse**, and double-click the name of the messaging account. This account will own the failover service.

The account you select must have the right to act as part of the operating system and to log on as a service, and must be a member of the Local Administrators group.



**Caution** You must specify the same account on the both the primary and secondary servers.

---

- Step 10** In the Password field, enter the password for the account that owns the failover service, and click **Next**.

- Step 11** On the Begin Configuring Your Server page, click **Configure**. The wizard verifies settings and configures failover on the secondary server.
- If the wizard does not finish the configuration successfully, an error message explains why the wizard failed. Exit the wizard, correct the problem, and click **Configure** again.
- Step 12** On the Completing page, click **Finish**.
- 

### To Confirm That Both Servers Can Be Pinged and That SQL Replication Has No Errors

---

- Step 1** On the primary server, on the Windows Start menu, click **Programs > Accessories > Command Prompt**.
- Step 2** In the Command Prompt window, enter **C:\Ping <IP address of secondary server>**, and press **Enter**.  
If the secondary server sends a reply, the IP address is valid.  
If the secondary server does not send a reply, either the primary server has a problem obtaining an address from the DHCP server, or the assigned IP address conflicts with the IP address of another computer on the network. Verify the network settings. If needed, troubleshoot any problem as you would a network connectivity problem.
- Step 3** In the Command Prompt window, enter **C:\Ping <Primary server name>**, and press **Enter**.  
If the primary server sends a reply, the server name is valid.
- Step 4** On the secondary server, on the Windows Start menu, click **Programs > Accessories > Command Prompt**.
- Step 5** In the Command Prompt window, enter **C:\Ping <IP address of primary server>**, and press **Enter**.  
If the primary server sends a reply, the IP address is valid.  
If the primary server does not send a reply, either the secondary server has a problem obtaining an address from the DHCP server, or the assigned IP address conflicts with the IP address of another computer on the network. Verify the network settings. If needed, troubleshoot any problem as you would a network connectivity problem.
- Step 6** In the Command Prompt window, enter **C:\Ping <Secondary server name>**, and press **Enter**.  
If the secondary server sends a reply, the server name is valid.
- Step 7** On the Windows Start menu, click **Programs > Microsoft SQL Server > Enterprise Manager**. The SQL Server Enterprise Manager window appears.
- Step 8** Confirm that no errors appear for the SQL replication agents.  
If errors appear for the Distribution agent, right-click the agent, and click **Start Synchronizing** to resume SQL replication. The errors will clear in a few minutes after the network connection between the primary and secondary servers is restored.
-

---

### To Restart the Primary Server

- Step 1** While the secondary server is active and answering calls, restart the primary server.  
The primary server becomes active, and the secondary server becomes inactive.
- Step 2** Confirm that the primary server starts and that there are no errors in the Application Event log.
- 

### To Confirm That the Primary Server Is Active and, If Applicable, To Re-enable Automatic Failover and Failback

- Step 1** On the secondary server, on the Windows Start menu, click **Programs > Cisco Unity > Failover Monitor**.
- Step 2** If the secondary server is active, click **Failback**, and click **OK**.
- Step 3** Re-enable automatic failover and failback, if applicable:
- a. Click **Advanced**.
  - b. Uncheck the **Disable Automatic Failover and Failback** check box.
  - c. Click **OK**.
- The setting will replicate to the primary server.
- Step 4** Close the Failover Monitor.
- 

### To Confirm That Failover and Failback Function Correctly

- Step 1** While the primary server is active, create a test file (for example, Test.txt) in the CommServer\Stream Files directory on the primary server.
- Step 2** Confirm that the file replicates to the secondary server within the time set in the File Replication Interval field in the Failover Monitor (the default is 10 minutes).  
If the file does not replicate, you must configure failover on both the primary and secondary servers, then do this procedure again.
- Step 3** On the primary server, modify the extension of a subscriber.
- Step 4** Confirm that the change replicates to the secondary server immediately. When you open the Cisco Unity Administrator on the secondary server, ignore the warnings that the secondary server is inactive.  
If the change does not replicate, you must configure failover on both the primary and secondary servers, then do this procedure again.
- Step 5** On the primary server, on the Windows Start menu, click **Programs > Microsoft SQL Server > Enterprise Manager**. The SQL Server Enterprise Manager window appears.
- Step 6** In the left pane, expand the **Microsoft SQL Servers** node.
- Step 7** Expand the **Replication Monitor** node.  
If the node does not exist, failover has not been configured. You must configure failover on both the primary and secondary servers, then do this procedure again.

- Step 8** If the Replication Monitor subnodes do not have red Xs on them in the left pane, UnityDb database replication for failover is functioning normally.
- If the Replication Monitor subnodes have red Xs on them, restore replication for failover:
- a. On the primary server, close the SQL Server Enterprise Manager window.
  - b. On the secondary server, run the failover configuration wizard.
- Step 9** Restore the original extension of the subscriber.
- Step 10** On the primary server, manually initiate failover.
- Step 11** Confirm that the primary server becomes inactive and that the secondary server becomes active.
- Step 12** Call in to Cisco Unity.
- Step 13** Confirm that the secondary server answers the call.
- If the secondary server does not answer the call, you must configure failover on both the primary and secondary servers, then do this procedure again.
- Step 14** On the secondary server, delete the test file from the CommServer\Stream Files directory.
- Step 15** Confirm that the file is deleted from the primary server within the time set in the File Replication Interval field in the Failover Monitor (the default is 10 minutes).
- Step 16** On the secondary server, manually initiate failback.
- Step 17** Confirm that the primary server becomes active and that the secondary server becomes inactive.
- Step 18** Call in to Cisco Unity.
- Step 19** Confirm that the primary server answers the call.
- 

## Changing the IP Address of the Secondary Server

When choosing an IP address for the secondary Cisco Unity server, note the following considerations:

- Do not choose an address accessible from the Internet. Doing so can expose the Cisco Unity server to unwanted intrusion from the Internet, even when the server is hardened.
- Do not select an address that puts the Cisco Unity server on the opposite side of a firewall from:
  - The Domino server to which Cisco Unity sends voice messages for delivery.
  - The Domino server that Cisco Unity monitors for changes to the directory.
  - Any Domino server that homes Cisco Unity subscriber mailboxes.
  - The domain controller/global catalog server that Cisco Unity accesses.

Do the following nine procedures in the order listed.

### To Disable Automatic Failover and Failback, and Stop File Replication

---

- Step 1** On the secondary server, on the Windows Start menu, click **Programs > Cisco Unity > Failover Monitor**.
- Step 2** Click **Advanced**.

- Step 3** Check the **Disable Automatic Failover and Failback** check box.
  - Step 4** Click **OK**.
  - Step 5** Click **Configure**.
  - Step 6** Uncheck the **Force Failover If Call Arrives on Inactive Secondary** check box.
  - Step 7** Click **OK**.
  - Step 8** Close the Failover Monitor.
- 

#### To Stop the Node Manager Service on the Primary and Secondary Servers

---

- Step 1** On the primary server, on the Windows Start menu, click **Programs > Administrative Tools > Services**.
  - Step 2** In the Services window, right-click **AvCsNodeMgr**, and click **Stop**.
  - Step 3** Close the Services window on the primary server.
  - Step 4** On the secondary server, on the Windows Start menu, click **Programs > Administrative Tools > Services**.
  - Step 5** In the Services window, right-click **AvCsNodeMgr**, and click **Stop**.
  - Step 6** Close the Services window on the secondary server.
- 

#### To Change the IP Address of the Secondary Server

---

- Step 1** On the secondary server, on the Windows Start menu, click **Settings > Control Panel > Network and Dial-Up Connections > Local Area Connection**.
  - Step 2** Click **Properties**.
  - Step 3** In the Components Checked Are Used by This Connection list, select **Internet Protocol (TCP/IP)**, but do not uncheck the check box.
  - Step 4** Click **Properties**.
  - Step 5** In the Internet Protocol (TCP/IP) Properties dialog box, change values as applicable. Refer to Windows Help for more information.
  - Step 6** Click **OK** to close the Internet Protocol TCP/IP Properties dialog box.
  - Step 7** Click **OK** to close the Local Area Connection Properties dialog box.
  - Step 8** Close the Local Area Connection Status window.
  - Step 9** If the IP address is in a different subnet, disconnect the network cable from the original subnet, and connect the cable from the target subnet to the Cisco Unity server.
  - Step 10** Confirm that the server name can be resolved to the new IP address.
-

---

### To Check the Consistency of the Cisco Unity Database

---

- Step 1** On the primary server, install the latest version of the Cisco Unity Directory Walker (DbWalker) utility, available at [http://ciscounitytools.com/App\\_DirectoryWalker4.htm](http://ciscounitytools.com/App_DirectoryWalker4.htm).
- Step 2** Run DbWalker, and correct all errors that the utility finds. Refer to DbWalker Help for detailed instructions on running the utility and on correcting errors in the database. (The Help file, DbWalker.htm, is in the same directory as DbWalker.exe.)
- 

---

### To Set the Registry of the Primary Server by Reconfiguring Failover

---

- Step 1** In Windows Explorer, browse to the **CommServer** directory.
- Step 2** Double-click **FailoverConfig.exe** to start the Configure Cisco Unity Failover wizard.
- Step 3** On the Welcome page, click **Next**.
- Step 4** On the Specify Server Role page, click **Primary Server**, and click **Next**.
- Step 5** On the Enter the Name of Your Server page, click **Browse**, select the name of the secondary server, and click **OK**. The IP address for the secondary server is filled in automatically.
- Step 6** Click **Next**.
- Step 7** On the Enter Failover Account Information page, click **Browse**, and double-click the name of the messaging account. This account will own the failover service.

The account you select must have the right to act as part of the operating system and to log on as a service, and must be a member of the Local Administrators group.



---

**Caution** You must specify the same account on the both the primary and secondary servers.

---

- Step 8** In the Password field, enter the password for the account that owns the failover service, and click **Next**.
- Step 9** On the Begin Configuring Your Server page, click **Configure**. The wizard verifies settings and configures failover on the primary server.
- If the wizard does not finish the configuration successfully, an error message explains why the wizard failed. Exit the wizard, correct the problem, and click **Configure** again.
- Step 10** On the Completing page, click **Finish**.
- 

---

### To Confirm That Both Servers Can Be Pinged and That SQL Replication Has No Errors

---

- Step 1** On the primary server, on the Windows Start menu, click **Programs > Accessories > Command Prompt**.

- Step 2** In the Command Prompt window, enter **C:\Ping <IP address of secondary server>**, and press **Enter**.  
If the secondary server sends a reply, the IP address is valid.  
If the secondary server does not send a reply, either the primary server has a problem obtaining an address from the DHCP server, or the assigned IP address conflicts with the IP address of another computer on the network. Verify the network settings. If needed, troubleshoot any problem as you would a network connectivity problem.
- Step 3** In the Command Prompt window, enter **C:\Ping <Primary server name>**, and press **Enter**.  
If the primary server sends a reply, the server name is valid.
- Step 4** On the secondary server, on the Windows Start menu, click **Programs > Accessories > Command Prompt**.
- Step 5** In the Command Prompt window, enter **C:\Ping <IP address of primary server>**, and press **Enter**.  
If the primary server sends a reply, the IP address is valid.  
If the primary server does not send a reply, either the secondary server has a problem obtaining an address from the DHCP server, or the assigned IP address conflicts with the IP address of another computer on the network. Verify the network settings. If needed, troubleshoot any problem as you would a network connectivity problem.
- Step 6** In the Command Prompt window, enter **C:\Ping <Secondary server name>**, and press **Enter**.  
If the secondary server sends a reply, the server name is valid.
- Step 7** On the Windows Start menu, click **Programs > Microsoft SQL Server > Enterprise Manager**. The SQL Server Enterprise Manager window appears.
- Step 8** Confirm that no errors appear for the SQL replication agents.  
If errors appear for the Distribution agent, right-click the agent, and click **Start Synchronizing** to resume SQL replication. The errors will clear in a few minutes after the network connection between the primary and secondary servers is restored.
- 

#### To Restart the Secondary Server

---

- Step 1** While the primary server is active and answering calls, restart the secondary server.
- Step 2** Confirm that the secondary server starts and that there are no errors in the Application Event log.
- 

#### To Confirm That the Primary Server Is Active and, If Applicable, to Re-enable Automatic Failover and Failback

---

- Step 1** On the secondary server, on the Windows Start menu, click **Programs > Cisco Unity > Failover Monitor**.
- Step 2** If the secondary server is active, click **Failback**, and click **OK**.
- Step 3** Re-enable automatic failover and failback, if applicable:
- a. Click **Advanced**.

- b. Uncheck the **Disable Automatic Failover and Failback** check box.
- c. Click **OK**.

The setting will replicate to the primary server.

**Step 4** Close the Failover Monitor.

---

### To Confirm That Failover and Failback Function Correctly

---

- Step 1** While the primary server is active, create a test file (for example, Test.txt) in the CommServer\Stream Files directory on the primary server.
- Step 2** Confirm that the file replicates to the secondary server within the time set in the File Replication Interval field in the Failover Monitor (the default is 10 minutes).
- If the file does not replicate, you must configure failover on both the primary and secondary servers, then do this procedure again.
- Step 3** On the primary server, modify the extension of a subscriber.
- Step 4** Confirm that the change replicates to the secondary server immediately. When you open the Cisco Unity Administrator on the secondary server, ignore the warnings that the secondary server is inactive.
- If the change does not replicate, you must configure failover on both the primary and secondary servers, then do this procedure again.
- Step 5** On the primary server, on the Windows Start menu, click **Programs > Microsoft SQL Server > Enterprise Manager**. The SQL Server Enterprise Manager window appears.
- Step 6** In the left pane, expand the **Microsoft SQL Servers** node.
- Step 7** Expand the **Replication Monitor** node.
- If the node does not exist, failover has not been configured. You must configure failover on both the primary and secondary servers, then do this procedure again.
- Step 8** If the Replication Monitor subnodes do not have red Xs on them in the left pane, UnityDb database replication for failover is functioning normally.
- If the Replication Monitor subnodes have red Xs on them, restore replication for failover:
- a. On the primary server, close the SQL Server Enterprise Manager window.
  - b. On the secondary server, run the failover configuration wizard.
- Step 9** Restore the original extension of the subscriber.
- Step 10** On the primary server, manually initiate failover.
- Step 11** Confirm that the primary server becomes inactive and that the secondary server becomes active.
- Step 12** Call in to Cisco Unity.
- Step 13** Confirm that the secondary server answers the call.
- If the secondary server does not answer the call, you must configure failover on both the primary and secondary servers, then do this procedure again.
- Step 14** On the secondary server, delete the test file from the CommServer\Stream Files directory.
- Step 15** Confirm that the file is deleted from the primary server within the time set in the File Replication Interval field in the Failover Monitor (the default is 10 minutes).

- Step 16** On the secondary server, manually initiate failback.
- Step 17** Confirm that the primary server becomes active and that the secondary server becomes inactive.
- Step 18** Call in to Cisco Unity.
- Step 19** Confirm that the primary server answers the call.
- 

## About Uninstalling Failover on a Cisco Unity Server

When converting a Cisco Unity server configured for failover to another purpose for which failover is not needed, it is necessary to change a number of settings and, for the secondary server, to copy the Cisco Unity data and reinstall the Cisco Unity software. A process that only uninstalls Cisco Unity failover will give unsatisfactory results.

To convert a Cisco Unity server configured for failover to a Cisco Unity server without failover, refer to the “Replacing or Converting a Cisco Unity Server or Failover Servers” chapter of the *Cisco Unity Reconfiguration and Upgrade Guide* at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/rug/dom/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/rug/dom/index.htm).

To convert a Cisco Unity server configured for failover to a server for another application, follow the installation instructions for that application.

## Replacing and Converting the Primary and Secondary Servers

Information and instructions for the following tasks are available in the “Replacing or Converting a Cisco Unity Server or Failover Servers” chapter of the *Cisco Unity Reconfiguration and Upgrade Guide*:

- Replacing only the primary server.
- Replacing only the secondary server.
- Replacing the primary and secondary servers at the same time.
- Converting the secondary server to a 60-day Cisco Unity server without a primary server.
- Converting the secondary server to a permanent regular Cisco Unity server without failover.
- Converting the primary server to a permanent regular Cisco Unity server without failover.

The guide is available at

[http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/rug/dom/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/rug/dom/index.htm).



## About Cisco Unity Failover

---

This chapter contains the following sections:

- [How Failover Works in Cisco Unity, page 4-1](#)
- [Requirements for Cisco Unity Failover, page 4-4](#)
- [Effects of Using or Not Using the Force Failover Setting, page 4-5](#)
- [Effects of Failover and Failback on Calls in Progress, page 4-6](#)
- [Status Monitoring and File Replication, page 4-6](#)
- [Events When Failover Occurs, page 4-9](#)
- [Events When Failback Occurs, page 4-9](#)
- [Automatic and Manual Failback, page 4-10](#)
- [Causes of Failover and Failback, page 4-10](#)
- [Intervals for Failover and Failback, page 4-12](#)
- [Causes of Both Servers Becoming Active at the Same Time, page 4-14](#)
- [Effects of Shutting Down and Restarting the Primary and Secondary Servers, page 4-15](#)
- [Licensing Restrictions on Using a Secondary Server Without a Primary Server, page 4-15](#)

## How Failover Works in Cisco Unity

Failover is a feature that provides a 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.



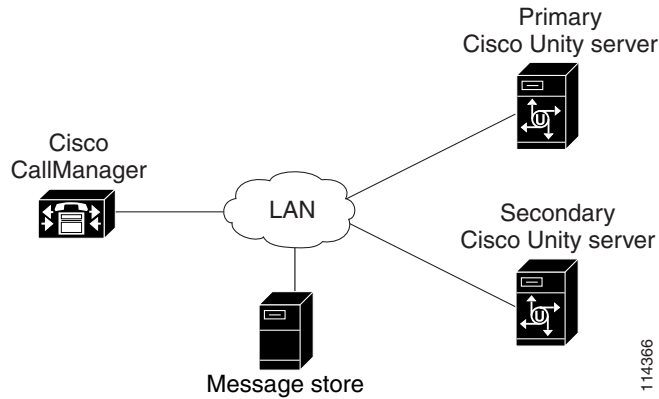
### Caution

The failover feature cannot be used for continuing Cisco Unity service (voice messaging) on one server while upgrading the Cisco Unity software on the other server. Both primary and secondary servers must be out of service while the Cisco Unity software is upgraded. The secondary server cannot handle voice messaging while the primary server is being upgraded.

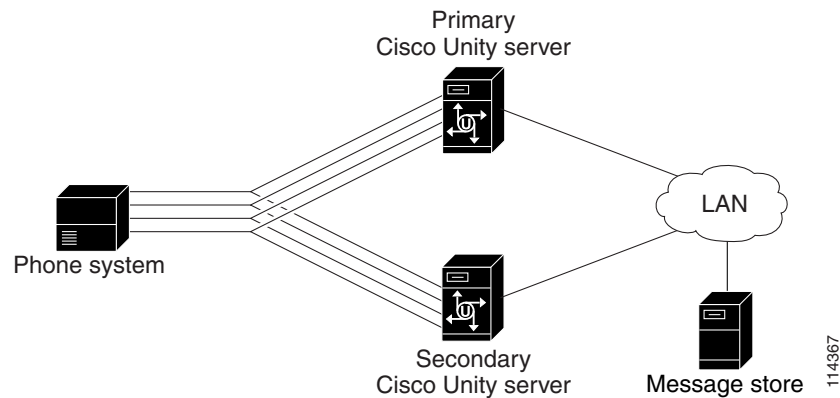
[Figure 4-1](#) shows a failover configuration for an IP (Internet Protocol) phone system. [Figure 4-2](#) shows a failover configuration for a circuit-switched phone system in a DTMF integration with voice cards. [Figure 4-3](#) shows one possible failover configuration for a circuit-switched phone system in a serial

integration (with voice cards) that uses a data splitter on the RS-232 serial cable to provide a data link to both Cisco Unity servers. For information on making the line connections, see [Appendix B, “Line Connections Between the Phone System and the Cisco Unity Servers.”](#)

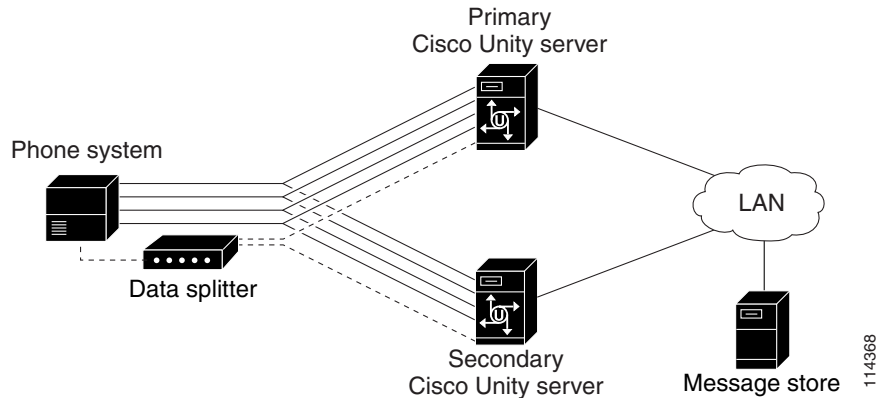
**Figure 4-1** Failover Configuration for an IP Phone System



**Figure 4-2** Failover Configuration for a Circuit-Switched Phone System in a DTMF Integration with Voice Cards



**Figure 4-3** One Possible Failover Configuration for a Circuit-Switched Phone System in a Serial Integration with Voice Cards



Under normal circumstances, the primary server is active—Cisco Unity answers phone calls and takes messages, sends message notifications, and turns message waiting indicators (MWIs) on and off. The secondary server is inactive—Cisco Unity is running, but it does not perform any voice messaging functions.

Table 4-1 shows the behavior of the two servers when the primary server is active.

**Table 4-1** Cisco Unity Behavior When the Primary Server Is Active

Cisco Unity Behavior	Primary Server	Secondary Server
Running	Yes	Yes <sup>1</sup>
Active (handles voice messaging processes)	Yes	No
Answers phone calls	Yes	No
Sends message notifications	Yes	No
Turns on and off MWIs	Yes	No

- Typically, Cisco Unity on the secondary server is running unless the server is shut down (for example, when the server is undergoing maintenance).

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 operations. This shift from primary to secondary Cisco Unity servers is called failover. If you want to stop the primary Cisco Unity server for maintenance, you can also initiate failover manually.

Table 4-2 shows the behavior of the two servers when the secondary server is active.

**Table 4-2** Cisco Unity Behavior When the Secondary Server Is Active

Cisco Unity Behavior	Primary Server	Secondary Server
Running	Depends <sup>1</sup>	Yes
Active (handles voice messaging processes)	No	Yes
Answers phone calls	No	Yes
Sends message notifications	No	Yes
Turns on and off MWIs	No	Yes

1. Under certain circumstances, Cisco Unity on the primary server continues to run after failover occurs. Under other circumstances, Cisco Unity is not running. For details, see the “Intervals for Failover and Failback” section on page 4-12.

When the secondary server is active, Cisco Unity functions normally, with the following exceptions:

- For a few seconds after a failure occurs and before the secondary server becomes active, subscribers hear a fast-busy tone when they dial the internal phone number to log on to Cisco Unity by phone.
- Subscribers cannot use the phone as a recording or playback device with the Media Master in the Cisco Unity Administrator unless they manually update the Cisco Unity server name specified in the Media Master. (For more information, see the “Notifying Subscribers to Update the Server Name in the Media Master” section on page 2-1.)
- Reports can be generated only while the primary server is active.

You can configure the secondary server to initiate failback daily. When failback succeeds, the primary server becomes the active server again. Alternatively, you can configure failover so that the secondary server fails back only when you manually initiate failback by using the Failover Monitor.

For the behavior of failover during outages of network components, see Appendix C, “Behavior of Cisco Unity Failover During Outages of Network Components.”

## Requirements for Cisco Unity Failover

- The primary and secondary servers must both be qualified for Cisco Unity. Refer to Part 1 of *Cisco Unity 4.0 System Requirements, and Supported Hardware and Software* at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_unity/sysreq/40\\_sysrq.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/sysreq/40_sysrq.htm).
- Both Cisco Unity servers must have the same platform overlay.
- Both Cisco Unity servers must be member servers of the same domain (they cannot be domain controllers). Do not install Active Directory on either Cisco Unity server.
- The Cisco Unity server names must be 15 characters or fewer, and the server names must not be identical for the primary and secondary servers.
- Both Cisco Unity servers must be connected to the same message store.
- The only IBM Lotus software installed on the Cisco Unity servers is Lotus Notes. All other IBM Lotus software is on a computer other than the Cisco Unity servers. Messages must not be stored on the Cisco Unity servers. (This separation allows the availability of messages when either the primary or secondary server is not functioning.)
- SQL Server 2000 Standard Edition must be installed on both Cisco Unity servers. (MSDE 2000 is not supported on either server with Cisco Unity failover.)
- One Cisco Unity server is designated the primary server, and the other Cisco Unity server is designated the secondary server.
- Both Cisco Unity servers must have the same enabled features and configurations.
- Both Cisco Unity servers must be connected to the network and have a reliable connection of 100 Mbps minimum. There is no option for installing failover without a network connection.
- Failover can be used with any supported Cisco Unity configuration except with one that has no network connection.
- Cisco Unity and SQL Server 2000 must be installed on both the primary and secondary servers with the same domain account.

- MSSQLSERVER and SQLSERVERAGENT services on both Cisco Unity servers must be configured to use the same domain account that is a member of the Local Administrators group on both servers. These services cannot be configured to run as Local System. SQLSERVERAGENT on the primary server must be able to log on to SQL Server on the secondary server by using Windows NT authentication.

## Effects of Using or Not Using the Force Failover Setting

How Cisco Unity failover responds to calls that are not answered on the primary server depends on the Force Failover If Call Arrives on Inactive Secondary setting in the Failover Monitor. Causes for the primary server not answering calls are:

- One or more voice messaging ports on the primary server lock up and fail to respond to calls.
- An insufficient number of voice messaging ports are available to handle phone traffic.
- The primary server experiences high CPU utilization.
- *Cisco CallManager integration only:* The voice messaging ports on the primary server unregister with the Cisco CallManager server.

By checking or not checking the Force Failover check box, you can control whether an unanswered call on the primary server causes failover to occur.

### Events When the Force Failover If Call Arrives on Inactive Secondary Check Box Is Checked

When a call is not answered on the primary server and the check box is checked in the Failover Monitor, the following events occur:

1. The call is presented to the secondary server.
2. The call causes an Event log entry on the secondary server, which can alert the system administrator to the potential problem on the primary server. (For details on setting up event notification, see the [“Setting Up Notification of When Failover Occurs”](#) section on page 1-5.)
3. The secondary server answers the call, causing failover to occur.

Customers may want the secondary server to become active when a voice messaging port on the primary server is locked up. However, other customers who install Cisco Unity servers with a large number of ports may be annoyed that failover occurs when just one port is locked.

### Events When the Force Failover If Call Arrives on Inactive Secondary Check Box Is Not Checked

When a call is not answered on the primary server and the check box is not checked in the Failover Monitor, the following events occur:

1. The call is forwarded to the next available voice messaging port on the primary server. (Failover does not occur, and the primary server remains active.)
2. The call causes an Event log entry on the secondary server, which can alert the system administrator to the potential problem on the primary server. (For details on setting up event notification, see the [“Setting Up Notification of When Failover Occurs”](#) section on page 1-5.)

Failover occurs only when the primary server fails or when the system administrator manually initiates failover.

Customers who install Cisco Unity servers with a large number of voice messaging ports do not experience failover when just one port is locked. However, if all ports are locked or the CPU utilization is high, Cisco Unity stops answering calls until the system administrator manually initiates failover.

## Effects of Failover and Failback on Calls in Progress

When failover or failback is initiated, calls in progress are maintained or dropped, depending on the status of the Cisco Unity service (AvCsMgr.exe) and of the network.

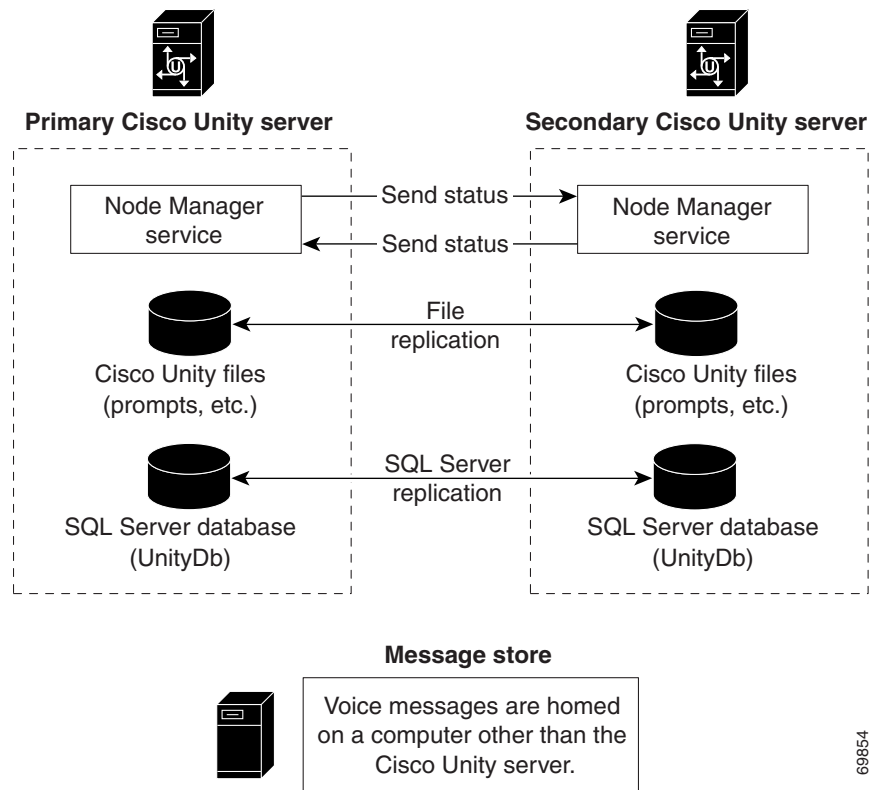
**Table 4-3** Failover and Failback Effects on Calls in Progress

Cisco Unity Service or Network Status	Action
The Cisco Unity service is stopped or crashes	Calls in progress are dropped. When the Cisco Unity service (AvCsMgr.exe) on the primary server becomes inactive, the secondary server becomes active, but the dropped calls cannot be recovered.
The Cisco Unity service is active when failover or failback occurs	Calls in progress are maintained until the callers hang up.
Network connections are lost	<p>Calls in progress from circuit-switched phone systems are maintained until the callers hang up.</p> <p>Calls in progress from IP phone systems (for example, Cisco CallManager) may be dropped, depending on the nature of the network problem.</p> <p>(For the behavior of failover during outages of network components, see <a href="#">Appendix C, “Behavior of Cisco Unity Failover During Outages of Network Components.”</a>)</p>

## Status Monitoring and File Replication

When failover is configured and Cisco Unity is functioning normally, monitoring and replication take place as shown in [Figure 4-4](#).

Figure 4-4 Monitoring and Replication Actions



69854

For the behavior of failover during outages of network components, see [Appendix C, “Behavior of Cisco Unity Failover During Outages of Network Components.”](#)

Details of the monitoring and replication actions are described below.

#### Node Manager Service

- The Node Manager service (AvCsNodeMgr in the Services window) on the active server sends its status to the inactive server (it sends keep-alive events to the inactive server) at a frequency the installer configures. The default is 1 second. The TCP packet is 785 bytes in size and uses port 3653, which the installer can change as a hidden registry setting.
- The Node Manager service in the inactive server sends its status to the active server (it sends keep-alive events to the active server) at a frequency the installer configures. The default is 1 second. The TCP packet is 785 bytes in size and uses port 3653, which the installer can change as a hidden registry setting.
- The Node Manager service monitors the Cisco Unity service (AvCsMgr) on the server.

#### Cisco Unity Files

- The frequency of replication between the active and inactive servers depends on the value of the File Replication Interval field in the Failover Monitor and how often the Cisco Unity files change.
- The Node Manager service monitors and replicates the files in the directories Localize\DefaultConfiguration, Localize\Prompts, Snapshot, Stream Files, Support, and UnityMTA (which contains the Unity Messaging Repository, or UMR) on the Cisco Unity server.

- The Node Manager service creates a snapshot in the Snapshot directory of the files in the replicated directories during each replication cycle. In subsequent replication cycles, the Node Manager service compares the current snapshot with the previous snapshot to determine the files that should be replicated.
- 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 such circumstances, the new information is not on the secondary server and may be lost or corrupted on the primary server.
- Replication of changed files is disabled when the Node Manager service is set to manual mode.

#### SQL Server Database (UnityDb)

- Replication occurs every minute if there are SQL data changes.
- The database on the primary server is configured as the publisher and distributor.
- The database publication is UnityDbPublication.
- The database on the secondary server is configured as the subscriber.
- Two-way replication between the two servers is enabled to let the primary server receive all changes made during periods it is online and inactive.
- If changed data has not been replicated to the secondary server when the AvCsMgr service is stopped or the Cisco Unity server crashes, the new data may be lost. Under such circumstances, the new data is not on the secondary server and may be lost or corrupted on the primary server.

#### Voice Messages

- Voice messages are not replicated because failover requires that the message store (Domino server) be on a separate computer from the Cisco Unity server. When voice messages are kept on a separate server, they are available to subscribers no matter which Cisco Unity server is active.
- Voice messages saved in the Unity Messaging Repository (UMR) when the message store (Domino server) is off line are replicated to the inactive server with other Cisco Unity files. (The UMR is located in the UnityMTA directory.)

## Data That Is Not Replicated

Changes to the following Cisco Unity settings are not replicated between the primary and secondary servers. You must manually change values on both servers.

- Registry settings
- Recording settings
- Phone language settings
- GUI language settings
- Port settings
- Integration settings
- Media Master server name settings
- Recording and playback device server name settings in the VCR-style recorder/player in the message form available with IBM Lotus Notes with IBM Lotus Domino Unified Communications (DUC) for Cisco.
- *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.)

## Events When Failover Occurs

1. Status monitoring and file replication occur when the primary server is active:
  - a. The Node Manager service monitors the Cisco Unity service and other services on the server to determine whether failover should be initiated.
  - b. The Node Manager services on both the primary and secondary servers send status to each other on a regular basis.
  - c. Certain Cisco Unity files when changed are replicated from the primary server to the secondary server.
  - d. Data from the SQL Database (UnityDb) when changed is replicated from the primary server to the secondary server.
  - e. The primary server answers calls, sends message notification, and turns MWIs on and off. The secondary server is inactive and performs none of these functions.
  - f. Voice messages are stored in the message store (Domino server), which is on a separate computer from the primary and secondary servers.
2. Failover occurs when any of the following events take place:
  - The Node Manager service on the secondary server does not receive a status update from the primary server within the period specified (for example, when the primary server crashes, the Node Manager service is stopped, or there are network connectivity problems).
  - 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.
3. The Node Manager service on the secondary server assumes that the Cisco Unity service is stopped on the primary server and activates the Cisco Unity service on its server. (In the case of the secondary server receiving a call, the Node Manager service on the secondary server instructs the Node Manager service on the primary server to initiate failover.) The secondary server starts answering calls, sending message notification, and turning MWIs on and off.
4. The Node Manager service on the secondary server writes a warning to the Event log.

For the behavior of failover during outages of network components, see [Appendix C, “Behavior of Cisco Unity Failover During Outages of Network Components.”](#)

## Events When Failback Occurs

1. Status monitoring and file replication occur when the secondary server is active and the primary server is running (but inactive):
  - a. The Node Manager service monitors the Cisco Unity service and other services on the server to determine whether failback should be initiated.
  - b. The Node Manager services on both the secondary and primary servers send status to each other on a regular basis.
  - c. Certain Cisco Unity files when changed are replicated from the secondary server to the primary server.
  - d. Data from the SQL Database (UnityDb) when changed is replicated from the secondary server to the primary server.

- e. The secondary server answers calls, sends message notification, and turns MWIs on and off. The primary server is inactive and performs none of these functions.
  - f. Voice messages are stored in the message store (Domino server), which is on a separate computer from the secondary and primary servers.
2. Failback occurs when either of the following events takes place:
    - When automatic failback is enabled, the time specified for failback arrives, and the Node Manager service on the secondary server notifies the Node Manger service on the primary server that the Cisco Unity service on the secondary server is inactive.
    - Manual failback is initiated by using the Failover Monitor.
  3. The Node Manager service on the primary server assumes that the Cisco Unity service is stopped on the secondary server and activates the Cisco Unity service on its server. (In the case of the primary server receiving a call, the Node Manager service on the primary server instructs the Node Manger service on the secondary server to initiate failback.) The primary server then starts answering calls, sending message notification, and turning MWIs on and off.
  4. The Node Manager service on the primary server writes a warning to the Event log.

For the behavior of failover during outages of network components, see [Appendix C, “Behavior of Cisco Unity Failover During Outages of Network Components.”](#)

## Automatic and Manual Failback

Failback can occur automatically at a time you specify, or you can manually initiate failback. The Failback Type setting is in the Failover Monitor and has the following options:

<b>Scheduled</b>	Use this option if you want the secondary server to fail back automatically. In the Failover Monitor, enter values for the Scheduled Failback Start and Scheduled Failback End fields to set the time for automatic failback. This option is useful when you want failback to occur, for example, at night. You can initiate failback manually before the scheduled time by using the Failover Monitor.
<b>Manual</b>	Use this option if you do not want the secondary server to automatically fail back to the primary server when the primary server becomes available. The secondary server fails back to the primary server only when you manually fail back by using the Failover Monitor.

For details on customizing the failback type in the Failover Monitor, see the [“Customizing Failover and Failback Settings for the Cisco Unity System \(Optional\)”](#) section on page 1-12.

## Causes of Failover and Failback

### Failover Causes

Failover from the primary server to the secondary server can occur for the following reasons:

- Manual failover is initiated from the Failover Monitor.

- The network connection to the primary server is lost. However, both primary and secondary servers remain active.
- The network connection between the primary and secondary servers experiences latency, which causes the Node Manager service on the secondary to miss 30 keep-alive events from the primary server (the default setting in the Failover Monitor).
- If the Force Failover If Call Arrives on Inactive Secondary check box is checked in the Failover Monitor and a call is answered by the secondary server.
- The primary server loses power while the secondary server is still powered.
- The primary server is turned off while the secondary server remains on.
- On the primary server, the Cisco Unity service is stopped or crashes.
- On the primary server, the Node Manager service stops.
- On the primary server, the Node Manager service fails to send keep-alive events to the Node Manager service on the secondary server as configured in the Failover Configuration dialog box of the Failover Monitor.
- There is excessive CPU usage on either the primary or secondary server. When this problem occurs on the primary server before failover and the secondary server after failover, the primary and secondary servers will failover and failback repeatedly until the CPU usage problem is resolved.
- The Event Monitoring Service (EMS) initiates manual failover when a user-specified event occurs.

## Failback Causes

Failback from the secondary server to the primary server can occur for the following reasons:

- The problem on the primary server is resolved, and manual failback is initiated from the Failover Monitor.
- The problem on the primary server is resolved, and the scheduled time for failback has arrived as configured in the Failover Configuration dialog box of the Failover Monitor.
- The secondary server loses power while the primary server is still powered but inactive.
- The secondary server is turned off while the primary server remains on but is inactive.
- On the secondary server, the Cisco Unity service is stopped or crashes, while the primary server is on but inactive.
- On the secondary server, the Node Manager service stops, while the primary server is on but inactive.
- On the secondary server, the Node Manager service fails to send keep-alive events to the Node Manager service on the primary server as configured in the Failover Configuration dialog box of the Failover Monitor, while the primary server is on but inactive.

# Intervals for Failover and Failback

## Failover Interval

When failover occurs, the time it takes for the secondary server to begin answering calls typically depends on what causes failover as described in [Table 4-4](#).

**Table 4-4** *Interval for Failover*

Failover Cause	Time
Manual failover	<ul style="list-style-type: none"> <li>The secondary server begins answering calls immediately.</li> <li>Calls in progress on the primary server are not dropped but are maintained until the callers hang up.</li> </ul>
Network outage	<ul style="list-style-type: none"> <li>The secondary server begins answering calls after waiting for the number of keep-alive events set in the Missed Events Before Failover field in the Failover Monitor. The time required depends on the value of the field and on the value of the Interval (ms) field. The default settings for the fields result in a 30-second delay for the secondary server to become active.</li> <li>A network outage may result in both primary and secondary servers being active at the same time. When the network outage is resolved, the primary server remains active and the secondary server becomes inactive.</li> <li>Calls in progress from a circuit-switched phone system are not dropped but are maintained until the callers hang up. Calls in progress from an IP phone system (for example, Cisco CallManager) may be dropped, depending on the nature of the network outage.</li> </ul>
Failure of the AvCsMgr service on the primary server	<ul style="list-style-type: none"> <li>The secondary server begins answering calls immediately.</li> <li>Calls in progress on the primary server are dropped.</li> </ul>
Failure of the operating system on the primary server	<ul style="list-style-type: none"> <li>The secondary server begins answering calls after waiting for the number of keep-alive events set in the Missed Events Before Failover field in the Failover Monitor. The time required depends on the value of the field and on the value of the Interval (ms) field. The default settings for the fields result in a 30-second delay for the secondary server to become active.</li> <li>Calls in progress on the primary server are dropped.</li> </ul>
Inactive secondary server answers a call	<ul style="list-style-type: none"> <li>The secondary server begins answering calls immediately.</li> <li>Calls in progress on the primary server are not dropped but are maintained until the callers hang up.</li> </ul>

## Failback Interval

When failback occurs, the time it takes for the primary server to begin answering calls typically depends on what causes failback as described in [Table 4-5](#). File replication occurs in the background and does not affect the failback interval.

**Table 4-5** *Interval for Failback*

<b>Failback Cause</b>	<b>Time</b>
Automatic failback, and the primary server is on but inactive	<ul style="list-style-type: none"> <li>• Failback is initiated only when the time scheduled in the Failover Monitor arrives.</li> <li>• When Cisco Unity is integrated with a circuit-switched phone system, the voice messaging ports on the primary server that are connected to that phone system begin answering calls immediately after failback is initiated.</li> <li>• When Cisco Unity is integrated with a SIP phone system, the voice messaging ports on the primary server that are registered to that phone system begin answering calls immediately after failback is initiated.</li> <li>• When Cisco Unity is integrated with Cisco CallManager, the primary server begins answering calls as soon as the first voice messaging port on the primary server connected to Cisco CallManager is registered after failback is initiated. All voice messaging ports connected to Cisco CallManager are registered in about 15 seconds.</li> <li>• Calls in progress on the secondary server are not dropped but are maintained until the callers hang up.</li> </ul>
Manual failback, and the primary server is on but inactive	<ul style="list-style-type: none"> <li>• Failback is initiated immediately.</li> <li>• When Cisco Unity is integrated with a circuit-switched phone system, the voice messaging ports on the primary server that are connected to that phone system begin answering calls immediately after failback is initiated.</li> <li>• When Cisco Unity is integrated with a SIP phone system, the voice messaging ports on the primary server that are registered to that phone system begin answering calls immediately after failback is initiated.</li> <li>• When Cisco Unity is integrated with Cisco CallManager, the primary server begins answering calls as soon as the first voice messaging port on the primary server connected to Cisco CallManager is registered after failback is initiated. All voice messaging ports connected to Cisco CallManager are registered in about 15 seconds.</li> <li>• Calls in progress on the secondary server are not dropped but are maintained until the callers hang up.</li> </ul>

Table 4-5 Interval for Failback (continued)

Failback Cause	Time
Failure of the AvCsMgr service on the secondary server, and the primary server is on but inactive	<ul style="list-style-type: none"> <li>• Failback is initiated immediately.</li> <li>• When Cisco Unity is integrated with a circuit-switched phone system, the voice messaging ports on the primary server that are connected to that phone system begin answering calls immediately after failback is initiated.</li> <li>• When Cisco Unity is integrated with a SIP phone system, the voice messaging ports on the primary server that are registered to that phone system begin answering calls immediately after failback is initiated.</li> <li>• When Cisco Unity is integrated with Cisco CallManager, the primary server begins answering calls as soon as the first voice messaging port on the primary server connected to Cisco CallManager is registered after failback is initiated. All voice messaging ports connected to Cisco CallManager are registered in about 15 seconds.</li> <li>• Calls in progress on the secondary server are dropped.</li> </ul>
Failure of the operating system on the secondary server, and the primary server is on but inactive	<ul style="list-style-type: none"> <li>• The primary server initiates failback after waiting for the number of keep-alive events set in the Missed Events Before Failover field in the Failover Monitor. The time required depends on the value of the field and on the value of the Interval (ms) field. The default settings for the fields result in a 30-second delay for the primary server to become active.</li> <li>• When Cisco Unity is integrated with a circuit-switched phone system, the voice messaging ports on the primary server that are connected to that phone system begin answering calls immediately after failback is initiated.</li> <li>• When Cisco Unity is integrated with a SIP phone system, the voice messaging ports on the primary server that are registered to that phone system begin answering calls immediately after failback is initiated.</li> <li>• When Cisco Unity is integrated with Cisco CallManager, the primary server begins answering calls as soon as the first voice messaging port on the primary server connected to Cisco CallManager is registered after failback is initiated. All voice messaging ports connected to Cisco CallManager are registered in about 15 seconds.</li> <li>• Calls in progress on the secondary server are dropped.</li> </ul>

## Causes of Both Servers Becoming Active at the Same Time

Under some circumstances, both the primary server and secondary server can become active at the same time, as indicated in the Failover Monitor. The condition can occur for the following reasons:

- The network connection to the primary server is lost, so both servers become active.

With Cisco CallManager and SIP phone systems, Cisco Unity will receive no calls. However, if the primary server loses its connection to the Cisco CallManager server or the SIP proxy server while the secondary server retains its connection, calls can reach the secondary server and initiate failover.

With circuit-switched phone systems, calls will be answered by both the primary server and the secondary server simultaneously.

- The Node Manager service on the primary server is stopped. The secondary server becomes active, but the components on the primary server remain active and continue to answer calls.

## Effects of Shutting Down and Restarting the Primary and Secondary Servers

When you shut down or restart either the primary or secondary server, the servers behave in the following ways:

- When both servers are running and the active server is shut down, the inactive server becomes active.
- When neither server is running, the first server started becomes the active server.
- When the secondary server is active and configured for automatic failback, and the primary server is also running, the secondary server attempts failback on the failback schedule.

## Licensing Restrictions on Using a Secondary Server Without a Primary Server

To prevent the secondary server from being used as the primary server in another location, the secondary server stops answering calls:

- Four hours after you restart the secondary Cisco Unity server, if you have never run the Configure Cisco Unity Failover wizard.
- Four hours after you restart the secondary Cisco Unity server, if you have run the Configure Cisco Unity Failover wizard but the secondary server has never been able to contact the primary server.
- 60 days after the last time that the secondary server was able to contact the primary server, if the secondary has contacted the primary server at least once. In this case, the only way to make the secondary server start answering calls again is to reconnect the primary server to the network.

There are no licensing restrictions on a primary server, so a primary server will operate without a secondary server. However, without a secondary server, the failover feature cannot work, and an error appears in the Event log whenever you restart the Cisco Unity server. To stop the errors from appearing, disable the Node Manager service (AvCsNodeMgr) in the Services window.





# Exiting and Starting the Cisco Unity Software and Server

---

This appendix contains the following sections:

- [Exiting the Cisco Unity Software, page A-1](#)
- [Shutting Down or Restarting the Cisco Unity Server, page A-3](#)
- [Starting the Cisco Unity Software, page A-3](#)

## Exiting the Cisco Unity Software

This section contains two procedures for exiting the Cisco Unity software: from the Cisco Unity server and from another computer.



**Caution**

Do not use `Kill av*.*` to exit the Cisco Unity software. `Kill av*.*` does not stop all Cisco Unity services.

Do not stop `AvCsMgr` by using the Services window or the Component Services window as a method to exit the Cisco Unity software. Stopping the `AvCsMgr` does not stop all Cisco Unity services and may cause unexpected results.

---

### To Exit the Cisco Unity Software from the Cisco Unity Server

---

- Step 1** If the system uses the automated attendant, route all calls to the operator.
  - Step 2** On the Cisco Unity server, log on to Windows by using either the Cisco Unity administration account or an appropriate Windows domain account.
  - Step 3** Right-click the **Cisco Unity** icon in the status area of the taskbar.  
(If the Cisco Unity icon is not in the taskbar, browse to the **CommServer** directory, and double-click `AvCsTrayStatus.exe`.)
  - Step 4** Click **Stop Cisco Unity**. Cisco Unity stops running when all calls are finished, and an “X” appears in the Cisco Unity icon.
  - Step 5** Press **Ctrl-Alt-Delete**, then lock or log off of Windows to prevent access by unauthorized users.
-

### To Exit the Cisco Unity Software from Another Computer

---

- Step 1** If the system uses the automated attendant, route all calls to the operator.
- Step 2** If the Cisco Unity Status Monitor does not use Integrated Windows authentication, skip to [Step 3](#).  
When the Cisco Unity Status Monitor uses Integrated Windows authentication, do the following substeps to access the Status Monitor:
- Log on to Windows by using either the Cisco Unity administration account or an appropriate Windows domain account.
  - Start Internet Explorer, and go to **http://<Cisco Unity server name>/status**.
  - If Internet Explorer prompts you for a user name and password, enter the user name, password, and domain for the administration account or the Windows domain account.
  - Skip to [Step 6](#).
- Step 3** When the Cisco Unity Status Monitor uses Anonymous authentication, do the following substeps to access the Status Monitor:
- Log on to Windows by using any domain account that has the right to log on locally.
  - Start Internet Explorer, and go to **http://<Cisco Unity server name>/status**.
- Step 4** On the Cisco Unity Log On Page, do one of the following:
- Enter the full name and Internet password of a Domino account that is associated with an appropriate Cisco Unity subscriber account, and click **Log On**, then skip to [Step 6](#).
  - Click **Log On Using Windows Authentication**.
- Step 5** On the Cisco Unity Log On page, enter the user name, password, and domain for the Cisco Unity administration account or the Windows domain account, and click **Log On**.
- Step 6** In the Cisco Unity Status Monitor, under Shutting Down Cisco Unity, choose a method:
- Cisco Unity stops running after all calls are finished.
  - Cisco Unity interrupts calls in progress with a voice message, disconnects all calls, then stops running.
- Step 7** Click **Shut Down**.
-

# Shutting Down or Restarting the Cisco Unity Server

If the Cisco Unity system has an expansion chassis or is set up for failover, note the following considerations before shutting down or restarting the Cisco Unity server:

<b>Expansion chassis connected to the Cisco Unity server</b>	When both the expansion chassis and the Cisco Unity server are turned off, turn on the expansion chassis before you turn on the server. Otherwise, the server may not detect the voice cards in the expansion chassis.
<b>Cisco Unity failover</b>	<ul style="list-style-type: none"> <li>• When both servers are running and the active server is shut down, the inactive server becomes active.</li> <li>• When neither server is running, the first server started becomes the active server.</li> <li>• When the secondary server is active and configured for automatic failback, and the primary server is also running, the secondary server attempts failback on the failback schedule.</li> </ul>

## To Shut Down or Restart the Cisco Unity Server

- 
- Step 1** Exit the Cisco Unity software, if it is running, by using one of the procedures in the [“Exiting the Cisco Unity Software”](#) section on page A-1.
- Step 2** On the Windows Start menu, click **Shut Down**.
- Step 3** Click **Shut Down** or **Restart**. During a restart, the Cisco Unity software starts automatically.
- When Cisco Unity starts successfully, three tones play and a check mark appears in the Cisco Unity icon in the status area of the taskbar.
- When Cisco Unity does not start successfully, two tones play and an “X” appears in the Cisco Unity icon in the status area of the taskbar.
- 

# Starting the Cisco Unity Software

This section contains two procedures for starting the Cisco Unity software: from the Cisco Unity server and from another computer.

Cisco Unity is a Windows service that is configured to start automatically when you turn on or restart the server. Do one of the procedures in this section only if you exited the Cisco Unity software and did not restart the server.

Domino must be running on the server that Cisco Unity connects with before you start the Cisco Unity software.

If Domino stops for any reason while Cisco Unity is running, Cisco Unity will continue to take messages.

### To Start the Cisco Unity Software from the Cisco Unity Server

---

- Step 1** On the Cisco Unity server, log on to Windows by using either the Cisco Unity administration account or an appropriate Windows domain account.
- Step 2** Right-click the **Cisco Unity** icon in the status area of the taskbar.  
(If the Cisco Unity icon is not in the taskbar, browse to the **CommServer** directory, and double-click **AvCsTrayStatus.exe**.)
- Step 3** Click **Start Cisco Unity**.  
When Cisco Unity starts successfully, three tones play and a check mark appears in the Cisco Unity icon.  
When Cisco Unity does not start successfully, two tones play and an “X” appears in the Cisco Unity icon.
- Step 4** Press **Ctrl-Alt-Delete**, then lock or log off of Windows to prevent access by unauthorized users.
- Step 5** If the system uses the automated attendant and you routed calls to the operator before you exited the Cisco Unity software, reroute calls to Cisco Unity.
- 

### To Start the Cisco Unity Software from Another Computer

---

- Step 1** If the Cisco Unity Status Monitor does not use Integrated Windows authentication, skip to [Step 2](#).  
When the Cisco Unity Status Monitor uses Integrated Windows authentication, do the following substeps to access the Status Monitor:
- a. Log on to Windows by using either the Cisco Unity administration account or an appropriate Windows domain account.
  - b. Start Internet Explorer, and go to **http://<Cisco Unity server name>/status**.
  - c. If Internet Explorer prompts you for a user name and password, enter the user name, password, and domain for the Cisco Unity administration account or the Windows domain account.
  - d. Skip to [Step 5](#).
- Step 2** When the Cisco Unity Status Monitor uses Anonymous authentication, do the following substeps to access the Status Monitor:
- a. Log on to Windows by using any domain account that has the right to log on locally.
  - b. Start Internet Explorer, and go to **http://<Cisco Unity server name>/status**.
- Step 3** On the Cisco Unity Log On Page, do one of the following:
- Enter the full name and Internet password of a Domino account that is associated with an appropriate Cisco Unity subscriber account, and click **Log On**, then skip to [Step 5](#).
  - Click **Log On Using Windows Authentication**.
- Step 4** On the Cisco Unity Log On page, enter the user name, password, and domain for the Cisco Unity administration account or the Windows domain account, and click **Log On**.
- Step 5** In the Cisco Unity Status Monitor, click the **System Status** icon (the first icon), at the top of the page.

- Step 6** Click **Start**.
- Step 7** If the system uses the automated attendant and you routed calls to the operator before you exited the Cisco Unity software, reroute calls to Cisco Unity.
-





## Line Connections Between the Phone System and the Cisco Unity Servers

---

This appendix describes the line connections between a circuit-switched phone system and the voice cards on the primary and secondary Cisco Unity servers.



### Note

For connections involving Cisco CallManager or SIP proxy servers, refer to the applicable Cisco Unity integration guide.

Integrations using PIMG units are not supported with Cisco Unity failover.

---

This appendix contains the following sections:

- [Analog Voice Line Connections for Failover, page B-1](#)
- [Serial Data Cable Connections for Failover, page B-6](#)

## Analog Voice Line Connections for Failover

Circuit-switched phone systems typically have 25-pair or 32-pair cables to provide analog voice connections. It is common that the cable is broken into individual lines that may attach to a punchdown cross-connect block (for example, 66-Type), or the cable may terminate with RJ-11 or RJ-14 connectors to accept analog voice lines.

A punchdown cross-connect block or line splitters may be used to split the analog lines. It is possible to use these devices in combination to manage and split the lines.



### Note

No devices other than those described in this appendix should be connected to the analog voice lines for any voice messaging port. Otherwise, the ring equivalency number (REN) may be exceeded and the primary and secondary servers may not receive sufficient ring current to answer calls.

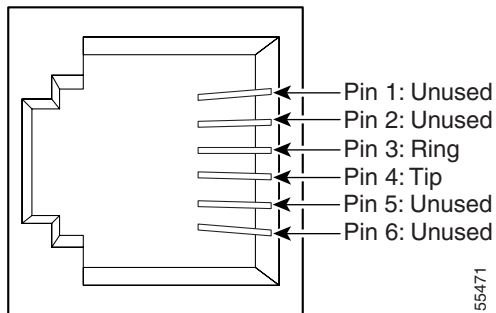
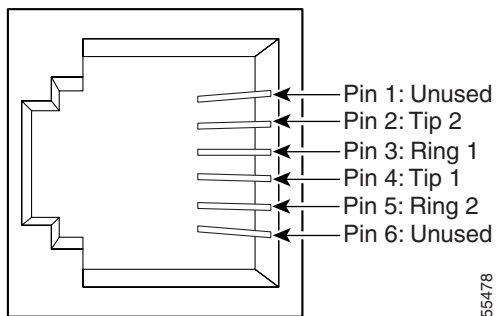
---

## Requirements

The following components are required for common configurations:

- Two or three analog voice patch cables for each port on the phone system.

- The appropriate device to split the analog lines:
  - One or more punchdown cross-connect blocks (for example, 66-Type), installed and ready to accept lines.
  - One line splitter for every one or two ports on the phone system. The line splitter accepts both RJ-11 and RJ-14 connectors.
- The appropriate connectors (RJ-11 and/or RJ-14) for the analog voice lines. [Figure B-1](#) shows the pinout for the RJ-11 connector, and [Figure B-2](#) shows the pinout for the RJ-14 connector.

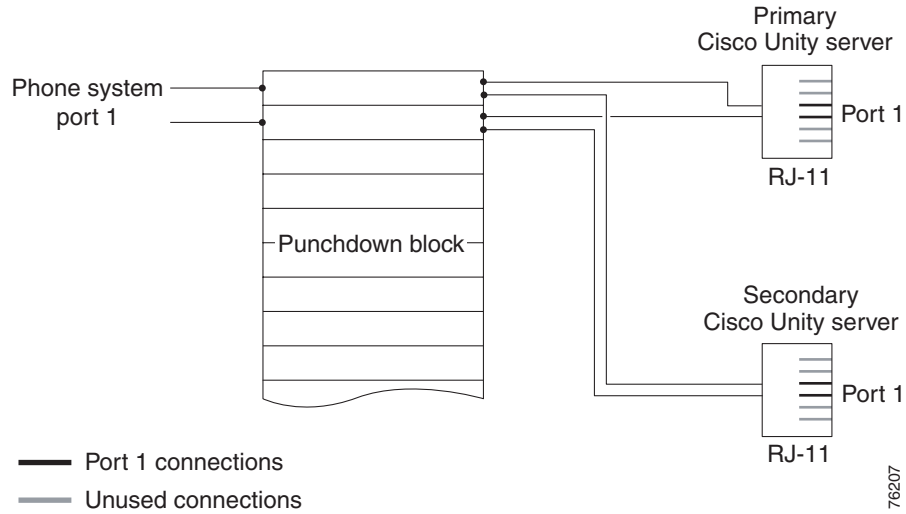
**Figure B-1 RJ-11 Connector Pinout****Figure B-2 RJ-14 Connector Pinout**

## Connections with D/41-Series Voice Cards

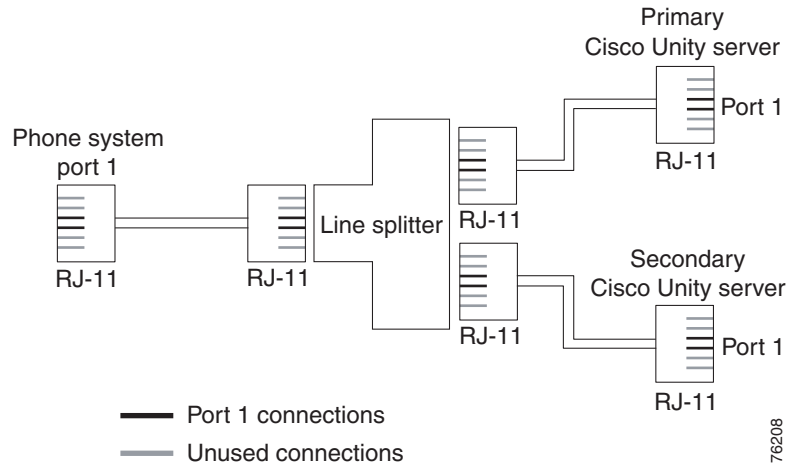
The following figures illustrate common configurations:

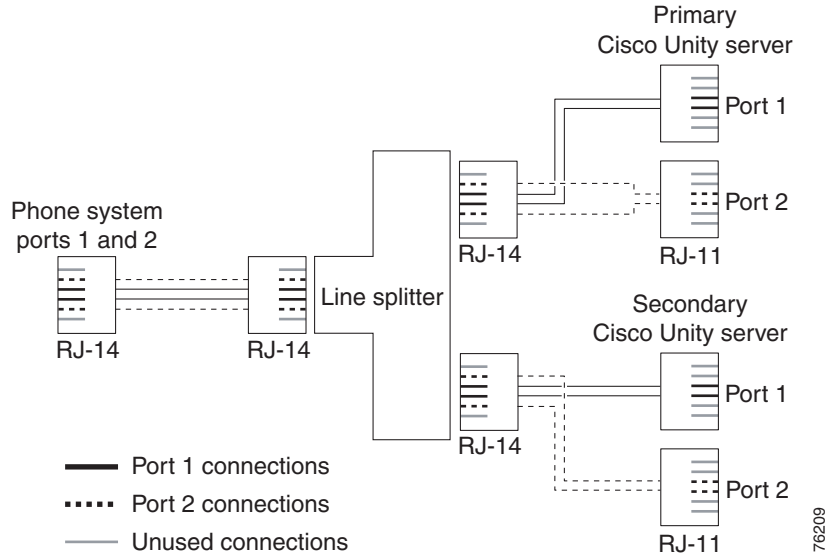
- [Figure B-3](#) shows the connections between a phone system and the voice cards on the primary and secondary servers, through a punchdown cross-connect block.
- [Figure B-4](#) shows the connections between a phone system with an RJ-11 connector and the D/41-series voice cards on the primary and secondary servers.
- [Figure B-5](#) shows the connections between a phone system with an RJ-14 connector and the D/41-series voice cards on the primary and secondary servers.

**Figure B-3** Connections from the Phone System Through a Punchdown Block to D/41-Series Voice Cards



**Figure B-4** Connections for an RJ-11 Connector from the Phone System to D/41-Series Voice Cards



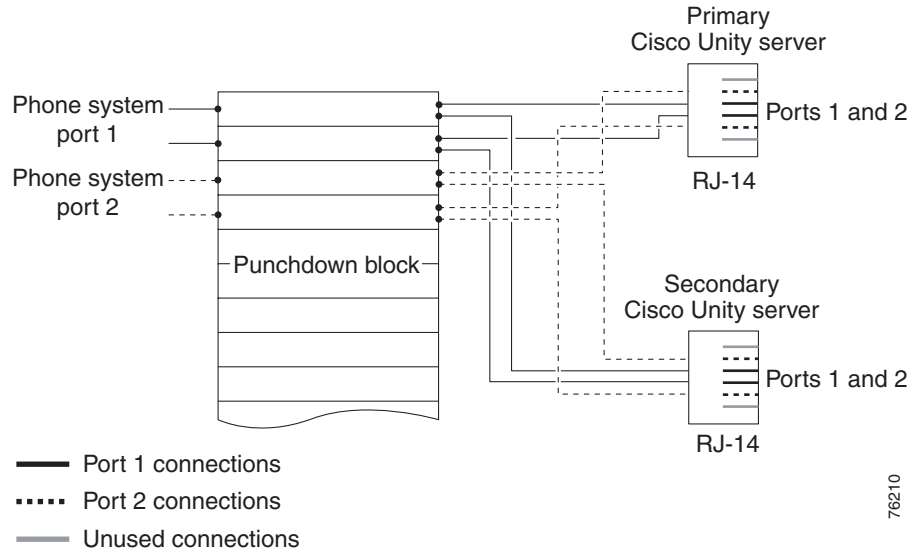
**Figure B-5** Connections from an RJ-14 Connector on the Phone System to D/41-Series Voice Cards

## Connections with D/120-Series Voice Cards

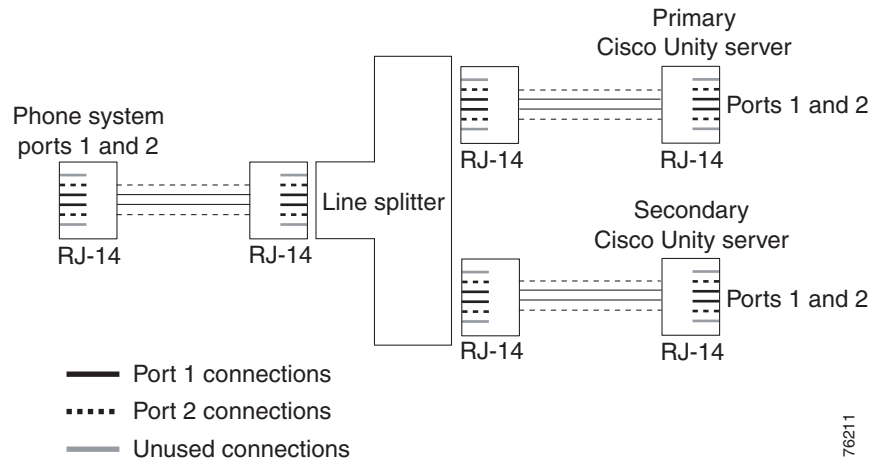
The following figures illustrate common configurations:

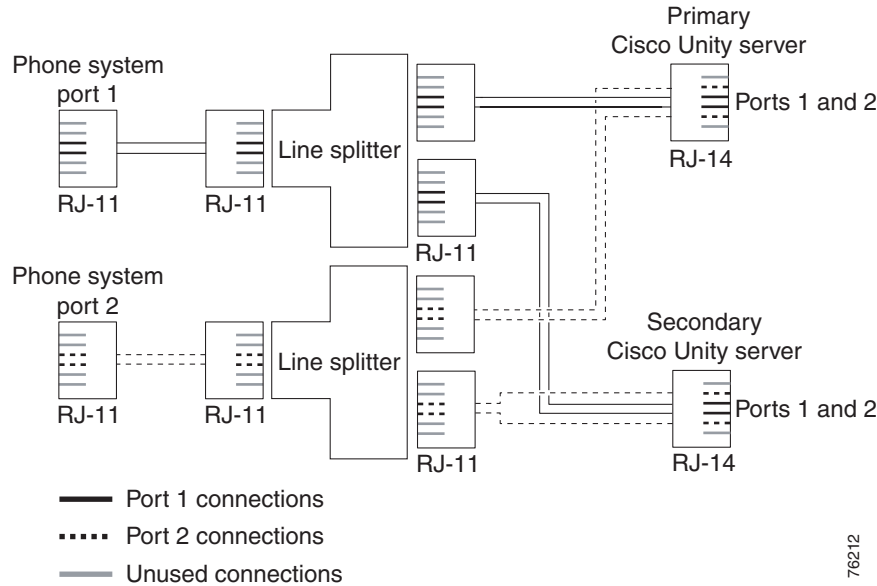
- [Figure B-6](#) shows the connections between a phone system and the voice cards on the primary and secondary servers, through a punchdown cross-connect block.
- [Figure B-7](#) shows the connections between a phone system with an RJ-14 connector and the D/120-series voice cards on the primary and secondary servers.
- [Figure B-8](#) shows the connections between a phone system with an RJ-11 connector and the D/120-series voice cards on the primary and secondary servers.

**Figure B-6** Connections from the Phone System Through a Punchdown Block to D/120-Series Voice Cards



**Figure B-7** Connections for an RJ-14 Connector from the Phone System to D/120-Series Voice Cards



**Figure B-8** Connections for an RJ-11 Connector from the Phone System to D/120-Series Voice Cards

76212

## Serial Data Cable Connections for Failover

Only serial integrations (for example, SMDI, MCI, or PBXLink) use RS-232 serial data cables.

Connecting RS-232 serial cables between a circuit-switched phone system and the primary and secondary Cisco Unity servers varies depending on the number of serial ports the phone system has.

### Requirements

The following components are required for phone systems with only one serial port:

- Three RS-232 serial cables
- Data splitter unit

The following components are required for phone systems with multiple serial ports:

- Two RS-232 serial cables

### Pinouts for the Serial Data Cables

The pinouts for the serial cables depend on whether the serial port on the phone system acts as data circuit-terminating equipment (DCE—it does not originate signals but acts as a modem) or as data terminal equipment (DTE—it originates signals).

## Serial Cables Between the Phone System and the Data Splitter

If the serial port on the phone system acts as DCE, use an RS-232 serial cable with the pinout shown in [Table B-1](#) for the data link between the phone system and the data splitter. The cable creates a DCE-to-DTE connection.

**Table B-1** Pinout for Phone System Serial Port Acting as DCE

Pin to the Data Splitter	Serial Port Pin Definition from the Phone System
1	DCD (data carrier detect)
2	RX (transmit)
3	TX (receive)
4	DTR (data terminal ready)
5	GND (signal ground)
6	DSR (data set ready)
7	RTS (request to send)
8	CTS (clear to send)
9	(no connection)

If the serial port on the phone system acts as DTE, use a null modem serial cable with the pinout shown in [Table B-2](#) for the data link between the phone system and the data splitter. The cable creates a DTE-to-DTE connection.

**Table B-2** Pinout for Phone System Serial Port Acting as DTE

Pin to the Data Splitter	Serial Port Pin Definition from the Phone System
1	RTS (request to send)
1	CTS (clear to send)
2	TX (transmit)
3	RX (receive)
4	DSR (data set ready)
5	GND (signal ground)
6	DTR (data terminal ready)
7	DCD (data carrier detect)
8	DCD (data carrier detect)
9	(no connection)

Phone systems with multiple serial ports use the applicable pinout for the two serial cables connecting the phone system to the Cisco Unity servers.

## Serial Cables Between the Data Splitter and the Cisco Unity Servers

The two serial cables between the data splitter and the primary and secondary Cisco Unity servers use wiring as shown in [Table B-3](#).

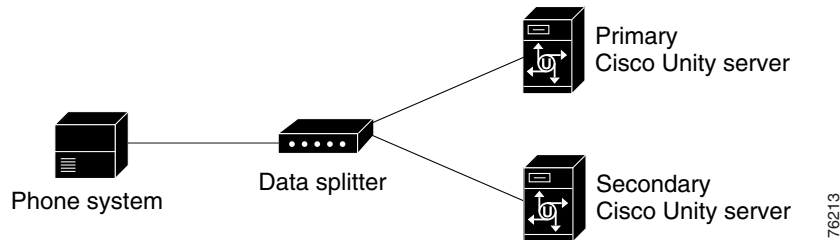
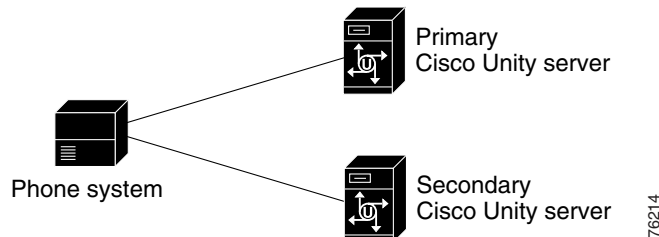
**Table B-3** Serial Cable Wiring Between the Data Splitter and the Cisco Unity Servers

Pin from the Data Splitter	Pin to the Cisco Unity Server
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9

## Connections for the Serial Data Cables

Figure B-9 shows the connections between the serial port on a phone system that has only one serial port to the serial ports on the primary and secondary Cisco Unity servers. Figure B-10 shows the connections between the serial ports on a phone system that has two serial ports to the serial ports on the Cisco Unity servers.

Note that the following figures do not show the analog voice lines, which are described in the “[Analog Voice Line Connections for Failover](#)” section on page B-1.

**Figure B-9** Serial Cable Connections from a Single Serial Port on the Phone System to the Serial Ports on the Cisco Unity Servers**Figure B-10** Serial Cable Connections from Multiple Serial Ports on the Phone System to the Serial Ports on the Cisco Unity Servers



# Behavior of Cisco Unity Failover During Outages of Network Components

---

This appendix contains the following sections:

- [Introduction, page C-1](#)
- [Outage Scenarios for Networks of Windows 2000 and IBM Lotus Domino, page C-1](#)

## Introduction

The second section in this appendix describes how the primary and secondary servers behave when the components that Cisco Unity uses over the network are disconnected (for example, due to a partial or complete network outage).

The scenarios described cover the range of probable component or network outages. Each scenario assumes the following before the outage occurs:

- Cisco Unity is running on both the primary and secondary servers.
- The primary server is active, and the secondary server is inactive.
- The phone system that Cisco Unity connects to is Cisco CallManager.

Except when Cisco Unity is shut down, all Cisco Unity services continue to run, though the functionality of certain services are affected by the outages.

## Outage Scenarios for Networks of Windows 2000 and IBM Lotus Domino

This section contains the following scenarios:

- [The Primary Server Is Disconnected from the Network, Then Reconnected, page C-2](#)
- [The Secondary Server Is Disconnected from the Network, Then Reconnected, page C-3](#)
- [The Primary and Secondary Servers Are Simultaneously Disconnected from the Network, Then the Primary Server Is Reconnected First, page C-4](#)
- [The Primary and Secondary Servers Are Simultaneously Disconnected from the Network, Then the Secondary Server Is Reconnected First, page C-5](#)

- [The Primary and Secondary Servers Are Simultaneously Disconnected from the Network, Then Both Servers Are Simultaneously Reconnected, page C-6](#)
- [The Publisher Cisco CallManager Server Is Disconnected from the Network, Then Reconnected, page C-7](#)
- [The Subscriber Cisco CallManager Server Is Disconnected from the Network, Then Reconnected, page C-8](#)
- [The Cisco CallManager Cluster Is Disconnected from the Network, Then Reconnected, page C-8](#)
- [The Primary Server Crashes, page C-9](#)
- [The Secondary Server Crashes, page C-10](#)
- [The Primary and Secondary Servers Crash Simultaneously, page C-10](#)
- [The Primary Server Is Disconnected from the Network, Then the Domino Server Is Disconnected from the Network, page C-11](#)

## The Primary Server Is Disconnected from the Network, Then Reconnected

In testing, this scenario was simulated by disabling the network interface card on the primary server.

### Disconnection Behavior

- The secondary server answers all calls.
- Subscribers are able to leave and listen to messages. External callers can leave messages for subscribers.
- All voice messaging ports on the primary server unregister with the Cisco CallManager server.
- The Node Manager services (AvCsNodeMgr) on the primary and secondary servers no longer receive status from each other.
- The Failover Monitor on the primary server shows that the primary server is active. The Failover Monitor on the secondary server shows that the secondary server is active.
- Messages, greetings, and other recordings made on the primary server but not replicated to the secondary server before the network outage are not available on the secondary server.
- UnityDb database replication between the primary and secondary servers stops.
- The secondary server handles directory synchronization, MWIs, event notification, and message notification.

### Reconnection Behavior

- The primary server becomes active, and the secondary server becomes inactive.
- All voice messaging ports on the primary server register with the Cisco CallManager server.
- The primary server answers all calls.
- Subscribers are able to leave and listen to messages. External callers can leave messages for subscribers.
- The Node Manager services (AvCsNodeMgr) on the primary and secondary servers send status to and receive status from each other.
- The Failover Monitors on the primary and secondary servers show that the primary server is active.
- Changes to the UnityDb database that occurred while the primary server was offline are replicated from the secondary server to the primary server.

- The primary server handles directory synchronization, MWIs, event notification, and message notification.
- Messages, greetings, and other recordings made on the primary server but not replicated to the secondary server before the network outage are replicated to the secondary server.
- Messages, greetings, and other recordings made on the secondary server during the network outage are replicated to the primary server.

## The Secondary Server Is Disconnected from the Network, Then Reconnected

In testing, this scenario was simulated by disabling the network interface card on the secondary server.

### Disconnection Behavior

- The primary server continues answering all calls.
- Subscribers are able to leave and listen to messages. External callers can leave messages for subscribers.
- All voice messaging ports on the secondary server unregister with the Cisco CallManager server.
- The Node Manager services (AvCsNodeMgr) on the primary and secondary servers no longer receive status from each other.
- The Failover Monitor on the primary server shows that the primary server is active. The Failover Monitor on the secondary server shows that the secondary server is active.
- UnityDb database replication between the primary and secondary servers stops.
- The primary server handles directory synchronization, MWIs, event notification, and message notification.

### Reconnection Behavior

- The primary server remains active, and the secondary server becomes inactive.
- The primary server continues answering all calls.
- Subscribers are able to leave and listen to messages. External callers can leave messages for subscribers.
- All voice messaging ports on the secondary server register with the Cisco CallManager server.
- The Node Manager services (AvCsNodeMgr) on the primary and secondary servers send status to and receive status from each other.
- The Failover Monitors on the primary and secondary servers show that the primary server is active.
- Changes to the UnityDb database that occurred while the secondary server was offline are replicated from the primary server to the secondary server.
- The primary server continues handling directory synchronization, MWIs, event notification, and message notification.
- Messages, greetings, and other recordings made on the primary server but not replicated to the secondary server before the network outage are replicated to the secondary server.
- Messages, greetings, and other recordings made on the primary server during the network outage are replicated to the secondary server.

## The Primary and Secondary Servers Are Simultaneously Disconnected from the Network, Then the Primary Server Is Reconnected First

In testing, this scenario was simulated by disabling the network interface card on the primary and secondary servers at the same time.

### Disconnection Behavior

- There is no voice messaging functionality. Neither the primary nor secondary server answers calls.
- Subscribers are not able to leave or listen to messages. External callers cannot leave messages for subscribers.
- Callers trying to leave messages hear a fast busy tone instead of the personal greeting for the subscriber.
- All voice messaging ports on the primary and secondary servers unregister with the Cisco CallManager server.
- The Node Manager services (AvCsNodeMgr) on the primary and secondary servers no longer receive status from each other.
- The Failover Monitor on the primary server shows that the primary server is active. The Failover Monitor on the secondary server shows that the secondary server is active.
- Subscribers can call other subscribers directly and talk to each other.
- UnityDb database replication between the primary and secondary servers stops.
- Neither server initiates directory synchronization, MWIs, event notification, or message notification.

### Reconnection Behavior (Only the Primary Server Is Reconnected)

- The Failover Monitor on the primary server shows that the primary server is active. The Failover Monitor on the secondary server shows that the secondary server is active.
- All voice messaging ports on the primary server register with the Cisco CallManager server.
- The primary server answers all calls.
- Subscribers are able to leave and listen to messages. External callers can leave messages for subscribers.
- Messages, greetings, and other recordings made on the primary server but not replicated to the secondary server before the network outage are not replicated to the secondary server because it is offline.
- Changes to the UnityDb database that occurred before the network outage and were not replicated to the secondary server are not replicated because the secondary server is offline.
- The primary server handles directory synchronization, MWIs, event notification, and message notification.

### Reconnection Behavior (the Secondary Server Is Also Reconnected)

- The Failover Monitors on the primary and secondary servers show that the primary server is active and the secondary server is inactive.
- All voice messaging ports on the secondary server register with the Cisco CallManager server.
- The primary server continues answering all calls.

- The Node Manager services (AvCsNodeMgr) on the primary and secondary servers send status to and receive status from each other.
- Changes to the UnityDb database that occurred while the secondary server was offline are replicated from the primary server to the secondary server.
- The primary server continues handling directory synchronization, MWIs, event notification, and message notification.
- Messages, greetings, and other recordings made on the primary server but not replicated to the secondary server before the network outage are replicated to the secondary server.
- Messages, greetings, and other recordings made on the primary server while the secondary server was offline are replicated to the secondary server.

## The Primary and Secondary Servers Are Simultaneously Disconnected from the Network, Then the Secondary Server Is Reconnected First

In testing, this scenario was simulated by disabling the network interface card on the primary and secondary servers at the same time.

### Disconnection Behavior

- There is no voice messaging functionality. Neither the primary nor secondary server answers calls.
- Subscribers are not able to leave or listen to messages. External callers cannot leave messages for subscribers.
- Callers trying to leave messages hear a fast busy tone instead of the personal greeting for the subscriber.
- All voice messaging ports on the primary and secondary servers unregister with the Cisco CallManager server.
- The Node Manager services (AvCsNodeMgr) on the primary and secondary servers no longer receive status from each other.
- The Failover Monitor on the primary server shows that the primary server is active. The Failover Monitor on the secondary server shows that the secondary server is active.
- Subscribers can call other subscribers directly and talk to each other.
- UnityDb database replication between the primary and secondary servers stops.
- Neither server initiates directory synchronization, MWIs, event notification, or message notification.

### Reconnection Behavior (Only the Secondary Server Is Reconnected)

- The Failover Monitor on the primary server shows that the primary server is active. The Failover Monitor on the secondary server shows that the secondary server is active.
- All voice messaging ports on the secondary server register with the Cisco CallManager server.
- The secondary server answers all calls.
- Subscribers are able to leave and listen to messages. External callers can leave messages for subscribers.
- Messages, greetings, and other recordings made on the primary server but not replicated to the secondary server before the network outage are not replicated to the secondary server because the primary server is offline.

- Messages, greetings, and other recordings made on the secondary server during the network outage are not replicated to the primary server because the primary server is offline.
- Changes to the UnityDb database that occurred before the network outage and were not replicated to the secondary server are not replicated because the primary server is offline.
- The secondary server handles directory synchronization, MWIs, event notification, and message notification.

#### **Reconnection Behavior (the Primary Server Is Also Reconnected)**

- The primary server becomes active and the secondary server becomes inactive.
- All voice messaging ports on the primary server register with the Cisco CallManager server.
- The primary server answers all calls.
- The Node Manager services (AvCsNodeMgr) on the primary and secondary servers send status to and receive status from each other.
- The Failover Monitors on the primary and secondary servers show that the primary server is active and the secondary server is inactive.
- Changes to the UnityDb database that occurred while the primary server was offline are replicated from the secondary server to the primary server.
- The primary server handles directory synchronization, MWIs, event notification, and message notification.
- Messages, greetings, and other recordings made on the primary server but not replicated to the secondary server before the network outage are replicated to the secondary server.
- Messages, greetings, and other recordings made on the secondary server while the primary server was offline are replicated to the primary server.

## **The Primary and Secondary Servers Are Simultaneously Disconnected from the Network, Then Both Servers Are Simultaneously Reconnected**

In testing, this scenario was simulated by disabling the network interface card on the primary and secondary servers at the same time.

#### **Disconnection Behavior**

- There is no voice messaging functionality. Neither the primary nor secondary server answers calls.
- Subscribers are not able to leave or listen to messages. External callers cannot leave messages for subscribers.
- Callers trying to leave messages hear a fast busy tone instead of the personal greeting for the subscriber.
- All voice messaging ports on the primary and secondary servers unregister with the Cisco CallManager server.
- The Node Manager services (AvCsNodeMgr) on the primary and secondary servers no longer receive status from each other.
- The Failover Monitor on the primary server shows that the primary server is active. The Failover Monitor on the secondary server shows that the secondary server is active.
- Subscribers can call other subscribers directly and talk to each other.

- UnityDb database replication between the primary and secondary servers stops.
- Neither server initiates directory synchronization, MWIs, event notification, or message notification.

**Reconnection Behavior**

- The primary server remains active, and the secondary server becomes inactive.
- All voice messaging ports on the primary and secondary servers register with the Cisco CallManager server.
- The primary server answers all calls.
- Subscribers are able to leave and listen to messages. External callers can leave messages for subscribers.
- The Node Manager services (AvCsNodeMgr) on the primary and secondary servers send status to and receive status from each other.
- The Failover Monitors on the primary and secondary servers show that the primary server is active.
- The primary server handles directory synchronization, MWIs, event notification, and message notification.
- Messages, greetings, and other recordings made on the primary server but not replicated to the secondary server before the network outage are replicated to the secondary server.

## The Publisher Cisco CallManager Server Is Disconnected from the Network, Then Reconnected

In testing, this scenario was simulated by disabling the network interface card on the publisher (primary) Cisco CallManager server.

**Disconnection Behavior**

- The primary Cisco Unity server continues to be active, and the secondary Cisco Unity server continues to be inactive.
- All voice messaging ports on the primary and secondary servers unregister with the publisher (primary) Cisco CallManager server and register with the subscriber (secondary) Cisco CallManager server.
- The primary Cisco Unity server continues answering all calls.

**Reconnection Behavior**

- The primary Cisco Unity server continues to be active, and the secondary Cisco Unity server continues to be inactive.
- If registering automatically with the publisher (primary) Cisco CallManager server is enabled, all voice messaging ports on the primary and secondary servers unregister with the subscriber (secondary) Cisco CallManager server and register with the publisher (primary) Cisco CallManager server.
- If registering automatically with the publisher (primary) Cisco CallManager server is not enabled, all voice messaging ports on the primary and secondary servers remain registered with the subscriber (secondary) Cisco CallManager server.
- The primary Cisco Unity server continues answering all calls.

## The Subscriber Cisco CallManager Server Is Disconnected from the Network, Then Reconnected

In testing, this scenario was simulated by disabling the network interface card on the subscriber (secondary) Cisco CallManager server.

### Disconnection Behavior

- The primary Cisco Unity server continues to be active, and the secondary Cisco Unity server continues to be inactive.
- All voice messaging ports on the primary and secondary Cisco Unity servers remain registered with the publisher (primary) Cisco CallManager server.
- The primary Cisco Unity server continues answering all calls.

### Reconnection Behavior

- The primary Cisco Unity server continues to be active, and the secondary Cisco Unity server continues to be inactive.
- All voice messaging ports on the primary and secondary Cisco Unity servers remain registered with the publisher (primary) Cisco CallManager server.
- The primary Cisco Unity server continues answering all calls.

## The Cisco CallManager Cluster Is Disconnected from the Network, Then Reconnected

In testing, this scenario was simulated by disabling the network interface card on all Cisco CallManager servers in the cluster.

### Disconnection Behavior

- The primary Cisco Unity server continues to be active, and the secondary Cisco Unity server continues to be inactive.
- All voice messaging ports on the primary and secondary Cisco Unity servers unregister with the publisher (primary) Cisco CallManager server. They do not register with another Cisco CallManager server.
- Cisco Unity does not answer calls.
- Subscribers are not able to leave or listen to messages. External callers cannot leave messages for subscribers because phones will not forward calls to Cisco Unity.
- Subscribers calling Cisco Unity hear a fast busy tone.
- Subscribers on a Cisco Unity connected to another Cisco CallManager cluster can leave messages for subscribers of the disconnected cluster.

### Reconnection Behavior

- The primary Cisco Unity server continues to be active, and the secondary Cisco Unity server continues to be inactive.
- All voice messaging ports on the primary and secondary Cisco Unity servers register with the publisher (primary) Cisco CallManager server.

- The primary Cisco Unity server answers all calls.

## The Primary Server Crashes

In testing, this scenario was simulated by turning off power to the primary server.

### Disconnection Behavior

- The secondary server answers all calls. Depending on network latency, this behavior may take a few minutes to begin.
- The Failover Monitor on the secondary server shows that the secondary server is active.
- Subscribers are able to leave and listen to messages. External callers can leave messages for subscribers.
- Messages, greetings, and other recordings made on the primary server but not replicated to the secondary server before the network outage are not available on the secondary server.
- The secondary server handles directory synchronization, MWIs, event notification, and message notification.

### Reconnection Behavior Before Failback

- The primary server is inactive, and the secondary server remains active.
- The secondary server answers all calls.
- All voice messaging ports on the primary server remain unregistered with the Cisco CallManager server.

### Reconnection Behavior After Failback

- When failback is manually initiated or when a scheduled failback occurs, the primary server becomes active and the secondary server becomes inactive.
- All voice messaging ports on the primary server register with the Cisco CallManager server.
- The primary server answers all calls.
- Subscribers are able to leave and listen to messages. External callers can leave messages for subscribers.
- The Node Manager services (AvCsNodeMgr) on the primary and secondary servers send status to and receive status from each other.
- The Failover Monitors on the primary and secondary servers show that the primary server is active.
- Changes to the UnityDb database that occurred while the primary server was offline are replicated from the secondary server to the primary server.
- The primary server handles directory synchronization, MWIs, event notification, and message notification.
- Messages, greetings, and other recordings made on the primary server but not replicated to the secondary server before the server outage are replicated to the secondary server.
- Messages, greetings, and other recordings made on the secondary server during the server outage are replicated to the primary server.

## The Secondary Server Crashes

In testing, this scenario was simulated by turning off power to the secondary server.

### Disconnection Behavior

- The primary server continues answering all calls.
- Subscribers are able to leave and listen to messages. External callers can leave messages for subscribers.
- The Failover Monitor on the primary server shows that the primary server is active.
- UnityDb database replication between the primary and secondary servers stops.
- The primary server handles directory synchronization, MWIs, event notification, and message notification.

### Reconnection Behavior

- The primary server remains active, and the secondary server becomes inactive.
- The primary server continues answering all calls.
- Subscribers are able to leave and listen to messages. External callers can leave messages for subscribers.
- All voice messaging ports on the secondary server register with the Cisco CallManager server.
- The Node Manager services (AvCsNodeMgr) on the primary and secondary servers send status to and receive status from each other.
- The Failover Monitors on the primary and secondary servers show that the primary server is active.
- Changes to the UnityDb database that occurred while the secondary server was offline are replicated from the primary server to the secondary server.
- The primary server continues handling directory synchronization, MWIs, event notification, and message notification.
- Messages, greetings, and other recordings made on the primary server but not replicated to the secondary server before the server outage are replicated to the secondary server.
- Messages, greetings, and other recordings made on the primary server during the server outage are replicated to the secondary server.

## The Primary and Secondary Servers Crash Simultaneously

In testing, this scenario was simulated by turning off power to the primary and secondary servers at the same time.

### Disconnection Behavior

- There is no voice messaging functionality. Neither the primary nor secondary server answers calls.
- Subscribers are not able to leave or listen to messages. External callers cannot leave messages for subscribers.
- Callers trying to leave messages hear a fast busy tone instead of the personal greeting for the subscriber.
- Subscribers can call other subscribers directly and talk to each other.

- Neither server initiates directory synchronization, MWIs, event notification, or message notification.

**Reconnection Behavior (Only the Primary Server Is Reconnected)**

- The Failover Monitor on the primary server shows that the primary server is active.
- All voice messaging ports on the primary server register with the Cisco CallManager server.
- The primary server answers all calls.
- Subscribers are able to leave and listen to messages. External callers can leave messages for subscribers.
- Messages, greetings, and other recordings made on the primary server but not replicated to the secondary server before the server outage are not replicated to the secondary server because the secondary server is offline.
- Changes to the UnityDb database that occurred before the server outage and were not replicated to the secondary server are not replicated because the secondary server is offline.
- The primary server handles directory synchronization, MWIs, event notification, and message notification.

**Reconnection Behavior (the Secondary Server Is Also Reconnected)**

- The Failover Monitors on the primary and secondary servers show that the primary server is active and the secondary server is inactive.
- All voice messaging ports on the secondary server register with the Cisco CallManager server.
- The primary server continues answering all calls.
- The Node Manager services (AvCsNodeMgr) on the primary and secondary servers send status to and receive status from each other.
- Changes to the UnityDb database that occurred while the secondary server was offline are replicated from the primary server to the secondary server.
- The primary server continues handling directory synchronization, MWIs, event notification, and message notification.
- Messages, greetings, and other recordings made on the primary server but not replicated to the secondary server before the server outage are replicated to the secondary server.
- Messages, greetings, and other recordings made on the primary server while the secondary server was offline are replicated to the secondary server.

## The Primary Server Is Disconnected from the Network, Then the Domino Server Is Disconnected from the Network

In testing, this scenario was simulated by disabling the network interface card on the primary server, then on the Domino server.

**Disconnection Behavior (Only the Primary Server Is Disconnected)**

- The secondary server answers all calls.
- Subscribers are able to leave and listen to messages. External callers can leave messages for subscribers.
- All voice messaging ports on the primary server unregister with the Cisco CallManager server.

- The Node Manager services (AvCsNodeMgr) on the primary and secondary servers no longer receive status from each other.
- The Failover Monitor on the primary server shows that the primary server is active. The Failover Monitor on the secondary server shows that the secondary server is active.
- Messages, greetings, and other recordings made on the primary server but not replicated to the secondary server before the network outage are not available on the secondary server.
- UnityDb database replication between the primary and secondary servers stops.
- The secondary server handles directory synchronization, MWIs, event notification, and message notification.

#### **Disconnection Behavior (the Domino Server Is Also Disconnected)**

- All subscribers hear the Unity Messaging Repository (UMR) conversation when they log on to Cisco Unity.
- External callers can leave messages for subscribers. The new messages are stored in the UnityMTA folder on the secondary server.
- Subscribers homed on a different Cisco Unity server can leave messages for subscribers on another Cisco Unity server by calling the Cisco Unity server. The new messages are stored in the UnityMTA folder on the secondary server.
- Subscribers can call the Cisco Unity server and listen to their new messages stored in the UnityMTA folder on the secondary server. Messages stored on the Domino server before the network outage are not available.
- The secondary server handles directory synchronization.
- MWIs, event notification, and message notification are not handled.

#### **Reconnection Behavior When the Domino Server Is Reconnected and the Primary Server Remains Disconnected**

- Subscribers who log on to Cisco Unity no longer hear the UMR conversation, but hear the appropriate conversation.
- Messages stored in the UnityMTA folder on the secondary server are delivered to the appropriate subscriber Inboxes.
- The secondary server sets MWIs for subscribers who have unheard messages stored on the Domino server.
- External callers and subscribers can leave messages for subscribers. The messages are stored on the Domino server.
- The secondary server handles directory synchronization, MWIs, event notification, and message notification.

#### **Reconnection Behavior After the Domino Server Is Reconnected, Then the Primary Server Is Reconnected**

- The primary server becomes active, and the secondary server becomes inactive.
- All voice messaging ports on the primary server register with the Cisco CallManager server.
- The primary server answers all calls.
- Subscribers are able to leave and listen to messages. External callers can leave messages for subscribers.
- The Node Manager services (AvCsNodeMgr) on the primary and secondary servers send status to and receive status from each other.
- The Failover Monitors on the primary and secondary servers show that the primary server is active.

- Changes to the UnityDb database that occurred while the primary server was offline are replicated from the secondary server to the primary server.
- The primary server handles directory synchronization, MWIs, event notification, and message notification.
- Messages, greetings, and other recordings made on the primary server but not replicated to the secondary server before the network outage are replicated to the secondary server.
- Messages, greetings, and other recordings made on the secondary server during the network outage are replicated to the primary server.

**Reconnection Behavior When the Primary Server Is Reconnected and the Domino Server Remains Disconnected**

- The primary server becomes active, and the secondary server becomes inactive.
- All voice messaging ports on the primary server register with the Cisco CallManager server.
- The primary server answers all calls.
- All subscribers hear the UMR conversation when they log on to Cisco Unity.
- The Node Manager services (AvCsNodeMgr) on the primary and secondary servers send status to and receive status from each other.
- The Failover Monitors on the primary and secondary servers show that the primary server is active.
- Changes to the UnityDb database that occurred while the primary server was offline are replicated from the secondary server to the primary server.
- The primary server handles directory synchronization, MWIs, event notification, and message notification.
- Messages, greetings, and other recordings made on the primary server but not replicated to the secondary server before the network outage are replicated to the secondary server.
- Messages, greetings, and other recordings made on the secondary server during the network outage are replicated to the primary server.

**Reconnection Behavior After the Primary Server Is Reconnected, Then the Domino Server Is Reconnected**

- Subscribers who log on to Cisco Unity no longer hear the UMR conversation, but hear the appropriate conversation.
- Messages stored in the UnityMTA folder on the primary server are delivered to the appropriate subscriber Inboxes.
- The primary server sets MWIs for subscribers who have unheard messages stored on the Domino server.
- External callers and subscribers can leave messages for subscribers. The messages are stored on the Domino server.
- The primary server handles directory synchronization, MWIs, event notification, and message notification.





---

## A

- about failover [4-1](#)
- accessing web applications after failover or failback [2-1](#)
- active
  - both servers at same time [4-14](#)
  - server, determining the [3-1](#)
- analog voice lines, connecting [B-1](#)
- automatic failover and failback, disabling for troubleshooting [3-3](#)

---

## B

- backing up Cisco Unity system [1-9](#)

---

## C

- cables
  - connecting analog voice lines [B-1](#)
  - enabling phone system to send calls to active server in T1 integration [2-2](#)
- calls in progress, effects of failover and failback [4-6](#)
- causes
  - of both servers becoming active [4-14](#)
  - of failback [4-11](#)
  - of failover [4-10](#)
- changing
  - IP address of primary server [3-8](#)
  - IP address of secondary server [3-13](#)
- Cisco Personal Communications Assistant, access after failover or failback [2-1](#)
- Cisco Unity
  - exiting software [A-1](#)
  - file replication [4-7](#)

- restarting server [A-2](#)
- server name requirements [4-4](#)
- shutting down server [A-2](#)
- starting software [A-3](#)

- Cisco Unity Administrator, access after failover or failback [2-1](#)
- Configure Cisco Unity Failover wizard, running [1-2](#)
- configuring
  - automatic daily resynchronization of MWIs [1-5](#)
  - event notification [1-5](#)
  - failover, task list [1-1](#)
  - failover and failback settings [1-12](#)
  - failover on Cisco Unity servers [1-2](#)
  - scheduled backups of Cisco Unity system [1-9](#)
  - voice messaging ports on secondary server [1-3](#)
- confirming that failover and failback function correctly [3-5](#)
- connections
  - analog voice lines [B-1](#)
  - DTMF integration (illustration) [4-2](#)
  - enabling phone system to send calls to active server in T1 integration [2-2](#)
  - IP integration (illustration) [4-2](#)
  - lines between phone system and Cisco Unity servers [B-1](#)
  - serial data cable [B-6](#)
  - serial integration (illustration) [4-3](#)
- conventions, documentation [-viii](#)
- converting primary or secondary server [3-18](#)
- customizing failover and failback settings [1-12](#)

---

## D

- data splitter for RS-232 serial cable (illustration) [4-3](#)

data that is not replicated [4-8](#)

default settings, failover and failback [1-12](#)

delay

for failback to occur [4-12](#)

for failover to occur [4-12](#)

disabling

automatic failover and failback for troubleshooting [3-3](#)

failover initiation for unanswered calls on primary server [1-14](#)

documentation

audience and use [-vii](#)

conventions [-viii](#)

---

## E

effects

of failover and failback on calls in progress [4-6](#)

of Force Failover setting [4-5](#)

enabling

phone system to send calls to active server in T1 integration [2-2](#)

subscriber logon by phone after failover [1-4](#)

event ID, using to determine cause of failover or failback [3-7](#)

Event Monitoring Service

configuring for failover notification [1-5](#)

initiating manual failover [3-2](#)

event notification [1-5](#)

events

when failback occurs [4-9](#)

when failover occurs [4-9](#)

exceptions to normal functionality on secondary server [4-4](#)

exiting Cisco Unity software [A-1](#)

---

## F

failback

cause, based on event ID [3-7](#)

configuration settings (table) [1-13](#)

confirming functionality [3-5](#)

customizing settings [1-12](#)

default settings [1-12](#)

disabling automatic for troubleshooting [3-3](#)

effects on calls in progress [4-6](#)

effects on using phone as recording or playback device [2-2](#)

interval [4-12](#)

list of possible causes [4-11](#)

manual [3-2](#)

process [4-9](#)

updating server name in Media Master after [2-2](#)

failover

behavior during network outages [C-1](#)

cause, based on event ID [3-7](#)

causes of both servers becoming active [4-14](#)

configuration settings (table) [1-13](#)

configuration wizard [1-2](#)

configuring, task list [1-1](#)

confirming functionality [3-5](#)

customizing settings [1-12](#)

default settings [1-12](#)

disabling automatic for troubleshooting [3-3](#)

disabling initiation for unanswered calls on primary server [1-14](#)

effects on calls in progress [4-6](#)

effects on using phone as recording or playback device [2-2](#)

how it works [4-1](#)

interval [4-12](#)

list of possible causes [4-10](#)

manual [3-2](#)

process [4-9](#)

requirements [4-4](#)

setting up notification of [1-5](#)

testing [1-9](#)

uninstalling [3-18](#)

updating server name in Media Master after [2-2](#)

file replication [4-6](#)

Force Failover setting, effects of using or not using [4-5](#)

**I**

- initiating failover and failback manually [3-2](#)
- installing lines between phone system and Cisco Unity servers [B-1](#)
- integrations
  - analog connections [B-1](#)
  - DTMF connections (illustration) [4-2](#)
  - IP connections (illustration) [4-2](#)
  - serial connections [B-1](#)
  - serial connections (illustration) [4-3](#)
- interval
  - failback [4-12](#)
  - failover [4-12](#)
- IP address
  - changing primary server [3-8](#)
  - changing secondary server [3-13](#)

**L**

- licensing, restrictions on using secondary server without primary server [4-15](#)
- lines
  - connecting analog voice [B-1](#)
  - connecting serial cable [B-6](#)
- Local Status, meanings of values (table) [3-1](#)

**M**

- manual failback, initiating [3-2](#)
- manual failover
  - initiating [3-2](#)
  - initiating by Event Monitoring Service [3-2](#)
- Media Master, failover behavior [2-2](#)
- monitoring status of servers [4-6](#)
- MWIs, automatically resynchronizing daily [1-5](#)

**N**

- network, failover behavior during outages [C-1](#)
- Node Manager service, replication [4-7](#)
- notification of failover, setting up [1-5](#)

**O**

- outages, network [C-1](#)
- overview of failover [4-1](#)

**P**

- PCA. See Cisco Personal Communications Assistant
- phone as recording or playback device, effects of failover and failback [2-2](#)
- pinouts
  - phone system serial port acting as DCE [B-7](#)
  - phone system serial port acting as DTE [B-7](#)
  - RJ-11 connector (illustration) [B-2](#)
  - RJ-14 connector (illustration) [B-2](#)
- ports, configuring on secondary server [1-3](#)
- primary server
  - causes of unanswered calls [4-5](#)
  - changing IP address [3-8](#)
  - configuring failover [1-2](#)
  - disabling failover initiation for unanswered calls [1-14](#)
  - enabling phone system to send calls to active server in T1 integration [2-2](#)
  - replacing or converting [3-18](#)
  - starting first [3-1](#)
  - voice messaging functions when active [4-3](#)
- prompt replication [4-7](#)

**R**

- Remote Status, meanings of values (table) [3-1](#)
- replacing primary or secondary server [3-18](#)

## replication

- Cisco Unity files [4-7](#)
  - confirming UnityDb changes on inactive server [3-2](#)
  - data that is not replicated [4-8](#)
  - Node Manager service [4-7](#)
  - of files [4-6](#)
  - SQL Server database [4-8](#)
  - UMR (Unity Messaging Repository) [4-8](#)
  - UnityDb database [4-8](#)
  - voice messages [4-8](#)
- requirements for Cisco Unity failover [4-4](#)
- restarting
- Cisco Unity server [A-2](#)
  - servers, effects of [4-15](#)
- resynchronizing MWIs daily, automatic [1-5](#)
- RJ-11, connector pinout (illustration) [B-2](#)
- RJ-14, connector pinout (illustration) [B-2](#)
- routing rule for subscriber logon by phone after failover [1-4](#)
- RS-232 serial cable, using data splitter for serial integration [B-6](#)

**S**

- scheduling backups of Cisco Unity system [1-9](#)
- secondary server
- changing IP address [3-13](#)
  - configuring failover [1-2](#)
  - configuring voice messaging ports [1-3](#)
  - DTMF integration connections [B-1](#)
  - DTMF integration connections (illustration) [4-2](#)
  - enabling phone system to send calls to active server in T1 integration [2-2](#)
  - enabling subscriber logon by phone after failover [1-4](#)
  - exceptions to normal functionality during failover [4-4](#)
  - IP integration connections (illustration) [4-2](#)
  - replacing or converting [3-18](#)
  - serial integration connections [B-1](#)
  - serial integration connections (illustration) [4-3](#)

- using without primary server [4-15](#)
  - voice messaging functions when active [4-3](#)
- serial cable
- connecting [B-6](#)
  - wiring between data splitter and Cisco Unity servers [B-8](#)
- server name
- requirements [4-4](#)
  - updating in Media Master after failover or failback [2-2](#)
- servers
- determining which is active [3-1](#)
  - order for starting [3-1](#)
  - restarting [A-2](#)
  - shutting down [A-2](#)
  - status monitoring [4-6](#)
- settings for failover and failback configuration (table) [1-13](#)
- shutting down
- Cisco Unity server [A-2](#)
  - servers, effects of [4-15](#)
- software
- exiting Cisco Unity [A-1](#)
  - starting Cisco Unity [A-3](#)
- SQL Server, database replication [4-8](#)
- starting
- Cisco Unity software [A-3](#)
  - order for servers [3-1](#)
- Status Monitor, access after failover or failback [2-1](#)
- status of servers [4-6](#)
- subscriber logon, enabling on secondary server [1-4](#)

**T**

- T1 integration, enabling phone system to send calls to active server [2-2](#)
- testing Cisco Unity failover [1-9](#)
- time
- for failback to occur [4-12](#)
  - for failover to occur [4-12](#)

troubleshooting, disabling automatic failover and failback  
for [3-3](#)

---

## U

uninstalling failover [3-18](#)

UnityDb

confirming that changes replicated to inactive  
server [3-2](#)

database replication [4-8](#)

UTIM, configuring voice messaging ports on secondary  
server [1-3](#)

---

## V

voice message replication [4-8](#)

voice messaging functions

when primary server is active [4-3](#)

when secondary server is active [4-3](#)

