



# CHAPTER 1

## Cisco Unity Bridge Networking Guide

---

This chapter should be used in conjunction with the *Cisco Unity Bridge Networking Guide, Release 3.0*. New features are described in individual sections. Information that has changed in the *Cisco Unity Bridge Networking Guide, Release 3.0*—either because Cisco Unity or Cisco Unity Bridge functionality changed, or because information was omitted or is incorrect—is described in the “[Errors and Changes](#)” section at the end of the chapter.

The Domino version of the guide is available at [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/bridge/31/networking/guide/30dom/dom.html](http://www.cisco.com/en/US/docs/voice_ip_comm/bridge/31/networking/guide/30dom/dom.html); the Exchange version of the guide is available at [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/bridge/31/networking/guide/30ex/ex.html](http://www.cisco.com/en/US/docs/voice_ip_comm/bridge/31/networking/guide/30ex/ex.html).

This chapter contains the following sections:

- [Private List Considerations, page 1-1](#)
- [Pushing Mailbox Information from the Avaya Interchange to Cisco Unity, page 1-1](#)
- [Upgrading from Cisco Unity 4.0\(5\) or Later with Bridge 3.x \(Cisco Unity with Domino Only\), page 1-2](#)
- [Errors and Changes, page 1-7](#)

### Private List Considerations

Consider notifying subscribers in the event that the following members are inadvertently removed from their private distribution lists:

- When you delete a delivery location, blind addressees are removed from all private lists.
- When an external subscriber becomes a regular subscriber, the external subscriber is removed from all private lists.

### Pushing Mailbox Information from the Avaya Interchange to Cisco Unity

When the Cisco Unity Bridge represents more than one node on the Octel analog network (when the Interchange has multiple location profiles with different serial numbers configured for the same Cisco Unity network), the configuration of the directory view for update pushes of mailbox information should be performed for only one of the Cisco Unity location profiles. Otherwise, the Bridge will receive redundant pushes when changes occur.

Depending on how many location profiles are set up for Cisco Unity on the Interchange, and how many changes are occurring, sending duplicate pushes could generate unnecessary use of Bridge ports for administrative calls. It could also generate unnecessary processing of duplicate modifications by Cisco Unity and other servers, such as a Microsoft Exchange server hosting the Voice Connector, or an IBM Lotus Domino server involved in routing the push messages.

## Upgrading from Cisco Unity 4.0(5) or Later with Bridge 3.x (Cisco Unity with Domino Only)

If you currently have Cisco Unity 4.0(5) or later servers configured for networking with a Bridge 3.x server (or servers), use the following task list and procedures to upgrade Cisco Unity. Networking with the Octel servers is not disrupted after upgrading Cisco Unity. Therefore, in installations with multiple Cisco Unity servers, you can upgrade the Cisco Unity servers as your schedule permits.

### Task List

#### Upgrade the Cisco Unity Bridgehead Server

1. Upgrade the Cisco Unity bridgehead server. For systems that use failover, upgrade the secondary server as well. See the “Upgrading Cisco Unity 4.x Software to the Shipping Version” chapter of the *Cisco Unity Reconfiguration and Upgrade Guide (With IBM Lotus Domino)* at [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/unity/42/upgrade/guide/dom/dom.html](http://www.cisco.com/en/US/docs/voice_ip_comm/unity/42/upgrade/guide/dom/dom.html).
2. Run ConfigMgr.exe on the Cisco Unity bridgehead server to redesignate it as the bridgehead server. See the “To Designate the Bridgehead Server” procedure on page 1-3.

#### Upgrade Non-Bridgehead Cisco Unity Servers

3. Upgrade all non-bridgehead Cisco Unity servers in the network. For systems that use failover, upgrade the secondary servers as well. See the “Upgrading Cisco Unity 4.x Software to the Shipping Version” chapter of the *Cisco Unity Reconfiguration and Upgrade Guide (With IBM Lotus Domino)* at [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/unity/42/upgrade/guide/dom/dom.html](http://www.cisco.com/en/US/docs/voice_ip_comm/unity/42/upgrade/guide/dom/dom.html).



**Note** Networking with the Octel servers is not disrupted after upgrading Cisco Unity. Therefore, in installations with multiple Cisco Unity servers, you can upgrade the Cisco Unity servers as your schedule permits.

#### Optionally, Upgrade the Bridge Server(s)

If a newer version of the Bridge 3.x software is available, we recommend that you upgrade the Bridge software to the latest version. It is best to upgrade when Bridge message traffic is light.

4. Disable and stop virus-scanning and Cisco Security Agent services. See the “To Disable and Stop Virus-Scanning and Cisco Security Agent Services” procedure on page 1-3.
5. Upgrade the Bridge software. See the “To Upgrade Cisco Unity Bridge 3.x to a Newer Version” procedure on page 1-4.
6. Re-enable and start virus-scanning and Cisco Security Agent services. See the “To Re-Enable and Start Virus Scanning and Cisco Security Agent Services” procedure on page 1-5.

7. Install the Cisco Unity Bridge Analog Network and Node Analyzer (BANANA). BANANA is a stand-alone application that runs on the Bridge server, and is designed to assist with monitoring and troubleshooting analog communication between the Bridge and the Octel nodes in the analog network. It also provides detail and summary information of call activity.

Do the following procedures to install BANANA and initiate test calls (see the BANANA Help file for information about other functionality provided by BANANA): the “[To Install BANANA](#)” procedure on page 1-5, the “[To Adjust the Message Delivery Window Settings](#)” procedure on page 1-6, and the “[To Initiate Test Calls to the Octel Nodes](#)” procedure on page 1-6.

#### Enable Optional Features

8. Optionally, if the Bridge is at version 3.0(6) or later, enable the Bridge server to accept requests to push remote mailbox information. See the “Enabling the Bridge to Accept Requests to Push Mailbox Information (Bridge 3.0(6) and Later)” section in the “Setting Up Cisco Unity and the Bridge for Networking” chapter of the *Cisco Unity Bridge Networking Guide, Release 3.0 (With IBM Lotus Domino)* at [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/bridge/31/networking/guide/30dom/bnet\\_010.html](http://www.cisco.com/en/US/docs/voice_ip_comm/bridge/31/networking/guide/30dom/bnet_010.html).

## Procedures

#### To Designate the Bridgehead Server

Run the ConfigMgr.exe utility with the Create Bridge Account option to redesignate the server as the bridgehead. (The CsBridgeConnector service will not start, and the Cisco Unity Administrator will not display Bridge-related pages until ConfigMgr.exe has been run.)

- 
- Step 1** On the Cisco Unity server, browse to the directory in which Cisco Unity is installed (the default location is CommServer).
  - Step 2** Double-click **ConfigMgr.exe**. The ConfigMgr dialog box appears.
  - Step 3** Click **Create Bridge Account**.
  - Step 4** Click **OK** in the dialog box that displays after the configuration has completed.
  - Step 5** Close the ConfigMgr dialog box.
- 

#### To Disable and Stop Virus-Scanning and Cisco Security Agent Services

- 
- Step 1** Refer to the virus-scanning software documentation to determine the names of the virus-scanning services.
  - Step 2** On the Windows Start menu, click **Programs > Administrative Tools > Services**.
  - Step 3** Disable and stop each virus-scanning service and the Cisco Security Agent service:
    - a. In the right pane, double-click the service.
    - b. On the General tab, in the Startup Type list, click **Disabled**. This prevents the service from starting when you restart the server.

- c. Click **Stop** to stop the service immediately.
- d. Click **OK** to close the Properties dialog box.

**Step 4** When the services have been disabled, close the Services MMC.

---

### To Upgrade Cisco Unity Bridge 3.x to a Newer Version

---

**Step 1** Log on to the Bridge server by using the Windows 2000 Server Administrator account.

**Step 2** Verify that the account has permission to access the Bridge Administrator.

- a. Open the Bridge Administrator.
- b. If you are allowed access and can view the Bridge Administrator pages, exit the Bridge Administrator and continue with [Step 3](#).



**Caution**

If you are denied access to the Bridge Administrator, do not continue, because the Bridge setup program will fail. You must log off and log back on using another account that is allowed access to the Bridge Administrator. It is possible that the account was denied access to the Bridge Administrator because it is not in the Access Control List of the <Bridge>\Starfish\Asp directory or does not have Full Control permissions to that directory. Access to the <Bridge>\Starfish\Asp directory may have been restricted when password protection was added to the Bridge Administrator as described in the “To Add Password Protection to the Bridge Administrator” procedure in the “Setting Up Cisco Unity and the Bridge for Networking” chapter of the *Cisco Unity Bridge Networking Guide (With IBM Lotus Domino)* at [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/bridge/31/networking/guide/30dom/bnet\\_010.html](http://www.cisco.com/en/US/docs/voice_ip_comm/bridge/31/networking/guide/30dom/bnet_010.html).

---

**Step 3** On the Windows Start menu, click **Programs > Administrative Tools > Services**, and stop the following two services:

- Digital Networking
- Unity Bridge

The Bridge services will complete the shutdown process when the last in-process message transmission or reception, rather than call, is complete. No additional message transmissions will begin on the in-process calls—either outbound or inbound—after shutdown has been initiated.

**Step 4** If you downloaded the Bridge software from the Software Center website, browse to the directory in which the files were extracted.

If you are using the Cisco Unity Bridge CD, insert the disc in the CD-ROM drive, and browse to the **Install** directory.

**Step 5** Double-click **Setup.exe**.

**Step 6** Click **Next**.

**Step 7** In the Choose Destination Location dialog box, change the installation directory, if applicable, and click **Next**.

**Step 8** If a device driver service was previously installed for the Brooktrout voice-fax card, a message asks if you want to overwrite the existing service. Click **Yes** twice.

- Step 9** In the Select Country dialog box, select the country for which the voice-fax cards will be configured, and click **Next**.
- Step 10** Verify the installation settings, and click **Next**.
- Step 11** When prompted, remove the disc from the CD-ROM drive.
- Step 12** Click **OK** to restart the server.
- 

### To Re-Enable and Start Virus Scanning and Cisco Security Agent Services

---

- Step 1** Refer to the virus-scanning software documentation to determine the names of the virus-scanning services.
- Step 2** On the Windows Start menu, click **Programs > Administrative Tools > Services**.
- Step 3** Re-enable and start each virus-scanning service and the Cisco Security Agent service:
- In the right pane, double-click the service.
  - On the General tab, in the Startup Type list, click **Automatic** to re-enable the service.
  - Click **Start** to start the service.
  - Click **OK** to close the Properties dialog box.
- Step 4** When the services have been re-enabled, close the Services MMC.
- 

### To Install BANANA

The drive on which BANANA will be installed requires at least 1 GB of free disk space.

---

- Step 1** Disable virus scanning services and the Cisco Security Agent service, if applicable.
- Step 2** Insert the Cisco Unity Bridge compact disc in the CD-ROM drive, and browse to the **BANANA** directory.
- Step 3** Double-click **setup.exe**.
- Step 4** Click **OK** at the welcome screen.
- Step 5** If applicable, change the directory where BANANA will be installed.
- Step 6** Click the **Installation** button.
- Step 7** If applicable, change the program group where BANANA will appear.
- Step 8** Click **Continue**.
- Step 9** If a Version Conflict message box is displayed warning that a file being copied is not newer than the file on your system, click **Yes** to keep the existing file.
- Step 10** When the installation is done, click **OK**.
- Step 11** Enable virus-scanning and the Cisco Security Agent services, if applicable



**Note** The most up-to-date version of BANANA is available at <http://www.CiscoUnityTools.com>. When you start BANANA, it checks the CiscoUnityTools website to see if a newer version is available, and if so, prompts you about upgrading.

### To Adjust the Message Delivery Window Settings

- Step 1** In the Bridge Administrator, click **Octel Nodes**.
- Step 2** In the Node list, click an Octel node that you want to be tested, and click **Edit**.
- Step 3** On the Octel Node page in the Message Delivery Windows section, adjust the schedule according to following illustration, so that the Bridge will not wait to initiate calls to the Octels to deliver normal, urgent, and administrative messages.

Message Delivery Windows				
Message Type	Enabled	Begin	End	Interval
Normal	<input checked="" type="checkbox"/>	12:00 AM	11:59 PM	1
Urgent	<input checked="" type="checkbox"/>	12:00 AM	11:59 PM	1
Administration	<input checked="" type="checkbox"/>	12:00 AM	11:59 PM	1

Note that BANANA makes only administrative calls when testing the Octel analog network. However, if you adjust the normal and urgent schedules as shown, you do not have to remember to adjust the schedule if you also send test messages from Cisco Unity subscribers to Octel subscribers.

- Step 4** Click **Save**.
- Step 5** Repeat [Step 2](#) through [Step 4](#) for each Octel node that you want to test.

### To Initiate Test Calls to the Octel Nodes

- Step 1** On the Bridge server on the Windows Start menu, click **Programs > BANANA > BANANA admin**. The BANANA admin main window displays.
- Step 2** Configure the log and output folder locations.
- Step 3** Specify the Octel nodes to be included when placing test calls.
- Step 4** Place the test calls.
- Step 5** Process the call data, and view the results.
- Refer to the BANANA Help for details.

# Errors and Changes

The following sections apply to the *Cisco Unity Bridge Networking Guide, Release 3.0 (With IBM Lotus Domino)* at

[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/bridge/31/networking/guide/30dom/dom.html](http://www.cisco.com/en/US/docs/voice_ip_comm/bridge/31/networking/guide/30dom/dom.html) and to the *Cisco Unity Bridge Networking Guide, Release 3.0 (With Microsoft Exchange)* at [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/bridge/31/networking/guide/30ex/ex.html](http://www.cisco.com/en/US/docs/voice_ip_comm/bridge/31/networking/guide/30ex/ex.html), unless otherwise noted:

- [Changes That Affect All Cisco Unity Guides, page 1-7](#)
- [Configuring the Interop Gateway \(Cisco Unity with Domino Only\), page 1-8](#)
- [Configuring the Cisco Unity Server Designated as the Bridgehead \(Cisco Unity with Exchange Only\), page 1-8](#)
- [Upgrading from Cisco Unity 4.0\(3\) or Later with Bridge 3.x \(Cisco Unity with Exchange Only\), page 1-8](#)

## Changes That Affect All Cisco Unity Guides

### Cross-References to System Requirements Document

In cross-references to *Cisco Unity 4.x System Requirements, and Supported Hardware and Software*, refer instead to the following documents:

- *Cisco Unity 4.2 System Requirements* at [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/unity/42/requirements/42cusysreq.html](http://www.cisco.com/en/US/docs/voice_ip_comm/unity/42/requirements/42cusysreq.html).
- *Supported Hardware and Software, and Support Policies for Cisco Unity 4.2 and Later* at [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/unity/42/support/42lsupp.html](http://www.cisco.com/en/US/docs/voice_ip_comm/unity/42/support/42lsupp.html).

### Exchange 5.5 No Longer Supported

Exchange 5.5 is no longer supported as the message store for Cisco Unity messages, for either new installations or upgrades. In Cisco Unity guides and Help, ignore any references to Exchange 5.5 as being supported. (Some Cisco Unity applications may contain Exchange 5.5 references as well.)

With Cisco Unity 4.2, installations and upgrades will fail when Exchange 5.5 is the message store. Before you can upgrade to version 4.2, you must upgrade to Exchange 2003 or Exchange 2000.

### Windows NT Domain No Longer Supported

Making a Cisco Unity server a member server in a Windows NT domain is no longer supported. In Cisco Unity guides and Help, ignore any references to a Windows NT domain as being supported. (Some Cisco Unity applications may contain Windows NT domain references as well.)

## Configuring the Interop Gateway (Cisco Unity with Domino Only)

In the “Configuring the Interop Gateway” section in the “[Setting Up Cisco Unity and the Bridge for Networking](#)” chapter, the procedures for setting up Cisco Unity and the Bridge for networking omitted information about configuring the permissions for the interop gateway that are required when Cisco Unity is integrated with IBM Lotus Domino release 7.0. The permissions must be set prior to performing the procedure to configure the interop gateway.

In Domino release 7.0, the default permissions set for the -Default- account on the access control list of the mailbox.ntf template do not include permission to replicate or copy documents. This permission is required when setting up the interop gateway. It can be granted either by adding the permission for the -Default- account, or by adding the UnityServers group that was created during Cisco Unity installation to the access control list, and granting permission to replicate or copy documents to the group. Refer to the applicable IBM Lotus documentation for information on adding this permission.

## Configuring the Cisco Unity Server Designated as the Bridgehead (Cisco Unity with Exchange Only)

The “Configuring the Cisco Unity Server Designated as the Bridgehead” section in the “[Setting Up Cisco Unity and the Bridge for Networking](#)” chapter omitted the following information relevant to running ConfigMgr.exe to designate the bridgehead server.

In Cisco Unity release 4.2(1), the Permissions wizard includes a new option to set permissions that are required for AMIS, Bridge, and VPIM networking. When you run ConfigMgr.exe, if you did not choose this option, the ConfigMgr.exe utility will indicate that you need to run the Permissions wizard, select the option for AMIS, Bridge, and VPIM networking, and manually delegate Exchange administration control to the installation and directory services accounts (if you have not already done so).

If you receive this error message, do the following tasks:

1. Click OK and exit the ConfigMgr.exe utility.
2. Download and run the latest version of the Permissions wizard from CiscoUnityTools.com, or run the version that appears in the Utilities\PermissionsWizard directory on the shipping Cisco Unity 4.2(1) CD or DVD.
3. Follow the Permissions wizard instructions to select the option for AMIS, Bridge, and VPIM networking, and to manually delegate Exchange administration control. For additional information, see Permissions wizard Help.
4. Rerun ConfigMgr.exe.

## Upgrading from Cisco Unity 4.0(3) or Later with Bridge 3.x (Cisco Unity with Exchange Only)

When upgrading the Cisco Unity bridgehead server to Cisco Unity release 4.2(1), note the following information, omitted from the “Task List: Upgrading from Cisco Unity 4.0(3) or Later with Bridge 3.x” section in the “[Upgrading from Cisco Unity 4.0\(3\) or Later with Bridge 3.x](#)” chapter.

### Active Directory Schema Updates

In Cisco Unity release 4.2(1), the property set `cisco-Ecsbu-Unity-Information` was added to the Cisco Unity Directory Monitor schema extensions to accommodate changes to the Cisco Unity Permissions wizard. Associated updates were also made to the Cisco Unity Bridge and Cisco Unity VPIM extensions.

When you upgrade the bridgehead Cisco Unity system to 4.2(1), you must update the Bridge extensions as well as the Directory Monitor extensions. The schema updates must be applied at a specific point during the upgrade process. Be sure to follow the instructions in the *Cisco Unity Reconfiguration and Upgrade Guide* as recommended in the task list.

Note that the changes are backward compatible with earlier versions of Cisco Unity; if you have multiple servers connected via Digital Networking, you can apply the required schema updates in order to upgrade one Cisco Unity server to 4.2(1) even if other servers continue to run earlier versions of Cisco Unity. (For a list of Cisco Unity version combinations that are supported for networked Cisco Unity servers, see the “Digital Networking Requirements for Cisco Unity with Exchange” section in *Cisco Unity Networking Options Requirements* at [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/unity/compatibility/matrix/cunetoptionsreqs4x.html](http://www.cisco.com/en/US/docs/voice_ip_comm/unity/compatibility/matrix/cunetoptionsreqs4x.html).)

### Redesignating the Bridgehead Server

In Cisco Unity release 4.2(1), the Permissions wizard includes a new option to set permissions that are required for AMIS, Bridge, and VPIM networking. When you run `ConfigMgr.exe`, if you did not choose this option, the `ConfigMgr.exe` utility will indicate that you need to run the Permissions wizard, select the option for AMIS, Bridge, and VPIM networking, and manually delegate Exchange administration control to the installation and directory services accounts (if you have not already done so).

If you receive this error message, do the following tasks:

1. Click OK and exit the `ConfigMgr.exe` utility.
2. Download and run the latest version of the Permissions wizard from `CiscoUnityTools.com`, or run the version that appears in the `Utilities\PermissionsWizard` directory on the shipping Cisco Unity 4.2(1) CD or DVD.
3. Follow the Permissions wizard instructions to select the option for AMIS, Bridge, and VPIM networking, and to manually delegate Exchange administration control. For additional information, see Permissions wizard Help.
4. Rerun `ConfigMgr.exe`.

