



CHAPTER 6

Monitoring and Maintaining Bridge Networking

This chapter provides information on monitoring and maintaining Bridge Networking.

See the following sections:

- [Controlling the Number of Ports Used for Outgoing Messages, page 6-1](#)
- [Bridge Analog Network and Node Analyzer \(BANANA\), page 6-3](#)
- [Bridge Traffic Analyzer, page 6-5](#)
- [Backing Up and Restoring a Bridge Server, page 6-6](#)
- [Changing the IP Address of the Bridge Server or a Microsoft Exchange Server, page 6-9](#)
- [Moving the UOmni Mailbox, page 6-10](#)
- [Monitoring Recommendations, page 6-10](#)

Controlling the Number of Ports Used for Outgoing Messages

Outgoing messages from the Bridge to an Octel node are placed in queues. The Bridge maintains three queues for each node—one queue each for normal and urgent messages, and a third for administrative tasks. Queued messages are processed in first-in-first-out (FIFO) order.

The Bridge can simultaneously use more than one port on the analog voice-fax cards in the Bridge server to send messages to a particular Octel node. For example, assume that there are several messages in the normal message queue for a specific node, and that the Bridge is using one port to transmit the messages. If an administrative or urgent message is then sent to that same node during the time that the normal message traffic is being transmitted, the Bridge will use another port to dial out to send the administrative or urgent message.

Two parameters on the System Settings page in the Bridge Administrator allow you to control the number of ports used for outgoing messages to a specific node: Queued Call Threshold and Max Ports Per Node. These values are applied to the normal and urgent outgoing message queues for each node. (Note that these values are not applied to administrative queues. Only one port at a time will ever be used for administrative calls to a particular node).

The value in Queued Call Threshold specifies the threshold number of messages that must be in the outgoing message queue of a specific node for an additional port to be used for message delivery. As the number of messages in the queue increases, an additional port is added when the number of messages in the queue reaches a multiple of this parameter.

For example, if the value of Queued Call Threshold is set to 10 (the default value), one port will be used for message delivery if there are fewer than 10 messages in the queue. For 10–19 messages, two ports will be used. For 20–29 messages, three ports will be used, and so on. The total number of ports used is limited by the Max Ports Per Node parameter.

Queued Call Threshold is also used to determine when to disconnect a port used for outgoing messages to a specific node. As the number of messages in the queue decreases, a port is disconnected when the number of messages in the queue is below the next lower multiple of this parameter. When only two ports are in use, as the number of messages in the queue drops below half of this parameter, the second port is disconnected.

For example, if the value of the Queued Call Threshold is set to 10, three ports will be used for message delivery if there are 20–29 messages in the queue. As the number of messages in the queue decreases, the third port is not disconnected until the number of messages in the queue drops to 10 or fewer. When the number of messages drops to 5 or fewer messages, the second port is disconnected, so only one port is used to transmit the remaining messages.

The Max Ports Per Node parameter allows you to specify the maximum number of ports that can be used simultaneously to deliver messages to a particular node. Again, this value is applied to each message queue. For example, if Max Ports Per Node is set to 4 (the default value), it is possible that 9 ports could be used simultaneously to send normal, urgent, and administrative messages to a specific node. In this example, up to 4 ports could be used for normal messages; up to 4 ports could be used for urgent messages; and 1 port would be used for administrative messages. (Outbound administrative calls to the same node are not placed simultaneously. Only one port at a time will ever be used for administrative calls to a particular node.)

Determining Optimal Values for Queued Call Threshold and Max Ports Per Node

The optimal values for Queued Call Threshold and Max Ports Per Node depend on the number of ports, the number of nodes, and on message traffic patterns. Start with the default values for these parameters, and use the Bridge Traffic Analyzer to observe message traffic patterns to see whether you need to adjust the settings. See the [“Bridge Traffic Analyzer” section on page 6-5](#) for more information.

The default values should be appropriate for light message traffic because with light traffic, the thresholds for the parameters are never reached. The default values should also be sufficient for installations with medium traffic and a small to medium number of Octel nodes. However, installations with medium traffic and ten or more Octel nodes, or with high traffic, should carefully watch the reports generated by the Bridge Traffic Analyzer, and adjust the values for the parameters as necessary.

If you decide to adjust the values for Queued Call Threshold and Max Ports Per Node, keep in mind that the Bridge ports are used for both outgoing messages to Octel nodes and incoming messages to the Bridge. If message traffic is heavy enough, it is possible to incorrectly adjust the values such that all of the ports will be used for outgoing messages, leaving no ports available for incoming messages. If this is a concern, you may want to designate one or more ports to be used only for incoming calls. The Line Status page in the Bridge Administrator allows you to specify whether each line is to be used for both incoming and outgoing calls or only for incoming calls.

Bridge Analog Network and Node Analyzer (BANANA)

BANANA is a stand-alone application that runs on the Bridge server. It 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.

BANANA contains an administration application called the BANANA admin that allows you to control how BANANA:

- Generates test calls to the Octel systems that are networked with the Bridge server.
- Extracts information from the call traces on the Bridge server and presents different views of the data.
- Monitors the call traces for error conditions, and logs warnings or errors to the Windows Event Viewer.

With the BANANA admin, you can also install and configure the BANANA service to do the tasks listed above at configurable intervals.

If you have already installed BANANA, skip to the “[Getting Started Using the BANANA admin to Monitor Analog Activity](#)” section on page 6-4.

To Install BANANA

- 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 to upgrade.

Getting Started Using the BANANA admin to Monitor Analog Activity

If the Bridge server sends and receives many messages, it is likely that when you view the call traces in BANANA admin, you will see some errors. Do not be alarmed; due to the nature of analog transmissions, some errors are to be expected. In order to send and receive messages between the Bridge and an Octel node, DTMF tones are exchanged in accordance with the Octel analog protocol. It is not uncommon for line noise to interfere with the transmission or reception of DTMF tones, particularly when the tones are transmitted over the PSTN. In an environment with Cisco Unified Communications Manager (CM) (formerly known as Cisco Unified CallManager) and Cisco gateways, the circuit-switched calls are encoded and repackaged into IP packets. The transcoding must be precise. The DTMF duration and interdigit timing on the Cisco gateways or Cisco Unified CM must be set to a value between 80 and 100 milliseconds. Incorrect settings will cause transmission problems.

When you first set up Bridge Networking, we recommend that you use the BANANA admin to frequently monitor the analog activity (at least daily, though more frequently if necessary) to find and fix problems. By monitoring the analog activity, you will become familiar with the message traffic patterns and learn what ratio of errors is within a “normal” range.

The following procedure will get you started using the BANANA admin. See BANANA Help for details about how to do each task.

To Get Started Using the BANANA admin

-
- Step 1** On the Windows Start menu on the Bridge server, click **Programs > BANANA > BANANA admin**.
- Step 2** If you have not already done so, configure the log and output folder locations.
- Step 3** Optionally, adjust the **Hours of Data to Retain in Database** setting.
- You may want to increase the setting if there is sufficient disk space on the Bridge server. Be careful if you decrease the setting from the default because only the most recent call data will be retained after the call data is subsequently processed, and you could lose data that you need for troubleshooting a problem.
- Step 4** Click **Process Call Data**.
- BANANA processes the call traces and then displays information about incoming and outgoing calls in the Calls grid. Calls that resulted in errors are displayed in the Errors grid.
- Step 5** Click **View Node Totals** to display the Totals per Octel Node dialog box.
- This view of the data is useful for identifying communication problems with a particular Octel node. For example, if the ratio of errors to calls for a particular Octel node is significantly higher than for the other nodes, you can investigate the problem further by doing the following sub-steps:
- a. Make note of the serial number of the Octel node with a high number of errors.
 - b. Click the main BANANA admin window, and then click the **octelserialnumber** column header in the Calls grid to sort the calls by Octel serial number.
 - c. In the Calls grid, click a row with the problematic serial number that has an exitcode other than OK. The corresponding record in the Errors grid is highlighted. This record provides specific details regarding the condition under which the call was terminated, including the state of the protocol that was in process, and the reason why the call could not be completed.
 - d. Click **View Call Detail for Selected Call**. This view of the data displays the mailboxes that were involved in the call, which is useful if someone notifies you that they received an NDR, or if you are tracking down a directory update problem that was logged in the Windows Event Viewer. You can also use this view of the data to verify that the message (or other action) involved in the failed call was repeated later in a successful call.

- Step 6** Configure BANANA to monitor the call traces for error conditions, and to log warnings or errors to the Windows Event Viewer. As needed, you can adjust the notification settings.
-

Bridge Traffic Analyzer

The Bridge Traffic Analyzer is a report-generation utility that reads the call traces on the Bridge server, and generates a graph and a summary table that can be saved as a comma-separated value (CSV) file. The Bridge Traffic Analyzer is available for download at <http://www.CiscoUnityTools.com>.

The Bridge Traffic Analyzer generates reports by using the data in the call traces in the \Starfish\Log directory on the Bridge server. The Call Log Retention parameter on the System Settings page in the Bridge Administrator allows you to specify the number of days of call history to retain. For more information about the Call Log Retention setting, see the “[System Settings](#)” section on page 10-2.

In the reports, the direction of the queues is from the perspective of Cisco Unity:

- The inbound queue contains messages from Octel nodes that the Bridge sends to Cisco Unity. Messages in the inbound queue are sent to Cisco Unity by using SMTP. Therefore, unless Cisco Unity or Exchange is down, messages move very quickly through the inbound queue.
- The outbound queue contains messages from Cisco Unity that the Bridge sends to the appropriate Octel nodes. Messages in the outbound queue are sent through the ports on the analog voice-fax cards on the Bridge server to the Octel nodes. Because the number of ports is a fixed resource, and because analog transmissions are slow in comparison to SMTP, it is possible that messages will back up in the outbound queue.

The Bridge Traffic Analyzer provides the following reports:

- **Port Availability**—Shows the availability of ports on the analog voice-fax cards on the Bridge server. You can choose to show how many ports were available to take calls from Octel nodes, how many ports were busy, or both. The summary CSV file presents a table with the maximum and minimum number of available ports for each hour during the day.
- **Message Queue Activity**—Shows how many messages and how much data is passing through the inbound and outbound message queues on the Bridge server. You can choose to show the number of messages, the message queue size in megabytes, or both. The summary CSV file presents a table with the maximum number of messages in the inbound and outbound queues, and the maximum message size of the inbound and outbound queues for each hour during the day.
- **Message Latency**—Shows the length of time that messages stayed in the outbound queue before being delivered to the Octel nodes. You can select a time range for the report (the default is 24 hours), and you can choose which Octel nodes to see in the report (by default, all nodes are shown). The Message Latency report shows only the outbound queue. Messages arrive quickly from Cisco Unity, but are delivered by analog lines to their target Octel node; therefore, it is possible for messages to back up in the queue waiting for an available port.
- **Node Message Traffic**—Shows how many messages and how much data is passing between different Cisco Unity and Octel nodes. For example, you can use this report to determine which Octel nodes a specific Cisco Unity server is messaging with most heavily. You can select one or more Cisco Unity nodes, one or more Octel nodes, and a time range for the report.

See Bridge Traffic Analyzer Help for more information about these reports.

Backing Up and Restoring a Bridge Server

This section explains how to back up data on the Bridge server, and how to restore that data to another Bridge server.

See the following sections:

- [Backing Up the Bridge Server, page 6-6](#)
- [Replacing a Bridge Server and Restoring Data, page 6-7](#)

Backing Up the Bridge Server

Both offline and online backups are supported for the Cisco Unity Bridge server. When backing up the Bridge server, you need to back up only the configuration and data files; you do not need to back up the Bridge software because it is easy to reinstall the Bridge software on another server.

The files that you back up on the Bridge server include:

- WAV files of voice names for Octel and Unity node directory entries
- A database that contains configuration data and information about Octel and Unity node directory entries
- Configuration files

For a list of backup and restore software supported for the Bridge server, see the “Supported Backup Software” section in the applicable version of the *System Requirements, and Supported Hardware and Software for Cisco Unity Bridge*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

No unique software agents are required. We recommend that you do the backup during off-peak hours.

See the following procedures for step-by-step instructions:

- [To Do an Online Backup of the Bridge Server by Using Third-Party Backup and Restore Software, page 6-6](#)
- [To Do an Offline Backup of the Bridge Server, page 6-7](#)

To Do an Online Backup of the Bridge Server by Using Third-Party Backup and Restore Software

Step 1 Back up the following files and directories:

- SN (include all files and subdirectories)
- Starfish\Db\StarFish.mdb
- VPIM\Vpim.cfg
- VPIM\Propagation (include all files and subdirectories)



Note The paths above are relative to the drive and directory in which the Bridge software is installed. The default is D:\Bridge.

For detailed instructions, refer to the manufacturer documentation or Help.

To Do an Offline Backup of the Bridge Server

Step 1 On the Bridge server, on the Windows Start menu, click **Programs > Administrative Tools > Services**, and stop the following services:

- Digital Networking
- Unity Bridge

Any calls that are in progress are allowed to finish before the services are stopped.

Step 2 Back up the following directories:

- SN (include all files and subdirectories)
- Starfish\Db\StarFish.mdb
- VPIM\Vpim.cfg
- VPIM\Propagation (include all files and subdirectories)



Note The paths above are relative to the drive and directory in which the Bridge software is installed. The default is D:\Bridge.

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

- Digital Networking
- Unity Bridge

Step 4 Close the Services window.

Replacing a Bridge Server and Restoring Data

When replacing a Bridge server, you install the Bridge software and then restore the configuration and data files.

To Replace a Bridge Server and Restore Data

We recommend that you replace the Bridge server during off-peak hours. Note that the paths below are relative to the drive and directory in which the Bridge software is installed. The default is D:\Bridge.

Step 1 Install the new Bridge server according to the instructions in the “Overview of Mandatory Tasks for Installing the Cisco Unity Bridge” chapter of the applicable version of the *Installation Guide for Cisco Unity Bridge*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Step 2 After the post-installation restart of the new Bridge server, on the Windows Start menu, click **Programs > Administrative Tools > Services**, and stop the following services:

- Digital Networking
- Unity Bridge

- Step 3** On the Exchange server on which the Voice Connector is installed, click **Programs > Administrative Tools > Services**, right-click **Exchange 2000 Voice Connector**, and select **Stop**. Messages from Cisco Unity subscribers and from the Bridge will be held in the Voice Connector mailbox until you restart the service.
- Step 4** If the old Bridge server has failed or is already offline, skip to [Step 11](#). Otherwise, confirm that there are no more messages queued in the following directories on the old Bridge server:
- VPIM\Xcode\Inbound
 - VPIM\VM\In
 - IN
- Messages pass through these directories quickly, in the order listed, before reaching the analog queues.
- Step 5** In the Bridge Administrator on the old Bridge server, click **Queue Status** to see if there are outgoing messages in the analog queues. Wait for all messages in the queues to be sent before proceeding. You can view call progress on the Line Status page to determine when the outbound calls have finished.
- Step 6** On the old Bridge server, on the Windows Start menu, click **Programs > Administrative Tools > Services**, right-click **Unity Bridge**, and select **Stop**. Any incoming calls that are in progress are allowed to finish before the service is stopped. When the Unity Bridge service has been stopped, the Bridge is unable to accept calls from the Octels.
- Step 7** On the old Bridge server, confirm that there are no more messages queued in the following directories:
- Starfish\Out
 - Out
 - VPIM\Xcode\Outbound
 - VPIM\Internet\Out
- Messages pass through these directories quickly, in the order listed, before being sent via SMTP to Exchange.
- Step 8** When you are sure that there are no more messages on the old Bridge server, in the Services MMC, right-click **Digital Networking**, and select **Stop**.
- Step 9** If you have a recent backup, skip to [Step 10](#). Otherwise, back up the following directories from the old Bridge server:
- SN (include all files and subdirectories)
 - Starfish\Db\StarFish.mdb
 - VPIM\Vpim.cfg
 - VPIM\Propagation (include all files and subdirectories)
- Step 10** Shut down the old Bridge server.
- Step 11** Restore the following directories from the backup medium to the new Bridge server:
- SN (include all files and subdirectories)
 - Starfish\Db\StarFish.mdb
 - VPIM\Vpim.cfg
 - VPIM\Propagation (include all files and subdirectories)
- Step 12** If the fully qualified domain name (FQDN) of the new Bridge server is the same as the old Bridge server, skip to [Step 13](#). Otherwise, change the FQDN in the following places:
- On the Bridge server, in the “Bridge Server Full Computer Name” field on the Digital Networking page in the Bridge Administrator.

- On the Cisco Unity bridgehead server, in the “Bridge Server Full Computer Name” field on the Bridge Delivery Location pages in the Cisco Unity Administrator.

If there are only a few delivery locations, use the Cisco Unity Administrator to change the FQDN on each delivery location.

If there are many delivery locations, modify the delivery locations by using the Cisco Unity Bulk Import wizard. See the “Modifying Existing Delivery Locations” section in the Cisco Unity Bulk Import wizard Help for details on preparing a CSV file and running the wizard.

- If you are using host files for name resolution with the Bridge, change the FQDN in the host file on the applicable Exchange or SMTP relay server.
- If you are using DNS for name resolution with the Bridge, change the FQDN in the MX and A records on the DNS server.

Step 13 In the Services MMC of the new Bridge server, start the following services:

- Digital Networking
- Unity Bridge

Step 14 Close the Services MMC on the new Bridge server.

Step 15 On the Exchange server on which the Voice Connector is installed, click **Programs > Administrative Tools > Services**, right-click **Exchange 2000 Voice Connector**, and select **Start**.

Step 16 Close the Services MMC.

Changing the IP Address of the Bridge Server or a Microsoft Exchange Server

Depending on your network, after changing the IP address of the Bridge server or a Microsoft Exchange server, you may need to update the Exchange SMTP virtual server settings on all other Microsoft Exchange servers in your network to reflect the new IP address so that Bridge messages are delivered correctly.

To Check and Update the SMTP Virtual Server Relay List

Step 1 On the Microsoft Exchange server, on the Windows Start menu, click **Programs > Microsoft Exchange > System Manager**.

Step 2 In the tree on the left, expand **Servers\<Server name>\Protocols\SMTP**.

Step 3 Right-click **Default SMTP Virtual Server** and select **Properties**.

Step 4 Click the **Access** tab.

Step 5 Click **Relay**.

Step 6 Do one of the following:

- If All Except the List Below is selected and the new server IP address does not appear in the list, skip to [Step 11](#).
- If All Except the List Below is selected and the new server IP address appears in the list, click the IP address and click **Remove**, then skip to [Step 10](#).
- If Only the List Below is selected, continue with [Step 7](#).

- Step 7** Click **Add**.
 - Step 8** Click **Single Computer**, and enter the new IP address of the server that changed addresses.
 - Step 9** Click **OK**.
 - Step 10** Verify that the **Allow All Computers Which Successfully Authenticate to Relay, Regardless of the List Above** check box is checked.
 - Step 11** Click **OK** twice to close the Properties dialog box.
 - Step 12** Close the Exchange System Manager.
 - Step 13** Repeat [Step 1](#) through [Step 12](#) on each Microsoft Exchange server in your network.
-

Moving the UOmni Mailbox

For information on moving the UOmni mailbox, see the “UOmni Mailbox” section in the “Cisco Unity Data and Log Files” chapter of the *Maintenance Guide for Cisco Unity*. The guide is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

Monitoring Recommendations

See the Unity and Bridge Monitoring Recommendations spreadsheet, available at <http://www.ciscounitytools.com/Documents.htm>. This Excel spreadsheet contains tabs that include events, performance monitor counters, and services that we recommend for monitoring Cisco Unity and Bridge deployments.