Cisco Unity Bridge 3.0 System Requirements, and Supported Hardware and Software

Revised June 8, 2005

This document lists requirements, supported hardware and software, and other necessary information for installing Cisco Unity Bridge version 3.0. It is divided into three parts:

(For requirements, and supported hardware and software for Cisco Unity, refer to *Cisco Unity System Requirements, and Supported Hardware and Software*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.)

PART 1: Cisco Unity Bridge 3.0 System Requirements

CISCO SYSTEMS

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Hardware Requirements

- A server that meets Cisco Unity Bridge specifications. Refer to the *Cisco Unity Supported Platforms List* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_data_sheets_list.html.

⚠

Caution   Cisco TAC does not provide any assistance for installing, customizing, or troubleshooting the Bridge on an unsupported platform.

- Brooktrout Technology TR114+P4L or TR114+uP4L PCI analog voice-fax card(s). See the "Supported Voice-Fax Cards" section on page 3, for a list of supported cards.

Software Requirements

- Microsoft Windows 2000 Server, which is supported in English only. The locale must be set to English (United States), and the language settings must be set only to Western Europe and United States. (Choosing additional language settings is not supported.)

  Note that Windows 2000 Server is included with a Bridge server purchased from Cisco. If the server is not purchased from Cisco, Windows 2000 Server must be purchased separately.

- Windows 2000 Server Service Pack 4 for Bridge versions 3.0(3) and later.

  Service Pack 4 is recommended for Bridge versions 3.0(2) and 3.0(1). Service Pack 3, which is the required service pack for versions 3.0(2) and 3.0(1), is still supported for those versions but is not recommended.

- Microsoft Internet Explorer 6 with Service Pack 1.

- MSXML 3.0 with Service Pack 1.

- One of the following remote-access applications is required for Cisco TAC support:

  - Microsoft Windows Terminal Services. (Terminal Services is the default remote-access software for the Bridge server and is included with Windows 2000 Server.)

  - Symantec pcAnywhere version 10.0 or later. (Use an external modem with pcAnywhere.)

- Cisco Unity Bridge.

Bridge Networking Requirements

Bridge Networking is the feature that allows messaging between Cisco Unity and Avaya Octel systems on an Octel analog network by using the Cisco Unity Bridge. Refer to the "Bridge Networking Requirements" section of *Cisco Unity Networking Options Requirements* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/sysreq/netrq.htm.

PART 2: Supported Hardware for Use with Cisco Unity Bridge 3.0

Supported Voice-Fax Cards

Table 1 lists supported voice-fax cards for the Cisco Unity Bridge server.

The line cord that ships with Brooktrout TR114+P4L and Brooktrout TR114+uP4L voice-fax cards has an RJ-45 connector on one end and four single-pair RJ-11 connectors on the other end.

When installing multiple voice-fax cards in a single Bridge server, do not mix voice-fax cards intended for different countries. However, universal PCI and non-universal PCI voice-fax cards designed for the same country can be used in a single Bridge server.

Table 1   Supported Voice-Fax Cards for the Cisco Unity Bridge Server

Voice-Fax Card	Countries in Which Voice-Fax Card Is Approved for Use	Brooktrout SKU[1]
TR114+P4L or TR114+uP4L	United States and Canada	900-944-08 904-032-60
TR114+P4L or TR114+uP4L TBR-21 version	Austria, Belgium, Denmark, France, Finland, Germany, Greece, Iceland, Ireland, Italy, Liechtenstein, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, and Switzerland When purchased from Cisco, the card is also approved for use in: Czech Republic, Hungary, Poland, Saudi Arabia, Slovak Republic, South Africa, Turkey, and United Arab Emirates.	900-954-08 904-033-30
TR114+P4L or TR114+uP4L Japan version	Japan	908-954-84 904-032-90
TR114+P4L or TR114+uP4L Hong Kong version	Hong Kong	908-954-86 904-033-10

Table 1   Supported Voice-Fax Cards for the Cisco Unity Bridge Server (continued)

Voice-Fax Card	Countries in Which Voice-Fax Card Is Approved for Use	Brooktrout SKU[1]
TR114+P4Lor TR114+uP4L United Kingdom version (TBR-21 card with a UK cable)	United Kingdom	908-954-61 904-033-20
TR114+P4L or TR114+uP4L Australia version (Not approved for New Zealand)	Australia	908-954-85 904-033-00

1. The SKU, or stock-keeping unit, is the product identifier that Brooktrout assigned to the voice card. If you order the voice card from Brooktrout, you can use the SKU to ensure that you are ordering the correct version.

Supported Voice Messaging Systems

Avaya Octel analog networking is required for use with the Cisco Unity Bridge and Cisco Unity version 3.1(3) and later. Octel analog networking allows Cisco Unity—together with the Bridge—to exchange voice messages with other voice messaging systems that support Octel analog networking.

Note that the Bridge supports Octel analog networking protocol levels 2 and 3. Neither Octel digital networking nor the VOICENET protocol is supported.

The following voice messaging system is supported for use with Cisco Unity Bridge 3.0(x), with Cisco Unity 4.0(3) and later:

• Avaya Interchange

The following voice messaging systems are supported for use with Cisco Unity Bridge 2.x and 3.0(x), with Cisco Unity 3.1(3) and later:

• Avaya Octel 100 Messaging—When using the Octel 100 with Cisco Unity 4.0(3) or later with Bridge 3.x, the Bridge and Cisco Unity bridgehead can represent only one node in the Octel analog network. Although you can configure more than one Unity Node on the Bridge server, doing so is not supported.

• Avaya Octel 200/300

• Avaya Octel 250/350

• Avaya Unified Messenger

Supported Cisco Gateways

The Cisco Unity Bridge is designed to use analog connectivity to communicate with Octel nodes that use Avaya Octel analog networking, a DTMF-based protocol. The Bridge server contains voice-fax cards that are connected to a phone system. In a pure Cisco CallManager environment, the Bridge ports require a Cisco gateway to provide the analog connectivity.

When using a Cisco gateway between the Bridge and Cisco CallManager, choose from the supported gateways listed in Table 2.

Table 2   *Cisco Gateways Supported for Use with the Cisco Unity Bridge*

Gateway	Software Version	Mode	Recommended Settings
WS-X6624 (blade in Cisco Catalyst 65XX)	Cisco CallManager 3.2 or later TFTP load	MGCP	None
WS-X6608 (blade in Cisco Catalyst 65XX)	Cisco CallManager 3.2 or later TFTP load	MGCP	None
26XX IOS Gateway	12.2(8) or later	h.323	None
36XX IOS Gateway	12.2(8) or later	h.323	None
VG200 IOS Gateway	12.2(13) or later	MGCP	mgcp dtmf-relay codec all mode out-of-band
VG248 Gateway	1.3(1) or later	SCCP	In Cisco CallManager Administration, disable Call Waiting for each VG248 port. On the VG248, disable fax relay on each port. Call-forwarding tones can interrupt DTMF sequences and result in frequent call failures or retries. Disable forwarding tones where possible in Cisco CallManager Administration.

Where applicable for Cisco CallManager and gateways, set DTMF duration and interdigit timing to 100 milliseconds.

Support varies for Octel analog networking fax transmission over these gateways by using Fax Relay.

If you are using a Cisco DPA 7630/7610 Voice Mail Gateway to connect the Octel server(s) to Cisco CallManager, the Cisco DPA must be running version 1.3(1) ES3.3 or later.

Supported Optional Hardware

The following optional hardware is supported for use with Cisco Unity Bridge 3.0(x):

- An external modem is supported for use when pcAnywhere is selected as the Cisco TAC remote-access method. Note that modems must be customer-provided.

- Tape drives for system backup. If an MCS-EXT-DAT= SCSI-based tape drive kit is used with the Cisco MCS-7815-I1-ECS1 server, a PCI-based SCSI Host Bus Adaptor (HBA) is required. We recommend the MCS-EXT-SCSI= or IBM 71P8594 or 13N2249 card (also known as Adaptec model

29320LP or 29320ALP). Refer to the IBM ServerProven website for compatibility of other HBAs. Note that the SCSI HBA uses one of the MCS-7815I server PCI I/O slots, which reduces the maximum Bridge port density to 16 ports.

• IBM Remote Supervisor Adapter out-of-band management card, all versions. See also the "Additional Supported Software" section on page 8 for software that is supported for use in conjunction with the management card to remotely restart the Bridge server.

PART 3: Supported Software for Use with Cisco Unity Bridge 3.0

Compatibility Information

Refer to the following documents on Cisco.com for compatibility information:

• *Cisco Unity Networking Options Requirements* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/sysreq/netrq.htm.

• *Recommended and Supported Service Packs and Updates for Use with Cisco Unity and the Cisco Unity Bridge* at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/cmptblty/msupdate.htm.

Support Policy for Backup Software

Cisco support policy is that customers can deploy third-party backup software on the Cisco Unity Bridge server. However, Cisco expects that customers (or their systems integration partners) will have tested the interoperability of such products with the Bridge and Cisco Unity before the products are deployed, to mitigate the risk of problems being discovered within the production environment among the Bridge, Cisco Unity, and the third-party products loaded on the Bridge server.

If a customer calls Cisco TAC with a problem, a Cisco TAC engineer may require that such third-party software be turned off or even removed from the Bridge server during the course of troubleshooting. If it is determined that the interoperability between the third-party software and the Bridge or Cisco Unity was the root cause of the problem, then the third-party software will be required to be disabled or removed from the Bridge server until such time that the interoperability issue is addressed, so that the customer can continue to have a functional Bridge and Cisco Unity system.

Before installing any qualified Microsoft service pack on the Bridge server, confirm that the manufacturer of any optional third-party software or hardware that you plan to install on the Bridge server—or that is already installed—also supports the service pack for use with its product.

Supported Monitoring Software

The following monitoring software has been qualified by Cisco for use with Cisco Unity Bridge 3.0(x):

- Adiscon EventReporter
- Concord SystemEDGE, version 4.1

Support Policy for Monitoring Software

Cisco support policy is that customers can deploy third-party monitoring software on the Bridge server. However, Cisco expects that customers (or their systems integration partners) will have tested the interoperability of such products with the Bridge and Cisco Unity before the products are deployed, to mitigate the risk of problems being discovered within the production environment among the Bridge, Cisco Unity, and the third-party products loaded on the Bridge server.

If a customer calls Cisco TAC with a problem, a Cisco TAC engineer may require that such third-party software be turned off or even removed from the Bridge server during the course of troubleshooting. If it is determined that the interoperability between the third-party software and the Bridge or Cisco Unity was the root cause of the problem, then the third-party software will be required to be disabled or removed from the Bridge server until such time that the interoperability issue is addressed, so that the customer can continue to have a functional Bridge and Cisco Unity system.

Before installing any qualified Microsoft service pack on the Bridge server, confirm that the manufacturer of any optional third-party software or hardware that you plan to install on the Bridge server—or that is already installed—also supports the service pack for use with its product.

Supported Virus-Scanning Software

McAfee NetShield for Microsoft Windows NT and Windows 2000, version 4.5 and later, has been qualified by Cisco for use with Cisco Unity Bridge 3.0(x).

Support Policy for Virus-Scanning Software

Cisco support policy is that customers can deploy third-party virus-scanning software on the Cisco Unity Bridge server. However, Cisco expects that customers (or their systems integration partners) will have tested the interoperability of such products with the Bridge and Cisco Unity before the products are deployed, to mitigate the risk of problems being discovered within the production environment among the Bridge, Cisco Unity, and the third-party products loaded on the Bridge server.

If a customer calls Cisco TAC with a problem, a Cisco TAC engineer may require that such third-party software be turned off or even removed from the Bridge server during the course of troubleshooting. If it is determined that the interoperability between the third-party software and the Bridge or Cisco Unity was the root cause of the problem, then the third-party software will be required to be disabled or removed from the Bridge server until such time that the interoperability issue is addressed, so that the customer can continue to have a functional Bridge and Cisco Unity system.

Before installing any qualified optional service pack on the Bridge server, confirm that the manufacturer of any optional software or hardware that you plan to install on the Bridge server—or that is already installed—also supports the service pack for use with its product.

Additional Supported Software

The following optional software has been qualified by Cisco for use with Cisco Unity Bridge 3.0(x):

*   Cisco Security Agent for Cisco Unity Bridge, versions 1.1(x) and 1.0(1).

*   IBM Director is supported when it is used in conjunction with the IBM Remote Supervisor Adapter card to remotely restart the Bridge server.

Support Policy for Optional Software

Cisco support policy is that customers can deploy third-party software on the Cisco Unity Bridge server. However, Cisco expects that customers (or their systems integration partners) will have tested the interoperability of such products with the Bridge and Cisco Unity before the products are deployed, to mitigate the risk of problems being discovered within the production environment among the Bridge, Cisco Unity, and the third-party products loaded on the Bridge server.

If a customer calls Cisco TAC with a problem, a Cisco TAC engineer may require that such third-party software be turned off or even removed from the Bridge server during the course of troubleshooting. If it is determined that the interoperability between the third-party software and the Bridge or Cisco Unity was the root cause of the problem, then the third-party software will be required to be disabled or removed from the Bridge server until such time that the interoperability issue is addressed, so that the customer can continue to have a functional Bridge and Cisco Unity system.

Before installing any qualified optional service pack on the Bridge server, confirm that the manufacturer of any optional software or hardware that you plan to install on the Bridge server—or that is already installed—also supports the service pack for use with its product.

Unsupported Software

Software that has not been qualified for use with the Cisco Unity Bridge is not supported on the Bridge server. Cisco TAC will ask that it be removed during troubleshooting.

The following software is not supported on the Cisco Unity Bridge server:

*   Cisco IDS Host Sensor Agent.

*   Fax server software.

*   Software-based RAID.

*   Windows 2000 Advanced Server or DataCenter Server.

*   Windows Server 2003.