CHAPTER 4

Preparing for Installation

Revised July 3, 2012

The following sections describe the activities that you must complete before installing the Cisco TelePresence Exchange System software:

- Preinstallation Checklist, page 4-1
- Recommendations for Rack Mounting the Cisco TelePresence Exchange System and Other Solution Components, page 4-2
- Cabling Requirements, page 4-2
- VLAN Requirements and Restrictions, page 4-5
- Gathering Required Information Before Installation, page 4-5
- Setting Up the IMM, page 4-7

Preinstallation Checklist

Preinstallation Tasks	Checkoff
Rack mount the Cisco TelePresence Exchange System and solution components. See the "Recommendations for Rack Mounting the Cisco TelePresence Exchange System and Other Solution Components" section on page 4-2.	
Check that the power cords for your servers and monitors are securely attached and plugged in to working power sources. We recommend that you use an uninterruptible power supply (UPS) or dual power sources, especially for the database servers.	
Check that the servers are properly cabled. See the "Cabling Requirements" section on page 4-2.	
Check that you can access the Cisco TelePresence Exchange System servers (database, administration, and call engine) by using a local console.	
Verify that your Cisco TelePresence Exchange System installation DVD has the latest software version. If you are not sure, or if you do not have the DVD, download the latest software from the following URL, and burn the disk image onto a DVD: http://www.cisco.com/go/ctx-download.	

Preinstallation Tasks	Checkoff
Verify that you have all the required information before you begin the installation. See the "Gathering Required Information Before Installation" section on page 4-5.	
If you plan to enable the domain name system (DNS) client on each Cisco TelePresence Exchange System server, enter each hostname and IP address into the DNS servers, including the virtual hostname and virtual IP (VIP) address that are shared by the database servers.	
Verify that each VLAN that will have a Cisco TelePresence Exchange System server can connect to the NTP servers.	
(Optional) Set up the IMM for each server to enable remote control of each server. See the "Setting Up the IMM" section on page 4-7.	

Recommendations for Rack Mounting the Cisco TelePresence Exchange System and Other Solution Components

Note Leave a space of one-third of a rack unit (RU) between each unit to provide proper ventilation.

Use the following list to determine the rack position of each solution component, where item 1 is at the top of the rack:

1. Cisco router with interactive voice response (IVR)—two systems
2. Cisco Application Control Engine (ACE)—two systems
3. Cisco TelePresence Video Communication Server
4. Cisco TelePresence Manager
5. Cisco TelePresence Multipoint Switch
6. Keyboard-video-mouse (KVM) switch for console access to all systems
7. Power distribution unit (PDU)—two units for redundancy
8. Cisco Catalyst Switch—two systems
9. Cisco TelePresence Exchange System database servers—two servers
10. Cisco TelePresence Exchange System administration servers—two servers
11. Cisco TelePresence Exchange System call engine servers—two servers

Note The Cisco Unified Communications Manager and Cisco Session Border Controller are also part of the Cisco TelePresence Exchange System solution, but Cisco expects that those components are already installed and in use in the network and therefore does not provide rack-mounting recommendations.

Cabling Requirements

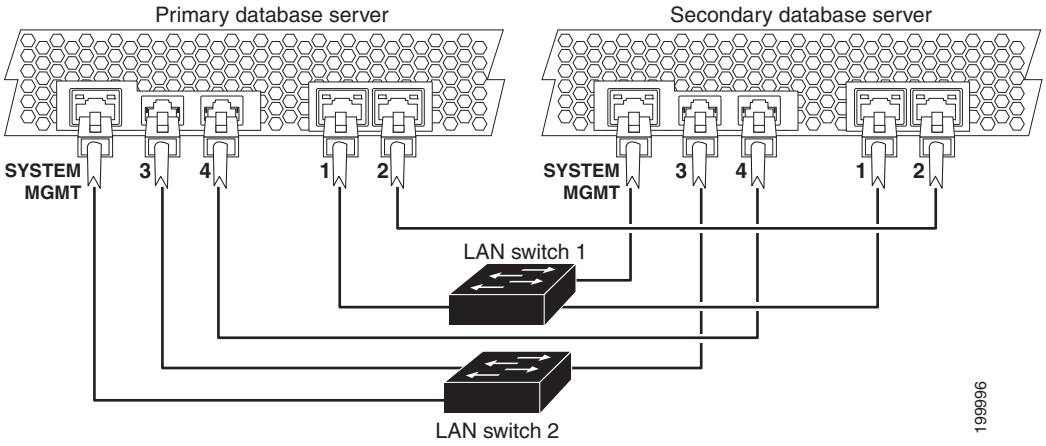
- Cabling Requirements for the Database Servers, page 4-3
- Cabling Requirements for the Administration and Call Engine Servers, page 4-4

Cabling Requirements for the Database Servers

To provide active/standby redundancy for the database servers, you must connect the primary and secondary database servers as shown in Figure 4-1.

Note You can use straight-through or crossover cables for these connections.

Figure 4-1 Required Cabling Between the Database Servers



Port label	Interface	Bonded Interface
1	Ethernet 0—application data and heartbeat	Bond 0
2	Ethernet 1—data replication between database servers	Bond 1
3	Ethernet 2—application data and heartbeat	Bond 0
4	Ethernet 3—data replication between database servers	Bond 1
SYSTEM MGMT (optional)	Integrated management module (IMM) You are not required to use the IMM interface, which enables remote control of the server.	—

When the servers are cabled as shown in Figure 4-1, the system remains connected if any one component or cable fails. Specifically:

- The NICs on each server are connected to separate switches.

  In each server, Ethernet 0 and Ethernet 1 are on one NIC, while Ethernet 2 and Ethernet 3 are on a second NIC.
- On each database server, the Cisco TelePresence Exchange System software automatically implements NIC teaming to bond the following interfaces together:
  - Ethernet 0 with Ethernet 2.
  - Ethernet 1 with Ethernet 3.
- Each NIC has a heartbeat connection to the redundant server.
- You are not required to use the IMM interfaces, but if you do, then we recommend that you cable them as shown in Figure 4-1 to connect the IMM interfaces to separate switches.

Related Topics

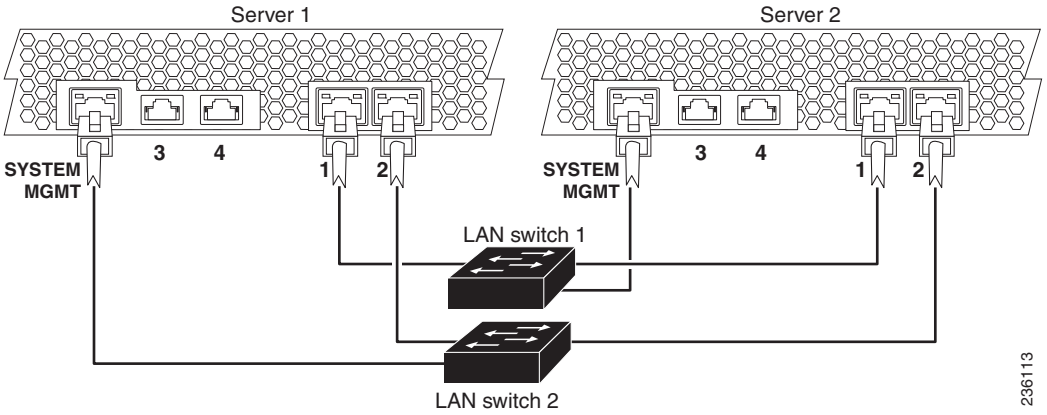
- Setting Up the IMM, page 4-7

Cabling Requirements for the Administration and Call Engine Servers

To provide switch and network redundancy for the administration servers and call engine servers, you must connect the servers as shown in Figure 4-2.

Note You can use straight-through or crossover cables for these connections.

Figure 4-2 Required Cabling Between Administration Servers and Between Call Engine Servers



Port label	Interface	Bonded Interface
1	Ethernet 0—data	Bond 0
2	Ethernet 1—data	Bond 0
3	Ethernet 2—currently not used	—
4	Ethernet 3—currently not used	—
SYSTEM MGMT (optional)	Integrated management module (IMM) You are not required to use the IMM interface, which enables remote control of the server.	—

On each administration server and call engine server, the Cisco TelePresence Exchange System software bonds Ethernet 0 with Ethernet 1. When the servers are cabled as shown in Figure 4-2, the bonded interface is connected to both LAN switches.

You are not required to use the IMM interfaces, but if you do, then we recommend that you connect the IMM interfaces to separate LAN switches.

VLAN Requirements and Restrictions

Apply the following requirements, restrictions, and recommendations as you assign IP addresses to the Cisco TelePresence Exchange System:

- You cannot assign any IP addresses in the 10.0.0.*x*/8 address space.
- The data network interfaces of all nodes in the Cisco TelePresence Exchange System server cluster must be on the same VLAN. Therefore, the same VLAN must be used for all of the following interfaces:
  - Ethernet 0 and Ethernet 2 of both database servers.
  - Ethernet 0 and Ethernet 1 of both administration servers and both call engine servers.

Note This VLAN is the inside network VLAN that you will configure on the Cisco Application Control Engine (ACE) in a redundant or non-redundant ACE configuration.

- The data VLAN of the Cisco TelePresence Exchange System must be separate from the data VLANs that are used by the following solution components:
  - Cisco Unified Communications Manager
  - Cisco Session Border Controller
  - Cisco TelePresence Multipoint Switch
  - Cisco Router with Integrated Voice Response (IVR)
- You must be able to ping the default gateway from each of the Cisco TelePresence Exchange System servers.
- If you use the integrated management module (IMM) interfaces on the Cisco TelePresence Exchange System servers, we recommend that you use a separate system management VLAN for the IMM interfaces.

Note Make sure that packets can be routed between all of the VLANs that you implement for the Cisco TelePresence Exchange System solution.

Gathering Required Information Before Installation

Complete the worksheets in Appendix A, "Installation Worksheets," as you collect the following information. Before you proceed, however, read the "VLAN Requirements and Restrictions" section on page 4-5.

- Unique hostnames:
  - One hostname for each of the database, call engine, and administration servers.
  - One virtual hostname to be shared by the two database servers.
- Unique IP addresses and their subnet masks:
  - One IP address for each of the database, call engine, and administration servers.
  - One virtual IP (VIP) address to be shared by the two database servers. The database VIP is the only address that the network recognizes for the database servers, only one of which is active at any given time.

  - (Optional) One IP address for each integrated management module (IMM) interface. The IMMs enable remote control of the servers.
- IP addresses of the default gateways:
  - IP address of the default gateway for the data network interfaces. (This address is the IP address of the inside network interface VLAN of the Cisco Application Control Engine.)
  - (Optional) IP address of the default gateway for the IMM interfaces.
- Administrator usernames and passwords:
  - For accessing the CLI of each database, administration, and call engine server. You must use the same administrator username and password on all Cisco TelePresence Exchange System servers, because the administration servers also use the administrator credentials over SSH to get the status of all nodes in the server cluster.
  - (Optional) For accessing each IMM interface, which enables remote control of the server.
- A security password.

  The database server uses this password to authenticate data requests from the administration and call engine servers. Therefore, you must define the same security password for the database, administration, and call engine servers.

  Note After you configure the security password on a server, you cannot change it without reinstalling the server.

- (Optional) Domain Name System (DNS) information:
  - IP address of a primary DNS server.
  - (Optional) IP address of a secondary DNS server.
  - Domain name.
- IP addresses, hostnames, or pool names for external Network Time Protocol (NTP) clocking sources. Cisco recommends that you use at least three external NTP clocking sources.

  You must configure the same NTP entries on the database, call engine, and administration servers.
- For the SIP load balancer, which is the Cisco Application Control Engine (ACE):
  - VIP address.
  - Port number—Cisco recommends that you use the default port 5060.
- For generating locally significant certificates (LSC) for each database, call engine, and administration server:
  - Organization—typically your company name.
  - Unit—typically your business unit and department.
  - Location—typically the building, floor, and rack in which the server is installed.
  - State and Country—where the server is located.

  Use the following guidelines to determine each entry for generating LSCs:
  - Refer to your company guidelines for format and entry requirements.
  - Supported characters include alphanumeric, space, and the following special characters: .,-_:;{}()[]#.
  - Each field supports up to 255 characters.

Setting Up the IMM

You may choose to set up the IMM on each Cisco TelePresence Exchange System server to enable you to control each server remotely; this remote access is available whenever the server is plugged in to a working power source, even if the server is turned off.

To set up the IMM, complete the following tasks:

- Setting Up the IMM Network Connection, page 4-7
- Creating an IMM User Account, page 4-8
- Enabling SSH for the IMM, page 4-9

Setting Up the IMM Network Connection

Before You Begin

Find your completed Appendix A, "Installation Worksheets."

Procedure

Step 1 Attach a console to the console port of the server.

The console port is located on the front of the server.

Step 2 Turn the server on by pressing the power button that is located on the front of the server.

After approximately one minute, an IBM System x screen is displayed on the console.

Step 3 Watch for the **F1 <setup>** option to appear at the bottom of the IBM System x screen. This may take another minute or two.

Step 4 Press the **F1** key as soon as the option appears.

If the option disappears before you press F1, then turn the server off and on, and try again.

Tip At any time in the following steps, if you accidentally end up in the wrong screen or select the wrong field, press the **Esc** key to back out of that screen or field selection.

Step 5 In the System Configuration and Boot Management screen, select **System Settings**.

Step 6 In the System Settings screen, select **Integrated Management Module**.

Step 7 In the Integrated Management Module screen, select **Network Configuration**.

Step 8 In the Network Configuration screen, select the **DHCP Control** field value.

Step 9 In the DHCP Control field, select the **Static IP** option.

Step 10 Enter the IP address, subnet mask, and default gateway IP address for the IMM interface.

Step 11 Select **Save Network Settings**.

Step 12 Press the **Enter** or **Return** key to continue.

Step 13 Press the **Esc** key repeatedly to exit each setup screen.

Step 14 When prompted, press the **Y** key to exit the setup utility.

The server reboots.

Step 15 Repeat this procedure for the redundant server.

What to Do Next

Proceed to the "Creating an IMM User Account" section on page 4-8.

Creating an IMM User Account

Before You Begin

- Complete the procedure in the "Setting Up the IMM Network Connection" section on page 4-7.
- Complete this task by using one of the following web browsers:
  - Microsoft Internet Explorer version 6.0 or later with the latest Service Pack
  - Mozilla Firefox version 1.5 or later
- Make sure that the browser allows popup windows from the IMM.

Procedure

Step 1 Point a web browser to the IP address of the IMM interface.

Step 2 Log in to the IMM web interface with following default username and password:

username: **USERID**

password: **PASSW0RD** (Enter a zero instead of the letter O.)

Step 3 (Optional) Set the inactive session timeout value.

Step 4 Click **Continue**.

Step 5 In the left navigation area, select **System > IMM Control > Login Profiles**.

Step 6 In the Login Profiles area, click **Add User**.

Step 7 In the **Login ID** field, enter the username.

The username must have between 4 and 16 characters, and may include uppercase and lowercase letters, numbers, periods, and underscores.

Step 8 In the **Password** and **Confirm password** fields, enter a password that contains a minimum of five characters, one of which must be a nonalphabetic character. You cannot use a null or empty password.

Step 9 Select the **Supervisor** authority level, which provides unlimited access.

Step 10 Click **Save**.

Step 11 (Optional) To prevent unauthorized access, change the password for the default IMM user account by completing these steps:

a. In the Login Profiles area, click the **USERID** Login ID.

b. Enter a new password into the **Password** and **Confirm password** fields.

c. Click **Save**.

What to Do Next

Proceed to the "Enabling SSH for the IMM" section on page 4-9.

Enabling SSH for the IMM

The secure shell (SSH) provides secure access to the command-line interface (CLI) and the serial redirect features of the IMM. An SSH user is authenticated by exchanging the username and password, which are sent after the encryption channel is established. The username and password can be one of the 12 username and password pairs that the server stores locally, or they can be stored on a lightweight directory access protocol (LDAP) server. Public key authentication is not supported.

Before You Begin

- Complete the procedure in the "Creating an IMM User Account" section on page 4-8.
- Complete this task by using one of the following web browsers:
  - Microsoft Internet Explorer version 6.0 or later with the latest Service Pack
  - Mozilla Firefox version 1.5 or later
- Make sure that the browser allows popup windows from the IMM.

Procedure

Step 1 In the IMM web interface, choose **System > IMM Control > Security**.

Step 2 Scroll down to the **SSH Server Key Management** area.

Step 3 Click **Generate SSH Server Private Key**.

An SSH server key is used to authenticate the identity of the SSH server to the client.

Step 4 Wait for the progress bar to indicate completion.

Step 5 In the **SSH Server** field, select **Enabled**.

Step 6 Click **Save**.

Step 7 In the left navigation area, select **System > IMM Control > Restart IMM**.

Step 8 Click **Restart**.

Step 9 Click **OK** to confirm the restart.