AG250 Application Gateway Server Hardware Installation Guide Release 2.1 (Service Pack)

16-300260
Issue 2.1
April 2006

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language as well as information regarding support for this product, while under warranty, is available through the following Web site: http://www.avaya.com/support.

Trademarks

DEFINITY is a registered trademark of Avaya, Inc. MultiVantage is a trademark of Avaya, Inc. Windows, Windows 2000, and Windows NT are trademarks or registered trademarks of Microsoft Corporation.

Preventing Toll Fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there may be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Fraud Intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, in the United States and Canada, call the Technical Service Center's Toll Fraud Intervention Hotline at 1-800-643-2353.

Disclaimer

Avaya is not responsible for any modifications, additions or deletions to the original published version of this documentation unless such modifications, additions or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

How to Get Help

For additional support telephone numbers, go to the Avaya support Web site: http://www.avaya.com/support. If you are:

- Within the United States, click the *Escalation Management* link. Then click the appropriate link for the type of support you need.
- Outside the United States, click the *Escalation Management* link. Then click the *International Services* link that includes telephone numbers for the international Centers of Excellence.

Providing Telecommunications Security

Telecommunications security (of voice, data, and/or video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based) or asynchronous (character-, message-, or packet-based) equipment or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company (including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Responsibility for Your Company's Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you - Avaya's customer system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products

TCP/IP Facilities

Customers may experience differences in product performance, reliability and security depending upon network configurations/design and topologies, even when the product performs as warranted.

Standards Compliance

Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment will be the responsibility of the user. Pursuant to Part 15 of the Federal Communications Commission (FCC) Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. could void the user's authority to operate this equipment.

To order copies of this and other documents:

Call: Avaya Publications Center
Voice 1.800.457.1235 or 1.207.866.6701
FAX 1.800.457.1764 or 1.207.626.7269

Write: Globalware Solutions
200 Ward Hill Avenue
Haverhill, MA 01835 USA
Attention: Avaya Account Management

E-mail: totalware@gwsmail.com

For the most current versions of documentation, go to the Avaya support Web site: http://www.avaya.com/support

Contents

Preface

This preface describes who should read the *Application GatewayHardware Installation Guide*, how it is organized, and its document conventions.

Audience

This installation guide is intended for service technicians who will install the Application Gateway and for administrators who need to troubleshoot the hardware.

Organization

This guide is organized as follows:

Chapter/Appendix	Title	Description
Chapter 1	Installing the Application Gateway	Contains pre-installation and installation procedures. Provides a general overview to the network configurations in which you might install the Application Gateway.
Chapter 2	Specifications and BIOS Self-Test Messages	Contains specifications and describes BIOS beep codes and error messages.

Conventions

This guide uses the following conventions:

Convention	Description
boldface font	Commands and HTML element names are in **boldface**.
`boldface screen` font	Information you must enter is in `boldface screen` font.

Notes use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or other important information.

Tips use the following conventions:

Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information.

Cautions use the following conventions:

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

Related Documentation

For additional information about the Application Gateway, refer to these guides:

- *Application Gateway Server Administration Guide*
- *Application Gateway Server Release Notes*

Chapter 1

Installing the Application Gateway

The Avaya Application Gateway Server is an appliance that transforms and delivers data and enhanced voice applications to a variety of microbrowser devices, including IP phones, Wireless Application Protocol (WAP) phones, and Personal Digital Assistants (PDAs). The Application Gateway transforms applications according to built-in transformation rules, as well as transformation rules created in the companion PC-based application, Design Studio.

After connecting Application Gateways into your network, phone users immediately benefit from the built-in transformation capabilities of the Application Gateway, gaining access to applications built for desktop browsers. The Application Gateway determines the type of device making a connection and formats the requested application to match the format and constraints of the device. Design Studio users supplement the built-in transformations to fine-tune the applications for microbrowser use.

Note For detailed information on Application Gateway features, configuration, and security considerations, refer to the *Application Gateway Administration Guide*.

The following topics describe how to prepare for and perform Application Gateway installation:

Preparing for Installation

The following topics explain the pre-installation requirements:

Verifying the Box Contents

The box in which your Application Gateway is shipped contains the following components. If something is missing, please contact support at http://www.avaya.com/support.

- Application Gateway device
- Power cord
- Null-modem cable
- Application Gateway CD-ROM (backup of pre-installed Application Gateway Server Software)
- Design Studio CD-ROM (installer)
- Broadcast Server CD-ROM (installer)
- Product documentation:
  - This installation guide
  - *Legal Information*
  - *Pre-Installation Checklist*
  - *Quick Start Guide*
  - *Release Notes*

Materials and Information Needed for Installation

Before installing the Application Gateway, collect the following materials:

- One network cable to connect the Application Gateway to a LAN (two cables are required if the Application Gateway will straddle two networks)
- A computer capable of hosting terminal console communication through a serial port

Collect the network information you need for the installation, using the *Pre-Installation Checklist* provided with the Application Gateway.

Note If the Application Gateway is connected to a server load balancer, your network administrator will need to determine, based on your network configuration, whether any server load balancer settings will need to be adjusted to operate with the Application Gateway.

Locating Application Gateways in Your Enterprise Network

This topic provides information intended to help you determine where to locate Application Gateways in your network. For more information about Application Gateways and your network, refer to the *Network Integration Guide*.

The location of an Application Gateway in a network is largely based on the configuration of the existing network. The flexible deployment of the Application Gateway enables you to connect it to application servers, routers, firewalls, and switches.

An Application Gateway that supports Phone Productivity Pack applications is typically connected to a router through the Application Gateway Interface 0 port (LAN1). If the Application Gateway straddles networks, you will need to use both Interfaces 0 and 1 to connect the Application Gateway to the networks.

An Application Gateway that is used to transform applications for delivery to mobile devices requires a configuration that permits secure access outside of the firewall.

Regardless of the network deployment chosen, the only requirements that must be met to ensure correct operation are as follows:

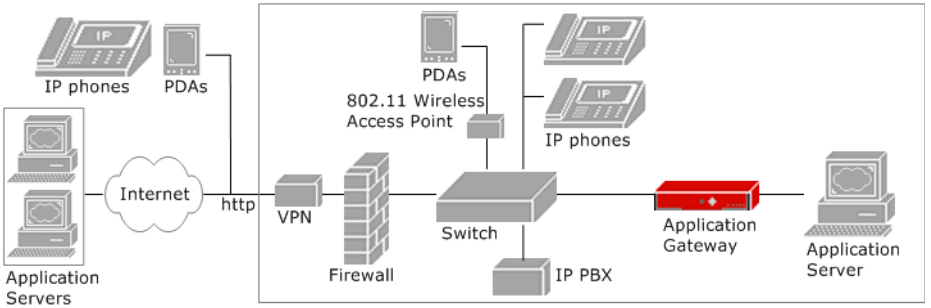
- The client devices (IP telephones; mobile devices) must be able to see the Application Gateway on the network.
- The Application Gateway must be able to see the requested content. Content may be generated by servers on the local network and the Web.

The following sections describe some possible deployment scenarios.

Connection to Application Server (In-Line)

In this configuration you connect an Application Gateway directly to an application server, as shown in Figure 1.

Figure 1 Application Gateway Connected In-Line to an Application Server

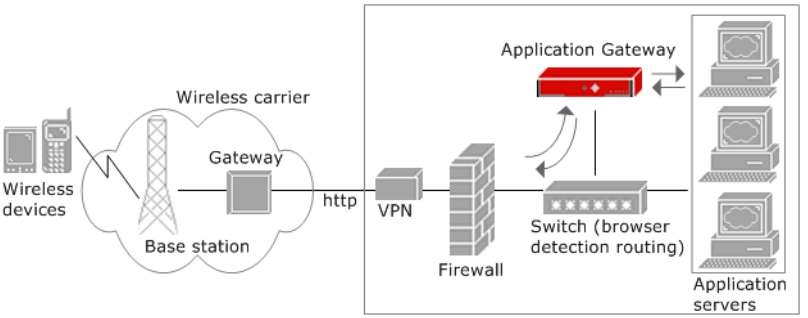


This configuration is recommended for sites with one application server or for sites that designate specific IP addresses for traffic. All traffic goes through the Application Gateway, which passes HTML/XML requests to the application server and handles requests from IP phones or other microbrowser devices.

Connection to Switch

In this configuration you connect the Application Gateway and application servers to a switch, as shown in Figure 2.

Figure 2 Application Gateway Connected to Switch



The switch is set up to direct requests for transformed applications according to browser type or requested URLs, as follows.

- Browser-detection routing

  URL requests, which are the same from desktop and microbrowser users, are directed by the switch to an application server. The application server checks the browser type associated with the request. If the request is from a microbrowser, the application server redirects the request back to the requesting device, pointing it to the Application Gateway.

- Directed URL routing

  The switch directs requests based on URL. URLs that are associated with sites intended for desktop browsers are directed to an application server. Special URLs that are set up for transformed sites are directed to the Application Gateway.

Note For information on other features of the Application Gateway, such as session and connection management, performance, cookie proxying, and security, see the *Application Gateway Administration Guide*.

Rack Mounting the Application Gateway

The enclosed rack-mounting kit can be used to install the Application Gateway in a four-post or two-post rack.

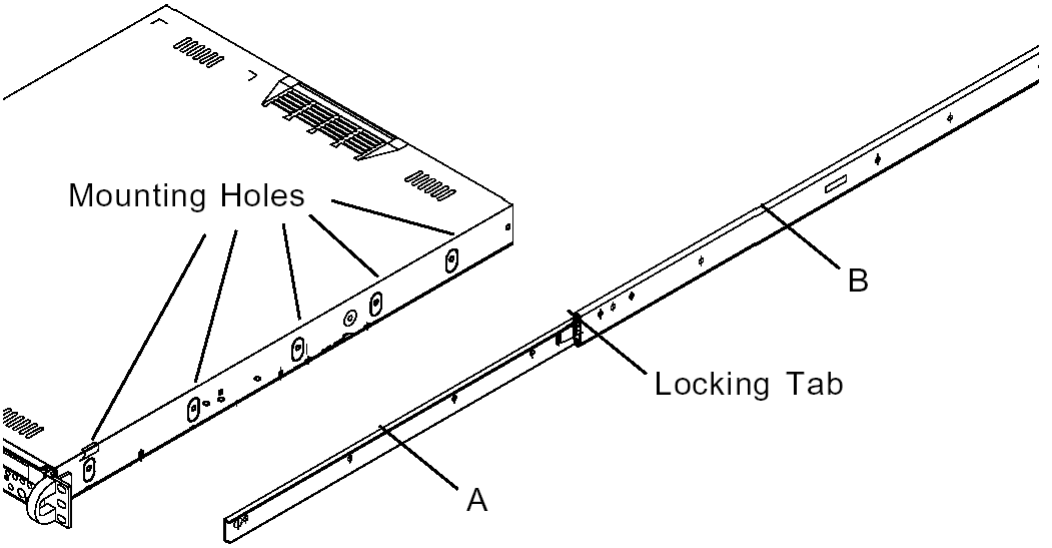
Separating the Rail Sections

The rack-mounting kit includes two sets of rail assemblies, two rail mounting brackets, and the mounting screws that you will need to install the system into the rack. Follow the steps in the order given to complete the installation process in a minimum amount of time. Please read this guide in its entirety before you begin the installation.

Each of the rail assemblies consist of two sections: an inner fixed chassis rail that secures to the server (A) and an outer fixed rack rail that secures directly to the rack itself (B), as illustrated below. A sliding rail guide sandwiched between the two should remain attached to the fixed rack rail. You must separate the A rail from the B rail to begin the installation.

To separate the A and B rails:

1. Pull the fixed chassis rail (A) out as far as possible — you should hear a click sound as a locking tab emerges from inside the rail assembly and locks the inner rail.
2. Depress the locking tab to pull the inner rail completely out. Do this for both the left and right side rack rail assemblies.

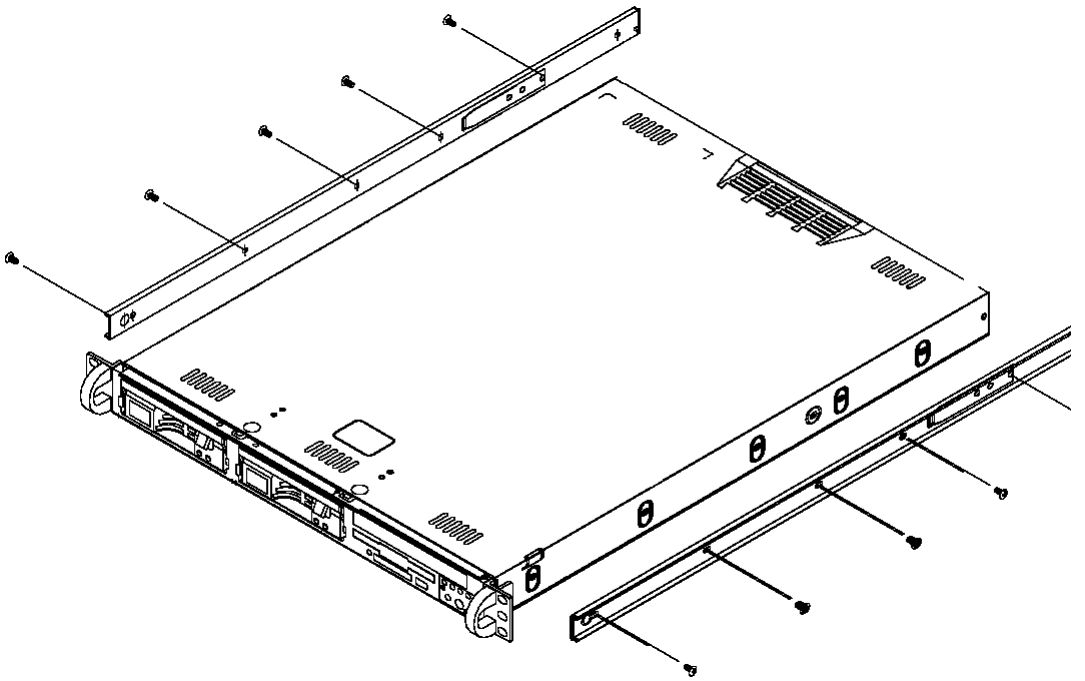


Connecting the Chassis Rails to the Server

Both chassis rails have a locking tab, which serves two functions. The first function is to lock the server into place when installed and pushed fully into the rack, which is its normal position. The second function is to lock the server in place when the rail is fully extended from the rack. This prevents the server from coming out of the rack when you pull it out for servicing.

To connect the chassis rails to the server:

1. Position the fixed chassis rail sections (A) that you just removed along the side of the server, making sure the five screw holes align. Note that the rails are left/right specific.
2. Screw the rail securely to the side of the chassis, as illustrated below.
3. Repeat this procedure for the other rail on the other side of the chassis.
4. If you are installing the server into a two-post rack, also attach the rail brackets.



Connecting the Rack Rails to the Rack

Determine where you want to place the server in the rack. Position the fixed rack rail/sliding rail guide assemblies (B) at the desired location in the rack, keeping the sliding rail guide facing the inside of the rack. Screw the assembly securely to the rack using the brackets provided. Attach the other assembly to the other side of the rack, making sure that both are at the same height and have the rail guides facing inward.

Installing the Server into a Four-Post Rack

You should now have rails attached to both the server and the rack unit. The next step is to install the server into the rack.

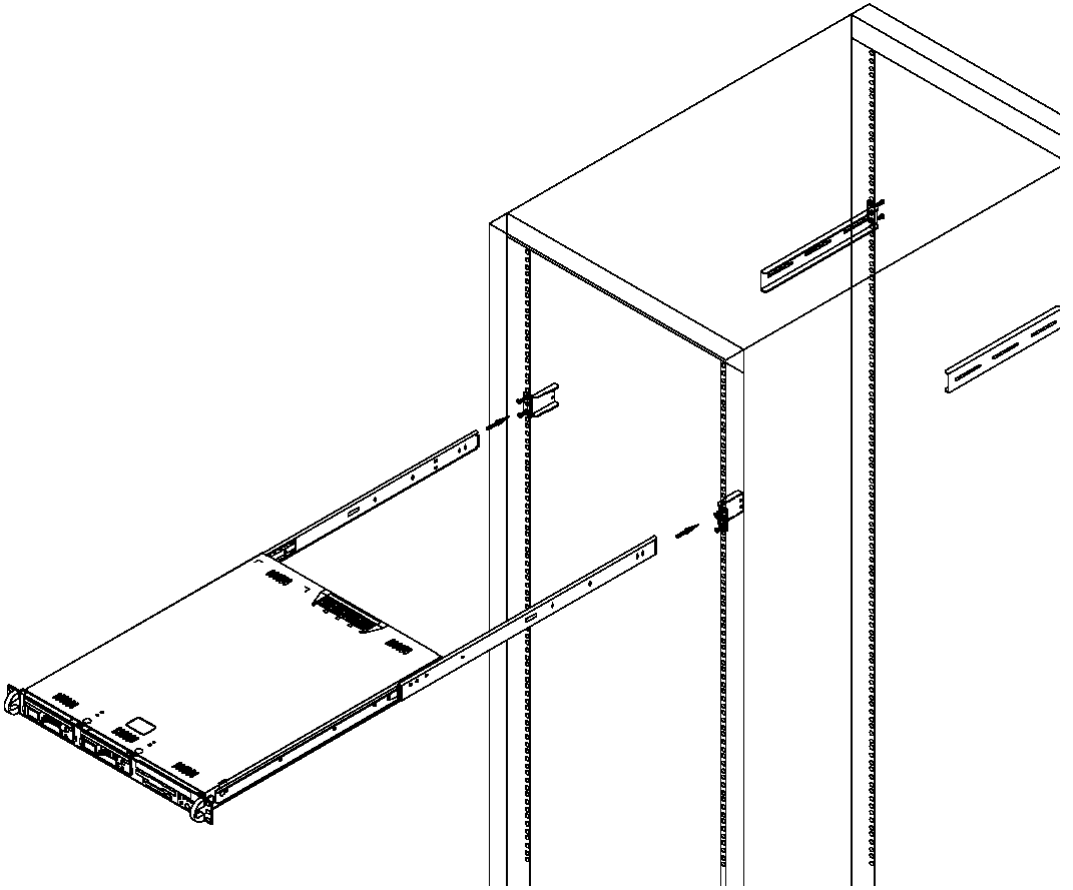
To install the server into a four-post rack:

1 Line up the rear of the chassis rails with the front of the rack rails.

2 Slide the chassis rails into the rack rails, keeping the pressure even on both sides (you may have to depress the locking tabs when inserting). Refer to the illustration below.

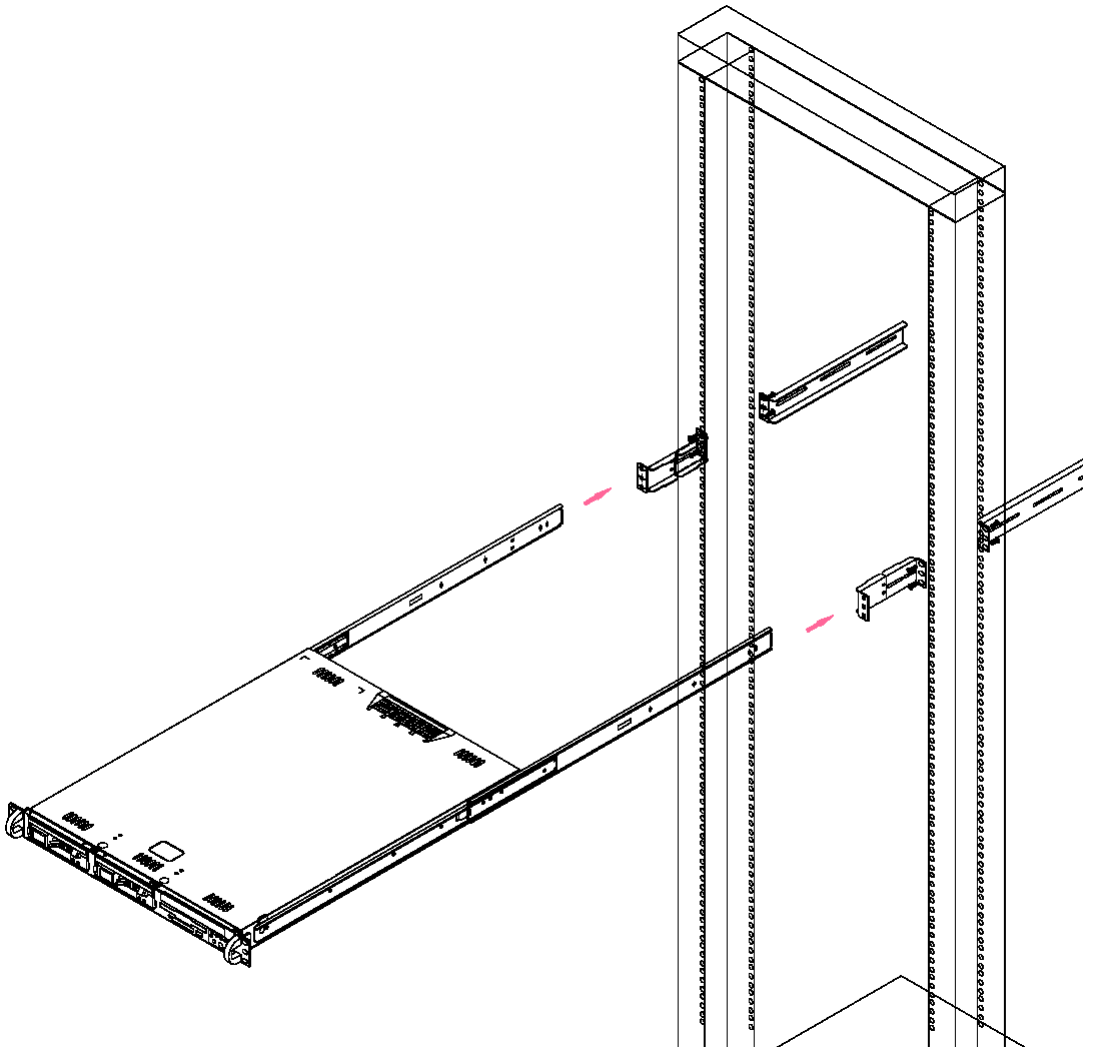
3 When the server has been pushed completely into the rack, you should hear the locking tabs click.

4 Finish by inserting and tightening the thumbscrews that hold the front of the server to the rack.



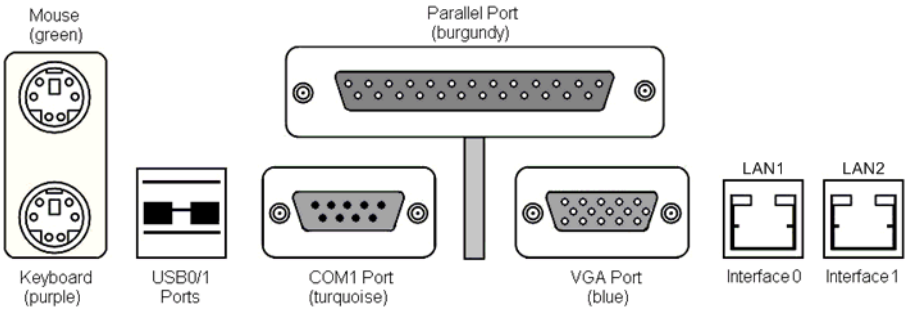
Installing the Server into a Two-Post Rack

If you are installing the server into a two-post (Telco) rack, follow the directions given on the previous pages for rack installation. The only difference in the installation procedure will be the positioning of the rack brackets to the rack. They should be spaced apart just enough to accommodate the width of the telco rack, as illustrated below.



Installing the Application Gateway

When installing the Application Gateway, refer to the following illustration for port locations.



To install the Application Gateway:

1. Install the Application Gateway in a rack (if rack-mounted).
2. Connect the power cord to the AC power receptacle.
3. Connect the 10/100 RJ45 NIC connectors located on the Application Gateway back panel as follows.
   - If the Application Gateway can access the connected device (router, application server, etc.) from the same subnet as it receives client requests, use one network cable. Connect Application Gateway interface port 0 (LAN1) to your network. This is the typical configuration.
   - If the Application Gateway will straddle two networks, use two network cables:
     - Connect Application Gateway Interface 0 (LAN1) to the client-side network.
     - Connect Application Gateway Interface 1 (LAN2) to the server-side network, directly or indirectly.
4. Connect the null-modem cable to the 9-pin serial port on the Application Gateway and connect the cable to a computer that is capable of running terminal emulation software.

5 On the computer, start a terminal emulation application. For example, start HyperTerminal.

6 When you create a connection using HyperTerminal, you will be prompted for Port Settings. Set the serial connection to 9600 bits per second, 8 data bits, no parity, and 1 stop bit; hardware flow control is optional. (Ctrl-u deletes a line in the terminal window.)

7 Power on the Application Gateway.

After about ten minutes, the Application Gateway Serial Console appears on the computer terminal. You are now ready to configure the Application Gateway with your network, as described in "Configuring the Application Gateway for the First Time," page 13.

Configuring the Application Gateway for the First Time

The first time that you power on the Application Gateway, you are prompted for basic connection information. You will need to know the following information:

- IP address and netmask for the client-facing interface port
- IP address of the gateway device

To configure the Application Gateway for the first time:

1 In the Application Gateway serial console, enter the default login **root** and the default password **rootadmin**.

2 Type **0** and press **Enter** to choose Express Setup.

3 Enter the IP address and netmask for Interface 0 when prompted.

Note The Application Gateway does not work with Dynamic Host Configuration Protocol (DHCP). You must use static IP addresses for the Application Gateway.

4 Enter the IP address of the gateway device when prompted.

A list of the settings displays.

5 Verify that the settings are correct.

If they are correct, type **y** when asked to commit your changes. The Application Gateway restarts and displays the login prompt.

If they are not correct, type **n** when asked to commit your changes, then type **0** (Express Setup) to change settings.

6 To test the connection, verify that the Application Gateway can ping connected network devices: Type **1** (Ping), press **Enter**, and enter the IP address that you want to ping.

If the ping is successful, you have completed the initial configuration. If the ping is not successful, check your connections, return to the serial console Main Menu, and type 0 (Express Setup) to change settings as needed.

7 To complete the Application Gateway configuration, refer to the *Administration Guide*.

Third-Party Software

We recommend that you not install any third-party software on the Application Gateway. Problems caused by the installation of third-party software are not supported.

.

Chapter 2

Specifications and BIOS Self-Test Messages

Specifications

Processor	Pentium 4 2.8Ghz HyperThreading 800MHz front side bus
Motherboard	Intel i875 chipset
Memory	1 gigabyte PC3200 (400MHz)
Power supply	260W,
AC Voltage	100 - 240V, 60-5 Hz, 5-3 Amp
Maximum BTU/hr	887.15
System cooling fan	1 x 90mm blower fan
Drive bay	1 x 3.5" internal drive bay; 40 gigabytes
Drives	1 x Slim 32x CD-ROM drive 1 x 3.5" 1.44MB floppy drive
NICs	Dual Intel gigabit NICs
System monitoring	LED indicators for power on, network activity, IDE HDD activity, overheat warning, and drive failure
Chassis size	16.8" (w) x 1.7" (h) x 14.1" (d); 23 pounds
Accessories	Rack-mounting kit

BIOS Self-Test Messages

During the Power-On Self-Test (POST), the BIOS checks for errors. If the BIOS detects an error that requires correction, the BIOS activates an alarm or display a message, as follows:

- POST beep codes
  - A single long beep followed by two short beeps indicates that a video error has occurred and that the BIOS cannot initialize the video screen to display any additional information.
  - A single long beep that sounds repeatedly indicates that a Rambus error has occurred.
- Error messages

  If a message is displayed, it will be accompanied by the following: PRESS F1 TO CONTINUE, CTRL-ALT-ESC OR DEL TO ENTER SETUP

  One or more of the following messages may be displayed if the BIOS detects an error during the POST. This list includes messages for both the ISA and the EISA BIOS.

CMOS BATTERY HAS FAILED

The CMOS battery is no longer functional. It should be replaced.

CMOS CHECKSUM ERROR

The CMOS checksum is incorrect. This can indicate that CMOS has been corrupted. This error may have been caused by a weak battery. Check the battery and replace if necessary.

DISK BOOT FAILURE, INSERT SYSTEM DISK AND PRESS ENTER

No boot device was found. This could mean that either a boot drive was not detected or the drive does not contain the proper system boot files. Insert a system disk into Drive A: and press <Enter>. If you assumed the system would boot from the hard drive, make sure the controller is inserted correctly and all cables are properly attached. Also make sure the disk has been formatted as a boot device. Then reboot the system.

DISKETTE DRIVES OR TYPES MISMATCH ERROR - RUN SETUP

The type of diskette drive installed in the system is different from the CMOS definition. Run Setup to reconfigure the drive type correctly.

DISPLAY SWITCH IS SET INCORRECTLY

The display switch on the motherboard can be set to either monochrome or color. This indicates that the switch is set to a different setting than indicated in Setup. Determine which setting is correct, and then either turn off the system and change the jumper or enter Setup and change the VIDEO selection.

DISPLAY TYPE HAS CHANGED SINCE LAST BOOT

Since last powering off the system, the display adapter has been changed. You must configure the system for the new display type.

ERROR ENCOUNTERED INITIALIZING HARD DRIVE

The hard drive cannot be initialized. Be sure the adapter is installed correctly and all cables are correctly and firmly attached. Also be sure the correct hard drive type is selected in Setup.

ERROR INITIALIZING HARD DISK CONTROLLER

Cannot initialize the controller. Make sure the cord is correctly and firmly installed in the bus. Be sure the correct hard drive type is selected in Setup. Also check to see if any jumper needs to be set correctly on the hard drive.

KEYBOARD ERROR OR NO KEYBOARD PRESENT

Cannot initialize the keyboard. Make sure the keyboard is attached correctly and no keys are being pressed during boot up. If you are intentionally configuring the system without a keyboard, set the error halt condition in Setup to HALT ON ALL, BUT KEYBOARD. This will cause the BIOS to ignore the missing keyboard and continue the boot.

Memory Address Error at ...

Indicates a memory address error at a specific location. You can use this location along with the memory map for your system to find and replace the bad memory chips.

Memory parity Error at ...
Indicates a memory parity error at a specific location. You can use this location along with the memory map for your system to find and replace the bad memory chips.

Memory Verify Error at ...
Indicates an error verifying a value already written to memory. Use the location along with your system's memory map to locate the bad chip.

OFFENDING ADDRESS NOT FOUND
This message is used in conjunction with the I/O CHANNEL CHECK and RAM PARITY ERROR messages when the segment that has caused the problem cannot be isolated.

OFFENDINGSEGMENT:
This message is used in conjunction with the I/O CHANNEL CHECK and RAM PARITY ERROR messages when the segment that has caused the problem has been isolated.

PRESS A KEY TO REBOOT
This will be displayed at the bottom screen when an error occurs that requires you to reboot. Press any key and the system will reboot.

PRESS F1 TO DISABLE NMI, F2 TO REBOOT
When BIOS detects a Non-maskable Interrupt condition during boot, this will allow you to disable the NMI and continue to boot, or you can reboot the system with the NMI enabled.

RAM PARITY ERROR - CHECKING FOR SEGMENT ...
Indicates a parity error in Random Access Memory.

SYSTEM HALTED, (CTRL-ALT-DEL) TO REBOOT ...
Indicates the present boot attempt has been aborted and the system must be rebooted. Press and hold down the CTRL and ALT keys and press DEL.

Hard Disk(s) fail (80) ® HDD reset failed

Hard Disk(s) fail (40) ® HDD controller diagnostics failed.

Hard Disk(s) fail (20) ® HDD initialization error.

Hard Disk(s) fail (10) ® Unable to recalibrate fixed disk.

Hard Disk(s) fail (08) ® Sector Verify failed.

Keyboard is locked out - Unlock the key.
BIOS detect the keyboard is locked. P17 of the keyboard controller is pulled low.

Keyboard error or no keyboard present.
Cannot initialize the keyboard. Make sure that the keyboard is attached correctly and no keys are being pressed during the boot.

Manufacturing POST loop.
System will repeat POST procedure infinitely while the P15 of keyboard controller is pulled low. This is also used for M/B burn in testing.

BIOS ROM checksum error - System halted.
The checksum of ROM address F0000H-FFFFFH is bad.

Memory test fail..
BIOS reports the a memory test fail if the onboard memory has an error.

Part Number: 300-60-00