Sun Cobalt™ RaQ™ XTR server appliance

User Manual

Sun Cobalt™

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at `http://www.sun.com/patents` and one or more additional patents or pending patent applications in the U.S. and other countries.

Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Sun, Sun Microsystems, the Sun Logo, Sun Cobalt, the Sun Cobalt Logo, Sun Cobalt RaQ, Java and JDK are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd.

Netscape and Netscape Navigator are trademarks or registered trademarks of Netscape Communication Corporation in the United States and other countries.

Legato NetWorker is a registered trademark of Legato Systems, Inc.

Federal Acquisitions: Commercial Software -- Government Users Subject to Standard License Terms and Conditions.

DOCUMENTATION IS PROVIDED “AS IS” AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Sun Microsystems, Inc. détient des droits de propriété intellectuelle sur la technologie réunie dans le produit qui est décrit par ce document. Ces droits de propriété intellectuelle peuvent s’appliquer en particulier, sans toutefois s’y limiter, à un ou plusieurs des brevets américains répertoriés à l’adresse `http://www.sun.com/patents` et à un ou plusieurs brevets supplémentaires ou brevets en instance aux Etats-Unis et dans d’autres pays.

Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Sun, Sun Microsystems, le logo Sun, Sun Cobalt, le logo Sun Cobalt, Sun Cobalt RaQ, Java et JDK sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d’autres pays.

LA DOCUMENTATION EST FOURNIE “EN L'ETAT” ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFAÇON.

Part Number / Numéro de pièce : 070-00263-02
Date : 08-2001

Important Safeguards

For your protection, please read and understand all of the safety and operating instructions regarding your Sun Cobalt™ RaQ™ XTR server appliance and retain for future reference.

1. Ventilation

The Sun Cobalt RaQ XTR server appliance's and fan openings protect the server from overheating. These openings must not be blocked or covered. This product should not be placed in a built-in installation unless proper ventilation is provided.

2. Lithium Battery

The lithium battery on the system board provides power for the real-time clock and CMOS RAM. The battery has an estimated useful life expectancy of 5 to 10 years. If your system no longer keeps accurate time and date settings, it may be time to change the battery. Contact Sun Microsystems for service information.

Warning: There is a danger of explosion if the battery is incorrectly replaced or replaced with the wrong type of battery. Replace only with the same or equivalent type recommended by the equipment manufacturer. Dispose of used batteries according to manufacturer's instructions.

Avertissement : Il y a danger d'explosion s'il y a remplacement incorrect de la pile. Remplacer uniquement avec une pile du même type ou d'un type équivalent recommandé par le fabricant. Mettre au rebut les piles usagées conformément aux instructions du fabricant.

Achtung: Explosionsgefahr wenn die Battery in umgekehrter Polarität eingesetzt wird. Nur mit einem gleichen oder ähnlichen, vom Hersteller empfohlenen Typ, ersetzen. Verbrauchte Batterien müssen per den Instructionen des Herstellers verwertet werden.

3. Power Cord

Caution: The power-supply cord is used as the main disconnect device. Ensure that the socket outlet is located or installed near the equipment and is easily accessible.

Attention : Le cordon d'alimentation sert d'interrupteur général. La prise de courant doit être située ou installée à proximité du matériel et offrir un accès facile.

Achtung: Zur sicheren Trennung des Gerätes vom Netz ist der Netzstecker zu ziehen. Vergewissern Sie sich, dass die Steckdose leicht zugänglich ist.

4. Electrical Shock

To reduce the risk of electrical shock, do not disassemble this product. Take the server appliance to a qualified service person when service or repair work is required. Opening or removing covers may expose you to dangerous voltage or other risks. Incorrect reassembly can cause electric shock when this product is subsequently used.

5. Equipment Rack

If you decide to mount the server appliance in an equipment rack, tak e the following precautions:

a. Ensure the ambient temperature around the server appliance (which may be higher than the room temperature) is within the limits specified in Appendix B. See "Physical data" on page 203.

b. Ensure there is sufficient air flow around the server.

c. Ensure electrical circuits are not overloaded; consider the nameplate ratings of all the of the connected equipment and ensure you have overcurrent protection.

d. Ensure the equipment is properly grounded, particularly any equipment connected to a power strip.

e. Do not place any objects on top of the server appliance.

6. Browsers

Both Netscape Navigator™ and Microsoft Internet Explorer have bugs that can cause intermittent, unexplained failures. When using a Web browser to interact with your Sun Cobalt RaQ XTR server appliance, you may occasionally experience a browser failure. Released product versions of the browsers are usually more reliable than beta versions and later versions typically work the most reliably. A browser program failure, although annoying, does not adversely affect your server appliance’s data.

To use the server appliance, you need a personal computer (attached to the network) that uses a Web browser (for example, Netscape Navigator, version 4.7 or later, or Microsoft Internet Explorer, version 5.0 or later). To manage the server appliance from the browser-based user interface (UI), known as the Server Desktop, you must enable cookies, cascading style sheets and Javascript on your browser (these features are normally enabled by default).

Regulations and Information

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his/her expense.

Preface

List of chapters

This user manual is for anyone who will set up the Sun Cobalt™ RaQ™ XTR server appliance for a group of users. You should be familiar with Microsoft Windows, Macintosh or other operating systems, and Netscape Navigator™, Microsoft Internet Explorer or other Web browsers.

This manual consists of the following chapters and appendices:

Chapter 1 — “Introduction” includes an overview of the Sun Cobalt RaQ XTR server appliance’s features.

Chapter 2 — “Setting up the server appliance” describes the hardware setup of the server appliance and the process of integrating the server appliance into a network.

Chapter 3 — “Site User” explains the features available to a user on a virtual site.

Chapter 4 — “Site Management” explains the features available to the Site Administrator of a virtual site.

Chapter 5 — “Server Management” explains the features available to the Server Administrator of the server appliance.

Chapter 6 — “Services” includes information on configuring an email client, and on creating and uploading Web pages.

Appendix A — “Using the LCD Console” explains the functions on the LCD console.

Appendix B — “Product Specifications” lists the technical specifications for the server appliance.

Appendix C — “Upgrading the Sun Cobalt™ RaQ™ XTR server appliance” explains how to upgrade the hardware of the server appliance.

Appendix D — “Advanced Information” describes processes and options that are outside the purview of normal operation.

Appendix E — “Domain Name System” gives an in-depth explanation of the DNS service.

Appendix F — “Disaster Recovery with Third-Party Software” explains how to configure the server software for the third-party backup and restore solutions.

Appendix G — “Contacting Sun Microsystems, Inc.” explains how to contact Sun Microsystems and provides additional resources and information.

Appendix H — “Licenses” lists the licensing information.

Appendix I — “Glossary” provides a glossary of terms in the user interface (UI) and the user manual for the server appliance.

Icons used on the UI and in the manual

Table 1 describes the icons used by the browser-based UI and in this manual. If you pass the mouse pointer over an icon, a short help message appears at the bottom of the screen.

Table 1. Icons used in the user interface

Icon	Description
🌐	**Web Server** In the “Service Settings” table under **Server Management > Control Panel**; Web Server is always on.
✉	**Email Server** In the “Service Settings” table under **Server Management > Control Panel**.
⇄	**FTP Server** In the “Service Settings” table under **Server Management > Control Panel**.
☎	**Telnet Server** In the “Service Settings” table under **Server Management > Control Panel**.
🖥	**Simple Network Management Protocol (SNMP)** In the “Service Settings” table under **Server Management > Control Panel**.

Table 1. Icons used in the user interface

Icon	Description
📄	**Active Server Page (ASP) Administrative Server** In the "Service Settings" table under **Server Management > Control Panel**.
DNS	**Domain Name System (DNS)** In the "Service Settings" table under **Server Management > Control Panel**.
✎	**Modify** In the "Virtual Site List" table under **Server Management > Site Management**; used to modify settings for a virtual site. In the "Bandwidth Limits" table under **Server Management > Control Panel**; used to modify a bandwidth limit for an IP address. In the "User List" table under **Site Management (<sitename>) > User Management**; used to modify the settings for a site user.
✉	**Email settings** In the "User List" table under **Site Management (<sitename>) > User Management**; used to modify the email settings for a site user.
🗑	**Delete** In the "Virtual Site List" table under under **Server Management > Site Management**; used to delete a virtual site from a Sun Cobalt RaQ XTR server appliance. In the "Bandwidth Limits" table under **Server Management > Control Panel**; used to delete a bandwidth limit for an IP address. In the "User List" table under **Site Management (<sitename>) > User Management**; used to delete a site user from a virtual site.
♛	**Site Administrator** In the "User List" table under **Site Management (<sitename>) > User Management**; indicates that the user is a Site Administrator for the virtual site.

Table 1. Icons used in the user interface

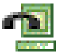
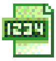
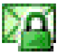
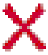
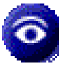
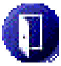
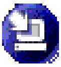
Icon	Description
	**Telnet** In the "User List" table under **Site Management (<sitename>) > User Management**; indicates that a user has telnet/shell access.
	**FrontPage** In the "User List" table under **Site Management (<sitename>) > User Management**; indicates that a FrontPage User Web is enabled for a site user.
	**Secure POP (APOP)** In the "User List" table under **Site Management (<sitename>) > User Management**; indicates that a Authentication POP is enabled for a site user.
	**Suspension / Disabled** In the "Virtual Site List" table under **Server Management > Site Management**; indicates that a virtual site has been suspended by the Sun Cobalt RaQ XTR server appliance Administrator. In the "User List" table under **Site Management (<sitename>) > User Management**; indicates that a user has been suspended by the Site Administrator. In the "Site Settings" table under **Site Management (<sitename>) > Site Settings** (read-only page for a Site Administrator); indicates that a service is disabled.
	Enabled In the "Site Settings" table under **Site Management (<sitename>) > Site Settings** (read-only page for a Site Administrator); indicates that a service is enabled.
	**Active Monitor Status** Viewable from all of the screens. A blue icon indicates that all of the monitored system components are functioning correctly; a red icon indicates that a monitored component has a problem.
	**Log Out** Viewable from all of the screens; allows users to log out of their accounts.

Table 1. Icons used in the user interface

Icon	Description
	**New Software / Software Update** Viewable to the Sun Cobalt RaQ XTR server appliance Administrator from all of the screens; turns red when new or updated software is available.
	Uninstall Software In the Installed Software List under **BlueLinQ > Installed Software**. A green icon indicates that a the software package can be uninstalled; a gray icon indicates that the software package cannot be uninstalled.

Contents

Introduction

The Sun Cobalt™ RaQ™ XTR server appliance provides a complete solution for hosting virtual sites, publishing Web pages, transferring files, hosting email and third-party applications, as well as offering new capabilities for high-traffic, complex Web sites and e-commerce applications.

The Sun Cobalt RaQ XTR server appliance offers a full suite of Internet services with remote administration capabilities, pre-packaged in a single rack-unit (1RU) industry-standard enclosure. The server appliance is pre-configured with the Linux operating system, Apache Web server, Sendmail, File Transfer Protocol (FTP) server, Domain Name System (DNS), FrontPage Server extensions, and support for Active Server Pages (ASP) and PHP.

All of these services can be used within an extranet or an intranet environment, or across the Internet.

The Sun Cobalt RaQ XTR server appliance further enhances the suite of services by offering from one to four hard disk drives, support for RAID Level 0, 1 or 5 (depending on the number of hard drives at initial configuration), enhanced backup and restore functionality, disaster recovery and comprehensive site-usage reporting. The unique design of the Sun Cobalt RaQ XTR server appliance allows the user to add hard disk drives through the front panel without having to remove the server from the equipment rack.

The server appliance also provides a flexible platform for developing solutions, including the development of third-party applications.

The Sun Cobalt RaQ XTR server appliance is pre-loaded with InterBase 6.0, an open-source, cross-platform SQL database from Inprise Corporation. For more information on InterBase, visit the URL http://www.interbase.com. Also, see "Enabling Interbase 6.0" on page 224.

Levels of user

The Sun Cobalt RaQ XTR server appliance has three levels of user:

- the ***Site User*** has access to his or her account information and the programs
- the ***Site Administrator*** manages a virtual site and the users on that site
- the ***Server Administrator*** manages the server appliance, and can manage all of the virtual sites and users as well

Organization of the user manual

This manual is organized according to the features that each level of user can access.

- Chapter 3, “Site User”, describes the features available to the site user.
- Chapter 4, “Site Management”, describes the features available to the Site Administrator. The Site Administrator can access all of the features described for the site user.
- Chapter 5, “Server Management”, describes the features available only to the Server Administrator. The Server Administrator can access all of the features described for the Site Administrator and the site user.

Site User

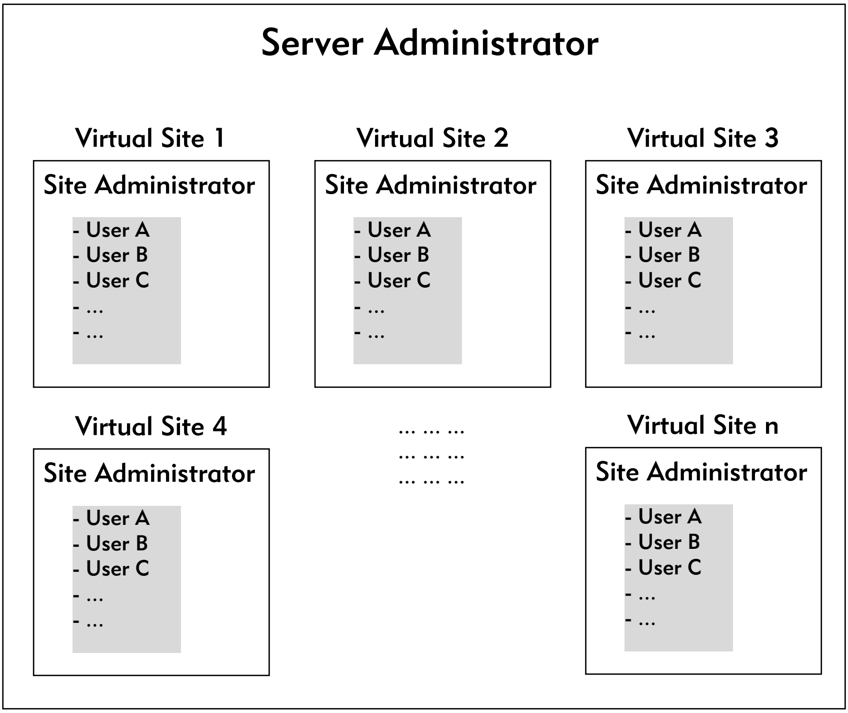
A ***Site User*** can send and receive email through the virtual site, upload and download files using the FTP service provided by the site, publish a personal Web page on the site, and back up and restore files and data located in the home directory.

A site user can also access third-party applications that the Server Administrator has loaded on to the server appliance. These programs appear under the **Programs** tab.

Site users are added to a virtual site by the Server Administrator or a Site Administrator. A site user only has control over the files located in his or her home directory on the server appliance.

Figure 1 illustrates the level of access, indicated by the shaded area, available to site users.

Figure 1. Level of access for a Site User



Site Administrator

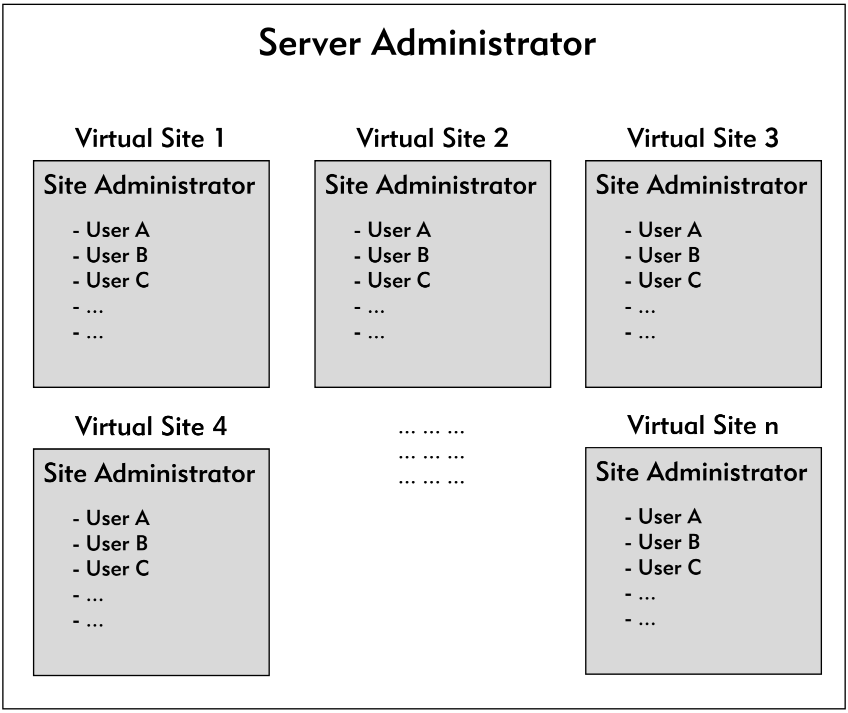
A ***Site Administrator*** manages a virtual site located on the Sun Cobalt RaQ XTR server appliance; the virtual site provides Web publishing, email and FTP services to the users of the site. The Site Administrator sets up user accounts and access privileges, maintains mailing lists, configures the secure-sockets layer (SSL) settings for the virtual site (if the Server Administrator has enabled SSL on the site), controls the settings for the virtual site and its FTP service, has access to users' email settings, can generate reports about the hard disk drive and Web usage on a virtual site, and can back up and restore files residing on the site.

The Server Administrator designates the Site Administrator for each site. The Site Administrator has control only over this virtual site (unless he or she is also the Server Administrator).

✍ ***Note:*** If the Server Administrator also serves as the Site Administrator for a virtual site, he or she has access to all of the server appliance administrative functions as well.

Figure 2 illustrates the level of access, indicated by the shaded area, available to Site Administrators.

Figure 2. Level of access for a Site Administrator



Server Administrator

The ***Server Administrator*** is the person who controls and manages the Sun Cobalt RaQ XTR server appliance . This person sets up the server appliance, sets up virtual sites, and sets access privileges and provides services for the Site Administrators and site users. The Server Administrator can also act as the Site Administrator for any virtual site.

Note: Whereas industry uses the term “virtual host”, we use the term “virtual site”. In our definition, a virtual site consists of a Domain Name System (DNS) domain with Web, FTP and email services. Each virtual site contains its own list of site-user accounts. Each site-user account has its own Web page, FTP directory, email spool and any number of email aliases. The fully qualified domain name of a virtual site is unique to that site, while its IP address can be shared by many sites. For more information, see “Definition of a virtual site” on page 103.

The Server Administrator has the user name *admin* and has full control of the server appliance; the Server Administrator is a member of the main site (which uses the IP address shown on the LCD screen of the server appliance).

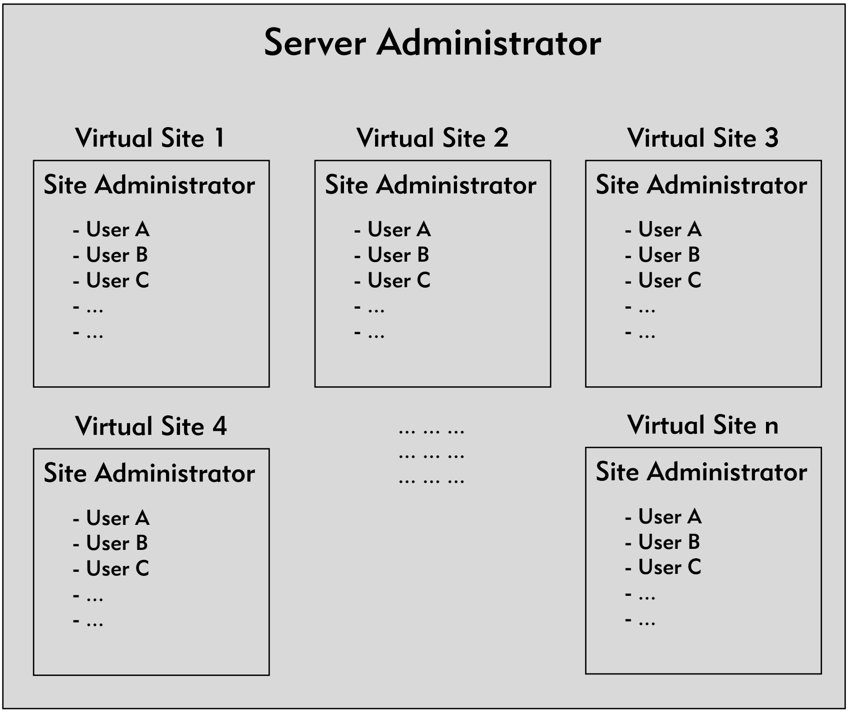
Alternate Administrator feature

The Alternate Administrator (*alteradmin*) feature allows a person to have the same level of access to the server as the Server Administrator (*admin*) but without having to use the user name *admin* and password to log in.

For more information, see “Alternate Administrator feature” on page 101.

Figure 3 illustrates the level of access, indicated by the shaded area, available to a Server Administrator or the user *alteradmin*.

Figure 3. Level of access for a ServerAdministrator



Server Desktop UI

You access the browser-based user interface (UI), known as the Server Desktop, with a Web browser such as Microsoft Internet Explorer or Netscape Communicator. Depending on the level of user, the Server Desktop UI presents five different tabs which are described in the following sections:

- **Programs**
- **Personal Profile**
- **Site Management** (the host name or IP address of the virtual site is displayed on the tab)
- **Server Management**
- **BlueLinQ**

Programs

The **Programs** tab provides access to third-party applications that the Server Administrator has loaded on to the server appliance.

For more information on third-party applications available for Sun Cobalt server appliances, visit the Solutions Web site at http://www.cobalt.com/solutions/.

Personal Profile

The **Personal Profile** tab allows a user to configure his or her personal settings on the server appliance.

For more information, see “Personal profile” on page 36.

Site Management

The Site Management chapter describes the functions that the Site Administrator normally performs. The Site Administrator accesses these functions under the **<fully qualified domainname>** tab on the Server Desktop UI.

For more information, see Chapter 4, “Site Management,” on page 45.

Server Management

The Server Management chapter describes the functions that the Server Administrator normally performs. The Server Administrator accesses these functions under the **Server Management** tab of the Server Desktop UI.

For more information, see Chapter 5, “Server Management,” on page 99.

BlueLinQ

The BlueLinQ™ Application Delivery Service provides instant access to product updates and new services as they become available.

For more information, see “BlueLinQ” on page 168.

Usage requirements for the Sun Cobalt™ RaQ™ XTR server appliance

To use the Sun Cobalt RaQ XTR server appliance, you need:

- A 10/100BaseTX Transmission Control Protocol/Internet Protocol (TCP/IP) -based local area network (LAN).
- A personal computer (attached to the network) that uses a Web browser (for example, Netscape Navigator, version 4.7 or later, or Microsoft Internet Explorer, version 5.0 or later).

  To manage the server appliance from the Server Desktop UI, you must enable cookies, cascading style sheets and Javascript on your browser (these features are normally enabled by default).
- Network parameters, which you can obtain from your network administrator; these include the server appliance’s assigned IP address, the subnet mask of your network and, if communicating with other networks, a gateway or router address.
- An Internet service provider (ISP), if you plan to connect to the Internet.

Setting up the server appliance

This chapter guides you through the process of connecting and configuring the Sun Cobalt™ RaQ™ XTR server appliance for your network and user community. A typical setup process takes less than 15 minutes, after which you can begin using all of the server appliance services.

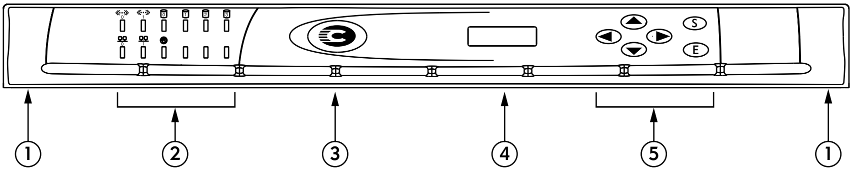
If the server appliance has been configured previously for a different network, refer to “Set up network” on page 186.

General

Figure 4 and Figure 5 show the controls, indicators and connectors on the Sun Cobalt RaQ XTR server appliance.

Front view of the Sun Cobalt™ RaQ™ XTR server appliance

Figure 4. Front view of the server appliance



1. **Recessed Finger Holds** allow you to pull out the front panel.
2. The **Status Indicators** signal ethernet, hard disk drive and Web activities.

   «··» blinks when there is traffic on the network interfaces (labelled 0 or 1).

   🖧 glows steadily to indicate an active connection on the network interfaces (labelled 0 or 1).

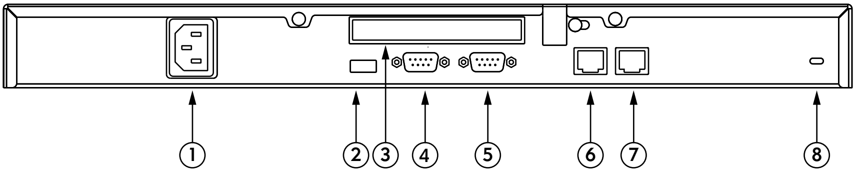
   ⛁ blinks when there is activity on a hard disk drive (labelled 0 through 3).

   🌐 blinks to indicate Web activity.

3. The **"C" Logo Badge** is the power switch. The logo badge glows when the server appliance is powered on; it blinks if there is a RAID failure or a fan failure.
4. The **LCD screen** displays messages and values entered. Use the arrow buttons to toggle between choices or to enter values. (See "Using the LCD console to configure the network" on page 17.)
5. The **LCD arrow buttons** allow you to enter network configuration information, configure a UPS unit, reboot the server, lock the LCD console and reset the Server Administrator password.

Rear view of the Sun Cobalt RaQ XTR server appliance

Figure 5. Rear view of the server appliance



1. The **Power socket** receives the AC cord that is provided.
2. The **USB port** provides a universal serial bus (USB) connection.
3. The **PCI expansion slot** provides space for adding a PCI card.
4. The **Serial connector** allows you to connect an uninterruptible power supply (UPS) to the serial port for Smart UPS support.
5. The **Serial console port** allows you to connect serial devices.

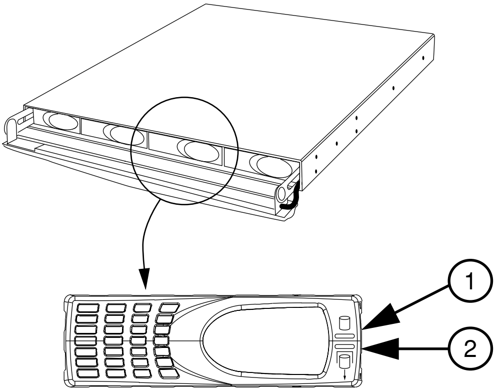
The **Network connectors** enable ethernet network connections and receive the 10/100 BaseT network cables.

6. **Network interface 2** (eth 1)
7. **Network interface 1** (eth 0)
8. The **Security lock hole** is used to lock the unit to a secure location.

View of hard-disk-drive bay

Figure 6 shows the LEDs on the front panel of the hard disk drive.

Figure 6. Disk drive front panel view



1. The **Activity LED** blinks to indicate activity on the hard disk drive.
2. The **Failure LED** lights to indicate a defective hard disk drive. This LED also tells you when it is safe to remove the hard disk drive from the drive bay.

   When you insert your finger into the front plate, the Failure LED lights indicating that it is safe to remove the drive. If the Failure LED was lit when you accessed the drive bay, it should stay lit when you grasp the front plate of the hard disk drive. If the LED does not light, or goes out, when your finger is inserted in the front plate, do not remove the hard disk drive. Allow a few seconds for the drive to complete its current task and then try again.

Setup of the Sun Cobalt RaQ XTR server appliance

The setup process occurs in two phases.

- "Phase 1: Making the connection" explains the physical connection of the server appliance to a power source and the network.
- "Phase 2: Setting up with the Web browser" explains the network integration process. It also allows the Server Administrator to select services on the server and configure the level of RAID on the hard disk drives, using a computer with a valid Web browser.

Phase 1: Making the connection

Installing the Sun Cobalt RaQ XTR server appliance

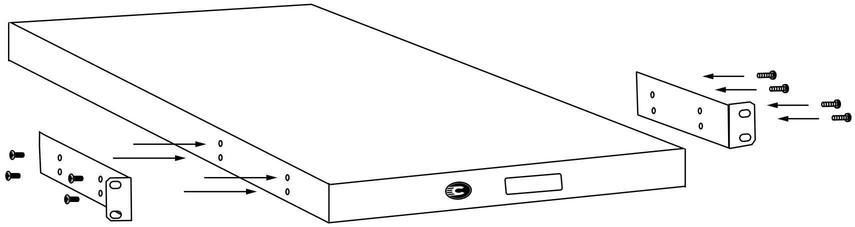
Warning: Due to the size and weight of the server appliance, it is highly recommended that you have a second person help you mount the server in an equipment rack.

You can place the Sun Cobalt RaQ XTR server appliance on a flat surface or mount it in a standard19-inch equipment rack. The server appliance is designed to allow you to mount it in an equipment rack either at the front or middle of the server. To mount the server in an equipment rack, you must first attach the mounting ears included with the server.

To attach the mounting ears, align the mounting ears over the four exposed screw holes on each side of the server chassis. To mount the server in the middle of the equipment rack, ensure that the mounting ears are aligned with the protruding edges facing the back end of the server; to mount the server towards the front of the equipment rack, ensure that the ears are aligned with the protruding edges facing towards the front of the server.

Attach the ears to the chassis with the eight mounting screws included with the server (see Figure 7). Now position the server appliance in the equipment rack and attach the ears securely to the rack.

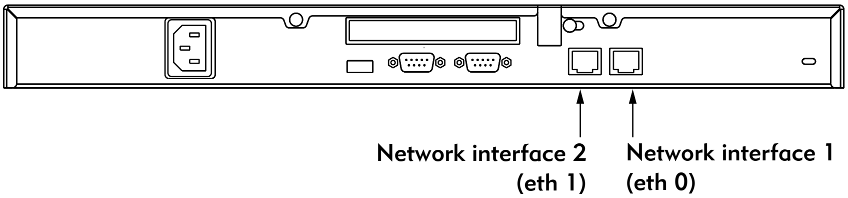
Figure 7. Mounting ears for the server appliance



Connecting to the network

Connect one end of a Category 5 ethernet cable to the 10/100 BaseT Network 1 interface on the server appliance; see Figure 8. Connect the other end of the cable to an existing network socket.

Figure 8. Network connectors



Connecting the power cord

Connect the power supply cord to the server appliance to an electrical outlet (100-240 volts AC, 50/60 Hz; see “Physical data” on page 203).

Powering on the server appliance

Caution: It is important to follow the proper power-down procedure before turning off the server appliance. Refer to “Power down” on page 192.

Note: Ensure that the hard disk drives are properly seated in their bays before powering up the server appliance.

Note: The “C” logo badge is a soft button; it does not click into place when you press it.

When the Sun Cobalt RaQ XTR server appliance is plugged into an electrical outlet, the **“C” logo badg**e on the front panel lights up. Turn on the power by pressing and releasing the “C” logo badge. The hard disk drive(s) “spins up”, the fans turn on and the front LCD screen lights up. The Cobalt logo and the Cobalt Networks name scroll across the screen.

The time required for the power-up process depends on the memory configuration and the number of hard disk drives in your server appliance.

A number of status messages are displayed on the LCD screen as the server appliance completes its boot process. When complete, the LCD screen displays

```
PRIMARY IP ADDR:
```

Configuring the Sun Cobalt RaQ XTR server appliance for the network

✍ ***Note:*** It is possible to configure the server appliance through the serial port. See “Initializing the server appliance through the serial console port” on page 226.

Now that you have made the network and power connections, you can configure the network settings.

The Sun Cobalt RaQ XTR server appliance requires specific network information in order to function properly. Before you proceed, make sure you have the following information:

- the IP address assigned to the server appliance
- the subnet mask of your network
- the gateway or router address (necessary only if communicating with other networks)

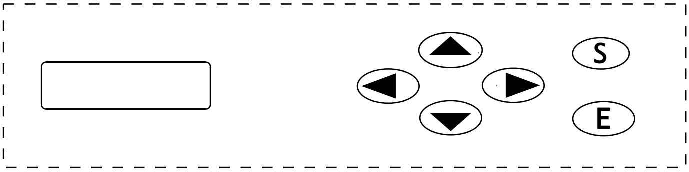
Using the LCD console to configure the network

Figure 9 shows the LCD console for the Sun Cobalt RaQ XTR server appliance.

The LCD screen on the front panel of the server appliance displays two lines of text. The top line of the LCD presents instructions on data to enter; the bottom line displays the data already entered. Use the arrow buttons next to the LCD screen to enter the required network information manually.

Appendix A, “Using the LCD Console”, provides more information about functions available through the LCD console.

Figure 9. LCD console



During startup, the LCD screen displays status information about the boot process itself. When setting up the server appliance, the LCD console is used to enter network configuration information. Once the server appliance is running, the LCD console is used to change network configuration information, configure a UPS unit, reboot the server, lock the LCD console and reset the Server Administrator password.

The arrow buttons function as follows:

◀ The **Left** arrow button moves the cursor to the left.

▶ The **Right** arrow button moves the cursor to the right.

▲ The **Up** arrow button increases the digit located at the cursor position.

▼ The **Down** arrow button decreases the digit located at the cursor position.

S The **S** (select) button displays the next option.

E The **E** (enter) button accepts the information entered or the options displayed.

Setting the configuration

☞ ***Important:*** In this phase, you configure only the primary network interface. To complete this phase, you must know:

- the IP address assigned to the server appliance
- the subnet mask of your network

During setup, the LCD console is used to enter network configuration information on the Sun Cobalt RaQ XTR server appliance. The LCD display reads:

```
PRIMARY IP ADDR:
000.000.000.000
```

A blinking cursor appears on the second line of the LCD display. The following steps explain how to enter the required network information for the primary network interface. The secondary network interface is configured through the browser-based Server Desktop UI; see “Network” on page 136”.

To configure the network manually:

1. When you see the prompt:

   ```
   PRIMARY IP ADDR:
   000.000.000.000
   ```

   use the arrow buttons on the LCD console to enter the IP address assigned to the server appliance.

2. Press E to accept the IP address.

   If the IP address is valid, the next prompt appears:

   ```
   ENTER NETMASK:
   255.000.000.000
   ```

3. Enter the netmask of your network.

4. Press E to accept the entry.

   If the netmask is valid, the following prompt appears:

   ```
   ENTER GATEWAY:
   000.000.000.000
   ```

5. Enter the IP address of the gateway for your network.

   If your network does not have a gateway, do not enter a number — leave the default value, “000.000.000.000.”

6. Press E to accept the entry

   The LCD displays:

   ```
   [S]AVE [C]ANCEL
   ```

7. To save the configuration information, use the left and right arrow buttons to select `[S]ave`, and then press E. After a few moments, you will see:

   ```
   Verifying and Saving...
   ```

Note: Selecting [C]ancel cancels the configuration and the LCD screen displays `PRIMARY IP ADDR:` again. You must go through the entry process again.

After verifying and saving the information, the server appliance server completes the boot process. The LCD screen shows several messages before displaying the IP address assigned to the server appliance.

Configuration is complete when the LCD screen displays the IP address assigned to the server appliance, for example:

```
IP Address:
192.168.25.77
```

Phase 2: Setting up with the Web browser

The remainder of the setup process is performed through a Web browser on a computer on your network. The user interface (UI) through which you manage the Sun Cobalt RaQ XTR server appliance server is called the Server Desktop. The Server Desktop UI has a number of tabs along the top and menu items down the left sidebar.

Use one of the standard Web browsers such as Netscape Navigator (version 4.7 or later) or Microsoft Internet Explorer (version 5.0 or later). Once the setup process is complete, the server appliance can be managed from any computer on the network with a valid Web browser.

Support for RAID-0, RAID-1 and RAID-5

☞ ***Important:*** The Sun Cobalt RaQ XTR server appliance Administrator can set the level of RAID only through the Setup Wizard.

Once the Setup Wizard process is complete, the level of RAID cannot be changed unless the system is returned to a factory-fresh state using an OS restore CD.

Ensure that you have decided on the level of RAID that you want to implement before launching the Setup Wizard.

A redundant array of independent disks (RAID) is a way of storing the same data in different places (thus, redundantly) on multiple hard disk drives. A RAID appears to the operating system to be a single virtual disk drive.

Redundancy means that there is protection against the failure of any single hard disk drive. Redundant data is used by a RAID system in the event of a failure; this redundant data can either be a mirror copy or parity data used to reconstruct the actual data.

The Sun Cobalt RaQ XTR server appliance offers three different levels RAID (depending on the configuration of the server), each with its own advantages and disadvantages:

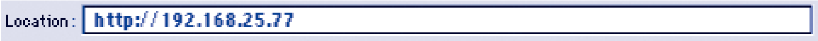
- **RAID-0** combines the separate hard disk drives into one virtual disk drive and offers the best performance of the three options. However, the data on the disk drives is not redundant and the system is thus not fault-tolerant. This option is available on server configurations with two or more hard disk drives.
- **RAID-1**, also known as disk mirroring, consists of a primary hard disk drive and a secondary hard disk drive; the secondary disk drive is an exact copy or “mirror image” of the primary disk drive. This option is only available on a configuration with two hard disk drives.
- **RAID-5** includes a rotating parity-bit array. All read and write operations can be overlapped. RAID-5 does not store redundant data but it does store the parity information which can be used to reconstruct data in the event of a single hard-disk-drive failure. RAID-5 requires at least three hard disk drives for the array.

Although RAID-1 and RAID-5 (but not RAID-0) can protect your data in case of a hard-disk-drive failure, they do not protect against operator and administrator (human) error, or against loss due to programming bugs.

The Sun Cobalt RaQ XTR server appliance implements RAID services through software. Each hard disk drive has its own independent master channel to allow high performance without extra RAID hardware.

To use the browser to set up the Sun Cobalt RaQ XTR server appliance, follow these steps:

1. Launch a standard Web browser on a computer connected to the network.
2. Enter the IP address of the server appliance (displayed on the LCD screen on the front panel of the server appliance) in the URL field of your browser; for example:



Location: http://192.168.25.77

3. Press **Return** (or **Enter**) on your keyboard.

If you configured the server appliance network settings successfully, the Sun Cobalt Welcome screen appears; see Figure 10.

Active Assist — Online Help

Active Assist provides real-time context-sensitive help on the Server Desktop UI. When you move the mouse pointer over a context-sensitive area of the screen, a description of the item appears at the bottom of the browser page.

A context-sensitive area can be a a blue *question-mark* icon, a menu item on the left side of the Server Desktop UIor a tab item at the top.

Configuring the server appliance with the Setup Wizard

To configure the Sun Cobalt RaQ XTR server appliance, enter information into the fields on the **Setup Wizard** screens. These fields are described in the sections that follow.

The Setup Wizard is a series of screens that guide you through the setup process. After completing each step, click on the right arrow at the bottom to apply the changes and move on to the next step. You can click on the left arrow to return to a previous screen.

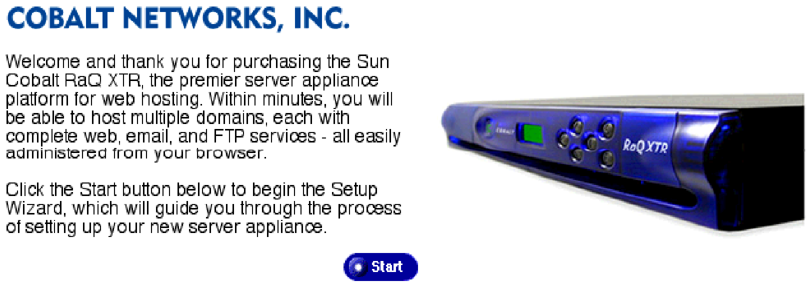
◁ ▷

The server appliance performs automatic checks on the information entered and alerts you when an illegal value or a problem is encountered. When the information is entered correctly at each stage, the server appliance enters the changes in its configuration files before proceeding to the next step. Changes may take several seconds to complete.

☞ ***Important:*** If you want to assign a domain name to your Sun Cobalt RaQ XTR server appliance, you must register the domain name with a name registrar accredited by the Internet Corporation for Assigned Names and Numbers (ICANN). For more information, visit the ICANN Web site at http://www.icann.org.

Click **Start** to begin the Setup Wizard.

Figure 10. Welcome screen



COBALT NETWORKS, INC.

Welcome and thank you for purchasing the Sun Cobalt RaQ XTR, the premier server appliance platform for web hosting. Within minutes, you will be able to host multiple domains, each with complete web, email, and FTP services - all easily administered from your browser.

Click the Start button below to begin the Setup Wizard, which will guide you through the process of setting up your new server appliance.

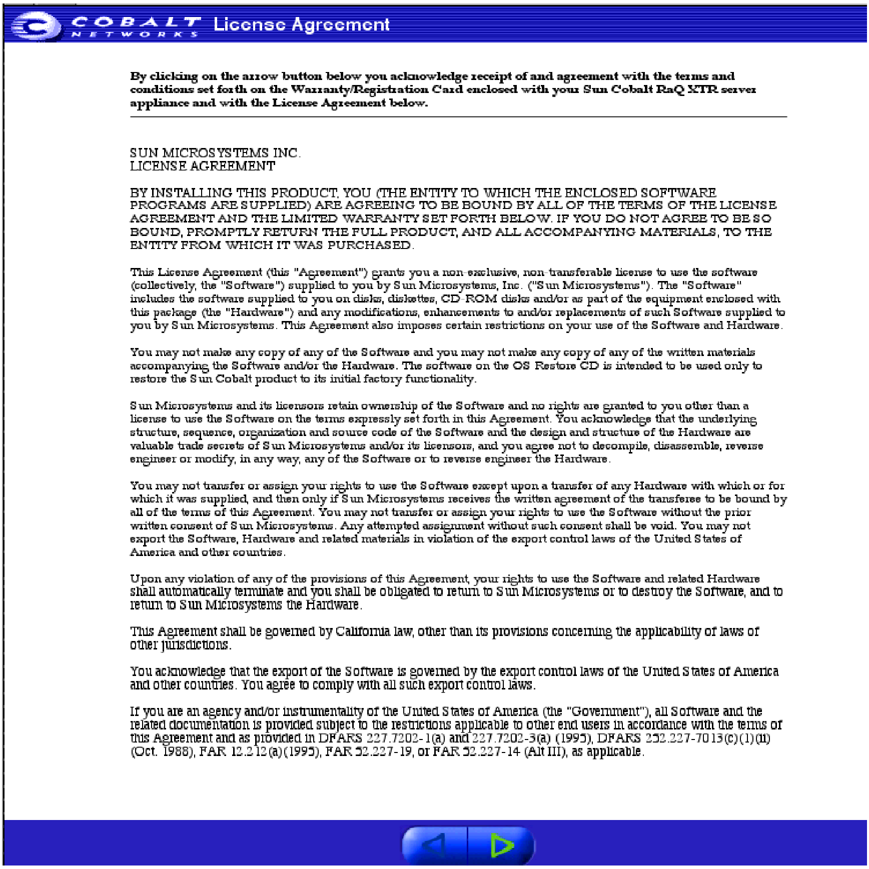
License agreement

You are presented with the Sun Microsystems License Agreement screen.

By clicking on the arrow button on this screen, you acknowledge receipt of and agreement with the terms and conditions set forth on the Warranty/Registration Card enclosed with your Sun Cobalt RaQ XTR server appliance and with the License Agreement shown in Figure 11.

Read through the License Agreement and, if you agree with its terms, click the right arrow at the bottom to signify your agreement.

Figure 11. License Agreement



By clicking on the arrow button below you acknowledge receipt of and agreement with the terms and conditions set forth on the Warranty/Registration Card enclosed with your Sun Cobalt RaQ XTR server appliance and with the License Agreement below.

SUN MICROSYSTEMS INC.
LICENSE AGREEMENT

BY INSTALLING THIS PRODUCT, YOU (THE ENTITY TO WHICH THE ENCLOSED SOFTWARE PROGRAMS ARE SUPPLIED) ARE AGREEING TO BE BOUND BY ALL OF THE TERMS OF THE LICENSE AGREEMENT AND THE LIMITED WARRANTY SET FORTH BELOW. IF YOU DO NOT AGREE TO BE SO BOUND, PROMPTLY RETURN THE FULL PRODUCT, AND ALL ACCOMPANYING MATERIALS, TO THE ENTITY FROM WHICH IT WAS PURCHASED.

This License Agreement (this "Agreement") grants you a non-exclusive, non-transferable license to use the software (collectively, the "Software") supplied to you by Sun Microsystems, Inc. ("Sun Microsystems"). The "Software" includes the software supplied to you on disks, diskettes, CD-ROM disks and/or as part of the equipment enclosed with this package (the "Hardware") and any modifications, enhancements to and/or replacements of such Software supplied to you by Sun Microsystems. This Agreement also imposes certain restrictions on your use of the Software and Hardware.

You may not make any copy of any of the Software and you may not make any copy of any of the written materials accompanying the Software and/or the Hardware. The software on the OS Restore CD is intended to be used only to restore the Sun Cobalt product to its initial factory functionality.

Sun Microsystems and its licensors retain ownership of the Software and no rights are granted to you other than a license to use the Software on the terms expressly set forth in this Agreement. You acknowledge that the underlying structure, sequence, organization and source code of the Software and the design and structure of the Hardware are valuable trade secrets of Sun Microsystems and/or its licensors, and you agree not to decompile, disassemble, reverse engineer or modify, in any way, any of the Software or to reverse engineer the Hardware.

You may not transfer or assign your rights to use the Software except upon a transfer of any Hardware with which or for which it was supplied, and then only if Sun Microsystems receives the written agreement of the transferee to be bound by all of the terms of this Agreement. You may not transfer or assign your rights to use the Software without the prior written consent of Sun Microsystems. Any attempted assignment without such consent shall be void. You may not export the Software, Hardware and related materials in violation of the export control laws of the United States of America and other countries.

Upon any violation of any of the provisions of this Agreement, your rights to use the Software and related Hardware shall automatically terminate and you shall be obligated to return to Sun Microsystems or to destroy the Software, and to return to Sun Microsystems the Hardware.

This Agreement shall be governed by California law, other than its provisions concerning the applicability of laws of other jurisdictions.

You acknowledge that the export of the Software is governed by the export control laws of the United States of America and other countries. You agree to comply with all such export control laws.

If you are an agency and/or instrumentality of the United States of America (the "Government"), all Software and the related documentation is provided subject to the restrictions applicable to other end users in accordance with the terms of this Agreement and as provided in DFARS 227.7202-1(a) and 227.7202-3(a) (1995), DFARS 252.227-7013(c)(1)(ii) (Oct. 1988), FAR 12.212(a)(1995), FAR 52.227-19, or FAR 52.227-14 (Alt III), as applicable.

System Settings

The **System Settings** screen appears; refer to Figure 12. On this screen, you enter information for the Network Settings, Administrator Settings and Time Settings for the server.

Network Settings

Enter the following network information:

- **Host name** Assign a host name (for example, raqxtr) to the Sun Cobalt RaQ XTR server appliance.

  Domain name Enter your domain name. The domain name is either the official domain name that is registered with an ICANN-accredited registrar (for example, "cobalt.com") or an intranet domain name specific to your network. This allows you to access your server appliance by host name and domain name, rather than by IP address only.

  Coordinate the host name and domain name with your Internet service provider (ISP) or the person in charge of you DNS infrastructure to ensure the integrity of your network. If your server appliance is integrated into a larger network, consult with your network administrator for this information.

  The Server Administrator can change the domain name on the server appliance server later on through the Server Desktop UI; see "Network" on page 136.

- **Primary DNS Server Address** Enter the IP address of your primary Domain Name System (DNS) server.

  A DNS server maintains a list of computer names and their IP addresses. The server appliance needs access to this list on the DNS server in order to convert between IP addresses and names. This conversion is essential for sending and receiving email external to the server appliance. For more information on DNS, see Appendix E, "Domain Name System".

- **Secondary DNS Server Address** You have the option of entering the IP address for a secondary DNS server.

Administrator Settings

The Server Administrator is responsible for the following:

- Setting up and maintaining the sites and services on the server appliance

- Responding to email alerts from the server appliance in order to forestall potential problems

Alternate Administrator feature

The Alternate Administrator (*alteradmin*) feature allows a person to have the same level of access to the server as the Server Administrator (*admin*) but without having to use the user name *admin* and password to log in.

For Internet service providers (ISPs) who offer Sun Cobalt RaQ XTR server appliances to their customers, this feature allows the ISP access to the server if the Server Administrator has forgotten or incorrectly entered the password for the user *admin*.

Once the user *alteradmin* has been set up, the user *alteradmin* does not appear on the server appliance to any other user, including the Server Administrator.

If the user *alteradmin* has not been set up, a field to enable the user *alteradmin* and enter a password is displayed in the “Administrator Settings” table for the user *admin* under the **Personal Profile** tab. See “Personal profile” on page 36.

Once the user *alteradmin* is enabled, only the *alteradmin* can disable the user *alteradmin*. This is performed through the “Administrator Settings” table for the user *alteradmin* under the **Personal Profile** tab. See “Personal profile” on page 36.

Password guidelines

Use the following guidelines when choosing a password:

1. Use between three and sixteen alphanumeric characters.

   The valid characters include: a-z A-Z 0-9%! @ $ ^ & * - _ =\ |., /?;: +

2. Use both upper- and lower-case letters.

   Note: A password is case-sensitive.

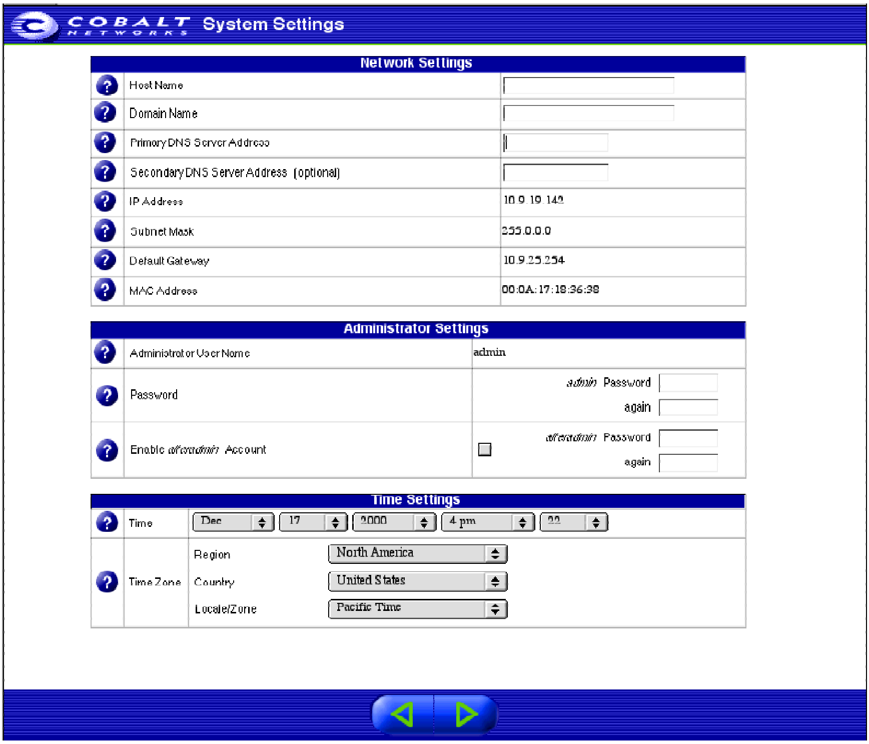
3. Do not use a proper name.
4. Do not use a word found in a dictionary.
5. Do not use a date.
6. Do not use a command word.
7. Do not use a string of consecutive keys on a keyboard (for example, “qwerty”).

Time Settings

Use the pull-down menus to enter the current date, time and time zone on the Sun Cobalt RaQ XTR server appliance.

Once you have configured these settings, click the right arrow at the bottom to move to the next screen.

Figure 12. System Settings



System Settings

Network Settings

Host Name	
Domain Name	
Primary DNS Server Address	
Secondary DNS Server Address (optional)	
IP Address	10.9.19.142
Subnet Mask	255.0.0.0
Default Gateway	10.9.25.254
MAC Address	00:0A:17:18:36:38

Administrator Settings

Administrator User Name	admin	
Password		*admin* Password again
Enable *alteradmin* Account	□	*alteradmin* Password again

Time Settings

Time	Dec · 17 · 2000 · 4 pm · 22	
Time Zone	Region	North America
	Country	United States
	Locale/Zone	Pacific Time

RAID Setup

☞ ***Important:*** The Server Administrator can set the level of RAID only through the Setup Wizard.

Once the Setup Wizard process is complete, the level of RAID cannot be changed unless the system is returned to a factory-fresh state using an OS restore CD.

On this screen, you choose the type of RAID that you want to implement on the server appliance. If the server appliance has only one hard disk drive, this screen does not appear.

The Sun Cobalt RaQ XTR server appliance offers three different levels RAID (depending on the configuration of the server), each with its own advantages and disadvantages:

- **RAID-0** combines the separate hard disk drives into one virtual disk drive and offers the best performance of the three options. However, the data on the disk drives is not redundant and the system is thus not fault-tolerant. This option is available on server configurations with two or more hard disk drives.
- **RAID-1**, also known as disk mirroring, consists of a primary hard disk drive and a secondary hard disk drive; the secondary disk drive is an exact copy or “mirror image” of the primary disk drive. This option is only available on a configuration with two hard disk drives.
- **RAID-5** includes a rotating parity-bit array. All read and write operations can be overlapped. RAID-5 does not store redundant data but it does store the parity information which can be used to reconstruct data in the event of a single hard-disk-drive failure. RAID-5 requires at least three hard disk drives for the array.

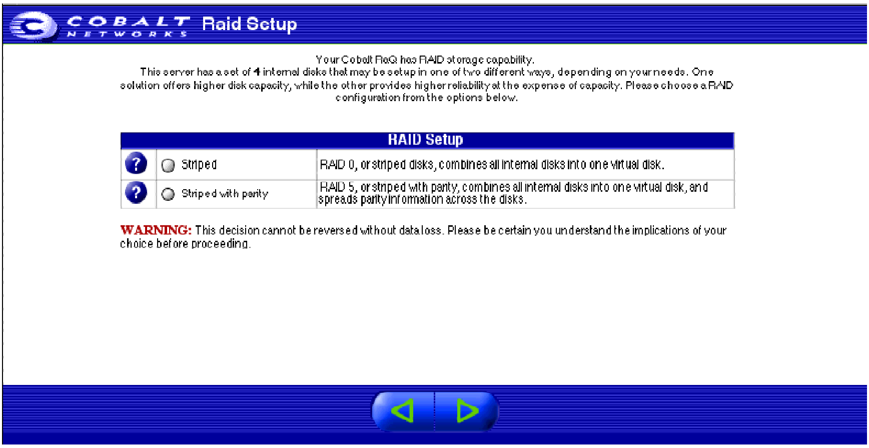
If the server appliance has two, three or four hard disk drives, Figure 13 appears.

- RAID-0 requires at least two hard disk drives.
- RAID-1 (disk mirroring) is only available on a configuration with two hard disk drives.
- RAID-5 requires at least three hard disk drives.

Click the radio button next to the type of RAID you want to implement.

Click the right arrow at the bottom to continue.

Figure 13. RAID setup



Your Cobalt RaQ has RAID storage capability.
This server has a set of **4** internal disks that may be setup in one of two different ways, depending on your needs. One solution offers higher disk capacity, while the other provides higher reliability at the expense of capacity. Please choose a RAID configuration from the options below.

RAID Setup

?	○ Striped	RAID 0, or striped disks, combines all internal disks into one virtual disk.
?	○ Striped with parity	RAID 5, or striped with parity, combines all internal disks into one virtual disk, and spreads parity information across the disks.

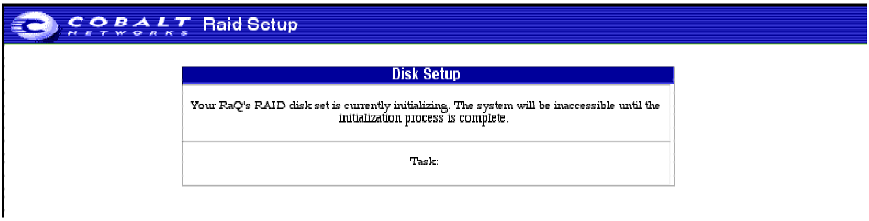
WARNING: This decision cannot be reversed without data loss. Please be certain you understand the implications of your choice before proceeding.

A confirmation dialog asks you to confirm the type of RAID you have selected and warns you that this selection cannot be changed once you have completed the Setup Wizard.

The Sun Cobalt RaQ XTR server appliance server takes a few minutes to initialize the RAID setup; see Figure 14.

Caution: Do not interrupt this process. Interrupting this process can damage the data on your hard disk drives and potentially affect the operating system on the server appliance.

Figure 14. RAID initialization



Disk Setup

Your RaQ's RAID disk set is currently initializing. The system will be inaccessible until the initialization process is complete.

Task:

Registration

The **Registration** screen appears; see Figure 15. If you are connected to the Internet, you can register the Sun Cobalt RaQ XTR server appliance by completing the online registration.

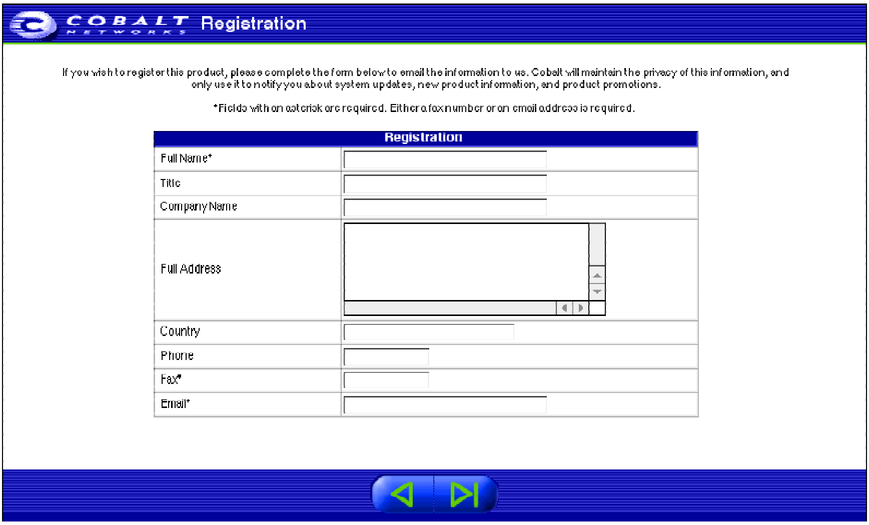
If you do not want to register online at this time, click the right arrow at the bottom to move to the next screen. A confirmation dialog confirms you do not want to register online. See Figure 16.

If you are not connected to the Internet, you cannot register online and the **Registration** screen does not appear.

To register the server online at a later time, see “System Information” on page 161.

Enter your contact information in the fields. Click the right arrow at the bottom to submit your registration; a confirmation dialog states that your registration was sent.

Figure 15. Online Registration

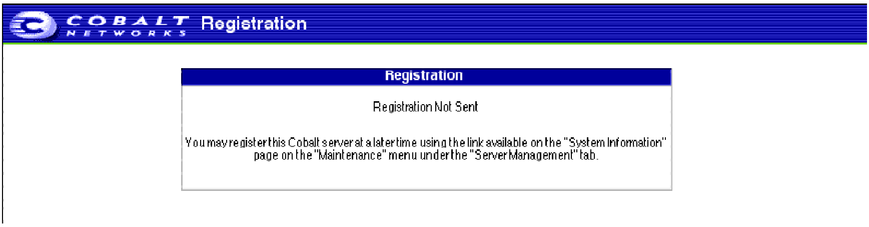


If you wish to register this product, please complete the form below to email the information to us. Cobalt will maintain the privacy of this information, and only use it to notify you about system updates, new product information, and product promotions.

*Fields with an asterisk are required. Either a fax number or an email address is required.

Registration	
Full Name*	
Title	
Company Name	
Full Address	
Country	
Phone	
Fax*	
Email*	

Figure 16. Registration not sent



Registration

Registration Not Sent

You may register this Cobalt server at a later time using the link available on the "System Information" page on the "Maintenance" menu under the "Server Management" tab.

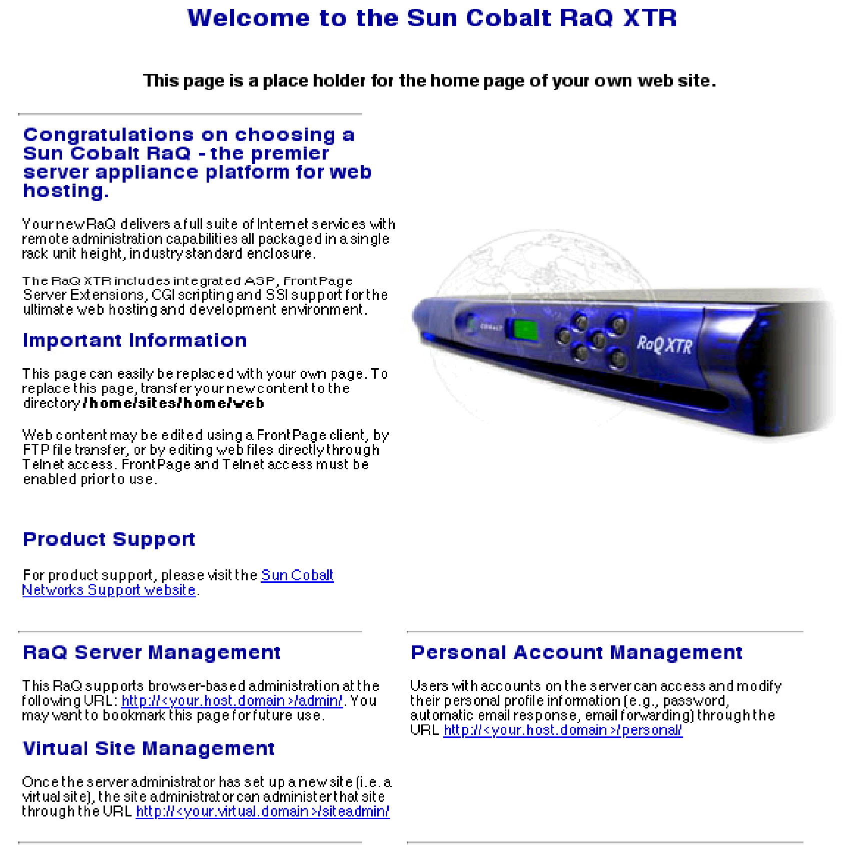
Completing configuration with the Setup Wizard

Once the Sun Cobalt RaQ XTR server appliance has been configured, the default home page of the server appliance appears; see Figure 17.

Choose the level of user at which you want to log on to the server appliance:

- Server Management (Server Administrator)
- Virtual Site Management (Site Administrator)
- Personal Account Management (Site User)

Figure 17. Default home page of the server appliance



Welcome to the Sun Cobalt RaQ XTR

This page is a place holder for the home page of your own web site.

Congratulations on choosing a Sun Cobalt RaQ - the premier server appliance platform for web hosting.

Your new RaQ delivers a full suite of Internet services with remote administration capabilities all packaged in a single rack unit height, industry standard enclosure.

The RaQ XTR includes integrated ASP, FrontPage Server Extensions, CGI scripting and SSI support for the ultimate web hosting and development environment.

Important Information

This page can easily be replaced with your own page. To replace this page, transfer your new content to the directory **/home/sites/home/web**

Web content may be edited using a FrontPage client, by FTP file transfer, or by editing web files directly through Telnet access. FrontPage and Telnet access must be enabled prior to use.

Product Support

For product support, please visit the Sun Cobalt Networks Support website.

RaQ Server Management

This RaQ supports browser-based administration at the following URL: http://<your.host.domain>/admin/. You may want to bookmark this page for future use.

Virtual Site Management

Once the server administrator has set up a new site (i.e. a virtual site), the site administrator can administer that site through the URL http://<your.virtual.domain>/siteadmin/

Personal Account Management

Users with accounts on the server can access and modify their personal profile information (e.g., password, automatic email response, email forwarding) through the URL http://<your.host.domain>/personal/

Site User

This chapter describes the features available to a *Site User* on the Sun Cobalt™ RaQ™ XTR server appliance.

- Programs
- Personal Profile

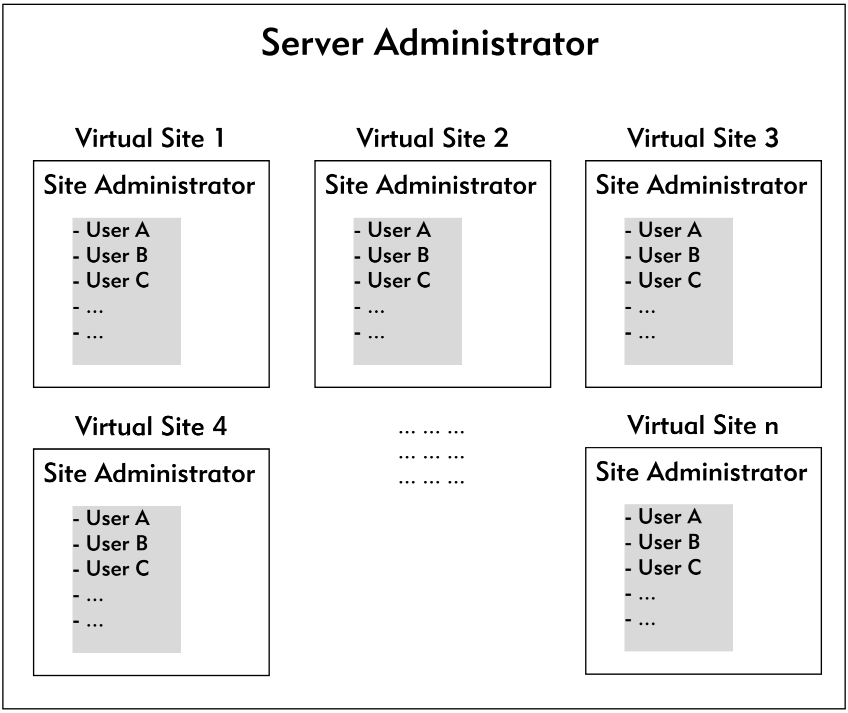
A ***Site User*** can send and receive email through the virtual site, upload and download files using the FTP service provided by the site, publish a personal Web page on the site, and back up and restore files and data located in the home directory.

A site user can also access third-party applications that the Server Administrator has loaded on to the server appliance. These programs appear under the Programs tab.

Site users are added to a virtual site by the Server Administrator or a Site Administrator. A site user has control only over the files located in his or her home directory on the server appliance.

Figure 18 illustrates the level of access, indicated by the shaded area, available to site users.

Figure 18. Level of access for the Site User



Overview of the Site User features

When you log on to the Sun Cobalt RaQ XTR server appliance as an individual user, the Server Desktop user interface (UI) consists of two tabs at the top of the screen: **Programs** and **Personal Profile**.

- The **Programs** tab provides access to third-party applications that the Server Administrator has loaded on to the server appliance.
- The **Personal Profile** tab allows you to configure your personal settings on the server appliance.

Note: To reduce the number of steps in each procedure, the menu commands are grouped together and shown in **bold** type face. Right angle brackets separate the individual items to click.

For example, **Personal Profile > Usage Data** means click on the **Personal Profile** tab in the top menu bar and then click on the **Usage Data** menu item on the left.

Programs

A site user can access third-party applications that the Server Administrator has loaded on to the server appliance.

For more information on third-party applications available for Sun Cobalt server appliances, visit the Solutions Web site at http://www.cobalt.com/solutions/.

Personal profile

The Personal Profile section allows you to view your user-account information.

On the Server Desktop UI, click on the **Personal Profile** tab. The menu items for your account appear on the left: See Figure 19.

- Account
- Email
- Usage Data
- Backup
- Restore

Account

In the Account section, you can change the name on your account and change your password.

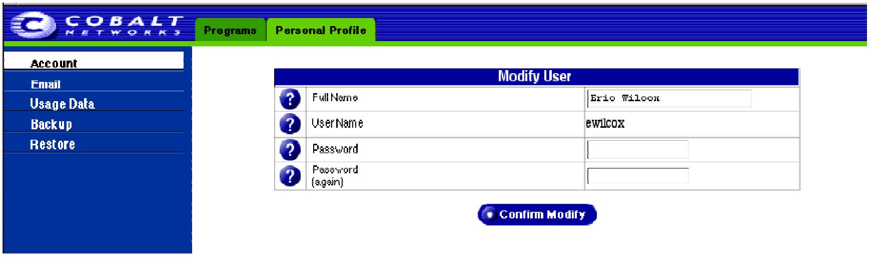
Modifying account information

To modify your account information:

1. Click **Personal Profile > Account**. The “Modify User” table appears; see Figure 19.
2. Modify the following fields:
   a. **Full Name**. This field is mandatory. Modify the name for your account.
   b. **Password.** You can change your password. Enter the password twice for confirmation.

      For more information on choosing a password, see “Password guidelines” on page 26.
3. Click **Confirm Modify**.

Figure 19. Modify User table



Modify User	
Full Name	Eric Wilcox
User Name	ewilcox
Password	
Password (again)	

Email

There are two options available in the Email section: Forward Email To and Vacation Message.

Forward Email To

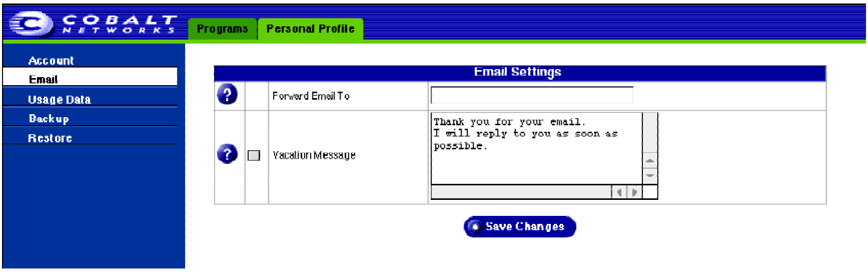
The Forward Email To feature allows you to forward incoming messages to another email address.

To forward your email automatically:

1. Click **Personal Profile > Email**. The "Email Settings" table appears; see Figure 20.
2. In the **Forward Email To** section of the table, enter an email address in the format <xxxxx@yyy.zzz> in the field.

   For more than one email address, separate the addresses with a comma.
3. Click **Save Changes**.

Figure 20. Email Settings table



Email Settings		
	Forward Email To	
□	Vacation Message	Thank you for your email. I will reply to you as soon as possible.

To disable the email forwarding feature:

1. Click **Personal Profile > Email**. The “Email Settings” table appears; see Figure 20.
2. In the **Forward Email To** section of the table, delete the email address from the field.
3. Click **Save Changes**.

Vacation message

The Vacation Message feature allows you to enter a vacation-reply message that is automatically sent to each person who sends you email. This feature is useful when you know that you will not be reading or responding to incoming email messages for a period of time.

A vacation-reply email is sent only once a week to each sender.

Enabling the vacation message

To enable the vacation message:

1. Click **Personal Profile > Email** on the left. The “Email Settings” table appears; see Figure 20.
2. In the **Vacation Message** section of the table, click to enable the check box.
3. In the scrolling text window, type the text of the message you want to send to users while you are away.
4. Click **Save Changes**.

Disabling the vacation message

To disable the vacation message:

1. Click **Personal Profile > Email** on the left. The “Email Settings” table appears; see Figure 20.
2. In the **Vacation Message** section of the table, click to disable the check box.
3. Click **Save Changes**.

Usage Data

In the Usage Data section, you can view the amount of hard-disk-drive space in use, the amount of space available on the hard disk drive, the amount of space allowed and the percentage of hard-disk-drive space in use.

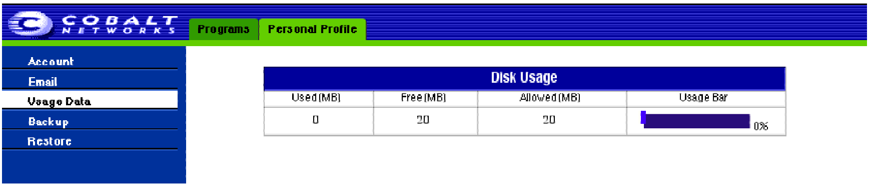
Viewing the usage data

To view the Usage Data statistics:

1. Click **Personal Profile > Usage Data**. The “Disk Usage” table appears with the usage statistics; see Figure 21.

   The table displays the amount of hard-disk-drive space used, the amount of space available on the hard disk drive, the amount of space allowed (all in MB) and the percentage of hard-disk-drive space in use.

Figure 21. Disk Usage screen



Disk Usage

Used (MB)	Free (MB)	Allowed (MB)	Usage Bar
0	20	20	0%

Backup

The Backup feature allows you to back up the data in your account to a personal computer through your browser. The backup captures the files and subdirectories in the home directory of your account on the Sun Cobalt RaQ XTR server appliance.

The extension for a backup file is *.tgz*.

Performing a backup

To perform a backup:

1. Click **Personal Profile > Backup**. The "Personal Data Backup" table appears; see Figure 22.

   The table displays the name of the backup file and the estimated size of the file in megabytes (MB).

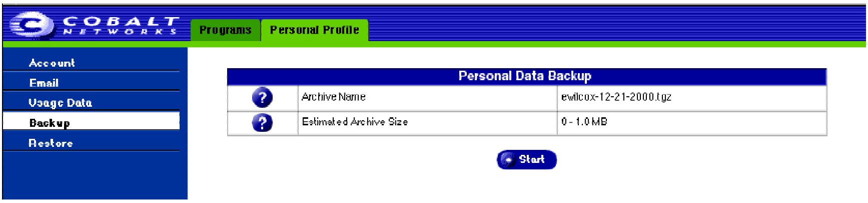
2. The server appliance assigns a default name in the **Archive Name** field; the default name comprises your user name and the date of the backup.

   The **Estimated Archive Size** field provides an estimate of the size of the backup file. The lower value displayed assumes a compression ratio of 2:1 of the files in your home directory. The larger value assumes no compression of the files.

3. Click **Start** to begin the backup process. A dialog appears, asking for a location on your personal computer in which to save the backup file.

4. Choose a location and click **Save**. A percentage bar appears to indicate the progress of the backup.

Figure 22. Personal Data Backup table



Personal Data Backup		
?	Archive Name	ewilcox-12-21-2000.tgz
?	Estimated Archive Size	0 - 1.0 MB

Restore

The Restore feature allows you to restore the files and subdirectories in your home directory from a *.tgz* backup file. For more information, see “Backup” on page 40.

⚠ ***Caution:*** The system does not merge the current data and backed-up data. When data is restored, any changes made to files in your home directory since the last backup are lost.

⚠ ***Caution:*** Be careful not to interrupt the restore operation as data could be corrupted.

Performing a restore

The amount of time required for a restore operation depends on two factors:

- the speed of the connection between the server appliance and the local computer on which the backup archive file resides
- the size of the backup archive file (a larger file takes longer to upload to the site user’s home directory and longer to process on the server appliance)

✍ ***Note:*** It may be more convenient to upload backup archive files to your home directory using an FTP-based application than to upload them through the browser interface.

To perform a restore:

1. Click **Personal Profile > Restore**. The “Personal Data Restore” table appears; see Figure 23.

   - **Existing Archives (.tgz)** You can choose to restore backup archive files (.tgz) that have already been uploaded to your home directory. Select an archive file from the pull-down menu.
   - **Upload an Archive** The server saves backed-up data in an archive file with a .tgz extension. Use the **Browse** button to select the .tgz archive on your computer, or the pull-down menu to select an archive in your home directory.
   - **Selective Restore** You can browse the contents of backup archive files and choose only the files you want to restore.

   ✍ *Note:* The Selective Restore option is enabled by default.

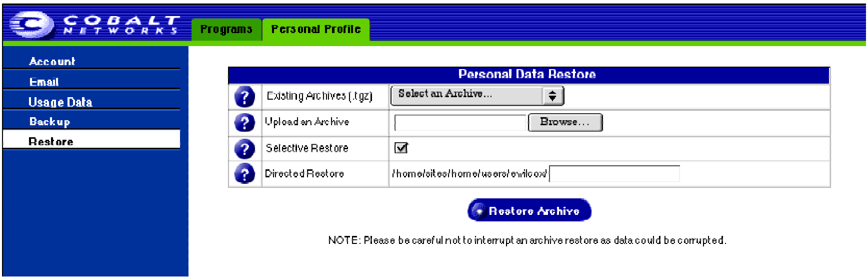
   - **Directed Restore** By default, all files are restored in your home directory. If you enter the name of a subdirectory in this field, the restored files are placed in that subdirectory instead of your home directory. If the specified subdirectory does not exist, the system creates it.
2. Click **Restore Archive** to begin the restore process.
3. If you chose Selective Restore, a separate browser window opens. This window lists the various files that you can restore.

   To select a file or files, click to the enable the check box next to that file name.

   Click **Restore** to continue. The browser window closes.
4. A confirmation dialog appears, asking whether you are sure that you want to continue with the restore process.

   Click **OK**.

Figure 23. Personal Data Restore table



Personal Data Restore	
Existing Archives (.tgz)	Select an Archive…
Upload an Archive	
Selective Restore	☑
Directed Restore	/home/sites/home/users/ewilcox/

NOTE: Please be careful not to interrupt an archive restore as data could be corrupted.

Chapter 4

Site Management

This chapter describes the features available to a *Site Administrator* on the Sun Cobalt™ RaQ™ XTR server appliance.

A ***Site Administrator*** manages a virtual site located on the Sun Cobalt RaQ XTR server appliance; the virtual site provides Web publishing, email and FTP services for the users of the site. The Site Administrator sets up user accounts and access privileges, maintains mailing lists, configures the secure-sockets layer (SSL) settings for the virtual site (if the Server Administrator has enabled SSL on the site), controls the settings for the virtual site and its FTP service, has access to users' email settings, can generate reports about the hard disk drive and Web usage on a virtual site, and can back up and restore files residing on the site.

As the Site Administrator, you can access all of the features described for the site user in Chapter 3, "Site User".

The Server Administrator designates the Site Administrator for each site. The Site Administrator has control only over this virtual site (unless he or she is also the Server Administrator).

The Site Administrator can also designate other site users as a Site Administrator.

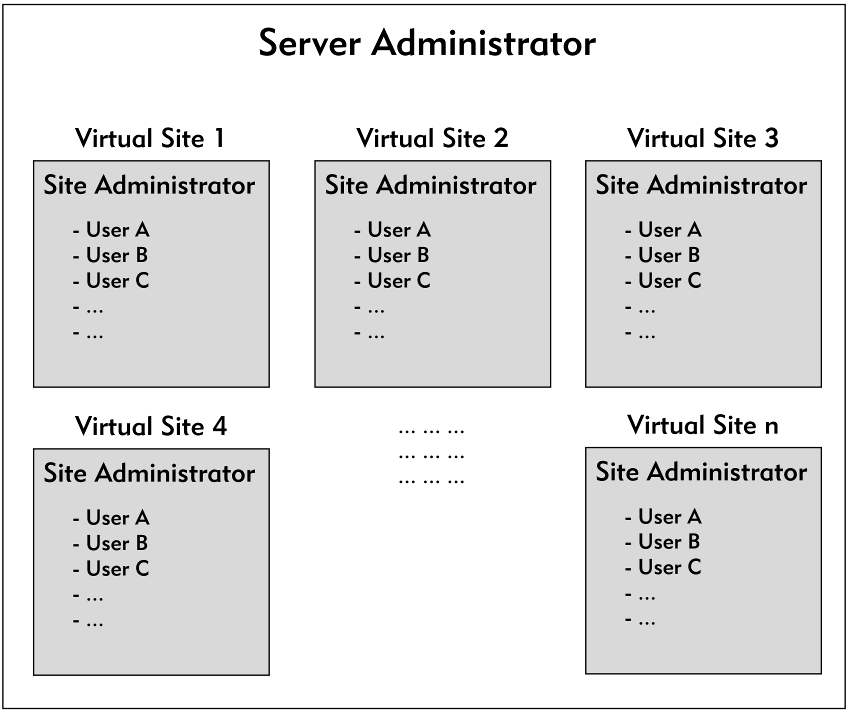
Note: If the Site Administrator for a virtual site is also the Server Administrator, he or she has access to all of the server administration functions as well by logging in as the user *admin*.

Figure 24 illustrates the level of access, indicated by the shaded area, available to Site Administrators.

Note: To reduce the number of steps in each procedure, the menu commands are grouped together and shown in **bold** type face. Right angle brackets separate the individual items to click.

For example, **Site Management > Control Panel > Network** means to click the **<sitename>** tab at the top, then click the **Control Panel** menu item on the left and finally click **Network** in the sub-menu.

Figure 24. Level of access for a Site Administrator



As Site Administrator, you can manage a virtual site using any standard Web browser. To access the **Site Management (<sitename>)** screen for your site, type the URL http://<sitename>/siteadmin/ into your browser. The browser-based user interface (UI), known as the Server Desktop, prompts you for the Site Administrator user name and password. Once you have responded to the prompts, the **Site Management (<sitename>)** screen appears; see Figure 25.

Note: The **Site Management** screen can only be accessed using the fully qualified domain name for the virtual site in the Web browser. The **Site Management** screen is not accessible if an incomplete or aliased site name is specified.

You cannot access the **Site Management** screen for a name-based virtual site by the URL http://<sitename>/siteadmin/ unless a DNS record has been properly set up to point to your server. However, the Server Administrator can always access the **Site Management** screen for a virtual site through the **Server Management** screen.

If you are the Server Administrator, you can also access the **Site Management** functions as the by selecting **Server Management > Site Management**. The “Virtual Site List” table appears, listing all of the virtual sites on the server appliance.

Click the green *pencil* icon next to the virtual site you want to administer. The **Site Management** screen appears; the name of the site is displayed on the tab at the top. From this screen, you can access the Site Management functions.

The **User Management** section appears when you first access the **Site Management** screen. The “User List” table displays the site users initially by user name in ascending order; see Figure 25.

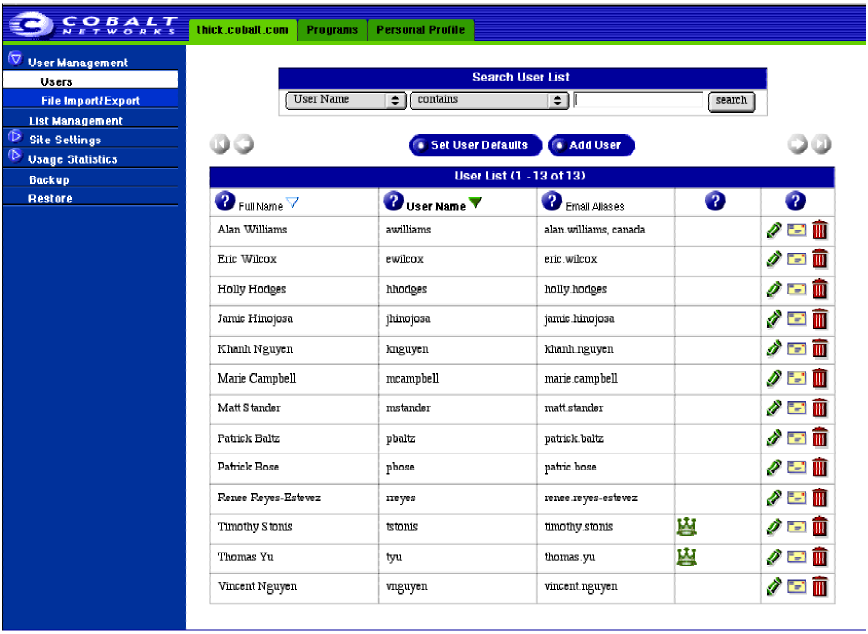
The “User List” table has five columns which display information about the each site user, and allow the Server Administrator or Site Administrator to manage or remove a site user.

- The first column displays the full name of the site user.
- The second column displays the user name of the site user.
- The third column displays the email alias(es) of the site user.
- The fourth column displays icons to indicate which services are enabled for a site user (telnet/shell access, FrontPage Server Extensions or Secure POP 3 [APOP]), to indicate that a site user is the Site Administrator, or to indicate that a site user is suspended.
- The fifth column displays icons to manage a site user’s settings or the email settings for the site user, or to remove a site user.

For an explanation of the icons, see “Preface” on page ix.

The Site Management functions are described in the following sections.

Figure 25. User List table



User List (1 - 13 of 13)

? Full Name ▽	? User Name ▼	? Email Aliases	?	?
Alan Williams	awilliams	alan.williams, canada		✎ ✉ 🗑
Eric Wilcox	ewilcox	eric.wilcox		✎ ✉ 🗑
Holly Hodges	hhodges	holly.hodges		✎ ✉ 🗑
Jamie Hinojosa	jhinojosa	jamie.hinojosa		✎ ✉ 🗑
Khanh Nguyen	knguyen	khanh.nguyen		✎ ✉ 🗑
Marie Campbell	mcampbell	marie.campbell		✎ ✉ 🗑
Matt Stander	mstander	matt.stander		✎ ✉ 🗑
Patrick Baltz	pbaltz	patrick.baltz		✎ ✉ 🗑
Patrick Bose	pbose	patric.bose		✎ ✉ 🗑
Renee Reyes-Estevez	rreyes	renee.reyes-estevez		✎ ✉ 🗑
Timothy Stonis	tstonis	timothy.stonis	♛	✎ ✉ 🗑
Thomas Yu	tyu	thomas.yu	♛	✎ ✉ 🗑
Vincent Nguyen	vnguyen	vincent.nguyen		✎ ✉ 🗑

Organization of the Site Management tab

The following functions are available under the **Site Management (<sitename>)** tab on the Server Desktop UI. These functions are described later in the chapter.

1. User Management (see “User management” on page 50)
   a. Users
   b. File Import/Export
2. List Management (see “Mailing list management” on page 64)
3. Site Settings (see “Site settings” on page 68)
   a. General
   b. FTP
   c. SSL
4. Usage Statistics (see “Usage statistics” on page 83)
   a. Web
   b. FTP
   c. Mail
   d. Disk
5. Backup (see “Backup” on page 91)
6. Restore (see “Restore” on page 95)

User management

The User Management section on the **Site Management** screen allows you to perform administrative functions related to site users: setting the site user defaults, adding or removing users; entering and modifying user names and passwords; managing users' space allocations on the hard disk drive; telnet access and email aliases; and importing or exporting lists of users by text file.

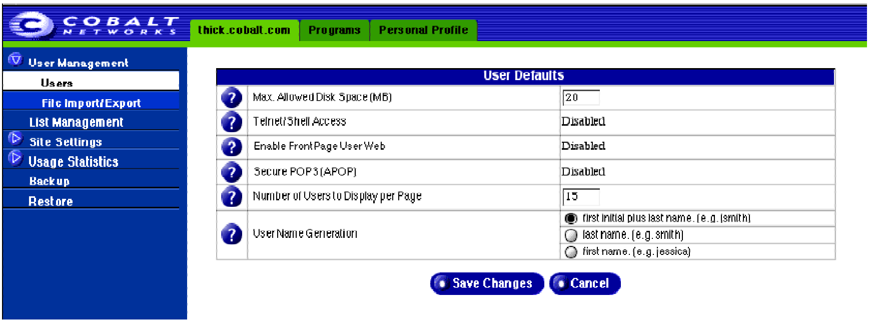
Setting defaults for a site user

Note: Both the Site Administrator and the Server Administrator can configure the site user default settings.

Before assigning the default values for a site user, you must decide on the needs of your users.

Figure 26 shows the screen for configuring the default settings of a site user.

Figure 26. Default settings for a site user



User Defaults	
Max. Allowed Disk Space (MB)	20
Telnet/Shell Access	Disabled
Enable FrontPage User Web	Disabled
Secure POP3 (APOP)	Disabled
Number of Users to Display per Page	15
User Name Generation	● first initial plus last name. (e.g. jsmith) ○ last name. (e.g. smith) ○ first name. (e.g. jessica)

Modifying the default user settings

To modify the default settings for a site user:

1. Select **Site Management > User Management > Users**. The “User List” table appears.
2. Click **Set User Defaults**. The “User Defaults” table appears.
3. Enter the information for the site. You can set the default value for

   - the maximum allowed amount of space (MB) on the hard disk drive available to a newly created user for their file storage and Web pages
   - the number of sites users to display at one time in the “User List” table

   Note: If there are more site users on a virtual site than the value you enter here, navigation buttons for scrolling through the “User List” table become active at the top of the table.

   - the format for generating user login names
     - initial plus last name
     - last name
     - first name

   You can also enable or disable services for telnet/shell access, FrontPage User Web and Secure POP3 (APOP), if the Server Administrator has enabled these services for the virtual site.

4. Click **Save Changes**. The system saves the settings and the “Users List” table reappears.

   Once you have configured the default settings, you can adjust some of the settings for each site user. See “Changing site-user settings” on page 58.

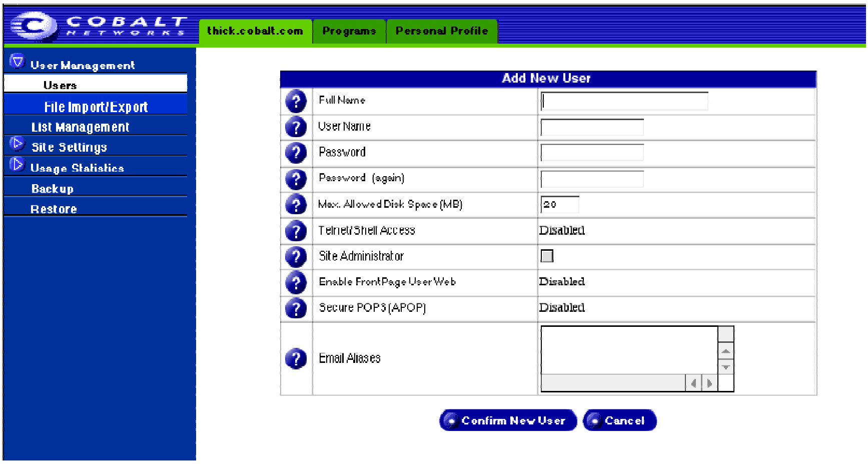
Adding a site user

You can add or remove site users for a virtual site, and assign a Site Administrator for the site.

To import a list of site users from a text file or to export a list of site users to a text file, see “Importing and exporting site users” on page 61.

Figure 27 shows the screen for adding a site user or Site Administrator.

Figure 27. Adding a site user



Add New User

Full Name	
User Name	
Password	
Password (again)	
Max. Allowed Disk Space (MB)	20
Telnet/Shell Access	Disabled
Site Administrator	□
Enable FrontPage User Web	Disabled
Secure POP3 (APOP)	Disabled
Email Aliases	

To add a site user or Site Administrator:

1. Select **Site Management > User Management > Users**. The “User List” table appears.
2. Click **Add User**. The “Add New User” table appears.
3. Enter the information for the site user.
    - site user’s full name
    - site user’s user name (this is generated by the system, but the Site Administrator can edit this field)
    - password (enter the password twice for confirmation)

    Note: The Sun Cobalt RaQ XTR server appliance supports long passwords through the UI. For guidelines on choosing a password, see “Password guidelines” on page 26.

    - maximum amount of space on the hard disk drive allocated to the site (in MB)
    - enable telnet/shell access (if the service has been enabled on the virtual site)
    - optionally, designate the site user as a Site Administrator
    - enable FrontPage user Web (if the service has been enabled on the virtual site)
    - enable Secure POP3 (APOP) (if the service has been enabled on the virtual site)

    You can also enter email aliases for this user. For more information, see “Entering user email settings and aliases” on page 56.
4. Click **Confirm New User**. The screen regenerates and the “User List” table reappears with the new site user.

Search and sort functions

The “User List” table offers a search function and a sort function. See Figure 25. These functions are useful if you have a large number of site users on your virtual site and you want to restrict the display to certain site users.

You can search the list of site users according to the following criteria:

- by user name, full name or email alias
- whether the user name, full name or email alias is equal to the search string, is contained in the search string or is not contained in the search string

The screen regenerates and the results of the search are displayed in a table with the same five columns. The heading of the table now states “Search Results (<x> Users found). To return to the full list of site users, select **User Management > Users** on the left.

Note: Suspended users are listed in the search results.

You can sort the list of site users according to the following criteria:

- by full name, in ascending or descending order
- by user name, in ascending or descending order

Ascending order means from lowest value to the highest value (a–z or 1–9). Descending order means from highest value to the lowest value (z–a or 9–1). By default, the User List table is sorted by user name in ascending order.

A green *triangle* icon indicates the column and order by which the user list is currently sorted. Click the green *triangle* icon on the column head to change the sort order of the user list. The screen regenerates and the results are displayed in a table with the same five columns. The green *triangle* icon points up indicating ascending order or down indicating descending order. In the heading of the column which has not been sorted, a hollow *triangle* icon indicates that the order for the column is random. You can click the hollow *triangle* icon to sort by the items in that column; the icon then turns to a green *triangle*.

You can use the search and sort functions together to produce the display that you need. For example, you can search the list for all site users with “joe” in the full name, and sort the results of that search by email alias in ascending order.

Searching a list of site users

To search the list of site users:

1. In the first field of the Search User List window, select “User Name”, “Full Name” or “Email Alias” from the pull-down menu.
2. In the second field, select “is”, “contains” or “does not contain” from the pull-down menu.
3. In the third field, enter the string of characters for which you want to search.
4. Click **Search**. The screen regenerates and displays the results in a table with the same five columns.

Sorting a list of site users

To sort the list of site users:

1. To sort according to Full Name, click the green *triangle* icon in the heading of the Full Name column. To sort according to User Name, click on the green *triangle* icon in the heading of the User Name column.
2. To sort in ascending (*up-triangle* icon) or descending order (*down-triangle* icon), click on the green *triangle* icon so that it points in the correct direction.
3. The screen regenerates and displays the results in a table with the same five columns.

Removing a site user

To remove a site user:

1. Select **Site Management > User Management > Users**. The “User List” table appears.
2. Locate the site user that you want to remove.
3. Click the red *trashcan* icon next to the site user. A confirmation dialog verifies the deletion.
4. Click **OK** to delete the site user’s account and files.

✍ ***Note:*** If you are deleting a site user who has a large amount of data or if the system determines that the operation will take some time, you are be presented with a status screen while the user is deleted. A final status screen informs you that the user has been deleted successfully.

Entering user email settings and aliases

Mail Forwarding and Vacation Message

Note: Site users can edit the Mail Forwarding and Vacation Message settings through the **Personal Profile** tab. See “Personal profile” on page 36.

Individual site users can choose to have their email forwarded to another email account. Site users can also choose to enable a vacation-reply message that is automatically sent to each person who sends the user an email. This feature is useful when users know they will not be reading or responding to incoming email messages for a period of time.

As the Site Administrator, you can enter these email settings for site users (at their request) as described in “Changing site-user settings” on page 58.

Note: A vacation-reply email is sent only once per week to each sender.

Email aliases

The Email Alias feature allows you to create arbitrary email addresses without creating a user account on the server appliance. An email message addressed to the alias is forwarded to an existing email address. For example, an email alias lets you setup a temporary or permanent alias email address such as sales@mycompany.com and automatically route messages to the mailbox of a specific email user.

Each registered user on the Sun Cobalt RaQ XTR server appliance must have a user name that is unique across all virtual sites on the Sun Cobalt RaQ XTR server appliance. You cannot create two users with the same name on different virtual sites because all users share the same password database file in the underlying operating system. For example, if there is a user with the user name <mary> on virtual site efgh.com, no other registered user on the Sun Cobalt RaQ XTR server appliance can have the user name <mary>. However, user names can be similar: mary, maryb, mary1, mary2.

An email alias is a way to create an account so that more than one user can have the same email name on different virtual sites (<mary> on efgh.com and <mary> on xyz.com). However, the underlying user name for each person must be unique.

For example, the Site Administrator of efgh.com can give Mary Brown the user name <mary>; her email address is mary@efgh.com. The Site Administrator of xyz.com (on the same Sun Cobalt RaQ XTR server appliance server) can give Mary Smith the user name <marys>; the Site Administrator can then set up an email alias mary@xyz.com for Mary Smith. The alias points Mary Smith's incoming messages to the unique user name of <marys> at xyz.com.

A site user can have several email aliases that point to a unique user name. For example, John Smith (user name <john1>) can have john@efgh.com, JS@efgh.com, john.smith@efgh.com, johnny@efgh.com and baseball@efgh.com which all point to his user name of <john1> at efgh.com.

A Site Administrator can also set up useful aliases such as webmaster@efgh.com, info@efgh.com, sales@efgh.com, comments@efgh.com or support@efgh.com that point to a specific user name.

Adding an email alias

To add an email alias for a site user, see "Modify email options for a site user" on page 59.

To create a catch-all account on a virtual site, see "Catch-all email account" on page 60.

Changing site-user settings

Modify settings for a site user

To modify the settings for a site user (to change the name, password, amount of space allocated on the hard disk drive or telnet access for an existing user, to enable FrontPage web use or Secure POP3 [APOP], to make an existing user the Site Administrator or to suspend a site user), click the green *pencil* icon.

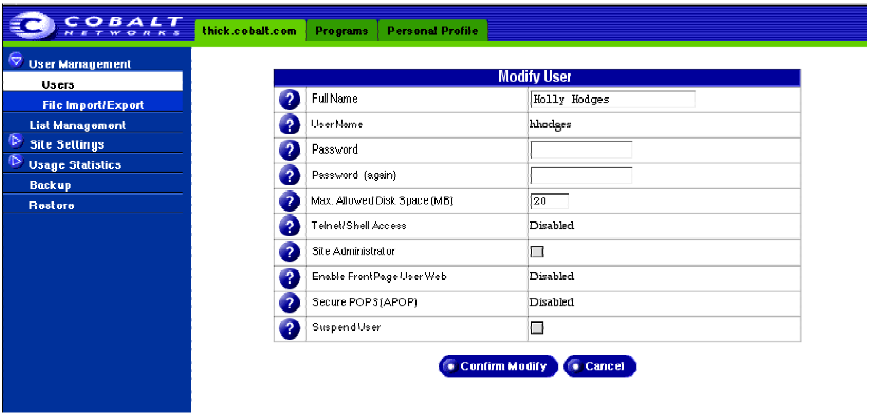
1. Select **Site Management > User Management > Users**. The “User List” table appears.
2. Click the green *pencil* icon for the site user who settings you want to modify. The “Modify User” table appears. See Figure 28.
3. Enter the changes in the Modify User table.

> ***Note:*** The Sun Cobalt RaQ XTR server appliance supports long passwords through the UI. For guidelines on choosing a password, see “Password guidelines” on page 26.

4. Click **Confirm Modify**. The screen regenerates and the “User List” table reappears.

Figure 28 shows the screen for modifying a site user.

Figure 28. Modify User table



Modify User

Full Name	Holly Hodges
User Name	hhodges
Password	
Password (again)	
Max. Allowed Disk Space (MB)	20
Telnet/Shell Access	Disabled
Site Administrator	□
Enable FrontPage User Web	Disabled
Secure POP3 (APOP)	Disabled
Suspend User	□

Modify email options for a site user

To set up or modify the email options for a site user (to enter a forwarding email address, email aliases and an automatic vacation reply), click the *envelope* icon next to the site user.

These options are described in “Entering user email settings and aliases” on page 56.

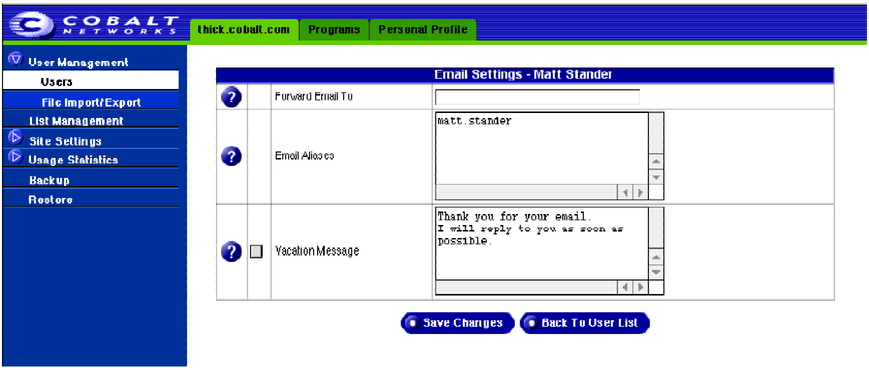
1. Select **Site Management > User Management > Users**. The “User List” table appears.
2. Click the *envelope* icon for the site user. The “Email Settings - <username>” table appears. See Figure 29.
3. To add a forwarding email address, enter the email address in the “Forward Email To” field.
4. To add an email alias, enter the additional names that the user will receive email as in the Email Aliases window. For example, for user <john1>, enter “john.smith”, “johnny” and “baseball”.

   DO NOT add the domain name to the additional names. Since the site user is part of the virtual site, he or she automatically inherits the domain name of the virtual site. If you do add the domain name in the Email Aliases field (for example, johnny@efgh.com), the software gets confused.

   To add several aliases, enter each alias on a separate line.
5. To enable an automatic vacation reply, click to enable the check box in the Vacation Message field and enter your message in the text window.
6. Click **Save Changes**.

Figure 29 shows the screen for modifying a site user’s email options.

Figure 29. Email Settings table



Email Settings - Matt Stander

?		Forward Email To	
?		Email Aliases	matt.stander
?	□	Vacation Message	Thank you for your email. I will reply to you as soon as possible.

Catch-all email account

A catch-all email account receives email messages addressed to former users or non-existent users on a virtual site. For example, if an email is addressed to mary@xyz.com but the user name “mary” does not exist on that domain, the email is routed to the catch-all account.

The Server Administrator or a Site Administrator can create a catch-all email account. This involves simply creating a certain alias for a designated user on the virtual site; this user does not have to be the Site Administrator.

For the user on a virtual site who will receive the messages routed to the catch-all account, you create an email alias of “@<hostname.domainname>”. The <hostname.domainname> is the fully qualified domain name of the virtual site.

1. Select **Site Management > User Management > Users**. The “User List” table appears.
2. Click the *envelope* icon for the site user who will receive the email for the catch-all account. The “Email Settings - <username>” table appears. See Figure 29.
3. Enter “@<hostname.domainname>” in the Email Aliases window.
4. If there is already an alias in the window, add this new alias on a separate line.
5. Click **Save Changes**.

Importing and exporting site users

As Site Administrator, you can import a list of users to a virtual site by uploading a specially formatted text file containing the names of the users and their settings. You can also export the list of users on the virtual site to a text file that is compatible with the import function.

These two functions allow you to rapidly create and maintain accounts for large numbers of site users.

Creating a TSV text file

The first step in importing a list of users is to generate a text file in the required format. The file format used is called tab-separated-value (TSV) format, and contains a separate line for each user you want to add. Each line contains the parameters for the user; a tab character separates each parameter.

The parameter order is the following:

```
<username><tab><fullname><tab><password><tab><email aliases>
```

To specify multiple email aliases for a user, separate each alias with a space character.

Other parameters for a site user, such as the amount of space quota and access privileges, cannot be specified in the file for individual users. However, the settings specified in the User Defaults page are applied to each user imported. Thus, for example, if you wanted all the users in your text file to have FrontPage enabled, you could configure FrontPage "enabled" by default in the User Defaults table.

Note: The Server Administrator must enable a particular service for the virtual site before the Site Administrator can enable that service for a site user.

An example file with two users might look like this:

```
dwest<tab>Doug West<tab>4ng3lf1r3<tab>doug douggie dw

tdurden<tab>Tyler Durden<tab>s04p<tab>tyler td fighter
```

Note: The `<tab>` indicator represents the tab key on your keyboard.

Importing a list of users

To import a list of users:

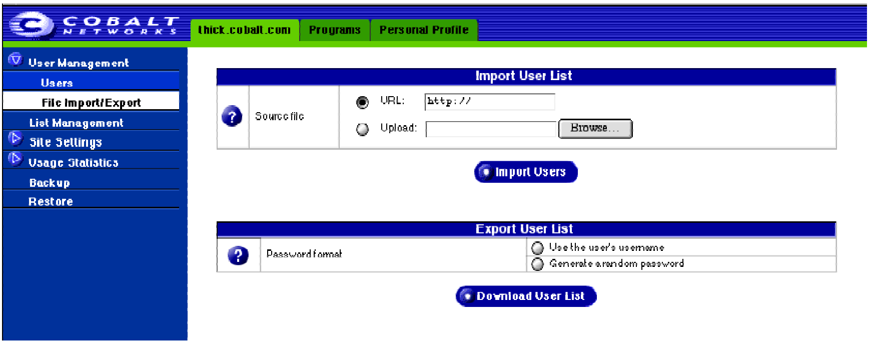
1. Select **Site Management > User Management > File Import/Export**. The “Import User List” and “Export User List” tables appear.
2. In the “Import User List” table (see Figure 30), select whether you would like to download the user list through HTTP from a remote URL or upload the user list from your local machine.

   Enter the URL in the URL field or click **Browse** to locate the file.
3. Click on **Import Users**. The server prompts you with a confirmation dialog.

   If you agree to continue, the server returns a status screen showing you how many lines of the text file have been processed and how many of the users have been successfully added (and not added).
4. Once all the lines in the file have been processed, if errors were encountered, the system displays a summary report. The summary report explains why a particular line failed to add a user.

   If no errors were encountered, the system returns you to the to the “User List” table, displaying the newly added users.

Figure 30. Import/Export User List tables



Import User List

Source file ● URL: http://
○ Upload:

Export User List

Password format ○ Use the user's username
○ Generate a random password

Exporting site users to a text file

You can export the list of users on the virtual site to a text file that is compatible with the Import feature described above. The file is downloaded to the your local machine.

Passwords for users are stored in an encrypted format that does not allow for the recovery of the actual password. Therefore, you have two options for the creating a temporary password for each exported user.

Exporting a list of users

To export a list of users:

1. Select **Site Management > User Management > File Import/Export**. The “Import User List” and “Export User List” tables appear.
2. In the “Export User List” table (see Figure 30), select a default password scheme for creating a temporary password for each exported user. You can have the system generate a random password or assign the site user’s user name as the password.

   Click the radio button for your selection.
3. Click **Download User List**. The server sends the text file to your local machine.

Mailing list management

In the List Management section of the **Site Management** screen, you can create and manage mailing lists for the virtual site.

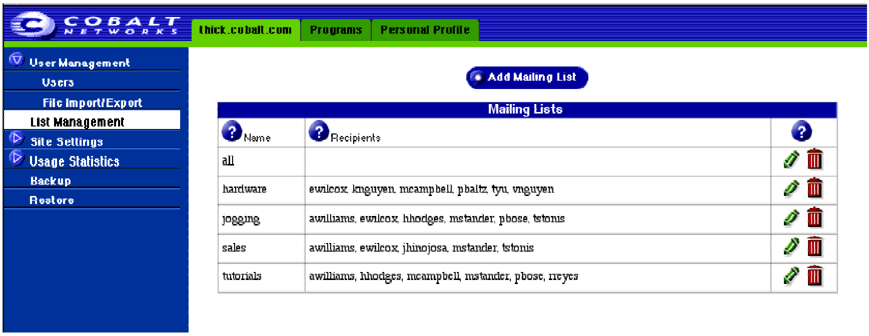
A mailing list allows a discussion by email between a group of people; the email addresses of the people in the group make up the list. The mailing list is given a name, for example monterey_project. The mailing list can include users on the Sun Cobalt RaQ XTR server appliance as well as external users.

A message addressed to the name of the mailing list is delivered to each person on the list.

When replying to a mailing-list message, you can reply either to the original sender only or to the entire mailing list. This function depends on the email client that you are using.

Figure 31 shows the “Mailing Lists” table.

Figure 31. Mailing Lists table



Mailing Lists

Name	Recipients	
all		
hardware	ewilcox, knguyen, mcampbell, pbaltz, tyu, vnguyen	
jogging	awilliams, ewilcox, hhodges, mstander, pbose, tstonis	
sales	awilliams, ewilcox, jhinojosa, mstander, tstonis	
tutorials	awilliams, hhodges, mcampbell, mstander, pbose, rreyes	

Adding a mailing list

To add a mailing list on the server appliance:

1. Select **Site Management > List Management**. The “Mailing Lists” table appears.
2. Click **Add Mailing List**. The “Add Mailing List” table appears. See Figure 32.
3. Enter a name for the mailing list in the Mailing List Name field.

   You can only use lowercase English letters, numbers, and the hyphen (-) and underscore (_) characters. There is no limit on the number of characters in the name.
4. Enter a password for the mailing list. You need the password for managing the mailing list.

   Note: For guidelines on choosing a password, see “Password guidelines” on page 26.
5. The option “Allow user subscriptions to list” allows the individual users to subscribe to or unsubscribe from the mailing list.

   To enable this option, click to enable the check box.

   To subscribe or unsubscribe, the user sends an email to **majordomo@<hostname.domainname>** with the words “subscribe listname” or “unsubscribe listname” in the body of the message. Replace the word <listname> with the name of the mailing list.
6. The option “Allow unsubscribed posting to list” allows email addresses that are not members of the mailing list to send email to the list.

   To enable this option, click to enable the check box.
7. Add external subscribers to the mailing list.

   To add an external subscriber to the mailing list, enter the complete email address in the “External Subscribers” text window (for example, tstonis@xyz.com).

8. Add local subscribers to the mailing list.

   To add an existing site user, select a name in the “Users Not Subscribed” text window and click the left arrow to move the subscriber to the “Users Subscribed” text window.

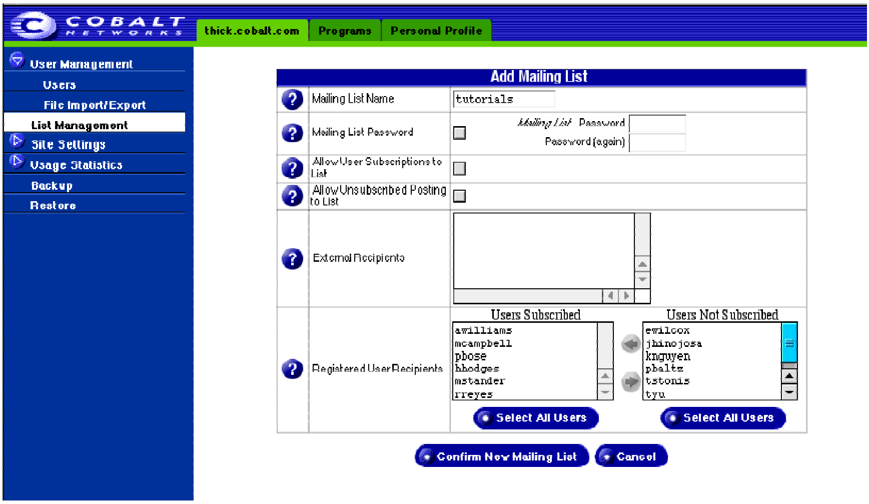
   To remove an existing site user from the mailing list, select a name in the “Users Subscribed” text window and click the right arrow to move the subscriber to the “Users Not Subscribed” text window.

   To select all the registered site users in either text window, click **Select All Users** under the appropriate window.

9. Click **Confirm New Mailing List**.

Figure 32 shows the “Add Mailing List” table in the List Management section.

Figure 32. Add Mailing List table



Add Mailing List

Mailing List Name	tutorials
Mailing List Password	□ *Mailing List* Password Password (again)
Allow User Subscriptions to List	□
Allow Unsubscribed Posting to List	□
External Recipients	
Registered User Recipients	Users Subscribed: awilliams, mcampbell, pbose, bhodges, mstander, rreyes Users Not Subscribed: ewilcox, jhinojosa, knguyen, pbaltz, tstonis, tyu

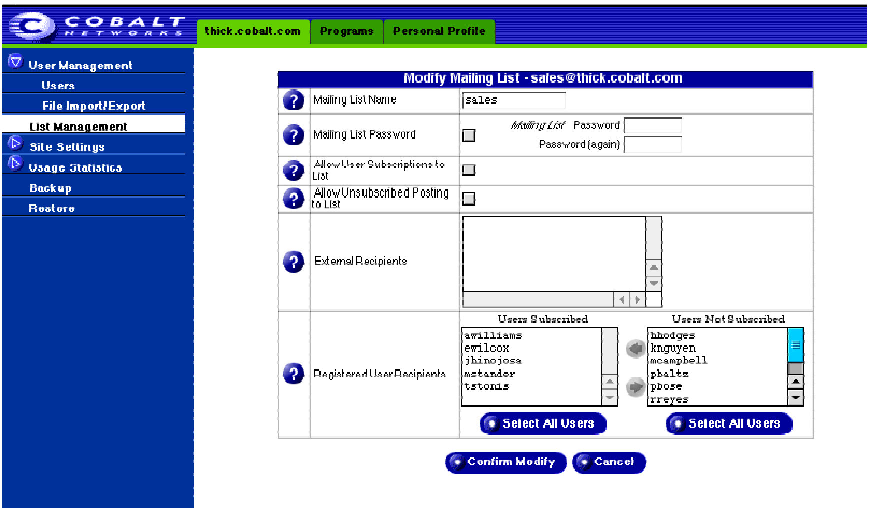
Modifying a mailing list

To modify a mailing list:

1. Select **Site Management > List Management**. The “Mailing Lists” table appears.
2. Click the green *pencil* icon next to the mailing list you want to modify. The “Modify Mailing List” table appears. See Figure 33.
3. Modify the information as necessary (see the procedure for adding a new mailing list for the options).
4. Click **Confirm Modify**.

Figure 33 shows the “Modify Mailing List” table in the List Management section.

Figure 33. Modify Mailing List table



Modify Mailing List - sales@thick.cobalt.com

Mailing List Name	sales
Mailing List Password	□ *Mailing List* Password Password (again)
Allow User Subscriptions to List	□
Allow Unsubscribed Posting to List	□
External Recipients	
Registered User Recipients	Users Subscribed: awilliams ewilcox jhinojosa mstander tstonis Users Not Subscribed: bhodges knguyen mcampbell pbaltz pbose rreyes

Removing a mailing list

To remove a mailing list:

1. Select **Site Management > List Management**. The “Mailing Lists” table appears.
2. Click the red *trashcan* icon next to the mailing list you want to delete. A confirmation dialog box appears.
3. Click **OK** to delete the mailing list.

Site settings

✍ ***Note:*** Only the Server Administrator can modify the virtual site settings.

For Site Administrators who are not the Server Administrator, the Site Settings section is a read-only status page. Services in the "Site Settings" table appear as enabled (a blue *check mark* icon) or disabled (a red *X* icon).

For an explanation of the fields on the Site Settings table, see"Overview of virtual sites" on page 110.

For a view of the Site Settings table, see Figure 34.

In the Site Settings section of the **Site Management** screen, the Server Administrator can:

- view the IP address, host name and domain name of the virtual site
- enable or disable Web server aliases
- enable or disable email server aliases
- change the maximum amount of space allocated on the hard disk drive for the virtual site
- limit the number of site users on a virtual site
- enable or disable access to telnet/shell accounts, CGI scripts, SSL, server side includes, FrontPage server extensions, Active Server Pages (ASP), PHP and Secure POP3 (APOP)
- suspend the virtual site

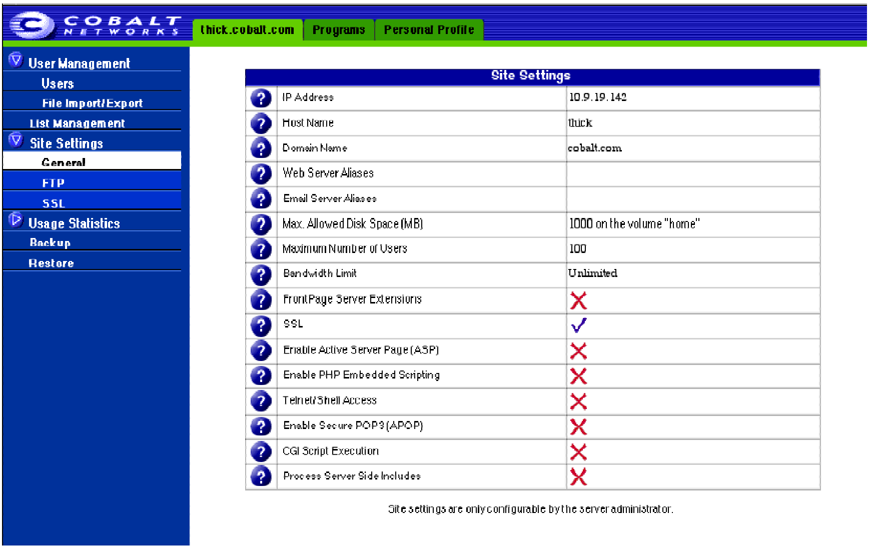
Changing site settings

To change the settings for a particular virtual site, click the green *pencil* icon.

Note: Only the Server Administrator can modify the settings for a virtual site. For Site Administrators who are not the Server Administrator, the Site Settings section is a read-only status screen.

Figure 34 shows the read-only status screen for the site settings of a virtual site.

Figure 34. Read-only status screen of site settings



Site Settings	
IP Address	10.9.19.142
Host Name	thick
Domain Name	cobalt.com
Web Server Aliases	
Email Server Aliases	
Max. Allowed Disk Space (MB)	1000 on the volume "home"
Maximum Number of Users	100
Bandwidth Limit	Unlimited
FrontPage Server Extensions	✗
SSL	✓
Enable Active Server Page (ASP)	✗
Enable PHP Embedded Scripting	✗
Telnet/Shell Access	✗
Enable Secure POP3 (APOP)	✗
CGI Script Execution	✗
Process Server Side Includes	✗

Site settings are only configurable by the server administrator.

To change settings for a particular site:

1. Select **Site Management > Site Settings**. The “Site Settings” table appears.
2. In the “Site Settings” table, you can set the values of the fields or enable the services:

   a. IP address

   b. Host name

   c. Domain name

   > ***Note:*** For the Server Administrator, the IP address, host name and domain name appear as hypertext links in the “Site Settings” table.
   >
   > If you click on a link, the system takes you to the network settings tables under **Server Management > Control Panel > Network**.

   d. Web server aliases

   e. Email server aliases

   f. Maximum allowed disk space (MB)

   g. Maximum number of users

   h. Enable FrontPage Server Extensions

   i. Enable Secure Sockets Layer (SSL)

   j. Enable Active Server Pages (ASP)

   k. Enable PHP Embedded Scripting

   l. Enable shell accounts

   m. Enable Secure POP3 (APOP)

   n. Enable CGI scripts

   o. Enable Server Side Includes

   p. Suspend Site

   > ***Note:*** A Site Administrator does not see the Suspend Site option.

3. Click **Save Changes**.

Common gateway interface (CGI) allows users to have Web sites run programs that dynamically generate HTML pages in response to specific user inputs. CGI scripts can be created on a user's desktop computer and then transferred to the server appliance with a file transfer protocol (FTP) application (as explained in Chapter 6, "Services"). CGI scripts must have a .pl or .cgi filename extension.

If "Email server aliases" are entered, site users can retrieve email at the aliases specified. For example, if the name of the site is raqxtr.efgh.com and the domain names efgh.com and mail.efgh.com are entered, users can receive mail addressed to <username>@raqxtr.efgh.com, <username>@efgh.com, and <username>@mail.efgh.com.

Suspend a virtual site

There are two ways to suspend a virtual site on the server appliance: a hard suspension and a soft suspension.

Soft suspension

The Server Administrator can suspend an individual virtual site.   All of the site users are denied access to telnet, FTP and POP3/IMAP/APOP services, as well as Web access to their files. The site user accounts do not receive email; messages bounce back to the original sender.

To suspend an individual virtual site:

1. Select **Site Management > Site Settings > General**. The "Site Settings" table appears.
2. At the bottom of the table, click to enable the check box Suspend Site.
3. Click **Save Changes**. The server appliance saves the new configuration.
4. If you want to see that the site is suspended, click **Server Management** on the left. The "Virtual Site List" table appears.

   The name and the IP address for the suspended site are grayed-out. You can still modify or delete a suspended site.

Suspend a site user

The Site Administrator or Server Administrator can suspend a site user on a virtual site. The site user is denied access to telnet, FTP, POP3/IMAP/APOP services, as well as Web access to their files. The site user account however still receives email.

To suspend a site user:

1. Select **Site Management > User Management > Users**. The “User List” table appears.
2. Click the green *pencil* icon next to the site user you want to suspend. The “Modify User” table appears.
3. Click to enable the check box Suspend User.
4. Click **Confirm Modify**.

   The “User List” table appears. The entry for the suspended user shows a red X in the fourth column; the full name, the user name and the email alias of the user are grayed-out.

FTP settings

☞ ***Important:*** The Server Administrator can enable anonymous FTP on only one name-based virtual site per IP address. The UI does not allow the administrator to enable anonymous FTP on a second name-based virtual site that shares the same IP address.

✍ ***Note:*** Only the Server Administrator can modify the virtual site settings. For Site Administrators who are not the Server Administrator, the FTP Settings section is a read-only status page.

The Server Administrator can enable the anonymous FTP server for the site, set limits on the size of files that can be uploaded and set the number of simultaneous anonymous users. This feature allows users without passwords to download and upload files through an FTP-based application, up to the specified amount of space allocated on the hard disk drive.

You can only enable anonymous FTP on one name-based virtual site per IP address. The UI does not allow you to enable anonymous FTP on a second name-based virtual site that shares the same IP address.

To change the FTP settings for your virtual site:

1. Select **Site Management > Site Settings > FTP**. The "FTP Settings" table appears.
2. Enter the settings you want. You can specify the number of megabytes (MB) of incoming files to accept and the number of simultaneous users.
3. Click **Save Changes**.

To download files by anonymous FTP, log on to the virtual site with the user name *guest* or *anonymous*—you do not need to enter a password. When you log on with one of these user names, you enter the directory `/home/sites/<sitename>/ftp/`. The Site Administrator can post files here for downloading through FTP client software or a Web browser.

Site Administrators can access the anonymous FTP directory as "/ftp" during an FTP session.

To upload files, you must use FTP client software (for example, Fetch) and access the directory `/home/sites/<sitename>/ftp/incoming/`. Once you have uploaded a file, you (as a guest) cannot see it or access it on the FTP site. All registered site users with telnet/shell privileges can access the file, but only the Site Administrator can access the file through FTP.

The size limit specified for FTP uploads is the total amount of space allocated on the hard disk drive for FTP uploads. If this number is set to 0, a guest cannot upload to the FTP site.

SSL settings

The Server Administrator can administer the Sun Cobalt RaQ XTR server appliance through secure sockets layer (SSL). SSL is provided in 128-bit encryption code and offers a secure Web connection to the end user. The implementation of SSL on the server appliance is based on mod_ssl and BSAFE cryptographic software from RSA Security.

A secure connection means two things: encryption and authentication. Encryption ensures that no one can snoop the connection between the browser and the server appliance; authentication ensures the client, through a certificate, that the server is who they say they are. The security is assured on two levels.

At the network level, the first time the browser connects to a server, the browser stores the server's certificate. This is the encryption part of the secure connection. Each time the browser "thinks" that it is communicating with this same server, it verifies that this same certificate is used to assure the secure connection.

At a higher level, a server's certificate is "signed" by a trusted external authority that the browser knows about, such as VeriSign. This is the authentication part of the secure connection. The server information (country, state, city, organization) is encoded into the certificate and certificate request. The external authority signs your request and guarantees that your server information is legitimate.

For example, if a Web site sends a signed certificate saying that it comes from Sun Microsystems, Inc. in Mountain View, California, United States, the end user can trust (due to the signed certificate from the external authority) that this Web site is indeed run by this company located in this city.

A self-signed certificate is a certificate that has not been signed by an external authority. A self-signed certificate simply ensures that an encrypted Web connection is in place; it does NOT provide authentication to a user that the server is who they say they are.

For more information on *authentication*, *encryption* and *SSL*, refer to Appendix I, "Glossary".

Obtain an externally signed SSL certificate

Most users want to create an externally signed SSL certificate. For e-commerce, an externally signed SSL certificate is required.

To do this, the Server Administrator must perform the following steps. These steps are explained in the following pages.

1. enable the SSL feature on a virtual site (see page 75)
2. generate a self-signed certificate (see page 76)
3. submit the information from the self-signed certificate to an external certification authority (see page 79)
4. receive the response and information from the external certification authority (see page 80)
5. in the SSL settings screen on the server appliance, replace the self-signed certificate with the information received from the externally signed certificate (see page 80)
6. save the changes on the server appliance

Enable SSL on a virtual site

Important: The Server Administrator can enable SSL on only one name-based virtual site on an IP address. The UI does not allow the administrator to enable SSL on a second name-based virtual site that shares the same IP address.

Note: Only the Server Administrator can modify the virtual site settings. For Site Administrators who are not the Server Administrator, the SSL Settings section is a read-only status page.

To enable SSL on a virtual site:

1. Select the **Server Management** tab at the top. The “Virtual Site List” table appears.
2. Click the green *pencil* icon next to the virtual site on which you want to enable SSL. The “User List” table appears.
3. Select **Site Settings > General** on the left side.
4. Click to enable the check box Enable SSL.

   Note: This feature only enables the public Web server; it does not enable the SSL administrative server. See “SSL certificate for the main site” on page 79.

5. Click **Save Changes**.

   The server appliance saves the configuration of the virtual site.

Generate a self-signed certificate

Once the Server Administrator has enabled SSL, the Site Administrator must now create a self-signed certificate. The self-signed certificate can be signed later by an external authority.

1. Under the **Site Management (<sitename>)** tab, select **Site Settings > SSL** on the left side. The “Certificate Subject Information” table appears. See Figure 35.
2. Enter the following information:

   Country—Enter the two-letter country code (for example, AU for Australia or US for United States).

   State—Enter the name of the state (for example, New South Wales or California).

   Locality—Enter the city or locality (for example, Sydney or Toronto).

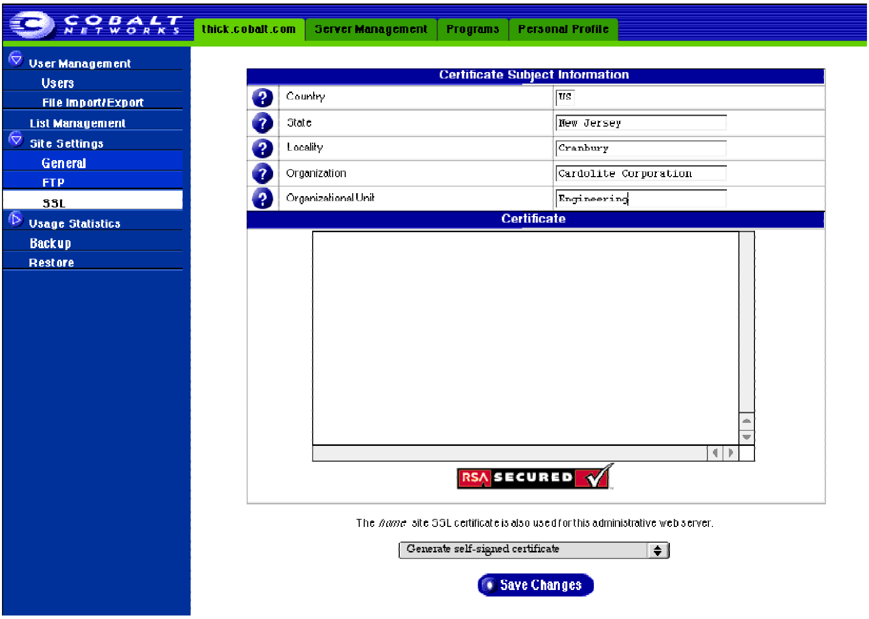
   Organization—Enter the name of the organization (for example, The Widgets Corporation).

   Organizational Unit—As an option, enter the name of a department (for example, Hardware Engineering).
3. Select **Generate self-signed certificate** from the pull-down menu at the bottom.
4. Click **Save Changes**.

   The server appliance processes the information and regenerates the screen with the new self-signed certificate in the Certificate Request and Certificate windows. See Figure 36.

Figure 35 shows the certificate subject information table for an SSL certificate.

Figure 35. Certificate subject information table for an SSL certificate



Certificate Subject Information

Country	US
State	New Jersey
Locality	Cranbury
Organization	Cardolite Corporation
Organizational Unit	Engineering

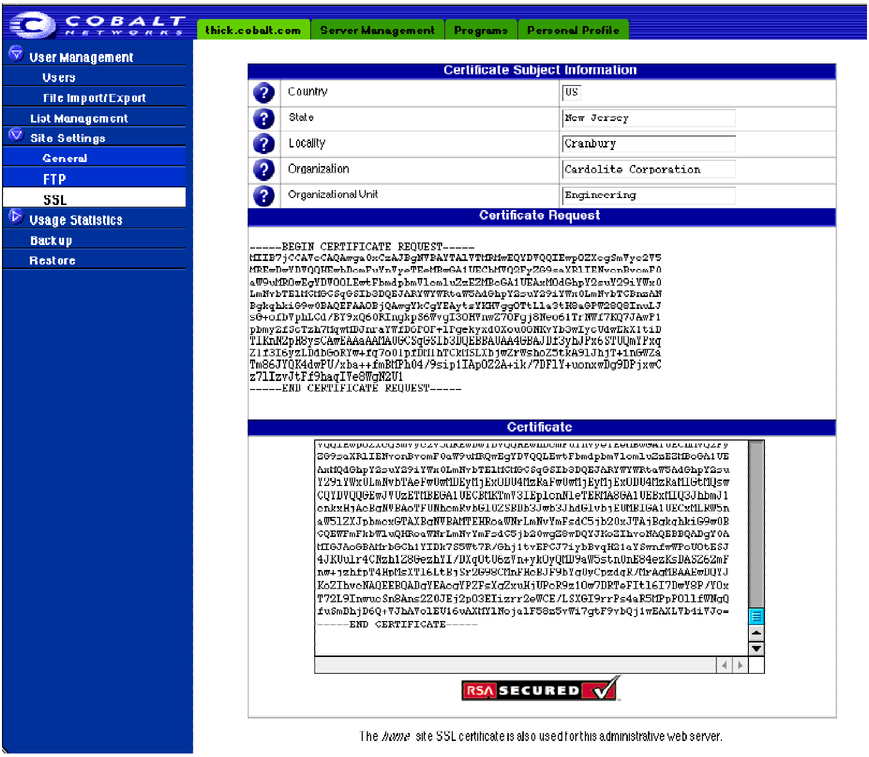
Certificate

The *name* site SSL certificate is also used for this administrative web server.

Generate self-signed certificate

Figure 36 shows the processed information of a self-signed SSL certificate.

Figure 36. Processed information of a self-signed SSL certificate



Certificate Subject Information

Country	US
State	New Jersey
Locality	Cranbury
Organization	Cardolite Corporation
Organizational Unit	Engineering

Certificate Request

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB7jCCAVcCAQAwga0xCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpOZXcgSmVyc2V5
MREwDwYDVQQHEwhDcmFuYnVyeTEeMBwGA1UEChMVQ2FyZG9saXRlIENvcnBvcmF0
aW9uMRQwEgYDVQQLEwtFbmdpbmVlcmluZzEZMBcGA1UEAxMQdGhpY2suY29iYWx0
LmNvbTElMCMGCSqGSIb3DQEJARYWYWRtaW5AdGhpY2suY29iYWx0LmNvbTCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAytsYKHVggOTtLla3tH8aGPW28Q8InuLJ
sG+ofbVphLCd/BY9xQ60RIngkpS6WvgI3OHVnwZ7OFgj8Neo61TrNWf7KQ7JAwP1
pbmy2fScTzh7MqwMDJnraYWfD6POF+lPgekyxd0Xou0GNKyYb3wIycUdwEkX1tiD
TIKnN2pH8ysCAwEAAaAAMA0GCSqGSIb3DQEBBAUAA4GBAJDf3ybJPx6STUQmYPxq
Z1f3I6yzLDdbGoRYW+fq7o01pfDM1hTCkMSLXbjwZrWshoZ5tkA91JhjT+1nGWZa
Tm86JYQK4dwPU/xba++fmBMPh04/9sip1IApOZ2A+ik/7DFlY+uonxwDg9DPjxwC
z7lIzvJtFf9baqIVe8WgN2U1
-----END CERTIFICATE REQUEST-----
```

Certificate

```
ZG9saXRlIENvcnBvcmF0aW9uMRQwEgYDVQQLEwtFbmdpbmVlcmluZzEZMBcGA1UE
AxMQdGhpY2suY29iYWx0LmNvbTElMCMGCSqGSIb3DQEJARYWYWRtaW5AdGhpY2su
Y29iYWx0LmNvbTAeFw0wMDEyMjExODU4MzRaFw0wMjEyMjExODU4MzRaMIGtMQsw
CQYDVQQGEwJVUzETMBEGA1UECBMKTmV3IEplcnNleTERMA8GA1UEBxMIQ3JhbmJ1
cnkxHjAcBgNVBAoTFUNhcmRvbGl0ZSBDb3Jwb3JhdGlvbjEUMBIGA1UECxMLRW5n
aW5lZXJpbmcxGTAXBgNVBAMTEHRoaWNrLmNvYmFsdC5jb20xJTAjBgkqhkiG9w0B
CQEWFmFkbWluQHRoaWNrLmNvYmFsdC5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBAMrbGCh1YIDk7S5Wt7R/Ghj1tvEPCJ7iybBvqH21aYSwnfwWPoU0tESJ
4JKUulr4CNzh1Z8GezhYI/DXqOtU6zVn+ykOyQMD9aW5stn0nE84ezKsDASZ62mF
nw+jzhfpT4HpMsXT16LtBjSr2G98CMnFHcBJF9bYg0yCpzdqR/MrAgMBAAEwDQYJ
KoZIhvcNAQEEBQADgYEAcgVPZFsXgZxuHjUPcR9z10w7DRTeFIt16I7DwY8P/YOx
T72L9InwucSn8Ans2Z0JEj2pO3EIizrr2eWCE/LSXGI9rrPs4aR5MPpPOl1fWNgQ
fuSmDhjD6Q+VJhAVolEU16uAXMYlNojalF58z5vWi7gtF9vbQj1wEAXLVb4iVJo=
-----END CERTIFICATE-----
```

The *Name* site SSL certificate is also used for this administrative web server.

SSL certificate for the main site

If the browser prompts you for your user name and password, you have enabled SSL on the main site of the Sun Cobalt RaQ XTR server appliance. The browser prompts you since this secure connection is in fact a new connection to the server appliance.

Generating a certificate for the main site is a special case and causes three things to happen:

1. SSL is enabled for all server appliance management screens (both server management and site management).
2. The SSL administration server is enabled for the server appliance.
3. The main site certificate request is propagated to all virtual sites that have SSL enabled but do not have their own certificate request.

Now that you have enabled SSL, you can access your virtual site over a secure connection at https://<sitename>.

For more information on obtaining an externally signed certificate, see “Submit the information to an external certification authority” on page 79.

Conversely, deleting the certificate from the main site removes the certificate from the virtual sites to which the certificate has been propagated.

Enable the administration server for SSL

The Sun Cobalt RaQ XTR server appliance supports secure administration. The certificate generated for the main site is also used for secure administration. Therefore, to enable secure administration on a virtual site, generate a certificate for the main site on the server appliance (if this has not already been done.)

Submit the information to an external certification authority

To submit the information from the self-signed certificate to an external certification authority:

1. On the **Site Settings > SSL** screen, highlight and copy the information from the “Certificate Request” window of your self-signed certificate.
2. Open a new browser window and go to the Web site for one of the certification authorities (for example, VeriSign).
3. Paste the information from Step 1 in the window on the Web site of the certification authority. Follow the instructions on the Web site.

Receive the response from the external certification authority

The certification authority either sends you a certificate by email or returns the information on the browser screen.

Enter the information from the external certification authority

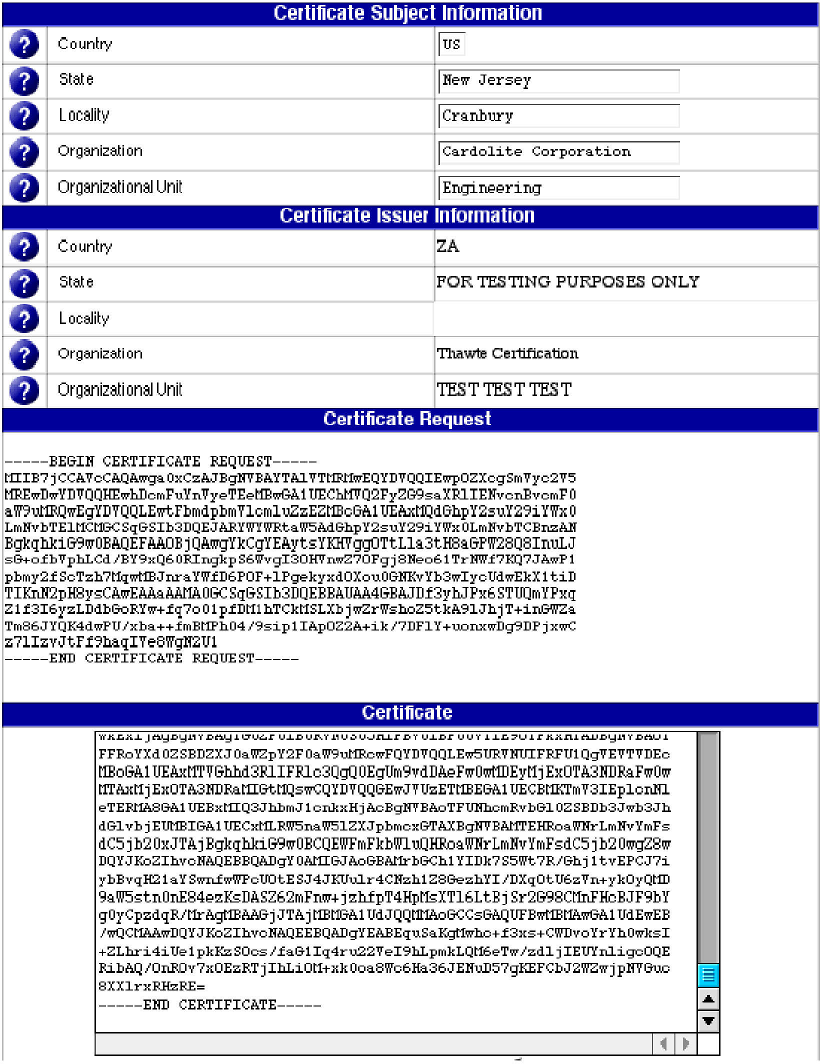
1. Under the **Site Management (<sitename>)** tab, select **Site Settings > SSL** on the left side. The “Certificate Subject Information” table appears.
2. Highlight and remove the information currently in the “Certificate” window.

> ⚠ ***Caution:*** DO NOT choose **Delete certificate** from the pull-down menu at the bottom. This action deletes your SSL certificate and your private key, and you will then have to purchase a new SSL certificate from the external certification authority.

3. On the Web site or in the email from the external certification authority, highlight and copy the information received. (See “Receive the response from the external certification authority” on page 80.)
4. Return to the Server Desktop UI and paste the new certificate information that you copied in Step 3 into the “Certificate” window.
5. Select **Use manually entered certificate** from the pull-down menu at the bottom.
6. Click **Save Changes**.

The browser screen refreshes and the externally signed certificate appears. Figure 37 shows a sample of an externally signed certificate.

Figure 37. Sample of an externally signed certificate



Certificate Subject Information

?	Country	US
?	State	New Jersey
?	Locality	Cranbury
?	Organization	Cardolite Corporation
?	Organizational Unit	Engineering

Certificate Issuer Information

?	Country	ZA
?	State	FOR TESTING PURPOSES ONLY
?	Locality	
?	Organization	Thawte Certification
?	Organizational Unit	TEST TEST TEST

Certificate Request

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB7jCCAVcCAQAwga0xCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpOZXcgSmVyc2V5
MREwDwYDVQQHEwhDcmFuYnVyeTEeMBwGA1UEChMVQ2FyZG9saXRlIENvcnBvcmF0
aW9uMRQwEgYDVQQLEwtFbmdpbmVlcmluZzEZMBcGA1UEAxMQdGhpY2suY29iYWx0
LmNvbTElMCMGCSqGSIb3DQEJARYWYWRtaW5AdGhpY2suY29iYWx0LmNvbTCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAytsYKHVggOTtLla3tH8aGPW28Q8InuLJ
sG+ofbVpbLCd/BY9xQ60RIngkpS6WvgI3OHVnwZ70Fgj8Neo61TrNWf7KQ7JAwP1
pbmy2fScTzh7MqwMBJnraYWfD6POF+lPgekyxdOXou0GNKvYb3wIycUdwEkX1tiD
TIKnN2pH8ysCAwEAAaAAMA0GCSqGSIb3DQEBBAUAA4GBAJDf3yhJPx6STUQmYPxq
Z1f3I6yzLDdbGoRYw+fq7o01pfDM1hTCkMSLXbjwZrWshoZ5tkA91JhjT+inGWZa
Tm86JYQK4dwPU/xba++fmBMPh04/9sip1IApOZ2A+ik/7DFlY+uonxwDg9DPjxwC
z7lIzvJtFf9baqIVe8WgN2U1
-----END CERTIFICATE REQUEST-----
```

Certificate

```
FFRoYXd0ZSBDZXJ0aWZpY2F0aW9uMRcwFQYDVQQLEw5URVNUIFRFU1QgVEVTVDEc
MBoGA1UEAxMTVGhhd3RlIFRlc3QgQ0EgUm9vdDAeFw0wMDEyMjExOTA3NDRaFw0w
MTAxMjExOTA3NDRaMIGtMQswCQYDVQQGEwJVUzETMBEGA1UECBMKTmV3IEplcnNl
eTERMA8GA1UEBxMIQ3JhbmJ1cnkxHjAcBgNVBAoTFUNhcmRvbGl0ZSBDb3Jwb3Jh
dGlvbjEUMBIGA1UECxMLRW5naW5lZXJpbmcxGTAXBgNVBAMTEHRoaWNrLmNvYmFs
dC5jb20xJTAjBgkqhkiG9w0BCQEWFmFkbWluQHRoaWNrLmNvYmFsdC5jb20wgZ8w
DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMrbGCh1YIDk7S5Wt7R/Ghj1tvEPCJ7i
ybBvqH21aYSwnfwWPcUOtESJ4JKUulr4CNzh1Z8GezhYI/DXqOtU6zVn+ykOyQMD
9aW5stn0nE84ezKsDASZ62mFnw+jzhfpT4HpMsXTl6LtBjSr2G98CMnFHcBJF9bY
g0yCpzdqR/MrAgMBAAGjJTAjMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAwGA1UdEwEB
/wQCMAAwDQYJKoZIhvcNAQEEBQADgYEABEquSaKgMwbc+f3xs+CWDvoYrYh0wksI
+ZLbri4iUe1pkKzSOcs/faG1Iq4ru22VeI9hLpmkLQM6eTw/zdljIEUYnligcOQE
RibAQ/OnROv7xOEzRTjIbLiOM+xk0oa8Wc6Ha36JENuD57gKEFCbJ2WZwjpNVGuc
8XXlrxRHzRE=
-----END CERTIFICATE-----
```

Delete an SSL certificate

Caution: If you delete the SSL certificate, you delete the private key as well. If you delete the private key, you will need to purchase a new SSL certificate from the external certification authority.

Note: Deleting the certificate from the main site removes the certificate from the virtual sites to which the certificate has been propagated. In addition, it removes the secure connection to the administration server (it reverts from https: to http:).

If for any reason you want to delete an SSL certificate for a virtual site, perform the following steps.

1. Under the **Site Management (<sitename>)** tab, select **Site Settings > SSL** on the left side. The “Certificate Subject Information” table appears.
2. Select **Delete certificate** from the pull-down menu at the bottom.
3. Click **Save Changes**.

   The server appliance processes the information and regenerates the screen; the Certificate Request and Certificate windows are now blank.

Usage statistics

The Usage Statistics section allows you to view overall usage statistics for the virtual site.

Note: For the Server Usage feature under the **Server Management** tab, see "Server Usage" on page 142.

As the Site Administrator, you can generate server-usage reports for a selected range of dates. The reports allow you to monitor the amount of bandwidth consumed by Web, FTP and email traffic generated by the virtual site, as well as statistics on hard-disk-drive usage for the site.

The reports contain both current data and data that has been compiled from past processed log files. Log files are processed daily at 04:00 a.m.; this process summarizes the data without retaining the actual log file.

The Web, FTP and Mail Usage Summary Statistics tables all share a common format. Reports for each type of statistics are generated in the same way.

Web

To view the statistics for Web traffic on the virtual site:

1. Select **Site Management > Usage Statistics > Web**. If a report has been generated, the "Web Usage Summary Statistics" table appears. See Figure 38.

   If a report has not yet been generated, the "Web Usage Summary Statistics" table does not appear. To generate a report, see Step 3 below.

2. The "Web Usage Summary Statistics" table displays a number of rows of information concerning Web usage, including the dates for which the report was generated.

   A second table entitled "Other Web Usage Statistics" offers hypertext links for more detailed information. Click on a link to see a detailed bar chart for a particular criterion.

   - **Periodic Reports**—This graphically represents the cumulative Web traffic broken down by hour of the day or day of the week. These statistics can help you determine the busy periods for the virtual site.

- **Historical Use**—This graphically represents the total Web traffic broken down by specific day, week or month during the report period. These statistics can help you determine the busiest specific day, week or month for Web traffic on the virtual site.
- **Requests by Domain**—This graphically represents the domains from which Web traffic originated, broken down by domain and, if available, by sub-domain; see Figure 39 for a sample. Sub-domains are indented under their parent domains; the values for the sub-domains are subsumed within, and add up to, the value for the parent domain.

✍ ***Note:*** For this report to contain resolved domain names (for example, .com, .edu or .org), the “Hostname lookups” option must be enabled at the time of the Web traffic. If this option is not enabled, all traffic appears to originate from unresolved IP addresses.

Only the Server Administrator can enable this option. To enable this option, see “Web server” on page 126.

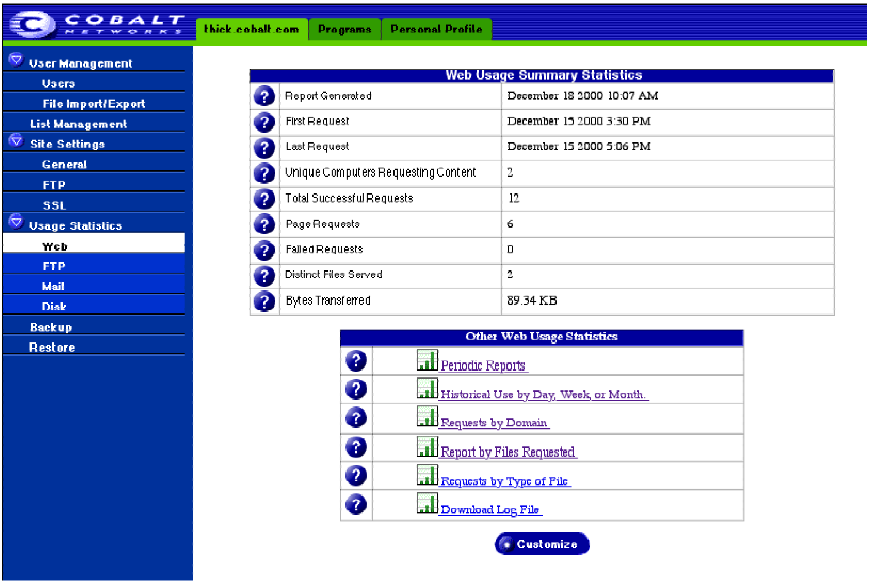
- **Report by Files Requested**—This graphically represents the Web traffic broken down by individual files requested.
- **Requests by Type of File**—This graphically represents the Web traffic broken down by type of file requested.
- **Download log file**—This allows you to download the current Web traffic log file. You can then analyze the log file with external analysis software.

3. To generate a report, click **Customize**. The “Configure Reporting Options” table appears. You can generate a new report for a selected range of dates.
4. From the pull-down menus, choose a start date and end date.
5. Click **Generate Report**. The “Web Usage Summary Statistics” table appears with the new data.

Figure 38 shows a sample summary of Web usage reports on a virtual site.

Figure 39 shows a sample of a Web usage – Requests by Domain report.

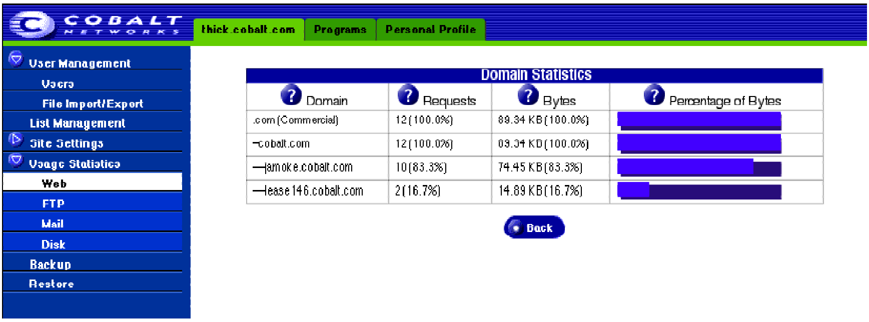
Figure 38. Sample summary of Web usage reports



Web Usage Summary Statistics	
Report Generated	December 18 2000 10:07 AM
First Request	December 15 2000 3:30 PM
Last Request	December 15 2000 5:06 PM
Unique Computers Requesting Content	2
Total Successful Requests	12
Page Requests	6
Failed Requests	0
Distinct Files Served	2
Bytes Transferred	89.34 KB

Other Web Usage Statistics
Periodic Reports
Historical Use by Day, Week, or Month.
Requests by Domain
Report by Files Requested
Requests by Type of File
Download Log File

Figure 39. Sample of Web usage – Requests by Domain report



Domain Statistics			
Domain	Requests	Bytes	Percentage of Bytes
.com (Commercial)	12 (100.0%)	89.34 KB (100.0%)	
¬cobalt.com	12 (100.0%)	89.34 KB (100.0%)	
—jamoke.cobalt.com	10 (83.3%)	74.45 KB (83.3%)	
—lease146.cobalt.com	2 (16.7%)	14.89 KB (16.7%)	

FTP

To view the statistics for FTP traffic on the virtual site:

1. Select **Site Management > Usage Statistics > FTP**. If a report has been generated, the “FTP Usage Summary Statistics” table appears. See Figure 40.

   If a report has not yet been generated, the “FTP Usage Summary Statistics” table does not appear. To generate a report, see Step 3 below.

2. The “FTP Usage Summary Statistics” table displays a number of rows of information concerning FTP usage, including the dates for which the report was generated.

   A second table entitled “Other FTP Usage Statistics” offers hypertext links for more detailed information. Click on a link to see a detailed bar chart for a particular criterion.

   - **Periodic Reports**—This graphically represents the cumulative FTP traffic broken down by hour of the day or day of the week. These statistics can help you determine the busy periods for the virtual site.
   - **Historical Use**—This graphically represents the total FTP traffic broken down by specific day, week or month during the report period. These statistics can help you determine the busiest specific day, week or month for FTP traffic on the virtual site.
   - **Requests by Domain**—This graphically represents the domains from which FTP traffic originated, broken down by domain and, if available, by sub-domain. Sub-domains are indented under their parent domains; the values for the sub-domains are subsumed within, and add up to, the value for the parent domain.
   - **Report by Files Requested**—This graphically represents the Web traffic broken down by individual files requested.
   - **Requests by Type of File**—This graphically represents the FTP traffic broken down by type of file requested.
   - **Download log file**—This allows you to download the current FTP traffic log file. You can then analyze the log file with external analysis software.

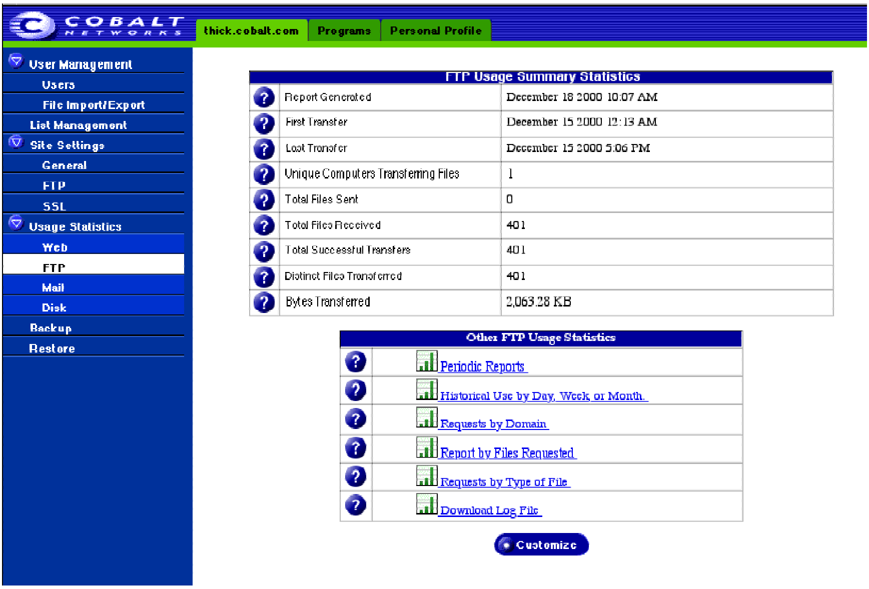
3. To generate a report, click **Customize**. The “Configure Reporting Options” table appears. You can generate a new report for a selected range of dates.

4. From the pull-down menus, choose a start date and end date.

5. Click **Generate Report**. The “FTP Usage Summary Statistics” table appears with the new data.

Figure 40 shows a sample summary of FTP usage reports on a virtual site.

Figure 40. Sample summary of FTP usage reports



FTP Usage Summary Statistics	
Report Generated	December 18 2000 10:07 AM
First Transfer	December 15 2000 12:13 AM
Last Transfer	December 15 2000 5:06 PM
Unique Computers Transfering Files	1
Total Files Sent	0
Total Files Received	401
Total Successful Transfers	401
Distinct Files Transferred	401
Bytes Transferred	2,063.28 KB

Other FTP Usage Statistics

- Periodic Reports
- Historical Use by Day, Week or Month
- Requests by Domain
- Report by Files Requested
- Requests by Type of File
- Download Log File

Mail

To view the statistics for email traffic on the virtual site:

1. Select **Site Management > Usage Statistics > Mail**. If a report has been generated, the “Mail Usage Summary Statistics” table appears. See Figure 41.

   If a report has not yet been generated, the “Mail Usage Summary Statistics” table does not appear. To generate a report, see Step 3 below.

2. The “Mail Usage Summary Statistics” table displays a number of rows of information concerning email usage, including the dates for which the report was generated.

   A second table entitled “Other Mail Usage Statistics” offers hypertext links for more detailed information. Click on a link to see a detailed bar chart for a particular criterion.

   - **Periodic Reports**—This graphically represents the cumulative email traffic broken down by hour of the day or day of the week. These statistics can help you determine the busy periods for the virtual site.
   - **Historical Use**—This graphically represents the total email traffic broken down by specific day, week or month during the report period. This statistic can help you determine the busiest specific day, week or month for email traffic on the virtual site.
   - **Mail Sent or Received by Address**—This shows the email addresses of the users on the virtual site who sent mail and the email addresses that received mail from users on the virtual site. See Figure 42 for a sample.
   - **Download log file**—This allows you to download the current email traffic log file. You can then analyze the log file with external analysis software.

3. To generate a report, click **Customize**. The “Configure Reporting Options” table appears. You can generate a new report for a selected range of dates.

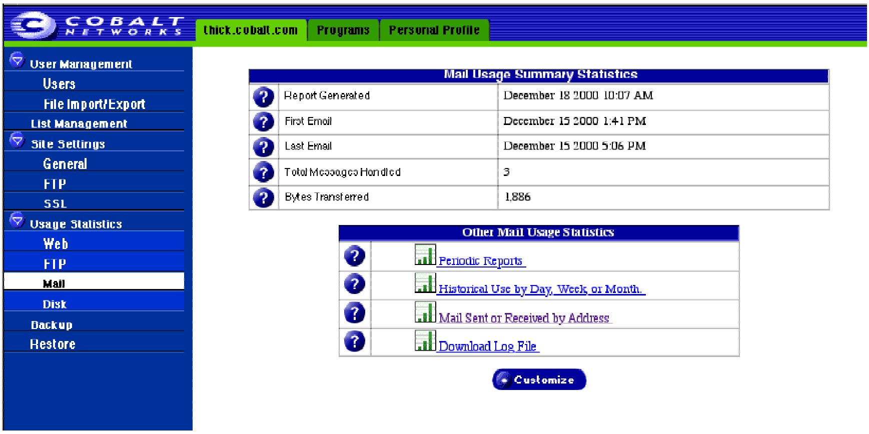
4. From the pull-down menus, choose a start date and end date.

5. Click **Generate Report**. The “Mail Usage Summary Statistics” table appears with the new data.

Figure 41 shows a sample summary of Mail usage reports on a virtual site.

Figure 42 shows a sample of a Mail usage – By Email Received report.

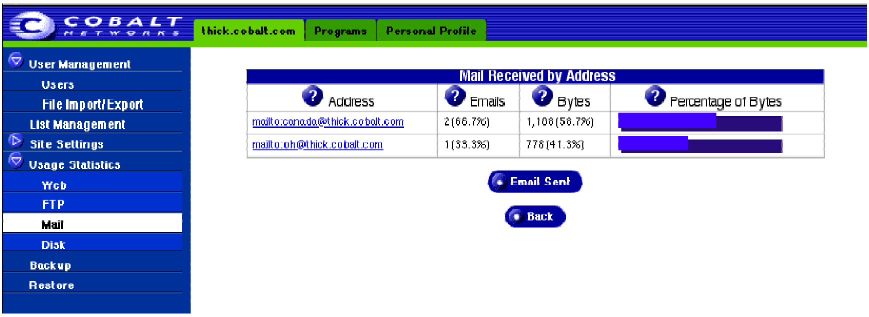
Figure 41. Sample summary of Mail usage reports



Mail Usage Summary Statistics	
Report Generated	December 18 2000 10:07 AM
First Email	December 15 2000 1:41 PM
Last Email	December 15 2000 5:06 PM
Total Messages Handled	3
Bytes Transferred	1,886

Other Mail Usage Statistics
Periodic Reports
Historical Use by Day, Week or Month.
Mail Sent or Received by Address
Download Log File

Figure 42. Sample of a Mail usage – By Email Received report



Mail Received by Address

Address	Emails	Bytes	Percentage of Bytes
mailto:canada@thick.cobalt.com	2 (66.7%)	1,108 (58.7%)	▬
mailto:oh@thick.cobalt.com	1 (33.3%)	778 (41.3%)	▬

Disk

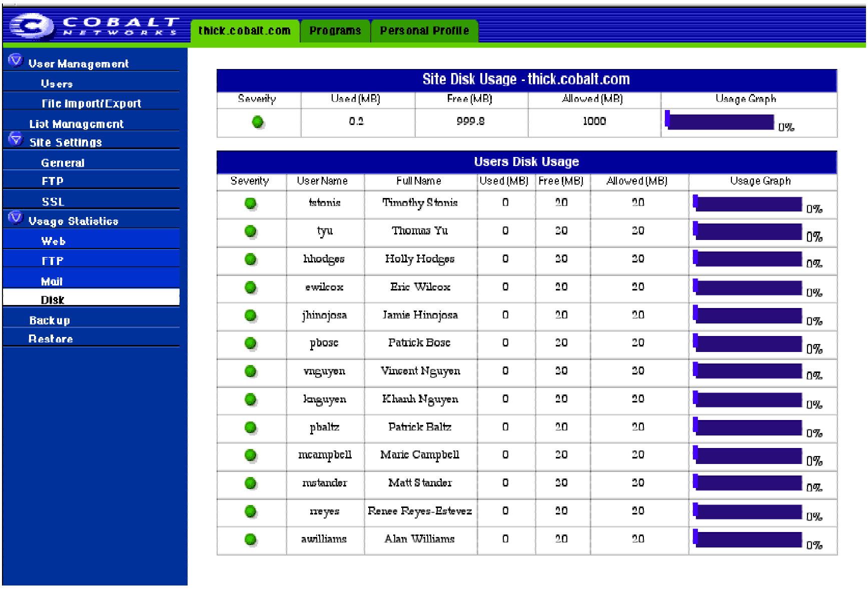
To view the statistics on hard-disk-drive usage on the virtual site, select **Site Management > Usage Statistics > Disk**.

Two tables appear:

- "Site Disk Usage - <sitename>" provides information on hard-disk-drive usage for the entire virtual site
- "Users Disk Usage" breaks down the information on hard-disk-drive usage by site user.

Figure 43 shows a sample summary of hard-disk-drive usage on a virtual site.

Figure 43. Sample summary of hard-disk-drive usage



Site Disk Usage - thick.cobalt.com

Severity	Used (MB)	Free (MB)	Allowed (MB)	Usage Graph
●	0.2	999.8	1000	0%

Users Disk Usage

Severity	User Name	Full Name	Used (MB)	Free (MB)	Allowed (MB)	Usage Graph
●	tstonis	Timothy Stonis	0	20	20	0%
●	tyu	Thomas Yu	0	20	20	0%
●	hhodges	Holly Hodges	0	20	20	0%
●	ewilcox	Eric Wilcox	0	20	20	0%
●	jhinojosa	Jamie Hinojosa	0	20	20	0%
●	pbose	Patrick Bose	0	20	20	0%
●	vnguyen	Vincent Nguyen	0	20	20	0%
●	knguyen	Khanh Nguyen	0	20	20	0%
●	pbaltz	Patrick Baltz	0	20	20	0%
●	mcampbell	Marie Campbell	0	20	20	0%
●	mstander	Matt Stander	0	20	20	0%
●	rreyes	Renee Reyes-Estevez	0	20	20	0%
●	awilliams	Alan Williams	0	20	20	0%

Backup

The Backup feature allows you to back up the data in a virtual site to a personal computer through the browser. The extension for a backup file is *.tgz*.

Caution: A backup operation captures data only (for example, email messages stored on the server or Web files). It does NOT back up the settings for a virtual site or site users.

To perform a backup:

1. Select **Site Management > Backup**. The “Scheduled Site Web Data Backup” table appears. See Figure 44.
2. Fill in the following fields:
   - **Archive Name** This is the suggested name for a backup archive file; it consists of the fully qualified domain name of the virtual site and the date the backup was performed. Your Web browser automatically provides the name of this archive.
   - **Estimated Archive Size** This is the estimated file size of the backup archive file. The lower value displayed assumes a compression ratio of 2:1 of the files. The larger value assumes no compression of the files
   - **Method of Backup** This field allows you to specify the backup method to transfer the backup archive file to your computer. Click the radio button select a method.

     For more information on the fields for each method, see “Backup file locations” on page 94.

     - **Windows File Sharing (SMB)** places the backup file onto a directory shared from a Windows machine.
     - **File Transfer Protocol (FTP)** writes the backup file to an FTP server.
     - **Networks File Sharing (NFS)** places the backup file on a mountable NFS resource.

- **Backup Interval** Select how frequently to back up the data: daily weekly or monthly.
- **Day** The day of the week needs to be set only for weekly or monthly backup intervals. For weekly backups, select the day of the week on which the backup takes. For monthly backups, select the day of the month.

Note: Keep in mind that not all months have 31 days.

If you select “Monthly” as the backup interval and select Day 31, your backup occurs only in months that have 31 days.

- **Start Time** Start Time can be used to specify the exact time of day at which the backup begins.

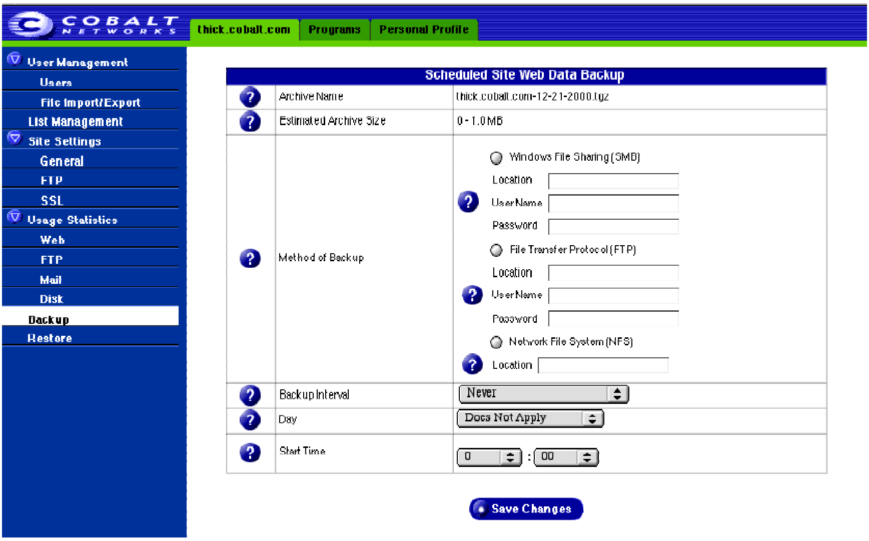
3. Click **Save Changes**.

The file transfer can takes several seconds to several minutes.

Caution: Do not interrupt or cancel the backup process. If you do, or if the file transfer fails for any other reason, delete the partial backup file stored on your personal computer and try again. If you attempt to use a partial file to restore data, you risk corrupting the data already stored on the server.

Figure 44 shows the “Scheduled Site Web Data Backup” table for a virtual site.

Figure 44. Scheduled Site Web Data Backup for a virtual site



Scheduled Site Web Data Backup

Archive Name	thick.cobalt.com-12-21-2000.tgz
Estimated Archive Size	0 - 1.0MB
Method of Backup	○ Windows File Sharing (SMB) Location User Name Password ○ File Transfer Protocol (FTP) Location User Name Password ○ Network File System (NFS) Location
Backup Interval	Never
Day	Does Not Apply
Start Time	0 : 00

Backup file locations

☞ ***Important:*** For all methods of backup, ensure that the target location is available and has enough space on the hard disk drive to hold the backup archive. Failure to do this may result in zero-length or truncated archives.

SMB server

For a backup by **SMB Server** (Windows File Sharing):

- specify a location (fileserver and directory), user name and password
- a location is in the form `\\server\share\dir1\dir2`

FTP server

For a backup by **FTP Server**:

- specify a location (fileserver and directory), user name and password
- a location is in the form `server.name.com/dir1/dir2`

NFS server

For a backup by **NFS Server**:

- specify a location only
- a location is in the form `server:/dir1/dir2`
- a password is not required

Restore

The Restore feature allows you to restore backed-up data from a backup archive file to the Sun Cobalt RaQ XTR server appliance. You can restore files only to their own site, and you must restore data from the same computer on which the data was backed up.

Caution: A restore operation restores data only (for example, email messages stored on the server or Web files). It does NOT restore the settings for a virtual site or site users.

Caution: The system does not merge the current data and backed-up data. When data is restored, any changes made to files on the server appliance since the last backup are lost.

Caution: Be careful not to interrupt the restore operation as data could be corrupted.

Performing a restore

The amount of time required for a restore operation depends on two factors:

- the speed of the connection between the server appliance and the local computer on which the backup archive file resides
- the size of the backup archive file (a larger file takes longer to upload and longer to process on the server appliance)

Note: It may be more convenient to upload backup archive files using an FTP-based application than to upload them through the browser interface.

To perform a restore:

1. Select **Site Management > Restore**. The “Site Data Restore” table appears. See Figure 45.
2. Fill in the following fields:
   - **Existing Archives (.tgz)** You can choose to restore backup archive files (.tgz) that have already been uploaded to the server appliance. Select an archive file from the pull-down menu.

     Once an archive file has been successfully restored, it is be deleted to conserve space on the hard disk drive.
   - **Upload an Archive** The server saves backed-up data in an archive file with a .tgz extension. Use the **Browse** button to select the .tgz archive on your computer, or the pull-down menu to select an archive.
   - **Selective Restore** You can browse the contents of backup archive files and choose only the files you wish to restore.

   ✍ ***Note:*** The Selective Restore option is enabled by default.

   - **Directed Restore** By default all files are restored to the site directory `/home/sites/home/`. If you enter the name of a subdirectory in this field, the restored files are placed in that subdirectory instead of the site directory. If the specified subdirectory does not exist, the system creates it.
3. Click **Restore Archive** to begin the restore process.
4. If you chose Selective Restore, a separate browser window opens. This window lists the various files that you can restore.

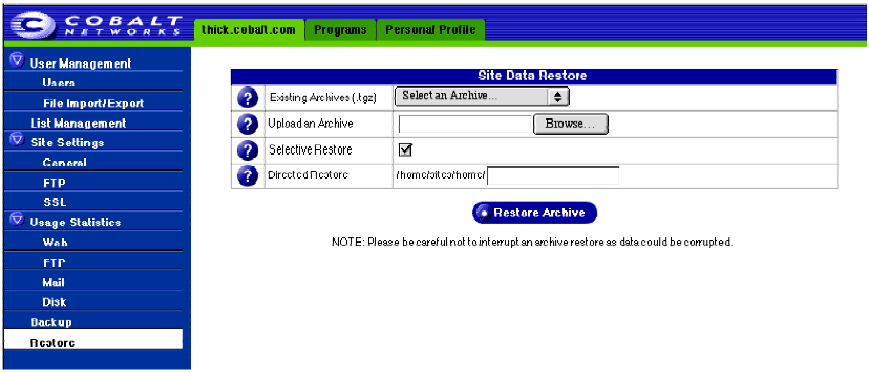
   To select a file, click to the enable the check box next to that file name.

   Click **Restore** to continue. The browser window closes.
5. A confirmation dialog appears, asking whether you are sure that you want to continue with the restore process.

   Click **OK**.

Figure 45 shows the “Site Data Restore” table for a virtual site.

Figure 45. Site Data Restore table



Site Data Restore

?	Existing Archives (.tgz)	Select an Archive...
?	Upload an Archive	Browse...
?	Selective Restore	☑
?	Directed Restore	/home/sites/home/

NOTE: Please be careful not to interrupt an archive restore as data could be corrupted.

Disaster recovery

The Sun Cobalt RaQ XTR server appliance supports the use of third-party solutions for performing disaster recovery. This is different from the backup and restore features within the **Site Management** section.

If you are the Server Administrator, you can configure the client-side software for the disaster-recovery solutions supported on the server appliance. For more information, see “Backup and Restore” on page 151.

For more information on performing disaster recovery and configuring the server-side software for the disaster-recovery solutions, see Appendix F, “Disaster Recovery with Third-Party Software”.

Server management

If you are the Server Administrator, you can return to the **Server Management** screen by clicking the **Server Management** tab at the top.

For more information on managing the server appliance, see Chapter 5, “Server Management”.

Developing and publishing Web pages

For information on developing Web pages, see “Developing Web pages” on page 180.

For information on publishing Web pages on the server appliance, see “Publishing Web pages using FTP” on page 181 and “Publishing Web pages with FrontPage for User Webs only” on page 183.

Server Management

This chapter describes the functions that the Server Administrator normally performs. The Server Administrator accesses these functions under the **Server Management** tab of the Server Desktop user interface (UI).

The ***Server Administrator*** is the person who controls and manages the Sun Cobalt™ RaQ™ XTR server appliance. This person sets up the server appliance, sets up virtual sites, and sets access privileges and provides services for the Site Administrators and site users. The Server Administrator can also act as the Site Administrator for any virtual site.

As Server Administrator, you can access all of the features described for the Site Administrator in Chapter 4, “Site Management” and the site user in Chapter 3, “Site User”.

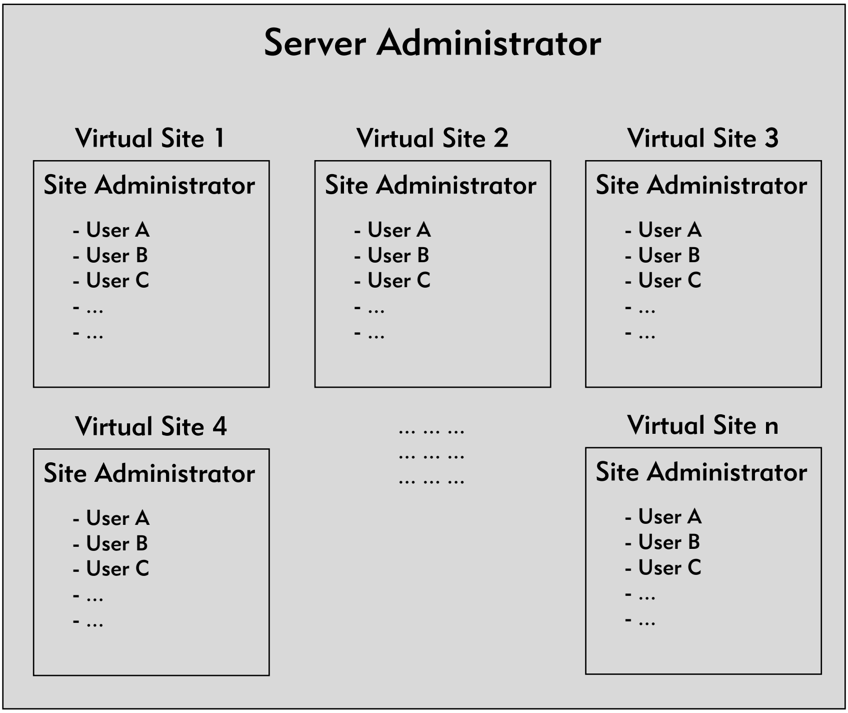
The Server Administrator has the user name *admin* and has full control of the server appliance; the Server Administrator is a member of the main site (which uses the IP address shown on the LCD screen of the server appliance).

Figure 46 illustrates the level of access, indicated by the shaded area, available to a Server Administrator.

✍ ***Note:*** To reduce the number of steps in each procedure, the menu commands are grouped together and shown in **bold** type face. Right angle brackets separate the individual items to click.

For example, **Server Management > Control Panel > Network** means to click the **Server Management** tab in the top menu bar, then click the **Control Panel** menu item on the left and finally click **Network** in the sub-menu.

Figure 46. Level of access for a Server Administrator



Alternate Administrator feature

The Alternate Administrator (*alteradmin*) feature allows a person to have the same level of access to the server as the Server Administrator (*admin*) but without having to use the user name *admin* and password to log in.

For Internet service providers (ISPs) who offer Sun Cobalt RaQ XTR server appliance servers to their customers, this feature allows the ISP access to the server if the Server Administrator has forgotten or incorrectly entered the password for the user *admin*.

Setting up an alteradmin account

As the Server Administrator, you can specify an *alteradmin* in two ways:

- in the Setup Wizard (see “System Settings” on page 25)
- in the “Administrator Settings” table for the user *admin* (see “Personal profile” on page 36)

Once the user *alteradmin* has been set up, the user *alteradmin* does not appear on the server appliance or in the Server Desktop UI to any other user, including the Server Administrator.

If the user *alteradmin* has not been set up, a field to enable the user *alteradmin* and enter a password is displayed in the “Administrator Settings” table for the user *admin* under the **Personal Profile** tab. See “Personal profile” on page 36.

Once the user *alteradmin* is enabled, only the *alteradmin* can disable the user *alteradmin*. This is performed through the “Administrator Settings” table for the user *alteradmin* under the **Personal Profile** tab. See “Personal profile” on page 36.

Approaches to server appliance administration

As Server Administrator, you can decide how many of the server functions he or she wants to manage directly and how much to delegate.

- **Full control**. If you want to control all the functions on the server appliance, you can create virtual sites without assigning any virtual Site Administrators. You are responsible for managing the main site and all the virtual sites. (See "Definition of a virtual site" on page 103.)
- **Hybrid control**. If you want to control some of the server appliance functions and delegate others, you can assign some of the virtual sites to virtual Site Administrators (for the sites that have a user capable of acting as a Site Administrator), and retain control of other virtual sites. You are responsible for managing only the sites that do not have a Site Administrator.
- **Distributed control**. If you want to delegate responsibility for all the virtual sites, you can create Site Administrators for all the virtual sites. In this case, you are responsible for managing only server settings and virtual site services. The Site Administrators are responsible for managing the virtual sites.

You manage the Sun Cobalt RaQ XTR server appliance using through a Web browser. Access the **Server Management** screen by typing either http://<IP address> /admin/ or http://<hostname.domainname> /admin/ into your browser. These Web pages are password-protected—you must enter your Server Administrator password.

When you log in to the server appliance with the user name *admin* or *alteradmin*, the Server Desktop UI has tabs (see Figure 47). This screen is used for the management tasks that are performed only by the Server Administrator (*admin*) or the alternate administrator (*alteradmin*).

1. Setting up and maintaining the Sun Cobalt RaQ XTR server appliance.
2. Creating virtual sites.
3. Creating access privileges and providing services for the Site Administrators and site users.

The Server Administrator functions are described in the sections that follow.

Definition of a virtual site

Whereas industry uses the term “virtual host”, we use the term “virtual site”.

In our definition, a virtual site consists of a Domain Name System (DNS) domain with Web, FTP and email services. Each virtual site contains its own list of site-user accounts. Each site-user account has its own Web page, FTP directory, email spool and any number of email aliases. The fully qualified domain name of a virtual site is unique to that site, while its IP address can be shared by many sites.

With the advent of name-based virtual hosting, it is no longer necessary to dedicate an IP address to a virtual site. The Web server can now differentiate among target virtual sites according to the name requested. Many virtual sites on the Sun Cobalt RaQ XTR server appliance can share one IP address. However, not all services are compatible with name-based virtual hosting: SSL encryption for Web data, bandwidth management and an anonymous FTP account can only be enabled on one name-based virtual site per IP address hosted by the server appliance.

The IP address of the server appliance can be shared by many virtual sites or it can be unique to one virtual site.

The server appliance has one main site (which cannot be deleted) and virtual sites. The main site uses the IP address assigned to the server appliance using the LCD console.

On the **Server Management > Site Management** screen, the main site is listed in the “Virtual Site List” table; the *trashcan* icon in the third column for the main site is grayed-out (disabled), as this site cannot be deleted from the list of virtual sites. The options and features available on a virtual site can also be configured for the main site.

Organization of the Server Management tab

The following functions are available under the **Server Management** tab on the Server Desktop UI. These functions are described later in the chapter.

1. Site Management (see “Site management” on page 106)
   a. Set default settings for a virtual site
   b. Add a virtual site
   c. Manage a virtual site (clicking the green pencil takes you to the **Site Management** screen for that virtual site)
   d. Delete a virtual site (clicking the green pencil takes you to the **Site Management** screen for that virtual site)
   e. Access the home page of a virtual site by clicking its host name (shown as a hypertext link)
   f. Search the list of virtual sites
2. Control Panel (see “Control panel” on page 124)
   a. Services
   b. Network
   c. Bandwidth
   d. Time
3. Server Usage (see “Server Usage” on page 142)
   a. Network
   b. Web
   c. FTP
   d. Mail
4. Backup and Restore (see “Backup and Restore” on page 151)
   a. Control
   b. Knox Arkeia
   c. Legato Networker
   d. Veritas NetBackup

5. Maintenance (see “Maintenance” on page 156)
    a. Storage
    b. Reboot
    c. Shutdown
    d. System Information
6. Active Monitor (see “Active Monitor” on page 162)

Organization of the BlueLinQ tab

The following functions are available under the **BlueLinQ** tab on the Server Desktop UI. For more information on these functions, see “BlueLinQ” on page 168.

1. New Software
2. Updates
3. Installed Software
4. Settings

Site management

The Sun Cobalt RaQ XTR server appliance is designed to host multiple virtual sites. A virtual site is an individual location on the Internet, such as www.efgh.com or www.xyz.com. Each virtual site can have a unique set of users who can send and receive email, publish Web pages, or upload and download files through FTP. A virtual site can also provide anonymous FTP access and SSL.

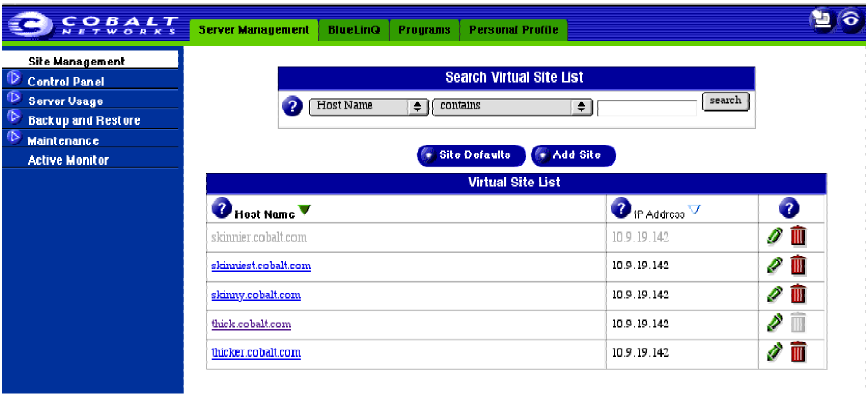
Note: A virtual site can be name-based or IP-based. If there are several name-based virtual sites on an IP address, only one name-based virtual site can use anonymous FTP and SSL services.

The server appliance can host a large number of IP-based virtual sites. The number of virtual sites depends on the amount of hard-disk-drive space available on the server, the amount of hard-disk-drive space allocated for each site, the amount of traffic generated on each site and the amount and complexity of the dynamic Web content on each site (for example, ASP, CGI, PHP and others). Dynamic Web content on an individual site induces a much heavier load on the server than does static content.

Under **Server Management > Site Management**, you can create and manage virtual sites hosted by the server appliance. A table displays the virtual sites on the server appliance; see Figure 47.

The main site of the Sun Cobalt RaQ XTR server appliance (the host name and domain name displayed on the LCD screen) also appears in this table; the *trashcan* icon in the third column for the main site is grayed-out (disabled), as this site cannot be deleted from the list of virtual sites. The options and features available on a virtual site can also be configured for the main site.

Figure 47. List of virtual sites in the Site Management section



Host Name	IP Address	
skinnier.cobalt.com	10.9.19.142	✎ 🗑
skinniest.cobalt.com	10.9.19.142	✎ 🗑
skinny.cobalt.com	10.9.19.142	✎ 🗑
thick.cobalt.com	10.9.19.142	✎ 🗑
thicker.cobalt.com	10.9.19.142	✎ 🗑

The “Virtual Site List” table has three columns which display information about the site, and allow you to manage or remove a site.

- the virtual sites are displayed by host name in ascending order
- The first column displays the host name of the virtual site.

  The host name appears as a hypertext link. If you click on the link, a separate browser window opens and displays the home page for that site.
- The second column displays the IP address of the virtual site.
- The third column displays icons to manage a site or to remove a site.

✍ ***Note:*** The *trashcan* icon for the main site on the server appliance is grayed-out (disabled), as this site cannot be deleted from the list of virtual sites.

✍ ***Note:*** If the host name and IP address of a virtual site appear in grayed-out text (disabled), the site has been suspended by the Server Administrator.

For an explanation of the icons, see “Preface” on page ix.

Search and sort functions

The “Virtual Site List” table offers a search function and a sort function. These functions are useful if you have a large number of virtual sites on your server appliance and you want to restrict the display to certain virtual sites.

You can search the list of virtual sites according to the following criteria:

- by host name (whether the host name is equal to, is contained in or is not contained in the search string)
- by IP address (whether the IP address is equal to, is within or is not within a specified subnet)
- by a specific service enabled on a site

The screen regenerates and the results of the search are displayed in a table with the same three columns. The heading of the table now states “Search Results (<x> Virtual Sites found). To return to the full list of virtual sites, click **Site Management** on the left.

Note: Suspended sites are included in the search results.

You can sort the list of virtual sites according to the following criteria:

- by host name, in ascending or descending order
- by IP address, in ascending or descending order

Ascending order means from lowest value to the highest value (a–z or 1–9). Descending order means from highest value to the lowest value (z–a or 9–1). By default, the “Virtual Site List” table is sorted by host name in ascending order.

The screen regenerates and the results are displayed in a table with the same three columns. In the heading of the column which has been sorted, a green *triangle* icon points up (ascending order) or down (descending order). In the heading of the column which has not been sorted, a hollow *triangle* icon indicates that the column is not sorted.

You can use the search and sort functions together to produce the display that you need. For example, you can search the list for all virtual sites with “test” in the host name, and sort the results of that search by IP address in ascending order.

Searching a list of virtual sites

To search the list of virtual sites:

1. In the “Search Virtual Site List” table, select “Host Name”, “IP Address” or “Site Uses” from the first pull-down menu.

   Figure 48 shows the screen for seaching by a particular service enabled on the virtual sites.

2. Select the criteria according to which you want to search from the second pull-down menu.

3. In the text field, enter the string of characters for which you want to search. If you are searching for sites with a specific service, leave this field blank.

4. Click **Search**. The screen regenerates and displays the results in a table with the same three columns.

Sorting a list of virtual sites

To sort the list of virtual sites:

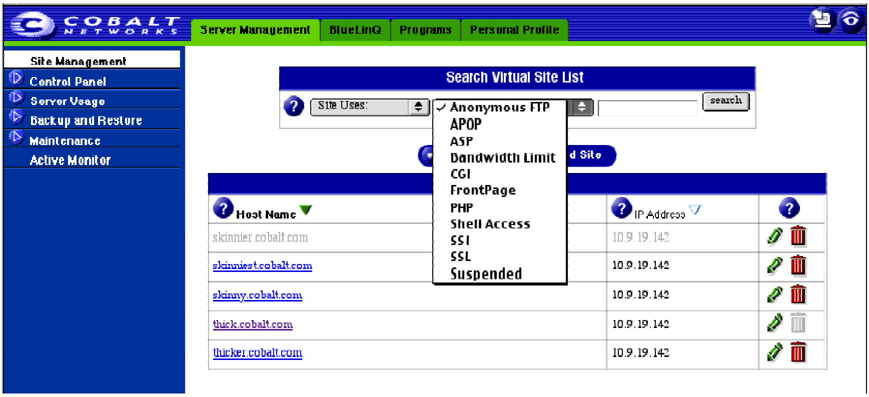
1. To sort according to Host Name, click on the green *triangle* icon in the heading of the Host Name column.

   To sort according to IP Address, click on the green *triangle* icon in the heading of the IP Address column.

2. To sort in ascending (*up-triangle* icon) or descending order (*down-triangle* icon), click on the green *triangle* icon so that it points in the correct direction.

   The screen regenerates and displays the results in a table with the same three columns.

Figure 48. Searching a virtual site by service enabled



Host Name ▼	IP Address ▽	
skinnier.cobalt.com	10.9.19.142	
skinniest.cobalt.com	10.9.19.142	
skinny.cobalt.com	10.9.19.142	
thick.cobalt.com	10.9.19.142	
thicker.cobalt.com	10.9.19.142	

Overview of virtual sites

The Sun Cobalt RaQ XTR server appliance supports both name-based and IP-based virtual hosting.

As the Server Administrator, you can set up the virtual sites, as described in “Adding a virtual site” on page 119. The following list of information is helpful when creating a site.

- **IP address**—To use the server appliance, you require an IP address or range of IP addresses.

✍ ***Note:*** The Sun Cobalt RaQ XTR server appliance supports name-based virtual sites allowing many sites to share a single IP address. You can create many virtual sites using the same IP address (for example, 192.168.25.77) as long as the fully qualified domain name for each site is different (for example, both www.efgh.com and www.xyz.com can use 192.168.25.77 as their IP address).

- **Host name**—Each virtual site requires a host name (for example, *www*, *ftp* or *raqxtr*). If the site is connected to the Internet, you must know the IP address used by the host name.
- **Domain name**—Each virtual site also requires a domain name (for example, *efgh.com* or *xyz.com*).

  You must register the domain name. Visit the Internet Corporation for Assigned Names and Numbers (ICANN) at http://www.icann.org. for a list of accredited domain-name registrars.

✍ ***Note:*** The Sun Cobalt RaQ XTR server appliance can serve as the DNS server and provide the host name.

- **Web server aliases**—You can add aliases for Web servers; you are not restricted to receiving web requests only on the domain name entered in the site settings.

  For the virtual site, enter additional host names or domain names for which to accept web requests. For example, enter the aliases *domain.com* and *www.domain.com*. This allows the same site to be accessed by the URLs *http://domain.com* and *http://www.domain.com*.

  Separate multiple entries with a comma.

  ✍ ***Note:*** You must configure the DNS records to resolve the alias addresses in addition to the virtual site name.

- **Email server aliases**—You can add aliases for email servers; you are not restricted to receiving email messages only on the *hostname.domainname* as entered in the site settings.

  For the virtual site, enter additional host names or domain names for which to accept email connections (on SMTP port 25). For example, enter the aliases *domain.com* and *mail.domain.com*.

  Separate multiple entries with a comma.

- **Automatic DNS configuration**—You can have the server automatically create DNS records for this virtual site. If enabled, the server appliance acts as the primary DNS server for this site. The default setting for this feature is OFF.

  If the Web server aliases or email server aliases have the same domain name as this site, DNS records are created for these aliases as well.

  For more information, see "Automatic configuration of DNS records" on page 117.

  ✍ ***Note:*** This feature does not register the new site name with a top-level domain name registrar. You must register the new site name.

  Visit the Internet Corporation for Assigned Names and Numbers (ICANN) at http://www.icann.org. for a list of accredited domain-name registrars.

- **Maximum allowed disk space (MB)**—You can set the amount of space on the hard disk drive that a virtual site can use, and can change this value at any time. The value is in megabytes (MB) and must be a whole number greater than zero.

  You can choose where to store a new virtual site. In the “Add New Virtual Site” table, in the Maximum allowed disk space (MB) parameter, a pull-down menu lists in alphabetical order the available disk storage devices. The storage device with the most available space is chosen by default.

  Once you have created a virtual site, you cannot change its location.

  For more information, see “Storage” on page 156.

- **Maximum Number of Users**—You can limit the number of users that a Site Administrator can create; you can change this value at any time.

- **Enable FrontPage Server Extensions**—You can enable Microsoft FrontPage™ Server Extensions for Web page development on each virtual site. Site Administrators can create and delete user FrontPage webs individually.

  When FrontPage Server Extensions are enabled on a virtual site, you must enter a password for the FrontPage client *webmaster* account. For more information, see “FrontPage Server Extensions” on page 114.

- **Enable Anonymous FTP**—Users without passwords can download and upload files through FTP up to the specified amount of space allocated on the hard disk drive. You can enable the anonymous FTP server for any virtual site. You can also limit the amount of data that can be uploaded anonymously and the total number of anonymous users who can access the virtual site simultaneously.

> ***Note:*** A virtual site can be name-based or IP-based. If there are several name-based virtual sites on an IP address, only one name-based virtual site can use anonymous FTP.

- **Enable SSL**—The server appliance provides an optional secure sockets layer (SSL) for web access. See “SSL settings” on page 73.

  Only the Server Administrator can enable SSL on a virtual site.

Note: A virtual site can be name-based or IP-based. If there are several name-based virtual sites on an IP address, only one name-based virtual site can use SSL service.

- **Enable Active Server Pages (ASP)**—The server appliance supports ASP scripting language. For more information, see “Active Server Pages (ASP)” on page 115.
- **Enable PHP Embedded Scripting**—The server appliance supports PHP embedded scripting. For more information, see “PHP embedded scripting” on page 116.
- **Enable Shell Accounts**—The site users of the virtual site being created can telnet to the server appliance and run commands from a Linux shell. If you have enabled this feature, you or the Site Administrator can grant shell access for an individual user.

Caution: Granting shell access can greatly compromise the security of your server appliance.

- **Enable Secure POP3 (APOP)**—You can enable the Authentication Post Office Protocol (APOP) for a virtual site. APOP is a challenge-response authentication scheme built on top of the standard POP protocol. APOP is designed in a way that protects your password when being sent across the network.

Note: If you enable APOP for a user, that user can check his or her email only through an APOP client; a regular POP3 client will not work unless APOP is disabled for that user.

- **Enable common gateway interface (CGI) scripts**—You can enable this virtual site and all the site users to have CGI-based dynamic Web content on the server appliance.

  CGI allows a user to have a Web site run programs that dynamically generate hypertext markup language (HTML) pages in response to specific user inputs. CGI scripts can be created on a user's desktop computer and then transferred to the server appliance with a file transfer protocol (FTP) application.

- **Enable Server Side Includes**—The server appliance can correctly display server-parsed Web pages (.shtml).

FrontPage Server Extensions

When you enable FrontPage Server Extensions on a virtual site, a FrontPage client *webmaster* account is created and you must provide a password for the *webmaster* account.

Note: The FrontPage user *webmaster* is a part of the FrontPage Server Extension software and is not a true Linux site-user account. As such, it does NOT have Web, email or FTP service. It is simply an account to use in the FrontPage client.

If FrontPage Server Extensions are enabled on a virtual site, the "Site Settings" table (**Site Management > Site Settings > General**) shows a check box indicating that the feature is enabled. If you disable FrontPage Server Extensions on a virtual site and save the changes, the "Site Settings" table refreshes to show the feature as disabled and a *webmaster* password field is now displayed in the table. If you re-enable FrontPage Server Extensions on that virtual site, you must provide a password again for the *webmaster* account.

If you do not enter a password after you enable FrontPage Server Extensions and then try to save changes, the UI will not accept the changes. An error message appears at the bottom of the screen informing you that you must enter a password for the *webmaster* account.

Each virtual site has a separate *webmaster* account and a unique *webmaster* password.

Once the *webmaster* has authenticated through the FrontPage client, he or she can:

- modify Web content
- manage FrontPage site Root Web subwebs
- add, modify or remove additional FrontPage user accounts
- change the *webmaster* password

Note: User webs cannot manage subwebs or FrontPage user accounts.

For more information on the FrontPage features, refer to the user documentation for the FrontPage client software.

Active Server Pages (ASP)

The Sun Cobalt RaQ XTR server appliance uses Sun Chili!Soft Active Server Pages (ASP) software.

ASP is an HTML-embedded scripting language that includes one or more small embedded programs, or *scripts*, that are processed on a Web server before the Web page is sent to the user. An ASP is somewhat similar to a server-side include or a common gateway interface (CGI) application in that all three involve programs that run on the server, usually tailoring a page for the user.

For example, an ASP script can use the input from the user's request for the page to access data from a database. The script then builds or customizes the page on the fly and returns it to the requestor. The Web server does all of the processing, and a standard HTML page is generated and sent to the browser.

It is not necessary to enable the ASP Administrative Server (under **Server Management > Control Panel > Services**) in order to enable ASP on an individual virtual site.

ASP Administrative Server

The ASP Administrative Server allows you to configure your ASP service through a separate browser-based UI. It does not need to be turned on to allow site users to serve ASP pages; this interface runs on port 5100.

You can access the ASP Administrative Server screen from the **Server Management** screen. The ASP Administrative Server user interface includes a link to the ASP HTML documentation files.

For more information, see “ASP Administrative Server” on page 135.

PHP embedded scripting

The Sun Cobalt RaQ XTR server appliance supports PHP Version 4 embedded scripting.

As with ASP, PHP is an HTML-embedded scripting language that includes one or more small embedded programs, or *scripts*, that are processed on a Web server before the Web page is sent to the user.

Much of the PHP syntax is borrowed from C, Java and Perl with a couple of unique PHP-specific features thrown in. The goal of the language is to allow Web developers to write dynamically generated pages quickly.

For more information on PHP, visit the URL http://www.php.net.

Automatic configuration of DNS records

This feature is disabled by default.

As the Server Administrator, you can enable or disable the Automatic DNS Configuration feature in three different tables:

- the “Virtual Site Defaults” table (under the **Server Management** tab, select **Site Management > Site Defaults**)
- the “Add a New Virtual Site” table (under the **Server Management** tab, select **Site Management > Add Site**)
- the “Site Settings” table for a virtual site (under the **Server Management** tab, click the green *pencil* icon for a virtual site in the “Virtual Site List” table, and then select **Site Settings > General**)

If you enable the Automatic DNS Configuration feature for a new or existing virtual site, the system creates DNS Forward (A) records for that virtual site. The system also creates Forward (A) records for any Web server aliases or email server aliases that share the virtual site’s domain name.

If you disable the Automatic DNS Configuration feature for a virtual site, the DNS records that were created automatically are not deleted. For this reason, the Site Administrator or Server Administrator can enable the Automatic DNS Configuration feature and then immediately disable the feature. This allows the administrator to create for the virtual site a basic set of DNS records that will be maintained manually.

If you delete a virtual site on which the Automatic DNS Configuration feature is enabled, the system deletes the DNS records that were automatically created for that site, including the records for any Web server and email server aliases that share the virtual site’s domain name.

If you delete a virtual site on which the Automatic DNS Configuration feature is disabled, the system does not deletes the DNS records for that virtual site.

For more information on DNS, see Appendix E, “Domain Name System”.

Setting defaults for a virtual site

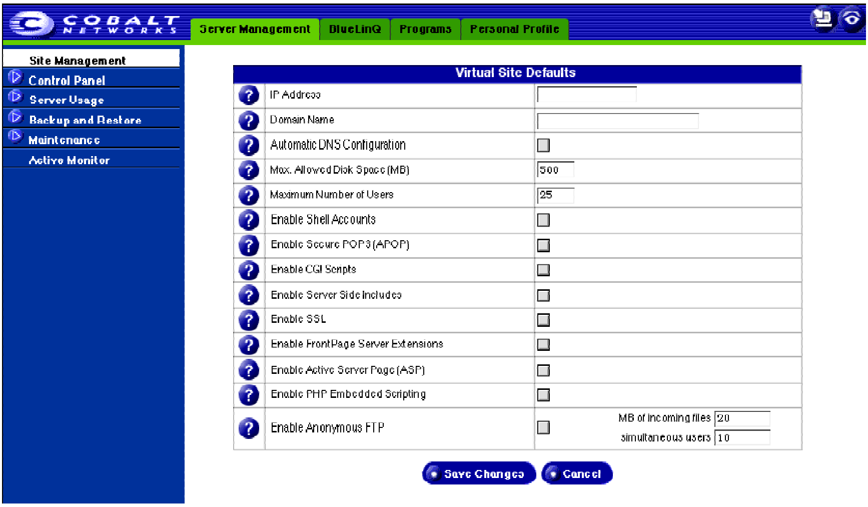
There are many advantages for setting defaults for the virtual sites. For example, since multiple sites can share an IP address, a default IP address can be set for all new virtual sites added. Also, since it is common for many sites to share a common domain name, it can be desirable to set a default domain name for your virtual sites.

The same is true for all of the options for a virtual site; it is best for you to decide the needs of your typical virtual site before assigning these values.

Site defaults and site settings can only be configured by the Server Administrator. If you (as the Server Administrator) enable either the FrontPage Server Extensions service or the Shell Accounts service, the Site Administrators can enable or disable FrontPage user webs, and enable or disable individual (per-user) shell access.

Figure 49 shows the screen for configuring the default settings of a virtual site.

Figure 49. Default settings for a virtual site



Virtual Site Defaults

IP Address	
Domain Name	
Automatic DNS Configuration	☐
Max. Allowed Disk Space (MB)	500
Maximum Number of Users	25
Enable Shell Accounts	☐
Enable Secure POP3 (APOP)	☐
Enable CGI Scripts	☐
Enable Server Side Includes	☐
Enable SSL	☐
Enable FrontPage Server Extensions	☐
Enable Active Server Page (ASP)	☐
Enable PHP Embedded Scripting	☐
Enable Anonymous FTP	☐ MB of incoming files 20 simultaneous users 10

Modifying the default site settings

To modify the default settings for a virtual site:

1. Select **Server Management > Site Management**. The “Virtual Site List” table appears.
2. Click **Site Defaults**. The “Virtual Site Defaults” table appears.
3. Enter the information for the site. Click the check boxes to enable or disable a particular service.

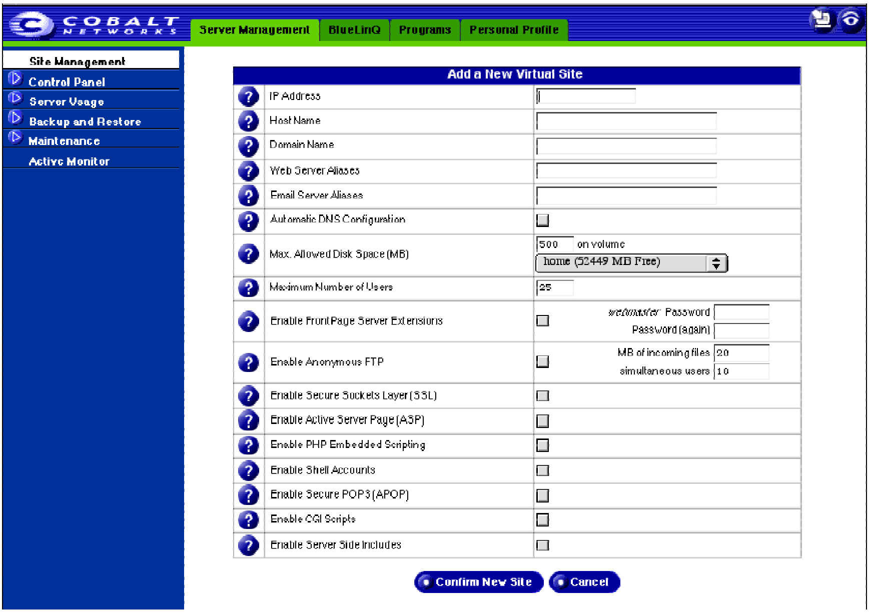
   See the descriptions in “Overview of virtual sites” on page 110.
4. Click **Save Changes**.

Once you have configured the default settings, you can modify the settings for each virtual site that you add.

Adding a virtual site

Figure 50 shows the screen for adding a virtual site.

Figure 50. Adding a virtual site



Add a New Virtual Site	
IP Address	
Host Name	
Domain Name	
Web Server Aliases	
Email Server Aliases	
Automatic DNS Configuration	□
Max. Allowed Disk Space (MB)	500 on volume home (52449 MB Free)
Maximum Number of Users	25
Enable FrontPage Server Extensions	□ *webmaster* Password Password (again)
Enable Anonymous FTP	□ MB of incoming files 20 simultaneous users 10
Enable Secure Sockets Layer (SSL)	□
Enable Active Server Page (ASP)	□
Enable PHP Embedded Scripting	□
Enable Shell Accounts	□
Enable Secure POP3 (APOP)	□
Enable CGI Scripts	□
Enable Server Side Includes	□

To add a virtual site:

1. Select **Server Management > Site Management**. The “Virtual Site List” table appears.
2. Click **Add Site**. The “Add New Virtual Site” table appears.
3. Enter the information for the site; information from the virtual site default settings is displayed here. Click the check boxes to enable or disable a particular service.

   For an explanation of the fields in this table, see “Overview of virtual sites” on page 110.
4. Verify the settings and click **Confirm New Site**.

Adding a name-based virtual site

If you are adding a name-based virtual site, you must have DNS records for that site before you can access the site. For more information, see “Definition of a virtual site” on page 103.

Note: To preview a name-based virtual site, you must first configure its DNS records and make those DNS records available to your workstation and the server appliance.

Requests to the IP address are directed to the first name-based site created on that IP address.

If you administer your DNS records on the server appliance, refer to Appendix E, “Domain Name System” for more information about creating DNS records. If your Internet service provider (ISP) administers your DNS records, ask your ISP to create the DNS records for the new name-based virtual site.

You can also enable the **Automatic DNS configuration** feature when creating a name-based virtual site. If this feature is enabled, the server automatically creates DNS records for this virtual site and the Sun Cobalt RaQ XTR server appliance acts as the primary DNS server for this site.

If the Web and email server aliases have the same domain name as this site, DNS records are created for these aliases as well.

> ***Note:*** This feature does not register the new site name with a top-level domain name registrar. The Server Administrator must register the new site name.
>
> Visit the Internet Corporation for Assigned Names and Numbers (ICANN) at http://www.icann.org. for a list of accredited domain-name registrars.

Once the virtual site has been created, you can manage it by clicking the green *pencil* icon for the site. See “Site settings” on page 68.

To assign a Site Administrator to the new virtual site, see “Adding a site user” on page 52.

Removing a virtual site

To remove a virtual site:

1. Select **Server Management > Site Management**. The “Virtual Site List” table appears.
2. Click the red *trashcan* icon for the virtual site you want to remove. A confirmation dialog verifies the deletion.
3. Click **OK** to delete all the virtual site accounts, site users and contents.
4. The screen refreshes and the virtual site is no longer listed.

Both the Site Administrator and the Server Administrator can configure the site user default settings.   See “Setting defaults for a site user” on page 50.

After creating a virtual site, you can add or remove users for that site, and assign a Site Administrator. See “Adding a site user” on page 52.

For information on removing a site user from a particular virtual site, see “Removing a site user” on page 55.

For information on changing the settings for a particular virtual site, see “Site settings” on page 68.

Server Administrator

Caution: Be sure to remember the password you enter here — otherwise, you will need to reset it (See “Reset password” on page 198).

In the “Administrator Settings” table under **Personal Profile > Account**, you can modify the user settings for the Server Administrator — including user name, password and, optionally, an email address where system alerts for failed services and problems are sent.

If a user *alteradmin* has not been set up, a field to enable the user *alteradmin* and enter a password is displayed in the “Administrator Settings” table.

To modify the your account information as the Server Administrator:

1. Select **Personal Profile > Account**. The “Administrator Settings” table appears.
   - Figure 51 shows the Server Administrator settings with the *alteradmin* account not enabled.
   - Figure 52 shows the Server Administrator settings with the *alteradmin* account enabled.
2. Enter the full name of the Server Administrator.
3. Enter the password twice to ensure that you have entered it as intended. For guidelines on choosing a password, see “Password guidelines” on page 26.

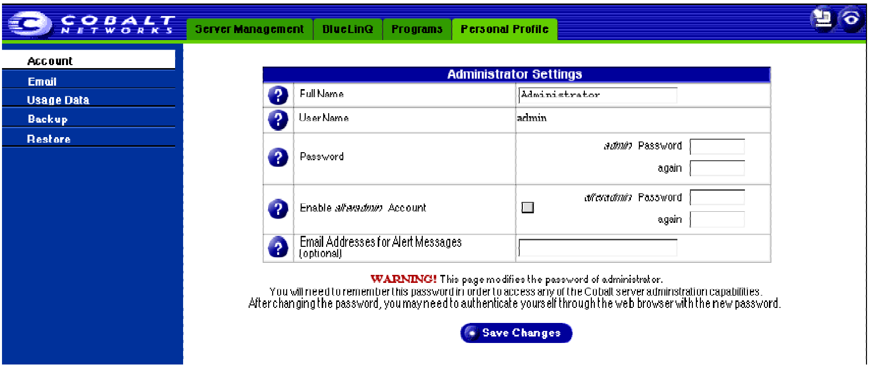
   Note: If you do not want to change the password, do not enter anything in the password fields.

4. If you want to enable the user *alteradmin*, click the check box.

   Enter the password twice to ensure that you have entered it as intended. For guidelines on choosing a password, see “Password guidelines” on page 26.

5. As an option, enter an email address that will receive system alerts for failed services.
6. Click **Save Changes**.

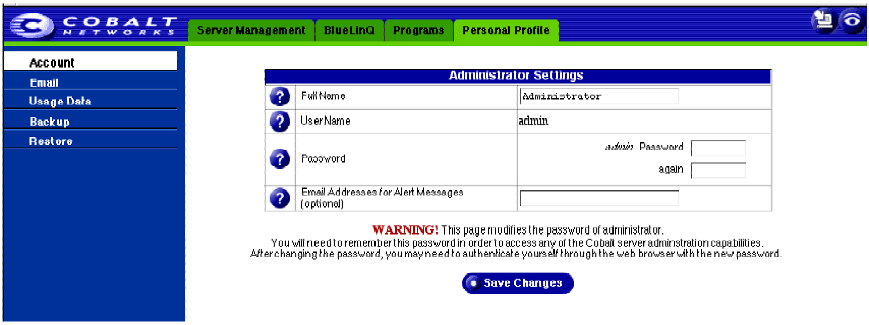
Figure 51. Administrator Settings with alteradmin account not enabled



Administrator Settings	
Full Name	Administrator
User Name	admin
Password	*admin* Password again
Enable *alteradmin* Account	□ *alteradmin* Password again
Email Addresses for Alert Messages (optional)	

WARNING! This page modifies the password of administrator.
You will need to remember this password in order to access any of the Cobalt server administration capabilities.
After changing the password, you may need to authenticate yourself through the web browser with the new password.

Figure 52. Administrator Settings with alteradmin account enabled



Administrator Settings	
Full Name	Administrator
User Name	admin
Password	*admin* Password again
Email Addresses for Alert Messages (optional)	

WARNING! This page modifies the password of administrator.
You will need to remember this password in order to access any of the Cobalt server administration capabilities.
After changing the password, you may need to authenticate yourself through the web browser with the new password.

Changing the Server Administrator password

To change your Server Administrator password:

1. Select **Personal Profile > Account**. The “Administrator Settings” table appears.
2. Enter the password twice to ensure that you have entered it as intended. The Sun Cobalt RaQ XTR server appliance supports long passwords through the UI.

   For guidelines on choosing a password, see “Password guidelines” on page 26.
3. Click **Save Changes.**

Resetting the Server Administrator password

If you forget your Sun Cobalt RaQ XTR server appliance Administrator password, you can reset it through the LCD panel. For more information, see “Reset password” on page 198.

Control panel

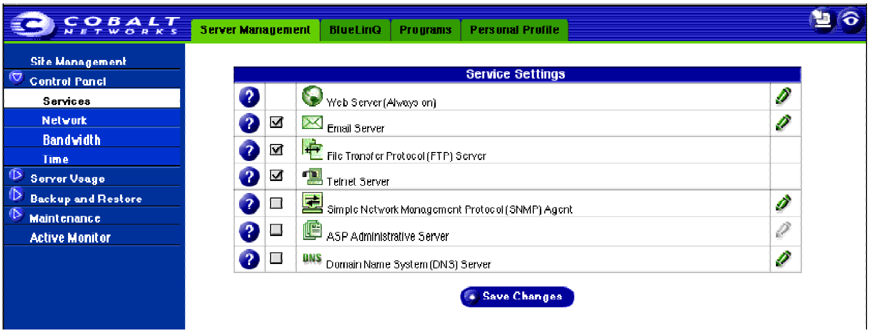
You can configure the services, network and time settings through the Control Panel section of the **Server Management** screen.

Note: For help with a particular field, move the mouse pointer over the Active Assist ? icon adjacent to the field. Help text appears at the bottom of the screen.

Services

Figure 53 shows the “Service Settings” table under **Server Management > Control Panel > Services**.

Figure 53. Service Settings table



Service Settings			
?		Web Server (Always on)	✎
?	☑	Email Server	✎
?	☑	File Transfer Protocol (FTP) Server	
?	☑	Telnet Server	
?	□	Simple Network Management Protocol (SNMP) Agent	✎
?	□	ASP Administrative Server	✎
?	□	Domain Name System (DNS) Server	✎

To manage the settings for the services:

1. Select **Server Management > Control Panel**. The “Service Settings” table appears.
2. To enable any of the services (except Web server, which is always on), click the check box next to that service. The services are described in the sections that follow.
3. Click **Save Changes**.

Web server

This service is always on. It allows site users to access Web content

You can modify the parameters for the Web server.

1. Select **Server Management > Control Panel**. The “Service Settings” table appears.
2. Click the green *pencil* icon next to Web server. The “Web Server Parameters” table appears; see Figure 54. You can configure the following:
   - **Minimum spare servers**—When the Web server starts or is in an idle state, this parameter is the minimum number of Web server processes available for serving Web requests.
   - **Maximum spare servers**—The Web server launches additional processes, as needed, to service additional load. This parameter is the maximum number of processes the system will launch. For high-traffic sites, increase this parameter for better performance.
   - **Maximum clients**—This is the maximum number of requests that can be made to the server at any time. If this number is exceeded, clients receive a message that the server is busy and are asked to try again later. This number is useful for controlling the load on your server.
   - **Hostname lookups**—This turns hostname lookups on for the Web server. This causes the server to do a DNS lookup on the client IP when it connects to the server, and record it in the log files. This information is then available in the server usage Web reports. Without this feature, only client IP addresses are reported in the Web server usage domain report.

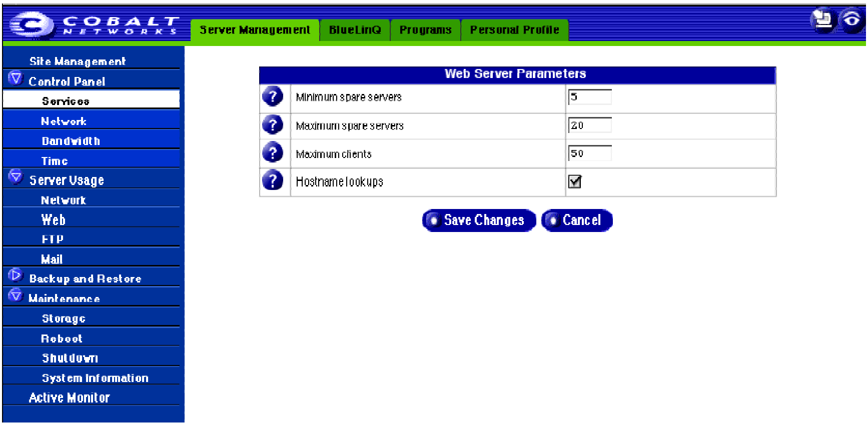
   ⚠ ***Caution:*** Hostname lookups can severely limit the performance of the server but they provide more detailed information in the “Requests by Domain” report under **Server Usage > Web**.

   For more information on server reports, see “Server Usage” on page 142.

3. Click **Save Changes**.

Figure 54 shows the “Web Server Parameters” table.

Figure 54. Web Parameters table



Web Server Parameters	
Minimum spare servers	5
Maximum spare servers	20
Maximum clients	50
Hostname lookups	☑

Email server

The Sun Cobalt RaQ XTR server appliance supports email for each virtual site on the host. It also supports email for entire domains (for example, *www.mydomain.com*). By default, each registered user has an email account created on the server appliance.

The server appliance supports multiple client and server email protocols but does not implement virtual email users. This means that for the entire server appliance, each user must have a unique user name, even if the users are on different virtual sites. For more information, see “Email relaying” on page 131.

SMTP server

The Sun Cobalt RaQ XTR server appliance can act as a Simple Mail Transfer Protocol (SMTP) server for sending and receiving Internet email. The Server Administrator can configure several parameters that can affect the performance of the SMTP server.

Users created on any virtual site can retrieve their email using the Post Office Protocol 3 (POP3) or the Authentication Post Office Protocol (APOP), in addition to the Internet Message Access Protocol 4 (IMAP4). Users can send mail using the Simple Mail Transfer Protocol (SMTP).

For the server appliance to receive email, you or your network administrator must enter a mail server host name in your organization's DNS server to designate the Sun Cobalt RaQ XTR server appliance as the mail server for a domain. Email service depends on DNS, so the IP address of a DNS server must be entered in the network settings for the server appliance; if not, the SMTP protocol will not work. For more information, see "Network" on page 136.

For more information on DNS, see "Domain Name System (DNS) server" on page 136.

POP-before-SMTP feature

The Sun Cobalt RaQ XTR server appliance provides an option that allows POP authentication before SMTP. To enable this feature, see "Configuring the email parameters" on page 129.

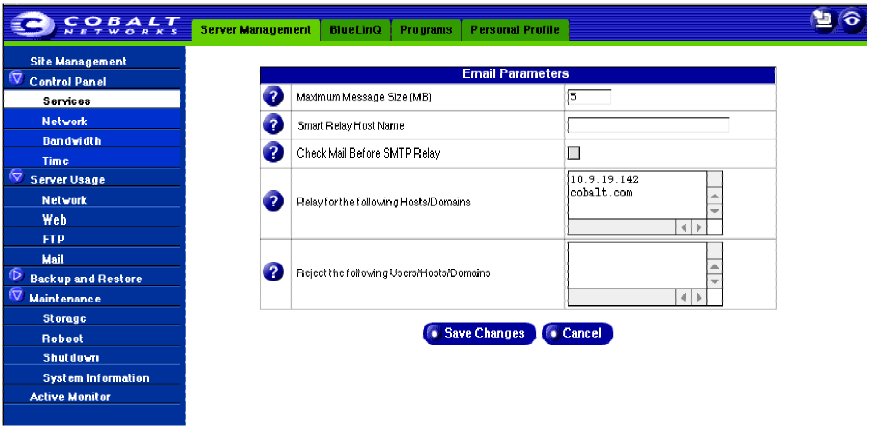
Normally, you only permit email relaying from within your own network. But some users travel and connect from other places (for example, sales people or field engineers) and you want to let those users relay email through your server. The way to allow this and still protect your server appliance from being used to relay spam mail is to authenticate the user through POP before allowing an SMTP connection for that user's IP address.

When a user logs in for POP3 email, the server appliance notes the IP address from which the connection was made and permits relays from that IP address for a limited time. Travelling users need only check their email to "unlock" the mail server; no changes to the client mail software are necessary.

The POP-before-SMTP implementation causes SMTP access for the IP address to expire after one hour.

Figure 55 shows the "Email Parameters" table.

Figure 55. Email Parameters table



Email Parameters	
Maximum Message Size (MB)	5
Smart Relay Host Name	
Check Mail Before SMTP Relay	□
Relay for the following Hosts/Domains	10.9.19.142 cobalt.com
Reject the following Users/Hosts/Domains	

Configuring the email parameters

To configure the email parameters:

1. Select **Server Management > Control Panel**. The “Service Settings” table appears.
2. Click the green *pencil* icon next to Email Server. The “Email Parameters” table appears; see Figure 55.
3. Fill in the fields in the “Email Parameters” table. The following paragraphs explain these fields.
4. Click **Save Changes** in the “Email Parameters” table.

You can modify the following parameters:

- **Maximum message size (MB)**—It is important to enter a value here to limit the size of incoming or outgoing email messages. If this field is blank, the server will not limit the size of incoming messages, which may allow a single message to fill up your available space on the hard disk drive. A message that exceeds the specified quota of space on the hard disk drive is returned to the sender as “undeliverable”. The default value is 5 MB; the value must be a whole number greater than zero.
- **Smart Relay Host Name**—You can enter an optional host name in this field. With this feature, you can configure the server appliance to send Internet email to a specific email server. Enter the host name of the email server through which you want to relay your email.

  This feature is useful if the server appliance does not have direct Internet access (for example, the server appliance is subject to a restrictive firewall), but can communicate with an email server that has direct Internet access.
- **Check mail before SMTP relay**—The server appliance provides an option that allows SMTP relay access for users based on previous POP authentication. Click the check box to enable this feature.
- **Relay for the following hosts/domains**—You can specify a list of hosts for which the SMTP server will relay email messages. You can enter IP addresses or domain names in this field.

  For more information, see “Email relaying” on page 131.
- **Reject the following users/hosts/domains**—In this field, enter email addresses or domains from which you want to block any email. Anyone trying to send you messages from one of these addresses or domains will receive an error message in return.

Email relaying

Simple Mail Transfer Protocol (SMTP) service is different from Post Office Protocol (POP), telnet and file transfer protocol (FTP) services in that SMTP does not try to authenticate a user when an SMTP connection is made.

Every email server on the Internet has to be able to deliver email to you, so the email servers must be able to connect freely to send and receive email. The Sun Cobalt RaQ XTR server appliance accepts email for processing if the recipient has a user account or an alias email account, or if the sending host (your client PC) is trusted to relay outgoing email messages to another domain. These trusts are defined by host or domain names, as well as by IP addresses and networks.

⚠ ***Caution:*** Some users advise you to open relay to all com, edu, net and other top-level domain addresses. However, doing so allows hosts belonging to com, edu, net and others to relay email through your server; this relayed mail is known as *spam mail*.

Spam mail can appear as though it originated from your server and as a result, others may blacklist your server as a known spam site. If your server is blacklisted, many mail servers will not relay your email and your customers will not receive a large amount of their email messages.

If you have users who access your server through the Internet, ask your Internet service provider (ISP) which networks are used by their remote access (dial-up) equipment.

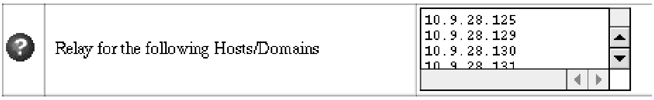
For example, if the ISP says the network 192.168.10.5 through 192.168.10.24, then enter “192.168.10” in the “Relay email from these hosts/domains” field of the “Email Parameters” table. If your ISP gives you a list of 30 networks used by 30 points-of-presence (POPs) (which are regional ISP offices) across the country and your clients can dial in from any of them, then you must trust all 30 networks or these users cannot send email through your Sun Cobalt RaQ XTR server appliance.

Enabling email relaying

To enable email relaying, add the IP addresses (or domain names, or both) of the machines which use your server appliance as the SMTP server.

1. Select **Server Management > Control Panel**. The “Service Settings” table appears.
2. Click the green *pencil* icon next to Email Server. The “Email Parameters” table appears; see Figure 55.

   One field is labeled “Relay for the following hosts/domains”. The following paragraphs explain how to fill in this field.



Relay for the following Hosts/Domains

```
10.9.28.125
10.9.28.129
10.9.28.130
10.9.28.131
```

3. Click **Save Changes** in the “Email Parameters” table.

The entries you add to this field serve as part of a pattern match against the email that the client is sending. As a result, some handy shortcuts are possible. If you have a number of hosts in the same network block, you can, as a shortcut, simply enter the number of the network block.

For example, specifying a network such as 192.168.1 in the “Relay email from these hosts/domains” field trusts all IP addresses from 192.168.1.1 through 192.168.1.254.

✍ ***Note:*** There is no trailing period on the number of the network block and there are only three octets entered in the field. It is important that you do not include a trailing dot after the part of the IP address that you want to match.

If you want to allow connections from a host that ends, for example, in *mydomain.com*, add the string “mydomain.com” in the text area.

✍ ***Note:*** If you enter a domain name or part of a domain name in the text box, you must have reverse DNS working on your clients.

File transfer protocol (FTP) server

Using the file transfer protocol, site users can upload and download files on the Sun Cobalt RaQ XTR server appliance server. Users can transfer files with FTP client software such as Fetch or WS-FTP.

You can enable or disable the FTP server.

1. Select **Server Management > Control Panel**. The “Service Settings” table appears.
2. Click to enable or disable the check box next to File Transfer Protocol (FTP) Server.
3. Click **Save Changes**.

Telnet server

Telnet access is available but only advanced users should use telnet. An advanced user is someone who is proficient in the internal workings of the Unix operating system.

It is possible to adversely affect the operation of your Sun Cobalt RaQ XTR server appliance if you modify system configuration files.

Caution: Granting shell access can greatly compromise the security of your server appliance.

Note: Disabling the telnet server in the “Service Settings” table denies telnet access to all users, even if they have been granted shell access.

You can enable or disable the telnet server:

1. Select **Server Management > Control Panel**. The “Service Settings” table appears.
2. Click to enable or disable the check box next to Telnet Server.
3. Click **Save Changes**.

Simple Network Management Protocol (SNMP) agent

If the SNMP agent is enabled, you can use SNMP software to remotely monitor server information such as CPU utilization and network traffic.

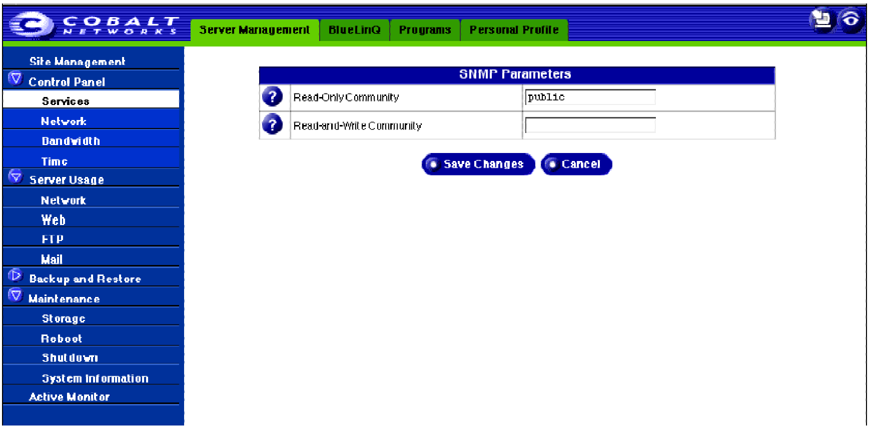
You can enable or disable the Simple Network Management Protocol (SNMP) agent:

1. Select **Server Management > Control Panel**. The “Service Settings” table appears.
2. Click to enable or disable the check box next to Simple Network Management Protocol (SNMP) agent.
3. If you are disabling the SNMP agent, click **Save Changes**.

   If you are enabling the SNMP agent, click on the green *pencil* icon for this service in the “Service Settings” table. The “SNMP Parameters” table appears; see Figure 56.
4. Enter the SNMP communities that can have read-only and read-and-write access to this SNMP agent. The default read-access community is *public*.
5. Click **Save Changes** in the “SNMP Parameters” table.
6. Click **Save Changes** in the “Service Settings” table.

Figure 56 shows the “SNMP Parameters” table.

Figure 56. SNMP Parameters table



SNMP Parameters	
Read-Only Community	public
Read-and-Write Community	

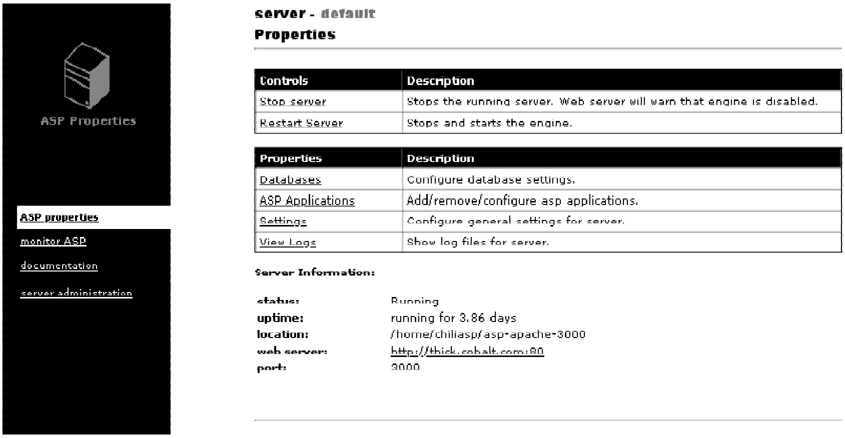
ASP Administrative Server

To access the ASP Administrative Server UI:

1. Select **Server Management > Control Panel**. The “Service Settings” table appears. If the ASP Administrative Server service is disabled, the *pencil* icon is grayed-out.
2. Click to enable the check box next to ASP Administrative Server.
3. Click **Save Changes**. The screen refreshes and the *pencil* icon is now enabled (a green *pencil*).
4. Click the green *pencil* icon for ASP Administrative Server. A confirmation dialog appears, asking for the user name and password for the ASP Management server at <hostname.domainname:5100>.
5. Enter the user name and password of the Server Administrator.
6. Click **OK**. A separate browser window opens with the UI for the ASP Server Administration screen. The link for “documentation” on the left guides you through the functionality of the Sun Chili!Soft ASP software.

Figure 57 shows the UI for the ASP Administrative Server.

Figure 57. ASP Administrative Server UI



server - default

Properties

Controls	Description
Stop server	Stops the running server. Web server will warn that engine is disabled.
Restart Server	Stops and starts the engine.

Properties	Description
Databases	Configure database settings.
ASP Applications	Add/remove/configure asp applications.
Settings	Configure general settings for server.
View Logs	Show log files for server.

Server Information:

status:	Running
uptime:	running for 3.86 days
location:	/home/chiliasp/asp-apache-3000
web server:	http://thick.cobalt.com:80
port:	3000

Domain Name System (DNS) server

Domain Name System (DNS) is a vital and integral part of the Internet. Setting up DNS correctly on your Sun Cobalt RaQ XTR server appliance server is very important. For this reason, we have created an appendix solely for explaining DNS. See Appendix E, “Domain Name System”.

The appendix covers the following items:

- basic DNS issues
- advanced DNS issues
- a quick start guide detailing a sample setup of DNS for a Sun Cobalt RaQ XTR server appliance
- a brief history of the DNS service

Network

The network settings make the Sun Cobalt RaQ XTR server appliance visible to other computers. If you change the IP address on the LCD console or in the Server Desktop UI, the server appliance reboots.

> ***Important:*** Coordinate the network configuration information with your network administrator to ensure the integrity of your network. Incorrect network settings can result in a loss of connectivity.

To enter or change the network configuration for the server appliance:

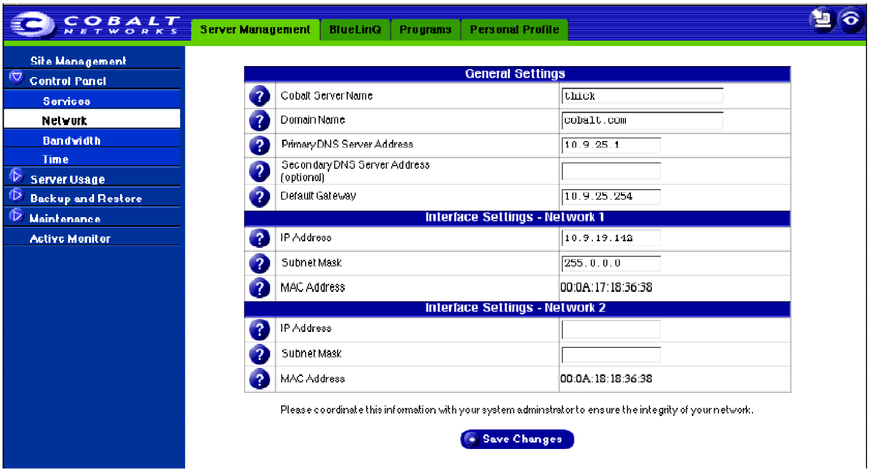
1. Select **Server Management > Control Panel > Network**. The settings tables for the network configuration appear; see Figure 58.
2. Enter configuration information for the General Settings, the Interface Settings for Network 1 or the Interface Settings for Network 2.

> ***Note:*** For help with a particular field, move the mouse pointer over the Active Assist ? icon adjacent to the field. Help text appears in a window at the bottom of the screen.

3. Click **Save Changes**.

Figure 58 shows the settings tables of the Network section.

Figure 58. Settings tables in the Network section



General Settings	
Cobalt Server Name	thick
Domain Name	cobalt.com
Primary DNS Server Address	10.9.25.1
Secondary DNS Server Address (optional)	
Default Gateway	10.9.25.254

Interface Settings - Network 1	
IP Address	10.9.19.142
Subnet Mask	255.0.0.0
MAC Address	00:0A:17:18:36:38

Interface Settings - Network 2	
IP Address	
Subnet Mask	
MAC Address	00:0A:18:18:36:38

Please coordinate this information with your system adminstrator to ensure the integrity of your network.

Bandwidth

The Sun Cobalt RaQ XTR server appliance allows you to set an output bandwidth limit for each IP address that you assign on a server appliance. The bandwidth limit applies to all of the name-based virtual sites associated with an IP address.

Note: The Bandwidth feature does not regulate input traffic.

The limit is specified in kilobits per second (kb/s), and the server appliance enforces a minimum bandwidth limit of 10 kb/s.

The bandwidth limit applies to all outgoing Transmission Control Protocol (TCP) traffic on a particular IP address. This includes Web, FTP, POP and telnet traffic, as well any other TCP-based application.

If multiple users are accessing a bandwidth-limited IP address, the system divides the bandwidth evenly among the users.

If multiple named-based virtual sites belong to one IP address, the bandwidth assigned to the IP address is divided evenly among the total number of users on those name-based virtual sites.

You can apply a bandwidth limit to an IP address that did not previously have one, modify an existing bandwidth limit or delete a bandwidth limit.

Bandwidth Limits table

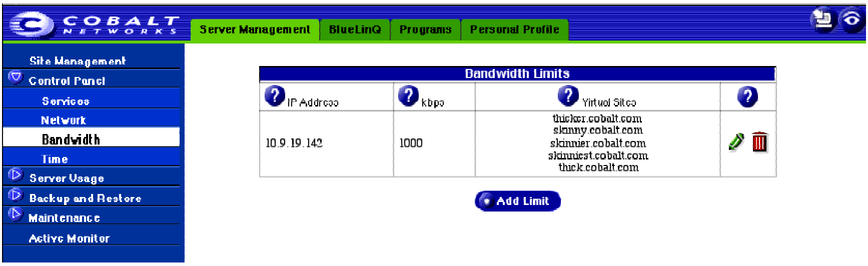
When you select the bandwidth-limit option, the “Bandwidth Limits” table appears; see Figure 59.

If you have not applied a bandwidth limit to any IP addresses, the table is blank. If you have applied a bandwidth limit to an IP address, the table displays four columns:

- the IP address to which the limit is applied
- the bandwidth limit (in kb/s)
- the fully qualified domain name(s) of the site(s) associated with the IP address
- the icons to modify the bandwidth limit (green pencil) or delete the bandwidth limit (red trashcan)

Figure 59 shows the “Bandwidth Limits” table.

Figure 59. Bandwidth Limits table



Bandwidth Limits

? IP Address	? kbps	? Virtual Sites	?
10.9.19.142	1000	thicker.cobalt.com skinny.cobalt.com skinnier.cobalt.com skinniest.cobalt.com thick.cobalt.com	✎ 🗑

Applying a bandwidth limit

To apply a bandwidth limit to an IP address:

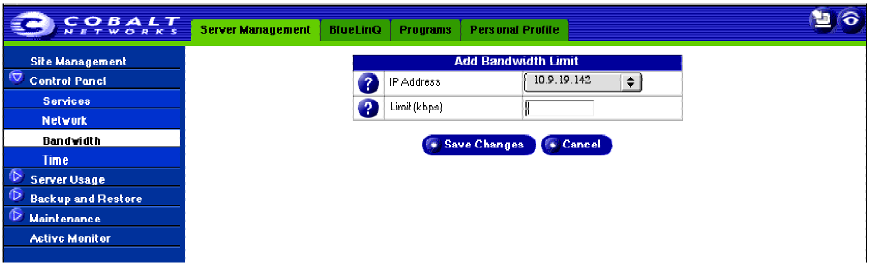
1. Select **Server Management > Control Panel > Bandwidth**. The “Bandwidth Limits” table appears.
2. Click **Add Limit**. The “Add Bandwidth Limit” table appears. See Figure 60.

> ***Note:*** If each of the IP addresses on the Sun Cobalt RaQ XTR server appliance already has a bandwidth limit assigned to it, an error message at the bottom of the screen alerts you to this fact.
>
> To modify a bandwidth limit, see “Modifying a bandwidth limit” on page 140. To delete a bandwidth limit, see “Deleting a bandwidth limit” on page 140.

3. In the first row of the table, use the pull-down menu to select the IP address to which you want to apply the bandwidth limit. The pull-down menu lists all the IP addresses that do not currently have a bandwidth limit.
4. In the second row, enter the value of the bandwidth limit in kb/s. The minimum value is 10 kb/s.
5. Click **Save Changes**. The screen refreshes and the “Bandwidth Limits” table is displayed with the IP address and the bandwidth limit.

Figure 60 shows the “Add Bandwidth Limit” table.

Figure 60. Add Bandwidth Limit table



Add Bandwidth Limit	
IP Address	10.9.19.142
Limit (kbps)	

Modifying a bandwidth limit

To modify a bandwidth limit applied to an IP address:

1. Select **Server Management > Control Panel > Bandwidth**. The “Bandwidth Limits” table appears.
2. In the table, locate the IP address for which you want to modify the bandwidth limit.
3. Click the green *pencil* icon next to that IP address. The “Modify Bandwidth Limit” table appears. The first row of the table displays the IP address.
4. In the second row, enter the new value of the bandwidth limit in kb/s. The minimum value is 10 kb/s.
5. Click **Save Changes**. The screen refreshes and the “Bandwidth Limits” table is displayed with the new bandwidth limit for that IP address.

Deleting a bandwidth limit

To delete a bandwidth limit to an IP address:

1. Select **Server Management > Control Panel > Bandwidth**. The “Bandwidth Limits” table appears.
2. In the table, locate the IP address for which you want to delete the bandwidth limit.
3. Click the red *trashcan* icon next to that IP address. A confirmation dialog verifies the deletion.
4. Click **OK**. The screen refreshes and the “Bandwidth Limits” table is displayed; the bandwidth limit for that IP address is removed.

Time

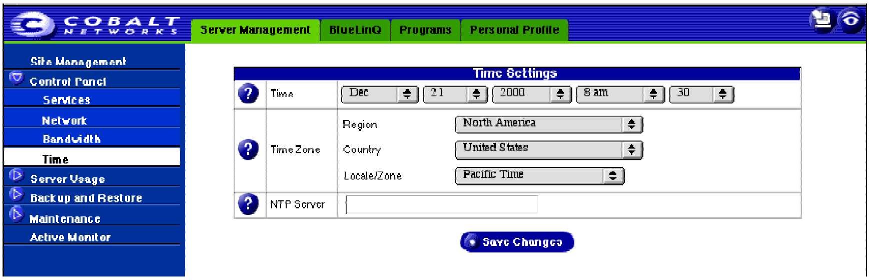
You can configure the correct time, date and time zone for the Sun Cobalt RaQ XTR server appliance.

1. Select **Server Management > Control Panel > Time**. The "Time Settings" table appears. See Figure 61.
2. Select the time and date with the pull-down menus.
3. Select the correct time zone by clicking in the Region, Country and Locale/ Zone fields.
4. As an option, you can also specify the name of a Network Time Protocol (NTP) server with which the server appliance will synchronize its internal clock every night. Enter the host name or IP address of the NTP server.

   You can find a list of publicly available NTP servers at: http://www.eecis.udel.edu/~mills/ntp/servers.html.
5. Click **Save Changes**.

Figure 61 shows the "Time Settings" table.

Figure 61. Time Settings table



Time Settings		
Time	Dec 21 2000 8 am 30	
Time Zone	Region	North America
	Country	United States
	Locale/Zone	Pacific Time
NTP Server		

Server Usage

The Server Usage section allows you to view overall usage statistics for the Sun Cobalt RaQ XTR server appliance.

Note: For the Usage Statistics feature under the **Site Management** tab, see “Usage statistics” on page 83.

You can generate server-usage reports for a selected range of dates. The reports allow you to monitor the amount of bandwidth consumed by network, Web, FTP and email traffic generated by the virtual sites.

The reports contain both current data and data that has been compiled from past processed log files. Log files are processed daily at 04:00 a.m.; this process summarizes the data without retaining the actual log file.

Network

To view the statistics for network traffic on the server:

1. Select **Server Management > Server Usage**. If a report has been generated, the “Network Usage Summary Statistics” table appears. See Figure 62.

   If a report has not yet been generated, the “Network Usage Summary Statistics” table does not appear. To generate a report, see Step 3 below.

2. The “Network Usage Summary Statistics” table displays a number of rows of information concerning network usage, including the dates for which the report was generated.

   A second table entitled “Other Network Usage Statistics” offers hypertext links for more detailed information. Click on a link to see a detailed bar chart for a particular criterion.

   - **Use by IP**—This graphically represents the network traffic broken down by IP addresses on the server, both past and present. See Figure 63 for a sample.

     There is always an entry for the IP address 127.0.0.1; this represents internal server appliance traffic. There is also an entry for “other” which represents traffic not destined for this server. These statistics can help you determine the IP addresses with the largest amount of traffic.

   - **Periodic Reports—**This graphically represents the cumulative network traffic broken down by hour of the day or day of the week. These statistics can help you determine the busy periods for your server.

- **Historical Use**—This graphically represents the total network traffic broken down by specific day, week or month during the report period. These statistics can help you determine the busiest specific day, week or month for network traffic on your server appliance.
- **Download log file**—This allows you to download the current network traffic log file. You can then analyze the log file with external analysis software.

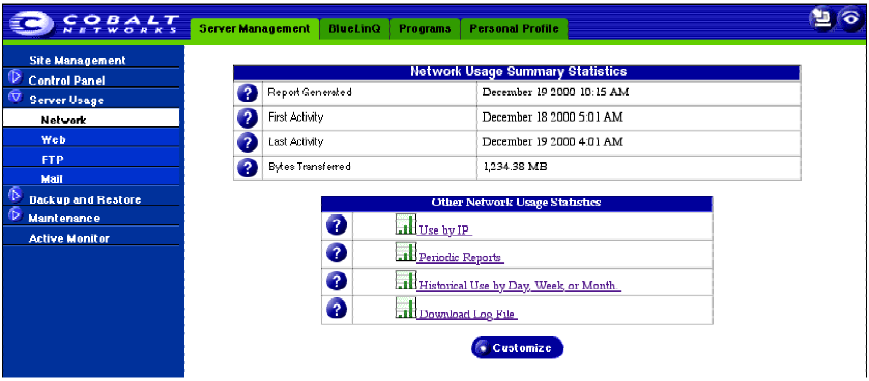
3. To generate a report, click **Customize**. The “Configure Reporting Options” table appears; see Figure 64. You can generate a new report for a selected range of dates.
4. From the pull-down menus, choose a start date and end date.
5. Click **Generate Report**. The “Network Usage Summary Statistics” table appears with the new data.

Figure 62 shows the “Network Usage Summary Statistics” table.

Figure 63 shows a sample of a Network Usage – Use by IP report.

Figure 64 shows the “Configure Reporting Options” table.

Figure 62. Network Usage Summary Statistics table



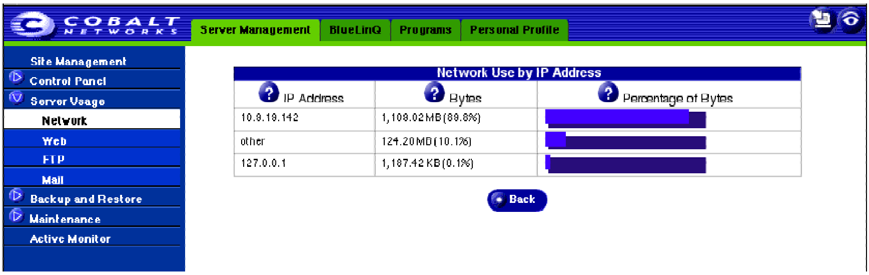
Network Usage Summary Statistics	
Report Generated	December 19 2000 10:15 AM
First Activity	December 18 2000 5:01 AM
Last Activity	December 19 2000 4:01 AM
Bytes Transferred	1,234.38 MB

Other Network Usage Statistics

- Use by IP
- Periodic Reports
- Historical Use by Day, Week, or Month
- Download Log File

Customize

Figure 63. Sample of a Network Usage – Use by IP report

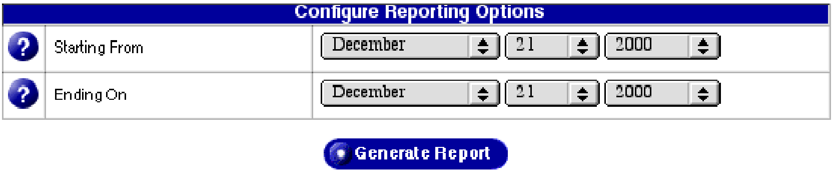


Network Use by IP Address

IP Address	Bytes	Percentage of Bytes
10.9.19.142	1,109.02 MB (89.8%)	
other	124.20 MB (10.1%)	
127.0.0.1	1,187.42 KB (0.1%)	

Back

Figure 64. Configure Reporting Options table



Configure Reporting Options				
?	Starting From	December	21	2000
?	Ending On	December	21	2000

Generate Report

Web

To view the statistics for Web traffic on the server:

1. Select **Server Management > Server Usage > Web**. If a report has been generated, the “Web Usage Summary Statistics” table appears. See Figure 65.

   If a report has not yet been generated, the “Web Usage Summary Statistics” table does not appear. To generate a report, see Step 3 below.

2. The “Web Usage Summary Statistics” table displays a number of rows of information concerning Web usage, including the dates for which the report was generated.

   A second table entitled “Other Web Usage Statistics” offers hypertext links for more detailed information. Click on a link to see a detailed bar chart for a particular criterion.

   - **Use by Virtual Site**—This graphically represents the amount of Web traffic broken down by virtual site on the server, for both past and present virtual sites. These statistics can help you determine the virtual site with the largest amount of Web traffic.
   - **Periodic Reports**—This graphically represents the cumulative Web traffic broken down by hour of the day or day of the week. These statistics can help you determine the busy periods for your server. See Figure 66 for a sample.
   - **Historical Use**—This graphically represents the total Web traffic broken down by specific day, week or month during the report period. These statistics can help you determine the busiest specific day, week or month for Web traffic on your server appliance.
   - **Requests by Domain**—This graphically represents the domains from which Web traffic originated, broken down by domain and, if available, by sub-domain. Sub-domains are indented under their parent domains; the values for the sub-domains are subsumed within, and add up to, the value for the parent domain.

Note: For this report to contain resolved domain names (for example, .com, .edu or .org), the “Hostname lookups” option must be enabled at the time of the Web traffic. If this option is not enabled, all traffic appears to originate from unresolved IP addresses.

To enable this option, see “Web server” on page 126.

- **Requests by Type of File**—This graphically represents the Web traffic broken down by type of file requested.
- **Download log file**—This allows you to download the current Web traffic log file. You can then analyze the log file with external analysis software.

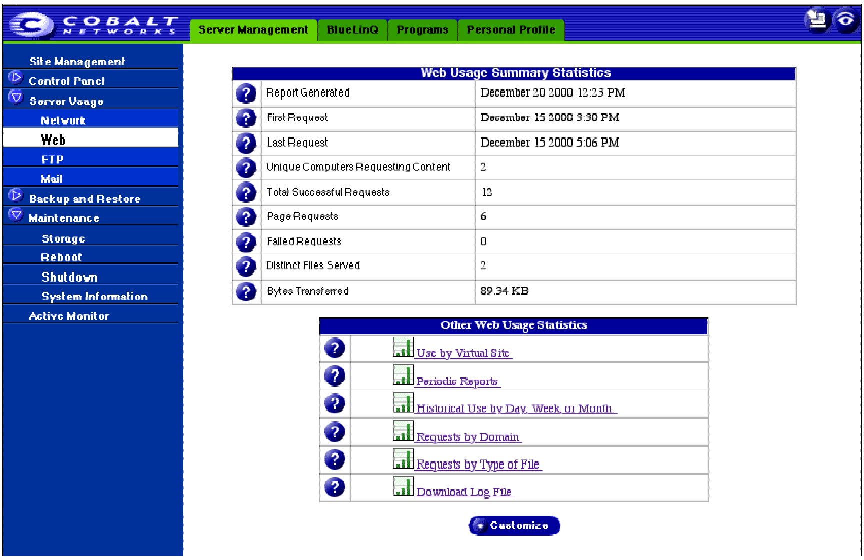
3. To generate a report, click **Customize**. The “Configure Reporting Options” table appears; see Figure 67. You can generate a new report for a selected range of dates.
4. From the pull-down menus, choose a start date and end date.
5. Click **Generate Report**. The “Web Usage Summary Statistics” table appears with the new data.

Figure 65 shows the “Web Usage Summary Statistics” table.

Figure 66 shows a sample of a Web Usage – Periodic Report.

Figure 67 shows the “Configure Reporting Options” table.

Figure 65. Web Usage Summary Statistics table

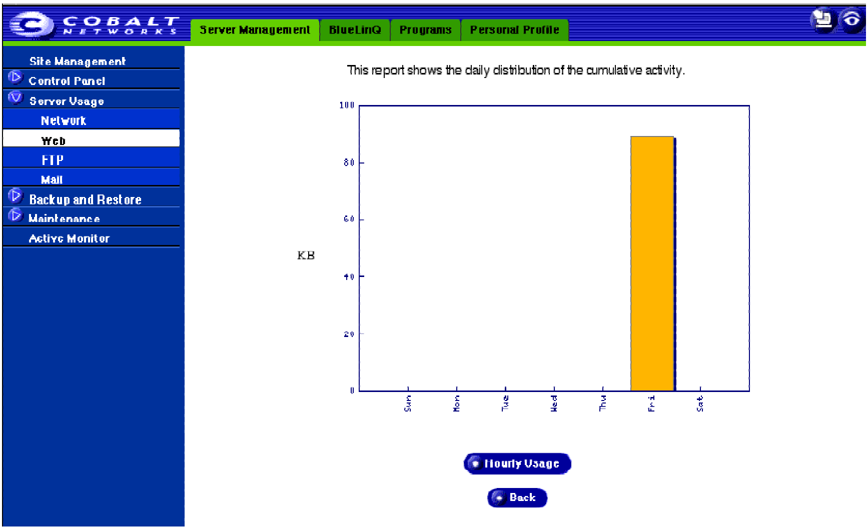


Web Usage Summary Statistics	
Report Generated	December 20 2000 12:23 PM
First Request	December 15 2000 3:30 PM
Last Request	December 15 2000 5:06 PM
Unique Computers Requesting Content	2
Total Successful Requests	12
Page Requests	6
Failed Requests	0
Distinct Files Served	2
Bytes Transferred	89.34 KB

Other Web Usage Statistics

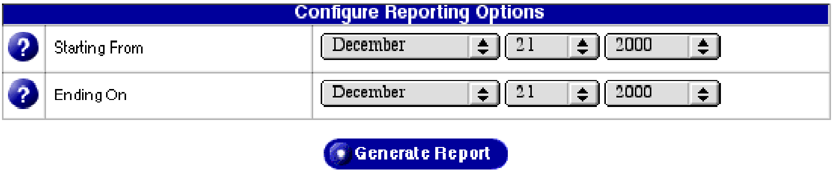
- Use by Virtual Site
- Periodic Reports
- Historical Use by Day, Week or Month
- Requests by Domain
- Requests by Type of File
- Download Log File

Figure 66. Sample of a Web Usage – Periodic Report



This report shows the daily distribution of the cumulative activity.

Figure 67. Configure Reporting Options table



Configure Reporting Options

?	Starting From	December	21	2000
?	Ending On	December	21	2000

FTP

To view the statistics for FTP traffic on the server:

1. Select **Server Management > Server Usage > FTP**. If a report has been generated, the “FTP Usage Summary Statistics” table appears.

   If a report has not yet been generated, the “FTP Usage Summary Statistics” table does not appear. To generate a report, see Step 3 below.

2. The “FTP Usage Summary Statistics” table displays a number of rows of information concerning FTP usage, including the dates for which the report was generated.

   A second table entitled “Other FTP Usage Statistics” offers hypertext links for more detailed information. Click on a link to see a detailed bar chart for a particular criterion.

   - **Use by Virtual Site**—This graphically represents the amount of FTP traffic broken down by virtual site on the server, for both past and present virtual sites. These statistics can help you determine the virtual sites with the largest amount of FTP traffic.
   - **Periodic Reports**—This graphically represents the cumulative FTP traffic broken down by hour of the day or day of the week. These statistics can help you determine the busy periods for your server.
   - **Historical Use**—This graphically represents the total FTP traffic broken down by specific day, week or month during the report period. These statistics can help you determine the busiest specific day, week or month for FTP traffic on your server appliance.
   - **Requests by Domain**—This graphically represents the domains from which FTP traffic originated, broken down by domain and, if available, by sub-domain. Sub-domains are indented under their parent domains; the values for the sub-domains are subsumed within, and add up to, the value for the parent domain.
   - **Requests by Type of File**—This graphically represents the FTP traffic broken down by type of file requested.
   - **Download log file**—This allows you to download the current FTP traffic log file. You can then analyze the log file with external analysis software.

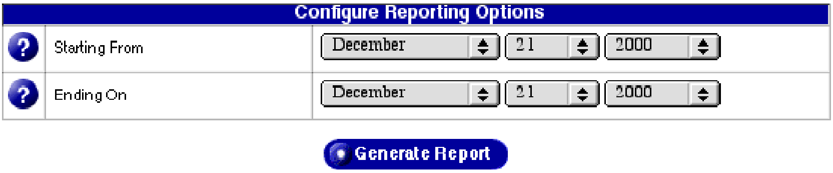
3. To generate a report, click **Customize**. The “Configure Reporting Options” table appears; see Figure 68. You can generate a new report for a selected range of dates.

4. From the pull-down menus, choose a start date and end date.

5. Click **Generate Report**. The “FTP Usage Summary Statistics” table appears with the new data.

Figure 68 shows the “Configure Reporting Options” table.

Figure 68. Configure Reporting Options table



Configure Reporting Options			
Starting From	December	21	2000
Ending On	December	21	2000

Mail

To view the statistics for email traffic on the server:

1. Select **Server Management > Server Usage > Mail**. If a report has been generated, the “Mail Usage Summary Statistics” table appears. See Figure 69.

   If a report has not yet been generated, the “Mail Usage Summary Statistics” table does not appear. To generate a report, see Step 3 below.

2. The “Mail Usage Summary Statistics” table displays a number of rows of information concerning email usage, including the dates for which the report was generated.

   A second table entitled “Other Mail Usage Statistics” offers hypertext links for more detailed information. Click on a link to see a detailed bar chart for a particular criterion.

   - **Use by Virtual Site**—This graphically represents the amount of email traffic broken down by virtual site on the server. You can view statistics based on which domains sent email and which domain received email.

     Mail traffic that has been relayed through the server appliance or destined for domains other than those served by this server is summarized in this report. These statistics show you the volume of email sent and received by a given domain.

   - **Periodic Reports**—This graphically represents the cumulative email traffic broken down by hour of the day or day of the week. These statistics can help you determine the busy periods for your server.

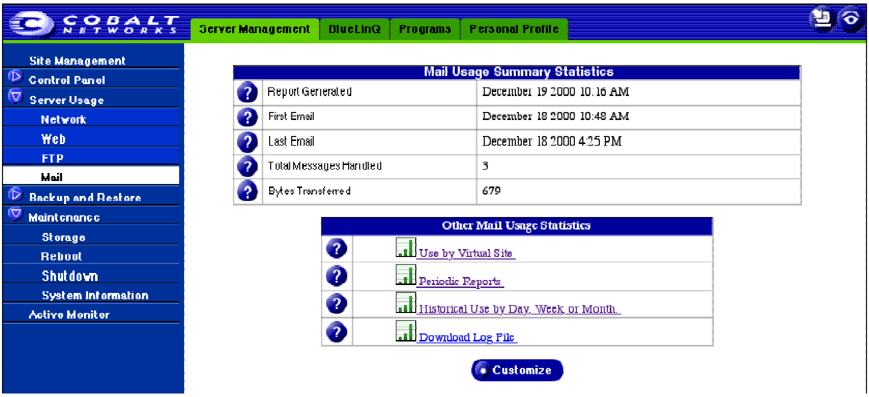
- **Historical Use**—This graphically represents the total email traffic broken down by specific day, week or month during the report period. This statistic can help you determine the busiest specific day, week or month for email traffic on your server appliance.
- **Download log file**—This allows you to download the current email traffic log file. You can then analyze the log file with external analysis software.

3. To generate a report, click **Customize**. The “Configure Reporting Options” table appears; see Figure 70. You can generate a new report for a selected range of dates.
4. From the pull-down menus, choose a start date and end date.
5. Click **Generate Report**. The “Mail Usage Summary Statistics” table appears with the new data.

Figure 69 shows the “Mail Usage Summary Statistics” table.

Figure 70 shows the “Configure Reporting Options” table.

Figure 69. Mail Usage Summary Statistics table

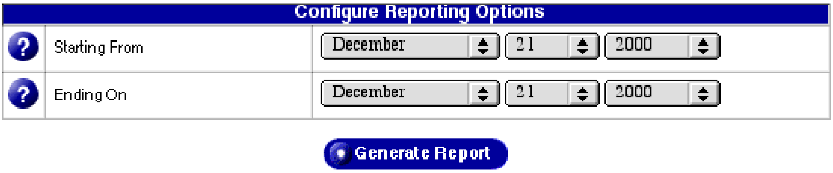


Mail Usage Summary Statistics	
Report Generated	December 19 2000 10:16 AM
First Email	December 18 2000 10:48 AM
Last Email	December 18 2000 4:25 PM
Total Messages Handled	3
Bytes Transferred	679

Other Mail Usage Statistics

- Use by Virtual Site
- Periodic Reports
- Historical Use by Day, Week or Month
- Download Log File

Figure 70. Configure Reporting Options table



Configure Reporting Options			
Starting From	December	21	2000
Ending On	December	21	2000

Backup and Restore

The Sun Cobalt RaQ XTR server appliance supports third-party backup and restore solutions from three companies:

- Knox Arkeia
- Legato NetWorker®
- Veritas NetBackup

Under the **Server Management > Backup and Restore** tab, the Server Administrator can configure the server appliance to use one of these solutions.

Note: This section explains how to enable the backup clients for these solutions on the server appliance.

To configure the backup server software, see Appendix F, “Disaster Recovery with Third-Party Software”.

Control

The Control feature allows the Server Administrator to “lock” the Server Desktop UI in read-only mode or to shut down all services currently running on the server, except for any configured backup programs.

- Locking the Server Desktop UI during the backup and restore process helps to guarantee that consistent configuration information for the server is saved and restored.
- Stopping all services currently running on the server enables the backup program to restore data to the system.

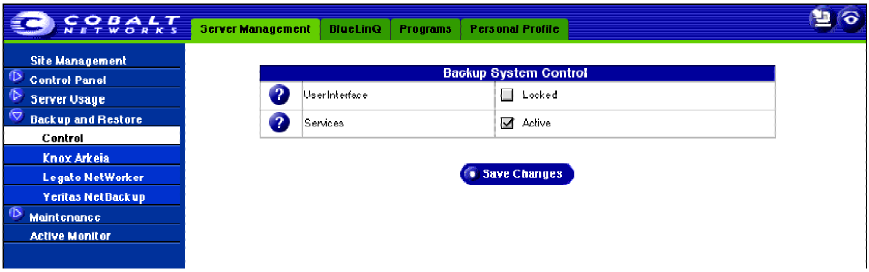
Note: Sun Microsystems recommends that the Server Administrator reboot the server after a restore operation.

To configure the control options:

1. Select **Server Management > Backup and Restore > Control**. The “Backup System Control” table appears. See Figure 71.
2. To lock the Server Desktop UI, click to enable the check box Locked.
3. To stop all services currently running on the server (except for any configured backup programs), click to disable the check box Active.
4. Click **Save Changes**. The table refreshes and displays the new configuration.

Figure 71 shows the “Backup System Control” table.

Figure 71. Backup System Control table



Backup System Control	
UserInterface	□ Locked
Services	☑ Active

Knox Arkeia

To configure the Knox Arkeia backup and restore solution:

1. Select **Server Management > Backup and Restore > Knox Arkeia**. The "Knox Arkeia Backup Settings" table appears. See Figure 72.
2. Enter the following information:
   - **Enable Client**—Click to enable the check box to enable the Knox Arkeia backup client.
   - **Backup Server Name**—Enter the fully qualified domain name of the Knox Arkeia backup server.
   - **Port Number**—The Knox Arkeia Backup client needs to know the port number through which to communicate with other hosts using Knox services including the Knox Arkeia Backup server.

     The default port is 617.

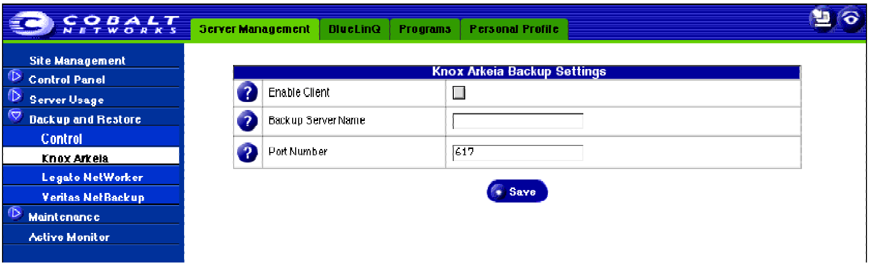
> ☞ ***Important:*** Changing this port number is not recommended unless absolutely necessary. If you change the port number, ensure that other hosts on the network using Knox services are also configured to use the port you specify here.

3. Click **Save**. The table refreshes and displays the new configuration.

For further information on the Knox Arkeia backup and restore solution, see Appendix F, "Disaster Recovery with Third-Party Software".

Figure 72 shows the "Knox Arkeia Backup Settings" table.

Figure 72. Knox Arkeia Backup Settings table



Knox Arkeia Backup Settings	
Enable Client	□
Backup Server Name	
Port Number	617

Legato NetWorker

To configure the Legato NetWorker backup and restore solution:

1. Select **Server Management > Backup and Restore > Legato NetWorker**. The “Legato NetWorker Backup Settings” table appears. See Figure 73.

2. Enter the following information:

   - **Enable Client**—Click to enable the check box to enable the Legato NetWorker backup client.

   - **Legato Server Hostnames**—Enter the fully qualified domain names of Legato NetWorker backup servers. Legato servers must have valid host names.

   - **Service port range**—Sets the range of the system’s service ports to the one specified (7937—9936).

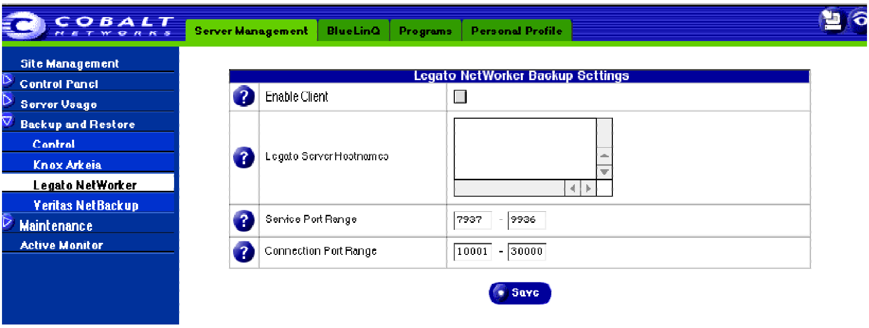
   - **Connection Port Range**—Sets the range of the system’s connection ports to the one specified (10001—30000).

3. Click **Save**. The table refreshes and displays the new configuration.

For further information on the Legato NetWorker backup and restore solution, see Appendix F, “Disaster Recovery with Third-Party Software”.

Figure 73 shows the “Legato NetWorker Backup Settings” table.

Figure 73. Legato NetWorker Backup Settings table



Legato NetWorker Backup Settings	
Enable Client	□
Legato Server Hostnames	
Service Port Range	7937 - 9936
Connection Port Range	10001 - 30000

Veritas NetBackup

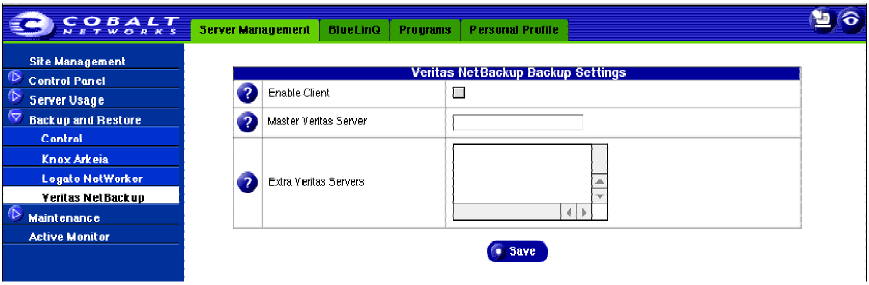
To configure the Veritas NetBackup backup and restore solution:

1. Select **Server Management > Backup and Restore > Veritas NetBackup**. The “Veritas NetBackup Backup Settings” table appears. See Figure 74.
2. Enter the following information:
   - **Enable Client**—Click the check box to enable the Veritas NetBackup backup client.
   - **Master Veritas Server**—Enter the fully qualified domain name of Veritas NetBackup master backup server. The Veritas master backup server must have a valid host name.
   - **Extra Veritas Servers**—Enter the fully qualified domain names of any extra Veritas NetBackup backup servers. All Veritas servers must have valid host names.
3. Click **Save**. The table refreshes and displays the new configuration.

For further information on the Veritas NetBackup backup and restore solution, see Appendix F, “Disaster Recovery with Third-Party Software”.

Figure 74 shows the “Veritas NetBackup Backup Settings” table.

Figure 74. Veritas NetBackup Backup Settings table



Veritas NetBackup Backup Settings	
Enable Client	□
Master Veritas Server	
Extra Veritas Servers	

Maintenance

In the **Maintenance** section under the **Server Management** tab, you can add new storage media, reboot the server and access system information, such as running a diagnostic test for trouble shooting problems on the server.

Storage

The Sun Cobalt RaQ XTR server appliance can hold up to four internal hard disk drives. If your server has less than four drives, you can add another hard disk drive. See Appendix C, “Upgrading the Sun Cobalt™ RaQ™ XTR server appliance” for installing an internal hard drive.

A virtual site cannot span multiple disks and the server appliance does not automatically recognize virtual sites on a hard disk drive that has been transferred from another Sun Cobalt RaQ XTR server appliance.

Note: If you have replaced a failed hard drive in the server appliance, you do not need to add the new hard drive through the Add Storage feature. When rebooting, the system automatically detects the new hard disk drive.

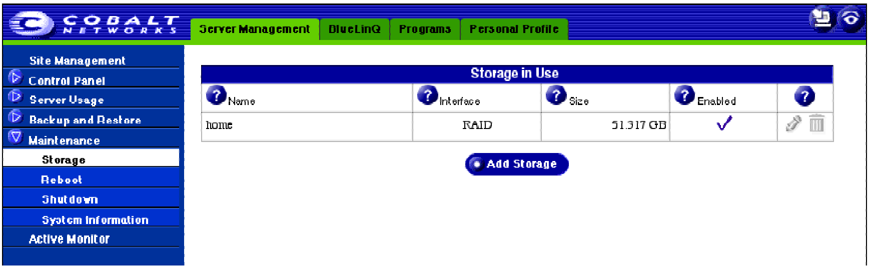
Once you replace a failed drive on the server appliance and reboot the server, the system detects the new hard disk drive and automatically begins to re-integrate it.

- For a RAID-1 configuration, the system synchronizes the new hard disk drive to the existing drive to recreate a mirrored disk drive.
- For a RAID-5 configuration, the system recreates the failed hard disk drive from the data available on the other hard disk drives.

During the process of re-integrating the new hard disk drive, the server appliance is not in a RAID configuration but it can still serve requests.

Figure 75 shows the “Storage in Use” table.

Figure 75. Storage in Use table



Storage in Use

Name	Interface	Size	Enabled	
home	RAID	51.317 GB	✓	

Adding a storage device

To add a hard disk drive through the UI:

1. Select **Server Management > Maintenance**. The “Storage in Use” table appears. See Figure 75.

2. Click **Add Storage**.

   A list of available hard disk drives appears. By default, if more than one hard disk drive is available, all of the drives are selected to be added. To de-select a drive, click the box beside that device.

   If there are no disks available to add, an error message at the bottom of the screen informs the Server Administrator.

3. To add a hard disk drive, give the drive a unique name. You can use only alphanumeric characters for the name. You cannot use the name “home” as that is the name of the primary hard disk of the Sun Cobalt RaQ XTR server appliance.

   Note: If you try to assign the name “home” to the second hard drive, you receive an error message stating “the name home is in use”.

   Note: You can choose to check the integrity of the hard disk drive when adding another drive. However, this option significantly increases the time required to format a drive.

   To enable this option, click the box in the Check column beside the hard drive.

4. Click **Confirm New Storage** to add the storage to the server appliance.

When adding a new virtual site to the server appliance, the Server Administrator can choose the hard disk drive on which to store the new site. In the “Add New Virtual Site” table, next to the Maximum allowed disk space (MB) parameter, a pull-down menu lists in alphabetical order the available hard disk drives. The drive with the most available space is chosen by default.

For more information, see “Adding a virtual site” on page 119.

Suspend a virtual site

There are two ways to suspend a virtual site on the server appliance: a hard suspension and a soft suspension.

For more information on soft suspensions, see “Site settings” on page 68.

Hard suspension

A hard suspension occurs when a hard disk drive is disabled through the Server Desktop UI. In this case, all virtual sites on that drive are inaccessible. You cannot administer these sites, and users cannot receive email.

To disable a hard disk drive:

1. Select **Server Management > Maintenance > Storage**. The “Storage in Use” table appears. See Figure 75.
2. Click the green *pencil* icon next to the hard disk drive you want to disable.
3. Click to disable the check box Enable disk.
4. Click **Confirm Modify**. The browser returns to the previous screen.

Reboot

Rebooting the Sun Cobalt RaQ XTR server appliance can sometimes cure problems with certain services and is required to recover from RAID failures. The Active Monitor software recommends when a reboot is necessary.

To reboot the server appliance through the Server Desktop UI:

1. Select **Server Management > Maintenance > Reboot**. The “Reboot Cobalt Server” table appears. See Figure 76.
2. A warning is displayed in the table that rebooting the server appliance will make it unavailable to the network for a few minutes.

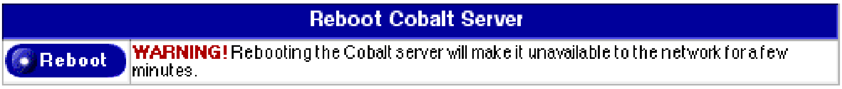
   Click **Reboot**. A confirmation dialog verifies the deletion.
3. Click **OK**.

You can also reboot the server appliance through its LCD console; refer to “Reboot” on page 191.

The reboot process can take a few minutes.

Figure 76 shows the “Reboot Cobalt Server” table.

Figure 76. Reboot Cobalt Server table



Reboot Cobalt Server

WARNING! Rebooting the Cobalt server will make it unavailable to the network for a few minutes.

Shutdown

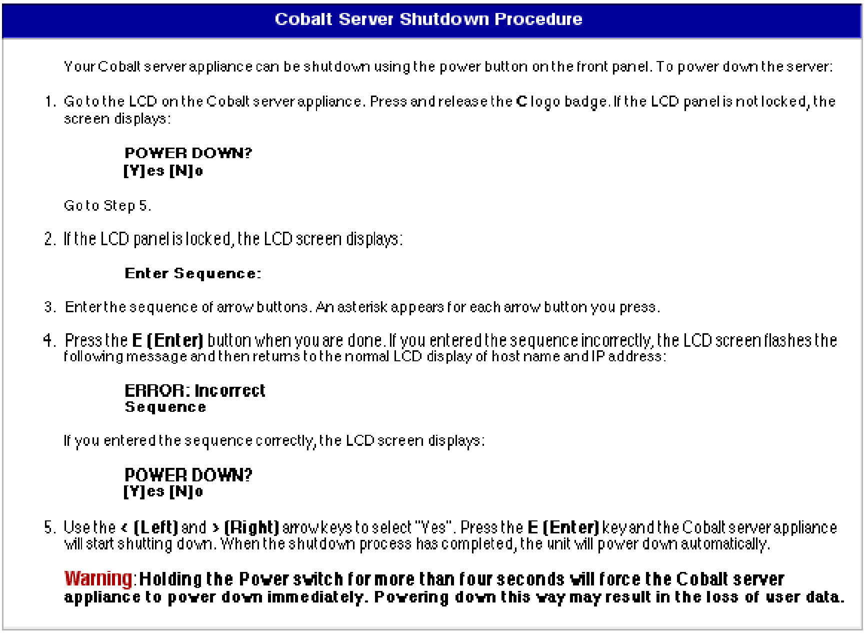
Caution: To prevent the potential loss of data, it is important to follow the proper power-down procedure before turning off the server appliance.

The Sun Cobalt RaQ XTR server appliance can only be shut down from the LCD console located on the front panel of the server. Refer to “Power down” on page 192.

Selecting **Server Management > Maintenance > Shutdown** displays the “Cobalt Server Shutdown Procedure” screen; see Figure 77.

Shutting down may take as long as a few minutes.

Figure 77. Shutdown Procedure screen



Cobalt Server Shutdown Procedure

Your Cobalt server appliance can be shutdown using the power button on the front panel. To power down the server:

1. Go to the LCD on the Cobalt server appliance. Press and release the **C** logo badge. If the LCD panel is not locked, the screen displays:

   POWER DOWN?
   [Y]es [N]o

   Go to Step 5.

2. If the LCD panel is locked, the LCD screen displays:

   Enter Sequence:

3. Enter the sequence of arrow buttons. An asterisk appears for each arrow button you press.

4. Press the **E (Enter)** button when you are done. If you entered the sequence incorrectly, the LCD screen flashes the following message and then returns to the normal LCD display of host name and IP address:

   ERROR: Incorrect
   Sequence

   If you entered the sequence correctly, the LCD screen displays:

   POWER DOWN?
   [Y]es [N]o

5. Use the **< (Left)** and **> (Right)** arrow keys to select "Yes". Press the **E (Enter)** key and the Cobalt server appliance will start shutting down. When the shutdown process has completed, the unit will power down automatically.

   Warning: **Holding the Power switch for more than four seconds will force the Cobalt server appliance to power down immediately. Powering down this way may result in the loss of user data.**

System Information

For more information on the Sun Cobalt RaQ XTR server appliance, select **Server Management > Maintenance > System Information**. The “Server Configuration Information” table appears. See Figure 78.

This table displays:

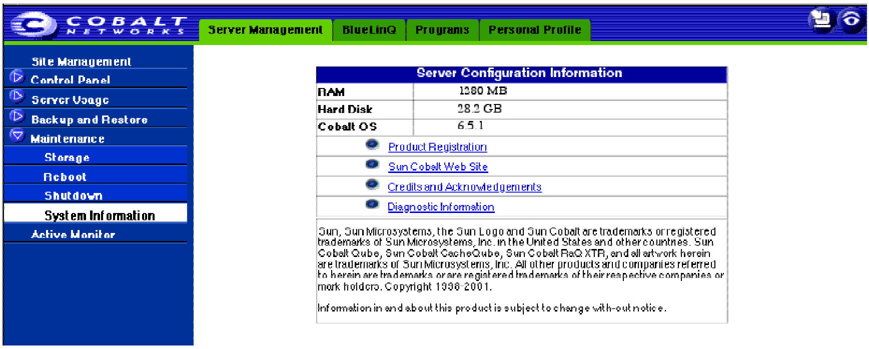
- the amount of RAM
- the size of the hard disk drive
- the version of the Cobalt OS
- Sun Microsystems trademark information

The table also contains four hypertext links:

- **Product Registration** allows you to register the server appliance online.
- **Sun Cobalt web site** takes you to the URL http://www.cobalt.com in a separate browser window.
- **Credits and Acknowledgements** acknowledges the software used on the server appliance.
- **Diagnostic Information**

Figure 78 shows the “Server Configuration Information” table.

Figure 78. Server Configuration Information table



Server Configuration Information	
RAM	1280 MB
Hard Disk	28.2 GB
Cobalt OS	6.5.1
● Product Registration	
● Sun Cobalt Web Site	
● Credits and Acknowledgements	
● Diagnostic Information	

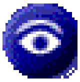
Sun, Sun Microsystems, the Sun Logo and Sun Cobalt are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. Sun Cobalt Qube, Sun Cobalt CacheQube, Sun Cobalt RaQ XTR, and all artwork herein are trademarks of Sun Microsystems, Inc. All other products and companies referred to herein are trademarks or are registered trademarks of their respective companies or mark holders. Copyright 1998-2001.

Information in and about this product is subject to change with-out notice.

Active Monitor

The Sun Cobalt RaQ XTR server appliance uses Active Monitor software. Active Monitor is a utility that runs on Sun Cobalt server appliances and updates key system information every 15 minutes.

Active Monitor icon



The Active Monitor icon in the top right corner of the Server Desktop UI allows you to view status information. The icon flashes red if any of the components or services monitored by Active Monitor fails or is under heavy use.

If you click this icon, the Active Monitor screen under the Server Management tab appears.

The Active Monitor icon and status page are displayed on the **Server Management** screen only.

Active Monitor status tables

To view the Active Monitor status of a system component or a service:

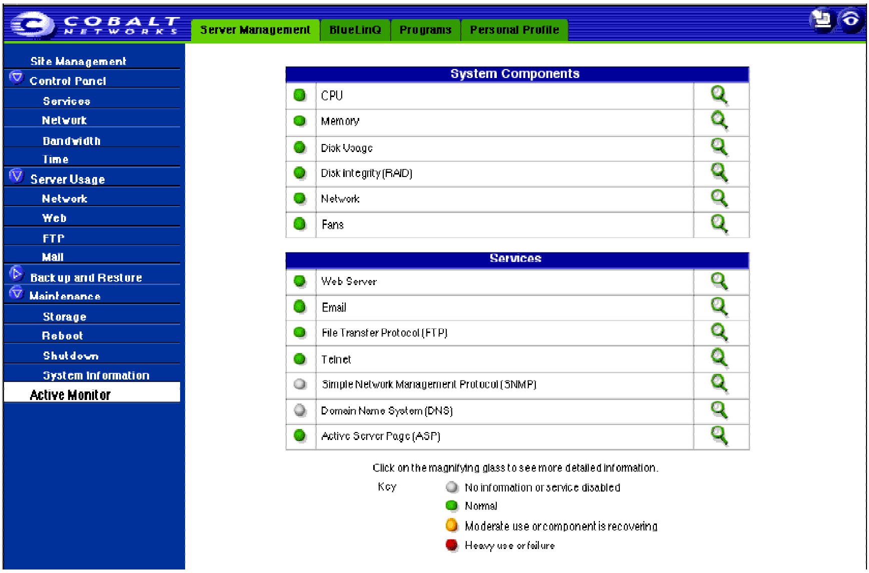
1. Select **Server Management > Active Monitor**. The status tables appear; see Figure 79.
2. The status of each of the items is indicated by a green, yellow, red or grey circle beside each item. The colors have the following significance:
   - **Grey**—No information is available or the service is not enabled.
   - **Green**—The services and components are functioning normally.
   - **Yellow**—There is moderate use on the server or a component is recovering.
   - **Red**—There is heavy use on the server or a failure.
3. To view detailed status information for a particular system component or service, click the green *magnifying-glass* icon in right column that corresponds to the name of the item.

   The detailed status information for the Disk Integrity (RAID) displays a text and graphic representation of the status of the hard disk drives in the server. It also indicates the number of hard disk drives present and the level of RAID that has been implemented.

   The detailed status information for the Fans displays a text and graphic representation of the status of the six fans in the server.

✍ ***Note:*** For more information on replacing a hard disk drive or a fan, see Appendix C, "Upgrading the Sun Cobalt™ RaQ™ XTR server appliance".

Figure 79. Active Monitor status tables



System Components		
🟢	CPU	🔍
🟢	Memory	🔍
🟢	Disk Usage	🔍
🟢	Disk Integrity (RAID)	🔍
🟢	Network	🔍
🟢	Fans	🔍

Services		
🟢	Web Server	🔍
🟢	Email	🔍
🟢	File Transfer Protocol (FTP)	🔍
🟢	Telnet	🔍
⚪	Simple Network Management Protocol (SNMP)	🔍
⚪	Domain Name System (DNS)	🔍
🟢	Active Server Page (ASP)	🔍

Click on the magnifying glass to see more detailed information.

Key		
	⚪	No information or service disabled
	🟢	Normal
	🟡	Moderate use or component is recovering
	🔴	Heavy use or failure

RAID failure

For a failed hard disk drive, Active Monitor indicates with a graphic (see Figure 80) the particular drive that has failed.

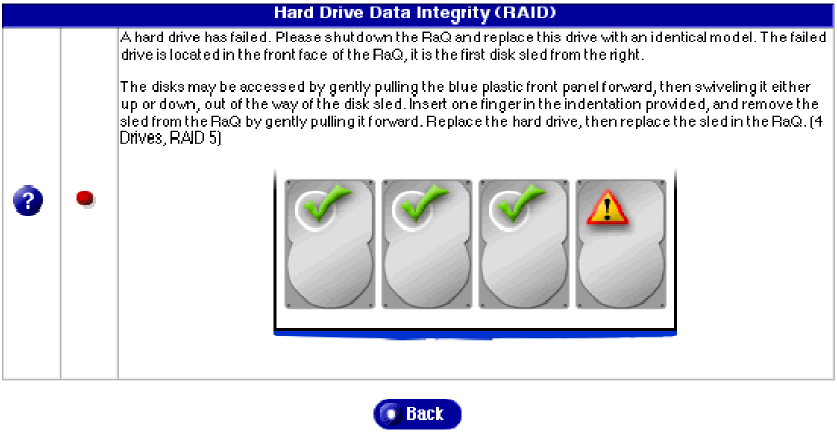
If a drive in a RAID-0 configuration fails, the server appliance fails. If a drive in a RAID-1 or RAID-5 configuration fails and the server is still operating, the system indicates the non-RAID status in three ways:

- An email is sent to the Server Administrator.
- Under **Server Management > Active Monitor**, the Disk Integrity (RAID) circle changes to red.
- The “C” logo badge on the front panel of the server appliance blinks.

To view the status of the RAID configuration:

1. Select **Server Management > Active Monitor**. The status tables appear.
2. Click the green *magnifying-glass* icon to see the detailed view of Disk Integrity (RAID).

Figure 80. Failed hard disk drive



Hard Drive Data Integrity (RAID)

A hard drive has failed. Please shutdown the RaQ and replace this drive with an identical model. The failed drive is located in the front face of the RaQ, it is the first disk sled from the right.

The disks may be accessed by gently pulling the blue plastic front panel forward, then swiveling it either up or down, out of the way of the disk sled. Insert one finger in the indentation provided, and remove the sled from the RaQ by gently pulling it forward. Replace the hard drive, then replace the sled in the RaQ. (4 Drives, RAID 5)

If the server appliance has been configured for RAID-0 and a hard disk drive fails, all data is lost.

If the server appliance has been configured for RAID-1 and a single hard disk drive fails, the server appliance can continue to operate. To restore the RAID-1 configuration (disk mirroring), you must replace the failed hard disk drive and reboot the server appliance.

If the server appliance has been configured for RAID-5 and a single hard disk drive fails, the server appliance cannot operate. To restore the RAID-5 configuration (parity striping), you must replace the failed hard disk drive and reboot the server.

Note: You can remove the failed hard disk drive and insert a replacement drive without powering down the server appliance. However, to re-establish RAID service, you must reboot the server so that the system will integrate the replacement drive.

In case of a failed hard disk drive, the replacement drive must be the same model number by the same manufacturer as the failed hard disk drive, and it should have the same storage capacity. If you cannot find a hard disk drive to match the failed drive, you can use a replacement drive that has a larger storage capacity than the failed drive.

See Appendix C, “Upgrading the Sun Cobalt™ RaQ™ XTR server appliance” for more information on replacing a failed hard disk drive.

Once you replace a failed drive on a Sun Cobalt RaQ XTR server appliance and reboot the server, the system detects the new hard disk drive and automatically begins to re-integrate it.

- For a RAID-1 configuration, the system synchronizes the new hard disk drive to the existing drive to recreate a mirrored disk drive.
- For a RAID-5 configuration, the system recreates the failed hard disk drive from the parity data available on the other hard disk drives.

Note: While the server appliance server is re-integrating the new hard disk drive, the server is not in a RAID configuration but it can still serve requests.

You can verify that the server is re-integrating the replacement disk drive through Active Monitor.

1. Select **Server Management > Active Monitor**. The status tables for the system components and services appear.

   The status for “Disk Integrity (RAID)” should be yellow.

2. Click the green *magnifying-glass* icon to see the detailed view of the re-integration process.

Important: If the detailed view of the “Disk Integrity (RAID)” component does not show the replacement hard disk drive being re-integrated, the replacement drive is not compatible with the remaining drives.

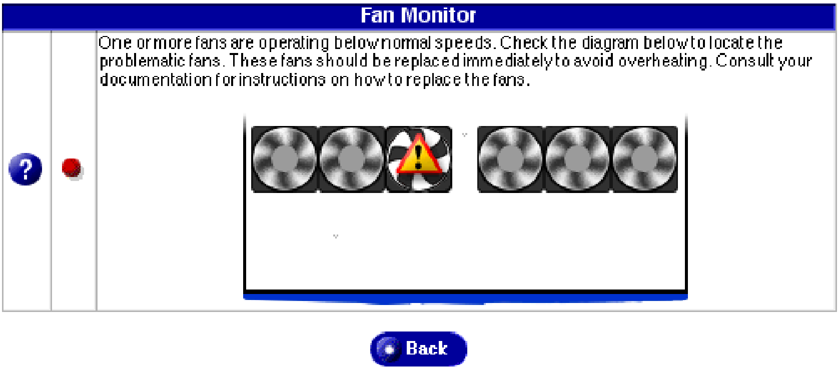
Verify that the replacement drive matches the make and model of the failed hard disk drive.

Fan failure

For a failed fan, Active Monitor indicates with a graphic (see Figure 81) the particular fan that has failed.

See Appendix C, “Upgrading the Sun Cobalt™ RaQ™ XTR server appliance” for more information on replacing a failed fan.

Figure 81. Failed fan



Fan Monitor

One or more fans are operating below normal speeds. Check the diagram below to locate the problematic fans. These fans should be replaced immediately to avoid overheating. Consult your documentation for instructions on how to replace the fans.

BlueLinQ

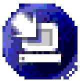
The BlueLinQ™ Application Delivery Service provides instant access to product updates and new services as they become available. Using the BlueLinQ technology, the Sun Cobalt RaQ XTR server appliance informs you when new software is available.

When you log into the server appliance as *admin* or *alteradmin*, the **BlueLinQ** tab appears in the top menu bar of the Server Desktop UI. When you select this tab, the left menu bar displays commands that allow you to add new software, update the current server appliance software, view the installed software and change the settings for the BlueLinQ feature.

The following functions are available under the **BlueLinQ** tab on the Server Desktop UI.

1. New Software
2. Updates
3. Installed Software
4. Settings

Software Notification icon



The Software Notification icon in the top right corner of the Server Desktop UI allows you to check for new or updated software packages and to install them if any are found. The icon changes color when new or updated software packages are available.

If you click this icon, the “Available New Software List” table under the BlueLinQ tab appears.

New Software

To install new software through BlueLinQ:

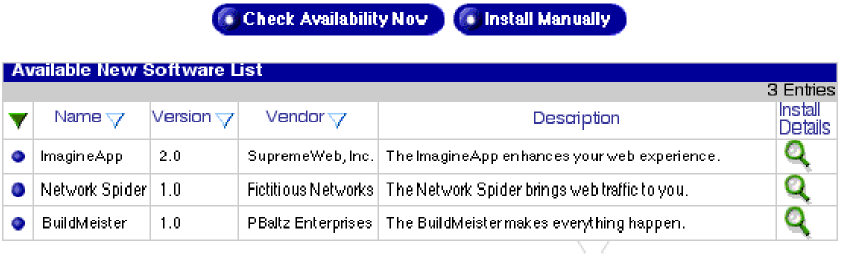
1. Select **BlueLinQ > New Software.** The “Available New Software List” table appears; see Figure 82.

   The table displays the name of the software, the version number, the vendor, a short description of the software and green *magnifying-glass* icon to view the installation details.

   The first column displays either a solid or hollow blue circle.

   - A solid blue circle indicates that you have not seen this new software package before.
   - A hollow blue circle indicates that you have already seen this software package.

Figure 82. Available New Software List table



Available New Software List

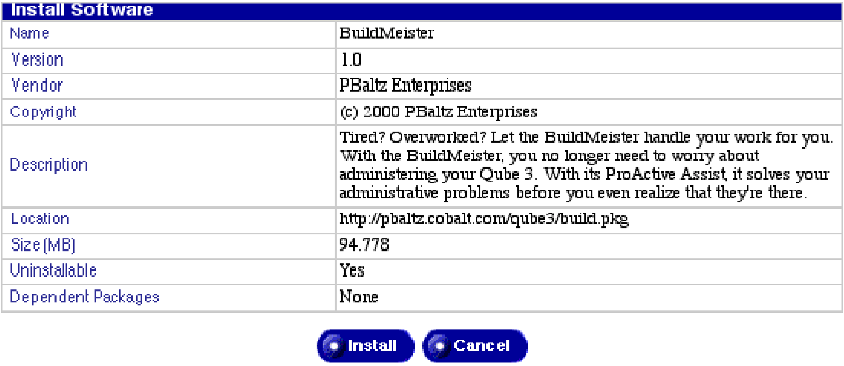
3 Entries

	Name	Version	Vendor	Description	Install Details
●	ImagineApp	2.0	SupremeWeb, Inc.	The ImagineApp enhances your web experience.	🔍
●	Network Spider	1.0	Fictitious Networks	The Network Spider brings web traffic to you.	🔍
●	BuildMeister	1.0	PBaltz Enterprises	The BuildMeister makes everything happen.	🔍

2. To install a software package listed in the table, click the green *magnifying-glass* icon. The “Install Software” table appears; see Figure 83. In addition to the information listed in Step 1, the following information is also provided for the software package:

   - the copyright information
   - a longer description of the software
   - the URL location
   - the size of the software package (in MB)
   - whether the software package is uninstallable
   - a list of software packages that must be installed on the system before this new package can be safely installed.

Figure 83. Install Software table



Install Software	
Name	BuildMeister
Version	1.0
Vendor	PBaltz Enterprises
Copyright	(c) 2000 PBaltz Enterprises
Description	Tired? Overworked? Let the BuildMeister handle your work for you. With the BuildMeister, you no longer need to worry about administering your Qube 3. With its ProActive Assist, it solves your administrative problems before you even realize that they're there.
Location	http://pbaltz.cobalt.com/qube3/build.pkg
Size (MB)	94.778
Uninstallable	Yes
Dependent Packages	None

3. Click **Install**. If a License Agreement has been included in the software package, a License screen appears. You can either accept or decline the license.

   If you click **Decline**, you return to the “Available New Software List” table.

   If you click **Accept**, a status table appears. The first field indicates the state of the software package during the operation; the second field indicates the progress of the upload with a percentage bar. Once it is completed, a message appears indicating that the software was loaded successfully or that an error occurred.

   If there is no License Agreement in the software package, a status table appears (as described above).

Check availability of new software

You can force the system to check for new software immediately.

1. Select **BlueLinQ > New Software**. The “Available New Software List” table appears.
2. Click **Check Availability Now**. If new packages are available, they are added to the “Available New Software List” table.

   To install a new software package, see “New Software” on page 169.

Install new software manually

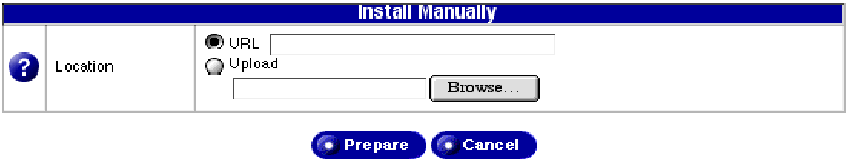
You can install new software manually if you know the location of the software package.

1. Select **BlueLinQ > New Software**. The "Available New Software List" table appears.
2. Click **Install Manually**. The "Install Manually" table appears; see Figure 84.
3. To specify the location of the software package, do one of the following:
   - Click the URL radio button.

     Enter a URL beginning with either http:// or ftp:// to download the package from a location on the Internet.
   - Click the Upload radio button.

     Click **Browse** to locate a file on your local hard disk drive.
   - If you have previously downloaded software packages to the `/home/packages` directory on your Sun Cobalt RaQ XTR server appliance, you can choose one of these packages from the table.
4. Click **Prepare**. The system verifies that the file is in the correct .pkg format. The system then begins to load the software.

Figure 84. Install Manually table



Updates

To install a software update through BlueLinQ:

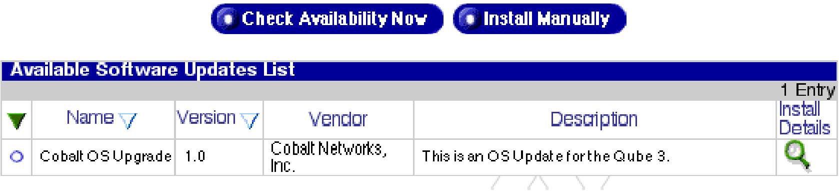
1. Select **BlueLinQ > Updates**.The “Available Software Updates List” table appears; see Figure 85.

   The table displays the name of the software, the version number, the vendor, a short description of the software and green *magnifying-glass* icon to view the installation details.

   The first column displays either a solid or hollow blue circle.

   - A solid blue circle indicates that you have not seen this software update package before.
   - A hollow blue circle indicates that you have already seen this software update package.

Figure 85. Available Software Updates List table



Available Software Updates List

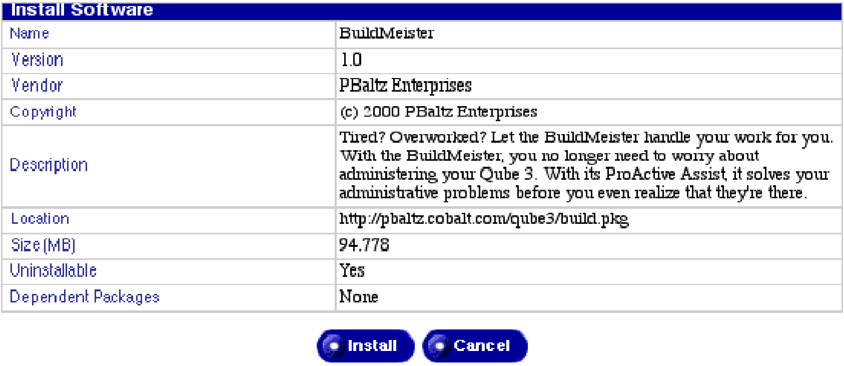
1 Entry

▼	Name	Version	Vendor	Description	Install Details
○	Cobalt OS Upgrade	1.0	Cobalt Networks, Inc.	This is an OS Update for the Qube 3.	🔍

2. To install a software update package listed in the table, click the green *magnifying-glass* icon. The “Install Software” table appears; see Figure 86. In addition to the information listed in Step 1, the following information is also provided for the software package:

   - the copyright information
   - a longer description of the software
   - the URL location
   - the size of the software package (in MB)
   - whether the software package is uninstallable
   - a list of software packages that must be installed on the system before this new package can be safely installed.

Figure 86. Install Software table



Install Software	
Name	BuildMeister
Version	1.0
Vendor	PBaltz Enterprises
Copyright	(c) 2000 PBaltz Enterprises
Description	Tired? Overworked? Let the BuildMeister handle your work for you. With the BuildMeister, you no longer need to worry about administering your Qube 3. With its ProActive Assist, it solves your administrative problems before you even realize that they're there.
Location	http://pbaltz.cobalt.com/qube3/build.pkg
Size (MB)	94.778
Uninstallable	Yes
Dependent Packages	None

3. Click **Install**. If a License Agreement has been included in the software package, a License screen appears. You can either accept or decline the license.

   If you click **Decline**, you return to the “Available Software Updates List” table.

   If you click **Accept**, a status table appears. The first field indicates the state of the software package during the operation; the second field indicates the progress of the upload with a percentage bar. Once it is completed, a message appears indicating that the software was loaded successfully or that an error occurred.

   If there is no License Agreement in the software package, a status table appears (as described above).

Check availability of software update packages

You can force the system to check for software update packages immediately.

1. Select **BlueLinQ > Updates**. The “Available Software Updates List” table appears.
2. Click **Check Availability Now**. If software update packages are available, they are added to the “Available Software Updates List” table.

   To install a software update package, see “Updates” on page 172.

Install software updates manually

You can install software update packages manually if you know the location of the software update package.

1. Select **BlueLinQ > Updates**. The "Available Software Updates List" table appears.

2. Click **Install Manually**. The "Install Manually" table appears; see Figure 87.

3. To specify the location of the software package, do one of the following:

   - Click the URL radio button.

     Enter a URL beginning with either http:// or ftp:// to download the package from a location on the Internet.

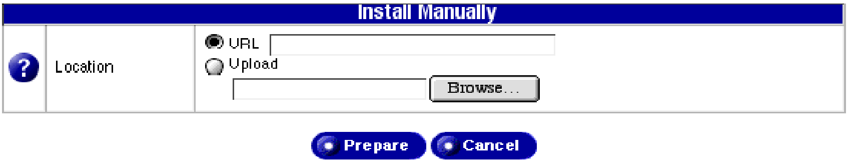
   - Click the Upload radio button.

     Click **Browse** to locate a file on your local hard disk drive.

   - If you have previously downloaded software packages to the `/home/packages` directory on your Sun Cobalt RaQ XTR server appliance, you can choose one of these packages from the table.

4. Click **Prepare**. The system verifies that the file is in the correct .pkg format. The system then begins to load the software.

Figure 87. Install Manually table



Install Manually		
?	Location	● URL ○ Upload Browse...

Installed Software

On the Sun Cobalt RaQ XTR server appliance, the package *Cobalt OS* is installed on the server appliance at the factory.

Note: You cannot un-install the default packages.

To view the software installed on the server appliance:

1. Select **BlueLinQ > Installed Software.** The “Installed Software” List table appears; see Figure 88.

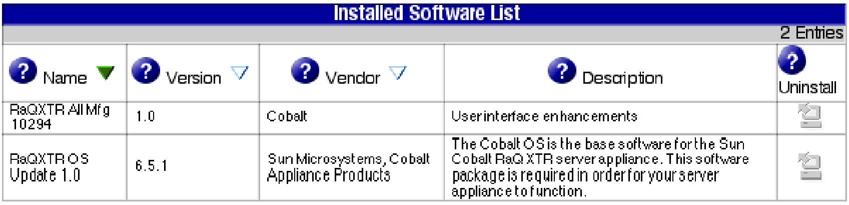
   The columns show the name of the software, the version number, the vendor and a short description of the software.

2. Click the icon in the Uninstall column if you wish to uninstall a particular software. A confirmation dialog appears to proceed with the uninstall procedure.

   Software packages for which the *uninstall* icon is disabled (grayed-out) cannot be uninstalled from the server appliance.

3. Click **OK**.

Figure 88. Installed Software List table



Installed Software List

2 Entries

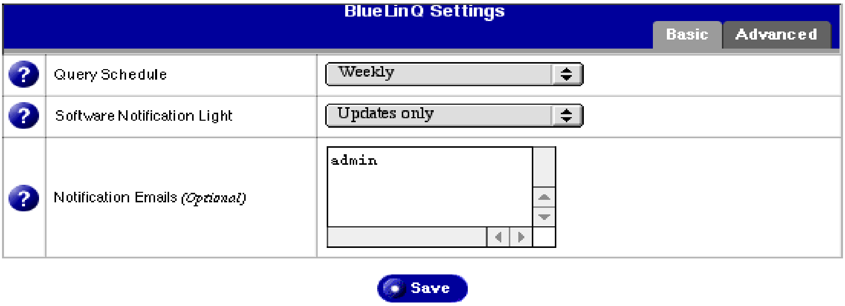
Name	Version	Vendor	Description	Uninstall
RaQXTR All Mfg 10294	1.0	Cobalt	User interface enhancements	
RaQXTR OS Update 1.0	6.5.1	Sun Microsystems, Cobalt Appliance Products	The Cobalt OS is the base software for the Sun Cobalt RaQ XTR server appliance. This software package is required in order for your server appliance to function.	

Settings

To view or modify the settings for the BlueLinQ feature:

1. Select **BlueLinQ > Settings**. The “BlueLinQ Settings” table appears; see Figure 89 for the Basic settings and Figure 90 for the Advanced settings. The active tab is a light-grey color.

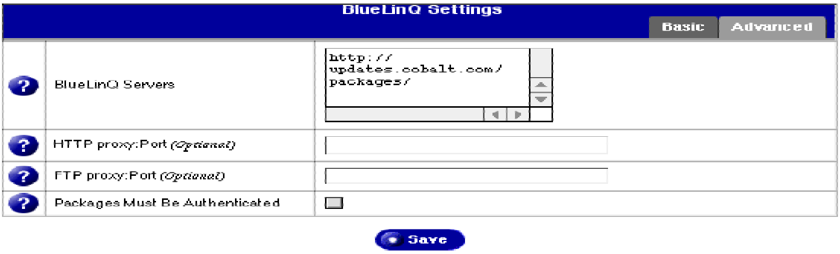
Figure 89. BlueLinQ Settings - Basic table



BlueLinQ Settings

Query Schedule	Weekly
Software Notification Light	Updates only
Notification Emails *(Optional)*	admin

Figure 90. BlueLinQ Settings - Advanced table



BlueLinQ Settings

BlueLinQ Servers	http:// updates.cobalt.com/ packages/
HTTP proxy:Port *(Optional)*	
FTP proxy:Port *(Optional)*	
Packages Must Be Authenticated	□

2. Configure the fields in the “BlueLinQ Settings” tables.

   Basic settings:

   - **Query Schedule**—Specify how frequently the Sun Cobalt RaQ XTR server appliance checks the BlueLinQ server for new or updated software packages: daily, weekly, monthly or never.
   - **Software Notification Light**—Specify the type of software that activates the Software Notification Light and, if applicable, the type of new software that appears in notification email messages.

     You can select “all software” or “updates only”.
   - **Notification Emails**—Enter an email address(es) to which notification of new software or errors in queries for software update are sent. The notification email is sent in accordance with the Software Notification Light setting.

     If you do not want to receive these notifications, leave this field blank.

   Advanced Settings:

   - **BlueLinQ Server(s)**—Enter the HTTP address(es) of the location(s) to query for software updates. You can enter more than one address in this scrolling window; enter each HTTP address on a separate line.

     The default location of the **Sun Cobalt** Update Server is http://updates.cobalt.com/packages/.

> ✍ ***Note:*** To receive updates from Sun Microsystems for the Sun Cobalt RaQ XTR server appliance, you must retain the URL http://updates.cobalt.com/packages/ in this field.

   - **HTTP proxy:port** *(optional)*—Enter the proxy server and port for HTTP queries if a proxy server is needed to reach outside your firewall.

     For example: proxy.mycompany.com:8080.
   - **FTP proxy:port** *(optional)*—Enter the proxy server and port for FTP queries if a proxy server is needed to reach outside your firewall.

     For example: proxy.mycompany.com:8080.
   - **Packages must be authenticated**—If enabled, BlueLinQ installs only packages that have passed an authentication check.

3. Click **Save**.

   The screen refreshes to the “BlueLinQ Settings - Basic” table.

Services

This chapter includes information on configuring your email client, and on creating and uploading Web pages.

Using email on the server appliance

To use all of the email capabilities on the Sun Cobalt™ RaQ™ XTR server appliance, the email parameter settings must be correct; see “Email server” on page 127. You must also configure your email application to send and retrieve email from the server appliance.

Ensure the following information is entered into your email program:

1. **Email address** The format is:

   <username>@hostname.domainname

   (for example, myname@raqxtr.cobalt.com) where:

   - <username> is the user ID assigned to you (for example, myname)
   - <hostname> is the name assigned to the server appliance (for example, raqxtr)
   - <domainname> is either the official domain name (for example, cobalt.com) that is registered with a name registrar accredited by the Internet Corporation for Assigned Names and Numbers (ICANN) or an intranet domain name specific to your network. Obtain this information from your system administrator.

     For more information on ICANN, visit the ICANN Web site at http://www.icann.org.

2. **SMTP server** The format is hostname.domainname (for example, raqxtr.cobalt.com).

3. **POP3 server** The format is hostname.domainname (for example, raqxtr.cobalt.com).

4. **IMAP server** The format is hostname.domainname (for example, raqxtr.cobalt.com).
5. **APOP server** The format is hostname.domainname (for example, raqxtr.cobalt.com).

Note: Occasionally, an email application asks for an *incoming* mail server. The incoming mail server is the POP3 server.

Developing Web pages

You can create complex Web pages using any of the standard HTML editors and the HTML publishing capabilities of many popular desktop productivity applications.

You can create and link the Web pages on your desktop computer, and then move them to the appropriate subdirectory on the Sun Cobalt RaQ XTR server appliance through a file transfer protocol (FTP) application; see “Publishing Web pages using FTP” on page 181.

CGI scripts

The server appliance supports common gateway interface (CGI) scripts, such as those written in Perl, C or other languages. If CGI is enabled for your virtual site (see the “Site Settings” table under the **Site Management > Site Settings** tab), you can add CGI scripts to work with your Web content.

You can develop CGI scripts on your desktop machine and then transfer them to the server appliance by means of any FTP-based application that allows permission bits to be set to *executable*.

Use FTP to upload .cgi and .pl files; use ASCII mode to upload CGI files. Once the file is on the server appliance, use your FTP program to make the script executable. You can also use the telnet command:

```
chmod 775 <filename>.cgi
```

In order for users (other than the Server Administrator) to add CGI files, CGI must be enabled for the user’s virtual site (see the “Site Settings” table under the **Site Management > Site Settings** tab). CGI scripts must use .pl or .cgi filename extensions in order to be executed by the Web server.

Server-side scripting languages

The Sun Cobalt RaQ XTR server appliance supports both the Active Server Pages (ASP) and PHP scripting languages. These features are enabled on a per-site basis (see the “Site Settings” table under the **Site Management > Site Settings** tab).

Like CGI scripts, you can develop ASP and PHP scripts on your desktop machine and then transfer them to the server appliance by means of an FTP-based application. Unlike CGI scripts, ASP and PHP do not require execute permissions to work correctly. However, ensure that the Web server process can read the scripts; you can use the telnet command:

`chmod 664 <filename>.asp` or `chmod 664 <filename>.php`

For the Web server to run the scripts correctly, ASP scripts must use the .asp filename extension and PHP scripts must use the .php filename extension.

Publishing Web pages using FTP

Note: For more information about the directory structure on the server appliance, see “Directory structure” on page 232.

After creating your Web pages, you can publish them on the Sun Cobalt RaQ XTR server appliance using an FTP-based application.

Make sure you have the following information:

- the host name or the IP address of your server appliance
- your user name and password
- a filename of your choice to save as your main page (the default is index.html)

Launch your FTP software and establish an FTP link to the server appliance. Upload your HTML files. If you need help, consult the instructions for your FTP application.

By default, the files you upload using an FTP-based application are stored in your personal directory; the directory path is:

```
/home/sites/<sitename>/users/<username>
```

where <sitename> is the fully qualified domain name of your virtual site and <username> is your user name.

Note to the Site Administrator: To post Web pages for your site, you must upload to the directory `/home/sites/<sitename>/web`.

Only Site Administrators or the Server Administrator can upload to this directory. If you do not specify this directory, your Web pages are stored in your personal directory which is not accessible from the Web.

The Site Administrator can access and edit the site root content in the directory `/web` during an FTP session. The site Web root is accessible on the Web at http://<sitename>/.

Site Administrators can edit their personal Web pages in the directory `/users/<username>/web` during an FTP session. Personal Web sites are accessible on the Web at

- http://<sitename>/users/<username>/
- http://<sitename>/~<username>/

Users who are not Site Administrators can edit their personal Web sites in the directory `/web` during an FTP session.

Publishing Web pages with FrontPage for User Webs only

If FrontPage Server Extensions are enabled on a site, a Site Administrator can enable FrontPage User Webs.

To publish a Web page using FrontPage:

1. Using FrontPage Explorer on a personal computer, select **Open Web**.
2. In the Folder Name field, enter the following:

   http://<exactvirtualsitename>/~<username>/

   For example, the user Jason Paez would enter

   http://raqxtr.cobalt.com/~jpaez/
3. Click **OK**. An authentication dialog appears.
4. Enter your user name and password assigned to you on the server appliance.
5. Click **OK**.

For FrontPage and FrontPage Web information and technical support, see http://www.microsoft.com/frontpage/ and http://www.rtr.com/.

Using the LCD Console

During startup, the liquid-crystal-display (LCD) screen on the front panel of the Sun Cobalt™ RaQ™ XTR server appliance displays status information about the boot process itself.

When setting up the server appliance, you use the LCD console to enter network configuration information for the server appliance.

Once the server appliance is running, the LCD console serves several purposes. Through the LCD console, you can:

- change the network configuration information, which is useful if the location of the server appliance is changed
- configure the uninterruptible power supply (UPS)
- reboot, which restarts the entire server appliance
- lock the LCD panel with a sequence arrow buttons
- set the server appliance to power up automatically after a loss of power
- reset the Server Administrator password for the server appliance
- exit from the LCD commands without making any changes

Important: To power down the server appliance server, press and release the “C” badge. The server appliance powers down in a manner that allows the server to close all open files and minimizes startup time the next time the server appliance is powered on.

Before turning off the server appliance, follow the proper power-down procedure, as described in “Power down” on page 192.

Locked LCD panel

The Sun Cobalt RaQ XTR server appliance offers a security feature that allows you to lock the LCD panel with a “password” consisting of a sequence of arrow buttons. This prevents unauthorized tampering with the server if people have physical access to it.

For any of the LCD functions, if the LCD panel is locked, the system prompts you to enter the key sequence before you can access the functions. Enter the sequence of arrow buttons and press the E (enter) button. For more information, see “Panel” on page 193.

Access to the functions

You access each of the LCD functions by holding down the S (select) button on the LCD console for approximately two seconds. This action causes the LCD screen to enter its function mode. If the LCD panel is locked, you must enter the correct sequence of arrow buttons to unlock the panel. Press the S button until the function you want appears on the LCD screen. To cancel the LCD function mode, select the **EXIT** function when it appears on the screen. Press the E button and select **YES**.

Set up network

To reset the IP address or change the network configuration of the Network 1 interface:

1. On the LCD console, hold down the S button for approximately 2 seconds.

   The LCD screen displays:

   ```
   SELECT:
       SETUP NETWORK
   ```

2. Press the E button.

3. Enter the IP address using the arrow buttons. The left and right arrow buttons move the cursor position to the left or right. The up and down arrow buttons increase or decrease the digit at the cursor position.
4. Press the E button.
5. Enter the Netmask using the arrow buttons.
6. Press the E button.
7. Enter the Gateway using the arrow buttons.
8. Press the E button.
9. Use the arrow buttons to toggle the cursor between [S]ave and [C]ancel.
10. Press the E button.

If you select the Save option, the server appliance reboots using the new network configuration. If you select Cancel, you return to step 1 of this procedure.

Note: You can also change the network configuration of the Network 1 or Network 2 interface on the Sun Cobalt RaQ XTR server appliance through the browser-based user interface (UI), known as the Server Desktop. See “Network” on page 136.

If you change the network IP address of the server appliance through the Web browser, the server appliance reboots automatically when you click **Save Changes**.

Configure UPS

The are two options for configuring the Sun Cobalt RaQ XTR server appliance for a UPS: as the *master* or as a *slave*.

Note: If the UPS unit tells the server appliance to power down, the server appliance goes through the normal power-down sequence.

If you then want to power up that server appliance, someone must be physically present to power up the server appliance from the fron panel. You cannot power up a server appliance remotely.

The *master* communicates directly to the UPS through the serial port. The *slave* (or *slaves*) communicates with a master (not a Sun Cobalt RaQ XTR server appliance) over the network to verify the status of the power supply.

Note: The server appliance cannot act as a *master* for other machines. Allowing *slave* access by arbitrary machines would pose a security risk.

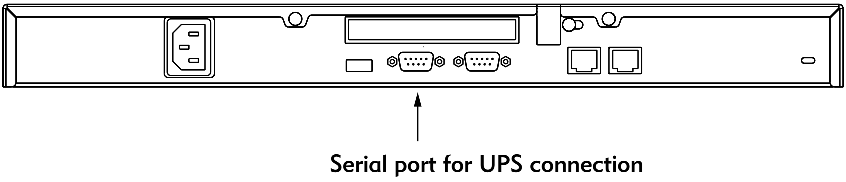
The distinction between *master* and *slave* is whether the server appliance is connected directly to the UPS (a *master*) or pointed to another machine that is connected to the UPS (a *slave*).

If you configure the server appliance as a *slave*, you must have, on the network, a machine acting as a UPS master that is configured to allow *slave* access for the IP address of your server appliance.

If you configure a server appliance as a *master*, the server appliance configures itself automatically. Before choosing this option, you must first connect the UPS to the server appliance through the serial port; see Figure 91 for the correct serial port.

If you configure a server appliance as a slave, the LCD screen prompts you for the IP address of the device that is configured as the master.

Figure 91. Serial port for UPS connection



To configure the server appliance for the UPS, first connect the UPS and the server appliance, and then configure the server appliance through the LCD panel. (Refer to the UPS manual for more information on connecting the devices.)

1. Plug the UPS unit into the wall socket.
2. Turn on the UPS.
3. Plug the server appliance units into the UPS power sockets.
4. Connect the UPS serial cable to the UPS unit and the serial port on the server appliance that will serve as the master. See Figure 91.

Important: You must use the serial cable shipped with the UPS unit.

5. On the LCD console, hold down the S button for approximately 2 seconds.

   The LCD screen displays:

   ```
   SELECT:
       SETUP NETWORK
   ```

6. Press the S button until **CONFIGURE UPS** appears in the LCD screen:

   ```
   SELECT:
       CONFIGURE UPS
   ```

7. Press the E button.
8. Use the arrow buttons to toggle the cursor between [ ] On and [ ] Off. Select [ ] On.
9. Press the E button.
10. Use the arrow buttons to toggle the cursor between [M]aster and [S]lave.
11. Press the E button. If you choose [M]aster, the server appliance configures itself automatically for the UPS.

12. If you choose [S]lave, the LCD screen prompts you for the IP address of the device configured as the master.

    Enter the IP address using the arrow buttons. The left and right arrow buttons move the cursor position to the left or right. The up and down arrow buttons increase or decrease the digit at the cursor position.

13. Press the (E) button.

    The LCD screen returns to the host name and IP address. The LCD screen does NOT prompt you to save the changes.

Verifying the UPS configuration

To verify that you have configured the UPS correctly:

1. Unplug the UPS unit from the wall socket to simulate a power outage to the UPS.
2. The UPS unit takes over the power supply to the server appliance servers. Each of the server appliances monitoring the UPS displays on the LCD screen:

   ```
   UPS:
       ON BATTERY
   ```

3. Plug the UPS unit into the wall socket again. Each of the server appliances monitoring the UPS unit displays on the LCD screen:

   ```
   UPS:
       POWER RESTORED
   ```

   After a few seconds, the LCD screen returns to the normal LCD display of host name and IP address.

Reboot

To reboot the Sun Cobalt RaQ XTR server appliance through the LCD console:

1. On the LCD console, hold down the (S) button for approximately 2 seconds.

   The LCD screen displays:

   ```
   SELECT:
       SETUP NETWORK
   ```

2. Press the (S) button until **REBOOT** appears in the LCD screen:

   ```
   SELECT:
       REBOOT
   ```

3. Press the (E) button.
4. Use the arrow buttons to toggle the cursor between [Y] and [N]. Select [Y] to reboot the system.
5. Press the (E) button.

Note: You can also reboot the server appliance through the Server Desktop UI. See “Reboot” on page 159.

Power down

Caution: To prevent the potential loss of data, it is important to follow the proper power-down procedure before turning off the server appliance.

Note: You can power down the server appliance remotely, but you cannot power up the server appliance remotely. Someone must physically power up the server.

For more information, see "Powering down the server appliance remotely" on page 228.

You power down the server appliance through the "C" logo badge on the front panel. To power down the server appliance:

1. On the front panel, press and release the "C" logo badge. DO NOT press the "C" logo badge for more than two or three seconds.
2. If the LCD panel is not locked, the LCD screen displays:

   ```
   POWER DOWN?
   [Y]ES [N]O
   ```

   Go to Step 6.
3. If the LCD panel is locked, the LCD screen displays:

   ```
   Enter Sequence:
   ```
4. Enter the sequence of arrow buttons. An asterisk appears for each arrow button you press.
5. Press the Ⓔ button.

   If you entered the sequence incorrectly, the LCD screen flashes the following message and then returns to the normal LCD display of host name and IP address:

   ```
   ERROR: Incorrect
       sequence
   ```

   If you entered the sequence correctly, the LCD screen displays:

   ```
   POWER DOWN?
   [Y]ES [N]O
   ```

6. Use the arrow buttons to toggle the cursor between [Y]ES and [N]O. Select [Y]ES.
7. Press the E button. The server appliance shuts down the services currently running and powers down.

Server not responding

Caution: Powering down the server appliance in the following manner is not recommended. It is the equivalent of unplugging the server from the power supply.

If you cannot use the arrow buttons to choose options on the LCD screen, you can force the server appliance to power down.

Press and hold the “C” logo badge for approximately five to ten seconds. After this interval, the server appliance shuts down.

Panel

This feature allows you to lock the LCD panel with a “password” consisting of a sequence of arrow buttons. When the LCD panel is locked, you must enter the correct sequence to access the functions on the LCD panel. This prevents unauthorized tampering with the server if people have physical access to it.

The default sequence to lock the LCD panel is blank.

Note: When you unlock the LCD panel to use the LCD functions, the lock on the LCD panel remains in place. To remove the lock, choose the “Unlock” option through the LCD panel. See “Unlock panel” on page 196.

Set sequence

Caution: Do NOT forget the sequence of arrow buttons that you enter. If you forget the sequence, you cannot override the lock on the LCD panel through the Server Desktop UI.

Instead, you have to telnet in to the server and remove a file. **Only advanced users should perform this operation.** You can adversely affect the operation of your server appliance if you modify system configuration files.

For more information, see “Removing a lock from the LCD panel” on page 229.

To change the default sequence of arrow buttons:

1. On the LCD console, hold down the Ⓢ button for approximately 2 seconds.

   The LCD screen displays:

   ```
   SELECT:
       SETUP NETWORK
   ```

2. Press the Ⓢ button until **PANEL** appears in the LCD screen:

   ```
   SELECT:
       PANEL
   ```

3. Press the Ⓔ button.

   The LCD screen displays:

   ```
   SELECT:
       LOCK PANEL
   ```

4. Press the Ⓢ button until **SET SEQUENCE** appears in the LCD screen:

   ```
   SELECT:
       SET SEQUENCE
   ```

5. Press the Ⓔ button.

   The LCD displays

   ```
   Enter Sequence:
   ```

6. Enter the sequence of arrow buttons and press the E button.

   The LCD screen asks you to confirm the sequence:

   ```
   Sequence Again:
   ```

7. Enter the sequence again and press the E button.

   If you entered the sequence incorrectly, the LCD screen flashes the following message and then returns to the normal LCD display of host name and IP address. The sequence is not changed.

   ```
   ERROR: Sequences
       do not match
   ```

   If you entered the sequence correctly, the LCD screen displays the following message for a few seconds and then returns to the normal LCD display of host name and IP address:

   ```
   ** Sequence set **
       successfully
   ```

Lock panel

If the LCD panel is currently unlocked, you can lock it. To lock the LCD panel on the server appliance:

1. On the LCD console, hold down the S button for approximately 2 seconds.

   The LCD screen displays:

   ```
   SELECT:
       SETUP NETWORK
   ```

2. Press the S button.

   ```
   SELECT:
       PANEL
   ```

3. Press the E button.

   The LCD screen displays:

   ```
   SELECT:
       LOCK PANEL
   ```

4. Press the E button.

   The LCD screen displays:

   ```
   Enter Sequence:
   ```

5. Enter the sequence of arrow buttons. An asterisk appears for each arrow button you press.
6. Press the E button.

   If you entered the sequence incorrectly, the LCD screen flashes the following message and then returns to the normal LCD display of host name and IP address:

   ```
   ERROR: Incorrect
       sequence
   ```

   If you entered the sequence correctly, the LCD screen displays the following message for a few seconds and then returns to the normal LCD display of host name and IP address:

   ```
   ** Panel is now **
       locked
   ```

Unlock panel

If the LCD panel is currently locked, you can unlock it. To unlock the LCD panel on the server appliance:

1. On the LCD console, hold down the S button for approximately 2 seconds.

   The LCD screen displays:

   ```
   Enter Sequence:
   ```

2. Enter the sequence of arrow buttons. An asterisk appears for each arrow button you press.
3. Press the E button.

   If you entered the sequence incorrectly, the LCD screen flashes the following message and then returns to the normal LCD display of host name and IP address:

   ```
   ERROR: Incorrect
       sequence
   ```

   If you entered the sequence correctly, the LCD screen displays:

   ```
   SELECT:
       SETUP NETWORK
   ```

4. Press the S button until **PANEL** appears in the LCD screen:

   ```
   SELECT:
       PANEL
   ```

5. Press the E button.

   The LCD screen displays:

   ```
   SELECT:
      UNLOCK PANEL
   ```

6. Press the E button.

   The LCD screen displays:

   ```
   ** Panel is now **
      unlocked
   ```

   The LCD screen returns to the normal display of host name and IP address.

After power loss

This feature allows you to tell the server appliance what to do once the power has been restored after a power outage. You can configure the server appliance to power up automatically or to remain in a powered-down state.

To enable the automatic power-up feature:

1. On the LCD console, hold down the S button for approximately 2 seconds.

   The LCD screen displays:

   ```
   SELECT:
      SETUP NETWORK
   ```

2. Press the S button until **AFTER POWER LOSS** appears in the LCD screen:

   ```
   SELECT:
      AFTER POWER LOSS
   ```

3. Press the E button.

   The LCD screen displays:

   ```
   AUTO POWER UP?:
      [Y]ES [N]O
   ```

4. Use the arrow buttons to toggle the cursor between [Y] and [N]. Select [Y] to reboot the system.

5. Press the E button.

   The LCD screen returns to the normal display of host name and IP address.

Reset password

If you simply want to change the Server Administrator password for the server appliance, you can do so through the Server Desktop UI. For more information, see “Changing the Server Administrator password” on page 124.

If you forget the Server Administrator password for the server appliance, you can reset the password. This is done in two steps:

a. Clear the password through the LCD console.

b. Enter a new password for the *admin* account through the Server Desktop UI.

Note: When the Server Administrator password for the server appliance is cleared, you cannot access the root account until a new password has been assigned.

Clearing the password through the LCD console

To clear the Server Administrator password for the server appliance:

1. On the LCD console, hold down the (S) button for approximately 2 seconds.

   The LCD screen displays:

   ```
   SELECT:
       SETUP NETWORK
   ```

2. Press the (S) button until **RESET PASSWORD** appears in the LCD screen:

   ```
   SELECT:
       RESET PASSWORD
   ```

3. Press the (E) button. The LCD screen displays:

   ```
       RESET PASSWORD?
       [Y]ES [N]O
   ```

4. Use the arrow buttons to toggle the cursor between [Y]ES and [N]O.
5. If you choose [N]O, the LCD screen returns to the host name and IP address.
6. If you choose [Y]ES, the LCD screen displays.

   ```
   Resetting admin
   password...
   ```

   The LCD screen then displays the host name and IP address again.

Caution: This function resets the Server Administrator password for the server appliance to blank.

After you clear the password, enter a new one as soon as possible to protect the security of the server appliance. At this point, anyone on the network can assign the Server Administrator password until you assign a new one.

Assigning a new password through the Server Desktop UI

You now need to assign a password to the *admin* account.

1. In your Web browser, enter the URL http://<IP address>/admin/ or http://<host name>/admin/ to access the Server Desktop UI.
2. If a prompt appears asking for a user name or password, enter *admin* as the user name. DO NOT enter a password.

   Click **OK**.
3. On the Server Desktop UI, select **Personal Profile > Account**. The “Administrator Settings” table appears.
4. Enter the password twice to ensure that you have entered it as intended. The Sun Cobalt RaQ XTR server appliance supports long passwords through the UI.

   For guidelines on choosing a password, see “Password guidelines” on page 26.
5. Click **Save Changes**.

Product Specifications

Hardware

The Sun Cobalt™ RaQ™ XTR server appliance has the following hardware components:

- x86-compatible processor
- Four memory slots supporting up to 2 GB SDRAM using 32 MB to 512 MB SDRAM DIMM modules (modules must be 168 pin, 3.3V, registered, ECC PC133)
- Up to four removable 7200 rpm Ultra ATA/100 hard disk drives
- Two 10/100 BaseT ethernet network interfaces
- Dual serial console interfaces
- LCD console for easy set-up and administration
- 64-bit PCI slot for expansion (PCI standard short card form factor, 6.875-inch length)
- Support for uninterruptible power supply (UPS)
- Universal serial bus

Software

The Sun Cobalt RaQ XTR server appliance has the following software features:

General features

- Linux 2.2 multitasking operating system
- Apache 1.3.12 Web server, HTTP/1.1 compliant
- Virtual hosting services: name-based and IP-based

- Common gateway interface (CGI) support
- Support for Sun Chili!Soft Active Server Pages (ASP) software
- PHP 4 support
- Support for Server Side Includes (SSI)
- Perl scripting
- Email protocol support: Simple Mail Transfer Protocol (SMTP), Internet Message Access Protocol (IMAP4), Post Office Protocol (POP3), Authentication Post Office Protocol (APOP)
- File transfer protocol (FTP), anonymous FTP access
- Telnet access
- Domain Name System (DNS) server
- 128-bit Secure Sockets Layer (SSL)
- FrontPage 2000 server extensions
- NTP client support
- Sun Cobalt Bandwidth Management software
- Support for Java™ runtime environment version 1.3 and JDK™ software from Sun Microsystems, Inc.
- Code development environment
- Legato NetWorker client, Knox Arkeia and Veritas NetBackup support
- Security: PAM/shadowed passwords

System management

- SSL support for secure administration
- Simple Network Management Protocol (SNMP) management support
- Browser-based Setup Wizard
- Browser-based server management and individual virtual site management interfaces
- Online ActiveAssist real-time help
- Active Monitor maintenance agents

- Advanced management using telnet
- Web-based performance and usage reporting
- Browser-based backup and restore utility
- Browser-based software upgrade (BlueLinQ)

Partner solutions

- E-commerce
- Database
- Backup
- Analysis and usage statistics

Physical data

The Sun Cobalt RaQ XTR server appliance has the following physical characteristics:

- Dimensions: 17.50 in. x 22.75 in. x 1.75 in (44.5 cm x 57.8 cm x 4.5 cm; fits in a standard single-unit, 19-inch equipment rack)
  - One chassis (not including any drives or sleds): 20 lbs (9 kg)

> ***Note:*** The server appliance ships with empty drive sleds in the bays where there are no hard disk drives installed.

  - One hard disk drive and drive sled: 2 lbs (0.9 kg)
  - Four-drive configuration: 28.0 lbs (12.7 kg)
  - Three-drive configuration: 26.5 lbs (12.0 kg)
  - Two-drive configuration: 25.0 lbs (11.3 kg)
  - One-drive configuration: 23.5 lbs (10.7 kg)
- Power requirements: Input rating 100-240 V, 50/60 Hz
- Power consumption: 100 watts (typical), 130 watts (max)

- Power requirement for the PCI slot:
  - 5V @ 1A
  - +12V @ 0.5A
  - -12V @ 0.1A
- Operating environment:
  - 32^{o}F to 95^{o}F (0^{o}C to 35^{o}C)
  - 10% to 90% humidity (non-condensing)
- Non-operating environment:
  - 14^{o}F to 122^{o}F (-10^{o}C to 50^{o}C)
  - 5% to 93% humidity (non-condensing)
- Light-emitting diodes (LEDs): Power, Transmit/Receive (2), Link (2), Disk Activity (4), Web Activity

Regulatory approvals

- FCC-A
- VCCI-A
- TUV (United States and Canada)
- CE (on European models only)
- Austel

Upgrading the Sun Cobalt™ RaQ™ XTR server appliance

Your Sun Cobalt™ RaQ™ XTR server appliance can be serviced or upgraded in the field in the following areas:

- add a memory module (DIMM)
- add a PCI expansion card
- replace the hard disk drives
- replace the fans

The hard disk drives can be removed and replaced while the server appliance is in an equipment rack. If you wish to add memory or an expansion card, or replace a fan, you must remove the server appliance from the equipment rack in order to gain access to the interior components. The following sections provide step-by-step upgrade and replacement instructions.

Installing or removing a hard disk drive

The Sun Cobalt RaQ XTR server appliance can contain up to four hard disk drives. The drives are mounted on drive “sleds” that allow them to be easily removed and installed.

Before you replace or add a disk drive to the server appliance, read all of the following Notes and Warnings .

Warning: Do not swap hard disk drives from one Sun Cobalt RaQ XTR server appliance to another. Also, do not install a drive, that was previously partitioned for RAID, in a Sun Cobalt RaQ XTR server appliance as an additional (non-RAIDed) drive.

Note: If possible, replace a defective drive with another drive of the same model. If the original model of drive is not available, ensure that the replacement drive has a storage capacity that is equal to or greater than that of the drive being replaced.

Check the specifications of the replacement drive to verify that the usable memory (not the rated capacity) is equivalent to the capacity of the drive being replaced.

If you have to replace a hard disk drive, please notify Technical Support and arrange to return the drive. See the “Customer Service and Technical Support” on page 275” section for contact information.

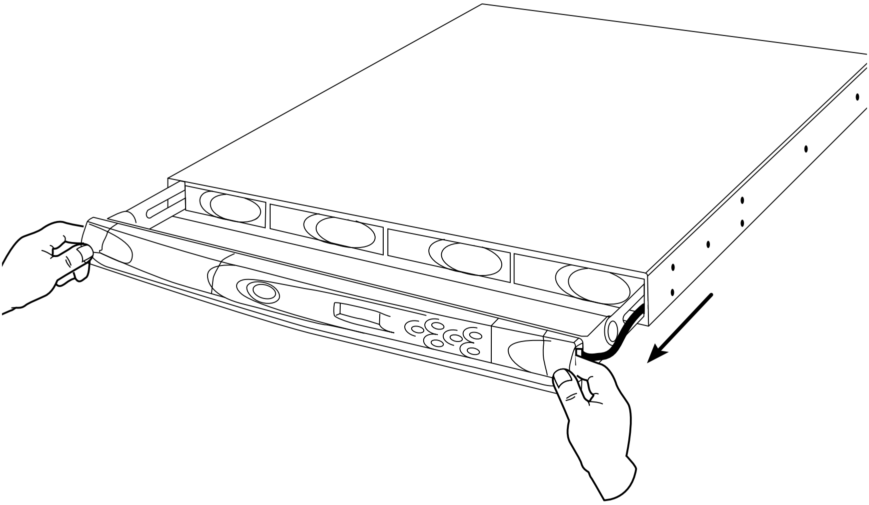
If you add a drive (rather than replace an existing one), the new drive can be utilized by the server appliance, but cannot be incorporated into the system’s RAID.

Drives can be replaced or added to the server appliance while it is powered up, but a new drive that was added as additional storage will not be seen by the system until you reboot the server.

Remove and replace a hard disk drive as follows:

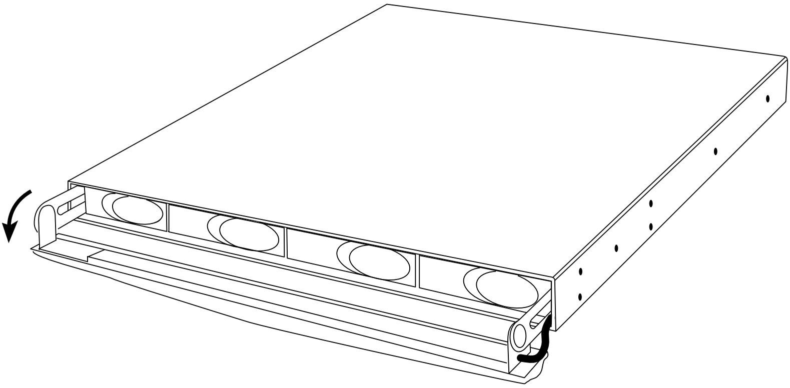
1. Grasp the front panel by inserting a finger in the indentation at each end, and gently pull the front panel towards you (see Figure 92).

Figure 92. WIthdrawing the front panel



2. When the front panel reaches the end of its travel, rotate it up or down 90 degrees (see Figure 93).

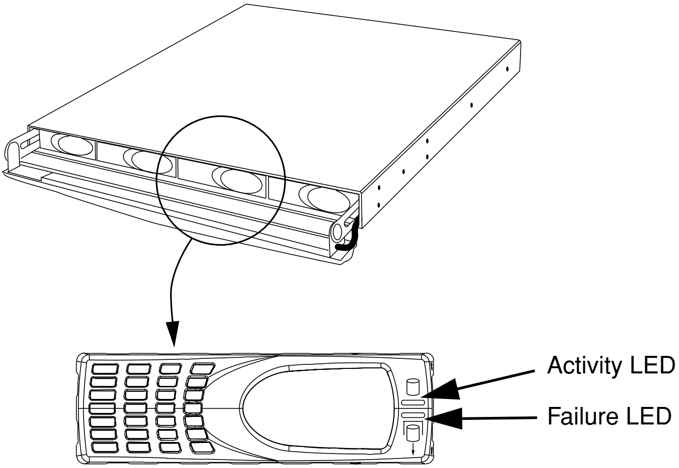
Figure 93. Rotating the front panel



3. Insert your index finger into the front plate of the drive sled and verify that the Failure LED lights, or remains lit if it was already on (see Figure 94).

Warning: If the Failure LED does not light, or goes out when you insert your finger in the front plate, **DO NOT** remove the drive. Wait a few seconds for the drive to complete the operation in progress, and check the LED again.

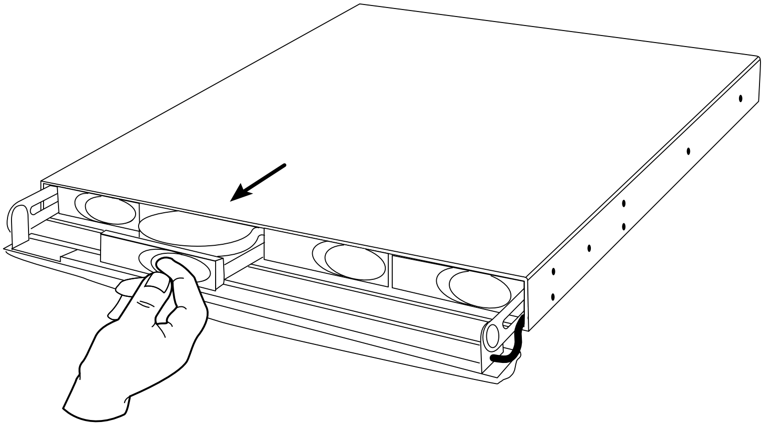
Figure 94. Disk Drive Failure LED



4. Pull the sled out of the Sun Cobalt RaQ XTR server appliance chassis (see Figure 95).

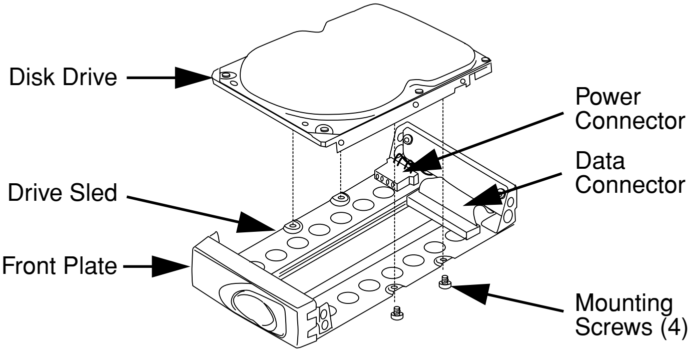
Caution: When you are removing a drive sled from the server appliance, it will seem to suddenly "pop" loose. Be careful not to pull the sled from the chassis too quickly and allow it to fall.

Figure 95. Withdrawing a drive sled



5. Remove the four mounting screws from the bottom of the drive sled (see Figure 96).

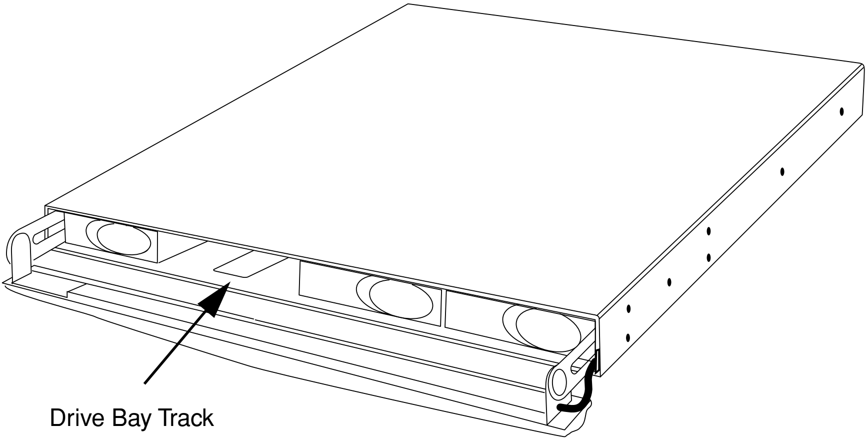
Figure 96. Drive sled and disk drive



6. Lift the disk drive slightly away from the drive sled and gently unfasten the power and data connectors from the rear of the drive.
7. Attach the data and power connectors, at the rear of the drive sled, to the corresponding connectors on the new disk drive.
8. Position the drive on the sled so that the four holes in the sled's bottom line up with the threaded holes in the bottom of the disk drive.
9. Re-insert the mounting screws and fasten the drive to the sled.

10. Re-insert the drive sled into the disk drive bay. Ensure that the track, on the bottom of the drive sled, is correctly aligned with the track in the drive bay (see Figure 97).

Figure 97. Re-inserting a drive sled



11. Push the drive sled into the bay until you feel it "snap" into place.
12. Rotate the front panel back to its original position.
13. Slide the front panel back into the chassis. Ensure that the cable, at the right side of the front panel, enters the chassis without being pinched or kinked.

Installing additional memory

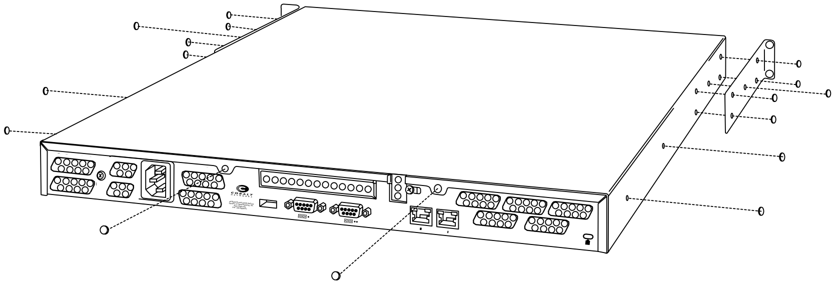
Caution: The chassis contains electrostatic-sensitive components. Observe proper ESD precautions whenever the Sun Cobalt RaQ XTR server appliance's cover is removed.

Note: Before attempting to install additional memory, ensure that the DIMM to be installed is less than 0.158 inches (4.0 mm) thick. Contact Cobalt Technical Support to receive a listing of approved memory vendors and the appropriate part numbers.

Note: You must fill the slots for the memory modules starting from the outside edge of the board and moving inward.

1. Power down and remove the server appliance from the equipment rack by reversing the installation procedure in Chapter 2.
2. Place the server appliance on a stable, flat surface.
3. Remove the mounting brackets from each side of the chassis. Each bracket is attached to the chassis with four screws (see Figure 98).

Figure 98. Mounting brackets and cover fasteners



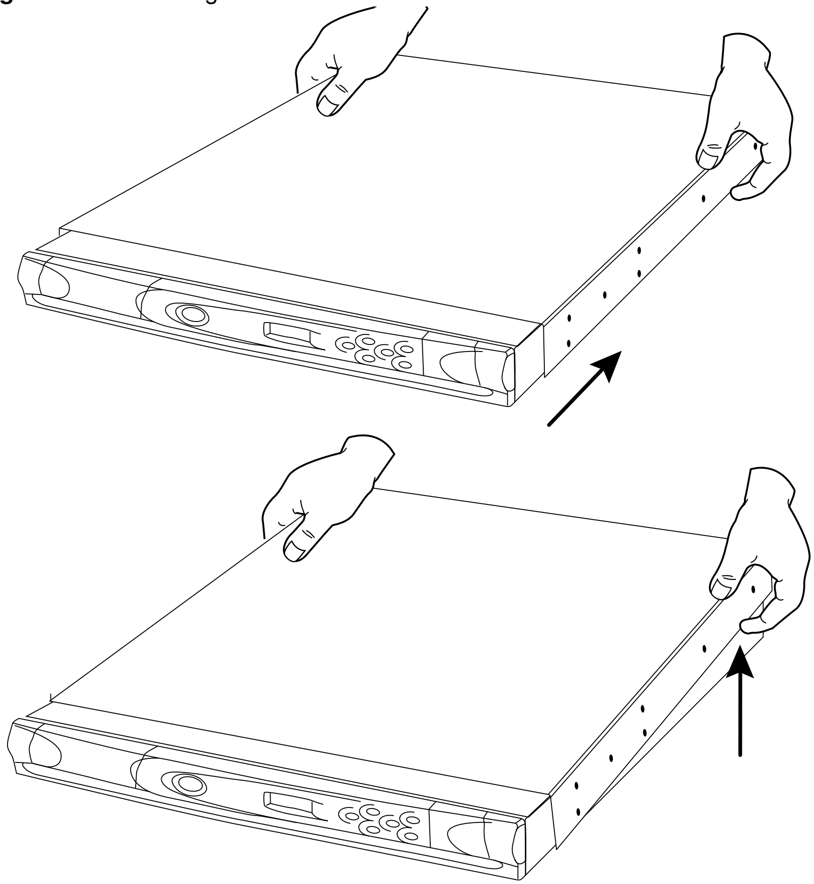
4. Unfasten the eight screws that attach the cover to the server appliance chassis (three screws on each side and two screws at the rear of the chassis).

Note: Ensure that the front panel is completely slid back into the chassis before attempting to remove the cover.

5. Working from the rear of the chassis, slide the cover back approximately three inches (see Figure 99).

6. Lift up the rear of the cover first and then remove the cover from the chassis.

Figure 99. Removing the cover



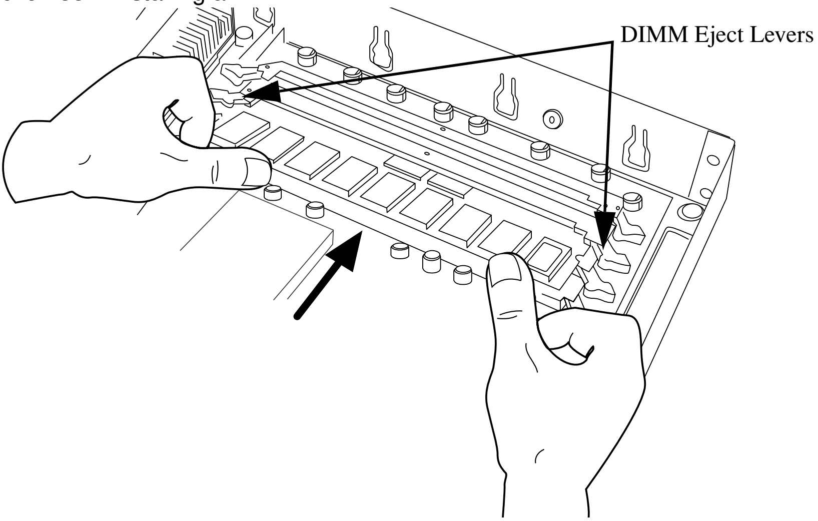
7. Locate the DIMM sockets at the right, rear corner of the chassis.

8. Ensure that the eject lever, at each end of the DIMM socket, is released (see Figure 100).

Caution: Observe proper ESD precautions and follow the manufacturer’s instructions when handling the DIMM.

9. Insert the DIMM in the target socket and use your thumbs to seat it. Note that the DIMM’s edge connector is keyed and can only be inserted one way. When the DIMM is completely seated in the socket, each eject lever will be seated in the cutout in each end of the DIMM.

Figure 100. Installing a DIMM



10. Re-install the cover and mounting brackets, and return the server appliance to the equipment rack.

Installing a PCI expansion card

Note: The PCI expansion slot accommodates the PCI standard short-card form factor. The PCI card must be less than 6.875 inches (174.63 mm) long.

The PCI slot provides the following voltages:

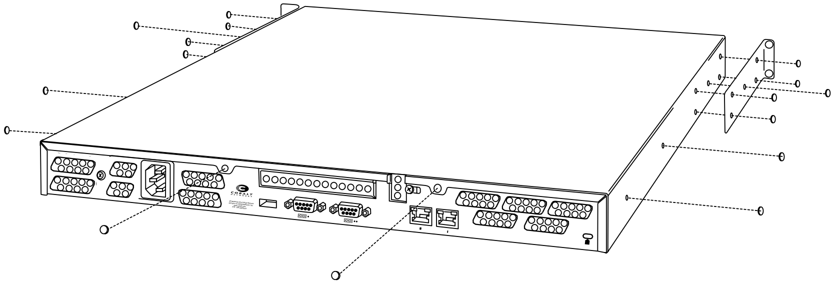
- +5V @ 1A
- +12V @ 0.5A
- -12V @ 0.1A

Ensure that the card that you are installing is compatible with the power budget of the PCI slot.

Caution: The chassis contains electrostatic-sensitive components. Observe proper ESD precautions whenever the server appliance's cover is removed.

1. Power down and remove the server appliance from the equipment rack by reversing the installation procedure in Chapter 2.
2. Place the server appliance on a stable, flat surface.
3. Remove the mounting brackets from each side of the chassis. Each bracket is attached to the chassis with four screws (see Figure 101).

Figure 101. Mounting brackets and cover fasteners



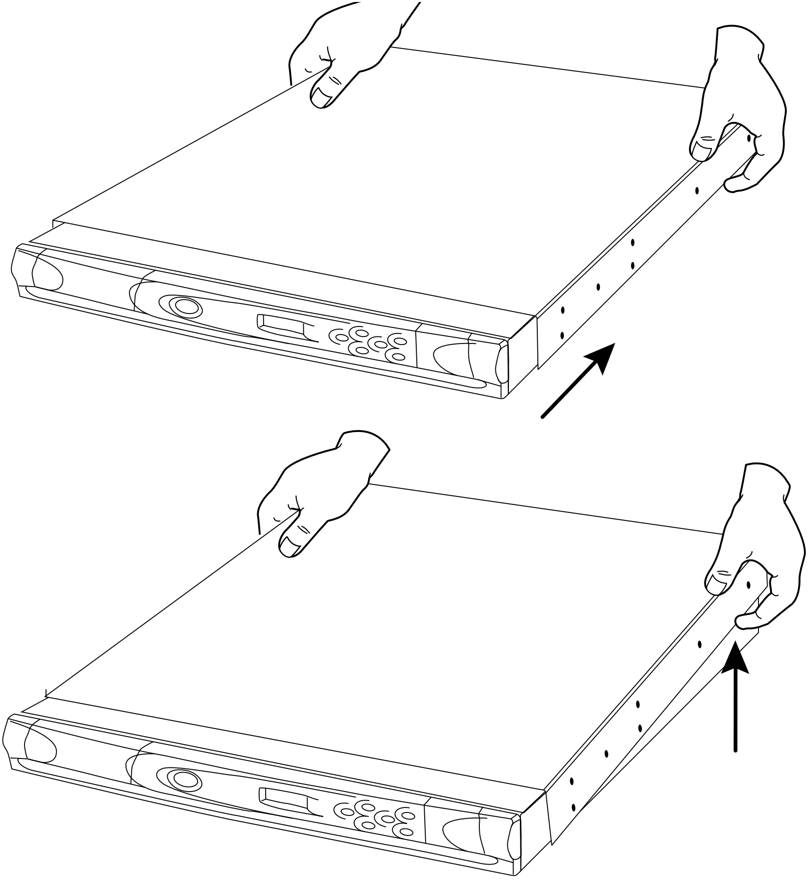
4. Unfasten the eight screws that attach the cover to the server appliance chassis (three screws on each side and two screws at the rear of the chassis).

Note: Ensure that the front panel is completely slid back into the chassis before attempting to remove the cover.

5. Working from the rear of the chassis, slide the cover back approximately three inches (see Figure 102).

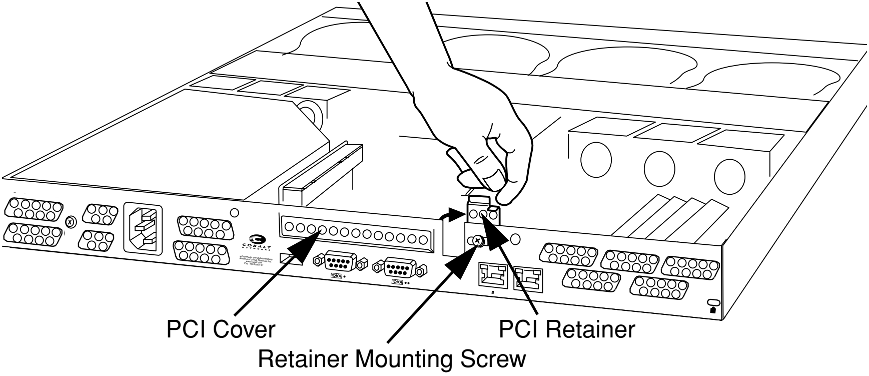
6. Lift up the rear of the cover first and then remove the cover from the chassis.

Figure 102. Removing the cover



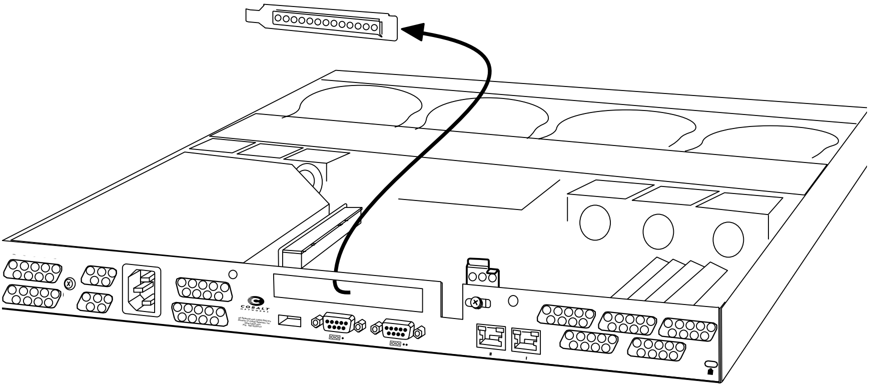
7. Working from the rear of the chassis, loosen the screw holding the PCI Retainer and rotate the retainer clockwise to release the PCI Cover (see Figure 103).

Figure 103. Releasing the PCI cover



8. Carefully withdraw the PCI Cover out through the interior of the chassis (see Figure 104). Do not allow the cover to fall onto the motherboard.

Figure 104. Removing the PCI cover

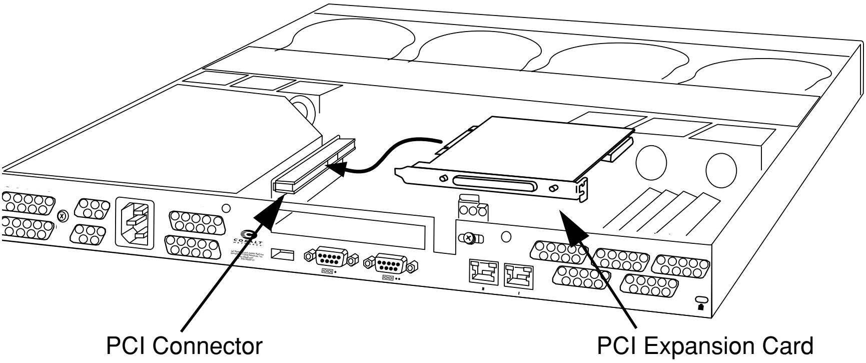


9. Unpack the PCI expansion card and remove any protective connector covers.

Caution: Observe proper ESD precautions and follow the manufacturer's instructions when handling the card.

10. Insert the expansion card's edge connector into the PCI connector on the system card (see Figure 105).

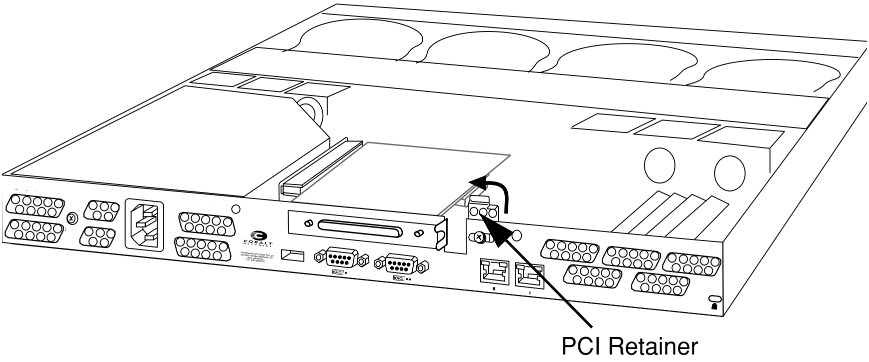
Figure 105. Installing the PCI expansion card



11. Rotate the PCI Retainer counterclockwise so that it captures the expansion card's mounting bracket (see Figure 106).

12. Verify that the top edge of the PCI Retainer is flush with the top edge of the rear panel of the chassis, then tighten the PCI Retainer's mounting screw.

Figure 106. Replacing the PCI retainer



13. Follow the manufacturer's instructions for the PCI card regarding any additional cabling or configuration.

14. Re-install the cover and mounting brackets, and return the Sun Cobalt RaQ XTR server appliance to the equipment rack.

Replacing a fan

⚠ ***Caution:*** The chassis contains electrostatic-sensitive components. Observe proper ESD precautions whenever the Sun Cobalt RaQ XTR server appliance's cover is removed.

✍ ***Note:*** Before replacing a fan, contact Technical Support to receive a listing of approved vendors and the appropriate part numbers.

All six fans are mounted to a common frame, which must be removed from the chassis before an individual fan is replaced. The fans are arranged in two banks of three fans each. The three fans comprising a bank are mounted in a plastic fan holder, which is attached to the frame with four plastic tabs.

The faulty fan is identified on the **Active Monitor > Fan Monitor** screen. Note that only a Server Administrator or Site Administrator can access this screen.

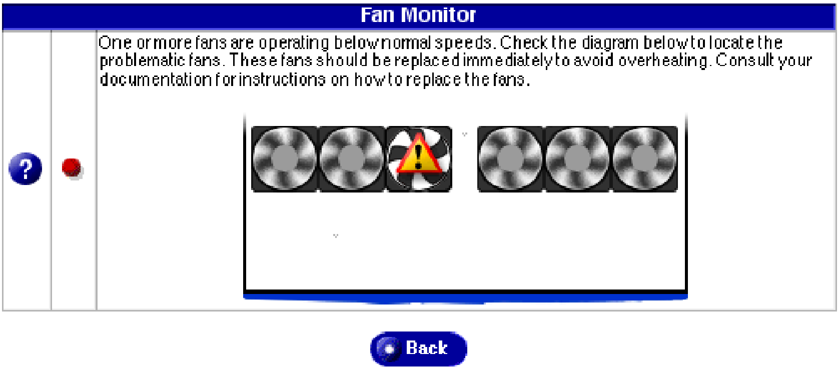
Replace a fan as follows:

1. Login as the Server Administrator or Site Administrator and select the **Active Monitor** menu item

2. When the "System Components and Services" table is displayed, go to the **Fans** entry and click on the green *magnifying-glass* icon. The "Fan Monitor" screen is displayed (see Figure 107). In this example, the third fan from the left is not functioning properly and has a warning symbol to indicate that this is the defective fan.

3. Note the location of the faulty fan(s).

Figure 107. Identifying the defective fan



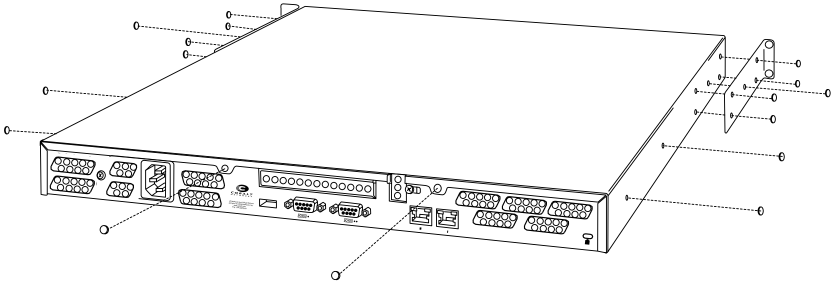
One or more fans are operating below normal speeds. Check the diagram below to locate the problematic fans. These fans should be replaced immediately to avoid overheating. Consult your documentation for instructions on how to replace the fans.

4. Power down and remove the server appliance from the equipment rack by reversing the installation procedure in Chapter 2.

5. Place the server appliance on a stable, flat surface.

6. Remove the mounting brackets from each side of the chassis. Each bracket is attached to the chassis with four screws (see Figure 108).

Figure 108. Mounting brackets and cover fasteners



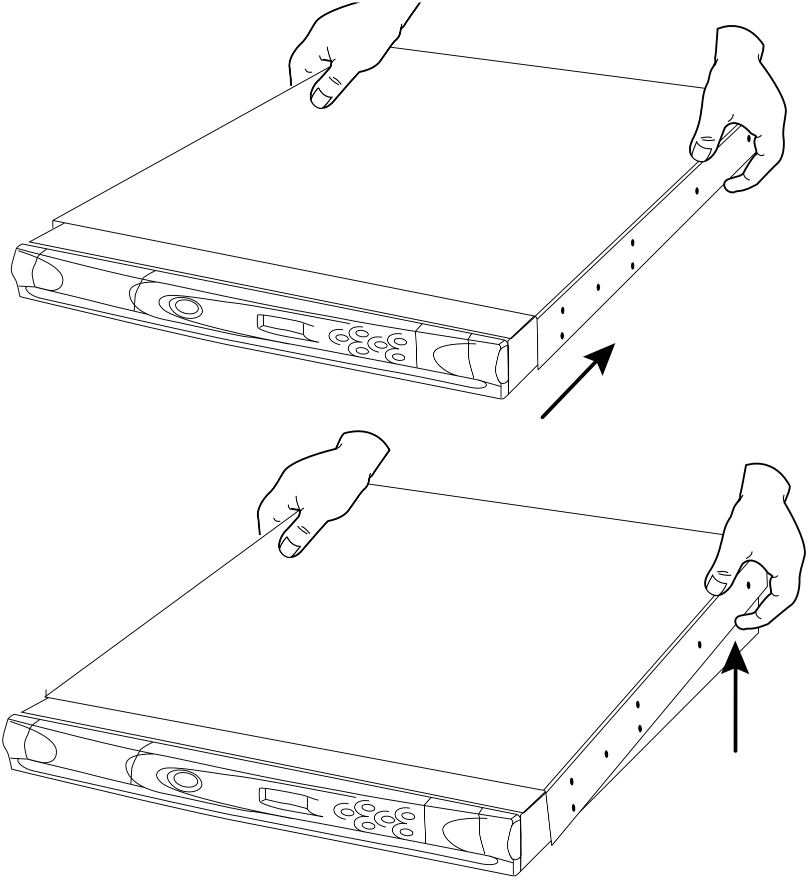
7. Unfasten the eight screws that attach the cover to the server appliance chassis (three screws on each side and two screws at the rear of the chassis).

> ***Note:*** Ensure that the front panel is completely slid back into the chassis before attempting to remove the cover.

8. Working from the rear of the chassis, slide the cover back approximately three inches (see Figure 109).

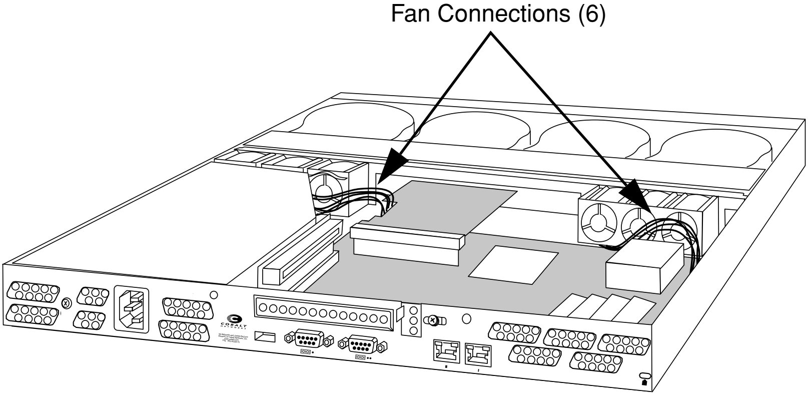
9. Lift up the rear of the cover first and then remove the cover from the chassis.

Figure 109. Removing the cover



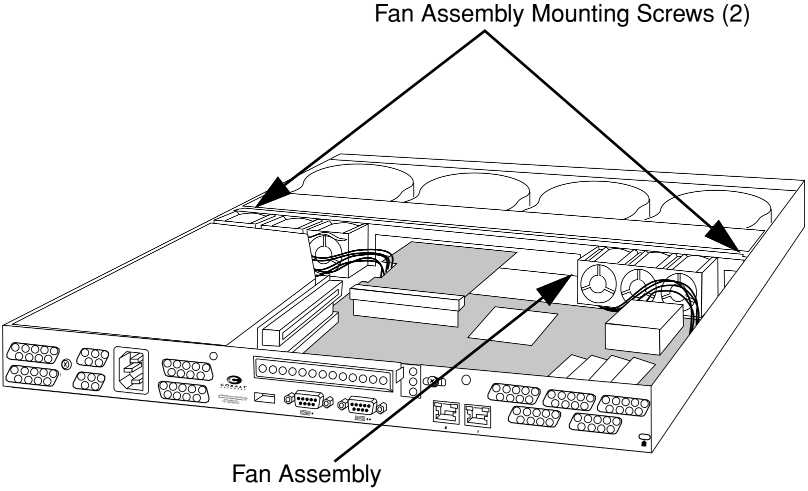
10. Working from the rear of the chassis, remove the six fan connectors from the motherboard (see Figure 110).

Figure 110. Disconnecting the fans



11. Unfasten the two screws securing the fan assembly (see Figure 111).

Figure 111. Removing the fan assembly

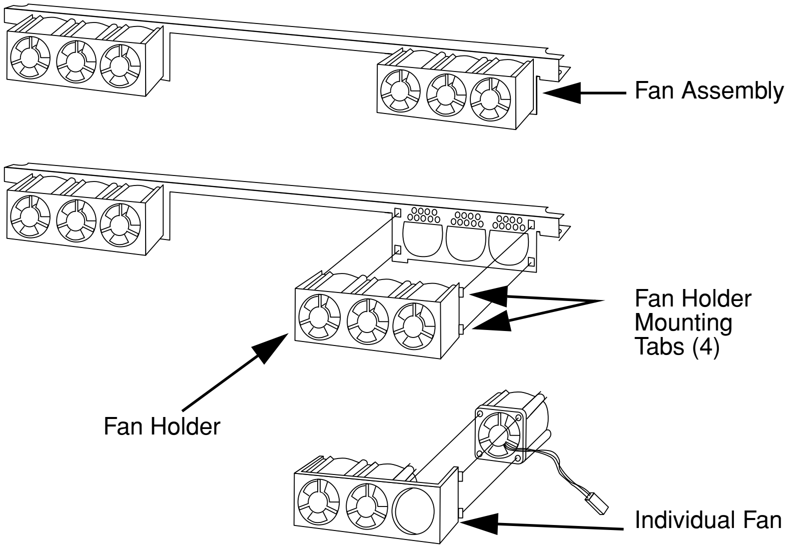


12. Gently tip the upper edge of the fan assembly away from you (towards the front of the chassis). Then withdraw the assembly from the chassis.

13. Lay the fan assembly on a flat surface with the fans facing downwards. Note the four plastic release tabs that secure the fans to the fan holder.

14. Release the fan holder’s tabs from the frame and withdraw the fan holder (see Figure 112).

Figure 112. Removing the fan assembly

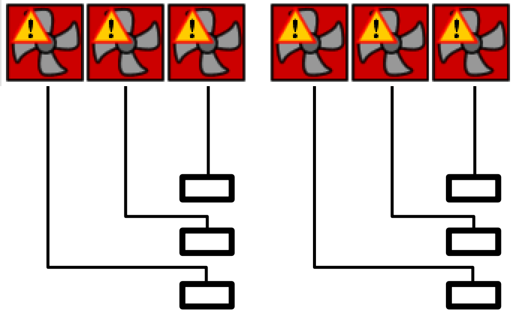


15. Note the orientation of the defective fan and how its wires are routed. Remove the defective fan and replace it with an equivalent model. Ensure that the replacement fan is installed with the same orientation as the original. Check the fan wiring for areas that are pinched or kinked.

16. Re-install the fan holder to the frame and the fan assembly to the chassis by reversing the preceding steps. Refer to Figure 113 for the correct fan wiring.

17. Re-install the cover and mounting brackets, and return the server appliance to the equipment rack.

Figure 113. Rewiring the fans



Advanced Information

⚠ ***Caution:*** The features described in this appendix are intended for advanced users who want to run shell scripts or use shell commands. An advanced user is someone who is proficient in the internal workings of the Unix operating system.

You can seriously adversely affect the operation of your Sun Cobalt™ RaQ™ XTR server appliance if you modify system configuration files. Check your warranty card for details.

⚠ ***Caution:*** Direct root logins are not allowed on the Sun Cobalt RaQ XTR server appliance. To obtain a root shell, telnet to the server and log in as the user *admin* or *alteradmin*. From the command prompt, type **su -** and press **Enter**. Enter the administrator's password at the password prompt. Only the Server Administrator or the alternate administrator can **su -** to root.

Removing the Server Desktop UI

You can alter the Sun Cobalt™ RaQ™ XTR server appliance server so that the Server Desktop user interface (UI) does not run.

⚠ ***Caution:*** You can seriously affect your server appliance if you modify the system configuration files. Only advanced users of Linux should perform this operation.

See your warranty card for more details.

☞ ***Important:*** **Turning off the Server Desktop UI is a permanent action.** You cannot toggle the UI on and off.

If you turn off the Server Desktop UI and then want to re-enable it, you will have to rebuild the server appliance with an OS restore CD; this returns the server to a factory-fresh state.

To turn off the Server Desktop UI:

1. Telnet in to the server appliance and log in as the user *admin* or *alteradmin*.
2. From the command prompt, enter:

   ```
   su -
   ```

   Note: Only the Server Administrator or the alternate administrator can **su -** to root.

3. Press **Enter**. A password prompt appears.
4. Enter the administrator password. A command-line interface appears.
5. Enter the command:

   ```
   /usr/local/sbin/Cobalt_Linux_unmanaged_conversion.sh
   ```

6. The system prompts you with a long warning that explains what will be changed in the files. **Read the entire message.**
7. If you do not want to proceed, enter `NO`.

   If you want to proceed, enter `YES`.

8. Enter `exit` to end your session as root.
9. Now reboot the server appliance server.

Enabling Interbase 6.0

The Sun Cobalt RaQ XTR server appliance is pre-loaded with InterBase 6.0, an open-source, cross-platform SQL database from Inprise Corporation. InterBase is not enabled by default.

For more information on InterBase, go to http://www.interbase.com.

InterBase offers free development and distribution rights. Interbase offers developers a sophisticated database with a small footprint, low maintenance cost and high reliability.

InterBase offers a number of database features—triggers, stored procedures, blobs, event alerters, user-defined functions, multi-dimensional arrays, two-phase commit, referential integrity, constraints and a flexible set of transaction options.

To enable the InterBase 6.0 database server:

Caution: You can seriously affect your Sun Cobalt RaQ XTR server appliance if you modify the system configuration files. Only advanced users of Linux should undertake these changes.

See your warranty card for more details.

1. Telnet in to the server appliance server and log in as the user *admin* or *alteradmin*.
2. From the command prompt, enter:

   ```
   su -
   ```

Note: Only the Server Administrator or the alternate administrator can **su -** to root.

3. Press **Enter**. A password prompt appears.
4. Enter the administrator password. A command-line interface appears.
5. Open an editor and edit the file:

   ```
   /etc/inetd.conf
   ```

6. Locate the line with `gds_db` service. This line is commented out with a # symbol.
7. Remove the # symbol. This enables inetd.conf to launch the InterBase 6.0 database server when requests are made to its port.
8. Save the file and exit the editor.
9. Enter the command

   ```
   killall -HUP inetd
   ```

   This causes the inetd server to re-read its configuration file and activate the InterBase 6.0 database server.
10. Enter `exit` to end your session as root.

Serial console port

You can connect a console terminal to the DB-9 connector on the back panel of the Sun Cobalt RaQ XTR server appliance. The terminal can be either an ASCII terminal or a PC running terminal software. The console terminal should have the following communications parameters—115 200 baud, 8 data bits, no parity and one stop bit.

Initializing the server appliance through the serial console port

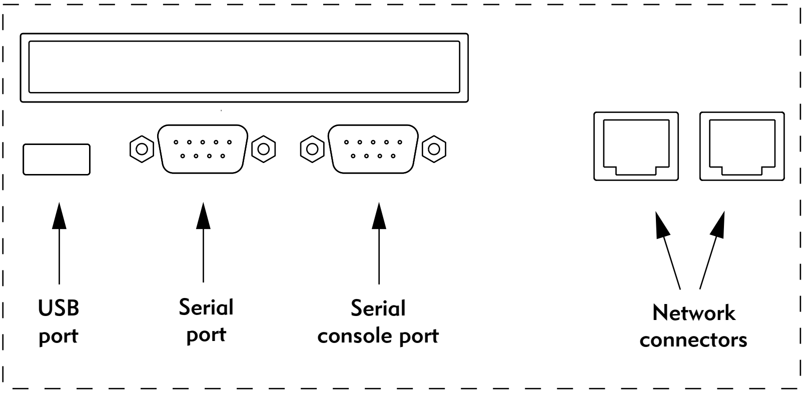
Instead of assigning the initial network settings for the server appliance server through the LCD console, you can connect the server to a terminal and assign the network settings through the serial console port.

This feature allows the assignment of network parameters only (IP address, netmask, gateway).

Note: You can use the initialize the server appliance through the serial console port only once, much like proceeding through the browser-based Setup Wizard.

To initialize the Sun Cobalt RaQ XTR server appliance through the serial console port:

1. Connect a null modem serial cable to the serial console port on the back panel of the server appliance. See the following figure.



2. Configure your terminal software to the following parameters:
   - 115 200 Baud
   - 8 data bits
   - no parity
   - 1 stop bit
3. Power on the server appliance with the power switch on the back panel. A number of boot messages are displayed on your terminal screen.
4. The first prompt asks for an IP address. Enter the Primary IP address for the server appliance (for example, 10.9.19.55).
5. The second prompt asks for the netmask address. Enter the Primary Netmask for the server appliance (for example, 255.0.0.0).
6. The third prompt asks for the gateway address. Enter the gateway for the server appliance (for example, 10.9.25.254).
7. Confirm the settings that you have entered:
   - Primary IP address: 10.9.19.55
   - Primary Netmask: 255.0.0.0
   - Gateway: 10.9.25.254

8. Another prompt is displayed: `[S]AVE / [C]ANCEL`. Enter “S” to save the configuration. The message `Verifying and saving...` appears.
9. Once the configuration is saved, the terminal screen displays the normal boot status messages. Continue administration of the server appliance through your Web browser.

Powering down the server appliance remotely

Caution: This feature requires you to access the server appliance through a telnet session. Only advanced users of Linux should undertake these changes.

Note: Direct root logins are not allowed on the Sun Cobalt RaQ XTR server appliance.

Note: You cannot power up a Sun Cobalt RaQ XTR server appliance remotely. Someone must physically power up the server.

You can power down the server appliance remotely through a telnet session. To obtain a root shell:

1. Telnet in to the server and log in as the user *admin* or *alteradmin*.
2. From the command prompt, enter:

   ```
   su -
   ```

   Note: Only the Server Administrator or the alternate administrator can **su -** to root.

3. Press **Enter**. A password prompt appears.
4. Enter the administrator password. A command-line interface appears.
5. Enter the command:

   ```
   shutdown -h now
   ```

   The system proceeds through its shutdown sequence and powers down.

Removing a lock from the LCD panel

Caution: This feature requires you to access the Sun Cobalt RaQ XTR server appliance through a telnet session. You can seriously affect your Sun Cobalt RaQ XTR server appliance if you modify the system configuration files. Only advanced users of Linux should undertake these changes.

See your warranty card for more details.

Caution: If you have forgotten both the Server Administrator password and the sequence of arrow keys, you will not be able to access the server.

Note: Direct root logins are not allowed on the Sun Cobalt RaQ XTR server appliance.

If you have forgotten the sequence of arrow keys to unlock the LCD panel, you can remove the “lock” file from the server:

1. Telnet to the server and log in as the user *admin* or *alteradmin*.
2. From the command prompt, enter:

   ```
   su -
   ```

   Note: Only the Server Administrator or the alternate administrator can **su -** to root.

3. Press **Enter**. A password prompt appears.
4. Enter the administrator’s password. A command-line interface appears.
5. Enter the command:

   ```
   rm /etc/cobalt/.LCK..cobtpanel
   ```

   You can now assign a new sequence through the LCD console. For more information, see “Set sequence” on page 194.

Development tools

The Sun Cobalt RaQ XTR server appliance provides a collection of utilities to support applications development and server administration. These tools include:

- GNU C/C++ compiler `(gcc)` and libraries
- Java Development Kit
- GNU Bourne Again Shell `(bash)`
- Text editors `(emacs, vi, pico)`
- File system utilities `(ls, mv, cp, ln, rm, chmod, chown, chgrp, du, df)`
- File parsing utilities `(sed, awk, diff)`
- File display utilities `(cat, more, less)`
- Search utilities `(find, grep, which)`
- Archive utilities `(gzip, tar, cpio, rpm)`
- Network utilities `(FTP, telnet, netstat, ping, finger, mail, pine)`
- Programming languages (`perl`, `python, tcl/tk`)

These utilities can be found in one of the following directories:

```
/sbin
/bin
/usr/sbin
/usr/bin
```

For an expanded set of development tools, visit the Solutions Directory at http://www.cobalt.com/solutions/. For more information, see “Further resources and information” on page 277.

Additionally, the Linux distribution on the Sun Cobalt RaQ XTR server appliance is based on the RedHat Linux 6.2 distribution for x86-compatible processor systems.

You can run most pre-compiled x86-based commercial software packages on the Sun Cobalt RaQ XTR server appliance, as long as the software does not require a mouse, keyboard or monitor. Ensure that the software is compatible with the Linux 2.2 kernel and the glibc library.

Configuration files

If necessary, you can change some of the configuration files for the Sun Cobalt RaQ XTR server appliance services for development purposes, but this may void your warranty. Please read your warranty card before making any changes.

> ***Caution:*** Changing any of the following configuration files can dramatically affect the operation of the services configured by means of the Sun Cobalt RaQ XTR server appliance's browser-based administration service or the administration service itself.
>
> Only advanced users of Linux should undertake these changes. See your warranty card for more details.

The services and some of their associated configuration files and directories are the following:

- Email

  ```
  /etc/inetd.conf
  /etc/mail/
  ```

- Domain Name Service (DNS)

  ```
  /etc/named/
  ```

- File transfer protocol (FTP)

  ```
  /etc/proftpd.conf
  ```

- Web

  ```
  /etc/httpd/conf/*.conf
  ```

- Mailing lists

  ```
  /usr/local/majordomo/
  ```

Directory structure

The hard disk drive on the server appliance is partitioned into four segments. Most of the available space on the disk drive is on the partition mounted from `/home`. It is recommended to do most of your work under this partition. By default, quotas are turned on in this partition and are used extensively by the system software.

Server appliance home page

The document root for the Web server is the server appliance's main site:

```
/home/sites/home/web
```

Web content in this directory is associated with the URL http://<IP address>/.

For example, a file saved as:

```
/home/sites/home/web/testdir/test.html
```

is accessed through the URL http://<IP address>/testdir/test.html

Note: <IP address> refers to the IP address or the fully qualified domain name of the server appliance.

Virtual site home page

The document root for the virtual sites' Web page content is:

```
/home/sites/<sitename>/web
```

For example, www.cobalt.com would have a document root of

```
/home/sites/www.cobalt.com/web
```

Only the Server Administrator or the Site Administrator can upload to this directory.

Web content in this directory is associated with the URL http://<sitename>/.

For example, a file saved as:

```
/home/sites/<sitename>/web/testdir/test.html
```

is accessed through the URL http://<sitename>/testdir/test.html

✍ ***Note:*** <Sitename> refers to the <hostname.domainname> of the corresponding virtual site.

Customized error Web pages

The Server Administrator or a Site Administrator can replace the default error Web pages for a virtual site on the Sun Cobalt RaQ XTR server appliance with customized error pages for four common Web server errors.

The errors the server appliance specifically handles with custom files for a virtual site are:

- **401: Authorization Failed**—This error page is displayed when you have protected a directory with an .htaccess file and the user does not authenticate correctly.
- **403: Forbidden**—This error page is displayed when you have changed the permissions of a file or directory so that the Web server cannot access it.
- **404: File Not Found**—This error page is displayed a request has been made for a file or directory that the Web server cannot find.
- **500: Internal Server Error**—This error page is usually displayed when a dynamic CGI page does not return data to the Web server correctly or cannot be executed properly.

The default error pages for these four errors are located in the Web directory for a virtual site under the error subdirectory. The full path to this directory is:

```
/home/sites/<sitename>/web/error
```

✍ ***Note:*** <Sitename> refers to the <hostname.domainname> of the corresponding virtual site.

For example, for a site named www.cobalt.com, the error pages would be located in:

```
/home/sites/www.cobalt.com/web/error
```

The filenames for each error begin with the corresponding error code mentioned above. For example, error 404 is handled by the file “404-file-not-found.html” in the error subdirectory.

Site user home page

When a user on the main site is added through the Server Desktop UI, the home directory for that site user is created in:

```
/home/sites/home/users/username/web
```

The content of their Web pages can be viewed at
http://<IP address>/users/<username>/ or http://<IP address>/~ <username>/

When a user on a virtual site is added through the Server Desktop UI, the home directory for that site user is created in:

```
/home/sites/<sitename>/users/<username>
```

The user’s default Web page is located in:

```
/home/sites/<sitename>/users/<username>/web
```

The content of their Web pages can be viewed at
http://<sitename>/~<username>/.

Domain Name System

Basic DNS

The Internet uses a distributed naming system called the Domain Name System (DNS). DNS allows us to refer to computers by host names as well as by Internet Protocol (IP) addresses.

IP addresses are hard to remember and are inconvenient to use. DNS allows us to use host names and domain names which can resolved to IP addresses. DNS servers translate host names and domain names (for example, www.cobalt.com) to an associated IP address (for example, 192.168.1.10.)

For example, Sun Microsystems, Inc. has registered the domain name “sun.com” for use by our servers “mail.sun.com”, “www.sun.com” and others. The host names “mail” and “www” represent different servers registered in the same domain.

A domain name is a computer name suffix shared by a group of computers in the same organization. A domain name should be associated with an IP address through a Forward Lookup record. Domain names are organized in a hierarchy; this hierarchy includes your company or server name, and a country code (for example, .uk or .ca) or a top-level domain (for example, .com or .edu).

A Web site on the server is created with one IP address, one host name and one domain name that together establish the identity of that Web site on the Internet.

Each domain name requires a primary domain authority on one DNS server. A secondary DNS server acts as a backup to the primary. DNS information is configurable only on the primary server, and not on the backup server.

Enabling the DNS server feature

☞ ***Important:*** Always click **Save Changes** after modifying DNS records. If you do not, the changes will not take effect.

To enable the DNS server on the Sun Cobalt™ RaQ™ XTR server appliance:

1. Select **Server Management > Control Panel**. The “Service Settings” table appears.
2. Click the check box to enable the Domain Name System (DNS) Server (if it is not already enabled).
3. Click **Save Changes**.

To set the optional DNS services, click green *pencil* icon next to the DNS service in the “Service Settings” table.

Configuring a primary DNS server

A primary DNS server maintains a list of name records and their associated IP addresses. This list is made available to other DNS servers if your domain is registered with your country-specific domain-naming organization. Your Internet service provider (ISP) can help you register your Internet server.

To configure a primary DNS server for your server appliance:

1. Select **Server Management > Control Panel**. The “Service Settings” table appears.
2. Click the check box for Domain Name System (DNS) Server to turn it on (if it is not already turned on).
3. Click **Save Changes**.
4. Click the green *pencil* icon next to the DNS service in the “Service Settings” table. The “DNS Settings for <sitename>” table appears.
5. Select Reverse Lookup (PTR) from the **Add...** pull-down menu.

6. Enter the IP address (for example, 192.168.10.10) and network mask (for example, 255.255.255.0).

   The network mask, or subnet size, is specified by an IP address in dot-quad notation. See Table 2 on page 242 to convert between dot-quad and network mask bit-count notations.

7. Enter the host name and domain name you want to serve (for example, www and mydomain.com).
8. You can enable the check box Generate Forward Address (A) Record for this IP address and host name pair so that the IP address/host name pair can be resolved in both directions.
9. Click **Update List**.
10. Click **Save Changes**.

Specifying a Forward Address (A) record

A DNS server can resolve a computer host name to an IP address; this is known as forward lookup.

To specify a Forward Address (A) record:

1. Select **Server Management > Control Panel**. The “Service Settings” table appears.
2. Click the green *pencil* icon next to the DNS service in the “Service Settings” table. The “DNS Settings for <sitename>” table appears.
3. Select Forward Address (A) Record from the **Add...** pull-down menu.
4. Enter the host name (optional) and domain name you want to serve (for example, www and mydomain.com).
5. Enter the IP address for that domain name (for example, 192.168.10.10) and the network mask (for example, 255.255.255.0).
6. Click **Update List**.
7. Click **Save Changes**.

Specifying a Reverse Lookup (PTR) record

A DNS server can resolve an IP address to a computer host name; this is known as a reverse lookup.

To specify a Reverse Lookup (PTR) record:

1. Select **Server Management > Control Panel**. The "Service Settings" table appears.
2. Click the green *pencil* icon next to the DNS service in the "Service Settings" table. The "DNS Settings for <sitename>" table appears.
3. Select Reverse Lookup (PTR) Record from the **Add...** pull-down menu. The "Add New Reverse Lookup (PTR) Record" table appears.
4. Enter the IP address for your domain name (for example, 192.168.10.10).
5. Enter the host name and domain name (for example, www and mydomain.com) to which that that IP address resolves.
6. Click **Update List**.
7. Click **Save Changes**.

Specifying a mail server (MX) record

To specify a mail server (MX) record:

1. Select **Server Management > Control Panel**. The “Service Settings” table appears.
2. Click the green *pencil* icon next to the DNS service in the “Service Settings” table. The “DNS Settings for <sitename>” table appears.
3. Select Mail Server (MX) from the **Add...** pull-down menu.
4. Enter the domain name (for example, mydomain.com) to be served by the mail server.
5. Enter the fully qualified domain name of the mail server (for example, mail.mydomain.com) that serves the domain name entered in the second field.
6. Under the Delivery Priority pull-down menu, select the priority for mail delivery to the mail server: very high, high, low, very low.

   The value of the delivery priority specifies the order in which a series of mail servers is contacted for mail delivery. The Delivery Priority setting is useful only if more than one MX record is configured for a domain or network.
7. Click **Update List**.
8. Click **Save Changes**.

Specifying an alias (CNAME) record

This feature allows you to alias one host name to another. The target host name does not need to be a member of the local domain. For example, you can create an alias record from “news.domain.com” to “uucp.isp.net”.

Caution: Do not use an Alias (CNAME) Record to cause a domain name to resolve to a host name.

For example, do not create an Alias (CNAME) Record for mydomain.com that resolves to www.mydomain.com. Instead, add a new Address (A) Record for mydomain.com to the IP address used by www.mydomain.com. See “Configuring a primary DNS server” on page 236.

To specify an alias (CNAME) record:

1. Select **Server Management > Control Panel**. The “Service Settings” table appears.
2. Click the green *pencil* icon next to the DNS service in the “Service Settings” table. The “DNS Settings for <sitename>” table appears.
3. Select Alias (CNAME) from the **Add...** pull-down menu.
4. Enter the host name and domain name for which you want to create an alias (for example, www and mydomain.com) and enter the host name and domain name for the target. The target host name is optional.
5. Click **Update List**.
6. Click **Save Changes**.

Configuring a secondary DNS server

The Server Administrator can configure a secondary DNS server to provide redundant DNS service to your computers. If the primary DNS server is turned off, a computer can use the secondary DNS server with no loss of performance.

Adding a secondary domain

To add a secondary name-server authority for a domain:

1. Select **Server Management > Control Panel**. The “Service Settings” table appears.
2. Click the green *pencil* icon next to the DNS service in the “Service Settings” table. The “DNS Settings for <sitename>” table appears.
3. Select Secondary Name Service for Domain from the **Add...** pull-down menu.
4. Enter the domain name to be serviced and the IP address of the primary DNS server.
5. Click **Update List**.
6. Click **Save Changes**.

Adding a secondary network

To add a secondary name-server authority for a network:

1. Select **Server Management > Control Panel**. The “Service Settings” table appears.
2. Click the green *pencil* icon next to the DNS service in the “Service Settings” table. The “DNS Settings for <sitename>” table appears.
3. Select Secondary Name Service for Network from the **Add...** pull-down menu.
4. In the first field, enter the IP address of a member on the network (for example, 192.168.1.1) whose DNS information is served by the IP address in the third field.
5. In the second field, enter the subnet mask corresponding to the IP address for the specified network authority.
6. In the third field, enter the IP address of the primary DNS server for the specified network.
7. Click **Update List**.
8. Click **Save Changes**.

Advanced DNS

Network Mask Notation Conversion

Use Table 2 to convert between dot-quad and network mask bit-count notations.

Table 2. Network Mask Notation Conversion

Dot-Quad	Bit count
255.0.0.0	8
255.128.0.0	9
255.192.0.0	10
255.224.0.0	11
255.240.0.0	12
255.248.0.0	13
255.252.0.0	14
255.254.0.0	15
255.255.0.0	16
255.255.128.0	17
255.255.192.0	18
255.255.224.0	19
255.255.240.0	20
255.255.248.0	21
255.255.252.0	22
255.255.254.0	23
255.255.255.0	24
255.255.255.128	25
255.255.255.192	26
255.255.255.224	27

Table 2. Network Mask Notation Conversion

Dot-Quad	Bit count
255.255.255.240	28
255.255.255.248	29

Delegating a subdomain

☞ ***Important:*** Always click **Save Changes** after modifying DNS records. If you do not, the changes will not take effect.

DNS servers are organized hierarchically. You can delegate the name-server authority for subdomains of any domain served by the Sun Cobalt RaQ XTR server appliance to other name servers.

For example, *domain.com* can be served authoritatively by a server appliance by defining a Forward Address (A) Record using that domain. A subdomain, such as remote.domain.com, can use its own set of DNS servers so that domain authority can be shared between multiple physical sites. This makes it easier to use multiple DNS servers in remote locations sharing a common domain.

To delegate the subdomain naming authority to another name server:

1. Select **Server Management > Control Panel**. The “Service Settings” table appears.
2. Click the green *pencil* icon next to the DNS service in the “Service Settings” table. The “DNS Settings for <sitename>” table appears.
3. Select the parent domain from the **Select Domain or Network...** pull-down menu.
4. Select Delegate Subdomain from the **Add...** pull-down menu.
5. Specify the subdomain name and the qualified host name(s) of the DNS server(s) that will be authoritative for that subdomain.
6. Click **Save Changes**.
7. Click **Save Changes** again.

Delegating a subnet

You can delegate the name-server authority for a network to a remote DNS server.

To delegate the subnet naming authority to a remote DNS server:

1. Select **Server Management > Control Panel**. The “Service Settings” table appears.
2. Click the green *pencil* icon next to the DNS service in the “Service Settings” table. The “DNS Settings for <sitename>” table appears.
3. Select the parent network from the **Select Domain or Network...** pull-down menu.
4. Select Delegate Subnetwork from the **Add...** pull-down menu.
5. Specify an IP address and the size of the network to be delegated. The IP address must be a member of the subnet to be delegated.
6. Specify the qualified host name of the DNS server that will be authoritative for that subnet.
7. Click **Save Changes**.
8. Click **Save Changes** again.

Configuring server settings

You can configure forwarding servers and zone transfer access control for the server appliance’s DNS server.

To configure the DNS server settings:

1. Select **Server Management > Control Panel**. The “Service Settings” table appears.
2. Click the green *pencil* icon next to the DNS service in the “Service Settings” table. The “DNS Settings for <sitename>” table appears.
3. Select Server Settings from the **Add...** pull-down menu.
4. If the Sun Cobalt RaQ XTR server appliance is being used on a private network or in conjunction with a restrictive firewall, you can specify forwarding servers.

   Enter the IP address of the Forwarding Server and, if you want, the Backup Forwarding Server.

5. A zone transfer allows another DNS server to download the complete list of hosts maintained by your DNS server. By default, zone transfers are unrestricted. However, you can restrict zone transfers if you want.

   Enter IP addresses or network addresses in the Zone Transfer Access field; this automatically causes zone transfers to become restricted. Now, only the IP addresses or network addresses listed in this field are able to perform zone transfers.

6. Click **Save Changes**.

7. Click **Save Changes** again.

Start of Authority (SOA) configuration

For the best reliability, you can fine tune all primary domain and network authority settings independently of each other.

To fine tune the primary domain and network authorities:

1. Select **Server Management > Control Panel**. The “Service Settings” table appears.

2. Click the green *pencil* icon next to the DNS service in the Service Settings table.

3. Select an authoritative domain or network from the **Select a Domain or Network...** pull-down menu.

   The first record in the record list is called the Start of Authority (SOA) record.

4. Click the green *pencil* icon to modify the SOA record.

   The SOA record defaults to acceptable values in the majority of server appliance configurations. You can fine tune the values for the following parameters:

   - Primary name server host name
   - Secondary name server host name (optional)
   - Domain administrator email address
   - Refresh interval
   - Retry interval
   - Expire interval
   - Time-to-live (TTL) interval

5. Click **Save Changes**.

6. Click **Save Changes** again.

Name server (NS)

The primary name server defaults to the host name of the server appliance. You can specify the fully qualified domain name of the secondary DNS server for that domain in the Secondary Name Server (NS) host name field. Some top-level domain registration organizations require that the secondary name server record be defined.

Domain administrator email address

The email address defaults to the user name *admin* of the server appliance. This email address is publicly available and is the administrative contact for the domains or networks served.

Refresh interval

You can configure the refresh interval between updates from a secondary DNS server.

- If DNS record changes occur infrequently, increase the default value.
- If DNS record changes occur often, decrease the default value.

Tune the refresh interval to avoid wasting bandwidth and to ensure the content on the secondary server is accurate at all times.

Retry interval

Due to a connection or service failure, a secondary DNS server may be unable to refresh data from the primary server. The secondary DNS server attempts to refresh data after the interval specified for trying again.

Expire interval

A secondary DNS server may be unable to refresh data from the primary server for a prolonged period of time. After the interval specified for expiry, the secondary server stops serving name requests.

Time-to-live period (TTL)

A caching DNS server other than the primary and secondary DNS servers for this domain or network can cache record lookups for the TTL period. During the TTL period, a caching DNS server does not poll the primary or secondary DNS servers for repeated lookups of the same record.

Sample setup of DNS service

Note: Sun Microsystems recommends that you enable the Automatic DNS Configuration feature on a virtual site to create the DNS records.

For more information, see “Automatic configuration of DNS records” on page 117.

This sample setup assumes that you have already done two things:

1. You have registered your domain name. For more information on registering a domain name, visit the Internet Corporation for Assigned Names and Numbers (ICANN) at http://www.icann.org.
2. You have created the Web site on the server appliance. For instructions on how to do this, see “Developing Web pages” on page 180 and “Directory structure” on page 232.

In the following examples, we will configure a sample Web site called “www.mydomain.com” for Web and email services using a sample IP address 192.168.10.10.

Important: Substitute your domain name and IP address where the sample domain name or sample IP address appears.

The recommended minimum configuration for Web and email services requires these records:

- A Reverse Lookup (PTR) record for 192.168.10.10 which points to www.mydomain.com
- A Forward Address (A) record for www.mydomain.com which resolves to 192.168.10.10 (this record can be automatically generated when creating the Reverse Lookup (PTR) record)
- A Forward Address (A) record for mydomain.com which resolves to 192.168.10.10
- A Mail Server (MX) Record for mydomain.com which resolves to www.mydomain.com

These records allow anyone on the Internet to type either “mydomain.com” or “www.mydomain.com” in order to access your Web site. To set up these records, go to the DNS server settings on the Server Desktop user interface (UI).

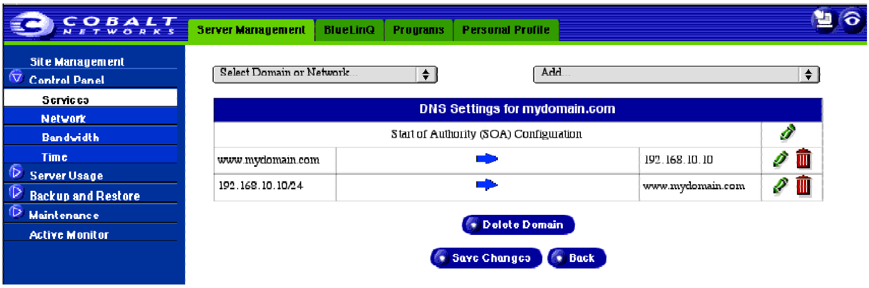
1. Select **Server Management > Control Panel**. The “Service Settings” table appears.
2. Click the check box to enable the Domain Name System (DNS) Server (if it is not already enabled).
3. Click **Save Changes**. The browser screen refreshes.
4. Click the green *pencil* icon next to the DNS service in the “Service Settings” table. The “DNS Settings for <sitename>” table appears.

Reverse Lookup (PTR) record

First, create a Reverse Lookup (PTR) record.

1. Select **Server Management > Control Panel**. The “Service Settings” table appears.
2. Click the green *pencil* icon next to the DNS service in the “Service Settings” table. The “DNS Settings for <sitename>” table appears.
3. Select Reverse Lookup (PTR) Record from the **Add...** pull-down menu. The “Add New Reverse Lookup (PTR) Record” table appears.
   - In the **IP address** field, enter 192.168.10.10.
   - In the **Host Name** field, enter www.
   - In the **Domain Name** field, enter mydomain.com.
   - Click the check box Generate Forward Address (A) Record to generate a Forward Address (A) Record.
4. Click **Save**. The “DNS Settings” table regenerates and displays www.mydomain.com, as in Figure 114.

Figure 114. DNS Settings table (www.mydomain.com)



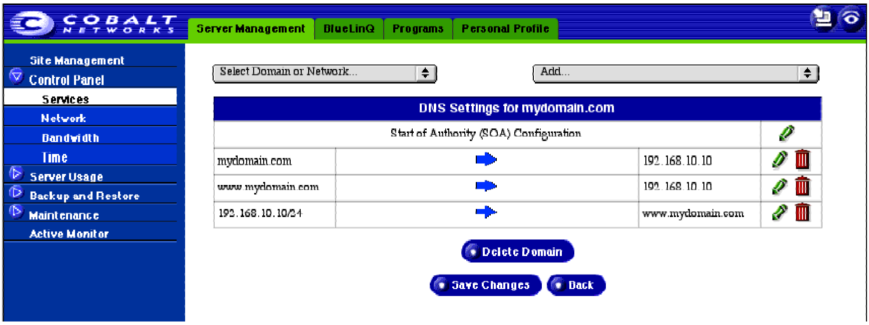
DNS Settings for mydomain.com		
Start of Authority (SOA) Configuration		
www.mydomain.com	→	192.168.10.10
192.168.10.10/24	→	www.mydomain.com

Forward Address (A) record

Next, create a Forward Address (A) record.

1. Select Forward Address (A) Record from the **Add...** pull-down menu. The "Add New Forward Address (A) Record" table appears.
   - Leave the **Host Name** field blank.
   - In the **Domain Name** field, enter mydomain.com.
   - In the **IP address** field, enter 192.168.10.10.
2. Click **Save**. The "DNS Settings" table regenerates and displays www.mydomain.com and mydomain.com, as in Figure 115.

Figure 115. DNS Settings table (www.mydomain.com and mydomain.com)



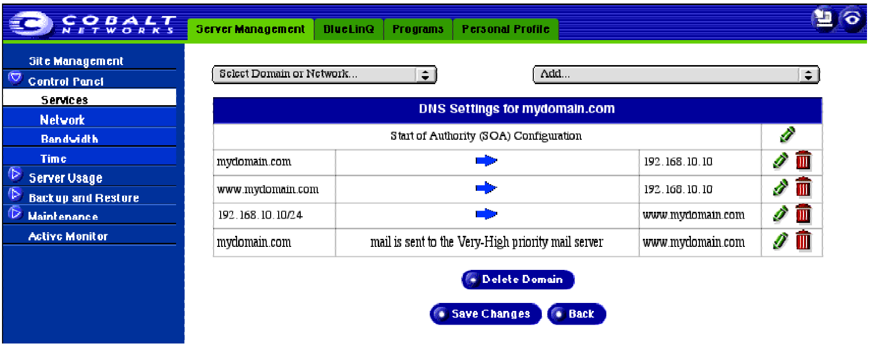
DNS Settings for mydomain.com		
Start of Authority (SOA) Configuration		
mydomain.com	→	192.168.10.10
www.mydomain.com	→	192.168.10.10
192.168.10.10/24	→	www.mydomain.com

Mail Server (MX) record

Finally, create a Mail Server (MX) record.

1. Select Mail Server (MX) Record from the **Add...** pull-down menu. The “Add New Mail Server (MX) Record” table appears.
   - Leave the **Host Name** field blank.
   - In the **Domain Name** field, enter mydomain.com.
   - In the **Mail Server** field, enter www.mydomain.com.
   - Under the **Delivery Priority** pull-down menu, leave the Delivery Priority as Very High.
2. Click **Save**. The “DNS Settings” table regenerates; see Figure 116. You are now finished with creating your DNS records.
3. **IMPORTANT!** Click **Save Changes**. This activates the changes you have made. If you exit this screen without saving your changes, they will not become active.

Figure 116. Completed DNS Settings table



DNS Settings for mydomain.com			
Start of Authority (SOA) Configuration			✎
mydomain.com	→	192.168.10.10	✎ 🗑
www.mydomain.com	→	192.168.10.10	✎ 🗑
192.168.10.10/24	→	www.mydomain.com	✎ 🗑
mydomain.com	mail is sent to the Very-High priority mail server	www.mydomain.com	✎ 🗑

To edit another domain, select another domain from the **Select Domain or Network...** pull-down menu. You can select any domain that you have configured for the DNS server.

To add a new domain, use the **Add...** pull-down menu again. In the **Domain Name** field, replace the default domain name with the new domain name that you want to create.

Further information

For further information, refer to the following:

- In the Sun Cobalt Knowledge Base, search on “DNS”.
- http://www.dnswiz.com/dnsworks.htm
- http://www-europe.cisco.com/warp/public/787/indexDNS.html

Brief history of the Domain Name System (DNS)

In the 1960s, the U.S. Department of Defense Advanced Research Projects Agency (ARPA, and later DARPA) began funding an experimental wide area computer network called the ARPAnet. The ARPAnet used a centrally administered file called HOSTS.TXT which held all name-to-address mapping for each host computer connected to the ARPAnet. Since there were only a handful of host computers at the start, HOSTS.TXT worked well.

When the ARPAnet moved to the Transmission Control Protocol/Internet Protocol (TCP/IP) suite of protocols and become known as the Internet, the population of the network exploded. HOSTS.TXT became plagued with problems, namely

- traffic and load
- name collisions
- consistency

A replacement for the HOSTS.TXT file was needed. The goal was to create a system that solved the problems inherent in a unified host table system. The new system should allow local administration of data and also make that data globally available.

In 1984, the architecture of a new system called Domain Name System (DNS) was designed and is the basis of the DNS service used today on the Internet.

DNS is a distributed database that allows local administration of the segments on the overall database. Data in each segment of the database are available across the entire network through a client-server scheme consisting of name servers and resolvers.

What is a DNS record?

People are much more comfortable dealing with names rather than strings of numbers. A domain name such as “cobalt.com” is much easier to remember than the IP address which consists of four octets of numbers such as 207.91.131.30. Domain names must be registered with Root Domain Registration Service; visit the Internet Corporation for Assigned Names and Numbers (ICANN) at http://www.icann.org. for a list accredited domain-name registrars.

Computers, on the other hand, prefer numbers to names. Since computers have the final say when a user is looking for a company Web site, a mechanism is needed to convert the human-friendly domain name to the computer-friendly IP address.

DNS records on a DNS server perform this function. The records translate a domain name to an IP address; a record equates a domain name such as “cobalt.com” to an IP address such as 207.91.131.30. Once the domain name has been converted or “resolved” to an IP address, then (and only then) can the user connect to your Web site.

Without DNS and domain names, the user would be required to remember the IP address of every site they wanted to visit. With DNS servers and DNS records, customers and their software can easily remember how to get to your site.

Who manages your DNS records?

Your DNS records can reside on any Sun Cobalt server appliance that has the DNS service enabled. You or your administrator can easily configure a Sun Cobalt server appliance to act as a DNS server. To provide DNS service, ICANN requires a site to maintain both a primary and a secondary server. Your Sun Cobalt server appliance can act as the primary server and a DNS server from your Internet service provider (ISP) can act as the secondary server.

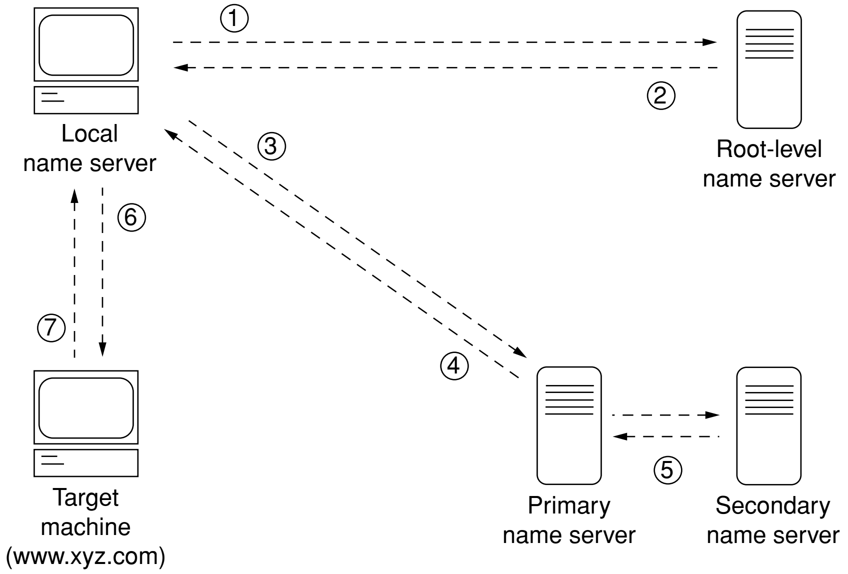
How does DNS work?

The basic method that allows a domain name to direct customers to your Web site is shown in Figure 117. This diagram describes a request made by a Web browser as the customer attempts to log on to your Web site.

To determine which primary name server contains your domain name:

1. The local name server (the DNS resolver/browser machine) contacts the root-level name server maintained by several Internet root server authorities.
2. The root-level name server returns the IP address of the primary name server responsible for the requested domain name.
3. The local name server contacts the primary name server.
4. The primary name server holds the IP address information for the domain name in a database and satisfies the request from the local name server.
5. If the primary name server is unavailable, the local name server contacts the secondary name server that satisfies the request from the local name server. The local name server returns to the Web browser with the IP address for the requested domain name.
6. Using the IP address, the Web browser contacts the company Web server.
7. The company Web server sends the Web page to the local name server.

Figure 117. Basic method of DNS



Disaster Recovery with Third-Party Software

The Sun Cobalt™ RaQ™ XTR server appliance supports the use of third-party backup solutions for performing disaster recovery. The supported backup solutions are:

- Knox Arkeia
- Legato NetWorker®
- Veritas NetBackup

Each of these solutions requires customization to correctly recover the two Cobalt configuration databases in the Sun Cobalt RaQ XTR server appliance (the databases in Postgres and Cobalt Configuration Engine [CCE]). This appendix describes how disaster recovery works on the server appliance, the steps required to perform general disaster recovery, and detailed instructions on how to customize and use each of the specific backup solutions.

How disaster recovery works

For the Sun Cobalt RaQ XTR server appliance, the term *disaster recovery* means restoring the server after performing an OS restore operation which wipes the hard drive clean and returns it to a factory-fresh state. This is also known as “bare-metal recovery”. The entire server appliance must be restored in order for the configuration database and the machine configuration to be in synchronization.

For most files on the server appliance, disaster recovery is straightforward: the files are recovered from the backup service and written to the file system. However, the two configuration databases require additional work and the three supported backup services must be tailored to handle these databases.

The approach used to recover the configuration databases using Knox Arkeia and Veritas NetBackup works as follows:

Before a backup operation begins, the pre-backup script `cobalt_prebackup` creates archives of the two configuration databases in the directory `/var/cobalt/backups`.

The backup makes copies of the archives:

```
/var/cobalt/backups/cce.tar
/var/cobalt/backups/cobalt.sql
```

When the backup is complete, the post-backup script `cobalt_postbackup` deletes the archives.

During the disaster-recovery process, the entire server appliance must be restored. This restores the archives to the directory `/var/cobalt/backups.` When the backup is complete, you must reboot the server appliance; the server does not reboot automatically. During the reboot process, the `cobalt_restore` startup script detects the archives and restores the configuration databases. At this point, everything should be in a consistent state and disaster recovery is complete.

Legato NetWorker works in a different manner: it recovers the databases during the file recovery phase since this service permits per-file scripting at both backup and recover time. The `postgresasm` and `cceasm` scripts are used for this purpose.

Locking the UI databases

For all types of backup, the databases for the Server Desktop user interface (UI) are locked for as short a period of time as possible. For Arkeia and NetBackup, the Server Desktop UI is locked during the pre-backup creation of the database archives. NetWorker locks the Server Desktop UI only during the backup of the individual databases.

☞ ***Important:*** Changes to the machine configuration should not be made during the backup of the machine; otherwise, the configuration of the machine and the configuration databases may not be synchronized after the disaster-recovery process is complete.

This is also true for modifications to system configurations that do not use the Server Desktop UI. After disaster recovery, the machine may be in an inconsistent state if the configuration databases and the system configuration files do not agree.

This begs the question: “So why not lock the UI until the backup ends?” Unfortunately, that would entail shutting down CCE for the duration of the process and locking `postgres` for an unknown duration while the machine writes to the backup server. Because this would affect both the responsiveness of the Server Desktop UI, Sun decided against locking the UI for the duration of the backup process.

Sun Microsystems recommends that you schedule backups for times when it is unlikely that system configuration changes are in progress. Partly for this reason, most backup systems automatically schedule backups for the early hours in the morning.

General steps to perform disaster recovery

The general procedure for performing disaster recovery is as follows:

1. Perform an OS restore to wipe the hard disk drive and return the Sun Cobalt RaQ XTR server appliance to a factory-fresh state.
2. Configure the server appliance through the Setup Wizard and return it to the network. The server appliance must be able to communicate with the backup server.
3. Through the Server Desktop UI on the server appliance, configure the backup service with which you backed up your server appliance. The tasks include enabling the backup client and entering a backup server name. The specific configuration information is discussed later in this appendix.
4. Use the backup solution to perform the recovery.
5. Reboot the server appliance.
6. Verify the restoration.

General notes regarding backup services

The following recommendations are stressed for configuring your backup service:

1. Backup systems are very sensitive to time. If possible, configure the Sun Cobalt RaQ XTR server appliance to use a network time protocol (NTP) server to set the clock on the server appliance.

   On the Server Desktop UI, select **Control Panel > Time** to configure the time settings or to specify an NTP server.

2. Backup systems are very sensitive to correct DNS configuration.

   Ensure that your server appliance has both forward and reverse DNS lookups available to the backup server so that the backup solution functions properly.

   For more information, see Appendix E, “Domain Name System”.

3. Always backup and recover the `/var`, `/etc`, and `/usr/sausalito` directories together.

   These directories contain both the machine configuration and the Cobalt configuration databases. Backing up and recovering these directories at different times can lead to inconsistencies between the configuration of your server appliance and the configuration reported in the Server Desktop UI.

Knox Arkeia

Tailoring the backup service

Server-side tailoring is required for Knox Arkeia. Arkeia performs backups with groups of clients called *savepacks*. When adding a Sun Cobalt RaQ XTR server appliance to a savepack on the Knox Arkeia backup server, the tree options must be modified to use a pre-backup and post-backup command.

To set these parameters, select the server appliance from the list of clients in the savepack and edit the tree options for that client.

Important: For the *hostname*, enter the host name only. Do not enter the fully qualified domain name.

1. Next to the option “command before tree”, uncheck the option “Backup tree if command fails”.
2. In the field following this option, enter:

   ```
   hostname:/usr/local/sbin/cobalt_prebackup
   ```

   where *hostname* is the client name of the server appliance you are backing up.
3. Next to the option “command after tree”, check the option “Execute if tree backup fails”.
4. In the field following this option, enter:

   ```
   hostname:/usr/local/sbin/cobalt_postbackup
   ```

   where *hostname* is the client name of the server appliance you are backing up.

Files associated with Knox Arkeia tailoring

Table 3 lists the files associated with the Knox Arkeia software. These files are located on the Sun Cobalt RaQ XTR server appliance.

Table 3. Files associated with Knox Arkeia tailoring

Path and file name	Description
/usr/local/sbin/ cobalt_prebackup	Script that runs before a backup to create archives of the cobalt postgres database and the CCE database.
/usr/local/sbin/ cobalt_postbackup	Script that runs after a backup to delete the archives created by cobalt_prebackup.
/etc/rc.d/init.d/cobalt_restore	Script that runs at startup and detects whether archives of the configuration databases exist. Extant archives are recovered and have their names changed.
/var/cobalt/backups/cce.tar	Archive of the CCE database. It is created by cobalt_prebackup, deleted by cobalt_postbackup, and renamed to restored.cce.tar by cobalt_restore after disaster recovery.
/var/cobalt/backups/cobalt.sql	Archive of the cobalt postgres database. It is created by cobalt_prebackup, deleted by cobalt_postbackup, and renamed to restored.cobalt.sql by cobalt_restore after disaster recovery.

Backing up a server appliance with Knox Arkeia

To back up your server appliance with Knox Arkeia, you must first configure and enable the Arkeia agent on the server appliance. For more information, see "Backup and Restore" on page 151.

Backups are started by using the Knox Arkeia UI. Once a backup of a server appliance has begun, the `cobalt_prebackup` script creates the `cobalt.sql` and `cce.tar` files in the `/var/cobalt/backups` directory if the tree options for the server appliance were configured correctly.

☞ ***Important:*** The server appliance will not restore properly if the tree options do not execute the `prebackup` and `postbackup` commands.

When the backup has successfully completed, the script `cobalt_postbackup` removes the `cobalt.sql` and `cce.tar` files.

Performing disaster recovery of a server appliance with Knox Arkeia

To perform a restore with the Knox Arkeia software, you must have backed up the server appliance to an Arkeia server.

Preparing for disaster recovery

Prepare your Sun Cobalt RaQ XTR server appliance for disaster recovery by performing the following steps:

1. Perform an OS restore to wipe the hard disk drive and return the server appliance to a factory-fresh state.
2. Configure the server appliance through the Setup Wizard and return it to the network. The server appliance must be able to communicate with the backup server; otherwise, the recovery will fail.
3. If possible, configure the server appliance to use a network time protocol (NTP) server to set the clock on the server appliance.

   On the Server Desktop UI, select **Control Panel > Time** to configure the time settings or to specify an NTP server.

4. Select **Backup and Restore > Knox Arkeia** and configure the Knox Arkeia client on the server appliance.
    - **Enable Client**—Click to enable the check box Enable Client.
    - **Backup Server Name**—Enter the fully qualified domain name of the Knox Arkeia backup server.
    - **Port Number**—Enter the port number to which your Knox Arkeia backup server is listening. The default port number is 617.
5. Click **Save**.
6. Select **Backup and Restore > Control**. The “Backup System Control” table appears.
    - Lock the UI by clicking the check box Locked.
    - Turn off the services by disabling the check box Active.
7. Click **Save Changes**.

Performing a disaster-recovery operation

After completing the preparation steps in the previous section, the Sun Cobalt RaQ XTR server appliance is now ready to be restored.

The restoration options on the Knox Arkeia backup server should include “Files modified since backup date” and “by user ID”.

Only certain directories can be recovered during disaster recovery. Select the following directories using the Arkeia tree navigator:

```
/home
/root
.nsr
/usr
/nsr
/var
/etc
opt
```

Important: DO NOT select `/lib`, `/boot`, or `/vmlinux.gz` or your server appliance will crash during recovery and most likely will not reboot.

When the restore process is complete, reboot the server appliance.

☞ ***Important:*** Disaster recovery is not complete until you reboot the server appliance.

The server appliance does not reboot automatically.

After the server appliance has rebooted, ensure that the CCE and Cobalt databases were recovered. Inspect the directory `/var/cobalt/backups/` for files. If `cce.tar` and `cobalt.sql` exist and do not have a ‘restored’ prefix, then you need to run the command:

```
/etc/rc.d/init.d/cobalt_restore start
```

as the root user and reboot the server appliance again.

The Arkeia log window indicates that the following files are “busy” and that it cannot overwrite the files. This is both normal and acceptable.

```
/usr/bin/perl5.00503
/usr/sbin/httpd
/usr/sausalito/cced.socket
/usr/sausalito/sbin/cced
/usr/knox/bin/opbs
/usr/knox/bin/nlservd
```

Legato NetWorker

Tailoring the backup service

No server-side tailoring is required for NetWorker other than adding the client to the backup server.

☞ ***Important:*** When adding a Sun Cobalt RaQ XTR server appliance to a Legato NetWorker backup server, select "Unix Standard Directives" when creating the server appliance client resource.

Do not select "Compression directives". If you select "Compression directives", the tailoring for the server appliance will not work properly.

Files associated with Legato NetWorker tailoring

Table 4 lists the files associated with the Legato NetWorker software. These files are located on the Sun Cobalt RaQ XTR server appliance.

Table 4. Files associated with Legato NetWorker

Path and file name	Description
/.nsr	Directives for handling the server appliance file systems.
/var/lib/pgsql/.nsr	Directives for handling the cobalt postgres database.
/usr/bin/postgresasm	An external Application Specific Module (ASM) for postgres databases. ***Note:*** External ASMs are not compatible with "Compression directives".
/usr/bin/cceasm	An external Application Specific Module (ASM) for the CCE database. ***Note:*** External ASMs are not compatible with "Compression directives".

Backing up a server appliance with Legato NetWorker

To back up your server appliance with Legato NetWorker, you must first configure and enable the NetWorker agent on the server appliance. For more information, see “Backup and Restore” on page 151.

Sun Microsystems recommends specifying the “All” saveset when using Legato NetWorker. If you must specify individual savesets for a server appliance, you must backup up the following directories together to ensure consistency:

```
/etc
/var/lib/pgsql
/usr/sausalito
```

Performing disaster recovery on a server appliance with Legato NetWorker

To perform a restore with the Legato NetWorker software, you must have backed up the server appliance to a NetWorker server.

Preparing for disaster recovery

Prepare your Sun Cobalt RaQ XTR server appliance for disaster recovery by performing the following steps:

1. Perform an OS restore to wipe the hard disk drive and return the server appliance to a factory-fresh state.
2. Configure the server appliance through the Setup Wizard and return it to the network. The server appliance must be able to communicate with the backup server; otherwise, the recovery will fail.
3. If possible, configure the server appliance to use a network time protocol (NTP) server to set the clock on the server appliance.

   On the Server Desktop UI, select **Control Panel > Time** to configure the time settings or to specify an NTP server.

4. Select **Backup and Restore > Legato NetWorker** and configure the Legato NetWorker client on the server appliance.

   - **Enable Client**—Click to enable the check box to enable the backup client.
   - **Legato Server Hostnames**—Enter the fully qualified domain names of Legato NetWorker backup servers. Legato servers must have valid host names.
   - **Service port range—**Sets the range of the system’s service ports to the one specified (default range is 9000—9010).
   - **Connection Port Range**—Sets the range of the system’s connection ports to the one specified (default range is 9011—9999).

5. Click **Save**.

6. Select **Backup and Restore > Control**. The “Backup System Control” table appears.

   - Unlock the UI by disabling the check box Locked.
   - Turn on the services by enabling the check box Active.

7. Click **Save Changes**.

Performing a disaster-recovery operation

After completing the preparation steps in the previous section, the Sun Cobalt RaQ XTR server appliance is now ready to be restored.

Important: The `/var` recover operation must complete before the "/" recover operation begins. The `/var` directory must be recovered before the `/etc` directory or an error will occur when recovering the Cobalt database in postgres. If this happens, the system administration database and the OS configuration files will be out of synchronization, and the UI will have inconsistent information.

Restore the file systems for your server appliance in the following order:

```
/var
/
/home
```

When the restore process is complete, reboot the server appliance for all the changes to take effect.

Important: Disaster recovery is not complete until you reboot the server appliance.

The server appliance does not reboot automatically.

Technical notes

If the root directory / is recovered before the directory /var, a *postgresasm* error occurs in the log, indicating that the password is invalid. During the OS restore process (using Sun's OS Restore Disc), a new random admininstration password is created for postgres. This password is stored in the file /etc/cobalt/.meta.id, which is restored by Legato NetWorker as part of the / file system. The Cobalt database is restored with the /var file system and uses the password stored in this file. After recovery, the password reflects the admin password that will be used after the database is restarted, not the password for the running database.

Legato NetWorker restores the two Cobalt configuration databases independently. It is possible to restore the cobalt postgres database or CCE database without restoring the machine configuration files in /etc. If this is done, the configuration database and the Server Desktop UI will have different information than the actual system, which is generally considered to be a bad situation.

The recover log may contain entries similar to the following when restoring the postgres database. These entries relate to dropping a non-existent index and are not actually errors.

```
> ERROR: pg_ownercheck: class "vsite_pkey" not found
> CREATE
> ERROR: pg_ownercheck: class "users_pkey" not found
> CREATE
> ERROR: pg_ownercheck: class "bw_pkey" not found
> CREATE
```

Veritas NetBackup

Tailoring the backup service

No server-side tailoring is required for Veritas NetBackup. Pre- and post-backup scripts are already installed and are run automatically by the NetBackup client. See Table 5 for a list of files associated with the Veritas NetBackup software.

Files associated with Veritas NetBackup tailoring

Table 5 lists the files associated with the Veritas NetBackup software. These files are located on the Sun Cobalt RaQ XTR server appliance.

Table 5. Files associated with Veritas NetBackup

Path and file name	Description
/opt/openv/netbackup/bin/ bpstart_notify	Started automatically by NetBackup before a backup runs. It calls the script cobalt_prebackup.
/opt/openv/netbackup/bin/ bpend_notify	Started automatically by NetBackup after a backup runs. It calls the script cobalt_postbackup.
/usr/local/sbin/ cobalt_prebackup	Runs before a backup to create archives of the cobalt postgres database and the CCE database.
/usr/local/sbin/ cobalt_postbackup	Runs after a backup to delete the archives created by cobalt_prebackup.
/etc/rc.d/init.d/cobalt_restore	Runs at startup and detects whether archives of the configuration databases exist. Extant archives are recovered and have their names changed.
/var/cobalt/backups/cce.tar	Archive of the CCE database. It is created by cobalt_prebackup, deleted by cobalt_postbackup, and renamed to restored.cce.tar by cobalt_restore after disaster recovery.
/var/cobalt/backups/cobalt.sql	Archive of the cobalt postgres database. It is created by cobalt_prebackup, deleted by cobalt_postbackup, and renamed to restored.cobalt.sql by cobalt_restore after disaster recovery.

Backing up a server appliance with Veritas NetBackup

To back up your server appliance with Veritas NetBackup, you must first configure and enable the NetBackup agent on the server appliance. For more information, see "Backup and Restore" on page 151.

Backups are started by using the Veritas NetBackup UI. Once a backup of a server appliance has begun, the `cobalt_prebackup` script creates the `cobalt.sql` and `cce.tar` files in the `/var/cobalt/backups` directory if the tree options for the server appliance were configured correctly.

Important: The server appliance will not restore properly if the tree options do not execute the `prebackup` and `postbackup` commands.

When the backup has successfully completed, the script `cobalt_postbackup` removes the `cobalt.sql` and `cce.tar` files.

Sun Microsystems recommends specifying the "ALL_LOCAL_DRIVES" option when using Veritas NetBackup. If you must specify individual savesets for a server appliance, you must backup up the following directories together to ensure consistency:

```
/etc
/var/lib/pgsql
/usr/sausalito
```

Performing disaster recovery on a server appliance with Veritas NetBackup

To perform a restore with the Veritas NetBackup software, you must have backed up the server appliance to a NetBackup server.

Preparing for disaster recovery

Prepare your Sun Cobalt RaQ XTR server appliance for disaster recovery by performing the following steps:

1. Perform an OS restore to wipe the hard disk drive and return the server appliance to a factory-fresh state.
2. Configure the server appliance through the Setup Wizard and return it to the network. The server appliance must be able to communicate with the backup server; otherwise the recovery will fail.
3. If possible, configure the server appliance to use a network time protocol (NTP) server to set the clock on the server appliance.

   On the Server Desktop UI, select **Control Panel > Time** to configure the time settings or to specify an NTP server.
4. Select **Backup and Restore > Veritas NetBackup** and configure the Veritas NetBackup client on the server appliance.
   - **Enable Client**—Click the check box to enable the Veritas NetBackup backup client.
   - **Master Veritas Server**—Enter the fully qualified domain name of Veritas NetBackup master backup server. The Veritas master backup server must have a valid host name.
   - **Extra Veritas Servers—**Enter the fully qualified domain names of any extra Veritas NetBackup backup servers. All Veritas servers must have valid host names.
5. Click **Save**.

6. Select **Backup and Restore > Control**. The “Backup System Control” table appears.
   - Lock the UI by clicking the check box Locked.
   - Turn on the services by enabling the check box Active.

   Important: Veritas NetBackup uses `inetd` to connect to the client. If you turn services off, your restore will not start.

7. Click **Save Changes**.

Performing a disaster-recovery operation

After completing the preparation steps in the previous section, the server appliance is now ready to be restored. When recovering your server appliance, include only the following files and directories:

```
/home
/root
.nsr
/usr
/nsr
/var
/etc
opt
```

Important: DO NOT select `/lib`, `/boot`, or `/vmlinux.gz` or your server appliance will crash during recovery and most likely will not reboot.

When the restore process is complete, reboot the server appliance for all the changes to take effect.

Important: Disaster recovery is not complete until you reboot the server appliance.

The server appliance does not reboot automatically.

After the server appliance has rebooted, ensure that the CCE and Cobalt databases were recovered. Inspect the directory `/var/cobalt/backups/` for files. If `cce.tar` and `cobalt.sql` exist and do not have a ‘restored’ prefix, then you need to run the command:

```
/etc/rc.d/init.d/cobalt_restore start
```

as the root user and reboot the server appliance again.

The restore is initiated at this point.

Note: The restore log indicates that the restore was only partially completed. This is due to warnings concerning any files that were in use during the recovery process.

You should verify the files for which you received a warning, but this not normally a problem.

Contacting Sun Microsystems, Inc.

Customer Service and Technical Support

For Sun Cobalt™ product information, visit the Sun Cobalt section of the Sun Web site at http://www.sun.com/service/suncobalt. On this site, customers can query the Sun Cobalt Knowledge Base, participate in the Sun Cobalt Support Forums moderated by Sun or submit a service request to Sun.

Knowledge Base

You can query the Sun's online database of common installation and configuration problems and solutions.

Go to the URL http://www.sun.com/service/suncobalt and click on the link in section Step 1.

Support forums

You can use the Sun Cobalt discussion forums to find answers, post problems, and read responses to posted problems. Sun Cobalt discussion forums are moderated by Sun Support.

Go to the URL http://www.sun.com/service/suncobalt and click on the link in section Step 2.

Service request

If you cannot find a solution through the Knowledge Base or the support forums, you can submit a service request and receive help from a Sun support engineer.

Go to the URL http://www.sun.com/service/suncobalt. In section Step 3, choose the geographical region in which you are located and click on that link.

Telephone numbers

In the United States, call (800) 526-0484.

In Europe, Middle East and Africa, call +31 (71) 565-7070 (The Netherlands).

Before contacting Technical Support

Note: To receive Technical Support, you must first register your Sun Cobalt product.

First, make an effort to resolve the problem on your own. Take note of all actions you perform and any error messages so that, if necessary, you can describe them to a member of the Technical Support team.

Refer to the user manual and to the Web-based resources, such as the Knowledge Base, the support forums and the Solutions Directory (see "Further resources and information" on page 277).

To speed up your support call

When contacting Technical Support, the more information you can provide, the better. Before you call or email, have the following information ready.

- the serial number, located on the back panel, or the MAC address of the primary network interface of your Sun Cobalt™ RaQ™ XTR server appliance (on the Server Desktop UI, select **Server Management > Control Panel > Network**)
- any additional software installed on your system
- any peripherals connected to your system
- any error messages you have received and the time when they occurred
- the process you were running or the changes you had made when the error occurred
- the steps you have taken to resolve the problem

Further resources and information

Cobalt also offers the following additional resources and information.

Product demonstrations

To view demonstrations of the Sun Cobalt server appliances, visit the Product Demos site at http://demo.cobalt.com/.

Solutions

For business-case information concerning Sun Cobalt products or for solutions that extend the functionality of our products, visit the Online Solutions Directory at http://developer.cobalt.com/sol/.

Sun Cobalt Developer Network

Sun Microsystems provides a wide range of resources, such as technical notes and white papers, for developers of Linux applications for the Sun Cobalt platforms. Premium resources are also available.

To register with the Sun Cobalt Developer Network at no cost, visit the Developer Network site at http://developer.cobalt.com/.

Support forums

Users can share information through a number of support forums. To view the current list of Sun Cobalt support forums, go to the URL http://www.sun.com/service/suncobalt and click on the link in section Step 2. In the new window, the names of the support forums show up as hypertext links.

To subscribe to or unsubscribe from a support forum, or to view previous postings to a group, click on the group name. A new browser window opens, displaying information about the support forum.

New support forums are added periodically. The current forums include:

- an announcement list concerning Sun Cobalt products
- an information list for developers working on Sun Cobalt products
- a user list for sharing information between users of Sun Cobalt products
- a security list for users to address network security issues on Sun Cobalt products

Education

For those who desire a premium level of technical expertise with Sun Cobalt products, Sun offers a number of training courses. The intended audiences includes end users, Sun Cobalt resellers, system and network administrators, systems engineers, product developers, support technicians, consultants and trainers.

You can access the Training Solutions site at http://suned.sun.com/HQ/cobalt/.

Licenses

The BSD Copyright

GNU General Public License

Version 2, June 1991

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program," below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification.") Each licensee is addressed as "you."

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above, provided that you also do one of the following:

a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated, so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING, THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT, UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING, WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SSL License

Copyright (c) 1998-1999 Ralf S. Engelschall. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

   "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.engelschall.com/sw/mod_ssl/)."
4. The name "mod_ssl" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact rse@engelschall.com.
5. Products derived from this software may not be called "mod_ssl" nor may "mod_ssl" appear in their names without prior written permission of Ralf S. Engelschall.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.engelschall.com/sw/mod_ssl/)."

THIS SOFTWARE IS PROVIDED BY RALF S. ENGELSCHALL "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL RALF S. ENGELSCHALL OR HIS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Glossary

The entries in this glossary are for your information. Not all of the concepts, technologies and protocols apply to the Sun Cobalt™ RaQ™ XTR server appliance.

10/100 BaseTX

An Ethernet connection over twisted-pair cables with a throughput of 10 Mb/s or 100 Mb/s.

10BaseT

A 10-Mb/s baseband Ethernet specification using two pairs of twisted-pair cabling (Category 3, 4, or 5): one pair for transmitting data and the other for receiving data. 10BaseT (part of the IEEE 802.3 specification) has a distance limit of approximately 328 feet (100 meters) per segment.

100BaseTX

A 100-Mb/s baseband Fast Ethernet specification using two pairs of either unshielded twisted pair (UTP) or shielded twisted pair (STP) wiring. The first pair of wires is used to receive data; the second pair is used to transmit. To guarantee proper signal timing, a 100BaseTX segment cannot exceed 328 feet (100 meters) in length. 100BaseTX is based on the IEEE 802.3 standard.

Active Server Pages (ASP)

ASP is an HTML-embedded scripting language that includes one or more small embedded programs, or *scripts*, that are processed on a Web server before the Web page is sent to the user. An ASP is somewhat similar to a server-side include or a common gateway interface (CGI) application in that all three involve programs that run on the server, usually tailoring a page for the user.

For example, an ASP script can use the input from the user's request for the page to access data from a database. The script then builds or customizes the page on the fly and returns it to the requestor. The Web server does all of the processing, and a standard HTML page is generated and sent to the browser.

APOP

See *Authentication Post Office Protocol (APOP).*

AppleShare

A file-sharing protocol in Apple system software that allows sharing of files and network services through a file server in the Apple Macintosh environment.

ASP

See *Active Server Page (ASP).*

Authentication

The process whereby a user or information source proves they are who they claim to be; in other words, the process of verifying the identity of a user, device or other entity in a computer system, often as a prerequisite to allowing access to resources in a system. Authentication is any technique enabling the receiver to automatically identify and reject messages that have been altered either deliberately or by channel errors.

See also *Encryption* and *Secure Sockets Layer (SSL).*

Authentication Post Office Protocol (APOP)

Authentication POP is a challenge-response authentication scheme built on top of the standard POP protocol. APOP is designed in a way that protects your password from being sent across the network. To keep your password safe, the server stores your password in a file on local disk drive. When your mail client connects to the APOP server, a magic string is sent back. That string contains a unique identifier for the current session based upon the process id (PID) and current time.

Carrier sense

In a local area network (LAN), an ongoing activity of a data station to detect whether another station is transmitting.

Carrier sense multiple access with collision detection (CSMA/CD)

A protocol that requires carrier sense and in which a transmitting data station that detects another signal while transmitting stops sending, sends a jam signal and then waits for a variable period of time before sending again. Used in ethernet LAN technology.

CGI

See *Common gateway interface (CGI).*

Common gateway interface (CGI)

A set of rules that describe how a Web server communicates with another application running on the same computer and how the application (called a CGI program) communicates with the Web server. Any application can be a CGI program if it handles input and output according to the CGI standard.

Collision

In an ethernet network, a collision is the result of two devices attempting to transmit data at exactly the same time. The network detects the "collision" of the two transmitted packets and discards them both. Collisions are a natural occurrence on an ethernet network.

Ethernet technology uses carrier sense multiple access/collision detect (CSMA/CD) to allow devices to take turns using the signal carrier line. When a device wants to transmit, it checks the signal level of the line to determine whether another device is already using it. If the line is already in use, the device waits and tries again, perhaps in a few seconds. If the line is not in use, the device transmits.

However, two devices can transmit at the same time in which case a collision occurs and both devices detect it. Each device then waits a random amount of time and retries until successful in getting the transmission sent.

CSMA/CD

See *carrier sense multiple access with collision detection (CSMA/CD).*

DHCP

See *Dynamic Host Configuration Protocol (DHCP).*

Digital Subscriber Line (DSL)

A technology for bringing high-bandwidth information to homes and small businesses over ordinary copper telephone lines. The term xDSL refers to different variations of DSL, such as asymmetric DSL (ADSL), high-bit-rate DSL (HDSL) and rate-adaptive DSL (RADSL). If your home or small business is close enough to a telephone company central office that offers DSL service, you may be able to receive data at rates of up to 6.1 Mb/s. More typically, individual connections provide from 512 kb/s to 1.544 Mb/s downstream and about 128 kb/s upstream. A DSL line can carry both data and voice signals and the data part of the line is continuously connected.

DNS

See *Domain Name System (DNS).*

Domain name

The location of an organization or other entity on the Internet. For example, the address www.cobalt.com locates an Internet address for the domain name “cobalt.com” at a particular IP address and a particular host server named “www.”

Domain Name System (DNS)

The Internet service responsible for translating a human-readable host name such as cobalt.com into a numeric IP address (111.123.45.67) for TCP/IP communications.

DSL

See *Digital Subscriber Line (DSL).*

Dynamic Host Configuration Protocol (DHCP)

A protocol that provides a mechanism for allocating IP addresses dynamically so that an address can be reused when a host no longer needs it.

Encryption

The transformation of data into a form unreadable by anyone without a secret decryption key. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended. In the area of security, encryption is the ciphering of data by applying an algorithm to plain text to convert it into cipher text.

See also *Authentication* and *Secure Sockets Layer (SSL).*

ESMTP

See *Extended Simple Mail Transfer Protocol (ESMTP).*

Ethernet

The most widely used technology for local area networks (LANs). Standard ethernet runs at 10 Mb/s, 100 Mb/s or 1000 Mb/s. It balances speed, price, ease of installation and availability.

ETRN

ETRN (Extended Turn) is an extension to the Simple Mail Transfer Protocol (SMTP) that allows an SMTP server to send a request to another SMTP server to send any email messages it has. Typically, SMTP is used with two other protocols, Post Office Protocol 3 (POP3) or Internet Message Access Protocol (IMAP), to request messages from a server; SMTP by itself cannot request mail to be sent by another server.

ETRN is designed for use by anyone who is traveling and wants to access their email. ETRN can only be used with Internet service providers (ISPs) that support ETRN.

Extended Simple Mail Transfer Protocol (ESMTP)

The Extended Simple Mail Transfer Protocol specifies extensions to the original SMTP protocol for sending email that supports graphics, audio and video files, and text in various national languages. ESMTP provides the capability for a client email program to inquire of a server email program about which capabilities it supports and then communicate accordingly.

File sharing

The public or private sharing of computer data or space in a network with various levels of access privileges.

File Transfer Protocol (FTP)

A standard Internet protocol and a way to exchange files between computers connected to the Internet. FTP is an application protocol that uses TCP/IP protocols. FTP is commonly used to transfer Web page files from the computer that was used to create the files to the computer that acts as the server for these files. It is also used to download programs and other files to your computer from other servers.

Using FTP, you can update—delete, rename, move and copy—files at a server. You need to log on to an FTP server. However, publicly available files are easily accessed using anonymous FTP.

FTP

See *File Transfer Protocol (FTP).*

Gateway

A network device that acts as an entrance to another network. A gateway can also be any device that passes packets from one network to another network across the Internet.

HTML

See *HyperText Markup Language (HTML).*

HTTP

See *HyperText Transfer Protocol (HTTP).*

HyperText Markup Language (HTML)

A set of “markup” symbols or tags inserted in a text file intended for display on a World Wide Web browser. The markup tags tell the Web browser how to display a Web page’s content, words, and images. HTML is a subset of Standardized Generalized Markup Language (SGML).

HyperText Transfer Protocol (HTTP)

A set of rules for exchanging files (text, graphic images, sound, video and other multimedia files) on the World Wide Web.

ICANN

See *Internet Corporation for Assigned Names and Numbers (ICANN).*

IEEE 802.3

IEEE local area network (LAN) protocol that specifies an implementation of the physical layer and the media access control (MAC) sublayer of the data link layer. IEEE 802.3 uses CSMA/CD access at a variety of speeds over a variety of physical media. Extensions to the IEEE 802.3 standard specify implementations for Fast Ethernet. Physical variations of the original IEEE 802.3 specification include 10Base2, 10Base5, 10BaseF, 10BaseT and 10Broad36. Physical variations for Fast Ethernet include 100BaseT, 100BaseT4 and 100BaseX.

IMAP

See *Internet Message Access Protocol (IMAP).*

Integrated Services Digital Network (ISDN)

A system of digital telephone connections. This system allows data to be transmitted simultaneously across the world using end-to-end digital connectivity.

With ISDN, voice and data are carried by bearer channels (B channels) occupying a bandwidth of 64 kb/s (some switches limit B channels to a capacity of 56 kb/s). A data channel (D channel) handles signaling at 16 kb/s or 64 kb/s, depending on the type of service.

There are two basic types of ISDN service: Basic Rate Interface (BRI) and Primary Rate Interface (PRI). BRI consists of two 64-kb/s B channels and one 16-kb/s D channel for a total of 144 kb/s. This basic service is intended to meet the needs of most individual users.

PRI is intended for users with greater capacity requirements. Typically, the channel structure is 23 B channels plus one 64-kb/s D channel for a total of 1536 kb/s. In Europe, PRI consists of 30 B channels plus one 64-kb/s D channel for a total of 1984 kb/s.

InterBase

The Sun Cobalt RaQ XTR server appliance is pre-loaded with InterBase 6.0, an open-source, cross-platform SQL database from Inprise Corporation. InterBase offers a number of database features—triggers, stored procedures, blobs, event alerters, user-defined functions, multi-dimensional arrays, two-phase commit, referential integrity, constraints and a flexible set of transaction options.

Internet Corporation for Assigned Names and Numbers (ICANN)

The private (non-government) non-profit corporation that has been formed to assume responsibility for the IP address space allocation, protocol parameter assignment, domain name system (DNS) management and root server system management functions.

Internet domain

An Internet domain is a host-naming convention used to ensure that no two individual hosts on the global Internet have the same host name. An Internet domain should not be confused with an NT Domain.

Internet Message Access Protocol (IMAP)

Internet Message Access Protocol is a standard protocol for accessing email from your local server. IMAP is a client/server protocol in which email is received and held for you by your Internet server. You (or your email client) can view just the heading and the sender of the letter and then decide whether to download the mail from the server. You can also create and manipulate folders or mailboxes on the server, delete messages or search for certain parts or an entire note. IMAP requires continuous access to the server during the time that you are working with your mail.

IMAP can be thought of as a remote file server. Another protocol, Post Office Protocol (POP), can be thought of as a store-and-forward service. In other words, your email messages are held at the server until you open your email client and download the messages to your local machine.

POP and IMAP deal with receiving email from your local server; Simple Mail Transfer Protocol (SMTP) is a protocol for transferring email between points on the Internet. You send email with SMTP and a mail handler receives it on your recipient's behalf. Then the mail is read using POP or IMAP.

See also *Post Office Protocol 3 (POP3)* and *Simple Mail Transfer Protocol (SMTP)*.

Internet Protocol (IP)

A network-layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security. IP is defined in RFC 791.

IP address

A 32-bit address assigned to hosts using Transmission Control Protocol/ Internet Protocol (TCP/IP) and written as four octets separated by periods (for example, 192.168.10.10), also called the dotted decimal format. Each address consists of a network number, an optional subnetwork number and a host number. The network and subnetwork numbers together are used for routing, while the host number is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and subnetwork information from the IP address. Also called an Internet address.

IP Masquerading

See *Network Address Translation (NAT)*.

ISDN

See *Integrated Services Digital Network (ISDN)*.

Kernel

The essential center of a computer operating system, the core that provides basic services for all other parts of the operating system. A kernel can be contrasted with a shell, the outermost part of an operating system that interacts with user commands. *Kernel* and *shell* are terms used more frequently in UNIX.

See also *Shell.*

LAN

See *local area network (LAN).*

Leased IP address

An IP address assigned by the Dynamic Host Configuration Protocol (DHCP) to an unrecognized computing device. This method involves setting up a leased pool of IP addresses that are allocated dynamically when new devices are booted and recognized on the network.

Local area network (LAN)

A high-speed, low-error data network covering a relatively small geographic area (up to a few thousand meters). A LAN connects workstations, peripherals, terminals and other devices in a single building or other geographically limited area. LAN standards specify cabling and signaling at the physical and data link layers of the Open Systems Interconnection (OSI) model. Widely used LAN technologies include Ethernet, fiber distributed data interface (FDDI) and token ring.

See also *wide area network (WAN).*

Logical memory

See *virtual memory.*

Media access control (MAC) sublayer

The lower of the two sublayers of the data link layer defined by the IEEE. The MAC sublayer handles access to shared media, such as whether token passing or contention is used.

Media access control (MAC) address

A standardized data-link-layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network, and to create and update routing tables and data structures. MAC addresses are six bytes long and are controlled by the IEEE. Also known as a hardware address, a MAC-layer address and a physical address.

When your computer is connected to the Internet, a correspondence table relates your IP address to your computer's physical (MAC) address on the network

Name server

A program that constitutes the server half of the DNS client-server mechanism. A name server contains information about a segment of the DNS database and makes it available to a client called a resolver. A resolver is often just a library routine that creates queries and sends them across a network to a name server.

NAT

See *Network Address Translation (NAT).*

Netmask

See *subnet mask*.

Network Address Translation (NAT)

A mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space. Also known as *Network Address Translator* and *IP Masquerading*.

Network Time Protocol (NTP)

A protocol that synchronizes the time of a local computer client or server to radio clocks and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods. Some configurations include cryptographic authentication to prevent accidental or malicious protocol attacks.

NTP

See *Network Time Protocol (NTP).*

Packet

The unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network. The packet includes a header containing control information and (usually) user data. Packets are most often used to refer to network layer units of data.

PCI

See *Peripheral Component Interface (PCI).*

Peripheral Component Interconnect (PCI)

Peripheral Component Interconnect (PCI) is an interconnection system between a microprocessor and attached devices in which expansion slots are spaced closely for high-speed operation.

PCI transmits 32 bits at a time in a 124-pin connection (the extra pins are for power supply and grounding) and 64 bits in a 188-pin connection in an expanded implementation. PCI uses all active paths to transmit both address and data signals, sending the address on one clock cycle and data on the next. Burst data can be sent starting with an address on the first cycle and a sequence of data transmissions on a certain number of successive cycles.

PHP embedded scripting

PHP is an HTML-embedded scripting language that includes one or more small embedded programs, or *scripts*, that are processed on a Web server before the Web page is sent to the user.

Much of the PHP syntax is borrowed from C, Java and Perl with a couple of unique PHP-specific features thrown in. The goal of the language is to allow Web developers to write dynamically generated pages quickly.

Point-to-Point Protocol (PPP)

A protocol for communication between two computers using a serial interface, typically a personal computer connected by telephone line to a server. For example, your Internet server provider may provide you with a PPP connection so that the provider’s server can respond to your requests, pass them on to the Internet and forward your requested Internet responses back to you. PPP uses the Internet protocol (and is designed to handle others).

PPP is a full-duplex protocol that can be used on various physical media, including twisted pair, fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control for packet encapsulation. PPP can handle synchronous as well as asynchronous communication.

Point-to-Point Protocol over Ethernet (PPPoE)

A specification for connecting multiple computer users on an ethernet to a remote site through common customer-premises equipment such as a modem and similar devices. PPPoE can be used to allow an office or building full of users share a common digital subscriber line (DSL), cable modem or wireless connection to the Internet. PPPoE combines the Point-to-Point Protocol (PPP), commonly used in dial-up connections, with the ethernet protocol, which supports multiple users in a local area network (LAN). PPP information is encapsulated within an Ethernet frame.

POP3

See *Post Office Protocol (POP3)*.

Post Office Protocol 3 (POP3)

Post Office Protocol (POP) is a standard protocol for receiving email. POP is a client/server protocol in which email is received and held for you by your Internet server. When you read your mail, all of it is immediately downloaded to your computer and no longer maintained on the server, unless specified otherwise in the email client. POP3 is built into the Netscape Navigator and Microsoft Internet Explorer browsers.

POP can be thought of as a store-and-forward service; in other words, your email messages are held at the server until you open your email client and download the messages to your local machine. Another protocol, Internet Message Access Protocol (IMAP), can be thought of as a remote file server.

POP and IMAP deal with receiving email from your local server; Simple Mail Transfer Protocol (SMTP) is a protocol for transferring email between points on the Internet. You send email with SMTP and a mail handler receives it on your recipient's behalf. The mail is then read using POP or IMAP.

See also *Internet Message Access Protocol (IMAP)* and *Simple Mail Transfer Protocol (SMTP)*.

PPP

See *Point-to-Point Protocol*.

PPPoE

See *Point-to-Point Protocol over Ethernet*.

RAID

See *Redundant Array of Independent Disks (RAID)*

Redundant Array of Independent Disks (RAID)

A redundant array of independent disks is a way of storing the same data in different places (thus, redundantly) on multiple hard disks. A RAID appears to the operating system to be a single virtual disk drive.

Redundancy means that there is protection against the failure of any single hard disk drive. Redundant data is used by a RAID system in the event of a failure; this redundant data can either be a mirror copy or parity data used to reconstruct the actual data.

There are a variety of different types and implementations of RAID, each with its own advantages and disadvantages.

- **RAID-0** combines the separate hard disk drives into one virtual disk drive and offers the best performance of the three options. However, the data on the disk drives is not redundant and the system is thus not fault-tolerant. This option is available on server configurations with two or more hard disk drives.
- **RAID-1**, also known as disk mirroring, consists of a primary hard disk drive and a secondary hard disk drive; the secondary disk drive is an exact copy or “mirror image” of the primary disk drive. This option is only available on a configuration with two hard disk drives.
- **RAID-5** includes a rotating parity-bit array. All read and write operations can be overlapped. RAID-5 does not store redundant data but it does store the parity information which can be used to reconstruct data in the event of a single hard-disk-drive failure. RAID-5 requires at least three hard disk drives for the array.

Although RAID-1 and RAID-5 (but not RAID-0) can protect your data in case of a hard-disk-drive failure, they do not protect against operator and administrator (human) error, or against loss due to programming bugs.

RAID can be implemented in hardware or in software. Hardware RAID is always a “disk controller”, that is, a device to which one can cable up the hard disk drives. Software RAID is a set of kernel modules, together with management utilities that implement RAID purely in software, and require no extra hardware.

Root name server

On the Internet, the root name server system is the manner in which an authoritative master list of all top-level domain names (such as .com, .net, .org and individual country codes) is maintained and made available.

SCSI

See *Small Computer System Interface (SCSI).*

Secure Sockets Layer (SSL)

Secure Sockets Layer is a program layer created by Netscape Communications for managing the security of message transmissions in a network. Netscape's idea was that the programming for keeping your messages confidential ought to be contained in a program layer between higher-level protocols (such as HTTP or IMAP) and the TCP/IP layers of the Internet. The "sockets" part of the term refers to the sockets method of passing data between a client and a server program in a network or between program layers in the same computer.

SSL allows an SSL-enabled server to authenticate itself to an SSL-enabled client, allows the client to authenticate itself to the server, and allows both machines to establish an encrypted connection.

These capabilities address fundamental concerns about communication over the Internet and other TCP/IP networks:

- SSL server authentication allows a user to confirm the identity of a server. SSL-enabled client software can use standard techniques of public-key cryptography to check that a server's certificate and public ID are valid and have been issued by a certificate authority (CA) listed in the client's list of trusted CAs. This confirmation can be important if, for example, the user is sending a credit card number over the network and wants to check the receiving server's identity.
- SSL client authentication allows a server to confirm a user's identity. Using the same techniques as those used for server authentication, SSL-enabled server software can check that a client's certificate and public ID are valid and have been issued by a certificate authority (CA) listed in the server's list of trusted CAs. This confirmation can be important if, for example, the server is a bank sending confidential financial information to a customer and wants to check the recipient's identity.
- an encrypted SSL connection requires all information sent between a client and a server to be encrypted by the sending software and decrypted by the receiving software, thus providing a high degree of confidentiality. Confidentiality is important for both parties to any private transaction. In addition, all data sent over an encrypted SSL connection is protected with a mechanism for detecting tampering—that is, for automatically determining whether the data has been altered in transit.

See also *Authentication* and *Encryption*.

Server

A system program that awaits requests from client programs in the same computer or across a network, and services those requests. A server can be dedicated, in which case this is its sole function, or non-dedicated, where the system can be used in other ways, such as a workstation.

Server Message Block (SMB)

A protocol that enables client applications in a computer to read and write files on a computer network and to request services from server programs in a computer network for systems running Microsoft Windows.

Shell

A UNIX term for the interactive user interface (UI) within an operating system. The shell is the layer of programming that understands and executes the commands entered by a user. In some systems, the shell is called a *command interpreter*. A shell usually implies an interface with a command syntax.

The root shell has "root" permissions and is the highest level of shell.

As the outer layer of an operating system, a shell can be contrasted with the kernel, the operating system's inmost layer or core of services.

See also *Kernel*.

Simple Mail Transfer Protocol (SMTP)

The TCP/IP standard protocol for transferring electronic mail messages between points on the Internet. SMTP specifies how two mail systems interact and the format of control messages they exchange to transfer mail.

SMTP is a protocol for transferring email between points on the Internet; Post Office Protocol (POP) and Internet Message Access Protocol (IMAP) deal with receiving email from your local server. You send email with SMTP and a mail handler receives it on your recipient's behalf. The mail is then read using POP or IMAP.

See also *Internet Message Access Protocol (IMAP)* and *Post Office Protocol 3 (POP3).*

Simple Network Management Protocol (SNMP)

A network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance and security on a network.

Small Computer System Interface (SCSI)

A parallel interface standard used by PCs, some Apple Macintosh computers and many Unix systems for attaching peripheral devices to computers. SCSI interfaces provide for faster data transmission rates (up to 160 Mb/s) than standard serial and parallel ports. In addition, you can attach many devices to a single SCSI port, so that SCSI is really an input/output bus rather than simply an interface.

SMB

See *Server Message Block (SMB).*

SMTP

see *Simple Mail Transfer Protocol (SMTP).*

SNMP

See *Simple Network Management Protocol (SNMP).*

SSL

See *Secure Sockets Layer (SSL).*

Subnet mask

A number that, in conjunction with an IP address, defines the set of IP addresses that are considered “local.” For example, if your IP address is 192.168.25.77 and your subnet mask is 255.255.255.0, then addresses between 192.168.25.1 and 192.168.25.255 are considered local. Also known as *netmask*.

Swap file

A space on a hard disk drive used as the virtual memory extension of a computer’s random access memory (RAM). Having a swap file allows the computer’s operating system to pretend that it has more RAM than it actually does. The least-recently-used files in RAM are “swapped out” to your hard disk drive until they are needed later; in their place, new program segments or data can be “swapped in” to RAM.

Transmission Control Protocol (TCP)

A connection-oriented transport-layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.

Transmission Control Protocol/Internet Protocol (TCP/IP)

A common name for the suite of protocols developed in the 1970s to support the construction of worldwide internetworks. TCP and IP are the two best-known protocols in the suite. The TCP/IP protocols enable computers and networks to connect to an intranet or Internet.

Virtual host

See *Virtual site*.

Virtual memory

A concept that, when implemented by a computer and its operating system, allows programmers to use a very large range of memory or storage addresses for stored data.

Virtual site

Whereas industry uses the term *virtual host*, we use the term *virtual site*.

In our definition, a virtual site consists of a Domain Name System (DNS) domain with Web, FTP and email services. Each virtual site contains its own list of site-user accounts. Each site-user account has its own Web page, FTP directory, email spool and any number of email aliases. The fully qualified domain name of a virtual site is unique to that site, while its IP address can be shared by many sites.

With the advent of name-based virtual hosting, it is no longer necessary to dedicate an IP address to a virtual site. The Web server can now differentiate among target virtual sites according to the name requested. Many virtual sites on the Sun Cobalt RaQ XTR server appliance can share one IP address. However, not all services are compatible with name-based virtual hosting: SSL encryption for Web data, bandwidth management and an anonymous FTP account can only be enabled on one virtual site per IP address hosted by the server appliance.

The IP address of the Sun Cobalt RaQ XTR server appliance can be shared by many virtual sites or it can be unique to one virtual site.

The server appliance has one main site (which by default cannot be deleted) and virtual sites. The main site uses the IP address assigned to the server appliance using the LCD console.

Wide area network (WAN)

A data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers. Asynchronous transfer mode (ATM), frame relay, Switched Multimegabit Data Service (SMDS) and X.25 are examples of WANs.

See also *local area network (LAN)*.

Index