COBALT CacheRaQ 4

User Manual

COBALT
NETWORKS

Important Safeguards

For your protection, please read all these instructions regarding your CacheRaQ™ 4 and retain for future reference.

1. **Read instructions**

   Read and understand all the safety and operating instructions before operating the appliance.

2. **Ventilation**

   The CacheRaQ 4's vents (on the front) and the fan opening(s) (on the back panel) are provided for ventilation and reliable operation of the product and to protect it 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.

3. **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 Cobalt Networks 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.

AVERTISSMENT: 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.

4. 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.

5. Electrical shock

To reduce the risk of electrical shock, do not disassemble this product. Take it 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.

6. Operating the unit in an equipment rack

If you plan to operate the CacheRaQ 4 in an equipment rack, take the following precautions:

a. Ensure the ambient temperature around the CacheRaQ 4 (which may be higher than the room temperature) is within the limits specified in Appendix B. See "Physical data" on page 64".

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

c. Ensure electrical circuits are not overloaded; consider the nameplate ratings of all 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 CacheRaQ 4.

7. **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 Cobalt CacheRaQ 4, 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 CacheRaQ 4's data. The CacheRaQ 4 has been tested with both Netscape Navigator version 4.7 and Microsoft Internet Explorer version 5.0.

Regulations and information

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. 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. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Re-orient or re-locate the receiving antenna.

- Increase the separation between the equipment and receiver.

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help.

In order to maintain compliance with FCC regulations, shielded cables must be used with this equipment. Operation with non-approved equipment or unshielded cables is likely to result in interference to radio and TV reception. The user is cautioned that changes and modifications made to the equipment without the approval of manufacturer can void the user's authority to operate this equipment.

This equipment is in compliance with Underwriters Laboratories (UL) and is UL listed.

Preface

This user manual is for anyone who will set up the CacheRaQ 4 network server appliance for a group of users. You should be familiar with Microsoft® Windows^{TM}, 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" on page 1 includes an overview of the CacheRaQ 4's features, explains how to contact Cobalt Networks and provides general information about Cobalt networks.

Chapter 2 — "Setting up the CacheRaQ 4" on page 11 explains how to set up the CacheRaQ 4 and integrate the server into the network.

Chapter 3 — "CacheRaQ 4 Administration" on page 31 describes how to configure various features of the CacheRaQ 4 and how to view the statistics and log files.

Appendix A — "Using the LCD Console" on page 55 describes the LCD console functions—configuring or resetting the CacheRaQ 4's network settings, rebooting the server and powering down.

Appendix B — "Product Specifications" on page 61 provides information about the CacheRaQ 4 hardware and software, regulatory approvals and physical data.

Appendix C — "Sample Network Topologies" on page 65 shows examples of how the CacheRaQ 4 can be used within a network.

Appendix D — "Advanced Information" on page 77 provides information on initializing the CacheRaQ 4 through the serial console port.

Appendix E— "Licenses" on page 79 lists licensing information.

Appendix F— "Glossary" on page 87 provides a glossary of terms used in the CacheRaQ 4 manual.

Table of Contents

A Using the LCD Console   55

B Product Specifications   61

Table of Contents

Introduction

The Cobalt CacheRaQ 4 is a dedicated World Wide Web caching device — it stores documents that have been retrieved from the Web. Once a document has been retrieved from the Web, users can obtain it from the CacheRaQ 4 without having to access the Web again. This reduces the communication load on the Wide Area Network (WAN) and helps users obtain Web documents much more quickly.

The Cobalt CacheRaQ 4 can operate in several modes:

- **Traditional Proxy Caching mode**. Client Web browsers are configured explicitly to request documents from the CacheRaQ 4. Either individual users or a central manager of the browser configuration files can configure the browser to do this. The CacheRaQ 4 also supports the use of a proxy auto-configuration (PAC) file for browser configuration.

- **Transparent Caching mode**. All client network traffic is automatically routed through the CacheRaQ 4. The CacheRaQ 4 detects users' requests for Web documents (HTTP requests), which are then handled by the CacheRaQ 4's software. No browser configuration is necessary.

- **Clustering**. Several CacheRaQ 4s are configured in a cluster. Depending on the method of clustering used, clustering can be established in either Traditional Proxy Caching mode or Transparent Caching mode. The CacheRaQ 4 supports a variety of clustering methods: InstaCache (based on Cache Array Routing Protocol [CARP]), Inter-Cache Communication Protocol (ICP) and Web Cache Communication Protocol (WCCP). WCCP works in Transparent Caching mode only.

  In a Cluster configuration, the *Cluster Master* receives HTTP requests from the client by either of the two methods described above. Each request is forwarded dynamically to one of several *Cluster Slaves*. The Cluster Slave retrieves the document, either from its cache or from the document's original server. The Cluster Slave returns the document to the Cluster Master, which forwards it on to the requestor. Because the work of managing cached documents is divided evenly among Cluster Slaves, clustering allows for a greater volume of HTTP traffic.

General

Figure 1 and Figure 2 show the CacheRaQ 4 controls, indicators and connectors.

Front view of the CacheRaQ 4

Figure 1. CacheRaQ 4 front view
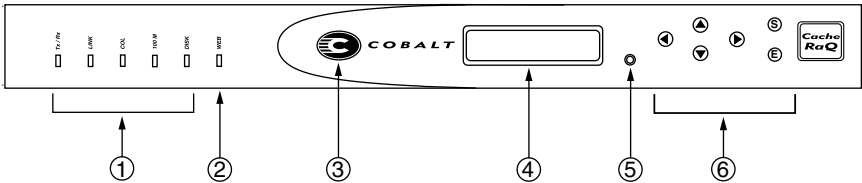
1. The **Status Indicators** signal Ethernet and hard drive activity:

    Tx/Rx (Transmit/Receive) blinks when there is network traffic on the primary interface.

    Link indicates an active network connection on the primary interface.

    Col blinks when a collision is detected on the primary interface.

    100 M indicates that 100BaseT ethernet is being used on the primary interface.

    Disk indicates activity on the hard disk drive.

2. The **Web** indicator blinks to indicate Web activity.

3. The **Logo Badge** glows when the CacheRaQ 4 is powered on.

4. The **LCD Screen** displays messages and entered values.

5. You can use the recessed **Reset Password** button if you forget the CacheRaQ 4 Administrator password. (See "Resetting the CacheRaQ 4 Administrator password" on page 60.)

6. The **LCD arrow buttons** allow you to enter network configuration information, shut down and reboot the CacheRaQ 4. (See "Using the LCD console to configure the network" on page 15.)

Rear view of the CacheRaQ 4

Figure 2. CacheRaQ 4 rear view
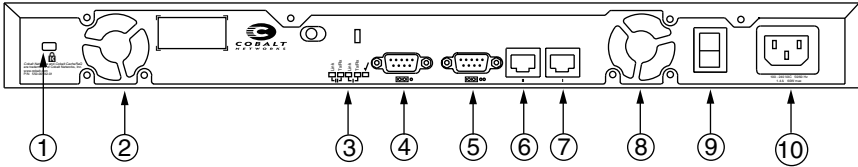
1. The **Security lock hole** is used to lock the unit to a secure location.

2. The **Cooling fans** maintain proper operating temperature. Ensure that the ventilation holes are not blocked.

3. The **Network status indicators/OK to Power Off** signal network activity and information. The **OK to Power Off light** flashes when it is safe to turn the power off.

4. The **Serial console port** allows you to connect serial devices.

5. **Serial connector**.

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

   Network connection 2

7. **Network connection 1**

8. **Cooling fan**.

9. The **Power switch** toggles the power on or off.

10. The **Power socket** receives the AC cord that is provided.

CacheRaQ 4 requirements

To use the CacheRaQ 4, you need the following:

- A10BaseT, 10/100BaseTX or 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, versions 4.7 or later, or Microsoft Internet Explorer, version 5.0 or later). To manage the CacheRaQ 4 from the user interface (UI), your browser must have Java and Javascript™ enabled.

- An IP address and netmask for each configured ethernet interface. You also need to have a gateway IP address and the IP address of a DNS server. To use Transparent Caching, follow the appropriate setup procedure, as described in Chapter 2, "Setting up the CacheRaQ 4."

Target audience for the user manual

The user manual is for CacheRaQ 4 Administrators; it describes how to configure and operate the CacheRaQ 4.

Administrators should be familiar with TCP/IP networking concepts, Microsoft® Windows™, Macintosh® or other operating systems, and Netscape Navigator®, Microsoft® Internet Explorer or other Web browsers.

Cobalt Developer Network

Cobalt provides a wide range of resources, such as technical notes and white papers, for developers of Linux applications for Cobalt platforms. Premium resources are also available.

To register with the Cobalt Developer Network at no cost, visit the Web site at http://developer.cobalt.com/.

How to use this user manual

Organization of the user manual

The user manual is organized according to the user interface (UI). See Figure 3. For a list of chapters and appendices, see "Preface" on page vii.

Figure 3. CacheRaQ 4 user interface

Customer Service and Technical Support

For Cobalt product information, visit the support section of the Cobalt Web site at http://www.cobalt.com/support/. The site includes a Knowledge Base that customers can query; a list of Frequently Asked Questions (FAQs) that provide additional information is also available through the Knowledge Base.

General Cobalt information

In the U.S.A., call (888) 70-COBALT or (888) 702-6225, or send email to info@cobalt.com.

Outside the U.S.A., call +1 650 623-2500, or send email to info@cobalt.com.

In Europe, the Middle East and Africa, call +31 71 565 7000 (Netherlands), or send email to info-emea@cobalt.com.

In Japan, send email to info-japan@cobalt.com.

Cobalt Technical Support and Service

Email contact

You can contact Cobalt Networks Technical Support by email using the Online Email Support Form. This form provides us all the information we need to service your request in a timely fashion.

Go to the URL http://www.cobalt.com/support/ and click on the **Contact Support** link.

Technical Support telephone numbers

In the United States, call (800) 266-4378.

In Europe, Middle East and Africa, call +31 (71) 565-7070 (Netherlands)

Customers in Japan can send email to support-japan@cobalt.com.

Further information

Cobalt also offers other information resources.

Discussion Groups Cobalt has made available a number of discussion groups through which users can share information.

To view the current list of Cobalt discussion groups, type the URL http://www.cobalt.com/support/resources/usergroups.html. The names of the discussion groups show up as hypertext links.

To subscribe to or unsubscribe from a discussion group, or to view previous postings to a group, click on the group name. A new browser window opens, displaying information about the discussion group.

New discussion groups are added periodically. The current groups include:

*   an announcement list concerning Cobalt products

*   an information list for developers working on Cobalt products

*   a users list for sharing information between users of Cobalt products

*   a security list for users to address network security issues on Cobalt products

The Knowledge Base Cobalt offers access to its online database of common installation and configuration problems and solutions. You can access the site at http://www.cobalt.com/support/kb/.

Online technical papers For customers looking for more in-depth technical information, there are a number of technical papers available on Cobalt Networks' web site at http://www.cobalt.com/support/.

Education For those who desire a premium level of technical expertise with Cobalt Networks products, we offer a number of training courses. The intended audience includes end users, Cobalt resellers, system and network administrators, systems engineers, product developers, support technicians, consultants and trainers. You can access the site at http://www.cobalt.com/support/education/index.html/.

Solutions For customers looking for business-case information concerning Cobalt products, there are also a number of white papers available on Cobalt's Web site at http://www.cobalt.com/solutions/.

Developers If you are a software or hardware developer, look for information at http://developer.cobalt.com/.

Before contacting Technical Support

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.

Try our online services to answer your questions. The Technical Support KnowledgeBase, the User Groups, the Online Documentation and the Solutions page offer a wealth of information and may answer your question quickly.

To speed up your support call

When contacting Cobalt Networks 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, accessible through the user interface, of your CacheRaQ 4

- any additional software installed on your system

- any peripherals connected to your system

- a hard copy of any error messages you have received and the time when they occurred

- the process you were running or what changes you had made when the error occurred, so that Technical Support can try to reproduce the error

- the steps you have taken to resolve the problem

Cobalt logo badge

For more information on the CacheRaQ 4 server, click on the Cobalt Networks logo badge in the top left corner.

- the amount of RAM

- the size of the hard disk

- the version of the Cobalt OS

- Cobalt Networks trademark information

The table also contains two hypertext links:

- **Cobalt Networks, Inc. Web site** takes you to the URL http://www.cobalt.com.

- **Credits and Acknowledgements** acknowledges the software used on the CacheRaQ 4.

Setting up the CacheRaQ 4

This chapter guides you through the process of connecting and configuring the CacheRaQ 4 for your network. If the CacheRaQ 4 has been configured previously for a different network, refer to "Changing the Network Configuration," in Appendix A.

The configuration process occurs in two phases.

- "Phase 1: Making the connection" covers the physical setup and connection of the CacheRaQ 4 to a power source and the network.

- "Phase 2: Setting up with the Web browser" covers the network integration and configuration of the CacheRaQ 4, using any browser-enabled computer.

Mode of operation

For more information on the setup of your network, see Appendix C, "Sample Network Topologies," on page 65. Detailed information is also available on the Cobalt Networks Web page at http://www.cobalt.com.

Before configuring the CacheRaQ 4, decide which mode of operation you will use — Traditional Proxy Caching or Transparent Caching.

- If you plan to use Traditional Proxy Caching mode, you only have to configure the Network 1 interface.

- If you plan to use Transparent Caching mode, you need to decide whether you want to use the Network 2 interface in addition to the Network 1 interface (the Network 1 interface is always used). Use the Network 2 interface if you want to force your clients' traffic to flow through the CacheRaQ 4. This mode is useful if, for example, you want to be able to filter or log all of your clients' HTTP traffic.

It is not necessary to use the Network 2 interface when using Transparent Caching mode. The only requirement for transparent caching is that client traffic must be routed to the CacheRaQ 4. For example, this can be done by assigning the clients' gateway IP address to the CacheRaQ 4's Network 1 IP address. In an

ISP POP environment, this can be done by configuring your access concentrators to use the CacheRaQ 4 as the gateway. Appendix C describes sample network configurations.

If you use Traditional Proxy mode, the HTTP and FTP proxy port numbers for browser configuration are both 3128 by default (they can be changed as described later in this chapter). Alternatively, you can configure the browsers to use the CacheRaQ 4's proxy auto-configuration (PAC) file; the URL for this file is http://<cacheraq-name>/proxy.pac.

Phase 1: Making the connection

Installing the CacheRaQ 4

You can place the CacheRaQ 4 on a flat surface — for example, a desk, shelf or table top — or install it in a standard 19-inch equipment rack.

> ⚠ **Caution**: If you operate the CacheRaQ 4 in an equipment rack, see the precautions described in "Operating the unit in an equipment rack," on page ii.

If you plan to use the CacheRaQ 4 on a flat surface, attach the rubber feet to the five indentations on the bottom of the case. See Figure 4.

Figure 4. Rubber feet for the CacheRaQ 4

Rubber feet
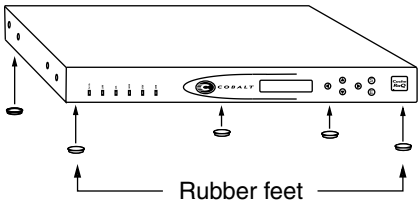
If you plan to operate the CacheRaQ 4 in an equipment rack, first connect the mounting ears to the sides of the CacheRaQ 4 (see Figure 5), near either the front or the rear of the case. Attach the ears to the equipment rack.

Figure 5. Mounting ears for the CacheRaQ 4
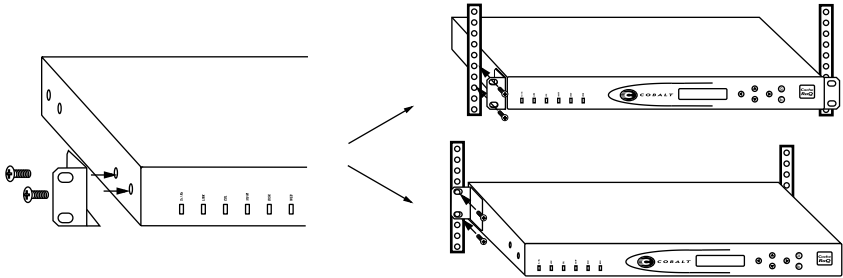
Connecting to the network

Determine which of the CacheRaQ 4's network interface(s) to use, according to the mode of operation you have chosen; see "Mode of operation" on page 11.

Connect one end of a Category 5 Ethernet cable to the 10/100 BaseT Network 1 connector on the CacheRaQ 4; see Figure 6. Connect the other end of the cable to an existing network socket.

Figure 6. Network connectors

Network connection 2 ⎯⎯⎯   ⎯⎯⎯ Network connection 1
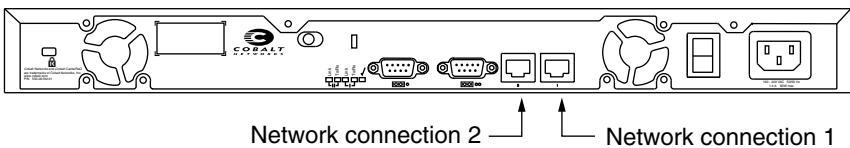
Connecting the power supply

Connect the power supply cord to the CacheRaQ 4 and to an electrical outlet (100-240 volts AC, 50/60 Hz, as listed in Appendix B, "Product Specifications").

Powering on the CacheRaQ 4

Turn on the power by pressing the **On/Off** switch on the back panel.

The hard disk spins up, the fan turns on, and the LCD screen lights up. The Cobalt logo and the Cobalt Networks name scroll across the screen.

A number of status messages are displayed on the LCD screen as the CacheRaQ 4 completes its boot process.

> *Caution:* It is important to follow the proper power-down procedure before turning off the CacheRaQ 4. Refer to "Power down" on page 58.

Configuring the CacheRaQ 4 for the network

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

The CacheRaQ 4 requires specific network information to function properly. You must enter the necessary information using the LCD console on the front panel.

Before you proceed, make sure you have the following information:

- the IP address assigned to the CacheRaQ 4

- the subnet mask of your network

- the gateway/router address (necessary only if communicating with other networks)

Using the LCD console to configure the network

Figure 7 shows the LCD console for the CacheRaQ 4.

The LCD screen on the front of the CacheRaQ 4 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 to the right of the LCD screen to enter the required network information manually.

Appendix A, "Using the LCD Console", provides more information about the LCD console.

Figure 7. LCD console

LCD screen   LCD arrow buttons
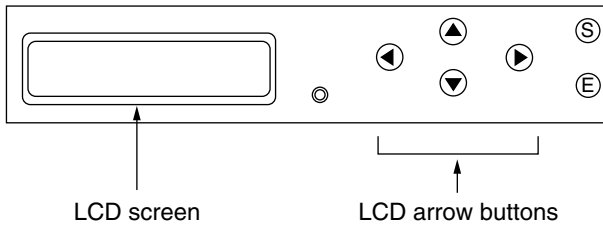
The arrow buttons function as follows:

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.

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

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

Configuring the network settings

During setup, the LCD console is used to enter network configuration information on the CacheRaQ 4.

Through the LCD console, you configure the IP addresses of the primary network interface (Network 1), the netmask and the gateway. You configure the other network settings through the browser-based user interface (UI).

Follow these steps to configure the network manually:

1. When you see the prompt

    ```
    PRIMARY IP ADDR:
    000.000.000.000
    ```

    enter the IP address assigned to the primary network interface (Network 1) of the CacheRaQ 4 using the arrow buttons on the LCD console.

2. Press (E).

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

    ```
    PRIMARY NETMASK:
    255.000.000.000
    ```

3. Enter the IP address of the netmask of your network.

4. Press (E).

    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.

6. Press (E).

    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). 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 CacheRaQ 4 completes the boot process. The LCD screen shows several messages before displaying the IP address assigned to the primary network interface of the CacheRaQ 4.

Configuration is complete when the LCD screen displays the IP address assigned to the CacheRaQ 4, for example:

```
IP ADDRESS:
192.168.25.77
```

To change the settings, see "Set up network" on page 56.

Phase 2: Setting up with the Web browser

The remainder of the setup process is performed through a Web browser on any computer on your network. Use one of the standard browsers available (for example, Netscape Navigator or Microsoft Internet Explorer, versions 4.0 or later) to do this; the browser must support HTML frames and JavaScripts. Once the setup process is complete, the CacheRaQ 4 can be managed from any computer on the network that has a browser.

To use a browser to set up the CacheRaQ 4, follow these steps:

1. Launch a standard Web browser on any computer connected to the network.

2. Enable JavaScript in your browser if you normally disable it.

3. Enter the IP address of the CacheRaQ 4 (shown on the LCD screen on the front panel) into the URL field of your browser — for example:

    Location: **http://192.168.25.77**

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

If the CacheRaQ 4's network settings were configured successfully, then the Cobalt Welcome screen appears; see Figure 8.

Click the **Start** button to begin using the Setup Wizard. A second browser window opens to the Setup Wizard.

Figure 8. CacheRaQ 4 Welcome screen
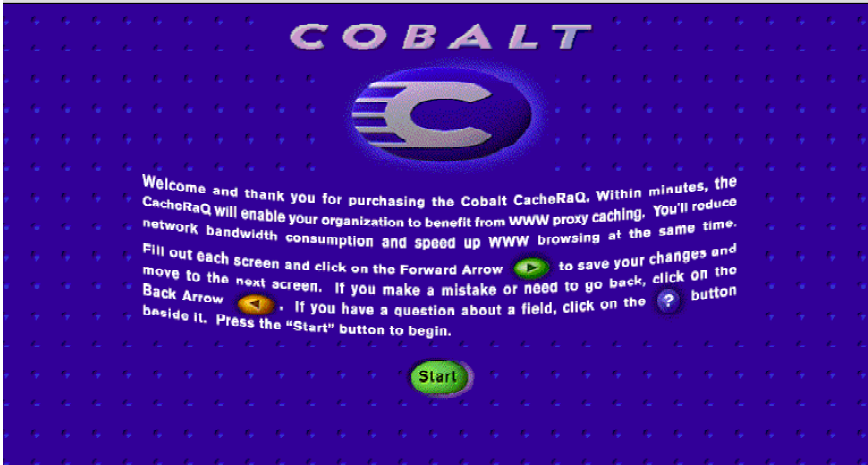
Active Assist — Online Help

Active Assist provides real-time context-sensitive help on the UI.

To access Active Assist, place the cursor over the icon beside any item. A description of the item appears at the bottom of the browser page.

Configuring the CacheRaQ 4 with the Setup Wizard

To configure the CacheRaQ 4, 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 five screens that guide you through the setup process. After completing each step, click on the **NEXT** button to apply the changes and move on to the next step. You can return to earlier screens by clicking on the **BACK** button.

The CacheRaQ 4 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 CacheRaQ 4 enters the changes in its configuration files before proceeding to the next step. Changes may take several seconds to complete.

All of the Setup Wizard configuration options can be accessed from the CacheRaQ 4's normal Web interface, so you can change or view the settings after finishing the Setup Wizard.

The Setup Wizard presents the following four steps, each with its individual screen: Cache Setup, Network Setup, Administrator Setup, and Time and Time Zone Setup. Cobalt recommends that you read through the descriptions of these screens before you begin, to make sure you have all the required information.

1. Cache setup

The **Cache Setup** screen allows you to configure the CacheRaQ 4's caching software. This screen has three tables: Cache Mode, Cache Settings and Cache Proxy Settings. See Figure 9.

Figure 9.   Cache Setup screen

Cache Mode table

The most important setting on this page is the Cache Mode. Select from among Traditional Proxy Caching mode, Transparent mode with one network interface and Transparent mode with two network interfaces. These modes are described in Chapter 1, "Introduction".

Cache Settings table

There are five fields in the Cache Settings table.

HTTP Proxy Port Number

The value for the is 3128. This is the standard port number used by Web browsers for connecting to a proxy server.

Document expiration age fraction (percentage)

A cached document expires after sitting in the cache for a specified fraction of its age. This fraction is expressed as a percentage. The age of a document is the difference in time between when the document is loaded into the cache and when the document was last modified.

The value in this field determines how often the CacheRaQ 4's caching software refreshes cached Web pages. A refresh occurs when the caching software decides that a requested document (that is already held in the cache) must be checked against the document on the original server to ensure that the cached copy of the document is up to date. The next paragraph describes the method used to determine when to refresh a document.

Cached documents are refreshed after they expire. Documents expire after they have been in the cache for a certain amount of time. This amount of time is set for each document according to the document's Last-Modified timestamp. When a document enters the cache, the CacheRaQ 4 software calculates the difference between the current time and the document's Last-Modified time. It multiplies this quantity by the value of the document expiration age fraction; the result is the amount of time that the document remains in the cache before it expires.

Consequently, a smaller value for the document expiration age fraction causes a document to expire sooner. This reduces the likelihood that an out-of-date document will be served from the cache, but it also increases the amount of HTTP traffic between the CacheRaQ 4 and the Web. For a document expiration age fraction of 10%, the likelihood that a given document is out of date when retrieved from the cache is about 1%. In practice, users' browser caches are much more likely than the CacheRaQ 4 to return out-of-date documents.

Document Maximum Time Before Expiration

This setting specifies the maximum amount of time (in hours) that a document remains in the cache before it expires. This value is used in conjunction with the value for the document expiration age fraction. A cached document expires by the earlier of the two methods: document expiration age fraction or maximum time before expiration.

Maximum Size of Cacheable Documents

This setting specifies the maximum size (in MB) for a cached document. It can prevent a very large document from evicting several small documents from the cache. A large value (for example, 20MB) is a good setting — very large documents (for example, multimedia files) can often be cached at this setting.

Disk Space for Log Files

This setting controls the amount of disk space (in MB) on the CacheRaQ 4 that is devoted to storing log files. One log file is generated each day and is used to generate the information in the Cache Statistics section of the UI.

It is recommended to enter a large value (up to one thousand MB [one GB]) in this field, enough for a one or two months of log files. If users on your network generate heavy HTTP traffic, increase this setting.

Disk Space for Usage Statistics

This setting controls the amount of disk space (in MB) dedicated to the per-client and per-server usage information that is calculated nightly. These statistics are described in more detail in the next chapter.

Cache Proxy Settings table

Enable Cache Look-ahead

This check box enables the "look-ahead" feature on the CacheRaQ 4. As the CacheRaQ 4 pulls in a Web page that a client machine has requested, it also examines the HTML code for other objects referenced from the same Web server (for example, image files). If the CacheRaQ 4 finds any objects, it requests them as well. If a user's browser subsequently requests these objects, the CacheRaQ 4 returns the pre-cached objects.

This look-ahead feature shows the greatest performance improvements on high-latency links. Normally, a client Web browser connects to a remote server to download the Web page; if the page has referenced objects, the client's browser may make a new connection to retrieve each object. With the look-ahead feature, the CacheRaQ 4 retrieves the referenced objects while the Web page is still downloading to the client's browser. With this feature enabled, the CacheRaQ 4 can retrieve multiple objects with fewer connections than if the feature is not enabled.

PAC file URL

Web clients often use proxy auto-configuration (PAC) files to forward requests to an appropriate proxy server or to determine how to redirect Web requests.

In the URL field, enter a URL specifying the location of the PAC file that the CacheRaQ 4 will use.

PAC refresh rate

You can specify the refresh rate in minutes, hours or days. This value specifies the period after which the CacheRaQ 4 re-examines the PAC file. If you enter "0" in this field, the CacheRaQ 4 retrieves the PAC file only when it is booted.

Click **NEXT** to move to the next screen.

2. Network setup

The **Network Setup** screen allows you to configure network-related settings that are not configured through the LCD console. See Figure 10.

Figure 10. Network Setup screen

Network settings

You can configure the following settings for the network:

- Host name

- Domain name

- Default gateway

- IP address of the primary DNS server

- IP address of the secondary DNS server

Network 1 interface settings

You can configure the following settings for the Network 1 interface:

- IP address

- Subnet mask

Network 2 interface settings

If you selected a configuration that requires the Network 2 interface, you can configure the following settings for the Network 2 interface:

- IP address

- Subnet mask

> *Note:* If the IP address that you assign to a secondary network interface is on the same subnet as the IP address of the primary network interface, both network interfaces must be connected to the same physical network. If they are not, the CacheRaQ 4 will not be available on the network.

You must enter the host name and domain name of the CacheRaQ 4 and the IP address for the primary DNS server. If you are not the network administrator, you can obtain the correct values for these fields from your network administrator. You can also configure the Network 2 IP address and subnet mask, if your configuration requires the use of the second network interface. Finally, you can configure the default Gateway IP address.

An optional CacheRaQ 4 feature is to run a local caching-only DNS server. If you enter 127.0.0.1 as the IP address of the primary DNS server, the local caching-only DNS server is enabled. You may wish to run the local DNS server if, for example, your normal DNS server is not in close network proximity to your CacheRaQ 4.

The **Network Setup** screen also displays the media access control (MAC) addresses of the two network interfaces. You cannot change the MAC addresses.

When you have entered the required information on the Network Setup screen, click **NEXT** to move to the next screen.

3. Administrator setup

The **Administrator Setup** screen appears. The CacheRaQ 4 has an Administrator user for performing normal administrative and maintenance tasks. These tasks are performed through the UI. You must authenticate yourself as user name *admin* before you can access the administrative functions.

The **Administrator Setup** screen lets you enter the administrator password, enter a full name for the *admin* user and specify an email address that the CacheRaQ 4 can use to notify the Administrator of any problems that might arise.

The Password field on this screen is mandatory; the other fields are optional. See Figure 11.

Figure 11. Administrator Setup screen

Password guidelines

Use the following guidelines when choosing a password:

1. Use between six and eight alphanumeric characters; you can use a password with more than eight characters, but Linux truncates the password at eight characters and verifies the password against those eight characters only.

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

    a. Use both upper- and lower-case letters. A password is case-sensitive.

    b. Do not use a proper name.

    c. Do not use a word found in a dictionary.

    d. Do not use a date.

    e. Do not use a command word.

    f. Do not use a string of consecutive keys on a keyboard (for example, "qwerty").

If you forget or want to reset the admin password, see "Resetting the Admin Password" in Appendix A.

Advanced administration is possible by logging in to the CacheRaQ 4 through a telnet session. Log in as user *root* with the password you assigned to *admin* on this setup page.

Click the **NEXT** button to move to the next screen.

4. Time setup

The **Time Setup** screen appears. On this screen, you enter time and time zone information. It is important to enter the correct values here to ensure that the nightly log-file rotation and statistics programs run at the correct times. See Figure 12.

Choose the correct settings from the pull-down menus on this screen.

When you are finished, click **NEXT**.

Figure 12. Time Setup screen

5. Registration

The **Product Registration** screen appears; see Figure 13. If you are connected to the Internet, you can register the CacheRaQ 4 by completing the online registration.

Note: If you are not yet connected to the Internet, you cannot register online.

Figure 13. Registration screen

If you are not connected to the Internet, this screen does not appear. Fill out the registration card included in the packaging materials and return it to Cobalt Networks, Inc. By doing so, you will receive notifications of system and security upgrades and new product information.

Cobalt Networks, Inc.
555 Ellis Street
Mountain View, CA
USA   94043

If the CacheRaQ 4 has been configured with a functional gateway and a functional DNS server, you can register your CacheRaQ 4 through email using the online registration form displayed in the Setup Wizard.

If not, use the printed registration card that came in the CacheRaQ 4 box. It is recommended that you register your CacheRaQ 4 so that you can be notified of software updates (including patches for bug fixes), new product information, special promotions and so on.

Click **FINISH** to finish the Setup Wizard configuration. Once this is complete, your CacheRaQ 4 is ready for operation.

CacheRaQ 4 Administration

This chapter describes the Cobalt CacheRaQ 4's administrative functions, which are available through the Web interface. This interface includes the following items:

- Home
- Network setup
- Cache setup
- Filter setup
- Report setup
- Cache statistics
- Cache logs
- Network usage
- CPU usage
- Maintenance

Home

The Home button takes you to a default home page that describes the CacheRaQ 4. See Figure 14.

Figure 14. CacheRaQ 4 home page
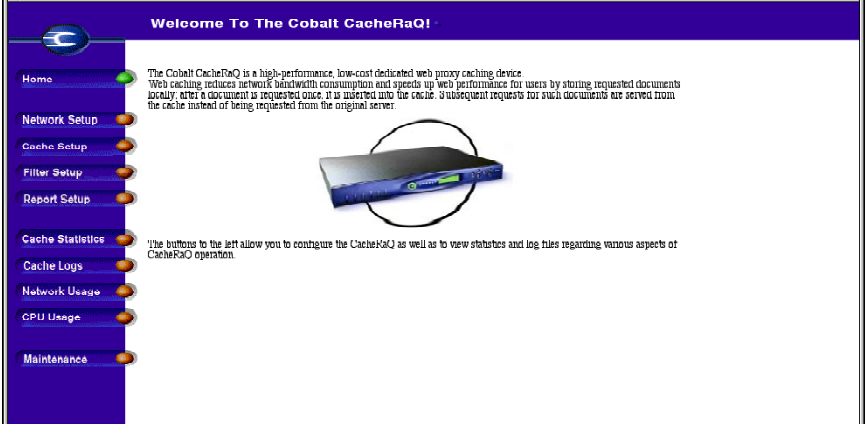
Network setup

The Network Setup screen (see Figure 15) is the same as described in the Setup Wizard. For information on this screen, see "2. Network setup" on page 24.

Figure 15. Network Setup screen
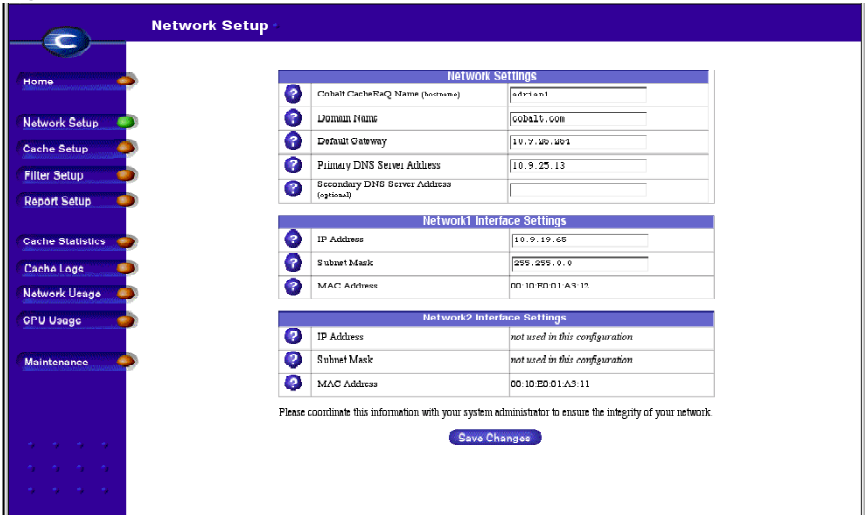
Cache setup

The first seven options on the **Cache Setup** screen—Cache Mode, HTTP Proxy Port Number, Documentation Expiration Age Fraction, Maximum Time Before Expire, Maximum Size of Cacheable Documents, Disk Space for Log Files and Disk Space of Usage Statistics—also appear in the Setup Wizard; see Figure 16. These options are described in "1. Cache setup" on page 20.

The **Cache Setup** screen presents some additional configuration options that are not in the Setup Wizard. This section describes the additional options:

- Cache Cluster settings

- Inter-Cache Communication Protocol (ICP) settings

- Web Cache Communication Protocol (WCCP) settings

- Disable Caching feature

The following two buttons are available on the main **Cache Setup** screen.

Empty Cache Now

If you need to empty the CacheRaQ 4's document cache, click **Empty Cache Now**.

Normally, this feature is not necessary because the CacheRaQ 4's caching software manages its own disk storage by removing old, infrequently requested documents when the available disk space is low.

Delete All Stats Now

This option removes all log files and statistics files stored on the CacheRaQ 4.

Figure 16. Cache configuration screen

Cache Cluster settings

To access the Cache Cluster Master Settings, click **Cluster** at the top. The Cache Cluster Master Settings table appears. See Figure 17.

This option lets you configure the CacheRaQ 4 as a Cluster Master. To do this, you simply enter the host names (or IP addresses) of Cluster Slaves in the fields marked "Cluster Slave 1", "Cluster Slave 2" and so on. Ensure that the specified Cluster Slaves are on the network and are up and running. Ensure also that the *admin* password on the Cluster Slaves is the same as the admin password on the Cluster Master. This is necessary for the Cluster Master to retrieve statistics data from the Cluster Slaves. For optimal performance, configure the Cluster Slaves for Traditional Proxy Caching only (that is, do not enable Transparent Caching on the Cluster Slaves).

The Cluster Master can operate in any caching mode — Traditional Proxy Caching mode or Transparent mode with one or two network interfaces. In Transparent Caching mode, all client traffic should be routed through the Cluster Master, just as if the Cluster Master were a standalone CacheRaQ 4 operating in Transparent mode.

If you make any changes, click **Save Changes** before leaving this screen.

Figure 17. Cache Cluster configuration screen

Inter-Cache Communication Protocol (ICP) settings

To access the ICP Settings, click **ICP** at the top. The Peer Settings table appears; see Figure 18.

Figure 18. ICP configuration screen

ICP is an Internet protocol used to create cache hierarchies. A cache hierarchy is a collection of caching proxy servers organized in a logical parent/child and sibling arrangement so that cache servers closest to Internet gateways (closest to the backbone transit entry-points) act as parents to cache servers at locations farther from the backbone. The parent cache server resolves "misses" for its children. In other words, when a cache requests an object from its parent, and the parent does not have the object in its cache, the parent fetches the object, caches it and delivers it to the child. This ensures that the hierarchy achieves the maximum reduction in bandwidth utilization on the backbone transit links, helps reduce load on Internet information servers outside the network served by the hierarchy, and builds a rich cache on the parent cache servers so that the other child cache servers in the hierarchy obtain better "hit" rates against their parents.

Figure 19 shows a parent/child configuration of cache servers.

Figure 19. Parent/child configuration
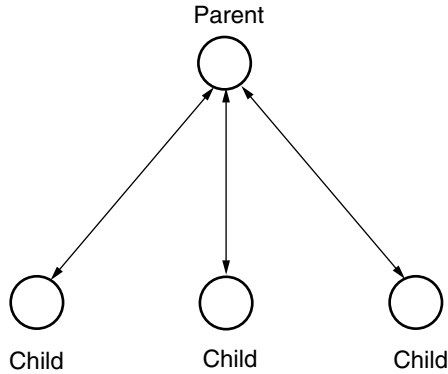
In addition to the parent-child relationships, the CacheRaQ 4 supports the notion of siblings. Siblings are cache servers at the same level in the hierarchy, provided to distribute cache server load. Each cache in the hierarchy independently decides whether to fetch the reference from the object's home site or from parent or sibling caches, using a simple resolution protocol. Siblings do not fetch an object for another sibling to resolve a cache "miss".

Figure 20 shows a sibling configuration of cache servers.

Figure 20. Sibling configuration
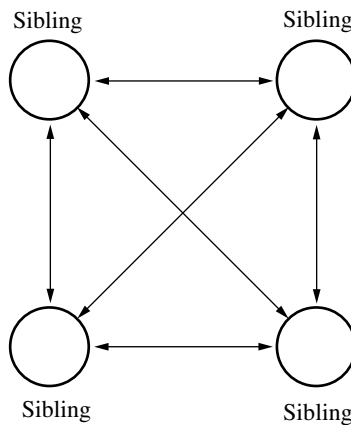
The Peer Settings table allows you to configure ICP peer hosts for the CacheRaQ 4. You may wish to configure ICP if, for example, your Internet service provider (ISP) operates an ICP-compliant cache with which you want to peer. In the Peer Settings table, specify the following information for each peer: the peer host name, an indication of whether the peer is a "parent" or a "sibling" (in ICP terminology), and the HTTP and ICP port numbers to use for the specified peer.

The default ICP port number is 3130.

Proxy-only and no-query options

There are two other configuration options for a peer: "proxy-only" and "no-query".

If the "proxy-only" option is enabled and the CacheRaQ 4 receives an object from elsewhere, the CacheRaQ 4 passes the object to the client but does not keep a copy in its cache. If the "proxy-only" option is not enabled, the CacheRaQ 4 caches the object that it receives.

If the "no-query" option is enabled, the CacheRaQ 4 does not ask the other cache servers if it has an object; it simply forwards the request and waits for a response.

If the "no-query" option is not enabled, the CacheRaQ 4 asks its parent or siblings if it has the object. If the CacheRaQ 4 receives a negative response, it continues asking the other peers in a round-robin format. If none of the other cache servers has the object, the CacheRaQ 4 retrieves the object itself.

Cache Clustering can be used in conjunction with ICP in the following way: Configure the Cluster Master as described in "Cache Cluster settings" on page 34, but do not configure any ICP peers for it. On the Cluster Slaves, configure the desired ICP peers as described in the previous paragraph. With this configuration, the Cluster Master sends all requests (as usual) to the Cluster Slaves, which then query the ICP peers that have been configured.

If you make any changes, click **Save Changes** before leaving this screen.

Web Cache Communication Protocol v1 (WCCP)

To access the WCCP Settings, click **WCCP** at the top. The WCCP Settings table appears.

WCCP allows the CacheRaQ 4 to communicate with a WCCP-enabled router (usually a piece of equipment from Cisco Systems®) and to be integrated into a WCCP-enabled network.

> *Note:* The CacheRaQ 4 only supports version 1 (v1) of the Web Cache Communication Protocol.

With WCCP v1, a single router services a cluster; this router is the device that redirects all IP packets.

The following sequence of events details how WCCP v1 configuration works:

1. Each cache server is configured by the system administrator with the IP address of the control router. Up to 32 cache servers can connect to a single control router.

2. A cache server transmits its IP address to the control router using WCCP, indicating its presence. Routers and cache servers communicate to each other through a control channel; this channel is based on UDP port 2048.

3. This information is used by the control router to create a cluster view (a list of caches in the cluster). This view is transmitted to each cache in the cluster, essentially making all the cache servers aware of each other. A stable view is established after the membership of the cluster remains the same for a certain amount of time.

4. Once a stable view has been established, one cache server is elected as the *lead cache server*. The lead is defined as the cache server with the lowest IP address that is seen by all the cache servers in the cluster. This lead cache engine uses WCCP to indicate to the control router how to redirect the IP packets. Specifically, the lead cache engine designates how redirected traffic should be distributed across the cache servers in the cluster.

To configure the WCCP-enabled router, refer to the manufacturer's documentation.

In the WCCP Router field, enter the fully qualified host name or the IP address of the WCCP v1 router.

If you make any changes, click **Save Changes** before leaving this screen.

Disable Caching

Note: The Disable Caching feature is available only when clients are using the CacheRaQ 4 in Transparent Caching mode.

Occasionally, CacheRaQ 4 users may have trouble accessing certain Web sites through the cache. This is often due to authentication schemes in which the server-side software authenticates users based on the IP address from which the user connects to the server. Schemes of this nature do not work with caches because the server software receives requests from the cache's IP address rather than from the clients' IP addresses.

Caching can be disabled for specific server addresses. Both individual server hosts or server networks can be configured not to be cached. Additionally, specific client addresses (hosts or networks) can also be configured not to be cached.

To disable caching for a specific host or network, click **Disable Caching** at the top. A table appears listing (if any) the hosts or networks whose traffic is not cached.

If there are entries in the table, you can modify an entry by clicking the green pencil icon or delete an entry by clicking the brown traschcan icon.

To configure a new host or network for which you want to disable caching, click **Add Entry** above the table. See Figure 21.

When you add an entry, the following items are required:

- **Host or Network number (IP address)**. This is the address of the host or network whose HTTP traffic you do not want to cache.

- **Subnet mask for this host or network**. This is the subnet mask for the host or network. Common values are 255.255.255.255 for a single host and 255.255.255.0 for a class C network.

- **HTTP Client(s) or HTTP Server(s)**. Choose Client Network/Host from the pull-down menu to avoid caching HTTP traffic that originates from the specified host or network. Choose Server Network/Host from the pull-down menu to avoid caching HTTP traffic that is destined for the specified host or network.

When you are finished, click **Save Changes**. The table reappears with the new entry.

Figure 21. Add Entry screen for Disable Caching feature

Filter setup

The CacheRaQ 4 is capable of filtering HTTP traffic that passes through it. The Filter Setup screen allows you to choose among three options. See Figure 22.

- **No Filtering**. The CacheRaQ 4 allows all HTTP traffic. This is the default option.

- **Deny Access**. The CacheRaQ 4 blocks access to specified sites and URLs.

- **Limit Access**. The CacheRaQ 4 blocks access to all sites and URLs except ones that are explicitly specified. This can be useful in environments (for example, educational environments) where only specific sites are intended to be accessed.

If you use the Deny Access or Limit Access modes, enter the list of relevant sites (server names or IP addresses) and URLs into the text window on this screen. Click **Save Changes** at the bottom to activate your filtering configuration.

Figure 22. Filter Setup screen
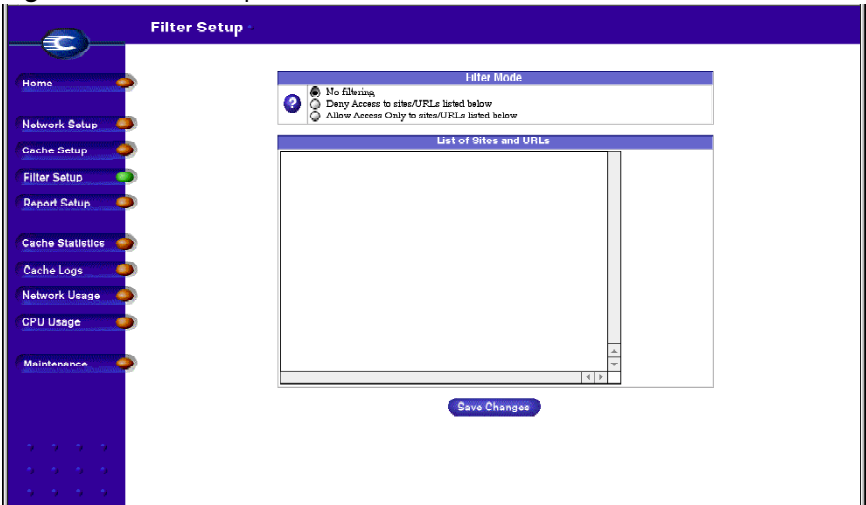
Report setup

You can configure optional email reports that the system sends nightly to the *admin* user. Email messages to the *admin* user can be forwarded to an arbitrary email address. See "Maintenance" on page 50 for information about how to configure the *admin* email alias.

Email Report settings

You can enable two types of email reports:

•   **Usage Report**. This report lists the names of client machines and server machines that have retrieved (or served, in the case of servers) more than a specified number of documents or more than a specified number of total bytes of content. For information on the thresholds, see "Threshold settings" on page 44.

•   **Summary Statistics**. This report describes cache performance in terms of traffic through the cache, documents through the cache, cache hit and miss response times, and so on.

    This information is identical to the Summary Statistics information available in the Cache Statistics section (described in "Summary Statistics" on page 45). The Summary Statistics output also includes three graphs. These graphs illustrate the number of requests as a function of time of day, the number of cache hits versus cache misses as a function of time of day, and the average cache hit latency versus average cache miss latency as a function of time of day.

Threshold settings

You can set four thresholds for generating reports: bytes per client, documents per client, bytes per server and documents per server.

In each of these fields, enter a value beyond which the CacheRaQ 4 generates a report.

To list all clients or servers (or both) in a report, enter "0" in these fields.

Figure 23 shows the Report Setup screen.

Figure 23. Report Setup screen

Cache statistics

The CacheRaQ 4's caching software records information on all HTTP requests it receives. Statistics are calculated nightly from this data and are available on a daily basis for the current month and the preceding month.

To use the Cache Statistics page, you first set the parameters for the statistics you want to view and then you generate the statistics.

- Select the type of statistics you want to display: summary statistics, all clients, a specific client, all servers or a specific server. For more information on the last four options, see "Usage statistics" on page 47.

    You can also choose to have all servers from the same domain listed as one server. For example, www10.cobalt.com, www42.cobalt.com, and www53.cobalt.com would all be listed under the single entry cobalt.com. To enable this option, click the check box *Combine server names into single domain.*

- Sort the result by bytes or by requests.

- Indicate the number of results to return.

- Specify a time period for which you want to see the statistics. You can select an arbitrary combination of days from the last two months for which you want to see statistics. You can also enter a time value (in minutes, seconds or hours) to have statistics calculated for the immediate past for the amount of time you have specified (up to the start of the current day).

There are two main types of statistics available: *summary statistics* and *usage statistics*.

Summary Statistics

This option displays the following information for the time period you specify:

- **Number of clients**. This is the number of unique client IP addresses that made requests through the CacheRaQ 4.

- **Number of cache hits**. A *cache hit* is a request in which the requested document was delivered from the cache — the document did not have to be retrieved from the original server.

- **Number of cache misses**. A *cache miss* is a request in which the requested document was not in the cache and had to be retrieved from the original server.

- **Total number of documents sent to clients**

- **Number of bytes sent to clients from cache hits**

- **Number of bytes sent to clients from cache misses**

- **Total number of bytes sent to clients**

- **Average cache hit object size**. This is the average document size for documents which were delivered from the cache.

- **Average cache miss object size**. This is the average document size for documents which had to be retrieved from their original servers.

- **Cache hit rate**. This number refers to the ratio of cache hits to total cache requests.

- **Bandwidth savings**. This number reflects the amount of client HTTP traffic (as a percentage) that was avoided because the documents were available in the cache, thus saving network bandwidth.

- **Average cache hit latency**. This is the average amount of time (in seconds) it took the CacheRaQ 4 to deliver a document from its cache to a client. The time measured is the difference between the time that the CacheRaQ 4 receives the request initially to the time that the CacheRaQ 4 has finished sending the complete object to the client.

- **Average cache miss latency**. This is the average amount of time it took the CacheRaQ 4 to deliver a document that had to be retrieved from the original server. It is calculated similarly to the cache hit latency (above), except that only cache misses are considered.

- **Weighted average request latency**. This value is calculated by the following formula:

  (Average cache hit latency X Cache hit rate) + (Average cache miss latency X Cache miss rate).

  The cache miss rate is equal to 1 minus the cache hit rate.

- **Request speedup**. This number quantifies the CacheRaQ 4's performance improvement in terms of user-perceived latency. It is the ratio of cache miss latency to the weighted average request latency.

The Summary Statistics output also includes three graphs. These graphs illustrate:

1. the number of client HTTP requests versus the number of cache hits as a function of time of day

2. the total amount of traffic (Kb) to clients versus the amount of traffic (Kb) to clients from the cache as a function of time of day

3. the average cache hit latency versus the average cache miss latency as a function of time of day

Usage statistics

Four options let you view HTTP traffic statistics for individual clients (users) and individual HTTP servers. Each option returns a list of client or server host names, and for each host name, a count of documents sent by a server or received by a client and a count of bytes sent by a server or received by a client.

- **All clients**. This option returns a list of clients that requested documents through the CacheRaQ 4. The list contains the number of bytes sent to each client and the number of documents sent to each client.

- **A specific client**. For a specified client host name or IP address, this option returns a list of servers accessed by this client.

- **All servers**. This option returns a list of all servers that were accessed by one or more clients through the CacheRaQ 4.

- **A specific server**. For a specified server host name or IP address, this option returns a list of clients who made requests for documents on that server.

Each of the above options can be sorted by number of documents or by number of bytes. Finally, you can specify the number of sites to be displayed by each of the above options.

> *Note:* The statistics can take some time to calculate. This is particularly true of statistics for the current day, which must be calculated from the raw *access.log* file.

Cache logs

The CacheRaQ 4's caching software logs data to two files in its normal course of operation—access.log and cache.log.

- **Access.log** contains one line per request served. Among other things, each line lists the URL of the requested document, the client's IP address, the size of the document and the time of the request. Access.log files can grow quite large (up to approximately 100 MB per day). The amount of disk storage devoted to access.log files can be set in the Cache Settings page, as described in "1. Cache setup" on page 20.

- **Cache.log** contains informational messages describing the state of the cache software. Cache.log also lists error messages that arise during normal operation. For example, a message is logged whenever the caching software fails to connect to a remote HTTP server.

Software on the CacheRaQ 4 rotates the access.log and cache.log files once per day. Log files are saved until they exceed the disk space allocation for log files. At this point, old log files are deleted until disk space consumption is within the specified limit.

The Cache Logs screen offers two options: **View Logs**, for viewing the current day's log files and **Download Logs**, for downloading log files from previous days.

- **View Log Files**. This page lets you select a log file (access.log or cache.log) and enter a number of lines (N). It then displays the most recent N lines of the selected log file. This is useful for diagnosing any immediate problems (by viewing cache.log) and for examining current client activity (by viewing access.log).

- **Download Log Files**. This page lets you download entire log files on a daily basis—it lists all the available access.log and cache.log files from previous days. To download a log file through your browser, shift-click the filename. You can also click a file to view it but keep in mind that these files (particularly access.log) can be quite large and therefore may be cumbersome to display in a Web browser.

Network usage

The Network Usage screen shows statistics for network packets sent and received on the CacheRaQ 4's two network interfaces; see Figure 24. If an interface is not used, the statistics are displayed as "0" for that interface.

Packets are counted in the following categories:

- **Good**. A packet was received or sent without error.

- **Error**. A send or receive error occurred that is not covered by the two following categories.

- **Dropped**. A packet was ignored (dropped) by the operating system because of a temporary lack of buffer memory.

- **Collisions**. The CacheRaQ 4 attempted to transmit a packet while another host was in the process of transmitting a packet. A high rate of collisions relative to packets sent indicates a potentially overloaded network.

Figure 24. Network Usage screen
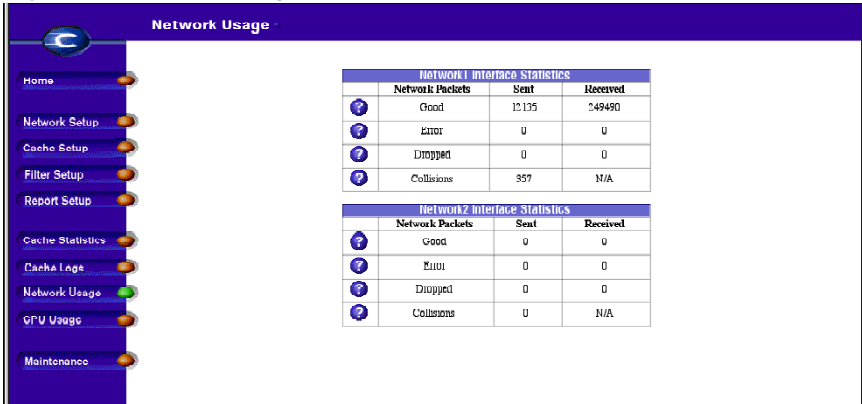
CPU usage

This screen displays a graph of the CacheRaQ 4's *load average* as it varies over time. The load average is a rough indicator of overall system activity. Generally, a high load average indicates a busy system. A CacheRaQ 4 with a load average that routinely exceeds 1.0 may be overloaded—a Cache Cluster might be appropriate for the workload in this situation.

Contact Cobalt Networks Technical Support for diagnostic assistance if you believe your CacheRaQ 4 is overloaded (see "Customer Service and Technical Support" on page 6).

Maintenance

The Maintenance section combines three unrelated maintenance features.

Admin Setup

This screen lets you configure the CacheRaQ 4 Administrator password (which is required) and an external email address that will receive mail to the *admin* user (this email address is optional). Email reports (described in "Report setup" on page 43) are sent to *admin*, so use the Admin Setup page to set the real email address to which you want the reports sent.

1. Click **Maintenance** on the left. The Administrator Settings table appears; see Figure 25.

2. Enter the following information in the table.

   a. the full name of the Administrator

   b. the user name is set as *admin*

   c. the administrator password (see "Password guidelines" on page 27)

   d. (optional) an email address to which the CacheRaQ 4 sends email if it detects problems that require administrative intervention. Email Reports, if configured, are also sent to this address.

3. Click **Save Changes**.

Figure 25. Admin Setup screen

Time Setup

This screen lets you set the time and time zone on the CacheRaQ 4.

It is important to set the time correctly, because the CacheRaQ 4 software rotates the log files and generates the statistics shortly after midnight each day. This time is chosen because it is close to the start of the day. This way, each day's log files and statistics accurately reflect the actual usage that occurred on the corresponding calendar day.

1. Click **Maintenance** on the left. The Administrator Settings table appears.

2. Click **Time** at the top. The Time Settings table appears; see Figure 26.

3. Choose the correct settings from the pull-down menus on this screen.

4. As an option, you can also specify the name of a Network Time Protocol (NTP) server with which the CacheRaQ 4 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 26. Time Setup screen

Upgrade Software

From time to time, Cobalt Networks, Inc. issues updates to critical software that runs on its products. Updates can be obtained from the Cobalt Networks Web page (http://www.cobalt.com). Updates come in the form of a "package" file with a ".pkg" file name suffix. The **Update Software** screen allows you to install new packages on the CacheRaQ 4; see Figure 27.

Installing a package file

To install a package file:

1. Obtain the .pkg file from the Cobalt Networks Web site at
   http://www.cobalt.com/support/download/index.html.

2. Save the .pkg file on the computer on which you run your Web browser.

3. On the CacheRaQ 4 UI, click **Maintenance** on the left. The Administrator Settings table appears.

4. Click **Upgrade Software** at the top. The Upgrade Software and Software on the Cobalt CacheRaQ 4 tables appear.

5. The Upgrade Software table offers three options for selecting a file.

   a. To install a .pkg file referenced by a URL, enter the URL into the URL field.

   b. To upload a .pkg file from your computer, enter the path and file name or click **Browse...** to search for the file on our computer.

   c. The *admin* user can also use FTP to upload packages to the directory /home/packages and then install them using the Loaded: option.

      To do so, the *admin* must first telnet in to the CacheRaQ 4 and then FTP out to get the package file. By default, you cannot FTP in to the CacheRaQ 4.

6. Enter the *admin* password and click **Install a '.pkg' Package**. The admin password is required as a security precaution.

Once the package is installed, the system may prompt you through the UI to reboot the CacheRaQ 4. Some packages require you to reboot the system for the new software package to take effect.

Cobalt recommends that you reboot the server now. You can choose not to reboot, but the new software will not come into effect and it may stop some processes from running.

Figure 27. Upgrade Software screen
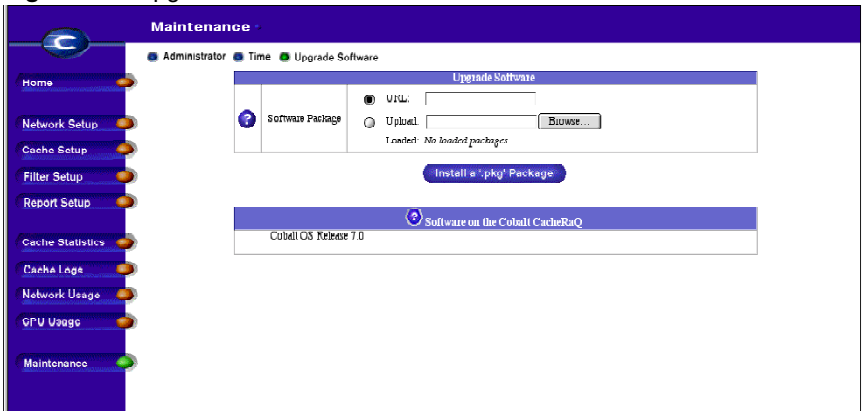
Using the LCD Console

During startup, the LCD screen on the front panel of the CacheRaQ 4 displays status information about the boot process itself.

When setting up the CacheRaQ 4, you use the LCD console to enter network configuration information for the CacheRaQ 4.

Once the CacheRaQ 4 is running, the LCD console serves several purposes. Through the LCD console, you can:

• change the network configuration information, which is useful if you change the location of the CacheRaQ 4

• reboot, which restarts the entire CacheRaQ 4

• power down in a way that allows the CacheRaQ 4 to close all open files, and minimizes startup time the next time the CacheRaQ 4 is powered on

• reset the network, which resets all IP addresses, netmasks and other network settings to that of a new, unconfigured system

• exit from the LCD commands without making any changes

> ☞ *IMPORTANT:* Before turning off the CacheRaQ 4, follow the proper power-down procedure, as described in "Power down" on page 58

You access each of these functions by holding down the Ⓢ (select) button for approximately two seconds. This action causes the LCD screen to enter its function mode. Press the Ⓢ 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 Ⓔ (enter) 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 two 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.

    If you select Save, the CacheRaQ 4 reboots using the new network configuration. If you select Cancel, you return to step 1 of this procedure.

10. Press the (E) button.

Reboot

To reboot the CacheRaQ 4:

1. On the LCD console, hold down the (S) button for approximately two 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. The CacheRaQ 4 reboots.

Power down

![warning triangle] *Caution:* To prevent the potential loss of data, it is important to follow the proper power-down procedure before turning off the CacheRaQ 4.

To power down the CacheRaQ 4:

1. On the LCD console, hold down the (S) button for approximately two seconds. The LCD screen displays:

    ```
    SELECT:
    SETUP NETWORK
    ```

2. Press the (S) button until **Power down** appears in the LCD screen:

    ```
    SELECT:
    POWER DOWN
    ```

3. Press the (E) button.

4. Use the arrow buttons to toggle the cursor between [Y] and [N]. Select [Y] to power down the system.

    The **OK to Power Off** light on the back panel blinks. The LCD screen displays:

    ```
    PLEASE SWITCH
    POWER OFF NOW
    ```

5. Toggle the **On/Off** switch on the back panel to the **Off** position.

Reset network

The Reset Network function resets the host name, IP address, subnet mask, gateway and DNS information to that of a new, unconfigured system. This function is useful if you are moving the CacheRaQ 4 to a new network.

To reset the CacheRaQ 4 to a factory-fresh state:

1. On the LCD console, hold down the (S) button for approximately two seconds. The LCD screen displays:

   ```
   SELECT:
   SETUP NETWORK
   ```

2. Press the (S) button until **Reset network** appears in the LCD screen:

   ```
   SELECT:
   RESET NETWORK
   ```

3. Press the (E) button.

4. Use the arrow buttons to toggle the cursor between [Y] and [N]. Select [Y] to reset the network configuration.

5. Press the (E) button.

   After resetting, the CacheRaQ 4 powers down. The **OK to Power Off** light on the back panel blinks. The LCD screen displays:

   ```
   PLEASE SWITCH
   POWER OFF NOW
   ```

Resetting the CacheRaQ 4 Administrator password

☞ **IMPORTANT:** After you clear the password, enter a new one as soon as possible to protect the security of the CacheRaQ 4. At this point, anyone on the network can assign the CacheRaQ 4 Administrator password until you assign a new one.

If you forget the CacheRaQ 4 Administrator password, you can clear it by following these steps.

1. Push and hold the end of a paper clip in the recessed Reset Password button (located between the LCD screen and the LCD arrow buttons, on the front of the CacheRaQ 4). Hold the button in for approximately two seconds.

    The LCD screen displays:

    ```
    Resetting admin
    password...
    ```

2. Release the button.

3. In your Web browser, enter the URL http://<IP address>/admin/ or http://<host name>/admin/ to access the CacheRaQ 4 UI.

4. If a prompt appears asking for a user name or password, enter "admin" as the user name. DO NOT enter a password. Click **OK**.

5. Click **Maintenance** on the left. The Administrator Setting table appears.

6. Enter the password twice to ensure that you have entered it as intended. The CacheRaQ 4 supports long passwords through the UI.

    For guidelines on choosing a password, see "Password guidelines" on page 27.

7. Click **Save Changes**.

Product Specifications

Caching features

- Caches HTTP and FTP traffic (only HTTP traffic is cached in transparent mode)

- Configurable for both Transparent Caching and Traditional Proxy Caching mode

- Supports HTTP/1.1 persistent connections (keep-alives)

- Domain Name System (DNS) caching (optional DNS server in caching-only mode)

- Inter-Cache Communication Protocol (ICP) support

- Web Cache Communication Protocol (WCCP) support

- Supports SSL tunneling and cookies

- Persistent cache across reboots

- Log files compatible with Harvest, Squid and CERN Proxy standards (log files can be downloaded through the browser-based user interface)

Performance

- Supports one or two T1 or E1 lines

- Supports 200 simultaneous requests

- Scalability through Cobalt InstaCache Clustering

- Built-in support for Level 4 switching for scalability and failover protection

- Stores meta-data and hot objects in RAM for fast cache lookups

System Management

Browser-based user interface

- Compatible with Netscape Navigator, version 4.7 or later, or Microsoft Internet Explorer, version 5.0 or later

- Setup Wizard for initial setup

- Password protection for browser-based user interface (UI)

- Online Active Assist real-time help

- Advanced management through telnet

Reporting and logging of performance and usage

- Detailed event logging and Web-based statistical reporting (see "Cache statistics" on page 45)

- Optional nightly email reports

- Complete log files available for download

- Automatic log file rotation

- Simple Network Management Protocol (SNMP) agent

Active Monitor

- Real-time pro-active system maintenance daemons

- Email alerts

Cache configuration settings

- User-definable parameters for refreshing cached documents

- User-definable maximum size for a cacheable object

Miscellaneous

- Automatic system restart (after power outage and restore)

- Browser-based utility for software upgrades

- Year-2000 compliant

Hardware

The CacheRaQ 4 has the following hardware components.

- x86-compatible superscalar processor
- 64-MB to 512-MB PC-100 SDRAM DIMMs (2 slots)
  (3.3 v, 168-pin, non-parity, unbuffered)
- One internal Ultra ATA/33 hard drive
- Two 10/100 BaseT ethernet network interfaces
- Dual serial console interface
- LCD console for easy set-up and administration

Software

The CacheRaQ 4 has the following software features.

Features

- Linux 2.2 multitasking operating system
- Telnet access
- Domain Name System (DNS) server
- NTP client support

System management

- Simple Network Management Protocol (SNMP) management support
- Browser-based Setup Wizard
- Browser-based server management
- Online ActiveAssist real-time help
- ActiveMonitor maintenance agents
- Advanced management using telnet
- Web-based performance and usage reporting
- Browser-based software upgrade

Physical data

The CacheRaQ 4 has the following physical characteristics.

- Dimensions: 17.00 in. x 12.50 in. x 1.75 in. (43.2 cm x 31.8 cm x 4.5 cm; fits in a standard single-unit, 19-in. equipment rack)

- Weight: 9 lbs. 3 oz. (4.2 kg)

- Power requirements: Input rating 100-240 V, 50/60 Hz

- Power consumption: 45 watts

- Operating environment:

    32°F to 95°F (0°C to 35°C)

    10% to 90% humidity (non-condensing)

- Non-operating environment:

    14°F to 122°F (-10°C to 50°C)

    5% to 93% humidity (non-condensing)

- Light-emitting diodes (LEDs): Power, Transmit/Receive, Link, Collision, 100 Mbit Operation, Disk Activity, Web Activity, OK to Power Off

Regulatory approval

- CISPR 22B

- VCCI-B

- UL

- C-UL

- TUV

- CE

- Austel

- BSMI/BCIQ

- RRL

Sample Network Topologies

This appendix shows how the Cobalt CacheRaQ 4 can be used in a variety of ways in different network environments. It illustrates the connections among the network components and gives configuration details for each setup.

Traditional Proxy Caching mode
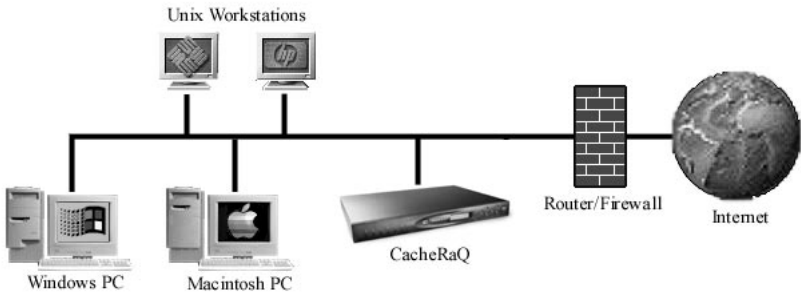
Installation notes

•   Configure the CacheRaQ 4 for Traditional Proxy Caching mode.

•   Configure the clients' browsers to use the CacheRaQ 4 as the HTTP proxy.

Instructions for Internet Explorer Version 5.0

1.   From the Tools menu, choose Internet Options.

2.   Click the Connection tab.

3.   Click the LAN Settings button at the bottom.

4.   In the Proxy Server section, click the check box for "Use a proxy server".

5.   In the Address field, enter the URL **http://<cacheraq-name>/proxy.pac**.

Instructions for Netscape Navigator Version 4.7

1. From the Edit menu, choose Preferences.

2. In the Category list, click Advanced.

3. Under the Advanced list, click Proxies.

4. Click the radio button for Automatic Proxy Configuration.

5. In the URL field, enter **http://<cacheraq-name>/proxy.pac**.

Advantage

• If the CacheRaQ 4 fails, the outside network is still accessible (contrast this with Transparent Caching mode discussed later).

Disadvantage

• You must change the browser configuration for each client.

Transparent Caching mode using one network interface
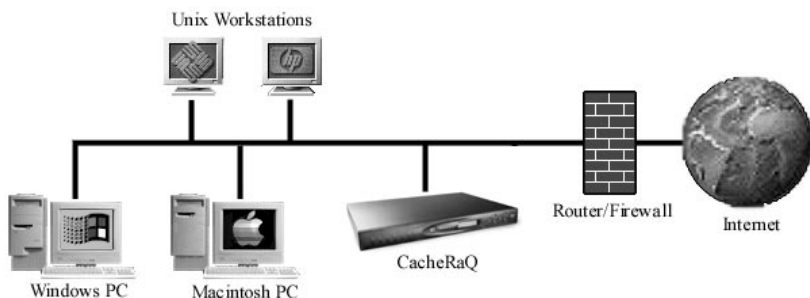
Installation notes

• To avoid changes to the clients' configuration, assign the existing gateway address used by the clients to the CacheRaQ 4's Network 1 interface.

• Assign a new IP address to the router/firewall.

• Use the new IP address of the router/firewall as the gateway setting on the CacheRaQ 4.

Advantage

• The client machines do not require a special configuration.

Disadvantage

• If the CacheRaQ 4 fails, the clients cannot access the outside network until the CacheRaQ 4 comes back online.

However, if the clients can be configured with multiple gateway addresses, you can configure them with the new IP address for the router/firewall. The clients can then use this address if the CacheRaQ 4 fails.

Transparent Caching mode using two network interfaces
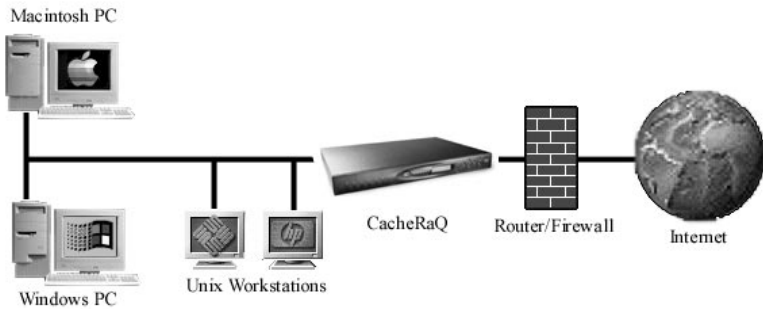
Installation notes

• To avoid changes to the clients' configuration, assign the existing gateway address used by the clients to the CacheRaQ 4's Network 2 interface.

• Create a new subnet containing two hosts: the router (assign it a new IP address) and the CacheRaQ 4's Network 1 interface. Ensure that the IP addresses you assign to the router and to Network 1 are on a subnet different from the clients' network. This is necessary for the CacheRaQ 4 to pass traffic through from the clients to the router.

Advantages

• The client machines do not require a special configuration.

• All traffic is forced through the CacheRaQ 4, so precise logs and statistics can be generated.

Disadvantage

• If the CacheRaQ 4 fails, the clients cannot access the outside network until the CacheRaQ 4 comes back online.

CacheRaQ 4 for workgroups
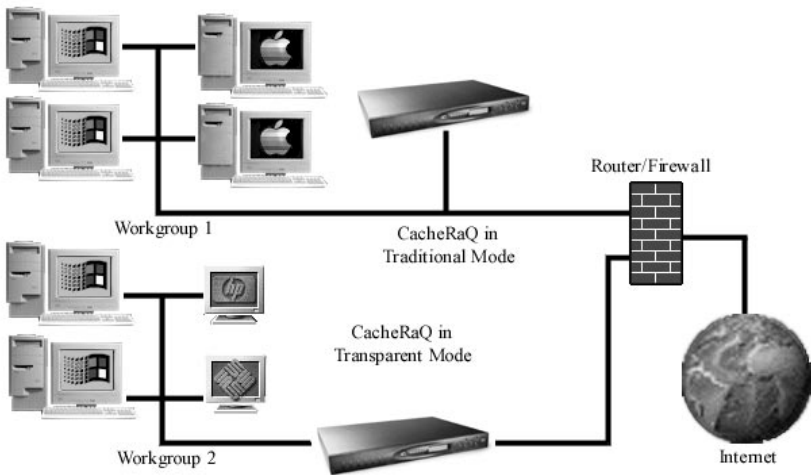
Installation notes

- You can configure the CacheRaQ 4 for either Traditional Proxy Caching mode or Transparent Caching mode (using one or two network interfaces).

- To set up the mode you choose, follow the instructions given in "Traditional Proxy Caching mode" on page 65 for Traditional mode, or "Transparent Caching mode using one network interface" on page 67 or "Transparent Caching mode using two network interfaces" on page 68 for Transparent mode.

Advantage

You can separate network traffic into workgroups to divide the client load among multiple caching servers. This increases scalability and allows geographically separated networks to be cached.

Deployment in an ISP
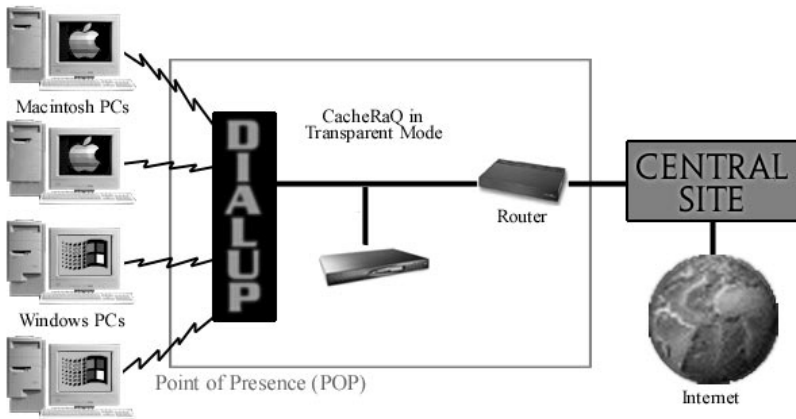
Installation notes

- Configure the CacheRaQ 4 for Transparent Caching mode using one network interface.

- Configure the access concentrators ("DIAL UP") to use the CacheRaQ 4 as their gateway.

- Enter the IP address of the router as the gateway for the CacheRaQ 4.

- One CacheRaQ 4 should be able to handle 1 Mb/s to 2 Mb/s of wide area network (WAN) traffic. Contact Cobalt Networks, Inc. for more detailed deployment guidelines.

Advantage

- You can keep quick-to-access copies of remote documents, saving bandwidth and speeding up page access for users.

Disadvantage

- For large ISP points-of-presence (POP), one CacheRaQ 4 may not be enough. In this case, a cluster of CacheRaQ 4s can be used.

Cluster deployment in an ISP
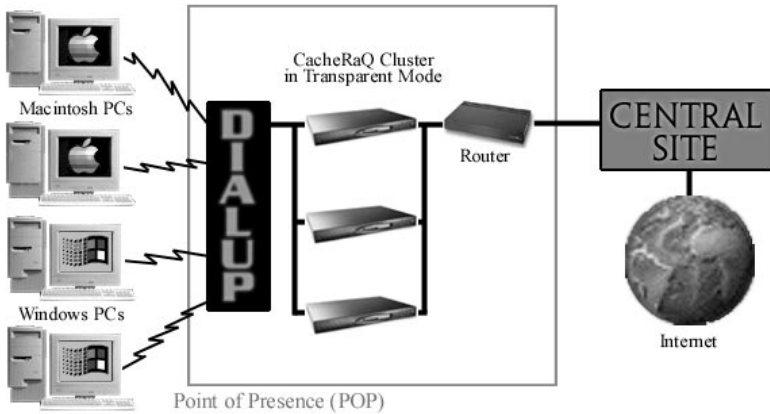
Installation notes

• Configure one CacheRaQ 4 as the Cluster Master (see "Cache Cluster settings" on page 34).

• Configure the Cluster Master to operate in Transparent Caching mode using one network interface.

• The Cluster Slaves require no special configuration.

• Enter the IP address of the router as the gateway for the Cluster Master.

• Configure the access concentrators ("DIAL UP") to use the Cluster Master as their gateway.

Advantages

• The clustered CacheRaQ 4s provide high-availability and high-speed cache access as well as larger cache storage.

• This solution is scalable—you can add up to five Cluster Slaves.

Disadvantage

• You cannot have more than five Cluster Slaves. If you want more capacity, you can use an L4 switch solution (see "Cluster deployment with an L4 switch in an ISP" on page 72).

Cluster deployment with an L4 switch in an ISP
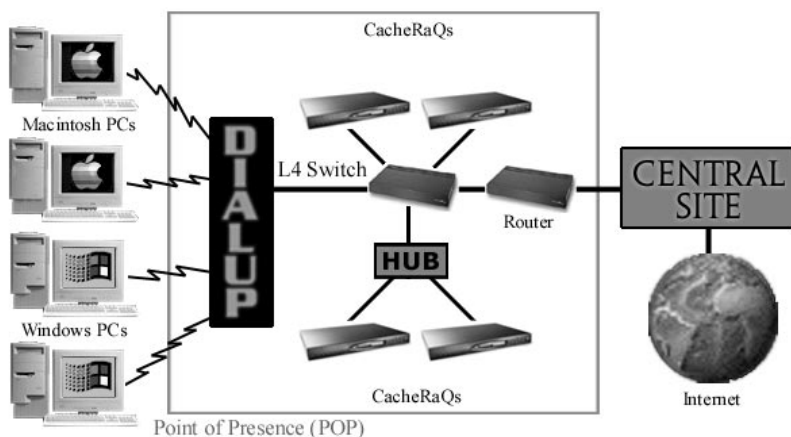
Installation notes

- Configure the CacheRaQ 4s for Transparent Caching mode using one network interface.

- You do not need a Cluster Master because the L4 switch replaces the Cluster Master.

- The CacheRaQ 4s can be connected either directly to the L4 switch or through a hub.

- Refer to the manual of the L4 switch for instructions on configuring the redirection of cache requests.

Advantages

- You do not need a Cluster Master.

- This solution is scalable—you can have dozens of CacheRaQ 4s for each L4 switch.

- This is the fastest, largest-capacity solution.

Disadvantage

- An L4 switch is expensive.

Cluster in Traditional Proxy Caching mode
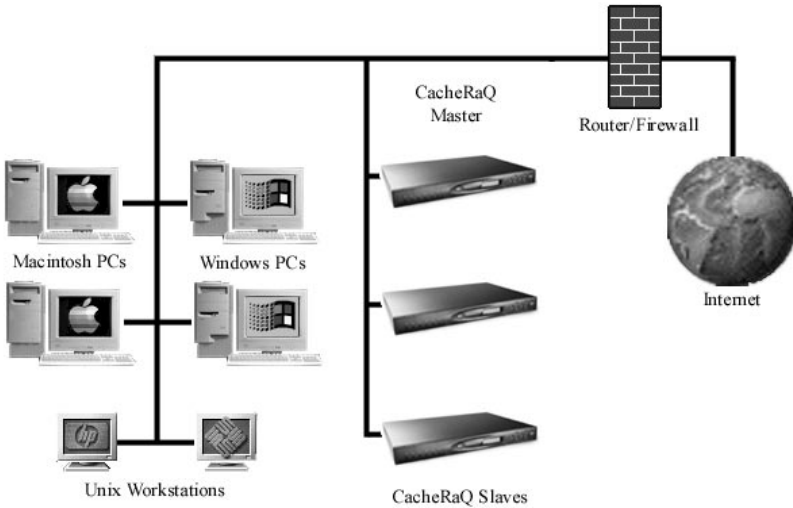
Installation notes

•   Configure one CacheRaQ 4 as the Cluster Master (see "Cache Cluster settings" on page 34).

•   The Cluster Slaves require no special configuration.

Advantages

•   Distributed caching allows for faster response time and more storage space.

•   Clustered CacheRaQ 4s are scalable—you can add more Cluster Slaves as needed.

Disadvantage

•   You must change the browser configuration of each client.

Cluster in Transparent Caching mode
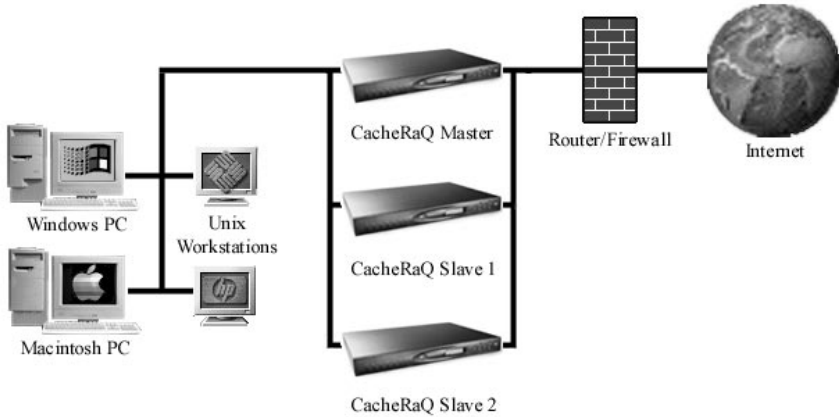
Installation notes

• Configure the Cluster Master for Transparent Caching mode. (The figure above shows a two-interface configuration. A one-interface configuration is also possible.)

• Configure the Cluster Slaves for Traditional Proxy Caching mode.

• Enter the Cluster Slave information into the Cluster Master configuration (see "Cache Cluster settings" on page 34).

Advantage

• You do not need to change the browser configuration of the clients.

Disadvantage

• If the Cluster Master fails, the clients cannot access the outside network until the Cluster Master comes back online.

Enterprise cluster with an L4 switch
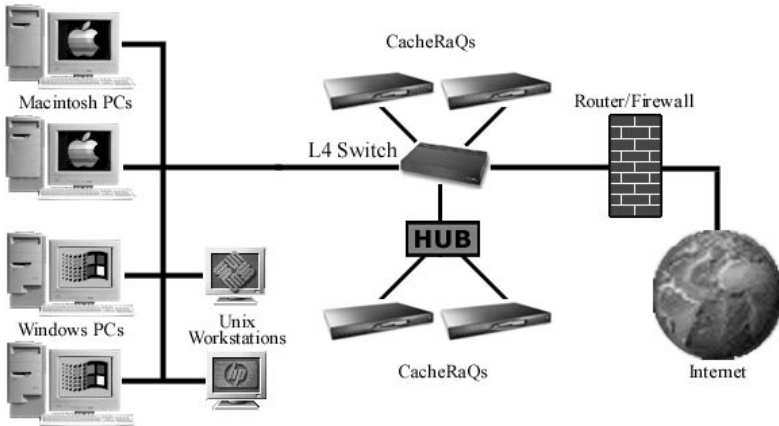
Installation notes

- Configure the CacheRaQ 4s for Transparent Caching mode using one interface.

- The CacheRaQ 4s can be connected either directly to the L4 switch or through a hub.

- You do not need a Cluster Master because the L4 switch replaces the Cluster Master.

- Refer to the manual of the L4 switch for instructions on configuring the redirection of cache requests.

Advantages

- This solution allows for high-speed clustering.

- It is fully scalable—you can add CacheRaQ 4s as needed. An L4 switch typically places few limits on the maximum number of cache servers.

- It provides increased cache storage space.

- You do not need a Cluster Master.

Disadvantage

- An L4 switch is expensive.

Advanced Information

Serial console port

You can connect a console terminal to the DB-9 connector on the back panel of the CacheRaQ 4. 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 CacheRaQ 4 through the serial console port

You can now initialize a large number of Cobalt servers through the serial console port rather than individually through the LCD console on each CacheRaQ 4.

This feature only allows the assignment of network parameters (IP address, netmask, gateway).

Note: You can use the initialize the CacheRaQ 4 through the serial console port only once, much like proceeding through the browser-based Setup Wizard.

To initialize the CacheRaQ 4 through the serial console port:

1. Connect a null modem serial cable to the serial console port on the back panel of the CacheRaQ 4. See the following figure.

Serial console port   Serial port   Network connectors
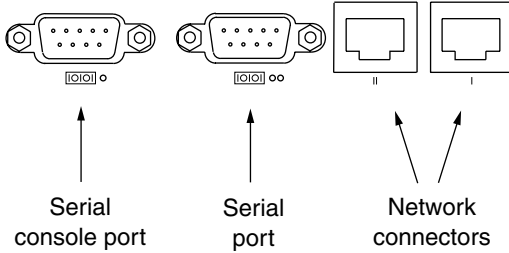
2. Configure your terminal software to the following parameters:

   • 115 200 Baud

   • 8 data bits

   • no parity

   • 1 stop bit

3. Power on the CacheRaQ 4 with the power switch on the back panel.

4. A number of boot messages are displayed on your terminal screen.

5. The first prompt asks for an IP address. Enter the Primary IP Address for the CacheRaQ 4 (for example, 10.9.19.55).

6. The second prompt asks for the netmask address. Enter the Primary Netmask for the CacheRaQ 4 (for example, 255.0.0.0).

7. The third prompt asks for the gateway address. Enter the gateway for the CacheRaQ 4 (for example, 10.9.25.254).

8. 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

9. Another prompt is displayed: [S]AVE / [C]ANCEL. Enter "S" to save the configuration.   The message "Verifying and saving..." appears.

10. Once the configuration is saved, the terminal screen displays the normal boot status messages. Continue administration of the CacheRaQ 4 through your Web browser.

Licenses

THE BSD COPYRIGHT

Copyright ©1991, 1992, 1993, 1994 The Regents of the University of California. 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 the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS 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 THE REGENTS OR 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.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

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 byRalf 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 byRalf 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

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.

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.

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)*.

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)*.

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.

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)*.

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.

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)*.

ICP

See *Inter-Cache Communication Protocol*.

Inter-Cache Communication Protocol (ICP)

An Internet protocol used to create cache hierarchies. A cache hierarchy is a collection of caching proxy servers organized in a logical parent/child and sibling arrangement so that cache servers closest to Internet gateways (closest to the backbone transit entry-points) act as parents to cache servers at locations farther from the backbone.

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. These functions were previously performed by the Internet Assigned Numbers Authority (IANA). The U.S. government is essentially turning over control of the Internet to ICANN, although domain name registration performed by Network Solutions, Inc. (NSI) will continue to be under U.S. government contract for a limited time.

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.

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)" on page 95 and "Simple Mail Transfer Protocol (SMTP)" on page 97.

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.

InterNIC

The former organization responsible for registering and maintaining the com, edu, gov, net and org domain names on the World Wide Web. Domain name registration is now performed by Network Solutions, Inc. who will continue to be under U.S. government contract for a limited time.

IP address

A 32-bit address assigned to hosts using Transmission Control Protocol/ Internet Protocol (TCP/IP). An IP address belongs to one of five classes (A, B, C, D or E) and is 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.

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.

Network Time Protocol (NTP)

A protocol built on top of the Transmission Control Protocol (TCP) 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 is designed to be synchronized with the clock speed of the microprocessor, in the range of 20 MHz to 33 Mhz.

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.

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. POP3 is built into the Netscape Navigator and Microsoft Internet Explorer browsers.

POP can be thought of as a store-and-forward service. 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.

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.

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)" on page 91 and "Post Office Protocol 3 (POP3)" on page 95.

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 Apple Macintosh computers, PCs and many Unix systems for attaching peripheral devices to computers. SCSI interfaces provide for faster data transmission rates (up to 80 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. Although SCSI is an ANSI standard, there are many variations, so two SCSI interfaces can be incompatible. For example, SCSI supports several types of connectors.

SMB

See *Server Message Block (SMB).*

SMTP

see *Simple Mail Transfer Protocol (SMTP)*.

SNMP

See *Simple Network Management Protocol (SNMP)*.

SSL

See *Secure Socket 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 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 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 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.

WCCP

See *Web Cache Communication Protocol (WCCP).*

Web Cache Communication Protocol (WCCP)

This protocol, developed by Cisco Systems, Inc., allows you to use a caching router to handle web traffic, reducing transmission costs and downloading time. This traffic includes user requests to view pages and graphics on World Wide Web servers, whether internal or external to your network, and the replies to those requests.

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).*

Appendix F: Glossary