

Sun Cobalt RaQ™ 550 Server Appliance

User Manual



Copyright © 1997-2002 Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, California 94303, U.S.A. All rights reserved.

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

This product is distributed under licenses restricting its use, copying, distribution and decompilation. No part of this product may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any.

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

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and in other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, Java, JavaScript, JavaServer Pages, JSP, Sun Cobalt, Sun Cobalt RaQ and the Sun Cobalt logo are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

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

PostScript is a trademark or registered trademark of Adobe Systems, Incorporated, which may be registered in certain jurisdictions.

Linux is a trademark of Linus Torvalds.

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

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

Copyright © 1997-2002 Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, California 94303, U.S.A. Tous droits réservés.

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

Ce produit est distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution et la décompilation. Aucune partie de ce produit ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a.

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

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, Java, JavaScript, JavaServer Pages, JSP, Sun Cobalt, Sun Cobalt RaQ et le logo Sun Cobalt sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

Netscape et Netscape Navigator sont des marques de fabrique ou des marques déposées de Netscape Communication Corporation aux Etats-Unis et dans d'autres pays.

PostScript est une marque de fabrique d'Adobe Systems, Incorporated, laquelle pourrait être déposée dans certaines juridictions.

Linux est une marque de fabrique de Linus Torvalds.

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

Part Number / Numéro de pièce : 816-4064-01

Date : 04-2002

Important Safeguards

For your protection, please read all these instructions regarding your Sun Cobalt RaQ™ 550 server appliance and retain for future reference.

1. Safety Precautions

For your protection, observe the following safety precautions when setting up your equipment:

- Follow all cautions and instructions marked on the equipment.
- Ensure that the voltage and frequency of your power source match the voltage and frequency inscribed on the equipment's electrical rating label.
- Never push objects of any kind through openings in the equipment. Dangerous voltages may be present. Conductive foreign objects could produce a short circuit that could cause fire, electric shock or damage to your equipment.

2. Symbols

The following symbols may appear in this book:



Caution: There is a risk of personal injury and equipment damage. Follow the instructions.



Warning: Hazardous voltages are present. To reduce the risk of electric shock and danger to personal health, follow the instructions.

3. Power Source and Power Cords

Ensure that the voltage and frequency of your power source match the voltage and frequency inscribed on the equipment's electrical rating label.



Warning: Sun Cobalt™ products are designed to work with single-phase power systems having a grounded neutral conductor. To reduce the risk of electric shock, do not plug Sun Cobalt products into any other type of power system. Contact your facilities manager or a qualified electrician if you are not sure what type of power is supplied to your building.



Warning: Not all power cords have the same current ratings. Household extension cords do not have overload protection and are not meant for use with computer systems. Do not use household extension with your Sun Cobalt products.



Warning: Your Sun Cobalt product is shipped with a grounding type (three-wire) power cord. To reduce the risk of electric shock, always plug the cord into a grounded power outlet.



Warning: The power switch of this product functions as a standby type device only. The power cord serves as the primary disconnect device for the system. Be sure to plug the power cord into a grounded power outlet that is nearby the system and is readily accessible. Do not connect the power cord when the power supply has been removed from the system chassis.

4. 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. See “Replacing the battery” on page 227.



Warning: Batteries may explode if mishandled or incorrectly replaced. Do not dispose of the battery in fire. Do not disassemble it or attempt to recharge it. Replace only with the same or equivalent type recommended by the equipment manufacturer. Dispose of used batteries according to manufacturer's instructions.

5. Electrical Shock

To reduce the risk of electrical shock, do not disassemble or tamper with the power supply assembly. Opening or removing the power supply may expose you to dangerous voltage or other risks. Incorrect reassembly can cause electric shock when this product is subsequently used.

6. Top Cover

You must remove the cover of your Sun Cobalt server appliance to add cards, memory or internal storage devices. Be sure to replace the top cover before powering on your server appliance.



Caution: Do not operate Sun Cobalt products without the top cover in place. Failure to take this precaution may result in personal injury and system damage.

7. Modifications to equipment

Do not make mechanical or electrical modifications to the equipment. Sun Microsystems, Inc. is not responsible for regulatory compliance of a modified Sun Cobalt product.

8. Ventilation

The fan openings on the Sun Cobalt RaQ 550 server appliance are provided for ventilation and reliable operation of the product, and to protect it from overheating. The openings must not be blocked or covered, and should be kept free of dust and debris. Never place a Sun Cobalt product near a radiator or heat register. Failure to follow these guidelines can cause overheating and affect the reliability of your product.

The Sun Cobalt RaQ 550 server appliance is designed to be a built-in installation, so adequate ventilation is required.

9. Placement of a Sun Product



Caution: Do not block or cover the openings of your Sun Cobalt product. Never place a Sun Cobalt product near a radiator or heat register. Failure to follow these guidelines can cause overheating and affect the reliability of your Sun Cobalt product.



Caution: The workplace-dependent noise level defined in DIN 45 635 Part 1000 must be 70Db(A) or less.

10. SELV Compliance

Safety status of I/O connections comply to SELV requirements.

11. Browsers

Both Netscape Navigator™ and Microsoft Internet Explorer have bugs that can cause intermittent, unexplained failures.



Note: You may experience problems logging on to the Sun Cobalt RaQ 550 server appliance with a secure connection if you are using Internet Explorer on a Macintosh machine.

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 data on a Sun Cobalt RaQ 550 server appliance.

To use the Sun Cobalt RaQ 550 server appliance, you need a personal computer (attached to the network) that uses one of the following standard Web browsers:

- Macintosh OS9: Internet Explorer 5 or Netscape 4.78
- Macintosh OSX: Internet Explorer 5.1
- Windows 98/NT/2000: Internet Explorer 5.5 and 6.0 or Netscape 4.78

To manage the server appliance from the user interface, you must enable cookies, cascading style sheets and JavaScript™ on your browser (these features are normally enabled by default).

12. Regulations and Information

FCC Class B Notice

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Note: 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:

- Reorient or relocate 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/television technician for help.

Shielded Cables: Connections between the workstation and peripherals must be made using shielded cables in order to maintain compliance with FCC radio frequency emission limits. Networking connections can be made using unshielded twisted pair (UTP) cables.

Modifications: Any modifications made to this device that are not approved by Sun Microsystems, Inc. may void the authority granted to the user by the FCC to operate this equipment.

Important Safeguards

Preface

This user manual is intended for anyone who will set up the Sun Cobalt RaQ™ 550 server appliance. You should be familiar with Microsoft Windows, Macintosh or other operating systems, and Netscape Navigator™, Microsoft Internet Explorer, or other Web browsers.

This manual consists of the following chapters and appendices:

Chapter 1 — “Introduction” on page 1 summarizes the features on the Sun Cobalt RaQ 550 server appliance.

Chapter 2 — “Setting up the Sun Cobalt RaQ 550 server appliance” on page 9 describes the hardware setup of the server appliance and the process to integrate the server appliance into the network.

Chapter 3 — “Services” on page 31 explains the services on the Sun Cobalt RaQ 550 server appliance.

Chapter 4 — “Server Management” on page 47 explains the features on the Server Management screens.

Chapter 5 — “Site Management” on page 103 explains the features available to a Site Administrator on the Sun Cobalt RaQ 550 server appliance.

Chapter 6 — “BlueLinQ” on page 143 explains how to use the software update feature.

Chapter 7 — “Personal Profile” on page 149 explains how to view your account information.

Appendix A — “Advanced Information” on page 153 gives information for advanced users.

Appendix B — “Domain Name System” on page 167 gives an in-depth explanation of the DNS service.

Appendix C — “LCD Menu Options” on page 195 shows the LCD menu options.

Appendix D — “Disaster Recovery with Third-Party Software” on page 205 explains how to use third-party software to perform disaster recovery on the server appliance.

Preface

Appendix E — “Servicing the Sun Cobalt RaQ 550 server appliance” on page 219 explains how to upgrade and service the server appliance.

Appendix F — “Product Specifications” on page 229 lists the technical specifications for the Sun Cobalt RaQ 550 server appliance.

Appendix G — “Licenses” on page 235 lists licensing information.

Appendix H — “Glossary” on page 243 provides a glossary of terms.

Contents

Important Safeguards	v
Preface	xi
List of Figures	xxi
1 Introduction	1
Services on the Sun Cobalt RaQ 550 server appliance	3
Documentation	3
Hardware	4
Usage requirements	4
Customer Service and Technical Support	5
Knowledge Base	5
Support fora	5
Service request	6
Telephone numbers	6
Before contacting Technical Support	6
Further resources and information	7
Warranty	7
Privacy policy	7
Online registration	7
Product demonstrations	8
Solutions	8
Sun Cobalt Developer Network	8
Education	8
2 Setting up the Sun Cobalt RaQ 550 server appliance	9
General	9
Front view of the Sun Cobalt RaQ 550 server appliance	10
Rear view of the Sun Cobalt RaQ 550 server appliance	12
Setup of the Sun Cobalt RaQ 550 server appliance	13

Phase 1: Making the connection	13
Connecting to the network	13
Connecting the power	13
Powering on the server appliance	14
Configuring network settings	14
Using the LCD console to configure the network	14
Configuring the Sun Cobalt RaQ 550 server appliance manually	16
Phase 2: Setting up with the Web Browser	18
Active Assist — Online Help	19
Configuring the Sun Cobalt RaQ 550 server appliance with the Setup Wizard	20
License Agreement	21
System Settings	22
RAID Setup	26
Product Registration	27
Completing configuration with the Setup Wizard	28
Software Auto-Provisioning (AutoUpdate)	30
3 Services	31
Managing your personal profile	31
Using email on the server appliance	32
Email aliases	32
Email relaying	33
POP-before-SMTP feature	34
Mailing lists	34
Developing Web pages	35
FrontPage 2002 Server Extensions	35
Using an HTML editor	37
CGI scripts	37
Server-side scripting languages	38
Publishing Web pages using FTP	38
Domain Name System (DNS)	39
RAID-1 and RAID-0 support	40
Hard disk drive failure	40

System health monitoring	42
Fan, voltage and temperature monitoring	42
Fan monitoring	42
Temperature monitoring	42
Voltage monitoring	42
System Fault LED	43
Back up and restore data	44
Secure sockets layer (SSL)	44
Install software	45
Simple Network Management Protocol (SNMP)	45

4 Server Management **47**

Resetting the Administrator password	48
Clearing the password through the LCD console	49
Accessing Server Management	50
Server Administrators	53
Network Services	55
Web	55
ASP Administration	57
FTP	58
Email Servers	59
Basic Tab	60
Advanced Tab	61
DNS	64
SNMP	65
Shell	66
Security	67
Scan Detection	67
Buffer Overflow	68
SSL	70
System Settings	74
TCP/IP	74
IP Address Allocation	78
Bandwidth Limits	80
Power	82

UPS	85
Configure As Master	88
Configure As Slave	88
Time	89
Information	89
Maintenance	90
Server Desktop UI	90
Knox Arkeia Backup Settings	91
Legato NetWorker™ Backup Settings	92
Additional Storage	93
Usage Information	95
Network	95
Web	96
FTP	96
Email	97
Disk	97
Active Monitor	99
Active Monitor icon	99
Status menu selection	99
Settings menu selection	102
5 Site Management	103
Introduction	103
Administrator privileges	104
Site Management screen (for Server Administrator)	106
Search Virtual Sites	107
Virtual Site List	108
Editing the virtual site template	111
Site Management screen (for Site Administrator)	116
Managing Virtual Sites	117
User Management	119
User List	119
Importing and exporting site users	123
Mailing Lists	127
General Settings	131

Services	132
Web	132
Anonymous FTP	134
Email	136
Shell	137
Web Deployment	137
SSL	139
Usage Information	140
Web	140
FTP	140
Email	141
Disk	141
Settings	142
6 BlueLinQ	143
Software Notification icon	143
New Software	143
Updates	144
Installed Software	146
Settings	147
7 Personal Profile	149
Account	149
Email	150
Forwarding	151
Enabling email forwarding	151
Disabling email forwarding	151
Vacation message	151
Enabling the vacation message	151
Disabling the vacation message	152
Disk Usage	152
Viewing the disk usage statistics	152
A Advanced Information	153
Enabling Interbase 6.0	154
Serial console port	155
Initializing the server appliance through the serial console port	156

Powering down the server appliance remotely	157
Removing a lock from the LCD panel	159
Development tools	161
Configuration files	162
Directory structure	163
Virtual site home page	163
Customized error Web pages	164
Site user home page	165

B Domain Name System 167

Basic DNS	168
Enabling the DNS server feature	168
Advanced DNS	169
Configuring SOA default values	169
Domain administrator email address	170
Refresh interval	170
Retry interval	171
Expire interval	171
Time-to-live period (TTL)	171
Configuring the server settings	171
Cache record lookups	171
Forwarding server	172
Zone transfer	172
Zone Format	173
Primary services	175
Selecting a domain	176
Modifying the SOA record	176
Deleting all DNS records	177
Modifying a specific DNS record	177
Deleting a specific DNS record	177
Configuring a Forward Address (A) record	178
Configuring a Reverse Address (PTR) record	179
Configuring a Mail Server (MX) record	180
Configuring an Alias (CNAME) record	181
Adding a Subdomain Delegation	182
Adding a Subnet Delegation	183

Secondary services	185
Secondary service for a domain	185
Secondary service for a network	186
Sample setup of DNS service	187
Reverse Address (PTR) record	188
Forward Address (A) record	189
Mail Server (MX) record	190
Brief history of the Domain Name System (DNS)	191
What is a DNS record?	192
Who manages your DNS records?	192
How does DNS work?	192
C LCD Menu Options	195
Setup network menu	197
Autoupdate menu	198
Configure UPS menu	199
Power menu	200
Panel menu	201
Language menu	202
Clear scandetect menu	203
Reset password menu	204
D Disaster Recovery with Third-Party Software	205
How disaster recovery works	205
Locking the UI database	206
General steps to perform disaster recovery	207
General notes regarding backup services	208
Knox Arkeia	209
Tailoring the backup service	209
Files associated with Knox Arkeia tailoring	210
Backing up a server appliance with Knox Arkeia	211
Performing disaster recovery of a server appliance with Knox Arkeia	211
Preparing for disaster recovery	211
Performing a disaster-recovery operation	212

Legato NetWorker™	214
Tailoring the backup service	214
Files associated with Legato NetWorker tailoring	214
Backing up a server appliance with Legato NetWorker	215
Performing disaster recovery on a server appliance with Legato NetWorker	215
Preparing for disaster recovery	215
Performing a disaster-recovery operation	217
E Servicing the Sun Cobalt RaQ 550 server appliance	219
Installing or removing a hard disk drive	221
Installing additional memory	223
Replacing the fans and power cables	224
Replacing the power supply	225
Replacing the battery	227
F Product Specifications	229
Hardware	229
Software	230
Features	230
System management	231
Physical data	232
Regulatory approvals	233
G Licenses	235
The BSD Copyright	235
GNU General Public License	236
SSL License	242
H Glossary	243

List of Figures

Front view—Sun Cobalt RaQ 550 server appliance	4
Front view of the server appliance	10
Rear view of the server appliance	12
Network and power connectors	13
LCD console	15
Sun Cobalt RaQ 550 server appliance Welcome screen	19
License Agreement	21
System Settings	22
RAID Setup	26
Online Registration	27
Server Management on the user interface	28
System Fault LED	43
Server Management screen	51
Add New Server Administrator screen	53
Web Settings screen	55
ASP Settings screen	57
FTP Settings screen	58
Email Servers Settings (Basic Tab) screen	60
Email Servers Settings (Advanced Tab) screen	61
SNMP Settings table	65
Shell table	66
Scan Detection Settings screen	67
Buffer Overflow Protection settings screen	69
Certificate Information for Server Desktop screen	70
Signing Request Information for Server Desktop screen	72
Certificate Authority Management for Server Desktop screen	72
Import Certificate for Server Desktop screen	73
TCP/IP Settings screen	75
Static Route List table	77
Add Static Route table	77
Interface Aliases Tab	78
Add Aliases table	78
IP Address Allocation screen	79
Acceptable Ranges screen	79
Bandwidth Limits screen	80
Setting a Bandwidth Limit screen	80
Bandwidth Limits screen	81

List of Figures

Power Options screen	82
Shutdown screen	83
UPS Connections	85
UPS Settings screen	87
Time Settings screen	89
Server Desktop screen	90
Knox Arkeia Backup screen	91
Legato NetWorker Backup Settings screen	92
Additional Storage Device List screen	93
Setup New Storage Device screen	93
Setup Disk screen	94
Configure Network Reporting Options screen	95
Network Statistics Summary screen	96
Configure Web Reporting Options screen	96
Configure FTP Reporting Options screen	96
Configure Email Reporting Options screen	97
Disk Usage screen	97
Sites Tab screen	98
All Users screen	98
Notifications Settings screen	98
System Status - Overview screen	101
Service Status - Overview screen	101
Other Status - Overview screen	101
Active Monitor Settings screen	102
Site Management screen for Server Administrator	106
Search Virtual Sites screen	107
Advanced Search screen	108
Virtual Site List screen	108
Add Virtual Site screen	110
Edit Virtual Site Template—Basic Settings tab	111
Edit Virtual Site Template—Services and Features tab	113
Edit Virtual Site Template—Web tab	114
Edit Virtual Site Template—Anonymous FTP tab	115
Site Management screen for Site Administrator	116
Virtual Site Management screen (for Server Administrator)	117
Search Users and User List screens	119
Add New User screen	120
User List screen	121
Modify User screen	121
Import User List screen	125
Export User List screen	126
Mailing Lists screen	127
Add Mailing Lists screen (Basic tab)	127
Add Mailing Lists screen (Subscriber tab)	128

Search and Add Users to Mailing List)	129
Add Mailing Lists screen (Advanced tab)	130
Virtual Site Settings screen	131
Web Settings screen	132
Anonymous FTP Settings screen	135
Email Settings screen	136
Shell Settings screen	137
Web Archive (.war) List screen	138
Add Web Archive (.war) List screen	138
Certificate Information screen	139
Configure Web Reporting Options screen	140
Configure FTP Reporting Options screen	140
Configure Email Reporting Options screen	141
Disk screen	141
Settings screen	142
Available New Software List table	144
Available Software Updates List table	144
Install Software table	145
Install Manually table	145
Installed Software List table	146
BlueLinQ Settings - Basic tab	147
BlueLinQ Settings - Advanced tab	147
Account Settings table	149
Email table	150
Disk Usage table	152
Serial console port location	156
Basic DNS table	168
Advanced DNS table	170
Zone Format table	174
Sample entries in the Primary Service List table	175
Add a Subdomain Delegation	182
DNS Primary Service List (after adding Reverse PTR Record)	183
Add a Subnet Delegation	184
Sample entries in the Secondary Service List table	185
Add Secondary Domain table	186
Add Secondary Network table	187
Add New Reverse Address (PTR) Record table	188
Add New Forward Address (A) Record table	189
Add New Mail Server (MX) Record table	190
Basic method of DNS	193
Setup Network LCD menu	197
Autoupdate LCD menu	198
Configure UPS LCD menu	199
Power LCD menu	200

List of Figures

Panel LCD menu	201
Language LCD menu	202
Clear scandetect LCD menu	203
Reset password LCD menu	204
Components in the server appliance	220
Removing a drive	222
Removing a DIMM	224
Removing the fans and power cables	225
Removing the power supply	226

Introduction

The Sun Cobalt RaQ™ 550 server appliance is a powerful and versatile network server. It fits easily within an existing network, and provides virtual hosting capabilities for email and Web hosting.

The Sun Cobalt RaQ 550 server appliance is a rack-mountable Internet server targeted at the ISP market as a dedicated and shared hosting platform. It has hardware and software features designed to meet the demands for mid-range hosting.

The Sun Cobalt RaQ 550 server appliance is primarily an Internet Web, mail, FTP and DNS server with extensive virtual hosting and dynamic content generation capabilities. After initial setup using the server's LCD or serial console, all server administration is done through a secure browser connection through either an intranet or Internet connection.

Server-wide service offerings are configured through a Web administration facility. This gives the administrator the ability to:

- Administer virtual sites
- Configure email, FTP, Telnet, SNMP, ASP and DNS services
- Install and upgrade software
- Configure network parameters
- Configure uninterruptible power supply (UPS) operation
- Configure wake options
- Monitor system services and resources

The administration Web pages allow the addition, configuration and monitoring of virtual sites, either based on name or IP address. Configuration options for virtual sites include:

- Adding users
- Creating mailing lists
- Configuring CGI, SSI, ASP, JSP and servlets, PHP, Telnet, Frontpage, FTP
- Assigning bandwidth limits

Additionally, the server administration interface gives status on sites, including traffic reports and disk usage information. Individual users on a virtual site have access to the Web administration facility where they can access the following:

- Email settings
- Personal preferences
- Usage data

The administrator also has the following configuration options through the LCD:

- Configure network settings
- Reboot and power down
- Configure UPS
- Lock menus
- Reset administrator's password
- Automatically download additional software packages

Services on the Sun Cobalt RaQ 550 server appliance

Here is a sample of what you can do with the Sun Cobalt RaQ 550 server appliance:

- **Web publishing.** You can access a broad range of Web publishing capabilities for users.
- **Email.** The server appliance's email service allows you to communicate internally and externally to individuals. It includes auto-forward and auto-response capabilities for each personal site. You can also create mailing lists that include external users. To access your email on the Sun Cobalt RaQ 550 server appliance, you can use any standard email client software.

These services can be used within an extranet or an intranet environment, or across the Internet.

Documentation



You can access the user manual in PDF format from the browser-based user interface. If you have installed third-party software on the Sun Cobalt RaQ 550 server appliance, the relevant documentation is available on the browser screen.

To access the PDF file for the user manual, click on the “question mark” help icon in the top right corner. A separate browser window opens displaying a list of PDF files in the languages available. Click the link for the PDF in your preferred language; you can open the PDF file in the browser window or save it to your personal computer.

Hardware

Figure 1 shows the front view of the Sun Cobalt RaQ 550 server appliance.

Figure 1. Front view—Sun Cobalt RaQ 550 server appliance



Usage requirements

To use the Sun Cobalt RaQ 550 server appliance, you need:

- A 10/100BASE-TX Transmission Control Protocol/Internet Protocol (TCP/IP) -based local area network (LAN).
- A personal computer (attached to the network) that uses one of the following Web browser:
 - Macintosh OS9: Internet Explorer 5 or Netscape™ 4.78
 - Macintosh OSX: Internet Explorer 5.1
 - Windows 98/NT/2000: Internet Explorer 5.5 and 6.0 or Netscape 4.78

To manage the server appliance from the user interface, you must enable cookies, cascading style sheets and JavaScript™ on your browser (these features are normally enabled by default).

- Network parameters, which you can obtain from your system or network administrator; these include the server appliance's assigned IP address, the subnet mask of your network and, if communicating with other networks, a gateway or router address.
- An Internet service provider (ISP), if you plan to connect to the Internet.

Customer Service and Technical Support

For Sun Cobalt™ product information, visit the Sun Cobalt section of the Sun Web site at the URL

<https://ebusiness.sun.com/OSCSW/svcportal?pageName=CobaltHomePage>.

On this site, customers can query the Sun Cobalt Knowledge Base, participate in the Sun Cobalt Support Fora moderated by Sun™, or submit a service request to Sun Microsystems™.

Knowledge Base

You can query the Sun's online database of common installation and configuration problems and solutions. Go to the URL

<https://ebusiness.sun.com/OSCSW/svcportal?pageName=CobaltHomePage>

and click on the link in the section Step 1.

Support fora

You can use the Sun Cobalt discussion fora to find answers, post problems and read responses to posted problems. Sun Cobalt discussion fora are moderated by Sun Support.

To view the current list of Sun Cobalt support fora, go to the URL

<https://ebusiness.sun.com/OSCSW/svcportal?pageName=CobaltHomePage>

and click on the link in section Step 2.

In the new window, the names of the support fora show up as hypertext links.

New support fora are added periodically. The current fora include:

- An announcement list concerning Sun Cobalt products
- An information list for developers working on Sun Cobalt products
- A user list for sharing information between users of Sun Cobalt products
- A security list for users to address network security issues on Sun Cobalt products

Service request

If you cannot find a solution through the Knowledge Base or the support fora, you can submit a service request and may receive help from a Sun support engineer. Go to the URL

<https://ebusiness.sun.com/OSCSW/svcportal?pageName=CobaltHomePage>.

In section Step 3, choose the geographical region in which you are located and click on that link.

Telephone numbers

In the United States, call (800) 526-0484.

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

Before contacting Technical Support



Note: To receive Technical Support, you must first register your Sun Cobalt product. See “Online registration” on page 7.

First, make an effort to resolve the problem on your own. See “Servicing the Sun Cobalt RaQ 550 server appliance” on page 219.

Take note of all actions you perform and any error messages so that, if necessary, you can describe them to a member of the Technical Support team.

Refer to the user manual and to the Web-based resources, such as the Knowledge Base and the Solutions Directory (see “Further resources and information” on page 7).

To speed up your support call

When contacting Technical Support, the more information you can provide, the better. Before you call or email, have the following information ready:

- The serial number, located on the back panel, or the MAC address of the primary network interface of your Sun Cobalt RaQ 550 server appliance (on the user interface, select **Server Management > System Settings > TCP/IP**)
- Any additional software installed on your system
- Any peripherals connected to your system
- Any error messages you have received and the time when they occurred
- The process you were running or the changes you had made when the error occurred
- The steps you have taken to resolve the problem

Further resources and information

Sun Cobalt also offers the following additional resources and information.

Warranty

Sun Cobalt hardware is warranted to be free from defects in workmanship or material for one year from the date the hardware is shipped. Software media is warranted to be free from defects in workmanship or material for a period of ninety (90) days from the date of shipment.

For specific details regarding your warranty, go to the URL <http://www.sun.com/service/support/warranty/index.html>.

Privacy policy

To review Sun Microsystems' privacy policy, visit <http://www.sun.com/privacy/>.

Online registration

To register your product online, go to the URL <https://ebusiness.sun.com/OSCSW/svcportal?pageName=CobaltRegistrationRequestPage>.

Product demonstrations

To view demonstrations of the Sun Cobalt server appliances, visit the Product Demos site at <http://demo.cobalt.com/>.

Solutions

For business-case information concerning Sun Cobalt products or for solutions that extend the functionality of our products, visit the Online Solutions Directory at <http://developer.cobalt.com/sol/>.

Sun Cobalt Developer Network

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

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

Education

For those who desire a premium level of technical expertise with Sun Cobalt products, Sun offers a number of training courses. The intended audience includes end users, Sun Cobalt resellers, system and network administrators, systems engineers, product developers, support technicians, consultants and trainers.

You can access the Training Solutions site at http://suned.sun.com/US/catalog/server/network_appliance.html/.

Setting up the Sun Cobalt RaQ 550 server appliance

This chapter guides you through the process of connecting and configuring the Sun Cobalt RaQ™ 550 server appliance for your network. A typical setup process takes less than 15 minutes, after which you can begin using all of the services on the server appliance.

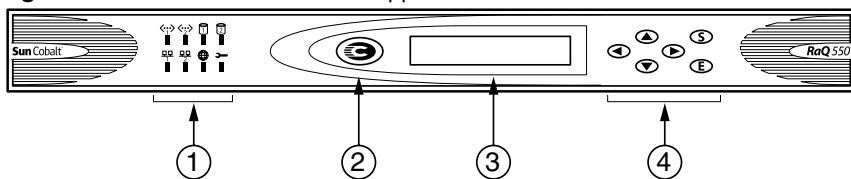
If the server appliance has been configured previously for a different network, refer to “Setup network menu” on page 197.

General

Figure 2 and Figure 3 show the controls, indicators and connectors on the Sun Cobalt RaQ 550 server appliance.


Front view of the Sun Cobalt RaQ 550 server appliance


Figure 2. Front view of the server appliance



1. The **Status Indicators** signal Ethernet, hard disk drive and Web activities as well as overall system health status.

«••» blinks when there is traffic on the network interfaces (labeled 1 and 2 on the front panel). The icon labeled “1” corresponds to the primary Ethernet connector on the back panel (labeled I on the back panel); the icon labeled “2” corresponds to the secondary Ethernet connector on the back panel (labeled II on the back panel).

 glows steadily to indicate an active connection on the network interfaces (labeled 1 and 2 on the front panel). The icon labeled “1” corresponds to the primary Ethernet connector on the back panel (labeled I on the back panel); the icon labeled “2” corresponds to the secondary Ethernet connector on the back panel (labeled II on the back panel).

 blinks when there is activity on a hard disk drive (labeled 1 or 2).



Note: In some of the user interface screens and dialog boxes, you will see eth0 and eth1. These labels refer to the primary and secondary Ethernet interfaces, respectively, on the back panel. Remember that the primary interface (eth0) is labeled I on the back panel and the secondary interface (eth1) is labeled II.



blinks to indicate Web activity.



(amber System Fault LED) lights up to indicate a system fault such as improper power supply voltages, enclosure or power supply fan problems, high temperature, hard disk drive failure, memory failure or low CMOS lithium-battery voltage.

2. The “**C**” **Logo Badge** is the power switch. The logo badge glows when the server appliance is powered on.



Note: If the front power button on the server appliance is momentarily depressed while the server appliance is powered on, the following message to be displayed on the LCD:

```
POWER DOWN:  
[Y]ES [N]O
```

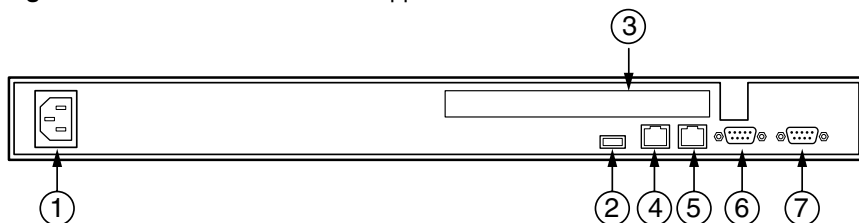
Select **YES** to power down or **NO** to keep power applied to the server appliance.

If the power button is pressed and held in for longer than 4 seconds, the server appliance is forced to power down. This is not recommended, as it may result in loss of data.

3. The **LCD screen** displays messages and values entered. Use the buttons to toggle between choices or to enter values. (See “Using the LCD console to configure the network” on page 14 and Appendix C, “LCD Menu Options,” on page 195.)
4. The **LCD buttons** allow you to enter network configuration information, configure a UPS unit, reboot the server, lock the LCD console and reset the Server Administrator password.

Rear view of the Sun Cobalt RaQ 550 server appliance

Figure 3. Rear view of the server appliance



1. The **Power socket** receives the AC cord that is provided.
2. The **Universal Serial Bus (USB) port** provides a USB 1.0-compliant connection (for printers only).



Note: The USB port is intended for value-added applications provided by third-party developers. Therefore, the port is not supported for the average end user.

3. The **PCI expansion slot** provides space for adding a PCI card
4. **Secondary network interface** (labeled II on the back panel)
5. **Primary network interface** (labeled I on the back panel)
The **Network connectors** accept 10/100BASE-T network cable and enable Ethernet network connections.
6. The **Serial connector** (serial port 2) allows you to connect an uninterruptible power supply (UPS) to the serial port for Smart UPS support. This connector is labeled with two dots (. .).
7. The **Serial console port** (serial port 1) allows you to connect serial devices. This connector is labeled with one dot (.).

Setup of the Sun Cobalt RaQ 550 server appliance

The setup process occurs in two phases:

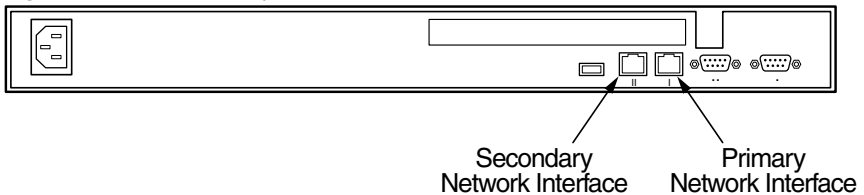
- “Phase 1: Making the connection” explains the physical connection of the server appliance to a power source and the network.
- “Phase 2: Setting up with the Web Browser” explains the network integration process and allows the administrator to select services and create users using a computer with a valid Web browser.

Phase 1: Making the connection

Connecting to the network

The Sun Cobalt RaQ 550 server appliance has two 10/100BASE-TX interface connectors on the back panel. The primary network interface connector is labeled I on the panel and the secondary interface is labeled II (see Figure 4).

Figure 4. Network and power connectors



Connect the primary network interface (I) of the server appliance to your local area network (LAN) with a twisted-pair Ethernet cable.

Connecting the power

Plug one end of the AC power cord into the back of the server appliance and the other end into an electrical outlet.

Powering on the server appliance

Turn on the power by pressing the “C” **Logo Badge** on the front of the server appliance; see Figure 1 on page 4.

The hard disk spins up and the fans start. The diagnostic LEDs will flash a few times as part of a LED diagnostic test.

A number of status messages are displayed on the LCD screen on the front panel as the Sun Cobalt RaQ 550 server appliance completes its boot process.



Caution: It is important to follow the proper power-down procedure before turning off the Sun Cobalt RaQ 550 server appliance. Refer to “Power menu” on page 200.

Configuring network settings

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

The Sun Cobalt RaQ 550 server appliance requires specific network information in order to function properly. You must use the LCD panel on the front of the server appliance to configure it.

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

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

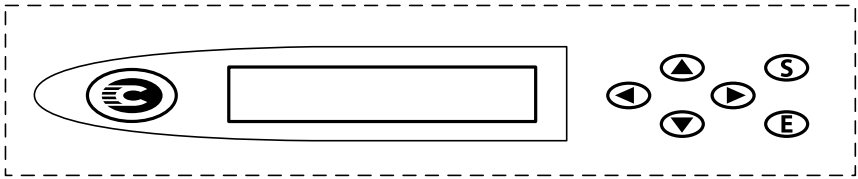
Using the LCD console to configure the network

Figure 5 shows the LCD console for the Sun Cobalt RaQ 550 server appliance.

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







Appendix C, “LCD Menu Options,” on page 195 provides more information about the LCD menus.

Figure 5. LCD console



During startup, the LCD screen on the front of the server appliance displays status information about the boot process itself. When setting up the server appliance, use the LCD console to enter network configuration information. Once the server appliance is running, the LCD console is used to change network configuration information, reboot the unit and power down the unit.

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** (select) button displays the next option.
-  The **E** (enter) button accepts the information entered or the options displayed.

Configuring the Sun Cobalt RaQ 550 server appliance manually



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

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

The LCD shows the following:

```
PRIMARY IP ADDR:  
000.000.000.000
```

A blinking cursor appears on the second line of the LCD display. The following steps explain how to enter the required network information for the primary network interface (I). The secondary network interface (II) is configured through the Web browser as described in the next section.

An IP address consists of four numbers, ranging from 0 to 255, separated by periods (for example, 192.168.25.77); this is often referred to as “dot-quad notation”.

To enter the IP address for the Sun Cobalt RaQ 550 server appliance:

1. Use the arrow buttons on the LCD console to enter the IP address assigned to the server appliance.
2. Press the **(E)** button to accept the IP address.

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

```
PRIMARY NETMASK:  
_000.000.000.000
```

3. Enter the netmask of your network.
4. Press the **(E)** button to accept the entry.

If the netmask is valid, the following prompt appears:

```
ENTER GATEWAY:  
_000.000.000.000
```

5. Enter the IP address of the gateway for your network. Press the **(E)** button to accept the entry.
6. Press the **(E)** button.

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 the **(E)** button. It pauses for a moment and then you will see:

```
Setting up Network
```



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

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

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

```
IP ADDRESS:  
192.168.25.77
```

Phase 2: Setting up with the Web Browser

The remainder of the setup process is performed through a Web browser running on a computer on your network. Use one of the following standard Web browsers:

- Macintosh OS9: Internet Explorer 5 or Netscape™ 4.78
- Macintosh OSX: Internet Explorer 5.1
- Windows 98/NT/2000: Internet Explorer 5.5 and 6.0 or Netscape 4.78

Once the setup process is complete, the Sun Cobalt RaQ 550 server appliance can be managed from any computer on the network with a valid Web browser.



Note: You may experience problems logging on to the server appliance with a secure connection if you are using Internet Explorer on a Macintosh machine.

To use the browser to set up the Sun Cobalt RaQ 550 server appliance, follow these steps:

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

Location:

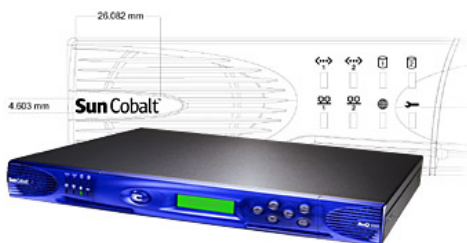
3. Press **Return** (or **Enter**) on your keyboard.

If you configured the network settings successfully, the Sun Cobalt Welcome screen appears; see Figure 6.

Figure 6. Sun Cobalt RaQ 550 server appliance Welcome screen



Welcome and thank you for purchasing the Sun Cobalt RaQ™ 550, the premier server appliance platform for web hosting. Within minutes, you will be able to host multiple domains, each with complete web, email, and FTP services - all easily administered from your browser.



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



Active Assist — Online Help

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

Configuring the Sun Cobalt RaQ 550 server appliance with the Setup Wizard

If the browser is set up to display a specific language, the Setup Wizard synchronizes with that language preference (if it is available in the software for Sun Cobalt RaQ 550 server appliance). The default language is English. The browser then displays the Welcome screen in the selected language. If the language selected in the browser preferences is not available on the server appliance, the server defaults to the Administrator's choice of language.



Note: You cannot use accented characters (for example, ä, é, ñ) in the following items:

- User names
- Email addresses and email aliases
- Host names and domain names

You can use accented characters in descriptive fields, for example, in the Full Name field for a user.

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

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



The Sun Cobalt RaQ 550 server appliance performs automatic checks on the information entered and alerts you when an illegal value or a problem is encountered. When the information is entered correctly at each stage, the server appliance enters the changes in its configuration files before proceeding to the next step. Changes may take several seconds to complete.

Click **Start** on the Welcome screen to begin the Setup Wizard.



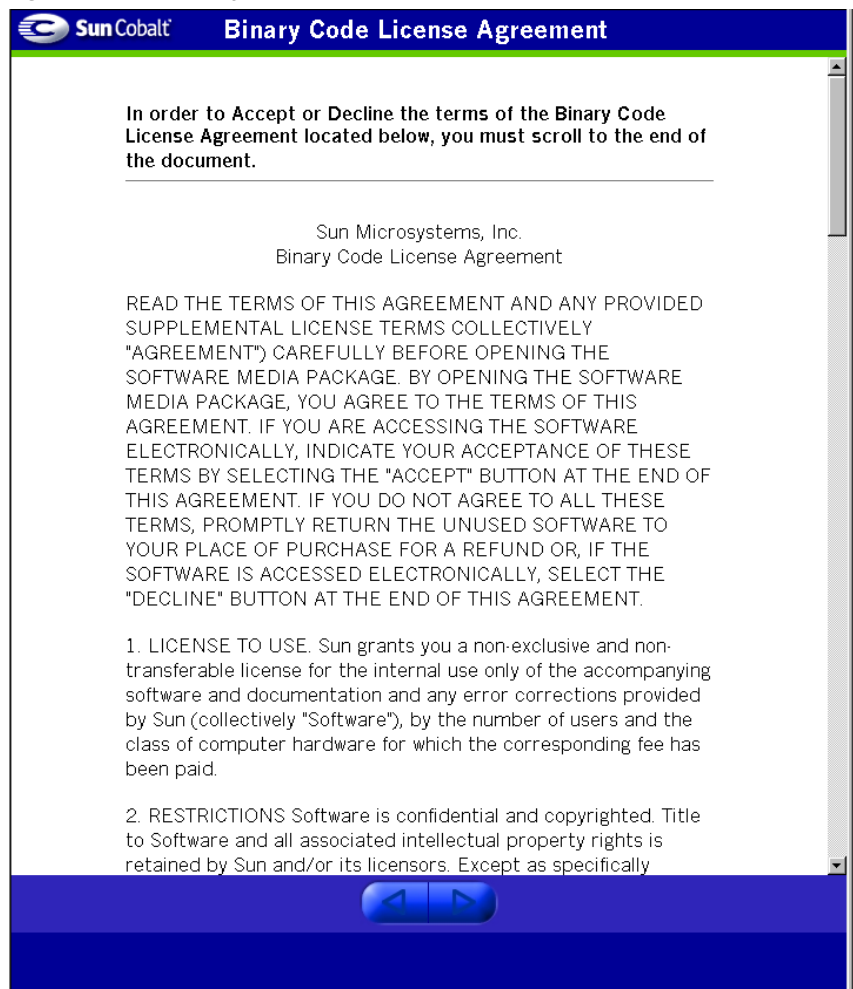
Note: For help with a particular item in the Setup Wizard, move the pointer over the item on the screen; help text appears at the bottom of the screen.

License Agreement

The first screen the Setup Wizard presents is the Binary Code **License Agreement** screen. A portion of this screen is shown in Figure 7.

You must accept the terms of the License Agreement to use the Sun Cobalt RaQ 550 server appliance. Click **Accept** at the bottom of the screen to indicate you have read and agreed to the terms of the agreement. If you do not agree to the terms of the License Agreement, the server appliance cannot be set up.

Figure 7. License Agreement



System Settings

After the license agreement is accepted, the **System Settings** screen appears; see Figure 8.

Figure 8. System Settings

System Settings

The following information is needed to configure this server appliance. You can mouse over the words on the left side of the form for help on the individual fields. If you do not know what to enter, please contact your system administrator.

System Settings	
Network Settings	
Host and Domain Name	Host Name: 127.0.0.1 Domain Name:
DNS Servers (optional)	
Administrator Settings	
UserName	admin
Password	(Enter a password)
Time Settings	
Date	April 12, 2002 4:43 PM
Time Zone	North America United States Pacific Time

Network Settings

On the Network Settings portion of the screen, you can do the following:

- Assign a host name (for example, raq550) to the server appliance.



Note: There are no spaces allowed in the host name.

- Enter your domain name. The domain name is either the official domain name that is registered with an ICANN-accredited registrar (for example, “sun.com”) or an intranet domain name specific to your network.

Coordinate the host name and domain name with your Internet service provider (ISP) to ensure the integrity of your network. If your Sun Cobalt RaQ 550 server appliance is integrated into a larger network, consult with your network administrator for this information.

This allows you to access your server appliance by host name and domain name, rather than only by IP address.

- Enter the IP address of your Domain Name System (DNS) server. A DNS server maintains a list of computer names and their IP addresses. The Sun Cobalt RaQ 550 server appliance needs access to this list on the DNS server in order to convert between IP addresses and names. This conversion is essential for sending and receiving email external to the server appliance. For more information on DNS, see Appendix B, “Domain Name System,” on page 167.

Administrator Settings

The Sun Cobalt RaQ 550 server appliance Administrator is responsible for the following:

- Setting up and maintaining the users and services on the server appliance
- Responding to email alerts from the server appliance in order to forestall potential problems

To set up the Sun Cobalt RaQ 550 server appliance for the Administrator, you must enter a **Password** in this field. For guidelines on choosing a password, see “Password Guidelines” on page 25.



Note: We recommend that you reserve the email account *admin* for system messages and alerts only and that you do not publicize this *admin* account.

Be sure to remember the password to access the Administration features in the future.

If you forget the password or want to reset the password, see “Resetting the Administrator password” on page 48.

If you want to change the password for the Administrator, see “Account” on page 149.

Password Guidelines

Use the following guidelines when choosing a password:

1. Use between three and sixteen alphanumeric characters.

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

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



Note: A password is case-sensitive.

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

Time Settings

On the Time Settings portion of the screen, you can set the day, date, time and time zone.

Click the right arrow at the bottom to move to the next screen.

RAID Setup

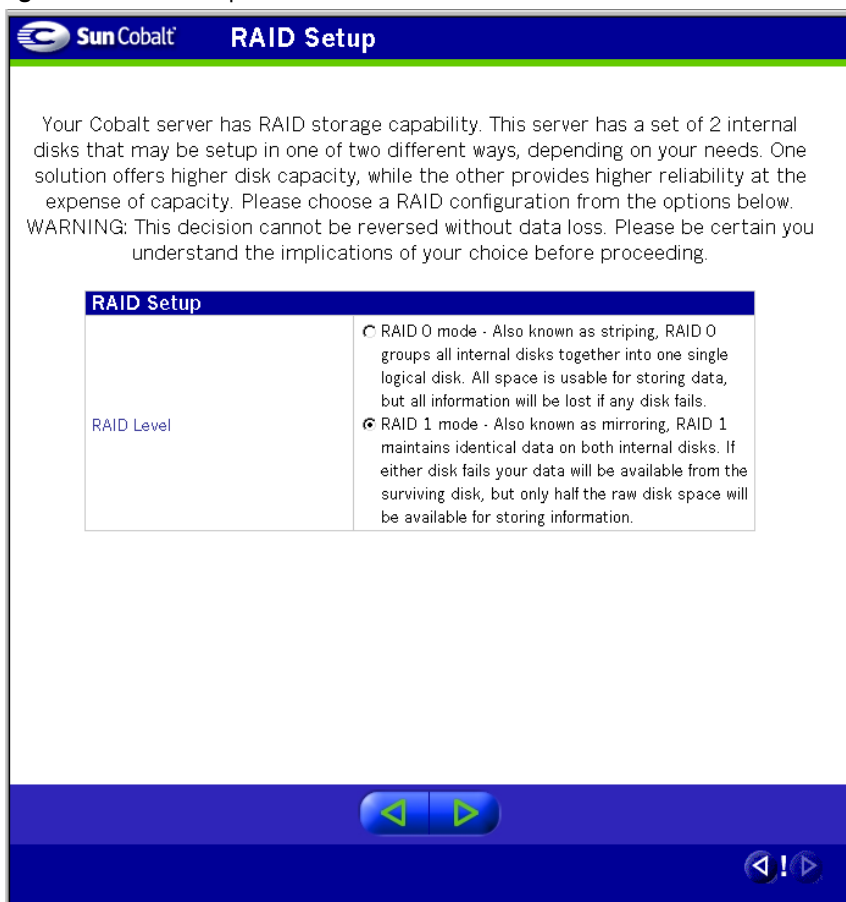
Use the RAID Setup screen in Figure 9 to select the two internal disks to operate in either RAID 0 mode or RAID 1 mode.



Note: You cannot later reverse the RAID configuration without data loss. If only a single disk is installed, the screen will not appear. Unless configured otherwise, the server appliance operates in RAID-1 mode (disk mirroring).

Click the right arrow at the bottom to move to the next screen.

Figure 9. RAID Setup



Product Registration

The **Product Registration** screen is shown in Figure 10. If you are connected to the Internet, you can register the Sun Cobalt RaQ 550 server appliance by completing the online registration.



Note: If you are not yet connected to the Internet, you cannot register online and the **Product Registration** screen does not appear. Instead, you will be directed to the online service center to register using the Web.

Click the right arrow at the bottom to continue.

Figure 10. Online Registration

You must register your Sun Cobalt RaQ 550 with Sun Microsystems to receive technical support. To register electronically, please provide the following information and click the right arrow. We are committed to respecting your privacy and recognize the need for appropriate protection and management of personally identifiable information you share with us. We urge you to review Sun Microsystems' privacy policy at <http://www.sun.com/privacy> prior to registration of your product to understand the steps we take to respect your privacy.

Product Registration	
Full Name	Mick Taylor
Job Title	President
Company Name	MTC Consulting, Inc.
Full Address	1234 Harmony Way Pleasant Burb, CA 91234
Country	USA
Email Address	user@example.com
Phone Number	1-800-111-2222

Navigation: Left arrow, Right arrow, and a warning icon (exclamation mark in a triangle) with a right arrow.

Completing configuration with the Setup Wizard

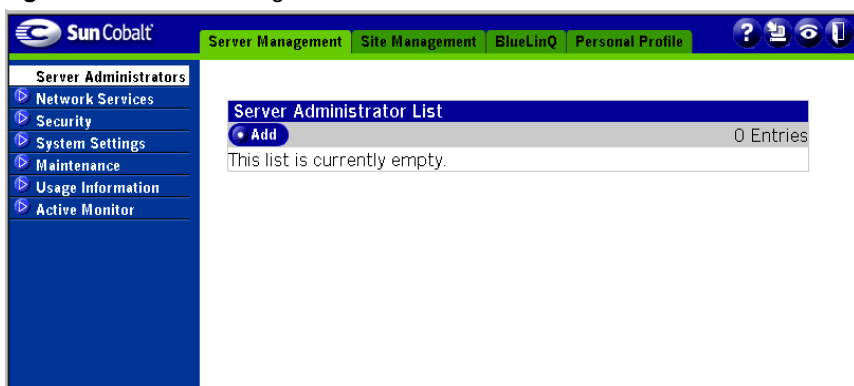
When you complete the **Product Registration** screen, click the right arrow at the bottom.

Once the Sun Cobalt RaQ 550 server appliance has been configured, the screen shown in Figure 11 appears.



Note: If you changed the system time in the System Settings screen, you may be presented with the login screen.

Figure 11. Server Management on the user interface



There are four tabs at the top of the screen:

- Server Management (for details, see Chapter 4, “Server Management”)
- Site Management (for details, see Chapter 5, “Site Management”)
- BlueLinQ (for details, see Chapter 6, “BlueLinQ”)
- Personal Profile (for details, see Chapter 7, “Personal Profile”)

The buttons on the left side of user interface provide access to the information and functions on this site. Move the mouse pointer over the menu buttons and a description of the user interface features appears in the help text frame at the bottom.

The icons in the upper right-hand corner of the screen are described below:

Help icon



You can access the user manual in PDF format from the user interface. If you have installed third-party software on the Sun Cobalt RaQ 550 server appliance, the relevant documentation is available on this screen.

To access the PDF file for the user manual, click on the help icon in the top right corner. A separate browser window opens displaying a list of PDF files in the languages available. Click the link for the PDF in your preferred language; you can open the PDF file in the browser window or save it to your personal computer.

Software Notification icon



The Software Notification icon allows you to check for new or updated software packages and to install them if any are found. The icon changes color when new or updated software packages are available.

For more information on installing software, see Chapter 6, “BlueLinQ”.

Active Monitor icon



The Active Monitor icon allows you to view system and services status information. The icon turns red and blinks if any of the components monitored by Active Monitor have severe problems.

For more information on the Active Monitor feature, see “Active Monitor” on page 99.

Logout icon



Click this icon to log out of the system.

Software Auto-Provisioning (AutoUpdate)



Note: Auto-provisioning is a very advanced feature and should be used only if the Sun Cobalt RaQ 550 server appliance is part of a service that uses this feature; otherwise, ignore this entire section.

For service deployment with this feature, please consult the service provider deployment guide (available separately from your service provider).

The AutoUpdate feature is aimed at organizations that wish to customize large numbers of Sun Cobalt RaQ server appliances with their own package, but do not wish to be locked into a Configure-to-Order (CTO) process. If your ISP has set up an auto-provisioning server, AutoUpdate allows the person doing the installation to point the Sun Cobalt RaQ 550 server appliance at the auto-provisioning server and have the server appliance automatically load the available packages. The connection takes place over a secure (HTTPS) channel, and the use of authentication, through the standard HTTP access mechanism, is supported (and recommended).

The AUTOUPDATE option is available through the LCD console. It can be found in a similar manner to all other LCD menu items:

1. Hold down the **Select** button on the server appliance until you are presented with the `SELECT: <name of a menu item>` prompt on the LCD screen (where `<name of a menu item>` is an item on the LCD menu).
2. Continue pressing the **Select** button until you see the `AUTOUPDATE` menu item.
3. Press the **Enter** button to view the `AUTOUPDATE` menu items.

The available menu items allow you to configure the IP address of an auto-provisioning server, enable an SSL connection and enter a token to authenticate. Sending commands through the LCD interface checks the availability of an external auto-provisioning server. If the specified server cannot be found, an error message is returned.



Note: You can only configure an AutoUpdate server through the LCD console. This feature is not available in the Server Desktop UI.

Services

This chapter offers a brief overview of the services available on the Sun Cobalt RaQ™ 550 server appliance.

These services include:

- Web publishing (see “Publishing Web pages using FTP” on page 38)
- Redundant array of independent disks Level 1 (RAID-1) and Level 0 (RAID-0) (see “RAID-1 and RAID-0 support” on page 40)
- Back up and restore data (see “Back up and restore data” on page 44)
- Secure sockets layer (SSL) (see “Secure sockets layer (SSL)” on page 44)
- Simple Network Management Protocol (SNMP) (see “Simple Network Management Protocol (SNMP)” on page 45 and “SNMP” on page 65)
- Managing virtual sites, each with their own Web, mail, usage statistics and FTP settings (see Chapter 5, “Site Management,” on page 103)
- Enabling JavaServer Pages™ (JSP™) and Servlets, ASP, PHP scripting, Common Gateway Interface (CGI) and FrontPage Extensions (see Chapter 5, “Virtual Site List,” on page 108)
- Installing software (Chapter 6, “BlueLinQ,” on page 143)
- Domain Name System (DNS) server (see Appendix B, “Domain Name System,” on page 167)

Managing your personal profile

Registered users on the Sun Cobalt RaQ 550 server appliance can manage their own Personal Profile, including changing their password, using a standard Web browser such as:

- Macintosh OS9: Internet Explorer 5 or Netscape™ 4.78
- Macintosh OSX: Internet Explorer 5.1
- Windows 98/NT/2000: Internet Explorer 5.5 and 6.0 or Netscape 4.78

The features accessible from the Personal Profile screen are:

- Account
- Email
- Disk usage

For more information, see Chapter 7, “Personal Profile,” on page 149.

Using email on the server appliance

To use all of the email capabilities on the Sun Cobalt RaQ 550 server appliance, you must configure the email settings correctly. You must also configure your email client to send email to and retrieve email from the server appliance.

Email aliases

Each registered user on the Sun Cobalt RaQ 550 server appliance must have a unique user name (for example, mary or john.smith or khoward). This user name is used to send or retrieve email.

The Email Alias feature allows you to create an arbitrary email address without creating a user account on the server appliance. An email message addressed to the alias is forwarded to an existing email address.

If you add more than one alias for a user, enter one alias per line. You can only use lowercase alphanumeric characters, periods (.), hyphens (-) and underscores (_) in the alias.

Let us say that the XYZ Company has a Sun Cobalt RaQ 550 server appliance and that the company’s domain name is xyz.com. The email addresses for the users of the server appliance is <username>@xyz.com. Employee Andrew Bose has a user name of “abose”; his email address is “abose@xyz.com”.

Users can have several email aliases that point to their user name. For example, Andrew Bose can have the aliases “andrew@xyz.com” and “andrew.bose@xyz.com”. If he were an avid soccer player, he might want to use the alias “striker@xyz.com”. All of these aliases point to his user name <abose> at xyz.com. Email messages addressed to any of these aliases are forwarded to “abose@xyz.com”.

However, having a large number of aliases for each user can cause problems. If a new user is added and the user name that is automatically generated by the server appliance is already in use, a warning appears in the help text at the bottom of the screen, stating that <username> has already been taken by another person. In this case, the server appliance does not accept the New User entry.

Following the previous example, let us say that Andrew Boisvert is a new employee at the XYZ Company. If he wanted to have “andrew” as his user name, the server appliance help text displays:

“Sorry, you have entered a value for User Name that has already been taken by another person on this system. Please enter another value for User Name.”

The system suggests an alternate user name.

The Sun Cobalt RaQ 550 server appliance verifies the alias that you enter. If the alias is already in use as a user name, as another user’s alias or as the name of a mailing list, the server appliance does not allow the new alias.

An Administrator can also set up aliases such as `webmaster@xyz.com`, `info@xyz.com`, `sales@xyz.com`, `comments@xyz.com` or `support@xyz.com` that point to a specific user name.

Email relaying

Simple Mail Transfer Protocol (SMTP) service is different from Post Office Protocol (POP), telnet and File Transfer Protocol (FTP) services in that SMTP does not try to authenticate a user when an SMTP connection is made. Every email server on the Internet has to be able to deliver email to you, so the email servers must be able to connect freely to send the email.

The Sun Cobalt RaQ 550 server appliance accepts email if the recipient has a user account or an alias email account, or if the sending host (your client computer) is trusted to relay outgoing email messages to another domain. These trusts are defined by host or domain names, as well as by IP addresses and networks. A network is a range of IP addresses; a network can be as small as one IP address, but that is not very practical.



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

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

If you have users who access your server through the Internet, ask your ISP which networks are used by their remote access (dial-up) equipment. If the ISP says the network 209.43.21.5/24 and 209.48.66.5/16, add “209.43.21.0” and

“209.48.0.0” to the “Relay email from these hosts/domains” field of the Email Parameters menu. If your ISP gives you a list of 30 networks used by 30 points-of-presence (which are regional ISP offices) across the country and your clients can dial in from any of them, then you must trust all 30 networks or these users cannot send email through your server appliance.



Note: By default, the domain name for the Sun Cobalt RaQ 550 server appliance is allowed to relay email.

If you do not want to allow email originating from the domain to which your server appliance belongs to be relayed through your server appliance, enter the domain name of your server appliance in the “Block Email From Hosts/Domains” field.

You will be then able to download email but not be able to send outgoing email messages through Sun Cobalt RaQ 550 server appliance.

POP-before-SMTP feature

The Sun Cobalt RaQ 550 server appliance provides an option to allow POP authentication before SMTP.

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

When a user logs in for POP3 email, the Sun Cobalt RaQ 550 server appliance notes the IP address from which the connection was made and permits relay from that IP address for a limited time. Travelling users need only check their email to “unlock” the mail server; no changes to the client mail software are necessary.

The POP-before-SMTP implementation causes the IP addresses to expire after 30 minutes.

Mailing lists

A mailing list allows you to send messages to a certain group of people without having to address them individually. You can create a mailing list comprising users registered on the Sun Cobalt RaQ 550 server appliance as well as email addresses external to the server appliance. See “Mailing Lists” on page 127 for more details on how to set up and use mailing lists.

Developing Web pages

The Sun Cobalt RaQ 550 server appliance automatically provides a default home page for each individual user. It also supports a broad range of Web publishing capabilities that allow both novice and expert users to build and publish custom Web pages.



Note: To access your home page, enter the URL `http://<hostname>/~<username>/`, where `<hostname>` is the fully qualified domain name of your Sun Cobalt RaQ 550 server appliance and `<username>` is your user name on the server appliance.

You must include the tilde mark (~) before your user name.

FrontPage 2002 Server Extensions

The Sun Cobalt RaQ 550 server appliance includes the FrontPage 2002 Server Extensions, which allow you to use the FrontPage client application to publish and edit Web content easily. You can create and post Web pages using standard style templates and pre-configured tools—including form processing and search tools. It is not necessary to know anything about FTP or other file transfer protocols.



Note: When you create a user with FrontPage web enables, files totaling approximately 14 MB are copied to the user's home directory. Creating an excessive number of such users may cause the disk partition to become full.

The Administrator can enable Microsoft FrontPage Server Extensions for each virtual site (see Chapter 5, “Virtual Site List,” on page 108).

When you enable FrontPage Server Extensions on the Sun Cobalt RaQ 550 server appliance, a FrontPage client *webmaster* account is created and you must provide a password for the *webmaster* account.

The “webmaster” account simply means that when you log in to the root web (`http://<your.host.domain>/`) using FrontPage, your user name is *webmaster* and the password is whatever you entered in the Web Settings table.



Note: The *webmaster* account does NOT have Web, email or FTP service. It is simply an account to use in the FrontPage client.

If FrontPage Server Extensions are enabled, the Web Settings table shows a check box indicating that the feature is enabled. If you disable FrontPage Server Extensions and save the changes, the Web Settings table refreshes to show the feature as disabled and a *webmaster* password field is now displayed in the table.

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

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

- Modify Web content
- Create and manage FrontPage subwebs
- Add, modify or remove additional FrontPage user accounts
- Change the *webmaster* password

If FrontPage Server Extensions are enabled on a site, a Site Administrator can enable FrontPage User Webs.

To publish a Web page using FrontPage:

1. Using FrontPage Explorer on a personal computer, select **Open Web**.
2. In the Folder Name field, enter the following:
`http://<exactvirtualsitename>/~<username>/`
For example, the user Jason Paez would enter
`http://raq550.cobalt.com/~jpaez/`
3. Click **OK**. An authentication dialog appears.
4. Enter your user name and password assigned to you on the server appliance.
5. Click **OK**.

For FrontPage and FrontPage Web information and technical support, see <http://www.microsoft.com/frontpage/> and <http://www.rtr.com/>.

Using an HTML editor

You can create Web pages using any of the standard HTML editors and the HTML publishing capabilities of many popular desktop productivity applications. You can create and link the Web pages themselves on your desktop computer, and then move them to the appropriate subdirectory in the Sun Cobalt RaQ 550 server appliance through an FTP application; see “Publishing Web pages using FTP” on page 38.

CGI scripts

The Sun Cobalt RaQ 550 server appliance supports common gateway interface (CGI) scripts, such as those written in Perl or C, as well as UNIX® shell scripts.

CGI scripts allow you to develop highly interactive, powerful Web-based applications by building server-side CGI scripts that generate Web pages in response to specific user inputs. These applications range from simple scheduling and conferencing applications to sophisticated electronic commerce solutions.

You can develop CGI scripts on your desktop machine and then transfer them to the server appliance through an FTP-based application that allows the permissions to be set to “Executable”.

CGI scripts must use .pl or .cgi filename extensions in order to be executed by the Web server.

Use FTP to upload .cgi and .pl files; use ASCII mode to upload CGI files. Once the file is on the Sun Cobalt RaQ 550 server appliance, use your FTP program to make the script executable. You can also use the telnet command:

```
chmod 775 <filename>.cgi
```

The path to Perl is

```
/usr/bin/perl/
```

Server-side scripting languages

The Sun Cobalt RaQ 550 server appliance supports both the Active Server Pages (ASP) and PHP scripting languages. These features are enabled on a per-site basis (see the “Web Settings” table under **Site Management > Services > Web**).

Like CGI scripts, you can develop ASP and PHP scripts on your desktop machine and then transfer them to the server appliance by means of an FTP-based application. Unlike CGI scripts, ASP and PHP do not require execute permissions to work correctly. However, ensure that the Web server process can read the scripts; you can use the telnet command:

```
chmod 664 <filename>.asp or chmod 664 <filename>.php
```

For the Web server to run the scripts correctly, ASP scripts must use the .asp filename extension and PHP scripts must use the .php filename extension.

The Sun Cobalt RaQ 550 server appliance is pre-configured with support for embedded PHP scripts. You can save PHP files in any directory on your site, provided that the file ends with a .php extension, as previously mentioned.

Publishing Web pages using FTP

After creating your Web pages, you can publish them on the Sun Cobalt RaQ 550 server appliance using an FTP-based application.

Make sure you have the following information:

- The host name or the IP address of your server appliance
- Your user name and password
- A filename of your choice to save as your main page (the default is `index.html`)

Launch your FTP software and establish an FTP link to the server appliance. Upload your HTML files. If you need help, consult the instructions for your FTP application.

By default, the files you upload using an FTP-based application are stored in your personal directory; the directory path is:

```
/home/sites/<sitename>/users/<username>
```

where <sitename> is the fully qualified domain name of your virtual site and <username> is your user name.



Note to the Site Administrator: To post Web pages for your site, you must upload to the directory `/home/sites/<sitename>/web`.

Only Site Administrators or the Server Administrator can upload to this directory. If you do not specify this directory, your Web pages are stored in your personal directory which is not accessible from the Web.

The Site Administrator can access and update the site root content in the directory `/web` during an FTP session. The site Web root is accessible on the Web at `http://<sitename>/`.

Site Administrators can update their personal Web pages in the directory `/users/<username>/web` during an FTP session. Personal Web sites are accessible on the Web at `http://<sitename>/~<username>/`

Users who are not Site Administrators can update their personal Web sites in the directory `/web` during an FTP session.

Domain Name System (DNS)

The Domain Name System (DNS) is a vital and integral part of the Internet. Setting up DNS correctly on your Sun Cobalt RaQ 550 server appliance is very important. For this reason, we have created an appendix solely for explaining DNS. See Appendix B, “Domain Name System,” on page 167.

The appendix covers the following items:

- Basic DNS issues
- Advanced DNS issues
- A quick start guide detailing a sample setup of DNS for a Sun Cobalt RaQ 550 server appliance
- A brief history of the DNS service

If your network administrator is using the Sun Cobalt RaQ 550 server appliance as a DNS server, you can enter the IP address of the server appliance into the “DNS server” field in the TCP/IP configuration on your desktop computer.

RAID-1 and RAID-0 support

RAID-1 and RAID-0 are both available on the Sun Cobalt RaQ 550 server appliance.

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

There are a variety of different types and implementations of RAID, each with its own advantages and disadvantages. The Sun Cobalt RaQ 550 server appliance implements RAID Level 1 (RAID-1), also known as disk mirroring, which consists of a primary hard disk and a secondary hard disk; the secondary hard disk is an exact copy or “mirror image” of the primary hard disk. RAID-0 is also available. RAID-0 stripes data across two disks, making the two disks appear as one large disk (about the size of the two disks combined). While this gives you more disk size, if either disk fails, data will be lost.

Although RAID can protect against disk failure, it does not protect against operator and administrator (human) error, or loss due to system errors.

The server appliance configuration uses Software RAID, meaning that it implements RAID in the software and requires no extra hardware.

RAID-0 must be enabled through the Setup Wizard. RAID-1 is enabled by default if your server contains two hard disk drives.

Hard disk drive failure

When RAID-1 is implemented, if one of the hard disk drives fails, the Sun Cobalt RaQ 550 server appliance can function with one drive, but the server can no longer provide disk mirroring. To restore RAID service, you must shut down the server appliance and replace the failed drive. If RAID-0 is implemented and a hard disk drive fails, there is no recovery.



Caution: The hard disk drives in the server appliance are not hot-swappable; the system must be powered off before removing and replacing drives.

When a drive fails, Active Monitor (see Chapter 4, “Active Monitor,” on page 99) indicates which drive has failed (Drive 1 or Drive 2). As viewed from the front, Drive 1 (known in Linux as `hda`) is closest to the front of the server appliance and Drive 2 (known in Linux as `hdc`) is behind it.



Note: To access the drives, remove the AC power cable, then remove the top cover by unscrewing the two thumbscrews towards the top outside position in the back of the server. Slide the cover back and lift it off.

If one of the RAID 1 hard disk drives fails on the Sun Cobalt RaQ 550 server appliance, the system indicates the RAID status in three ways:

- An email is sent to the Administrator
- The Active Monitor Disk Integrity indicator circle changes to red
- The amber Service Fault LED illuminates

Once you replace a failed drive and then reboot the server appliance, the system detects the new hard drive. It then automatically begins to synchronize the new hard drive to the existing hard drive so that the server will be able to provide disk mirroring.



Note: During the synchronization process, the Sun Cobalt RaQ 550 server appliance cannot provide disk mirroring but it can still serve requests.

System health monitoring

Through a combination of software and hardware monitoring techniques, the Sun Cobalt RaQ 550 server appliance monitors the events described in this section.

Fan, voltage and temperature monitoring

Through the use of built-in sensors, the server appliance monitors internal voltage and temperature levels as well as fan operation. If inappropriate behavior is observed, action is taken to protect the system.

Fan monitoring

The speed of the enclosure fans and power supply fan is monitored. If it is verified that any fan is rotating too slowly, or has stopped, the amber System Fault LED is illuminated.

Temperature monitoring

There are two temperature sensors in the server appliance: one that monitors the CPU core temperature and another that monitors the ambient temperature inside the enclosure. If the temperature for either sensor exceeds a preset threshold, an event is triggered. If it is verified that the temperature is indeed too high, the software issues a shutdown command and the server powers off. The amber System Fault LED is illuminated and an email is sent to the Administrator.

Voltage monitoring

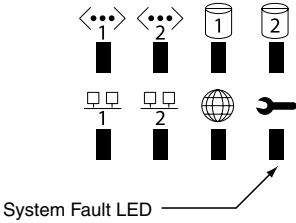
Three voltages are monitored in the server: V_{TT} , V_{CORE} and V_{BAT} . The first two voltages pertain to the CPU, and the third pertains to the button-cell battery on the motherboard that preserves CMOS memory configuration data for the server.

If the CPU voltages exceed preset thresholds, the software issues a shutdown command and the server appliance powers down. If the battery voltage drops too low, Active Monitor, if so configured, can send emails periodically warning that the battery voltage is low and that the battery needs replacement. The amber System Fault LED is illuminated.

System Fault LED

The amber System Fault LED (wrench symbol) is shown in Figure 12.

Figure 12. System Fault LED



The System Fault LED illuminates if any of the following conditions exist:

- Failure of either enclosure cooling fan (runs too slowly or stops altogether)
- Failure of the power supply fan (runs too slowly or stops altogether)
- Overheating of the enclosure
- Overheating of the CPU
- Hard disk drive failure (failed, missing or defective drive)
- Any abnormal power supply voltage level
- Major failure in DIMM memory (any uncorrectable ECC error or more than 10 correctable ECC errors within 24 hours)
- Low CMOS lithium battery level (checked once every 24 hours)



Note: When the server appliance is powered off, if the server is still connected to AC wall power, the amber System Fault LED remains on if it was on before power removal.

If AC power is removed, the state of the LED is lost. However, the LED does illuminate during power up after AC power is restored, which indicates that AC power was lost. If all the power-up self tests pass, the LED is extinguished. If any test fails, the LED remains illuminated.

Back up and restore data

For complete system-wide scheduled backup and restore operations, including virtual sites and all personal data, it is recommended that you use a third-party product, such as Legato Networker® or Knox Arkeia. See “Maintenance” on page 90 for more information on system-wide backups.

Secure sockets layer (SSL)

The Administrator can administer the Sun Cobalt RaQ 550 server appliance through secure sockets layer (SSL). SSL is provided in 128-bit encryption code and offers a secure Web connection to the end user. The implementation of SSL on the server appliance is based on `mod_ssl` and includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”

A secure connection means two things: encryption and authentication. Encryption ensures that no one can snoop the connection between the browser and the Sun Cobalt RaQ 550 server appliance; authentication ensures the client, through a certificate, that the server is who they say they are. The security is assured on two levels.

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

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

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

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

On the Sun Cobalt RaQ 550 server appliance, a self-signed certificate is generated by the server appliance during configuration.

For more information on *authentication*, *encryption* and *secure sockets layer*, refer to Appendix H, “Glossary”.

Install software

You can add new software to the Sun Cobalt RaQ 550 server appliance through the browser interface. You can install new software obtained either from the Sun Cobalt Web site or from a CD supplied by Sun Microsystems, Inc. You can also add third-party software.

For more information, see Chapter 6, “BlueLinQ,” on page 143.

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) is 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. See “SNMP” on page 65 for how SNMP is used to access the Sun Cobalt RaQ 550 server appliance.

Server Management

This chapter describes the server management functions that only the Administrator of the Sun Cobalt RaQ™ 550 server appliance is allowed to perform. The Administrator, with the user name *admin*, has full control of the server appliance.

The Administrator of the Sun Cobalt RaQ 550 server appliance:

- Creates other server administrators
- Enters the network settings
- Enables or disables the various services
- Adds and deletes sites
- Adds and deletes users and mailing lists
- Performs maintenance functions
- Receives system alerts and warnings by email



Note: In most of the short procedures in this chapter, the first step is to click the **Server Management** tab in the top menu bar and the second step is to click on a selection from the left menu bar.

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

For example, select **Server Management > System Settings > TCP/IP** means to click the **Server Management** tab in the top menu bar, click the **System Settings** menu category in the left menu bar and finally click the **TCP/IP** sub-menu item.



Note: You cannot use accented characters (for example, ä, é, ñ) in the following items:

- User names
- Email addresses and email aliases
- Host names and domain names

You can use accented characters in descriptive fields, for example, in the Full Name field for a user.

Server Management on the user interface is available only when you log in under the user name *admin*. Besides the options on the standard user interface, there are two other options: the Administration menu and the BlueLinQ. See Figure 13.

Resetting the Administrator password

If you simply want to change the Administrator password for the server appliance, you can do so through the Server Desktop UI.

If you forget the Administrator password for the server appliance, you can reset the password. This is done in two steps:

- a. Clear the password through the LCD console.
- b. Enter a new password for the *admin* account through the Server Desktop UI.



Note: When the Administrator password for the server appliance is cleared, the default password (*admin*) is assigned. Because you can access the *root* and *admin* account until a new password has been assigned, you should assign a new password as soon as possible.

Clearing the password through the LCD console

To clear the Administrator password for the server appliance:

1. On the LCD console, hold down the **(S)** button for approximately 2 seconds.

The LCD screen displays:

```
SELECT:
  SETUP NETWORK
```

2. Press the **(S)** button until the following message appears on the LCD screen:

```
SELECT:
  RESET PASSWORD
```

3. Press the **(E)** button. The LCD screen displays:

```
RESET PASSWORD?
[Y]ES [N]O
```

4. Use the arrow buttons to toggle the cursor between [Y]ES and [N]O.
5. If you choose [N]O, the LCD screen returns to the host name and IP address.
6. If you choose [Y]ES, the LCD screen displays.

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

The LCD screen then displays the host name and IP address again.



Caution: This function resets the Administrator password for the server appliance to admin.

After you clear the password, enter a new one as soon as possible to protect the security of the server appliance. At this point, anyone on the network can assign the Administrator password until you assign a new one.

7. To modify the Administrator password, follow the steps under “Account” on page 149.

Accessing Server Management

To access the Server Management: tab on the Sun Cobalt RaQ 550 server appliance:

1. Enter the following URL into your browser:

`http://<hostname>.<domainname>/login/`

2. At the login screen that appears, enter the user name:

`admin`

Only this user name and the server administrators added by the Administrator can access the Server Management section. Any other user name brings up the normal Server Desktop UI. A server administrator can be given different levels of access by the Administrator.

3. Enter the admin password.
4. If you want to establish a secure connection when you log in to the server appliance, click the Secure Connect check box. This establishes a Secure Sockets Layer (SSL) connection between your browser and the server appliance. Sun Cobalt recommends that you enable the secure connection so that any data sent to or received from the Sun Cobalt RaQ 550 server appliance is encrypted.

If your browser does not support SSL or has problems accessing the server appliance, try connecting without enabling the secure connection. Some browsers do not handle SSL properly and the only option is not to use SSL.

5. Click **Login**. If you enabled the Secure Connect option, your browser may prompt you to accept a self-signed certificate. This certificate is generated automatically for you and is required for SSL encryption. If you do not accept the certificate, you cannot use the Secure Connect option.

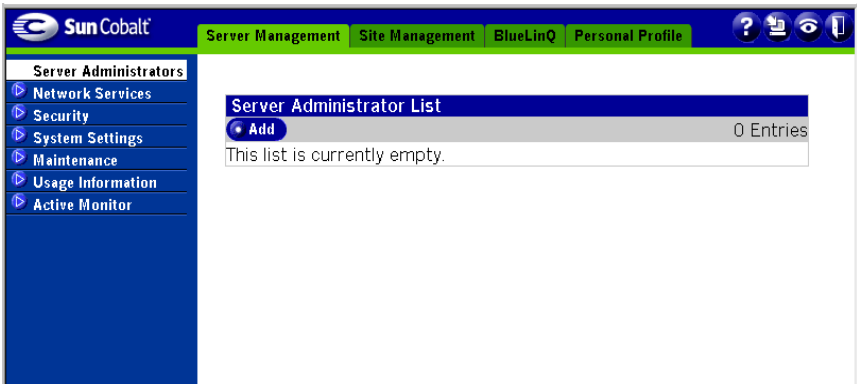


Note: The Sun Cobalt RaQ 550 server appliance generates a self-signed certificate during configuration. A self-signed certificate encrypts the data but it does not authenticate the identity of the server at the other end of the connection.

For more information, see the entries for *Authentication*, *Encryption* and *Secure Sockets Layer* in Appendix H, “Glossary”.

6. The **Server Management** screen of the user interface appears; see Figure 13.

Figure 13. Server Management screen



The following bullet items represent the fully expanded menu items on the left side of **Server Management** screen. These are the functions and services that the Administrator can manage from the **Server Management** screen. They are explained in this chapter.

- Server Administrators (see page 53)
- Network Services (see page 55)
 - Web
 - ASP
 - FTP
 - Email
 - DNS
 - SNMP
 - Shell
- Security (see page 67)
 - Scan Detection
 - Buffer Overflow
 - SSL

- System Settings (see page 74)
 - TCP/IP
 - IP Address Allocation
 - Bandwidth Limits
 - Power
 - UPS
 - Time
 - Information
- Maintenance (see page 90)
 - Server Desktop
 - Knox Arkeia
 - Legato NetWorker
 - Additional Storage
- Usage Information (see page 95)
 - Network
 - Web
 - FTP
 - Email
 - Disk
- Active Monitor (see page 99)
 - Status
 - Settings

Server Administrators

The Server Administrators section is where you create and manage server administrator accounts. Creating separate server administrator accounts other than the *admin* account allows the Administrator to allow trusted third parties to manage the server. Server administrator accounts can be created to have all the same powers, except for managing the administrator accounts controlled from the *admin* account. Server administrator accounts can also be created with more limits on which aspects of the server appliance they are allowed to control.

Click **Add** to add a new server administrator account. The screen shown in Figure 14 appears.

Figure 14. Add New Server Administrator screen

Add New Server Administrator	
User Information	
Full Name	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="password"/>
	<input type="password"/> (Enter Again)
Maximum Allowed Disk Space (MB)	<input type="text" value="20"/>
Administrator Options	
Additional Access Rights (optional)	Extra Abilities
	Available Abilities
	<input type="text" value="Empty"/>
	<input type="checkbox"/> IP Address Allocation <input type="checkbox"/> Control Power <input type="checkbox"/> Root Access
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

There are two areas within the Add New Server Administrator main screen:

- User Information
- Administrator Options

Configure the User Information fields:

1. Enter the full name, user name and password of the new Server Administrator.
2. Enter the maximum amount of disk space in megabytes (MB) that this user should be allowed to use on this server. Leave the field blank to give the user access to an unlimited amount of disk space.

Configure the Administrator Options:

1. Move extra abilities that this server administrator account should be allowed from the **Available Abilities** column to the **Extra Abilities** column.
 - **IP Address Allocation:** used to specify acceptable IP address ranges for this server. See “IP Address Allocation” on page 78 for more details.
 - **Control Power:** used to specify how the system reacts to power outages. See “Power” on page 82 and “UPS” on page 85 for more details.
 - **Root Access:** used to allow Server Administrators to have root access to the server over a telnet connection.
2. Click **Save**.



Note: This optional area of the screen allows restoration of certain abilities to a Server Administrator that are normally reserved for the *admin* user alone.

Network Services

This section allows you to control the server's services. The following submenus are available:

- Web
- ASP
- FTP
- Email
- DNS
- SNMP
- Shell

Web

Selecting the **Web** menu item brings up the **Web Settings** screen shown in Figure 15.

Figure 15. Web Settings screen

Web Settings	
Hostname Lookups	<input type="checkbox"/>
Maximum Simultaneous Connections	<input type="text" value="125"/> (1 - 292)
Minimum Spare Servers	<input type="text" value="10"/> (1 - 146)
Maximum Spare Servers	<input type="text" value="25"/> (1 - 146)

• Save

1. Configure the settings in the table:

- **Hostname Lookups.** Use this to turn on host name lookups for the Web server. This causes the server appliance to do a DNS lookup on the client IP address when it connects to the server and record it in the log files. This host name information is then available in the server appliance usage Web reports. Without this feature, only client IP addresses are reported in the Web server usage domain report.



Warning: Enabling this option will decrease the performance of your Web server.

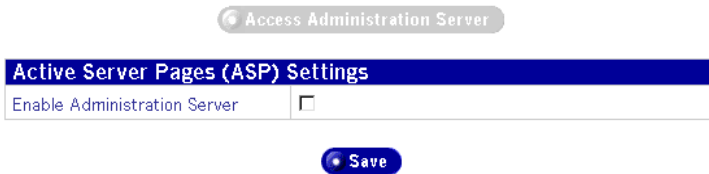
- **Maximum Simultaneous Connections.** This is the maximum number of requests that can be made to the server at any instance. Each connection requires its own Web server process. If this number is exceeded, clients will receive a message that the server is busy and will be asked to try again later. This setting is useful for controlling the load on your server. The maximum number of Web servers is limited by the amount of RAM installed in this server.
- **Minimum Spare Servers.** When the Web server starts or is in an idle state, this is the minimum number of Web server processes available for serving Web requests. The maximum number of Web servers is limited by the amount of RAM installed in this server.
- **Maximum Spare Servers.** The Web server will launch additional processes, as needed, to service additional load. This number is the maximum number of processes the system will launch. High traffic sites should increase this number for better performance. The maximum number of Web servers is limited by the amount of RAM installed in this server.

2. Click **Save**.

ASP Administration

Selecting the **ASP Administration** menu item brings up the **Active Server Pages (ASP) Settings** screen shown in Figure 16.

Figure 16. ASP Settings screen



1. Click the **Enable Administration Server** checkbox to enable the ASP Administration Server
2. Click **Save**.

After enabling the ASP Administration Server, the **Access Administration Server** button becomes active.

3. Click **Access Administration Server** to access the ASP Administration Server for advanced control and database connectivity support.

The public ASP service is automatically enabled if any site is using the ASP service.

FTP

Selecting the **FTP** menu item brings up the **File Transfer Protocol (FTP) Settings** screen shown in Figure 17.

Figure 17. FTP Settings screen

File Transfer Protocol (FTP) Settings	
Enable Server	<input checked="" type="checkbox"/>
Maximum Connection Rate	<input type="text" value="80"/> (1 - 1,024)

[Save](#)

1. Configure the settings in the table:

- **Enable Server.** Use this to turn File Transfer Protocol (FTP) functionality on or off. Anonymous FTP access is configured by going to guestShare.
- **Maximum Connection Rate.** Enter the maximum number of allowed connections per minute. New connections will be denied if the connection rate has reached this limit.

Email Servers

This section describes how the Administrator configures the email settings on the Sun Cobalt RaQ 550 server appliance. For additional information about setting up your email client to access email on the server appliance, see “Using email on the server appliance” on page 32.

The server appliance supports email for entire domains such as `www.mydomain.com`. By default, each registered user has an email account created on the server appliance.

The server appliance supports multiple client and server email protocols but does not implement virtual email users. This means that for the entire server appliance, each user must have a unique username.

The server appliance can act as a Simple Mail Transfer Protocol (SMTP) server for sending and receiving Internet email.

Users can retrieve their email using the Post Office Protocol 3 (POP3) and the Internet Message Access Protocol 4 (IMAP4). Users can send mail using the Simple Mail Transfer Protocol (SMTP).



Important: If your Internet service provider (ISP) also provides your Domain Name System (DNS) service, the ISP must create a Mail Server (MX) record specifying your Sun Cobalt RaQ 550 server appliance as the mail server for your registered domain in order for the server appliance to receive email.

If your server appliance is integrated into a larger network, consult with your network administrator for this information.

The IP address of the DNS server must be entered in the network settings for the server appliance or the SMTP protocol will not work.

For more information, see “Product Registration” on page 27.

If you are providing your own DNS service through the Sun Cobalt RaQ 550 server appliance, you need to create an MX record for the server appliance. For more information on DNS, see Appendix B, “Domain Name System,” on page 167.

Selecting the **Email Servers** menu item brings up the **Email Servers Settings** screen shown in Figure 18.

Figure 18. Email Servers Settings (Basic Tab) screen

Email Servers Settings	
	<input type="button" value="Basic"/> <input type="button" value="Advanced"/>
Enable SMTP Server	<input checked="" type="checkbox"/>
Enable IMAP Server	<input checked="" type="checkbox"/>
Maximum IMAP Connection Rate	<input type="text" value="1024"/> (1 - 4,096)
Enable POP Server	<input checked="" type="checkbox"/>
Maximum POP Connection Rate	<input type="text" value="80"/> (1 - 1,024)

Basic Tab

- Fill in the Basic tab settings on the **Email Servers Settings** table:
 - Enable SMTP Server.** Use this checkbox to turn the Simple Mail Transfer Protocol (SMTP) service on or off. Enabling SMTP allows this server appliance to act as an SMTP server for sending and receiving Internet email between other servers. SMTP also allows users to use this server appliance for sending email.
 - Enable IMAP Server.** Use this checkbox to turn the Internet Message Access Protocol (IMAP) service on or off. Enabling this service allows users to retrieve email from this server appliance using email clients that support IMAP. IMAP allows users to store email on the server but requires continuous access to the server during the time the user is working with their mail.
 - Maximum IMAP Connection Rate.** Enter the maximum number of allowed connections per minute. New connections will be denied if the connection rate has reached this limit.
 - Enable POP Server.** Use this check box to turn the Post Office Protocol (POP) mail retrieval service on or off. Enabling this service allows users to retrieve email from this server appliance using most standard email clients.
 - Maximum POP Connection Rate.** Enter the maximum number of allowed connections per minute. New connections will be denied if the connection rate has reached this limit.
- Click **Save** to save the settings.

Advanced Tab

Clicking the Advanced tab brings up the screen shown in Figure 19.

Figure 19. Email Servers Settings (Advanced Tab) screen

Email Servers Settings	
Basic Advanced	
Delivery Schedule	Immediate
Maximum Email Size (MB) <i>(optional)</i>	
Force Sender Domain <i>(optional)</i>	
Smart Relay Server <i>(optional)</i>	
POP Authenticated Relaying	<input type="checkbox"/>
Relay Email From Hosts/Domains/IP Addresses <i>(optional)</i>	
Block Email From Hosts/Domains <i>(optional)</i>	
Block Email From Users <i>(optional)</i>	

Save

1. Fill in the Advanced tab fields in the **Email Servers Settings** table.
 - **Delivery Schedule.** This setting specifies how frequently email is delivered by the email server on the Sun Cobalt RaQ 550 server appliance. The server appliance queues the messages, sending them at the specified frequency.

If you connect to the Internet through a dedicated phone line or by Ethernet (through the secondary network interface, labeled II on the back panel), then you can choose to have your email delivered and retrieved more often.

- **Maximum Email Size (MB).** Sets the maximum size of email messages this email server will send or receive. Enter an integer greater than 0. The default value is to leave this field empty, which allows this server to send and receive email messages of any size.

- **Force Sender Domain.** An optional domain name can be specified to override the From: address of mail sent by users of this server. This feature is also called Domain Masquerade.
- **Smart Relay Server.** You can enter an optional host name in this field. With this feature, you can configure the Sun Cobalt RaQ 550 server appliance to send Internet email to a specific email server. Enter the host name of the email server through which you want to relay your email.

This feature is useful if the server appliance does not have direct Internet access, but can communicate with an email server that has direct Internet access.

- **POP Authenticated Relaying.** Check this box to enable SMTP relay trusts by POP authentication. If checked, any user who successfully uses POP to check mail is trusted for 30 minutes to send email using the SMTP service. This feature is useful for users who frequently travel.
- **Relay Email from Hosts/Domains/IP Addresses.** Enter the IP addresses, host names or domain names that are allowed to relay email through this Sun Cobalt RaQ 550 server appliance. For more information, see “Email relaying” on page 33.

A user cannot send outgoing email through this server unless the IP address, host name or domain name of the machine from which they are connecting is entered in this field. Networks may be specified in addition to IP addresses. For example, to allow relaying for a network 192.168.1.1 with subnet mask 255.255.0.0, specify the address 192.168.0.0.



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

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



Note: By default, the domain name for the Sun Cobalt RaQ 550 server appliance is allowed to relay email.

If you do not want to allow email originating from the domain to which your server appliance belongs to be sent through your server appliance, enter the domain name of your server appliance in the “Block Email From Hosts/Domains” field.

You will be able to download email but not be able to send outgoing email messages through Sun Cobalt RaQ 550 server appliance.

The entries you add to this field serve as part of a pattern match against the email that the client is sending. As a result, some handy shortcuts are possible. If you have a number of hosts in the same network block, you can, as a shortcut, simply enter the number of the network block.

For example, specifying a network such as 192.168.1.0 in the “Relay email from these hosts/domains” field trusts all IP addresses from 192.168.1.0 through 192.168.1.254.

If you want to allow connections from a host that ends, for example, in mydomain.com, add the string mydomain.com in the text area.



Note: If you are entering a domain name or part of a domain name in the text box, you must have reverse DNS working on your clients.

- **Block Email from Hosts/Domains.** In this field, enter email addresses or domains from which you want to block any email. Anyone trying to send you messages from one of these addresses or domains will receive an error message in return.
- **Block Email from Users.** In this field, enter email addresses of users from which you want to block any email. Anyone trying to send you messages from one of these addresses will receive an error message in return.

2. Click **Save** in the Email Servers Settings table.

DNS

The Domain Name System (DNS) is a vital and integral part of the Internet. Setting up DNS correctly on your Sun Cobalt RaQ 550 server appliance is very important. For this reason, we have created an appendix solely for explaining DNS. See Appendix B, “Domain Name System,” on page 167.

The appendix covers the following items:

- Basic DNS issues
- Advanced DNS issues
- Zone format
- A quick start guide detailing a sample setup of DNS for a Sun Cobalt RaQ 550 server appliance
- A brief history of the DNS service

SNMP

If the SNMP agent is enabled, you can use SNMP software to remotely monitor server information such as CPU utilization and network traffic.

You can specify the Simple Network Management Protocol (SNMP) communities that can have read-only and read-and-write access to this SNMP agent.

The default read-only access community is “public.”

The default read-and-write access community is “private.”



Note: We recommend that you change the default string for the Read and Write SNMP Community to a unique value.

To specify the SNMP communities:

1. Select **Server Management > Network Services > SNMP**. The SNMP Settings table appears; see Figure 20.

Figure 20. SNMP Settings table

Simple Network Management Protocol (SNMP) Settings	
Enable Server	<input type="checkbox"/>
Read Only SNMP Community (optional)	<input type="text" value="public"/>
Read and Write SNMP Community (optional)	<input type="text" value="private"/>

[Save](#)

2. Configure the following settings:
 - **Enable Server.** Turns the Simple Network Management Protocol (SNMP) server on or off.
 - **Read Only SNMP Community.** Enter the Read Only SNMP Community to which this Sun Cobalt RaQ 550 server appliance server belongs. The Read Only SNMP Community you enter can only contain alphanumeric characters along with '-' and '_'.
 - **Read and Write SNMP Community.** Enter the Read and Write SNMP Community to which this server appliance server belongs. The Read and Write SNMP Community you enter can only contain alphanumeric characters along with '-' and '_'.
3. Click **Save**.

Shell

The Shell menu allows you to configure services, such as telnet and ssh, that users with shell access can use to connect to this server appliance.

To specify the Shell settings:

1. Select **Server Management > Network Services > Shell**. The Shell table appears; see Figure 21.

Figure 21. Shell table

Shell	
Enable Telnet Server	<input checked="" type="checkbox"/> Enable Maximum Connection Rate <input type="text" value="40"/> (1 - 1,024)
Enable SSH Server	<input checked="" type="checkbox"/>



2. Configure the selections as follows:
 - **Enable Telnet Server.** Enabling telnet allows users with shell access to connect to this server using telnet client software.

Enter the maximum number of allowed connections per minute. New connection requests will be denied if the connection rate has reached this limit.
 - **Enable SSH Server.** Enabling the SSH server allows users with shell access to connect to this server using SSH client software. Use of SSH is generally considered more secure than use of telnet because SSH encrypts all data, including passwords, that are sent between the client and the server.

Security

The Security section allows you to manage certificates and server security. The following submenus are available:

- Scan Detection
- Buffer Overflow
- SSL

Scan Detection

IP port scanning is the act of systematically scanning a computer's IP addresses. Port scanning can be malicious in nature if someone is looking for a weakened access point to break into your server. If an IP address connects to a specified number of ports within a specified time, the Scan Detection settings allow blocking those IP addresses from connecting to the server.

To specify the Scan Detection settings:

1. Select **Server Management > Security > Scan Detection**. The Scan Detection Settings table appears; see Figure 22.

Figure 22. Scan Detection Settings screen

• View Log • View Blocked IP addresses

Scan Detection Settings	
Action Against Detected Scans	Log only <input type="button" value="v"/>
Time Between Scans (In Seconds)	300 (60 - 600)
Number of Ports Scanned	5 (3 - 8)
Enable Email Alerts	<input type="checkbox"/>
IP Addresses Always Blocked <i>(optional)</i>	<input type="text"/>
IP Addresses Never Blocked <i>(optional)</i>	<input type="text"/>

• Save

2. Configure the selections as follows:
 - **Action Against Detected Scans.** Choose what action to take when a scan is detected. Your choices are to do nothing, log the scans (default), or log the scans and block the machine scanning you.
 - **Time Between Scans (In Seconds).** Maximum time between probes to keep an alert alive.
 - **Number of Ports Scanned.** The number of ports that must be probed by an IP before an alert is generated and, if enabled, the IP is blocked.
 - **Enable Email Alerts.** Enables email alerts when a scan is detected. If enabled, alerts go to the email addresses set in Active Monitor.



Note: To enter an email address for Active Monitor, select **Server Management > Active Monitor > Settings**. For more information, see “Active Monitor” on page 99.

- **IP Addresses Always Blocked.** This list of IP addresses is always denied access to any port on or through the appliance.
 - **IP Addresses Never Blocked.** This list of IP addresses CANNOT be denied access to any port on or through the appliance.
3. Click **View Log** to view the scan detection log file.
 4. Click **View Blocked IP Addresses** to show the list of currently blocked IP addresses.

Buffer Overflow

Malicious buffer overflow can lead to a security problem that allows data to be executed as code, thus compromising the security of your server and its files.

A buffer overflow occurs when you write a set of values (usually a string of characters) into a fixed length buffer and write at least one value outside that buffer’s boundaries (usually past its end). A buffer overflow can occur when reading input from the user into a buffer, but it can also occur during other kinds of processing in a program.

If a secure program permits a buffer overflow, the overflow can often be exploited by an adversary. If the buffer is a local C variable, the overflow can be used to force the function to run code of an attacker’s choosing. This specific variation is often called a “stack smashing” attack. A buffer in the heap is not much better; attackers may be able to use such overflows to control other variables in the program.

The Buffer Overflow menu allows you to manage Buffer Overflow Protection settings.

To specify the Buffer Overflow Protection settings:

1. Select **Server Management** > **Security** > **Buffer Overflow**. The Buffer Overflow Protection settings table appears; see Figure 23.

Figure 23. Buffer Overflow Protection settings screen

Buffer Overflow Protection settings	
Enable Buffer Overflow Protection alerts	<input checked="" type="checkbox"/>



2. Activate the checkbox to be notified by email of Buffer Overflows. If enabled, email will be sent to the addresses set in Active Monitor.



Note: To enter an email address for Active Monitor, select **Server Management** > **Active Monitor** > **Settings**. For more information, see “Active Monitor” on page 99.

SSL

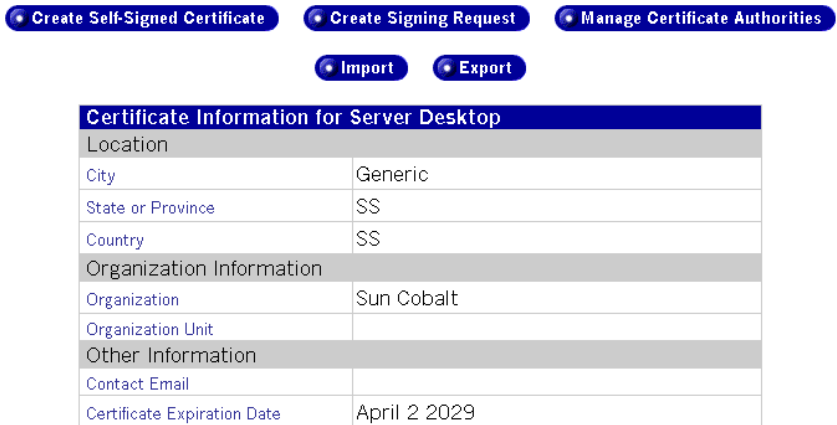
The Secure Sockets Layer (SSL) is a commonly used protocol for managing the security of a message transmission on the Internet. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.

The SSL menu allows you access information about the SSL certificate used for secure access to the Server Desktop UI.

To specify the SSL settings:

1. Select **Server Management > Security > SSL**. The Certificate Information for Server Desktop screen appears along with its associated buttons; see Figure 24.

Figure 24. Certificate Information for Server Desktop screen



• Create Self-Signed Certificate • Create Signing Request • Manage Certificate Authorities

• Import • Export

Certificate Information for Server Desktop	
Location	
City	Generic
State or Province	SS
Country	SS
Organization Information	
Organization	Sun Cobalt
Organization Unit	
Other Information	
Contact Email	
Certificate Expiration Date	April 2 2029

2. To create a new self-signed certificate, click **Create Self-Signed Certificate** and configure the selections as follows:

- **City.** The city in which the organization is located or registered. It is important that this information is correct and can be verified with a local, regional, or national government, or other official organization.
- **State or Province.** The state, province, or region in which the above city is located. It is important that this information is correct and can be verified with a local, regional, or national government or other official organization.



Note: In some cases, the state and province information does not apply, depending on the country and how it is divided into different areas.

- **Country.** Select the country in which the organization that will use this certificate is located or registered. It is important that this information is correct and can be verified with a local, regional, or national government or other official organization.
 - **Organization.** The official name of the organization owning this certificate. In order to obtain a signed certificate from a certificate authority, the organization name and location must be verifiable with a local, regional, or national government or other official organization. In addition, the certificate authority must be able to verify that the person requesting the certificate is the owner or employee of the named organization.
 - **Organization Unit.** The division or unit of the organization that is using this certificate. This is optional, but may be useful if the person applying for a signed certificate is an employee of a subsidiary of a larger organization.
 - **Contact Email.** The email address to be contacted for information about this certificate.
 - **Certificate Expiration Date.** The date after which the certificate should no longer be considered valid by client software attempting to connect to this server.
3. Click **Create Signing Request** to create a certificate signing request. The Signing Request Information for Server Desktop screen appears; see Figure 25.

Figure 25. Signing Request Information for Server Desktop screen

Signing Request Information for Server Desktop	
Generate Self-Signed Certificate	<input checked="" type="checkbox"/>
Location	
City	<input type="text"/>
State or Province	<input type="text"/>
Country	Select country...
Organization Information	
Organization	<input type="text"/>
Organization Unit (optional)	<input type="text"/>
Other Information	
Contact Email (optional)	<input type="text"/>
Valid Period	1 <input type="text"/> year(s)

Create Signing Request Cancel

- After the fields are filled in, activate the **Generate Self-Signed Certificate** checkbox. This allows you to generate a self-signed certificate along with the signing request. The self-signed certificate can be used temporarily while you wait for the Certificate Authority to process your signing request. The certificate signing request can be submitted to a Certificate Authority to create a signed certificate that Web browsers can verify as authentic.
- Click **Manage Certificate Authorities** to add or remove secondary certificate authorities for this site. The Certificate Authority Management for Server Desktop screen appears; see Figure 26.



Note: Secondary certificate authorities are usually not needed, but certain authorities issue an extra certificate to be used for client authentication in addition to the usual server certificate that most certificate authorities issue.

Figure 26. Certificate Authority Management for Server Desktop screen

Certificate Authority Management for Server Desktop	
Management Actions	<input checked="" type="checkbox"/> Add
	Certificate Authority <input type="text"/> Name <input type="text"/> Select Certificate <input type="text"/>

Save Cancel

6. Configure the settings as follows:
 - **Certificate Authority Name.** Enter a unique name to identify this secondary certificate authority.
 - **Select Certificate.** Click **Browse** to select the file that contains the certificate authority's certificate. The certificate should be the only thing in the file.
7. Click **Import** to import a signed certificate; see Figure 27.

Figure 27. Import Certificate for Server Desktop screen

The screenshot shows a dialog box titled "Import Certificate for Server Desktop". It features a text input field labeled "Certificate" and a "Browse..." button. Below the input field are two buttons: "Import" and "Cancel", both with a small circular icon to their left.

8. Click **Browse** to select the text file containing the certificate to import.

The certificate file must contain both the private key and certificate sections if you are transferring it from another server. If the certificate is from a certificate authority to which you submitted a certificate signing request generated by this server, only the certificate is necessary, but it is okay if a private key is included with the signed certificate.
9. Click **Export** to download the current private key and certificate, so the certificate can be transferred to another server.

System Settings

The System Settings section allows you to configure the server appliance's network, bandwidth and time settings. The following submenus are available:

- TCP/IP
- IP Address Allocation
- Bandwidth Limits
- Power
- UPS
- Time
- Information

TCP/IP

To specify the TCP/IP settings:

1. Select **Server Management > System Settings > TCP/IP**. The TCP/IP Settings table appears; see Figure 28.
2. Click the **Primary Settings** tab and configure the selections as follows:
 - **Host Name.** Enter the host name of this Sun Cobalt RaQ 550 server appliance. The host name and the domain name combined together should uniquely identify this server. Enter only lowercase alphanumeric characters, dashes, or periods. For example, www is a valid entry.
 - **Domain Name.** Enter the domain name of this Sun Cobalt RaQ 550 server appliance. The host name and the domain name combined together should uniquely identify this server. Enter only lowercase alphanumeric characters, dashes or periods. For example, sun.com is a valid entry.

Figure 28. TCP/IP Settings screen

Modify Static Routes

TCP/IP Settings	
Primary Settings	
Interface Aliases	
Host and Domain Name	<input type="text" value="www"/> <input type="text" value="example.com"/> <div style="display: flex; justify-content: space-around; font-size: small;"> Host Name Domain Name </div>
DNS Servers <i>(optional)</i>	<input type="text" value="63.77.128.10"/> <input type="text" value=""/> <input type="text" value=""/>
Server Gateway <i>(optional)</i>	<input type="text" value="63.77.128.1"/>
Primary Interface	
IP Address	<input type="text" value="63.77.128.201"/>
IP Network Mask	<input type="text" value="255.255.255.0"/>
MAC Address	<input type="text" value="00:10:E0:04:CA:67"/>
Secondary Interface	
IP Address <i>(optional)</i>	<input type="text"/>
IP Network Mask <i>(optional)</i>	<input type="text"/>
MAC Address	<input type="text" value="00:10:E0:04:CA:68"/>

Save

- DNS Servers.** Enter the IP address or addresses of your local domain name server or servers. A domain name server translates textual host names and domain names into numerical IP addresses and vice-versa. Enter a series of four numbers between 0 and 255 separated by periods. For example, 192.168.1.1 is a valid entry. Leaving this field empty will prevent this machine from finding other machines by host name or domain name and will cause networking difficulties.



Note: Be sure to enter the IP address of your DNS server(s) here. Otherwise, the Simple Mail Transfer Protocol (SMTP) will not work. SMTP is used for transferring electronic mail messages.

For more information, see Appendix B, “Domain Name System,” on page 167.

- **Server Gateway.** Enter the IP address of the local network gateway for this server appliance. This is the gateway for both the primary and secondary interfaces. A network gateway allows your server to connect to the world outside of your local network area. Please enter a series of four numbers between 0 and 255 separated by periods. For example, 192.168.1.1 is a valid entry.
- **IP Address (Primary Interface).** Enter the IP address of the primary interface. If you are using only one network interface connection to the server appliance, use the primary Ethernet interface (labeled I on the back panel) and leave the secondary Ethernet interface (labeled II on the back panel) empty. Enter a series of four numbers between 0 and 255 separated by periods. For example, 192.168.1.1 is a valid entry.
- **IP Network Mask (Primary Interface).** Enter the network mask of the primary interface. If you are using only one network interface connection to the server appliance, use the primary interface and leave the secondary interface empty. Enter a series of four numbers between 0 and 255 separated by periods. For example, 255.255.255.0 is a valid entry.
- **MAC Address (Primary Interface).** The Media Access Control (MAC) address is the hardware address of the network interface card. This hardware address is a unique identifier and cannot be changed after manufacture.
- **IP Address (Secondary Interface).** Enter the IP address of the secondary interface. If you are using only one network interface connection to the server appliance, use the primary interface and leave the secondary interface empty. Enter a series of four numbers between 0 and 255 separated by periods. For example, 209.43.21.5 is a valid entry.
- **IP Network Mask (Secondary Interface).** Enter the network mask of the secondary interface. If you are using only one network interface connection to the server appliance, use the primary interface and leave the secondary interface empty. Enter a series of four numbers between 0 and 255 separated by periods. For example, 255.255.255.0 is a valid entry.
- **MAC Address (Secondary Interface).** The MAC address is the hardware address of the network interface card. This hardware address is a unique identifier and cannot be changed after manufacture.

3. Click **Modify Static Routes**. The Static Route List table appears; see Figure 29.

If you have more than one router or gateway on a local area network (LAN), you need to configure the static routes so that TCP/IP traffic is delivered correctly.

Figure 29. Static Route List table

Static Route List	
Add	0 Entries
This list is currently empty.	
Back	

4. Click **Add**. The Add Static Route table appears; see Figure 30.

Figure 30. Add Static Route table

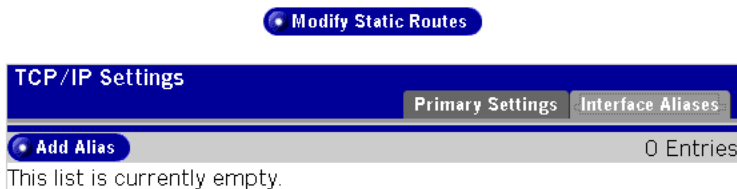
Add Static Route	
Target Subnet	<input type="text"/>
Target Network Mask	<input type="text"/>
Gateway	<input type="text"/>
Network Interface	Primary Ethernet Interface (eth0) <input type="button" value="v"/>
Save Cancel	

5. Configure the Add Static Routes table fields:
 - **Target Subnet.** Enter the IP address of the subnet to be re-routed. Enter a series of four numbers between 0 and 255 separated by periods. For example, 192.168.1.0 is a valid entry.
 - **Target Network Mask.** Enter the network mask of the subnet to be re-routed. Enter a series of four numbers between 0 and 255 separated by periods. For example, 255.255.255.0 is a valid entry.
 - **Gateway.** Enter the IP address of the network gateway through which the target subnet's packets will be re-routed. Enter a series of four numbers between 0 and 255 separated by periods. For example, 192.168.1.1 is a valid entry.
 - **Network Interface.** Select the network interface through which the target subnet's packets will be re-routed. If no device is specified, a device will be selected based on the IP address of the network gateway. Your choices are Primary Ethernet Interface and Secondary Ethernet Interface
6. Click **Save**.

You can use a TCP/IP alias to establish an additional network address for the same network interface. This can be useful in permitting a single physical interface to accept packets addressed to several different addresses such as when you are changing network numbers and you wish to accept packets addressed to the old interface. Another case is when you would like to have multiple addresses assigned to a single network interface.

1. Return to the main screen and click the **Interface Aliases** tab; see Figure 31.

Figure 31. Interface Aliases Tab



2. Click **Add** to display the Add Alias table; see Figure 32.

Figure 32. Add Aliases table

Add Alias	
Interface	Primary Interface (eth0)
IP Address	<input type="text"/>
Netmask	<input type="text"/>

3. Configure the table as follows:
 - **Interfaces.** The interface field is changeable if there is more than one interface configured on the TCP/IP > Primary Settings page. For example, if the primary and secondary interface are set up, then on the Add Alias page you can select either interface.
 - **IP Address.** The IP address on which this alias should listen.
 - **Netmask.** The netmask for this alias.

IP Address Allocation

IP address allocation provides a way to select from allowable IP addresses for the server. This is a convenience feature for assigning IP addresses for sites on the machine and is also intended to help prevent incorrect assignments and potential conflicts or misuse. Increasing numbers of supportable sites per server makes this scaling feature all the more important and useful.

The IP Address Allocation menu is used to specify an acceptable IP address range for the Ethernet ports for the server. Later, when an IP address is assigned to a virtual site, it must fall within this range to be accepted (see Figure 67, “Edit Virtual Site Template—Basic Settings tab,” on page 111). To specify the IP Address Allocation settings:

1. Select **Server Management > System Settings > IP Address Allocation**. The IP Address Allocation screen appears; see Figure 33.

Figure 33. IP Address Allocation screen

The screenshot shows the 'IP Address Allocation' configuration page. At the top, there is a blue header bar with the title 'IP Address Allocation'. Below the header, there is a white box containing the text 'Enabled' followed by an unchecked checkbox. Below this box is a blue button with a white arrow and the text 'Save'. Below the 'Save' button is another blue header bar with the title 'Acceptable Ranges'. Below this header, there is a white box containing the text 'Add' in a blue button, followed by the text 'This list is currently empty.' and '0 Entries' on the right side.

2. Make sure the Enabled checkbox is not checked. If you check it before you enter an acceptable IP address range, the system will send you an error message.
3. Click **Add** in the Acceptable Ranges table to add an address range. The resulting screen is shown in Figure 34.

Figure 34. Acceptable Ranges screen

The screenshot shows the 'IP Address Allocation' configuration page with the 'Acceptable Ranges' table populated. The top section is identical to Figure 33. The 'Acceptable Ranges' section has a blue header bar with the title 'Acceptable Ranges' and '1 Entry' on the right. Below the header is a table with two columns: 'Beginning of Range' and 'End of Range'. Both columns are currently empty. Below the table are three buttons: a blue button with a white arrow and the text 'Save', a red trash can icon, and a blue button with a white arrow and the text 'Cancel'.

4. Enter the starting and ending IP address ranges in the table and click **Save** to save the changes made to the range.
5. Check the Enabled checkbox to enable IP Address Allocation. Only IP addresses within the ranges listed in the Acceptable Ranges table will be allowed for use by virtual sites.
6. Use the red *trash can* icon to delete an entry in the table.

Bandwidth Limits

Bandwidth limits control how much bandwidth a user receives from their IP address. Note that it is controlled at the IP address level, not the Virtual Site level. If there are two users, each with different Virtual Sites but with the same IP address, they share the limit together. The bandwidth limit must be greater than or equal to 10 kbps.

To specify the Bandwidth Limits settings:

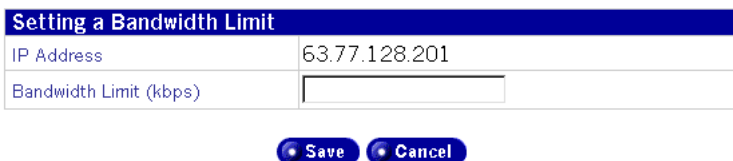
1. Select **Server Management > System Settings > Bandwidth Limits**. The Bandwidth Limits screen appears; see Figure 35.

Figure 35. Bandwidth Limits screen



2. Click **Add** to set the bandwidth limits. The Setting a Bandwidth Limit screen appears; see Figure 36.

Figure 36. Setting a Bandwidth Limit screen



3. Configure the Setting a Bandwidth fields:



- **IP Address.** IP Address that is having its bandwidth limit modified.



Note: Figure 36 shows a single IP address. If more than one IP has been set up for bandwidth limits, a dropdown box is available, allowing you to select from all configured IP addresses. To modify the IP Address, see “IP Address Allocation” on page 78.

- **Bandwidth Limit (kbps).** Bandwidth Limit (in kbps) to place on the IP address listed. Valid values are 10 kbps and up.
4. Click **Save** to save the settings. The Bandwidth Limits screen appears; see Figure 37. Click the green *pencil* icon to modify the settings or the trash can to delete.

Figure 37. Bandwidth Limits screen

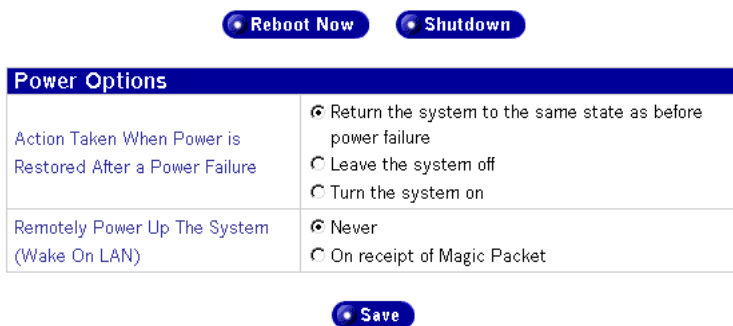
Bandwidth Limits			
Add			1 Entry
IP Address ▼	Limit (kbps)	Virtual Sites Affected	Actions
63.77.128.201	2000	thishost.thisdomain	 

Power

This menu is used to configure remote booting (Wake On LAN with Magic Packet) and power up options. To specify the Power Options settings:

1. Select **Server Management > System Settings > Power**. The Power Options screen and its associated buttons appear; see Figure 38.

Figure 38. Power Options screen



2. Configure the Power Options fields:
 - **Action Taken When Power is Restored After a Power Failure.** This sets the behavior of the system when power is restored after a power failure. If the server appliance is configured as a master connected to a UPS (see “UPS” on page 85), activate the **Turn the system on** radio button. This allows the master to power up after power is restored to the UPS power outlets subsequent to a power failure.
 - **Return the system to the same state as before power failure.** When power fails and then returns, the server appliance will power back up if it was powered up before the power failure. If it was powered down before the power failure, it will remain powered down when power returns.
 - **Leave the system off.** Regardless of whether the server appliance was powered up or not before the power failure, when power returns, the server appliance will remain off.
 - **Turn the system on.** Regardless of whether the server appliance was powered up or not before the power failure, when power returns, the server appliance will power up.

- **Remotely Power Up The System (Wake On LAN).** This sets the system's Wake On LAN capability, which allows you to remotely power up the server appliance over a network. If the server appliance is configured as a slave, activate the **On receipt of Magic Packet** radio button. This allows the master to remotely “wake up” the slave over the network after power is restored (see “UPS” on page 85 for more details on how to use Wake-on-LAN)



Note: The Wake-on-LAN capability is supported only by the primary Ethernet interface (labeled I on the rear panel).

3. Click **Shutdown** for instructions on shutting down the server appliance. For security reasons, you cannot power down the Sun Cobalt RaQ 550 server appliance through the Desktop Server UI; you must power down the server appliance through the LCD console. This screen lists the steps for powering down; see Figure 39.

Figure 39. Shutdown screen

For security reasons, this server appliance cannot be shutdown through the web user interface.

Please use the LCD Panel on the server appliance to shutdown instead.

To power down the server appliance:

1. On the LCD console, press the Power button.
The LCD screen displays:
`POWER DOWN?`
2. Use the arrow buttons to toggle the cursor between [Y] and [N]. Place the cursor on [Y] and press Enter to power down the system.
The LCD screen displays:
`SYSTEM
POWERING DOWN`
3. The server appliance will shutdown and turn off.

4. Click **Reboot Now** in the Power Options screen to reboot the server appliance. A confirmation dialog appears



Note: Rebooting the Sun Cobalt RaQ 550 server appliance sometimes cures problems with certain services. The Active Monitor software recommends when a reboot is necessary.

5. Click **OK** in the confirmation dialog box. A new dialog box appears stating that the server is rebooting and that the reboot can take as long as a few minutes.
6. Once the server appliance reboots, the Server Management screen will be available again.



Note: As indicated in Figure 39, you cannot shut down (power off) the server appliance through the browser. Powering down is done locally at the server appliance using the LCD controls and the power off switch.

You can also reboot the Sun Cobalt RaQ 550 server appliance through the LCD console; refer to “Power menu” on page 200.

UPS

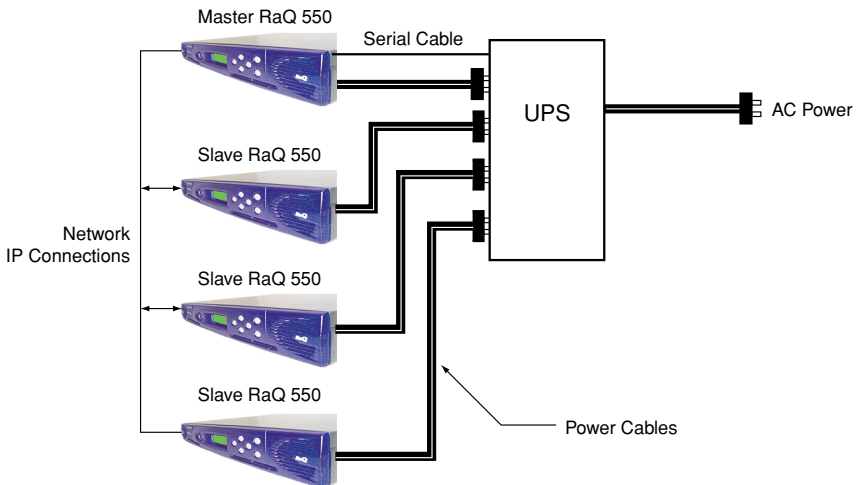
This menu is used to configure Uninterruptible Power Supplies (UPS) options.

The uninterruptible power supply (UPS) functions described in this section work properly only with the following supported UPS modules:

- Matrix-UPS
- Smart-UPS
- Back-UPS Pro

Figure 40 shows generally how master and slave server appliances are connected to a UPS.

Figure 40. UPS Connections



As shown in the diagram, the UPS receives AC power and in turn supplies AC power to the master and slave server appliances. The master controls how power is applied to the slaves.

A UPS master server appliance has the UPS directly connected to its second serial port. A UPS slave server appliance communicates with a UPS master server appliance over the network for information on the UPS.

A serial cable between the UPS and the second serial port of the master server appliance allows status and commands to be exchanged between the server appliance and the UPS. An IP connection between the master and the slaves allows the slaves to shut down in an orderly manner in case of a low battery condition at the UPS and for the master server appliance to issue “Wake-on-LAN” magic packets to power up the slaves after power is restored.

A typical power outage scenario is described in the following steps. This is only one of many scenarios possible and depends on the configuration of the UPS options described later.

1. The power is on and everything is normal. In this state the master server appliance queries the status of the UPS. A daemon process also runs that the slave server appliances query for UPS status.
2. A power outage occurs. The UPS supplies backup power to the server appliances from its battery. If the power is restored before the battery low condition occurs, the power outage is transparent to the servers. However, if the UPS reaches a low battery state, the UPS software running on the master takes action (the slaves and the master poll a daemon process on the master every few seconds).
3. A low battery condition occurs at the UPS. The master and slaves query the daemon process and notice the state change. The slaves shut themselves down and power off. The master delays, waiting for the slaves to power off, then the master notifies the UPS that it should shut down. The master then shuts itself down and sets a state (if “Wake-on-LAN” is selected) that, when the power is restored from the UPS, it must wake up the slaves.
4. Power is restored. The UPS detects that power is restored and powers up. This wakes the master if the master is set for “Turn the system on.” The slaves also power up if they are set for “Turn the system on.” If the master is configured to wake the slaves, it sends out Wake-on-LAN magic packets the slaves.



Note: The Wake-on-LAN capability is supported only by the primary Ethernet interface (labeled I on the rear panel).

5. Normal operation resumes.

To specify the Power Options settings:

1. Select **Server Management > System Settings > UPS**. The UPS Settings screen appears; see Figure 41.

Figure 41. UPS Settings screen

UPS Settings

UPS Options

Disabled
 Configure as Master
 Wake slaves on power return
 Delay between waking slaves
 (seconds) (optional)
 Slave MAC Addresses (optional)
 Configure as Slave
 Master's IP Address (optional)

Save

2. Configure the UPS Settings fields.

You can choose three states:

- The UPS control on the server appliance is disabled
- The server appliance is a UPS master
- The server appliance is a UPS slave.

Configure As Master

- Activate the **Wake slaves on power return** checkbox to have this UPS master attempt to send Wake-on-LAN magic packets to each of the slaves when it is powered up.
- **Delay between waking slaves (seconds) (optional)**. Enter here the amount of time to wait between each slave server appliance being awakened. Values of 0 to 300 seconds are acceptable, with 30 seconds being the default. The reason for this interval is so that all the server appliances are prevented from powering on at the same time. The boot process involves heavy CPU and disk usage, so it is recommended that the power up process is staggered, especially when UPS power reserves may be low.
- **Slave MAC Addresses (optional)**. Enter the list of MAC addresses of the slaves that will receive Wake-on-LAN magic packets. Note that you will need to enable the **Turn the system on** selection for when the power is returned after a power failure. This selection is found in the “Power Options” menu for each of the slave machines. See “Power” on page 82 for details.

Configure As Slave

- Master’s IP Address (optional). Enter the IP address of the UPS system of the master server appliance. You will need to enable the **On receipt of Magic Packet** option in the “Power Options” menu for each of the slave server appliances. See “Power” on page 82 for details.



Note: The LCD panel also allows UPS configuration. You can enable or disable UPS operation, select the server appliance to operate as master or slave, and enter the master’s IP address if you are configuring the server appliance as a slave.

Time

This menu is used to configure the server time settings. To specify the Time settings:

1. Select **Server Management > System Settings > Time**. The Time Settings screen appears; see Figure 42.

Figure 42. Time Settings screen

Time Settings	
Date and Time	November ▾ 30 ▾ 2001 ▾ 2 ▾ : 57 ▾ PM ▾
Time Zone	North America ▾ United States ▾ Pacific Time ▾
NTP Server Address (optional)	<input type="text"/>

 Save

2. Configure the Time Settings fields.
 - **Date and Time.** Set the current date and time.
 - **Time Zone.** Set the proper time zone.
 - **NTP Server Address (optional).** Enter the network address or fully qualified domain name of a Network Time Protocol (NTP) server to which your system date and time will be periodically synchronized. You can find a list of other publicly available NTP servers at:

<http://www.eecis.udel.edu/~mills/ntp/servers.htm>.



Note: If you have manually entered time settings, the server appliance time is updated to those values as soon as you click **Save**. If you have entered an NTP server address only and no manual data and time settings, after you click **Save**, the time settings on the server appliance are synchronized to the NTP server at the next scheduled NTP server update.

Information

Click this menu item to display system information for the server appliance, such as serial numbers and MAC addresses. This menu can also be used to register the Sun Cobalt RaQ 550 server appliance as well as access the Sun Cobalt Web site.

Maintenance

The Maintenance section allows you to perform server maintenance such as system-wide backup, storage control and system restart. The following submenus are available:

- Server Desktop
- Knox Arkeia Backup Settings
- Legato NetWorker™ Backup Settings
- Additional Storage

Server Desktop UI

A server administrator or third-party backup software may lock the Server Desktop UI during backup to prevent modification of server configuration parameters while they are being backed up.

To specify the Server Desktop UI settings:

1. Select **Server Management > Maintenance > Server Desktop**. The Server Desktop table appears; see Figure 43.

Figure 43. Server Desktop screen



2. Configure the Server Desktop settings.
 - Lock Server Desktop. This option gives the ability to make the administrative user interface (Server Desktop) read-only. Locking the Server Desktop during the backup and restore process will help guarantee that server configuration is properly saved and restored.
3. Click **Save** to save the settings.

Knox Arkeia Backup Settings

To specify the Knox Arkeia Backup settings:

1. Select **Server Management > Maintenance > Knox Arkeia**. The Knox Arkeia Backup Settings table appears; see Figure 44.

Figure 44. Knox Arkeia Backup screen

Knox Arkeia Backup Settings	
Enable Client	<input type="checkbox"/>
Knox Arkeia Server Name	<input type="text"/>
Firewall Support	
Port Number	<input type="text" value="617"/>

2. Configure the Knox Arkeia Backup Settings fields.
 - **Enable Client.** Turns the Knox Arkeia backup client on or off.
 - **Knox Arkeia Server Name.** A valid server is a fully qualified domain name or IP address. A fully qualified domain name is of the form server.domain.com such as www.example.com.
 - **Firewall Support Port Number.** The Knox Arkeia Backup client uses a port to communicate with the Knox Arkeia Backup server. The default is 617. Changing this value is not recommended unless absolutely necessary. If you change this, make sure other hosts on the network that use Knox services are also configured to use the port you specify. For more information, see the Knox Arkeia documentation.
3. Click **Save** to save the settings.



Note: The Knox Arkeia software locks the server desktop (see “Server Desktop UI” on page 90) during the portion of the backup in which the server configuration data is being backed up.

Legato NetWorker™ Backup Settings

To specify the Legato NetWorker Backup settings:

1. Select **Server Management > Maintenance > Legato NetWorker**. The Legato NetWorker Backup Settings table appears; see Figure 45.

Figure 45. Legato NetWorker Backup Settings screen

Legato NetWorker Backup Settings	
Enable Client	<input type="checkbox"/> Enable Client
Legato Server Hostnames	<input type="text"/>
Service Port Range	<input type="text" value="7937"/> - <input type="text" value="7938"/>
Connection Port Range	<input type="text" value="10001"/> - <input type="text" value="10100"/>

2. Configure the Legato NetWorker Backup fields.
 - **Enable Client.** Turns the Legato NetWorker backup client on or off.
 - **Legato Server Hostnames.** Enter the fully qualified domain names (one per line) of the Legato NetWorker backup servers. Legato servers must have valid host names. Separate the names with carriage returns.
 - **Service Port Range.** Sets the system's service ports range to the one specified.
 - **Connection Port Range.** Sets the system's connection ports range to the one specified.



Note: Refer to the Legato NetWorker documentation or the Legato Web site for more details on the Service Port Range and Connection Port Range values. These ports are used for firewall support.

3. Click **Save** to save the settings.



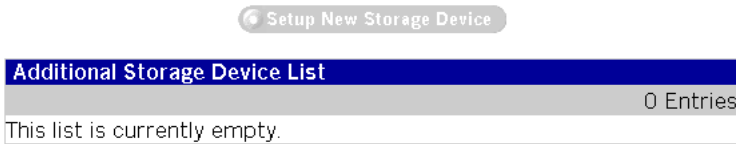
Note: The Legato NetWorker software locks the Server Desktop UI (see “Server Desktop UI” on page 90) during the portion of the backup in which the server configuration data is being backed up.

Additional Storage

This selection allows you to add, remove or modify additional storage devices. New storage devices must be connected to the server appliance while it is powered down before they will appear in the list as new storage. Third-party backup software also detects the addition of new storage. To specify the Additional Storage settings:

1. Select **Server Management > Maintenance > Additional Storage**. The Additional Storage Device List appears; see Figure 46.

Figure 46. Additional Storage Device List screen



2. Add additional storage devices while the server appliance is powered down.
3. Click the **Setup New Storage Device** button when it becomes active after the storage devices have been added and the server appliance is powered back on. The Setup New Storage Device appears; see Figure 47

Figure 47. Setup New Storage Device screen

New Storage Device List			
			1 Entry
Disk Name	Size (GB) ▼	Disk Partitions	Setup
/dev/hdc	28.0	0	

[Back](#)

4. Click the green *pencil* icon to set up the disk. The Setup Disk screen appears; see Figure 48.

Figure 48. Setup Disk screen



5. Set up the disk using the **Select Disk Setup Option** pulldown menu.
6. To remove additional storage, remove the storage device by clicking the red *trash can* icon in the Additional Storage Device List (see Figure 46), then shut down the server appliance and physically remove the disk drive from the server appliance.

Usage Information

The Usage Information section allows you to browse server and network service usage statistics. The following submenus are available:

- Network
- Web
- FTP
- Email
- Disk

Network

To configure Network usage information for display:

1. Select **Server Management > Usage Information > Network**. The Configure Network Reporting Options screen appears; see Figure 49.

Figure 49. Configure Network Reporting Options screen

Configure Network Reporting Options			
Starting From	April	12	2002
Ending On	April	12	2002

Generate Report

2. Enter the start and end dates for network activity to be included in the report.
3. Click **Generate Report**.

The Network Statistics Summary screen appears; see Figure 50.

4. Use the drop down box to display the data in various ways.
5. Click **Generate New Report** to return to the screen shown in Figure 49.
6. Click **Download Log** to download a log file of the network activity.

Figure 50. Network Statistics Summary screen

View Detailed Usage... ▾ **Generate New Report** **Download Log**

Network Statistics Summary	
Report Generated	November 30 2001 8:58 AM
First Activity	November 30 2001 9:01 AM
Last Activity	November 30 2001 11:01 PM
Data Transferred	2,941.24 KB

Web

To configure Web usage information for display:

1. Select **Server Management > Usage Information > Web**. The Configure Web Reporting Options screen appears; see Figure 51.
2. Enter the start and end dates for Web activity to be included in the report.
3. Click **Generate Report** to display a summary of the Web activity.

Figure 51. Configure Web Reporting Options screen

Configure Web Reporting Options			
Starting From	February ▾	21 ▾	2002 ▾
Ending On	February ▾	21 ▾	2002 ▾

Generate Report

FTP

To configure FTP usage information for display:

1. Select **Server Management > Usage Information > FTP**. The Configure FTP Reporting Options screen appears; see Figure 52.
2. Enter the start and end dates for FTP activity to be included in the report.
3. Click **Generate Report** to display a summary of the FTP activity.

Figure 52. Configure FTP Reporting Options screen

Configure FTP Reporting Options			
Starting From	November ▾	30 ▾	2001 ▾
Ending On	November ▾	30 ▾	2001 ▾

Generate Report

Email

To configure email usage information for display:

1. Select **Server Management > Usage Information > Email**. The Configure Email Reporting Options screen appears; see Figure 53.
2. Enter the start and end dates for email activity to be included in the report.
3. Click **Generate Report** to display a summary of the email activity.

Figure 53. Configure Email Reporting Options screen

Configure Email Reporting Options			
Starting From	November	30	2001
Ending On	November	30	2001




Generate Report

Disk

To display the statistics for disk usage on a virtual site, follow these steps:

1. Select **Server Management > Usage Information > Disk**. The Disk Usage screen appears; see Figure 54.

Figure 54. Disk Usage screen

Disk Usage				
Summary Sites All Users Notification Settings				
				3 Entries
Partition	Disk Usage (MB)	Total Size (MB)	Percentage Used	
/	824.16	1995.44	 41%	
/home	152.13	24612.00	 1%	
/var	29.05	1495.44	 2%	


2. Click the **Summary** tab.

The Disk Usage table displays the disk usage by partition name; see Figure 54.

3. Click the **Sites** tab.

The Disk Usage table displays the disk usage by site host name; see Figure 55.

Figure 55. Sites Tab screen


Disk Usage				
Summary Sites All Users Notification Settings				
1 Entry				
Full Host Name	Disk Usage (MB)	Allowed Disk Space (MB)	Percentage Used	
www.example.com	0.10	500.00	 0%	

Click on a site above to see the disk usage information for the users in that site.

4. Click the **All Users** tab.

The Disk Usage table displays the disk usage by user; see Figure 56.

Figure 56. All Users screen

Disk Usage				
Summary Sites All Users Notification Settings				
1 Entry				
User Name	Disk Usage (MB)	Allowed Disk Space (MB)	Percentage Used	
admin	0.19	Unlimited	 0%	

5. Click the **Notification Settings** tab.

The Disk Usage table lists the types of notifications to be sent when the user or the site exceed the allocated disk space; see Figure 57.



Note: Refer to “Active Monitor” on page 99 for information on how to set up an email address for alert notification.

Figure 57. Notifications Settings screen

Disk Usage	
Summary Sites All Users Notification Settings	
When User Exceeds Allowed Disk Space	<input type="checkbox"/> Send Alert Notification Email <input checked="" type="checkbox"/> Email User
When Site Exceeds Allowed Disk Space	<input checked="" type="checkbox"/> Send Alert Notification Email

 Save

Active Monitor

The Sun Cobalt RaQ 550 server appliance uses Active Monitor software, a Sun Cobalt utility that runs on a server appliance and updates key system and service status every 15 minutes. This section describes how to use the Active Monitor.



Note: System software events are triggered in the event of serious system conditions that may damage the server appliance (for example critical overtemperature or overvoltage). See “System health monitoring” on page 42 for more details.

Active Monitor icon



The Active Monitor icon in the top right corner of the user interface allows you to view status information. The icon turns red if any of the components monitored by Active Monitor have severe problems. The amber System Fault LED on the front panel is illuminated for any hardware failure detected by Active Monitor.

The Active Monitor section allows you to check for correct operation of system components. The following submenus are available:

- **Status** menu selection. Brings up the Overview screen (System Status, Service Status and Other Status)
- **Settings** menu selection. Brings up the Active Monitor Settings screen

Status menu selection

This menu item displays the **Check Status Now** button and three screens. A colored dot at the left of each item indicates its status.

1. To view detailed status information for a particular system component or service, click the colored circle to the left of the item’s name in the table or click the magnifying glass in the Action column that corresponds to the name of the item. See Figure 58.

The status of each of the above items is indicated by a green, yellow, red or grey circle beside each item. The colors have the following significance:

- **Grey.** No information is available or monitoring is not enabled
- **Green.** Normal functioning
- **Yellow.** A problem exists that should be investigated by the Administrator (for example, low disk space)
- **Red.** A severe problem exists that needs immediate attention by the Administrator.



Note: When a condition that results in the activation of a red or yellow indicator is corrected, the indicator will not change color until Active Monitor is run manually or automatically (every 15 minutes). Thus, after a defective fan is replaced, for example, both the Active Monitor status indicator and the amber System Fault LED remain active until Active Monitor runs.

2. Click the **Check Status Now** button to retrieve the current status of the server.



Note: Clicking this button immediately begins the process of updating system and service status information. This may take as long as several minutes and will proceed in the background.

3. View the System Status - Overview screen. This screen displays server hardware and environmental status; see Figure 58.
4. View the Service Status - Overview screen. This screen displays status of the various servers (DNS, FTP, Email, Telnet, Web and SNMP), status of pages (ASP and JSP), Buffer Overflow Protection, Scan Detection and Server Desktop; see Figure 59.
5. View the Other Status - Overview screen. This screen shows the status of the backup clients; see Figure 60.



Note: Clicking the magnifying glass icon for a status item displays more details and, in some cases (fan and DIMM status, for example), provides graphical illustrations to help identify, locate and correct a fault condition.

Figure 58. System Status - Overview screen

System Status - Overview		
		10 Entries
▼	Component Name ▼	Action
<input checked="" type="radio"/>	CPU Usage	
<input checked="" type="radio"/>	Disk Integrity	
<input checked="" type="radio"/>	Disk Usage	
<input checked="" type="radio"/>	ECC Memory Correction	
<input checked="" type="radio"/>	Fans	
<input checked="" type="radio"/>	Memory Usage	
<input checked="" type="radio"/>	Network Status	
<input checked="" type="radio"/>	System Power	
<input checked="" type="radio"/>	Temperature	
<input type="radio"/>	UPS	

Figure 59. Service Status - Overview screen

Service Status - Overview		
		11 Entries
▼	Component Name ▼	Action
<input type="radio"/>	Active Server Pages (ASP)	
<input checked="" type="radio"/>	Buffer Overflow Protection	
<input type="radio"/>	Domain Name Service (DNS) Server	
<input checked="" type="radio"/>	Email Servers	
<input checked="" type="radio"/>	File Transfer Protocol (FTP) Server	
<input type="radio"/>	JavaServer Pages (JSP) and Servlets	
<input checked="" type="radio"/>	Scan Detection	
<input checked="" type="radio"/>	Server Desktop	
<input type="radio"/>	Simple Network Management Protocol (SNMP) Server	
<input checked="" type="radio"/>	Telnet Server	
<input checked="" type="radio"/>	Web Server	

Figure 60. Other Status - Overview screen

Other Status - Overview		
		2 Entries
▼	Component Name ▼	Action
<input type="radio"/>	Knox Arkeia	
<input type="radio"/>	Legato NetWorker	

Settings menu selection

This menu item allows you to configure Active Monitor Settings. To configure Active Monitor settings:

1. Select **Server Management > Active Monitor > Settings**. The Active Monitor Settings screen appears; see Figure 61.

Figure 61. Active Monitor Settings screen

Active Monitor Settings					
Enable Monitoring	<input checked="" type="checkbox"/>				
Alert Notification Emails (optional)	admin				
Monitored Components (optional)	<table border="1"> <thead> <tr> <th>Components Monitored</th> <th>Components Not Monitored</th> </tr> </thead> <tbody> <tr> <td>ECC Memory Correction Temperature Email Servers Domain Name Service (DNS) Server Telnet Server Scan Detection</td> <td>Empty</td> </tr> </tbody> </table>	Components Monitored	Components Not Monitored	ECC Memory Correction Temperature Email Servers Domain Name Service (DNS) Server Telnet Server Scan Detection	Empty
Components Monitored	Components Not Monitored				
ECC Memory Correction Temperature Email Servers Domain Name Service (DNS) Server Telnet Server Scan Detection	Empty				

Save

2. Configure the Active Monitor Settings fields:
 - **Enable Monitoring.** Turn Active Monitor on or off. Enabling this functionality allows specific system components to be regularly checked for proper operation. These system components can be selected in the other portion of the screen.
 - **Alert Notification Emails (optional).** Enter the list of email addresses to which Active Monitor will send alert messages. Each email address must be on an individual line, separated by a carriage return.
 - **Monitored Components (optional).** Select the specific system components to be regularly checked by Active Monitor. The left column shows the system components that are currently being monitored. The right column shows the system components which could possibly be monitored. To add a system component to be monitored, select the component and use the left arrow to move the system component from the right column to the left column.

Site Management

Introduction

The Sun Cobalt RaQ™ 550 server appliance is designed to host multiple virtual sites. A virtual site is an individual location on the Internet, such as `www.efgh.com` or `www.xyz.com`. Each virtual site can have a unique set of users who can send and receive email, publish Web pages, or upload and download files through FTP. A virtual site can also provide anonymous FTP access and SSL.



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

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

Administrator privileges

This section describes the features available to a *Server Administrator* and a *Site Administrator* on the Sun Cobalt RaQ 550 server appliance.

A *Site Administrator* is allowed to do the following:

- Setup and manage users
- Import and export users
- Create and manage mailing lists
- Use Web deployment
- Manage SSL (for this vsite)
- Generate usage reports

A *Server Administrator* is allowed to do all of the Site Administrator functions as well as the following:

- Search for virtual sites by host name or IP address
- Edit the virtual site template
- Add virtual sites

A Site Administrator, can access all of the features described for the site user in Chapter 7, “Personal Profile.”



Note: If desired, all of the virtual sites may be removed and the server appliance may be used as a dedicated DNS server or email server.

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

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



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

A Site Administrator, can manage a virtual site using any standard Web browser. To access the **Site Management** (<sitename>) screen for your site, type the URL `http://<sitename>/login/` into your browser. The browser-based user interface (UI), known as the Server Desktop, prompts you for a user name and password. You can log in as a regular user or as a Site or Server Administrator. Once you have responded to the prompts, if you are an authorized Site Administrator, the **Site Management** (<sitename>) screen appears.



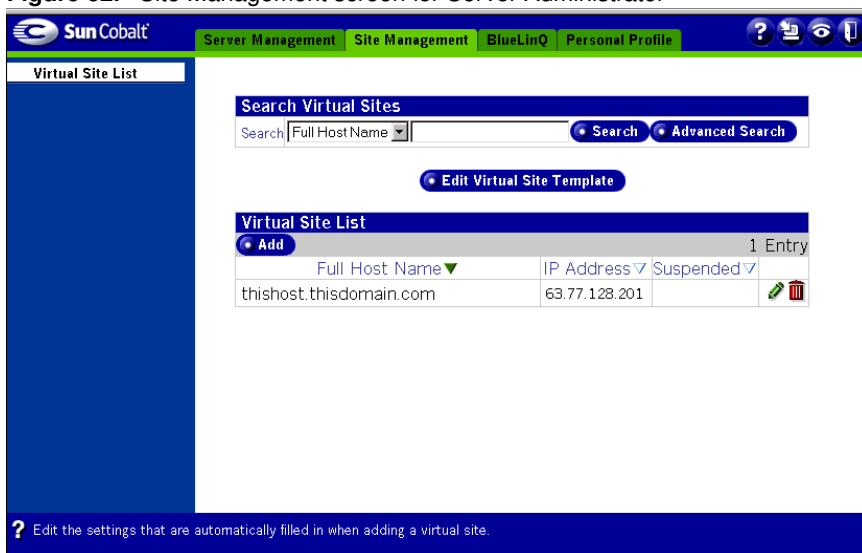
Note: The **Site Management** screen can only be accessed using the fully qualified domain name for the virtual site in the Web browser. The **Site Management** screen is not accessible if an incomplete or aliased site name is specified.

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

Site Management screen (for Server Administrator)

When you log in as a Server Administrator and go to Site Management, the Site Management screen appears with the **Virtual Site List** menu item highlighted, as shown in Figure 62.

Figure 62. Site Management screen for Server Administrator



As shown above, a Server Administrator can search for virtual sites, edit the virtual site template, or add virtual sites. Only a Server Administrator can perform these functions. After performing these functions, the Server Administrator can click the green *pencil* icon on the Virtual Site List to bring up the screen shown in Figure 71. This screen shown in Figure 71 is the one that either a Site Administrator or a Server Administrator can use to manage virtual site users.

There are three main areas on the Site Management main screen (see Figure 62) that are available to Server Administrators:

- Search Virtual Sites dialog box
- Virtual Site List dialog box
- Edit Virtual Site Template button

Search Virtual Sites

The **Search Virtual Sites** dialog box, shown in Figure 63, allows you to search for virtual sites that match the properties entered in the dialog box. These functions are useful if you have a large number of virtual sites on your server appliance and you want to restrict the display to certain virtual sites.

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

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

Figure 63. Search Virtual Sites screen



1. Configure the settings shown in the screen:
 - **Search.** The Search drop down box allows you to choose the site property on which to search (full host name or IP address). Sites with names or IP addresses that contain the text entered in the field to the right of the drop down box for the chosen property will be listed when you click Search.
 - **Advanced Search.** An advanced search allows you to perform a more refined search on site properties. When you click **Advanced Search**, the dialog box shown in Figure 64 appears. Choose the search criteria that you desire to make your search more refined.
2. Click **Search** to begin the search.



Figure 64. Advanced Search screen

Search Virtual Sites	
Search Options	
Search Criteria	Full Host Name <input type="text"/> Contains <input type="text"/>
Site Uses	<input type="checkbox"/> SSL <input type="checkbox"/> Shell Access <input type="checkbox"/> Usage Information <input type="checkbox"/> Common Gateway Interface (CGI) <input type="checkbox"/> Anonymous FTP <input type="checkbox"/> PHP Scripting <input type="checkbox"/> Frontpage Server Extensions <input type="checkbox"/> Server-Side Includes (SSI) <input type="checkbox"/> Authenticated POP (APOP) <input type="checkbox"/> JavaServer Pages (JSP) and Servlets <input type="checkbox"/> Active Server Pages (ASP)
Suspended	<input type="checkbox"/>
Display Options	
Sites Per Page	<input type="text" value="25"/>

Virtual Site List

The **Virtual Site List** dialog box, shown in Figure 65, displays the existing virtual sites and allows you to add or delete them.

Figure 65. Virtual Site List screen

Virtual Site List			
<input type="button" value="Add"/>			1 Entry
Full Host Name ▼	IP Address ▼	Suspended ▼	
www.example.com	63.77.128.201		 

The settings shown in the screen are:

- **Full Host Name.** The Full Host Name is the complete name of the site and is also known as the fully qualified domain name. This is a combination of the host name and the domain name.
- **IP Address.** This is the IP address of the site.
- **Suspended.** This indicates if the site is suspended. If a site is suspended, access for users of the site as well as the Web and FTP site associated with it will be disabled.

Click the green *pencil* icon to modify an item in the Virtual Site List (see “Managing Virtual Sites” on page 117 for more details) or the red *trash can* icon to delete an item in the list.

Click **Add** to add a new item to the Virtual Site List. The screen shown in Figure 66 appears.

Fill in this dialog box as needed to create a new virtual site.



Note: Automatic DNS configuration manages DNS records for this site. Web and Email server aliases are supported only if they share the site domain name. This service does not register the domain name with a top-level registrar.

Figure 66. Add Virtual Site screen

Add New Virtual Site	
IP Address	<input type="text"/>
Host and Domain Name	<input type="text"/> <input type="text"/> Host Name Domain Name
Web Server Aliases <i>(optional)</i>	<input type="text"/>
Email Server Aliases <i>(optional)</i>	<input type="text"/>
Catch-All Email Address <i>(optional)</i>	<input type="text"/>
Maximum Allowed Disk Space (MB)	<input type="text" value="500"/> (1 - 140,595)
Maximum Allowed Number of Users	<input type="text" value="25"/>
Automatic DNS Configuration	<input checked="" type="checkbox"/>
Services and Features	
Anonymous FTP	<input type="checkbox"/> Enable Maximum Allowed Upload Disk Space (MB) <input type="text" value="20"/> Maximum Simultaneous Connections <input type="text" value="10"/>
Enable JSP and Servlets	<input type="checkbox"/>
Enable ASP	<input type="checkbox"/>
Enable PHP Scripting	<input type="checkbox"/>
Enable Common Gateway Interface (CGI)	<input type="checkbox"/>
Enable Server-Side Includes (SSI)	<input type="checkbox"/>
Enable FrontPage Server Extensions	<input type="checkbox"/> Enable webmaster Password <input type="text"/> <input type="text"/> <i>(Enter Again)</i>
Enable APOP	<input type="checkbox"/>
Enable Shell Access	<input type="checkbox"/>
Enable SSL	<input type="checkbox"/>

Editing the virtual site template

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

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

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

Follow these steps to edit the virtual site template:

1. Click the **Edit Virtual Site Template** button to edit the settings that are automatically filled in when adding a virtual site.

When you click this button, the Virtual Site Template table appears, see Figure 67.

Figure 67. Edit Virtual Site Template—Basic Settings tab

Virtual Site Template	
Basic Settings	Services and Features
IP Address	<input type="text"/>
Domain Name	<input type="text"/>
Maximum Allowed Disk Space (MB)	<input type="text" value="500"/>
Maximum Allowed Number of Users	<input type="text" value="25"/>
Catch-All Email Address	<input type="text"/>
Automatic DNS Configuration	<input checked="" type="checkbox"/>

2. Use the **Basic Settings** tab to configure the default network, user and disk limits, and email settings for new virtual sites. See .
 - **IP Address.** The default IP address that will be filled in when adding a site. To use the server appliance, you require an IP address or range of IP addresses.



Note: The Sun Cobalt RaQ 550 server appliance supports name-based virtual sites, allowing many sites to share a single IP address. You can create many virtual sites using the same IP address (for example, 192.168.25.77) as long as the fully qualified domain name for each site is different (for example, both *www.efgh.com* and *www.xyz.com* can use 192.168.25.77 as their IP address).

- **Domain Name.** The default domain to which new sites will belong. Each virtual site also requires a domain name (for example, *efgh.com* or *xyz.com*).

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



Note: The Sun Cobalt RaQ 550 server appliance can serve as the DNS server and provide the host name.

- **Maximum Allowed Disk Space.** The maximum disk space on the server appliance in megabytes (MB) available to a site for files.
- **Maximum Allowed Number of Users.** The maximum number of user accounts that a site can have.
- **Catch-All Email Address.** Specify an email address to receive messages that are addressed to unknown users and mailing lists. If left blank, email addressed to unknown users or mailing lists will not be accepted. If the specified address does not exist, mail to unknown users and mailing lists may be rejected just as if no address was specified.

- **Automatic DNS Configuration.** Automatic DNS configuration manages DNS records for this site. Web and Email server aliases are supported only if they share the site domain name. This service does not register the domain name with a top level registrar. You can have the server appliance automatically create DNS records for this virtual site. If enabled, the server appliance acts as the primary DNS server for this site. The default setting for this feature is OFF.

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



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

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

3. Use the **Services and Features** tab to enable or disable various services. See Figure 68.
 - **Enable APOP.** Enable authenticated POP (APOP). See “Email” on page 136 for more detailed information.
 - **Enable SSL.** Enable SSL to allow secure access to the Web server for the site. See “SSL” on page 70 for more detailed information.
 - **Enable Shell Access.** Enable shell access to allow the creation of users who can connect to the server using services such as telnet and ssh.



Note: If any of these are enabled for a site, they may be enabled or disabled on a per user basis.

See “Shell” on page 137 for more detailed information.

Figure 68. Edit Virtual Site Template—Services and Features tab

Virtual Site Template	
Basic Settings	Services and Features
Enable APOP	<input type="checkbox"/>
Enable SSL	<input type="checkbox"/>
Enable Shell Access	<input type="checkbox"/>

4. Use the **Web** tab to configure Web options, such as scripting languages. See Figure 69.

The following items are explained more fully under the section titled “Web” on page 132.

- **Enable JSP and Servlets.** Allow the use of JavaServer Pages™ (JSP™) software and Servlets.
- **Enable ASP.** Enable the use of active server pages (ASP).
- **Enable PHP Scripting.** Enable the use of PHP scripts.
- **Enable Common Gateway Interface (CGI).** Enable the use of CGI applications.
- **Enable Server-Side Includes.** Enable the use of Server-Side Includes.
- **Enable FrontPage Server Extensions.** Check the box to have FrontPage Server Extensions turned on by default when creating a new site.

Figure 69. Edit Virtual Site Template—Web tab

Virtual Site Template	
Basic Settings	Services and Features
Enable JSP and Servlets	<input type="checkbox"/>
Enable ASP	<input type="checkbox"/>
Enable PHP Scripting	<input type="checkbox"/>
Enable Common Gateway Interface (CGI)	<input type="checkbox"/>
Enable Server-Side Includes (SSI)	<input type="checkbox"/>
Enable FrontPage Server Extensions	<input type="checkbox"/>

5. Use the **Anonymous FTP** tab to modify settings for anonymous FTP. Anonymous FTP is explained more fully in the section titled “Anonymous FTP” on page 134.
 - Activate the **Enable** checkbox to enable anonymous FTP for the site.
 - **Maximum Allowed Upload Disk Space**. Enter the limit in megabytes (MB) for anonymous FTP uploads.
 - **Maximum Simultaneous Connections**. Enter the maximum number of anonymous FTP users that can be connected to the server at one time.

Figure 70. Edit Virtual Site Template—Anonymous FTP tab

The screenshot shows the 'Virtual Site Template' configuration window with the 'Anonymous FTP' tab selected. The window has a blue header with the title 'Virtual Site Template' and four tabs: 'Basic Settings', 'Services and Features', 'Web', and 'Anonymous FTP'. The 'Anonymous FTP' tab is active. On the left side, the text 'Anonymous FTP' is displayed. On the right side, there is a configuration area with a checkbox labeled 'Enable' which is currently unchecked. Below the checkbox are two input fields: 'Maximum Allowed Upload Disk Space (MB)' with the value '20' and 'Maximum Simultaneous Connections' with the value '10'. At the bottom center of the window are two blue buttons: 'Save' and 'Cancel'.

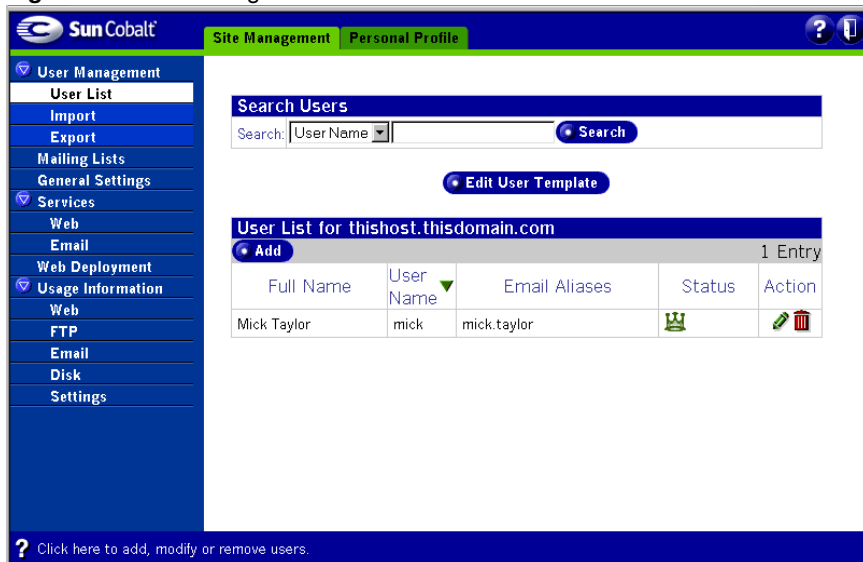
6. Click **Save**.

The information now appears filled in on the **Add Virtual Site** screen each time you click **Add** to add a new item to the Virtual Site List.

Site Management screen (for Site Administrator)

When you log in as a Site Administrator and go to Site Management, the Site Management screen appears as shown in Figure 71. Notice that the screen shown in Figure 62, which is restricted to Server Administrators, is not available to the Site Administrator.

Figure 71. Site Management screen for Site Administrator



As shown above, a Site Administrator (and Server Administrator) has access to all the menu items shown at the left of the screen. However, in the User List menu (which is active in the screen), the Site Administrator can only search for users, edit the user template and add users. A Site Administrator cannot search for virtual sites, edit the virtual site template, or add virtual sites. Only a Server Administrator can perform these functions.

Managing Virtual Sites

When you click the crayon icon in the Virtual Site List screen as a Server Administrator (see Figure 65, “Virtual Site List screen,” on page 108), or when you come to Site Management as a Site Administrator, the screen shown in Figure 72 appears, which allows you to modify the virtual site selected.



Note: The Virtual Site Modification screen for Site Administrators has only two tabs at the top: Site Management and Personal Profile. The other two tabs (Server Management and BlueLinQ) are available only to Server Administrators.

Figure 72. Virtual Site Management screen (for Server Administrator)

The screenshot displays the Sun Cobalt Virtual Site Management interface. At the top, there are four tabs: Server Management, Site Management (selected), BlueLinQ, and Personal Profile. The left sidebar contains a navigation menu with categories like Virtual Site List, User Management, Services, and Usage Information. The main content area features a 'Search Users' section with a search bar and a 'Search' button. Below this is an 'Edit User Template' button. A 'User List for thishost.thisdomain.com' section shows a table with one entry for 'Mick Taylor'.

Full Name	User Name	Email Aliases	Status	Action
Mick Taylor	mick	mick.taylor		

The following bullet items represent the fully expanded menu items on the left side of the **Virtual Site Modification** screen. These are the functions and services that the Administrator can manage. They are explained in this section.

- User Management (see page 119)
 - User List
 - Import
 - Export
- Mailing Lists
- General Settings
- Services (see page 132)
 - Web
 - Anonymous FTP (only available to Server Administrator)
 - Email
 - Shell (only available to Server Administrator)
- Web Deployment
- SSL (only available to Server Administrator)
- Usage Information (see page 140)
 - Web
 - FTP
 - Email
 - Disk
 - Settings

User Management

The User Management menu item is used to add, modify, or remove users.

User List

Selecting the User List menu item brings up the Search Users and User List screens; see Figure 73.

Figure 73. Search Users and User List screens



Search Users

Search: User Name

User List for www.example.com

0 Entries

This list is currently empty.

1. Configure the settings in the Search Users table:
 - **Search.** You can use the search tool to find users based on the criteria you specify using the dropdown box. Select the field on which to search and choose how the text you enter should be compared against the field.
2. In the User List table, click **Add** to add a new user. The Add New User screen appears; see Figure 74.

Figure 74. Add New User screen

Add New User to site0.cobalt.com	
Full Name	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="password"/> <i>(Enter Again)</i>
Maximum Allowed Disk Space	<input type="text" value="20"/>
Enable Front Page Server Extensions	<input type="checkbox"/>
Site Administrator	<input type="checkbox"/>
Email Aliases <i>(optional)</i>	<input type="text"/>
Remarks <i>(optional)</i>	<input type="text"/>

3. Configure the settings on the Add New User table:

- Full Name.** Enter the full name of the user. Please enter any characters except colons. For example, John Doe is a valid entry.
- User Name.** Enter the name to be used by the system to identify the user. Please enter no more than 12 characters containing only lowercase alphanumeric characters, periods, hyphens and underscores. The first character must be a letter. For example, john.doe is a valid entry
- Password.** Enter the password to be used by the system to identify this user. The password should be between 3 and 16 characters long. A good password should contain at least 5 characters with a mix of uppercase and lowercase letters as well as numbers and punctuation. It should not spell out any words found in the dictionary. Passwords are case sensitive.
- Maximum Allowed Disk Space.** Set the disk quota of this user. This is the maximum disk space available to this user for the storage of Web pages, email messages and all other user files. The quota can not be smaller than 1 MB. The default value for new users is set in the User Template. For site level accounts, you cannot leave the Maximum Allowed Disk Space (MB) field blank. You must enter a number in this field.
- Site Administrator.** Site administrators are users who are capable of configuring settings for a site, adding and removing users, and so on.

- **Email Aliases (optional).** Enter additional names under which the user will receive email. Enter characters containing only lowercase alphanumeric characters, periods, hyphens and underscores. The default value is the lowercase first and last name of the user separated by a period. For example, john.doe is a valid entry.
- **Remarks (optional).** Enter additional information or comments about the user here.

4. Click **Save** to save the settings.

After a user has been added, the new user is listed in the User List screen (see Figure 75).

Figure 75. User List screen

[Edit User Template](#)

User List for www.example.com				
Add				1 Entry
Full Name	User Name	Email Aliases	Status	Action
Mick Taylor	mick	mick.taylor		

Use the green *pencil* icon to modify the user settings or the red *trash can* icon to delete the user.

When you click the green *pencil* icon to modify user settings, the Modify User Settings screen appears (see Figure 76).

Figure 76. Modify User screen

Modify User Settings for mick		Account	Email
Full Name	<input type="text" value="Mick Taylor"/>		
New Password (optional)	<input type="password"/> <input type="password"/> (Enter Again)		
Maximum Allowed Disk Space	<input type="text" value="20"/> (1 - 500)		
Site Administrator	<input checked="" type="checkbox"/>		
Suspended	<input type="checkbox"/>		
Remarks (optional)	<div style="border: 1px solid gray; height: 60px;"></div>		

[Save](#) [Cancel](#)

1. Configure the settings in the Modify User Settings screen (Account tab).
 - **Full Name.** Enter the full name of the user. Please enter any characters except colons. For example, John Doe is a valid entry.
 - **New Password.** Enter the password to be used by the system to identify this user. The password should be between 3 and 16 characters long. A good password should contain at least 5 characters with a mix of uppercase and lowercase letters as well as numbers and punctuation. It should not spell out any words found in the dictionary. Passwords are case sensitive.
 - **Maximum Allowed Disk Space.** Set the disk quota of this user. This is the maximum disk space available to this user for the storage of Web pages, email messages and all other user files. The quota can not be smaller than 1 MB. The default value for new users is set in the User Template. For site-level accounts, you cannot leave the Maximum Allowed Disk Space (MB) field blank. You must enter a number in this field.
 - **Site Administrator.** Site administrators are users who are capable of configuring settings for a site, adding and removing users, and so on.
 - **Suspended.** Suspending a user will prevent that user from accessing system services associated with that account such as telnet, FTP, mail and Web access to their files. Email sent to this account will be rejected and the sender will receive an error message.
 - **Remarks (optional).** Enter additional information or comments about the user here.
2. Configure the settings in the Modify User Settings screen (Email tab).
 - **Email Aliases (optional).** Enter additional names that the user will receive email as. Please enter characters containing only lowercase alphanumeric characters, periods, hyphens and underscores. The default value is the lowercase first and last name of the user separated by a period. For example, john.doe is a valid entry.
 - **Email Forwarding.** Enabling email forwarding causes email received in the future to be automatically forwarded to the email addresses specified. In the **Email Addresses** area, enter the email addresses to which you would like your email forwarded. The values entered must be valid email addresses such as user@example.com. To specify multiple addresses, separate the addresses with a comma, or put each address on a separate line.

- **Save Copy.** Checking Save Copy saves a copy of every email received to the mailbox in addition to forwarding a copy to the email addresses specified.
 - **Vacation Message.** Vacation Message allows you to automatically send a custom message to everyone who sends you email. This is useful if you are unable to read your email, or want to send an automatic response message to the sender.
 - **Auto Reply.** Enter the message that will be sent automatically as a reply to the sender of every email you receive.
3. Click the **Edit User Template** button (see Figure 73) to configure default settings to use when adding other new users.



Note: The following features, if enabled for the site, can also be enabled or disabled on a per user basis:

- FrontPage Server Extensions (see “Web” on page 132)
- APOP (see “Email” on page 136)
- Shell Access (see “Shell” on page 137)

Importing and exporting site users

The purpose of importing and exporting users is to provide an easy way to migrate users from one virtual site to another or from one server appliance to another.

A Site Administrator can import a list of users to a virtual site by uploading a specially formatted text file containing the names of the users and their settings. The list of users can also be exported on the virtual site to a text file that is compatible with the import function.

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

Creating a TSV text file

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

The parameter order is the following:

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

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

Other parameters for a site user, such as the user's maximum allowed disk space and site administrator privileges cannot be specified in the file for individual users. However, the settings specified in the User Templates page are applied to each user imported. Thus, for example, if you wanted all the users in your text file to have FrontPage enabled, you could configure FrontPage "enabled" by default in the User Templates table.



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

An example file with two users might look like this:

```
dwest<tab>Doug West<tab>4ng3lf1r3<tab>doug dougie dw  
tdurden<tab>Tyler Durden<tab>s04p<tab>tyler td fighter
```



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

Importing Users

Selecting the Import menu item brings up the Import User List screen; see Figure 77.

Figure 77. Import User List screen

1. Configure the settings on the Import User List screen:

- **Source File.** Enter the location from which to obtain the TSV (Tab Separated Value) format file containing a list of users to be uploaded to the system. Enter a URL beginning with either `http://` or `ftp://` to download the file from a location on the internet, or enter the full path to a file to upload. Click **Browse** to choose a file on your local hard drive.
- Click **Import Now**. The server prompts you with a confirmation dialog.

If you agree to continue, the server returns a status screen showing you how many lines of the text file have been processed and how many of the users have been successfully added (and not added).

After all the lines in the file have been processed, if errors were encountered, the system displays a summary report. The summary report explains why a particular line failed to add a user.

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

Exporting Users

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

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

Click **Export** to export users from the server. The export function returns a TSV (Tab Separated Value) format file that is compatible with the user import function.

Selecting the Export menu item brings up the Export User List screen; see Figure 78.

Figure 78. Export User List screen



1. Configure the settings on the Export User List screen:
 - **Password Format.** Due to the encryption algorithm used to store user passwords, the user's actual password cannot be exported. If you choose to use User Names, users will be able to use their login name as their password. Choosing Random Strings prevents other users from being able to easily guess another user's password.
 - Click **Export Now**. The server sends the text file to your local machine.

Mailing Lists

This menu item is used to manage mailing lists. A mailing list allows a discussion by email between a group of people; the email addresses of the people in the group make up the list. The mailing list is given a name, for example `new_project`. The mailing list can include users on the Sun Cobalt RaQ 550 server appliance as well as external users.

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

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

Selecting the Mailing List menu item brings up the Mailing Lists screen; see Figure 79.

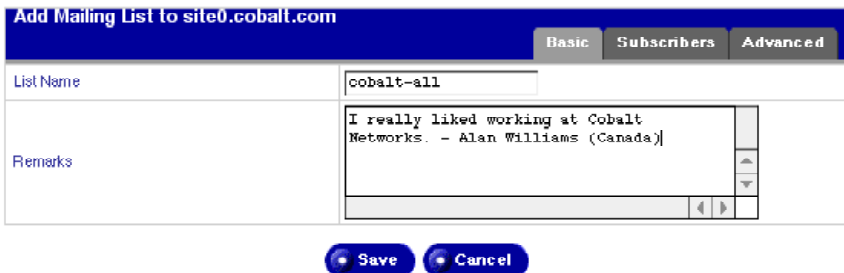
Figure 79. Mailing Lists screen



1. Click **Add** to add a mailing list; see Figure 80.

Use the Basic, Subscribers and Advanced tabs to configure the mailing lists.

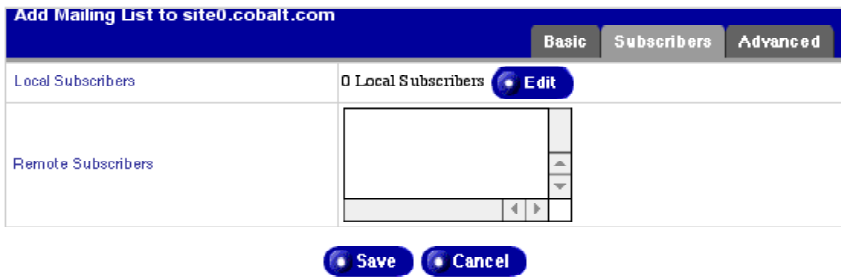
Figure 80. Add Mailing Lists screen (Basic tab)



2. Click the **Basic** tab and configure the settings:
 - **List Name.** Enter the name of the mailing list. Please enter only lowercase alphanumeric characters, hyphens and underscores. For example, sales is a valid entry.
 - **Remarks.** Enter additional information or comments about the mailing list here.
3. Click the **Subscribers** tab.

The dialog box shown in Figure 81 appears.

Figure 81. Add Mailing Lists screen (Subscriber tab)



4. Configure the settings:
 - **Local Subscribers.** Click the **Edit** button to select the local users that are subscribers to this mailing list. The dialog boxes shown in Figure 82 appear. They allow you to search for and add users to the mailing list.
 - **Remote Subscribers.** Enter the remote users (Figure 81) that are subscribers to this mailing list. Remote users are users who do not have accounts on this server appliance. Please enter a properly formatted email address. For example, user@example.com is a valid entry.

Figure 82. Search and Add Users to Mailing List)

Search User List

Search **Search**

Show All Users **Show Only Selected Users**

All Users on thishost.thisdomain

Select All Users **Select This Page** 1 Entry

	User Name ▼
<input type="checkbox"/>	mick

Use Current Selection **Cancel**

5. Click the **Advanced** tab and configure the settings:

The dialog box shown in Figure 83 appears.

- **Owner/Moderator.** Enter the email address of the user performing all administrative duties (for example, approving subscriptions or moderating messages) for the mailing list. Please enter a properly formatted email address or the user name of a valid user on this server appliance. The default value is admin. For example, user@example.com and admin are valid entries.
- **Password.** Enter an administrative password for this mailing list. This password is used when performing certain list administration tasks via email. If you do not plan on using these features, you may leave this field blank.
- **Posting Policy.** Select a posting policy for this mailing list.
 - **Only Subscribers Can Post Messages.** Only subscribers to this mailing list are allowed to post messages.
 - **All Users Can Post Messages.** Any user, subscriber or not, can post messages.
 - **Moderator Confirms All Messages.** Every message will require approval from the list owner/moderator.

- **Subscription Policy.** Select a subscription policy for the mailing list.
 - **Open.** Any user may subscribe.
 - **Confirm.** An email confirmation is required to subscribe.
 - **Closed.** The approval of the list owner is required before subscribing.



Note: Users can subscribe or unsubscribe from the list by sending mail to `majordomo@thishost.thisdomain.com` with the words ‘subscribe list’ or ‘unsubscribe list’ (list is the mailing list name) in the body of the message. If the policy is ‘Closed’, the message is sent to the list owner for approval before the subscription is allowed. Approval is never required to unsubscribe.

- **Maximum Message Length.** Select the maximum size in kilobytes or megabytes allowed for messages sent to this mailing list. Messages exceeding this size will be rejected.
- **Reply Policy.** Set the reply policy for this mailing list. If you choose Reply to List, replies will go to the list. Otherwise, replies will go only to the original author of the message.

Figure 83. Add Mailing Lists screen (Advanced tab)

Add Mailing List to site0.cobalt.com	
Basic Subscribers Advanced	
Owner/Moderator	<input type="text" value="admin"/>
Password	<input type="password"/>
Policies	
Posting Policy	<input type="text" value="Only Subscribers Can Post Messages"/>
Subscription Policy	<input type="text" value="Open: any user may subscribe"/>
Maximum Message Length	<input type="text" value="50 kb"/>
Reply Policy	<input type="text" value="Reply to Sender"/>


General Settings

This menu item is used to modify settings for this site and configure some services.

Selecting the General Settings menu item brings up the Virtual Site Settings screen; see Figure 84.

Figure 84. Virtual Site Settings screen

Virtual Site Settings for www.example.com	
IP Address	<input type="text" value="63.77.128.201"/>
Host and Domain Name	<input type="text" value="www"/> <input type="text" value="example.com"/> <small>Host Name Domain Name</small>
Maximum Allowed Disk Space (MB)	<input type="text" value="500"/> (1 - 24,612)
Maximum Allowed Number of Users	<input type="text" value="25"/>
Automatic DNS Configuration	<input checked="" type="checkbox"/>
Suspend	<input type="checkbox"/>



1. Configure the settings:

- **IP Address.** Enter the IP address of the site.
- **Host and Domain Name.** Enter the host name of the site in the first field and the domain name in the second field. For example, the host name could be www, mail, etc. The domain name could be example.com, cobalt.com, and so on.
- **Maximum Allowed Disk Space (MB).** The maximum disk space on the server in megabytes (MB) available to a site for files.
- **Maximum Allowed Number of Users.** The maximum number of user accounts that a site can have.
- **Automatic DNS Configuration.** Automatic DNS configuration manages DNS records for this site. Web and Email server aliases are supported only if they share the site domain name. This service does not register the domain name with a top level registrar.
- **Suspend.** If checked, access to the site is disabled for users of the site as well as services such as FTP, FrontPage, public Web and email for the site.

Services

This menu item is used to configure various services for the site.

Web

This menu item is used to configure Web options such as scripting languages.

Selecting the Web menu item brings up the Web Settings screen; see Figure 85.

Figure 85. Web Settings screen

Web Settings for raq550.localdomain	
Enable JSP and Servlets	<input type="checkbox"/>
Enable ASP	<input type="checkbox"/>
Enable PHP Scripting	<input type="checkbox"/>
Enable Common Gateway Interface (CGI)	<input type="checkbox"/>
Enable Server-Side Includes (SSI)	<input type="checkbox"/>
Enable FrontPage Server Extensions	<input checked="" type="checkbox"/> Enable webmaster <input type="text"/> Password <input type="text"/> (Enter Again)
Web Server Aliases (optional)	<div style="border: 1px solid gray; height: 40px; width: 100%;"></div>

1. Configure the settings:

- **Enable JSP and Servlets.** Enable to allow the use of JavaServer Pages (JSP) software and Servlets.
- **Enable ASP.** Enable the use of active server pages (ASP). An ASP is an HTML page that includes one or more scripts (small embedded programs) that are processed on a Microsoft Web server before the page is sent to the user. An ASP is somewhat similar to a server-side include or a common gateway interface (CGI) application in that all involve programs that run on the server, usually tailoring a page for the user. Typically, the script in the Web page at the server uses input received as the result of the user's request for the page to access data from a database and then builds or customizes the page on the fly before sending it to the requestor.
- **Enable PHP Scripting.** Enable the use of PHP scripts. In Web programming, PHP is a script language and interpreter that is freely available. PHP is an alternative to Microsoft's Active Server Page (ASP) technology. As with ASP, the PHP script is embedded within a Web page along with its HTML. Before the page is sent to a user that has requested it, the Web server calls PHP to interpret and perform the operations called for in the PHP script. An HTML page that includes a PHP script is typically given a file name suffix of ".php", ".php3," or ".phtml". Like ASP, PHP can be thought of as "dynamic HTML pages," since content will vary based on the results of interpreting the script.
- **Enable Common Gateway Interface (CGI).** Enable the use of CGI applications. CGI programs are the most common way for Web servers to interact dynamically with users. Many HTML pages that contain forms, for example, use a CGI program to process the form's data once it is submitted. Another increasingly common way to provide dynamic feedback for Web users is to include scripts or programs that run on the user's machine rather than the Web server. These programs can be Java™ applets, Java scripts, or ActiveX controls. These technologies are known collectively as client-side solutions, while the use of CGI is a server-side solution because the processing occurs on the Web server.

- **Enable Server-Side Includes (SSI).** SSIs are directives that are placed in HTML pages and evaluated on the server while the pages are being served. They let you add dynamically generated content to an existing HTML page, without having to serve the entire page via a CGI program, or other dynamic technology.

The decision of when to use SSI and when to have your page entirely generated by some program is usually a matter of how much of the page is static, and how much needs to be recalculated every time the page is served. SSI is a great way to add small pieces of information, such as the current time. But if a majority of your page is being generated at the time that it is served, you need to look for some other solution.

- **Enable FrontPage Server Extensions.** Enable creation of a FrontPage web for the site. The extensions are a set of server-side scripts and programs that enable users of Microsoft FrontPage to use its special components (called Web Bots).
- **Web Server Aliases (optional).** Enter additional host or domain names for which this virtual site should accept Web requests. Separate multiple entries with a comma. Example: example.com, www.example.com. Note that DNS must be configured to resolve alias addresses in addition to the site name. You can add aliases for Web servers; you are not restricted to receiving Web requests only on the domain name entered in the site settings.

2. Click **Save** to save the settings.

Anonymous FTP

This menu item is used to change File Transfer Protocol (FTP) Settings and is only available to Server Administrators.

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

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

Selecting the Anonymous FTP menu item brings up the Web Settings screen; see Figure 86.

Figure 86. Anonymous FTP Settings screen

Anonymous FTP Settings for www.example.com	
Anonymous FTP	<input type="checkbox"/> Enable
	Maximum Allowed Upload Disk Space (MB) <input type="text"/> (1 - 500)
	Maximum Simultaneous Connections <input type="text"/>
<input type="button" value="Save"/>	

1. Configure the settings:

- **Enable.** Check this box to allow anonymous FTP for the user.
- **Maximum Allowed Upload Disk Space (MB).** This sets the limit in megabytes (MB) for anonymous FTP uploads.
- **Maximum Simultaneous Connections.** The maximum number of anonymous FTP users that can be connected to the server at one time.

2. Click **Save** to save the settings.

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

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

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

The size limit specified for FTP uploads is the total amount of space allocated on the hard disk drive for FTP uploads.

Email

This menu item is used to configure email options for a virtual sites.

Selecting the Email menu item brings up the Email Settings screen; see Figure 87.

Figure 87. Email Settings screen

Email Settings for www.example.com	
Enable APOP	<input type="checkbox"/>
Email Server Aliases (optional)	<div style="border: 1px solid gray; padding: 2px;">example.com, mail.example.com</div>
Catch-All Email Address (optional)	<input type="text"/>

[Save](#)

1. Configure the settings:

- **Enable APOP.** Check this box to enable authenticated POP (APOP). APOP prevents your popmail password from traveling over the network, instead using it to encrypt a session password which can be checked against one encrypted by the popmail server also using your password. This means that a hacker using a network sniffer can only capture your session password, which cannot be used on a second session to read your electronic mail or do any other damage. Using APOP means that your email password is less able to be electronically “stolen” and used by someone else.
- **Email Server Aliases (optional).** Enter additional host or domain names for which this virtual site should accept email [SMTP port 25] connections. Separate multiple entries with a comma. Example: **example.com, mail.example.com**. You can add aliases for email servers; you are not restricted to receiving email messages only on the *hostname.domainname* as entered in the site settings.
- **Catch-All Email Address (optional).** Specify an email address to receive messages that are addressed to unknown users and mailing lists. If left blank, email addressed to unknown users or mailing lists will not be accepted.

2. Click **Save** to save the settings.

Shell

This menu item is used to configure shell settings for this site and is only available to Server Administrators.

Selecting the Shell menu item brings up the Shell Settings screen; see Figure 88.

Figure 88. Shell Settings screen



1. Click the **Enable Shell Access** checkbox to enable shell access. This allows the creation of users who can connect to the server using services such as telnet and ssh.
2. Click **Save** to save the setting.

Web Deployment

J2EE Web clients are packaged in Web Application Archives (with the .war extension). The Web Deployment menu item is used to load and manage .war lists.

The .war archive usually contains JavaServer Pages software, servlets, server-side utility classes and static Web content such as HTML, images, sound files, and so on.

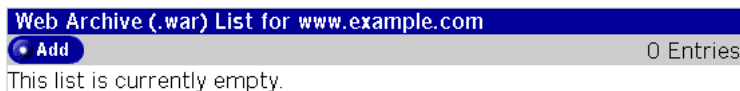
Tomcat is a servlet container with a JSP environment. A servlet container is a runtime shell that manages and invokes servlets on behalf of users. Currently Tomcat is configured as an out-of-process servlet container through an Apache plugin called mod_jk.

The .war deployment usually involves deploying the servlets, Java server pages under Tomcat and then registering the relevant URLs with Tomcat and Apache. Once deployed, Apache forwards all requests for the registered servlets and JSP pages to the Tomcat engine.

Advanced users are advised to refer to documentation of Apache, Tomcat and mod_jk.

Selecting the Web Deployment menu item brings up the Web Archive (.war) Lists screen; see Figure 89.

Figure 89. Web Archive (.war) List screen



1. Click **Add** to add a Web Archive list; see Figure 90.

Figure 90. Add Web Archive (.war) List screen



2. Configure the settings:

- **Web Archive File.** Enter the location from which to obtain the .war file. Enter a URL beginning with either `http://` or `ftp://` to download the archive from a location on the internet, or enter the file location of a .war file to upload. Click **Browse** to choose a file on your local hard drive. If you have downloaded .war archives to the web root, an option to choose one of these files will also be available.
- **Installation Location.** The contents of the Web Archive (.war) will be extracted to this directory. The directory will be created if necessary.



Note: The Web Archive (.war) cannot be installed in the home directory of a user.

SSL

This menu item is used access information about the SSL certificate used to provide secure access to your site using https on port 443 and is only available to Server Administrators. For example, SSL allows users to access your site by going to `https://www.example.com:443`.

Selecting the SSL menu item brings up the Certificate Information screen with its associated buttons; see Figure 91.

Figure 91. Certificate Information screen



Check the Enable SSL checkbox to allow secure access to the Web server for the site.

See “SSL” on page 70 for detailed information on the SSL menu item.

Usage Information

Use this menu item to view information about resource usage for this site.

Web

This menu item is used to configure Web usage information for display.

1. Selecting this menu item brings up the Configure Web Reporting Options screen; see Figure 92.

Figure 92. Configure Web Reporting Options screen

Configure Web Reporting Options for www.example.com			
Starting From	December	04	2001
Ending On	December	04	2001

Generate Report

2. Enter the start and end dates for Web activity to be included in the report.
3. Click **Generate Report** to display a summary of the Web activity.

FTP

This menu item is used to configure FTP usage information for display.

1. Selecting this menu item brings up the Configure FTP Reporting Options screen; see Figure 93.

Figure 93. Configure FTP Reporting Options screen

Configure FTP Reporting Options for www.example.com			
Starting From	December	04	2001
Ending On	December	04	2001

Generate Report

2. Enter the start and end dates for FTP activity to be included in the report.
3. Click **Generate Report** to display a summary of the FTP activity.

Email

This menu item is used to configure email usage information for display.

1. Selecting this menu item brings up the Configure Email Reporting Options screen; see Figure 94.

Figure 94. Configure Email Reporting Options screen

Configure Email Reporting Options for www.example.com			
Starting From	December	04	2001
Ending On	December	04	2001

Generate Report

2. Enter the start and end dates for email activity to be included in the report.
3. Click **Generate Report** to display a summary of the email activity.


Disk


This menu item is used to display disk usage information.


1. Selecting this menu item brings up the Disk Usage screen; see Figure 95.

The Disk screen displays the disk usage by site host name, by system and by user.

Figure 95. Disk screen

Disk Usage for www.example.com	
Disk Space Used (MB)	0.11
Disk Space Free (MB)	499.89
Percentage Used	 0%

System Disk Usage			
			1 Entry
Service	Disk Usage (MB)	Allowed Disk Space (MB)	Percentage Used
● Usage Logs	0.00	500	 0%

User Disk Usage			
			1 Entry
User Name	Disk Usage (MB)	Allowed Disk Space (MB)	Percentage Used
● taylor	0.00	20	 0%

Settings

This menu item is used to configure usage information and statistics generation for this site.

1. Selecting this menu item brings up the Settings screen; see Figure 96.

Figure 96. Settings screen

Usage Information Settings for raq550.localdomain	
Enable Statistics Generation	<input checked="" type="checkbox"/>
Detail Level	Daily
Statistics History	Forever

[Save](#)

2. Use the Enable Statistics Generation checkbox to enable Virtual Site web, FTP and email usage statistics.
3. Use the **Detail Level** drop-down box to determine whether daily statistics information files are combined into one monthly statistics information file per month. This does not affect statistics information for the current month. If Daily is selected, you can generate reports containing less than one month's worth of statistics for months prior to the current month. If Monthly is selected, you can only generate reports containing the statistics for whole months for months prior to the current month. Statistics combination cannot be undone for months that have been combined already. Selecting Monthly will consume less disk space compared to Daily.
4. Use the **Statistics History** drop-down box to determine how far back in time you will be able to cover in statistics reports. A longer period of time allows you to generate reports with a longer history at the expense of disk space.

BlueLinQ

This chapter describes how to use BlueLinQ to check for and install new or updated software packages.

When you log into the Sun Cobalt RaQ™ 550 server appliance as *admin*, the BlueLinQ tab appears in the top menu bar of the Server Desktop user interface (UI). When you select BlueLinQ, the left menu bar presents commands that allow you to update the Sun Cobalt RaQ 550 server appliance software, add new software and view the installed software. This section describes how to use these commands.

Software Notification icon



The Software Notification icon in the top right corner of the user interface allows you to check for new or updated software packages and to install them if any are found. The icon changes color when new or updated software packages are available. It also changes color when mail is being sent to email accounts specified in the Active Monitor settings section to indicate that new software packages have arrived.

New Software

1. Select **BlueLinQ > Sun Cobalt Software** or **BlueLinQ > Third Party Software**. The Available New Software table for Sun Cobalt or third-party software appears, as appropriate; see Figure 97.
2. Click **Check Availability Now** to check availability of new software.
3. Click **Install Manually** if you already know the location of new software that you want to install on the Sun Cobalt RaQ 550 server appliance.

Figure 97. Available New Software List table

Available New Software List					3 Entries
	Name ▾	Version ▾	Vendor ▾	Description	Install Details
	ImagineApp	2.0	SupremeWeb, Inc.	The ImagineApp enhances your web experience.	
	Network Spider	1.0	Fictitious Networks	The Network Spider brings web traffic to you.	
	BuildMeister	1.0	PBallz Enterprises	The BuildMeister makes everything happen.	

Updates

1. Select **BlueLinQ > Sun Cobalt Updates** or **BlueLinQ > Third Party Updates**. The Available Software Updates List table for Sun Cobalt or third-party software appears, as appropriate; see Figure 98.

Figure 98. Available Software Updates List table

Available Software Updates List					1 Entry
	Name ▾	Version ▾	Vendor	Description	Install Details
	Cobalt OS Upgrade	1.0	Sun Cobalt	This is an OS Update for the RaQ 550	

2. Click **Check Availability Now** to update the list of available software or click **Install Manually** if you already know the location of new software that you want to install on the Sun Cobalt RaQ 550 server appliance.
3. Click the green *magnifying-glass* icon to see more detailed information about the software package. The Install Software table appears; see Figure 99.

Figure 99. Install Software table

Install Software	
Name	BuildMeister
Version	1.0
Vendor	PBaltz Enterprises
Copyright	(c) 2000 PBaltz Enterprises
Description	Tired? Overworked? Let the BuildMeister handle your work for you. With the BuildMeister, you no longer need to worry about administering your RaQ 550. With its ProActive Assist, it solves your administrative problems before you even realize that they're there.
Location	http://pbaltz.cobalt.com/raq550/build.pkg
Size (MB)	94.778
Uninstallable	Yes
Dependent Packages	None



4. Click **Install Manually**. The Install Manually table appears; see Figure 100.

Figure 100. Install Manually table

Install Manually	
Location	<input checked="" type="radio"/> URL <input type="text"/> <input type="radio"/> Upload <input type="text"/> <input type="button" value="Browse..."/>



5. Enter a URL in the URL field or enter a path and filename to load the software package from your computer. You can also click **Browse** to locate the software package.
6. Click **Prepare**. The system verifies that the file you are loading is in the correct.pkg format. The system then begins to load the software.

Installed Software

The following packages are installed on the Sun Cobalt RaQ 550 server appliance at the factory; you cannot un-install these packages.



- Sun Cobalt OS
- RAID

It is not usually possible to un-install various updates and additions that have been made to your server appliance through BlueLinQ.

To view the software installed on the server appliance:

1. Select **BlueLinQ > Installed Software**. The Installed Software List table appears; see Figure 101.
2. Click the icon in the Uninstall column if you wish to uninstall a particular software. A confirmation dial appears to proceed with the uninstall procedure.
3. Click **OK**.

Figure 101. Installed Software List table

Installed Software List				
				2 Entries
Name ▼	Version ▼	Vendor ▼	Description	Uninstall
Cobalt DiskMirror	1.1	Cobalt Networks	Cobalt DiskMirror provides enhanced reliability by actively mirroring content across a pair of hard drives.	
Sun Cobalt OS	7.0	Sun Microsystems, Inc.	The Sun Cobalt OS is the base software for the Sun Cobalt RaQ 550. This software package is required in order for your server appliance to function.	

Settings

To view or modify the settings for the BlueLinQ feature:

1. Select **BlueLinQ > Settings**. The BlueLinQ Settings table appears; see Figure 102 for the Basic settings and Figure 103 for the Advanced settings. The active tab shows up as a light grey.

Figure 102. BlueLinQ Settings - Basic tab

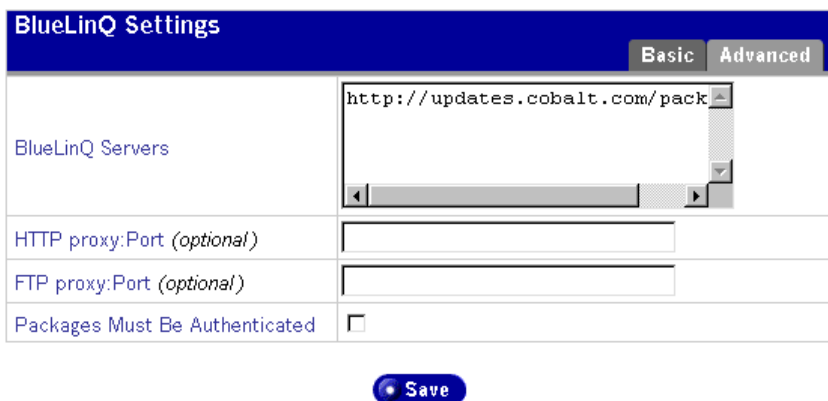


The screenshot shows the 'BlueLinQ Settings' window with the 'Basic' tab selected. It contains two rows of settings: 'Query Schedule' set to 'Weekly' and 'Software Notification Light' set to 'Updates only'. A 'Save' button is located below the settings table.

BlueLinQ Settings	
	Basic Advanced
Query Schedule	Weekly
Software Notification Light	Updates only

Save

Figure 103. BlueLinQ Settings - Advanced tab



The screenshot shows the 'BlueLinQ Settings' window with the 'Advanced' tab selected. It contains four rows of settings: 'BlueLinQ Servers' with a text area containing 'http://updates.cobalt.com/pack', 'HTTP proxy:Port (optional)' with an empty text box, 'FTP proxy:Port (optional)' with an empty text box, and 'Packages Must Be Authenticated' with an unchecked checkbox. A 'Save' button is located below the settings table.

BlueLinQ Settings	
	Basic Advanced
BlueLinQ Servers	http://updates.cobalt.com/pack
HTTP proxy:Port (optional)	
FTP proxy:Port (optional)	
Packages Must Be Authenticated	<input type="checkbox"/>

Save

2. Configure the fields in the BlueLinQ Settings tables.

- **Query Schedule.** Specify how frequently the BlueLinQ server is checked for new or updated software packages.
- **Software Notification Light.** Specify the type of new software that activates the Software Notification Light and, if applicable, the type of new software that appears in notification email messages.
- **BlueLinQ Server(s).** Enter the HTTP address(es) of the location(s) to query for software updates. You can enter more than one address in this scrolling window; enter each HTTP address on a separate line.

The default location of the Sun Cobalt Update Server is
<http://updates.cobalt.com/packages/>.



Note: To receive updates from Sun Cobalt, you must retain the URL <http://updates.cobalt.com/packages/> in this field.

- **HTTP proxy:port.** (*optional*) Enter the proxy server and port for HTTP queries if a proxy server is needed to reach outside your firewall.

Example: proxy.mycompany.com:8080.

- **FTP proxy:port.** (*optional*) Enter the proxy server and port for FTP queries if a proxy server is needed to reach outside your firewall.

Example: proxy.mycompany.com:8080.



Note: If the server appliance is behind a firewall and therefore does not have direct access to the Internet, you may need to specify FTP and HTTP proxies. Typically, if you need to specify proxies to access the Internet with a browser, you can use those same proxies for BlueLinQ. If proxies are specified, BlueLinQ connects to the proxy in order to access the BlueLinQ server, rather than connecting directly.

- **Packages must be authenticated.** If enabled, BlueLinQ installs only packages that have passed an authentication check.

3. Click **Save**.

Personal Profile

This chapter describes how to view your user account information.

When you log into the Sun Cobalt RaQ™ 550 server appliance, the Personal Profile tab appears in the top menu bar of the Server Desktop user interface (UI). When you select Personal Profile, the left menu bar presents commands that allow you to manage your account. This section describes how to use these commands.

The menu items for your account appear on the left.

- Account
- Email
- Disk Usage

Account

In the Account section, you can change the full name, select a language and change your password

To modify your account information:

1. Click **Personal Profile** at the top.
2. Click **Account** on the left. The Account Settings - <username> table appears; see Figure 104.

Figure 104. Account Settings table

Account Settings for admin	
Full Name	<input type="text" value="Administrator"/>
Language Preference	<input type="text" value="English"/> ▾
New Password <i>[optional]</i>	<input type="text"/> <input type="text"/> <i>[Enter Again]</i>

3. Modify any of the following fields:
 - a. **Full Name.** This field is mandatory. Modify the real name associated with your login account.
 - b. **Language Preference.** The Sun Cobalt RaQ 550 server appliance uses the language option selected in your browser software (as long as the text strings for that language are available on the server appliance). If the language selected in your browser is not available, the server appliance defaults to English.
 - c. **New Password.** (*optional*) You can change your password. Enter the password twice for confirmation.

For more information on choosing a password, see “Password Guidelines” on page 25.

4. Click **Save**.

Email

There are two options available in the Email section: Email Forwarding and Vacation Message; see Figure 105.

Figure 105. Email table

Email Settings for admin	
Email Forwarding	<input type="checkbox"/> Enable Email Addresses <input type="checkbox"/> Save Copy
Vacation Message	<input type="checkbox"/> Enable Auto-Reply

Forwarding

The Forwarding feature allows you to forward incoming messages to another email address.

Enabling email forwarding

To enable email forwarding:

1. Click the **Enable** check box in the Email Forwarding area.
2. In the scrolling text window labeled Email Addresses, enter an email address in the format <xxxxx@yyy.zzz>.

For more than one email address, separate the addresses with a comma or enter each address on a separate line.

3. You can save a copy of the email messages that you forward by clicking the **Save Copy** check box.
4. Click **Save**.

Disabling email forwarding

To disable email forwarding:

1. In the Email Forwarding section of the table, uncheck the **Enable** check box.
2. Click **Save**.

Vacation message

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

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

Enabling the vacation message

To enable the vacation message:

1. In the Vacation Message section of the table, click the **Enable** check box.
2. In the scrolling text window labeled Auto-Reply, type the text of the message you want to send to users while you are away.
3. Click **Save**.

Disabling the vacation message

To disable the vacation message:

1. In the Vacation Message section of the table, uncheck the **Enable** check box.
2. Click **Save**.

Disk Usage

In the Disk Usage section, you can view the amount of disk space in use, the amount of disk available and the percentage of the disk in use.


Viewing the disk usage statistics

To view the Disk Usage statistics:

1. Click **Personal Profile** at the top.
2. Click **Disk Usage** on the left. The Disk Usage table appears with the usage statistics; see Figure 106.

The table displays the amount of disk space used (MB), the amount of disk space free (MB) and the percentage of disk space used.

Figure 106. Disk Usage table

Disk Usage for admin	
Disk Space Used (MB)	0.28
Disk Space Free (MB)	24,459.87
Percentage Used	 0%

Advanced Information



Caution: The features described in this appendix are intended for advanced users who want to run shell scripts or use shell commands. An advanced user is someone who is proficient in the internal workings of the Linux operating system.

You can adversely affect the operation of your Sun Cobalt RaQ™ 550 server appliance if you modify system configuration files. Check your warranty card for details.



Caution: Direct root logins are not allowed on the Sun Cobalt RaQ 550 server appliance. To obtain a root shell, connect to the server using ssh or telnet and login as the user *admin* or with one of the server administrator accounts that has root access enabled. From the command prompt, type `'su -'` if you are logged in as *admin* or `'su - root-<username>'`, where `<username>` is the login name for the account, if logged in as a server administrator.

Press **Enter**. Enter the password for the account used to login to the machine at the password prompt. Only the *admin* account and server administrators who are allowed root access can `'su'` to root.

Enabling Interbase 6.0

The Sun Cobalt RaQ 550 server appliance is pre-loaded with InterBase 6.0, an open-source, cross-platform SQL database from Inprise Corporation. InterBase is not enabled by default.

For more information on InterBase, go to <http://www.interbase.com>.

InterBase offers free development and distribution rights. Interbase offers developers a sophisticated database with a small footprint, low maintenance cost and high reliability.

InterBase offers a number of database features—triggers, stored procedures, blobs, event alterers, user-defined functions, multi-dimensional arrays, two-phase commit, referential integrity, constraints, and a flexible set of transaction options.

To enable the InterBase 6.0 database server:



Caution: You can seriously affect your Sun Cobalt RaQ 550 server appliance if you modify the system configuration files. Only advanced users of Linux should undertake these changes.

For more details, see “Warranty” on page 7.

1. Connect to the server appliance using ssh or telnet and log in as the user *admin* or using a server administrator account that has root access enabled.
2. From the command prompt, if logged in as the *admin* user, enter:

```
su -
```

If logged in as a server administrator, enter:

```
su - root-<username>
```

where ‘<username>’ is the login name for the server administrator account used to connect.



Note: Only the *admin* user or server administrators can `su -` to root.

3. Press **Enter**. A password prompt appears.
4. Enter the password for the account used to connect to the server in step 1.
5. Open an editor and edit the file:

```
/etc/inetd.conf
```

6. Locate the line with `gds_db` service. This line is commented out with a `#` symbol.
7. Remove the `#` symbol. This enables `inetd.conf` to launch the InterBase 6.0 database server when requests are made to its port.
8. Save the file and exit the editor.
9. Enter the command

```
killall -HUP inetd
```

This causes the `inetd` server to re-read its configuration file and activate the InterBase 6.0 database server.
10. Enter `exit` to end your session as root.

Serial console port

You can connect a console terminal to the DB-9 connector on the back panel of the Sun Cobalt RaQ 550 server appliance. The terminal can be either an ASCII terminal or a PC running terminal software. The console terminal should have the following communications parameters—115 200 baud, 8 data bits, no parity and one stop bit.

Initializing the server appliance through the serial console port

Instead of assigning the initial network settings for the server appliance through the LCD console, you can connect the server to a terminal and assign the network settings through the serial console port.

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

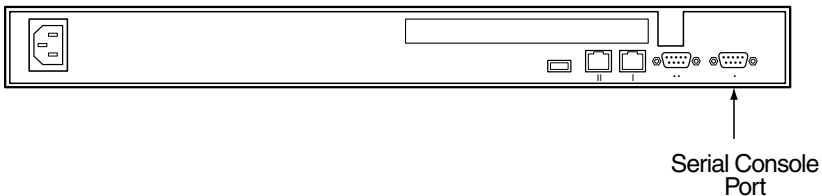


Note: You can initialize the server appliance through the serial console port only once, much like proceeding through the browser-based Setup Wizard.

To initialize the Sun Cobalt RaQ 550 server appliance through the serial console port:

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

Figure A-1. Serial console port location



2. Configure your terminal software to the following parameters:
 - 115 200 Baud
 - 8 data bits
 - no parity
 - 1 stop bit
3. Power on the server appliance with the power switch on the front panel. A number of boot messages are displayed on your terminal screen.
4. If there is more than one language available on the system, you will be prompted to select the default system language to use. This language is also used as the *admin* user's language.

5. The first prompt asks for an IP address. Enter the Primary IP address for the server appliance (for example, 10.9.19.55).
6. The second prompt asks for the netmask address. Enter the Primary Netmask for the server appliance (for example, 255.0.0.0).
7. The third prompt asks for the gateway address. Enter the gateway for the server appliance (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 server appliance through your Web browser.

Powering down the server appliance remotely



Caution: This feature requires you to access the server appliance through an ssh or telnet session. Only advanced users of Linux should undertake these changes.



Note: Direct root logins are not allowed on the Sun Cobalt RaQ 550 server appliance.



Note: You cannot power up a Sun Cobalt RaQ 550 server appliance remotely. Someone must physically power up the server.

Appendix A: Advanced Information

You can power down the server appliance remotely through an ssh or telnet session. To obtain a root shell:

1. Connect to the server appliance using ssh or telnet and log in as the user *admin* or using a server administrator account that has root access enabled.
2. From the command prompt, if logged in as the *admin* user, enter:

```
su -
```

If logged in as a server administrator, enter:

```
su - root-<username>
```

where '*<username>*' is the login name for the server administrator account used to connect.



Note: Only the *admin* user or server administrators can `su -` to root.

3. Press **Enter**. A password prompt appears.
4. Enter the password for the account used to connect to the server appliance in step 1.
5. Enter the command:

```
shutdown -h now
```

The system proceeds through its shutdown sequence and powers down.

Removing a lock from the LCD panel



Caution: This feature requires you to access the Sun Cobalt RaQ 550 server appliance through an ssh or telnet session. You can seriously affect your server appliance if you modify the system configuration files.

Only advanced users of Linux should undertake these changes. For more details, see “Warranty” on page 7.



Caution: If you have forgotten both the Administrator password and the sequence of arrow keys, you will not be able to access the server.



Note: Direct root logins are not allowed on the Sun Cobalt RaQ 550 server appliance.

If you have forgotten the sequence of arrow keys to unlock the LCD panel, you can remove the “lock” file from the server:

1. Connect to the server appliance using ssh or telnet and log in as the user *admin* or using a server administrator account that has root access enabled.
2. From the command prompt, if logged in as the *admin* user, enter:

```
su -
```

If logged in as a server administrator, enter:

```
su - root-<username>
```

where ‘<username>’ is the login name for the server administrator account used to connect.



Note: Only the *admin* user or server administrators can `su -` to root.

Appendix A: Advanced Information

3. Press **Enter**. A password prompt appears.
4. Enter the password for the account used to connect to the server in step 1.
5. Enter the command:

```
rm /etc/cobalt/.LCK..cobtpanel
```

You can now assign a new sequence through the LCD console. For more information, see “Panel menu” on page 201.

Development tools

The Sun Cobalt RaQ 550 server appliance provides a collection of utilities to support applications development and server administration. These tools include:

- GNU C/C++ compiler (`gcc`) and libraries
- Java™ Development Kit
- GNU Bourne Again Shell (`bash`)
- Text editors (`emacs`, `vi`, `pico`)
- File system utilities (`ls`, `mv`, `cp`, `ln`, `rm`, `chmod`, `chown`, `chgrp`, `du`, `df`)
- File parsing utilities (`sed`, `awk`, `diff`)
- File display utilities (`cat`, `more`, `less`)
- Search utilities (`find`, `grep`, `which`)
- Archive utilities (`gzip`, `tar`, `cpio`, `rpm`)
- Network utilities (`FTP`, `telnet`, `netstat`, `ping`, `finger`, `mail`, `pine`)
- Programming languages (`perl`, `python`, `tcl/tk`)

These utilities can be found in one of the following directories:

```
/sbin
/bin
/usr/sbin
/usr/bin
/usr/local/bin
```

For an expanded set of development tools, visit the Solutions Directory at <http://www.cobalt.com/solutions/>. For more information, see “Customer Service and Technical Support” on page 5.

You can run most pre-compiled x86-based commercial software packages on the Sun Cobalt RaQ 550 server appliance, as long as the software does not require a mouse, keyboard or monitor. Ensure that the software is compatible with the Linux 2.4 kernel and the glibc 2.1 or 2.2 library.

Configuration files

If necessary, you can change some of the configuration files for the services on the Sun Cobalt RaQ 550 server appliance for development purposes, but this may void your warranty. Before making any changes, see “Warranty” on page 7.



Caution: Changing any of the following configuration files can dramatically affect the operation of the services configured by means of the server appliance’s browser-based administration service or the administration service itself.

Only advanced users of Linux should undertake these changes. For more details, see “Warranty” on page 7.

The services and some of their associated configuration files and directories are the following:

- Email
 - `/etc/inetd.conf`
 - `/etc/mail/`
- Domain Name Service (DNS)
 - `/etc/named/`
- File transfer protocol (FTP)
 - `/etc/proftpd.conf`
- Web
 - `/etc/httpd/conf/*.conf`
- Mailing lists
 - `/usr/local/majordomo/`

Directory structure

The hard disk drive on the server appliance is partitioned into four segments. Most of the available space on the disk drive is on the partition mounted from /home. It is recommended to do most of your work under this partition. By default, quotas are turned on in this partition and are used extensively by the system software.

Virtual site home page

The document root for the virtual sites' Web page content is:

```
/home/sites/<sitename>/web
```

For example, www.cobalt.com would have a document root of

```
/home/sites/www.cobalt.com/web
```

Only the Server Administrator or the Site Administrator can upload to this directory.

Web content in this directory is associated with the URL `http://<sitename>/`.

For example, a file saved as:

```
/home/sites/<sitename>/web/testdir/test.html
```

is accessed through the URL `http://<sitename>/testdir/test.html`



Note: <Sitename> refers to the <hostname.domainname> of the corresponding virtual site.

The home directory for the *admin* user and the server administrator accounts can be accessed as:

```
/home/users/<username>
```

where <username> is the login name for the account. Also, the *admin* user and server administrator accounts have no Web directory that is accessible through the Web server.

Customized error Web pages

The Server Administrator or a Site Administrator can replace the default error Web pages for a virtual site on the Sun Cobalt RaQ 550 server appliance with customized error pages for four common Web server errors.

The errors the server appliance specifically handles with custom files for a virtual site are:

- **401: Authorization Failed**—This error page is displayed when you have protected a directory with an .htaccess file and the user does not authenticate correctly.
- **403: Forbidden**—This error page is displayed when you have changed the permissions of a file or directory so that the Web server cannot access it.
- **404: File Not Found**—This error page is displayed a request has been made for a file or directory that the Web server cannot find.
- **500: Internal Server Error**—This error page is usually displayed when a dynamic CGI page does not return data to the Web server correctly or cannot be executed properly.

The default error pages for these four errors are located in the Web directory for a virtual site under the error subdirectory. The full path to this directory is:

```
/home/sites/<sitename>/web/error
```



Note: <Sitename> refers to the <hostname.domainname> of the corresponding virtual site.

For example, for a site named `www.cobalt.com`, the error pages would be located in:

```
/home/sites/www.cobalt.com/web/error
```

The filenames for each error begin with the corresponding error code mentioned above. For example, error 404 is handled by the file “404-file-not-found.html” in the error subdirectory.

Site user home page

When a user on a virtual site is added through the Server Desktop UI, the home directory for that site user is created in:

```
/home/sites/<sitename>/users/<username>
```

The user’s default Web page is located in:

```
/home/sites/<sitename>/users/<username>/web
```

The content of their Web pages can be viewed at `http://<sitename>/~<username>/`.

Domain Name System

The Internet uses a distributed naming system called the Domain Name System (DNS). DNS allows us to refer to computers by host names as well as by Internet Protocol (IP) addresses.

IP addresses are hard to remember and are inconvenient to use. DNS allows us to use host names and domain names which can be resolved to IP addresses. DNS servers translate host names and domain names (for example, `www.sun.com`) to an associated IP address (for example, `192.168.10.10`) and vice-versa.

For example, Sun Cobalt has registered the domain name “`sun.com`” for use by our servers “`mail.sun.com`”, “`www.sun.com`” and others. The host names “`mail`” and “`www`” represent different servers registered in the same domain.

A domain name is a computer name suffix shared by a group of computers in the same organization. A domain name should be associated with an IP address through a Forward Lookup record. Domain names are organized in a hierarchy; this hierarchy includes your company or server name, and a country code (for example, `.uk` or `.ca`) or a top-level domain (for example, `.com` or `.edu`).

A Web site on the server appliance is created with one IP address, one host name and one domain name that together establish the identity of that Web site on the Internet.

Each domain name requires a primary domain authority on one DNS server. A secondary DNS server acts as a backup to the primary. DNS information is configurable only on the primary server, and not on the backup server.

There are three tabs in the DNS Settings table. The active tab is a light shade of gray; the inactive tab is a dark shade of gray.

- **Basic.** You can enable the DNS server feature.
- **Advanced.** You can configure the Start of Authority (SOA) default values and the server settings.
- **Zone Format.** You can create and select a zone file format for delegating subnets on non-octet boundaries.

There are also two buttons on the DNS screen, available under all three tabs. These are explained later in this appendix.

- **Edit Primary Services.** You can configure the primary DNS server.
- **Edit Secondary Services.** You can configure the secondary DNS server.

Basic DNS

Enabling the DNS server feature

To enable the DNS server on the Sun Cobalt RaQ™ 550 server appliance:

1. On the user interface, select **Server Management > Network Services > DNS**. The Basic Settings section of the Domain Name System (DNS) Settings table appears; see Figure B-1.
2. Click to enable the check box for Enable server (if it is not already enabled).



Note: DNS service is automatically enabled if 127.0.0.1 or another local IP address is specified as a DNS server in the Setup Wizard.

3. Click **Save**.

Figure B-1. Basic DNS table

The screenshot shows the 'DNS Settings' interface. At the top, there are two buttons: 'Edit Primary Services' and 'Edit Secondary Services'. Below these is a header bar for 'DNS Settings' with three tabs: 'Basic', 'Advanced', and 'Zone Format'. The 'Basic' tab is selected. Under the 'Basic' tab, there is a table with one row: 'Enable Server' with a checked checkbox. Below the table is a 'Save' button.

DNS Settings			
	Basic	Advanced	Zone Format
Enable Server	<input checked="" type="checkbox"/>		

Save

Advanced DNS



Important: Always click **Save** after modifying the settings in the Advanced section. If you do not, the changes will not take effect.

Configuring SOA default values

You can fine tune the primary domain and network authority settings—known as the Start of Authority (SOA) settings—independently of each other.

To modify the SOA settings, see “Modifying the SOA record” on page 176.

To configure the default values for the SOA settings:

1. On the user interface, select **Server Management > Network > DNS**. The Advanced Settings section of DNS Settings table appears; see Figure B-2.
2. Click **Advanced** on the right side of the table. The fields for the SOA default values and server settings appear. You can configure the values for the following parameters. The parameters are explained in the following paragraphs.
 - Domain administrator email address (optional)
 - Refresh interval (in seconds)
 - Retry interval (in seconds)
 - Expire interval (in seconds)
 - Time-to-live (TTL) interval (in seconds)
3. Enter the IP address(es) of any forwarding DNS server(s).
4. Enter the IP address(es) for zone transfer access.
5. Click **Save**.

Figure B-2. Advanced DNS table

Edit Primary Services Edit Secondary Services

DNS Settings	
	Basic Advanced Zone Format
Start of Authority (SOA) Default Values	
Default DNS Administrator Email Address <i>(optional)</i>	<input type="text"/>
Default Refresh Interval (Seconds)	<input type="text" value="10800"/>
Default Retry Interval (Seconds)	<input type="text" value="3600"/>
Default Expire Interval (Seconds)	<input type="text" value="604800"/>
Default Time-To-Live Interval (Seconds)	<input type="text" value="86400"/>
Server Settings	
Cache Record Lookups	<input checked="" type="checkbox"/>
Forwarding Servers <i>(optional)</i>	<input type="text"/>
Zone Transfer Access by IP Address <i>(optional)</i>	<input type="text"/>

Save

Domain administrator email address

The email address defaults to the user name *admin* of the Sun Cobalt RaQ 550 server appliance. This email address is publicly available and is the administrative contact for the domain or network served. The form *my.name@xyz.com* is not acceptable in this field (there can be no “dot” in the user name).

Refresh interval

You can configure the refresh interval between updates from a secondary DNS server.

- If DNS record changes occur infrequently, increase the default value
- If DNS record changes occur often, decrease the default value

Tune the refresh interval to avoid wasting bandwidth and to ensure the content on the secondary server is accurate at all times.

Retry interval

Due to a connection or service failure, a secondary DNS server may be unable to refresh data from the primary server. The secondary DNS server attempts to refresh data after the interval specified for trying again.

Expire interval

A secondary DNS server may be unable to refresh data from the primary server for a prolonged period of time. After the interval specified for expiry, the secondary server stops serving name requests.

Time-to-live period (TTL)

A caching DNS server other than the primary and secondary DNS servers for this domain or network can cache record lookups for the TTL period. During the TTL period, a caching DNS server does not poll the primary or secondary DNS servers for repeated lookups of the same record.

Configuring the server settings

You can also configure the server settings and the zone transfer access control for the DNS server. on the Sun Cobalt RaQ 550 server appliance.

Cache record lookups

Enabling caching, also called recursion, allows resolution of domains and network zones that other name servers are authoritative for. Disabling caching is useful when operating this server on a private network.

Forwarding server

If the Sun Cobalt RaQ 550 server appliance is being used on a private network or in conjunction with a restrictive firewall, you can specify a forwarding DNS server(s) by IP address. If a DNS server cannot answer a DNS query, it forwards the query to the forwarding DNS server to get the needed response, then answers back to the client.



Note: If you have a primary or secondary DNS entry in a given domain provided by the Sun Cobalt RaQ 550 server appliance, no requests in that domain will be forwarded to the forwarding server.

Zone transfer

A zone transfer allows another DNS server to download the complete list of hosts maintained by your DNS server. Zone transfers are used by secondary domain name servers to synchronize their records with primary domain name servers.

By default, zone transfers are not allowed to any domain. You must explicitly enter any domain names that are allowed to perform zone transfers, or no domain will be able to perform zone transfers.

Zone Format

You can create and select a zone file format for delegating subnets on non-octet boundaries that is compatible with your local reverse-delegation method. RFC2317 is the international standard format. Consult your ISP to determine the type of subnet DNS delegation they are using.

The DNS server on the Sun Cobalt RaQ 550 server appliance can support user-defined network-delegation formats. If your company uses a proprietary zone file format, you can enter the format parameters in the table on this page.



Note: If you select the option “User-defined”, you must fill in all four fields in the table.

The symbols in the fields are defined as follows:

%1 represents the first octet of a four-octet IP address.

%2 represents the second octet of a four-octet IP address.

%3 represents the third octet of a four-octet IP address.

%4 represents the fourth octet of a four-octet IP address.

%n represents the size of the network (in bits)

For example, if the IP address is 192.168.10.19/0-31:

%1 is 192.

%2 is 168.

%3 is 10.

%4 is 19.

%n is an integer number from 0 to 31.



Important: Consult your network administrator or ISP for the correct order of the data in the proprietary format they are using.

To configure the Zone Format settings:

1. On the user interface, select **Server Management > Network > DNS**. The Domain Name System (DNS) Settings table appears.
2. Click **Zone Format** on the right side of the table. The fields and default values for the Zone File Formats appear; see Figure B-3.

Figure B-3. Zone Format table

Edit Primary Services Edit Secondary Services

DNS Settings	
Basic Advanced Zone Format	
Zone File Format Settings	
Zone File Format	RFC2317
User Defined Zone File Format Settings	
Zone File Format for > 24-bit networks. (optional)	%4/%n.%3.%2.%1.in-add
Zone File Format for > 16-bit networks. (optional)	%3/%n.%2.%1.in-addr.arj
Zone File Format for > 8-bit networks. (optional)	%2/%n.%1.in-addr.arpa
Zone File Format for > 0-bit networks. (optional)	%1/%n.in-addr.arpa

Save

3. Select a zone file format.

RFC2317 is the international standard format.

You can also select the option “User-defined”. If you select the option “User-defined”, fill in the four fields.

4. Click **Save**.


Primary services

A primary DNS server maintains a list of name records and their associated IP addresses. This list is made available to other DNS servers if your domain is registered with your country-specific domain-naming organization. Your Internet service provider (ISP) can help you register your Internet server.

Figure B-4 shows some sample entries in the Primary Service List table.

Figure B-4. Sample entries in the Primary Service List table

Select Domain... Add Record...

DNS Primary Service List - localdomain			
Modify SOA		Remove Records	
1 Entry			
Query ▾	Type ▾	Response ▾	Action
raq550 . localdomain	Forward	63.77.128.201	 

Apply Changes Now Back

To set up the primary DNS server on the Sun Cobalt RaQ 550 server appliance, you need to use the Add Record... pulldown menu to configure the following DNS records.

- Forward Address (A) record
- Reverse Address (PTR) record
- Mail Server (MX) record
- Alias (CNAME) record
- Subdomain Delegation
- Subnet Delegation

If there are no records defined, there are no authority selection options available.

If there are records defined, the Select Domain ... menu is available at the top of the screen. There are also two buttons available at the top of the Primary Service List table: Modify SOA and Remove Records.

Selecting a domain

To display the DNS records for a particular domain, click on the Select Domain... pull-down menu and select the domain.

The screen refreshes and the Primary Service List table displays the DNS records for that domain. The domain name shows up in the title bar.

Modifying the SOA record

You can modify the SOA record for a particular domain or network. For an explanation of the fields you can modify, see “Configuring SOA default values” on page 169.

1. From the pull-down menu, select the domain for which you want to modify the SOA record. The defined records for that domain appear in the Primary Service List table.
2. Click **Modify SOA** at the top of the Primary Service List table. The Modify SOA Record table appears. The first field displays either the domain name or the network authority that you selected.
 - **Primary Name Server**
Enter the fully qualified domain name of the primary name server for the selected domain or network authority.
 - **Secondary Name Server**
Enter the fully qualified domain name(s) of the secondary name server(s) for the selected domain or network authority. If you want to specify more than one secondary name server, separate the names with a space.
 - **DNS Administrator email address**
 - **Refresh interval**
 - **Retry interval**
 - **Expire interval**
 - **Time-to-live interval**
3. Click **Save**. The screen refreshes and the Primary Service List table appears.

Deleting all DNS records

You can delete all the DNS records for a particular domain name from the Primary Service List table.

1. From the pull-down menu, select the domain for which you want to modify the SOA record. The defined records for that domain appear in the Primary Service List table.
2. Click **Remove Records** at the top of the Primary Service List table. A confirmation dialog appears, asking you if you want to remove all of the DNS records displayed in the table.
3. Click **OK**. The screen refreshes and the Primary Service List table is now empty.

Modifying a specific DNS record

To modify an individual entry in the Primary Service List table, click on the green *pencil* icon next to that entry. The Modify Record table appears.

Click **Save**. The screen refreshes.

Deleting a specific DNS record

To delete an individual entry from the Primary Service List table, click on the red *trash can* icon next to that entry. A confirmation window appears, asking if you want to delete the record.

Click **OK**. The screen refreshes and the Primary Service List table no longer display that record.

Configuring a Forward Address (A) record

A Forward Address (A) record translates a fully qualified domain name into an IP address.

To configure a Forward Address (A) record for your server appliance:

1. Select **Server Management > Network Services > DNS**.

The DNS Settings table appears.

2. Click **Edit Primary Services** above the table. The Primary Service List table appears.
3. Select Forward Address (A) Record from the **Add Record...** pull-down menu. The Add New Forward Address (A) Record table appears.
4. Enter the host name (optional) and domain name you want to serve (for example, www and mydomain.com).
5. Enter the IP address (for example, 192.168.10.10) that is used by the host and domain names entered in the first two fields.
6. Click **Save**. The Primary Service List table reappears with the new entry.
7. To add another record, select a record type from the pull-down menu again.

To apply the changes to the DNS settings, click **Apply Changes Now**. The DNS Settings table appears.

Configuring a Reverse Address (PTR) record

A Reverse Address (PTR) record translates an IP address into a fully qualified domain name.

To configure a Reverse Address (PTR) record for your server appliance:

1. Select **Server Management > Network Services > DNS**.

The DNS Settings table appears.

2. Click **Edit Primary Services** above the table. The Primary Service List table appears.
3. Select Reverse Address (PTR) Record from the **Add Record...** pull-down menu. The Add New Reverse Address (PTR) Record table appears.
4. Enter the IP address (for example, 192.168.10.10) that you want to resolve to a fully qualified domain name.
5. The Subnet Mask field holds the default value of 255.255.255.0. You can edit this value if necessary.
6. Enter the host name (optional) and domain name (for example, www and mydomain.com) to which the IP address in the first field resolves.
7. If you have not already created a Forward Address (A) record to resolve this host name and domain name to the specified IP address, you can automatically generate one.

To do so, click the check box **Generate Forward Address (A) Record**.

8. Click **Save**. The Primary Service List table reappears with the new Reverse Address (PTR) entry. If you generated a Forward Address (A) record, that entry appears as well.
9. To add another record, select a record type from the pull-down menu again.

To apply the changes to the DNS settings, click **Apply Changes Now**. The DNS Settings table appears.

Configuring a Mail Server (MX) record

To receive mail for your domain name (for example, mydomain.com), you need to create a Mail Server (MX) Record.

A Mail Server (MX) record identifies the mail server responsible for delivering email messages to a specified host name (optional) and domain name. An MX record is similar to an A record but resolves to a fully qualified domain name rather than an IP address.



Important: It is critical that the MX record resolve to a fully qualified domain name that has a corresponding A record.

To configure a Mail Server (MX) record for your server appliance:

1. Select **Server Management > Network Services > DNS**.

The DNS Settings table appears.

2. Click **Edit Primary Services** above the table. The Primary Service List table appears.
3. Select Mail Server (MX) Record from the **Add Record...** pull-down menu. The Add New Mail Server (MX) Record table appears.
4. Enter the host name (optional) and domain name (for example, www and mydomain.com) to be served by the mail server.
5. Enter the fully qualified domain name of the mail server (for example, mail.mydomain.com) that serves the domain name entered in the second field.
6. Under the Delivery Priority pull-down menu, select the priority for mail delivery to the mail server: very high, high, low, very low.

The value of the delivery priority specifies the order in which a series of mail servers is contacted for mail delivery. The Delivery Priority setting is useful only if more than one MX record is configured for a domain or network.

7. Click **Save**. The Primary Service List table reappears with the new entry.
8. To add another record, select a record type from the pull-down menu again.

To apply the changes to the DNS settings, click **Apply Changes Now**. The DNS Settings table appears.

Configuring an Alias (CNAME) record

An Alias (CNAME) record provides the translation from one fully qualified domain name to another fully qualified domain name.

The source domain name is known as the alias and the target domain name is known as the canonical name or real name. The target host name does not need to be a member of the local domain. For example, you can create an Alias (CNAME) record of “news.domain.com” resolving to “uucp.isp.net”.



Important: Do not use an Alias (CNAME) record to cause a domain name to resolve to a host name.

For example, do not create an Alias (CNAME) record for mydomain.com that resolves to www.mydomain.com. Instead, add a Forward Address (A) record for mydomain.com to the IP address used by www.mydomain.com. See “Configuring a Forward Address (A) record” on page 178.

CNAME host names must be unique. A and MX records must not share host names with a CNAME record.

To configure an Alias (CNAME) record for your server appliance:

1. Select **Server Management > Network Services > DNS**.

The DNS Settings table appears.

2. Click **Edit Primary Services** above the table. The Primary Service List table appears.
3. Select Alias (CNAME) Record from the **Add Record...** pull-down menu. The Add New Alias (CNAME) Record table appears.
4. Enter the host name (optional) and domain name (for example, news and mydomain.com) of the alias.
5. Enter the host name (optional) and domain name (for example, news and otherplace.com) of the real domain name.
6. Click **Save**. The Primary Service List table reappears with the new entry.
7. To add another record, select a record type from the pull-down menu again.

To apply the changes to the DNS settings, click **Apply Changes Now**. The DNS Settings table appears.

Adding a Subdomain Delegation

Select **Subdomain Delegation** from the **Add Record...** pull-down menu. The Add a Subdomain Delegation screen is shown in Figure B-5.

Figure B-5. Add a Subdomain Delegation

Add a Subdomain Delegation	
Parent Domain Name	thisdomain
Subdomain Name	<input type="text"/>
Name Servers	<div style="border: 1px solid gray; height: 60px; width: 100%;"></div>

To configure the Add a Subdomain settings:

1. **Parent Domain Name.** Select the Parent Domain Name. For example, to delegate the subdomain `remote.example.com`, select `example.com`.
2. **Subdomain Name.** Specify the unqualified Subdomain Name. For example, to delegate the subdomain `remote.example.com`, this server must be authoritative for the domain `example.com`. Specify only the subdomain name, `remote`.
3. **Name Server.** Specify a comma-separated list of fully qualified host names that are authoritative for the specified subdomain. At least one name server must be specified.

Adding a Subnet Delegation

To add a subnet delegation, you must first add a Reverse PTR Record (see “Configuring a Reverse Address (PTR) record” on page 179).

After you add the record and apply the changes, the DNS Primary Service List appears similar to the screen shown in Figure B-6.

Figure B-6. DNS Primary Service List (after adding Reverse PTR Record)

Select Domain... | Select Network... | Add Record...

DNS Primary Service List - 192.168.1.0/255.255.255.0			
Modify SOA Remove Records			3 Entries
Query ▾	Type ▾	Response ▾	Action
seconddomain	Forward	192.168.1.50	
192.168.1.1	Reverse	thishost . thisdomain	
192.168.1.50	Reverse	seconddomain	

[Apply Changes Now](#) [Back](#)

To configure the Add a Subnetwork settings:

1. Select **Subnet Delegation** from the **Add Record...** pull-down menu. The Add a Subnet Delegation appears; see Figure B-7.
2. **Parent Network.** This is the parent network for which this server is authoritative. All IP addresses in the specified subnet must belong to this parent network.
3. **Subnet IP Address.** Specify an IP address within the desired subnet that will be delegated to another DNS server.

Figure B-7. Add a Subnet Delegation

Add a Subnet Delegation	
Parent Network	192.168.1.0/255.255.255.0
Subnet IP Address	<input type="text" value="192.168.1.0"/>
Subnet Network Mask	<input type="text" value="255.255.255.128"/>
Name Servers	<input type="text"/>

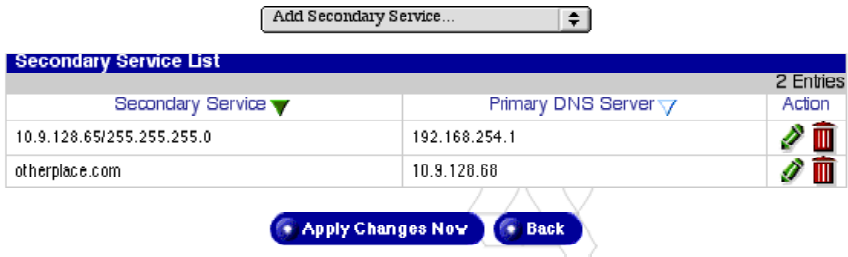
4. **Subnet Network Mask.** Specify the subnet network mask in dot-quad notation.
5. **Name Servers.** Specify a comma-separated list of fully qualified host names that are authoritative for the specified subnet. At least one name server must be specified.
6. Click **Save** to save the subnet delegation.

Secondary services

The Administrator can configure a secondary DNS server to provide redundant DNS service to your computers. If the primary DNS server is unavailable, the secondary DNS server takes over.

Figure B-8 shows some sample entries in the Secondary Service List table.

Figure B-8. Sample entries in the Secondary Service List table



Secondary service for a domain

To add a secondary name-server authority for a domain:

1. Select **Server Management > Network Services > DNS**. The DNS Settings table appears.
2. Click **Edit Secondary Services** above the table. The Secondary Service List table appears.
3. Select Domain Secondary Service for a domain from the **Add Secondary Service...** pull-down menu. The Add Secondary Service table appears; see Figure B-9.
4. In the first field, enter the domain name for which DNS information is served by the IP address in the second field.
5. In the second field, enter the IP address of the primary DNS server for the domain name specified in the first field.
6. Click **Save**. The Secondary Service List table reappears with the new entry.
7. To add another secondary service, select a service from the pull-down menu again.

To apply the changes to the DNS settings, click **Apply Changes Now**. The DNS Settings table appears.

Figure B-9. Add Secondary Domain table

DNS Add Secondary Service	
Domain Name	<input type="text"/>
Primary DNS Server IP Address	<input type="text"/>

Secondary service for a network

To add a secondary name-server authority for a network:

1. Select **Server Management > Network > DNS**.

The DNS Settings table appears.

2. Click **Edit Secondary Services** above the table. The Secondary Service List table appears.
3. Select Network Secondary Service from the **Add Secondary Service...** pull-down menu. The Add Secondary Service table appears; see Figure B-10.
4. In the first field, enter the IP address of a member on the network (for example, 192.168.1.1) whose DNS information is served by the IP address in the third field.
5. In the second field, enter the subnet mask corresponding to the IP address for the specified network authority.
6. In the third field, enter the IP address of the primary DNS server for the specified network.
7. Click **Save**. The Secondary Service List table reappears with the new entry.
8. To add another secondary service, select a service from the pull-down menu again.

To apply the changes to the DNS settings, click **Apply Changes Now**. The DNS Settings table appears.

Figure B-10. Add Secondary Network table

DNS Add Secondary Service	
Network	<input type="text"/>
Network Subnet Mask	255.255.255.0
Primary DNS Server IP Address	<input type="text"/>

Sample setup of DNS service

This sample setup of DNS service on your Sun Cobalt RaQ 550 server appliance assumes that you have already registered your domain with InterNIC or another registration service. If you have not, refer to the FAQ section on Sun Cobalt's Web site (<http://www.sun.com/service/suncobalt> under the Knowledge Base link) for information on registering your domain name.

For more information on registering a Web site, visit the Internet Corporation for Assigned Names and Numbers (ICANN) at <http://www.icann.org>.

In the following examples, we will configure a sample domain called "mydomain.com" for Web service and email service using a sample IP address 192.168.10.10.



Important: Substitute your domain name and IP address where the sample domain name or sample IP address appears.

The recommended minimum configuration for Web and email service requires the following records. These records allow anyone on the Internet to type either "mydomain.com" or "www.mydomain.com" to access your Web site.

- A Reverse Address (PTR) record for 192.168.10.10., which resolves to mydomain.com
- A Forward Address (A) record for mydomain.com, which resolves to 192.168.10.10 (You can generate this record automatically from the PTR record.)
- A Forward Address (A) record for www.mydomain.com, which resolves to 192.168.10.10
- A Mail Server (MX) record for mydomain.com, which resolves to www.mydomain.com

Reverse Address (PTR) record

First, create a Reverse Address (PTR) record.

1. Select **Server Management > Network Services > DNS**. The DNS Settings table appears.
2. Click **Edit Primary Services** above the table. The Primary Service List table appears.
3. Select Reverse Address (PTR) Record from the **Add Record...** pull-down menu. The Add New Reverse Address (PTR) Record table appears; see Figure B-11.
 - In the IP Address field, enter 192.168.10.10.
 - Leave the subnet mask as 255.255.255.0.
 - In the Host Name field, enter www.
 - In the Domain Name field, enter mydomain.com.
4. Click the check box **Generate Forward Address (A) Record** to generate a Forward Address (A) record.
5. Click **Save**. The Primary Service List table reappears with the new Reverse Address (PTR) and Forward Address (A) entries.

Figure B-11. Add New Reverse Address (PTR) Record table

DNS Add New Reverse Address (PTR) Record	
IP Address	<input type="text"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Host Name <i>(optional)</i>	<input type="text"/>
Domain Name	<input type="text"/>
Generate Forward Address (A) Record	<input type="checkbox"/>

Forward Address (A) record

Next, create a Forward Address (A) record.

1. Select **Server Management > Network > DNS**. The DNS Settings table appears.
2. Click **Edit Primary Services** above the table. The Primary Service List table appears.
3. Select Forward Address (A) Record from the **Add Record...** pull-down menu. The **Add New Forward Address (A) Record** table appears; see Figure B-12.
 - Leave the Host Name field blank
 - In the Domain Name field, enter mydomain.com
 - In the IP Address field, enter 192.168.10.10
4. Click **Save**. The Primary Service List table reappears with the new Forward Address (A) entry.

Figure B-12. Add New Forward Address (A) Record table

DNS Add New Forward Address (A) Record	
Host Name <i>(optional)</i>	<input type="text"/>
Domain Name	<input type="text" value="localdomain"/>
IP Address	<input type="text"/>

• Save • Cancel

Mail Server (MX) record

Finally, create a Mail Server (MX) record.

1. Select **Server Management > Network > DNS**. The DNS Settings table appears.
2. Click **Edit Primary Services** above the table. The Primary Service List table appears.
3. Select Mail Server (MX) Record from the **Add Record...** pull-down menu. The Add New Mail Server (MX) Record table appears; see Figure B-13.
 - Leave the Host Name field blank
 - In the Domain Name field, enter mydomain.com
 - In the Mail Server Name field, enter mail.mydomain.com
 - Under the Delivery Priority pull-down menu, leave the priority as Very High
4. Click **Save**. The Primary Service List table reappears with the new Mail Server (MX) entry.

Figure B-13. Add New Mail Server (MX) Record table

DNS Add New Mail Server (MX) Record	
Host Name <i>(optional)</i>	<input type="text"/>
Domain Name	<input type="text" value="localdomain"/>
Mail Server Name	<input type="text"/>
Delivery Priority	<input type="text" value="Very High (20)"/>

You are now finished with creating your DNS records.

To edit another domain, select another domain from the **Select Domain or Network...** pull-down menu. You can select any domain that you have configured for the DNS server,



Important: Click **Apply Changes Now**. This activates the changes you have made. If you exit this screen without saving your changes, they will not become active.

To add a new domain, use the **Add Record...** pull-down menu again. In the **Domain Name** field of the type of record you select, replace the default domain name with the new domain name that you want to create.

For further information, refer to the following:

- In the Sun Cobalt Knowledge Base, search on “DNS”
- <http://www.dnswiz.com/dnsworks.htm> (not affiliated with Sun Cobalt)

Brief history of the Domain Name System (DNS)

In the 1960s, the U.S. Department of Defense Advanced Research Projects Agency (ARPA, and later, DARPA) began funding an experimental wide area computer network called the ARPAnet. The ARPAnet used a centrally administered file called HOSTS.TXT that held all name-to-address mapping for each host computer connected to the ARPAnet. Since there were only a handful of host computers at the start, HOSTS.TXT worked well.

When the ARPAnet moved to the Transmission Control Protocol/Internet Protocol (TCP/IP) suite of protocols and become known as the Internet, the network population exploded. HOSTS.TXT became plagued with problems, namely

- traffic and load
- name collisions
- consistency

A replacement for the HOSTS.TXT file was needed. The goal was to create a system that solved the problems inherent in a unified host table system. The new system should allow local administration of data and also make that data globally available.

In 1984, the architecture of a new system called Domain Name System (DNS) was designed and is the basis of the DNS service used today on the Internet.

DNS is a distributed database that allows local administration of the segments on the overall database. Data in each segment of the database are available across the entire network through a client-server scheme consisting of name servers and resolvers.

What is a DNS record?

People are much more comfortable dealing with names rather than strings of numbers. A domain name such as “sun.com” is much easier to remember than the IP address, which consists of four octets of numbers such as 63.77.128.100. Domain names must be registered with Root Domain Registration Service; visit the Internet Corporation for Assigned Names and Numbers (ICANN) at <http://www.icann.org> for a list accredited domain-name registrars.

Computers, on the other hand, prefer numbers to names. Since computers have the final say when a user is looking for a company Web site, a mechanism is needed to convert the human-friendly domain name to the computer-friendly IP address.

DNS records on a DNS server perform this function. The records translate a domain name to an IP address; a record equates a domain name such as “sun.com” to an IP address such as 207.91.131.30. Once the domain name has been converted or “resolved” to an IP address, then (and only then) can the user connect to your Web site.

Without DNS and domain names, the user would be required to remember the IP address of every site they wanted to visit. With DNS servers and DNS records, customers and their software can easily remember how to get to your site.

Who manages your DNS records?

Your DNS records can reside on any Sun Cobalt server appliance that has the DNS service enabled. You or your administrator can easily configure a Sun Cobalt server appliance to act as a DNS server. To provide DNS service, InterNIC requires a site to maintain both a primary and a secondary server. Your Sun Cobalt server appliance can act as the primary server and a DNS server from your Internet service provider (ISP) can act as the secondary server.

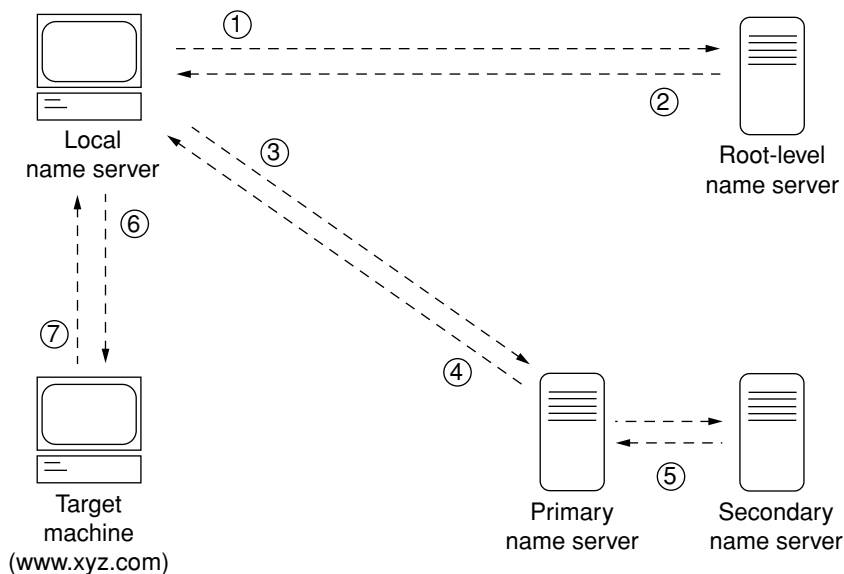
How does DNS work?

The basic method that allows a domain name to direct customers to your Web site is shown in Figure B-14. This diagram describes a request made by a Web browser as the customer attempts to log on to your Web site.

To determine which primary name server contains your domain name:

1. The local name server (the DNS resolver/browser machine) contacts the root domain name server maintained by the several Internet root server authorities.
2. The root domain name server returns the IP address of the primary name server responsible for the requested domain name.
3. The local name server contacts the primary name server.
4. The primary name server holds the IP address information for the domain name in a database and satisfies the request from the local name server.
5. If the primary name server is unavailable, the local name server contacts the secondary name server that satisfies the request from the local name server. The local name server returns to the Web browser with the IP address for the requested domain name.
6. Using the IP address, the Web browser contacts the company Web server.
7. The company Web server sends the Web page to the local name server.

Figure B-14. Basic method of DNS



LCD Menu Options

The menu options on the LCD panel on the front of the Sun Cobalt RaQ™ 550 server appliance are detailed in this appendix.


As the server appliance powers up, the LCD menu displays several temporary messages. After the server appliance has finished booting, the LCD displays the following message:

```
PRIMARY IP ADDR:  
000.000.000.000
```

If the IP information has already been set up using the Setup Wizard, the LCD displays something like:

```
user.company.com  
001.009.025.087
```

Press the **(S)** button and hold it down for a second or two to enter the LCD menu.

While in the LCD menu, depressing the Select button, , advances the menu through all of the following the top-level menu choices:

PRIMARY IP ADDR:
000.000.000.000

SETUP NETWORK

AUTOUPDATE

CONFIGURE UPS

POWER

PANEL



LANGUAGE

CLEARSCANDETECT

RESET PASSWORD

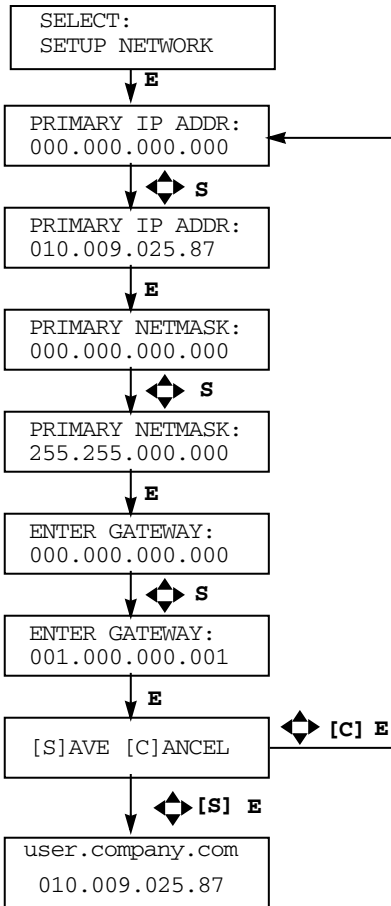
EXIT

The **Select** button is also used to move across same-level choices within the above menus.

Depressing the **Enter** button  at any of these menus takes you deeper into that menu. The remainder of this chapter diagrammatically shows all the menu choices for each menu option. When there are values to enter or choices to select in a particular menu, you do so by clicking the Up, Down, Right or Left arrows on the front panel, represented by the following symbol on the diagrams: .

Setup network menu

Figure C-1. Setup Network LCD menu



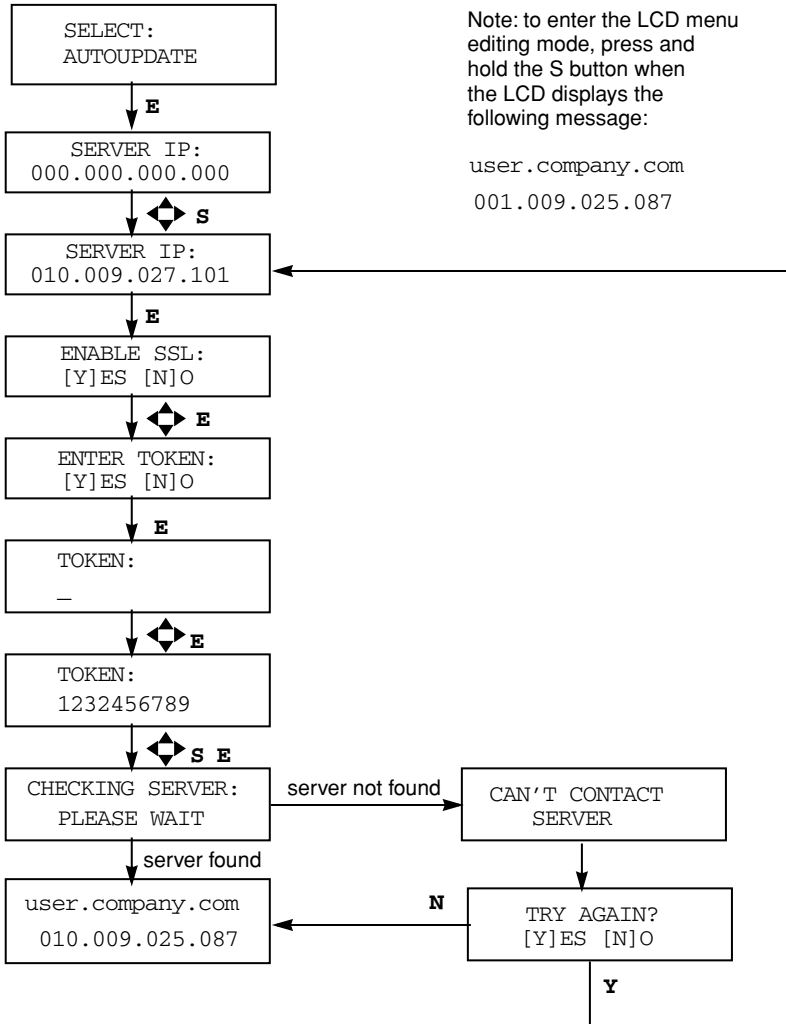
Note: to enter the LCD menu editing mode, press and hold the S button when the LCD displays the following message:

```
PRIMARY IP ADDR:
000.000.000.000
```

Autoupdate menu

For additional information, see “Software Auto-Provisioning (AutoUpdate)” on page 30.

Figure C-2. Autoupdate LCD menu

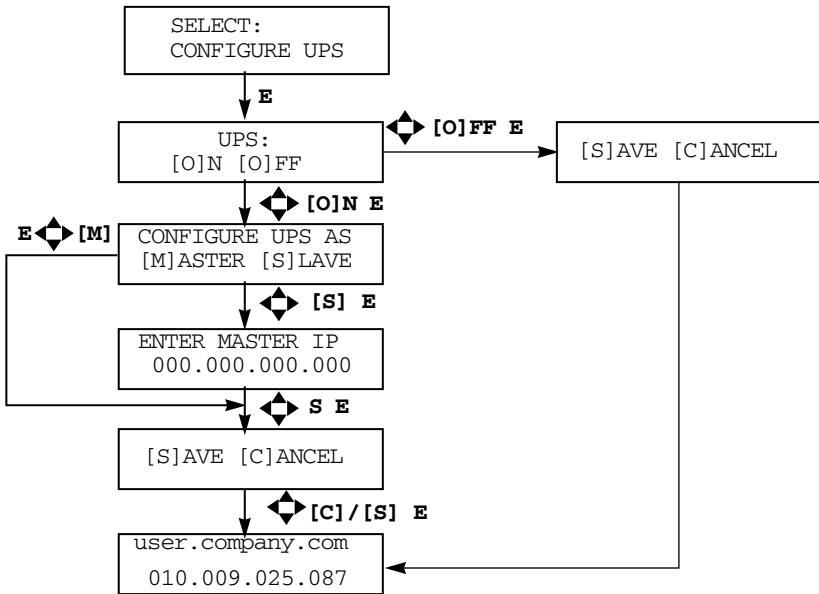


1. If the autoupdate server is found, the admin gets mail indicating that software packages were downloaded and can be reviewed under the BlueLinQ menus on the UI.
2. If the autoupdate server IP is valid, but other options are not, the admin receives mail with the subject “Autoload error” and an explanation of why packages could not be downloaded.

Configure UPS menu

For additional information, see “UPS” on page 85.

Figure C-3. Configure UPS LCD menu



Note: to enter the LCD menu editing mode, press and hold the S button when the LCD displays the following message:

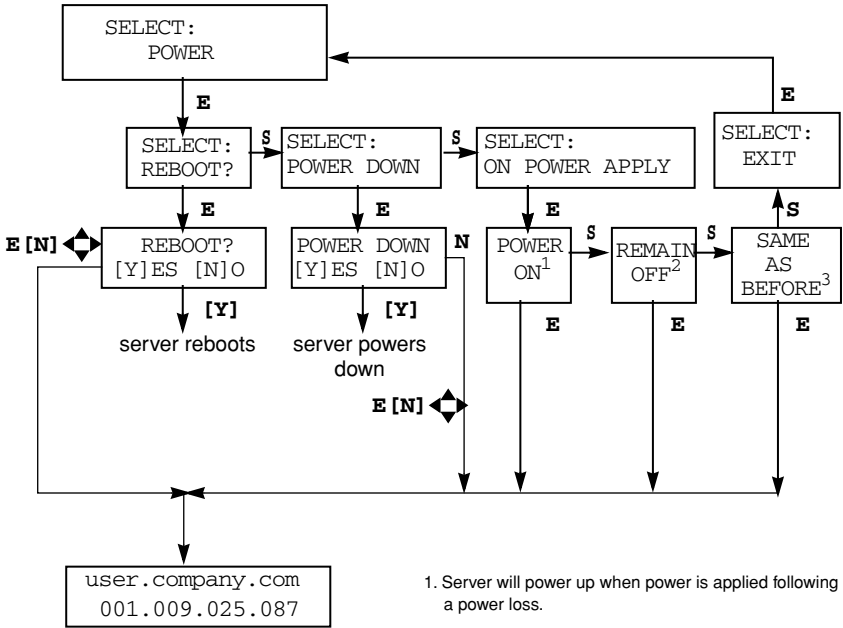
```

user.company.com
001.009.025.087
  
```

Power menu

For additional information, see “Power” on page 82.

Figure C-4. Power LCD menu



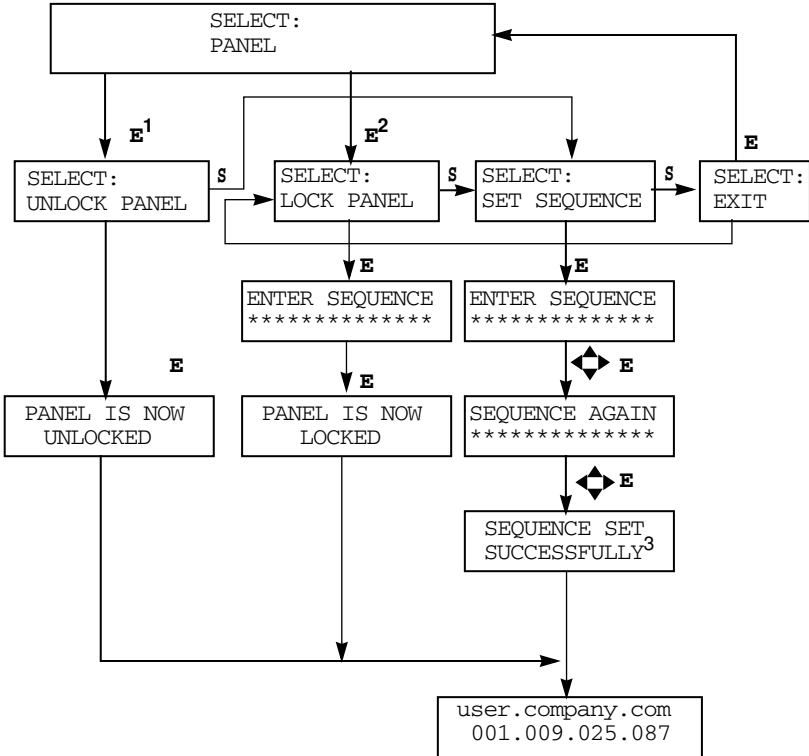
1. Server will power up when power is applied following a power loss.
2. Server will remain off when power is applied following a power loss.
3. Server will power up when power is applied following a power loss if server was on prior to the power loss. If server was off prior to the power loss, it will remain off when power is applied.

Note: to enter the LCD menu editing mode, press and hold the S button when the LCD displays the following message:

```
user.company.com
001.009.025.087
```


Panel menu

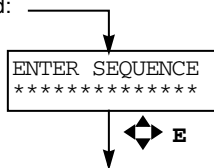
Figure C-5. Panel LCD menu



Note: to enter the LCD menu editing mode, press and hold the S button when the LCD displays the following message:

```
user . company . com
001 . 009 . 025 . 087
```

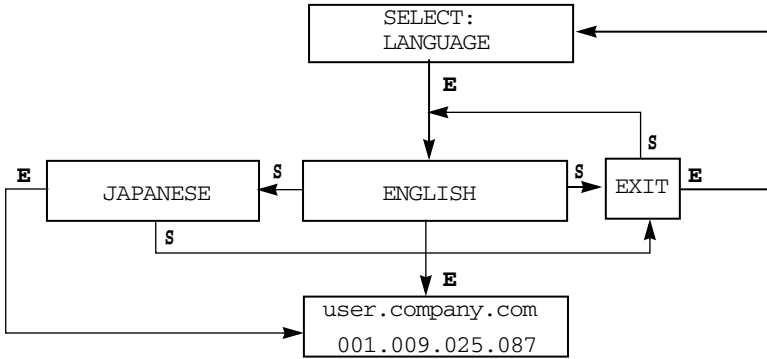
1. Current panel state is locked
2. Current panel state is unlocked
3. If panel use is attempted after panel is locked:



You can now use the panel

Language menu

Figure C-6. Language LCD menu



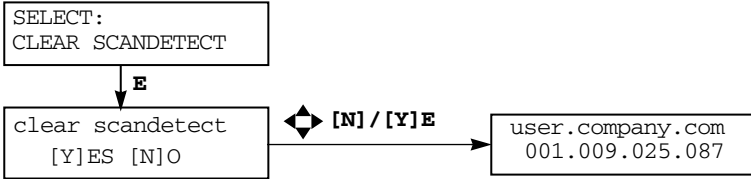
Note: to enter the LCD menu editing mode, press and hold the S button when the LCD displays the following message:

```
user . company . com  
001 . 009 . 025 . 087
```

Clear scandetect menu

For additional information, see “Scan Detection” on page 67.

Figure C-7. Clear scandetect LCD menu



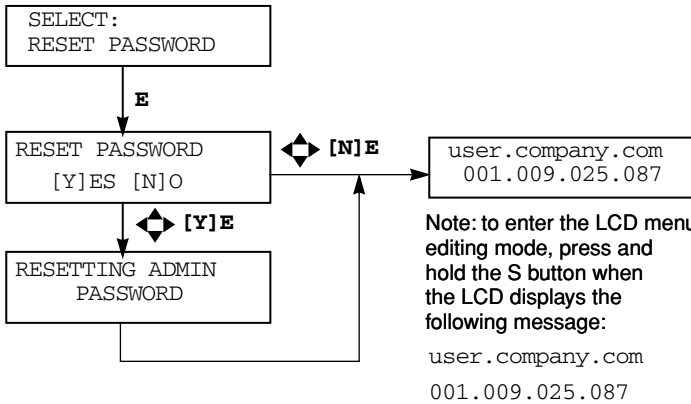
Note: to enter the LCD menu editing mode, press and hold the S button when the LCD displays the following message:

```
user.company.com
001.009.025.087
```

Reset password menu

For additional information, see “Resetting the Administrator password” on page 48.

Figure C-8. Reset password LCD menu



Disaster Recovery with Third-Party Software

The Sun Cobalt RaQ™ 550 server appliance supports the use of third-party backup solutions for performing disaster recovery. The supported backup solutions are:

- Knox Arkeia
- Legato NetWorker™

Each of these solutions requires customization to correctly recover the Sun Cobalt configuration database in the Sun Cobalt RaQ 550 server appliance (the database in Cobalt Configuration Engine [CCE]). This appendix describes how disaster recovery works on the server appliance, the steps required to perform general disaster recovery, and detailed instructions on how to customize and use each of the specific backup solutions.

How disaster recovery works

For the Sun Cobalt RaQ 550 server appliance, the term *disaster recovery* means restoring the server after performing an OS restore operation which wipes the hard disk drive clean and returns it to a factory-fresh state. This is also known as “bare-metal recovery”. The entire server appliance must be restored in order for the configuration database and the machine configuration to be in synchronization.

For most files on the server appliance, disaster recovery is straightforward: the files are recovered from the backup service and written to the file system. However, the configuration database requires additional work and the two supported backup services must be tailored to correctly restore the server appliance.

The approach used to recover the configuration database using Knox Arkeia works as follows:

Before a backup operation begins, the pre-backup script `cobalt_prebackup` creates an archive of the configuration database in the directory `/var/cobalt/backups`.

The backup makes copies of the archive:

```
/var/cobalt/backups/cce.tar
```

When the backup is complete, the post-backup script `cobalt_postbackup` deletes the archive.

During the disaster-recovery process, the entire server appliance must be restored. This restores the archive to the directory `/var/cobalt/backups`. When the backup is complete, the server appliance must be rebooted; the server appliance does not reboot automatically. During the reboot process, the `cobalt_restore` startup script detects the archive and restores the configuration database. At this point, everything should be in a consistent state and disaster recovery is complete.

Legato NetWorker works in a different manner: it recovers the database during the file recovery phase since this service permits per-file scripting at both backup and recover time. The `cceasm` script is used for this purpose.

Locking the UI database

For all types of backup, the configuration database for the Server Desktop user interface (UI) is locked for as short a period of time as possible. For Arkeia, the Server Desktop UI is locked during the pre-backup creation of the database archives. NetWorker locks the Server Desktop UI only during the backup of the individual databases.



Important: Changes to the machine configuration should not be made during the backup of the machine; otherwise, the configuration of the machine and the configuration databases may not be synchronized after the disaster-recovery process is complete.

This is also true for modifications to the system configuration that does not use the Server Desktop UI. After disaster recovery, the machine may be in an inconsistent state if the configuration database and the system configuration files do not agree.

Sun Cobalt recommends that you schedule backups for times when it is unlikely that system configuration changes will be made. Partly for this reason, most backup systems automatically schedule backups for the early hours in the morning.

General steps to perform disaster recovery

The general procedure for performing disaster recovery is as follows:

1. Perform an OS restore to wipe the hard disk drive and return the Sun Cobalt RaQ 550 server appliance to a factory-fresh state.



Important: Be sure to remove any additional storage devices before the OS restore. If they are present, the OS restore process will incorporate them into a RAID array.

2. Configure the server appliance through the Setup Wizard and return it to the network. The server appliance must be able to communicate with the backup server.
3. Through the Server Desktop UI on the server appliance, configure the backup service with which you backed up your server appliance. The tasks include enabling the backup client and entering a backup server name. The specific configuration information is discussed later in this appendix.
4. Reattach and erase any additional storage connected to the server appliance before recovery. The hard disk drives must be attached in the same locations as before the disaster recovery process.
5. Use the backup solution to perform the recovery.
6. Reboot the server appliance.
7. Verify the restoration.

General notes regarding backup services

The following recommendations are stressed for configuring your backup service:

1. Backup systems are very sensitive to time. If possible, configure the Sun Cobalt RaQ 550 server appliance to use a network time protocol (NTP) server to set the clock on the server appliance.

On the Server Desktop UI, select **System Settings > Time** to configure the time settings or to specify an NTP server.

2. Backup systems are very sensitive to correct DNS configuration.

Ensure that your server appliance has both forward and reverse DNS lookups available to the backup server so that the backup solution functions properly.

For more information, see Appendix B, “Domain Name System”.

3. Always backup and recover the `/var`, `/etc` and `/usr/sausalito` directories together.

These directories contain both the machine configuration and the Cobalt configuration databases. Backing up and recovering these directories at different times can lead to inconsistencies between the configuration of your server appliance and the configuration reported in the Server Desktop UI.

Knox Arkeia

Tailoring the backup service

Server-side tailoring is required for Knox Arkeia. Arkeia performs backups with groups of clients called *savepacks*. When adding a Sun Cobalt RaQ 550 server appliance to a savepack on the Knox Arkeia backup server, the tree options must be modified to use a pre-backup and post-backup command.

To set these parameters, select the server appliance from the list of clients in the savepack and edit the tree options for that client.



Important: For the *hostname*, enter the host name only. Do not enter the fully qualified domain name.

1. Next to the option “command before tree”, uncheck the option “Backup tree if command fails”.
2. In the field following this option, enter:


```
hostname:/usr/local/sbin/cobalt_prebackup
```

 where *hostname* is the client name of the server appliance you are backing up.
3. Next to the option “command after tree”, check the option “Execute if tree backup fails”.
4. In the field following this option, enter:


```
hostname:/usr/local/sbin/cobalt_postbackup
```

 where *hostname* is the client name of the server appliance you are backing up.
5. Select “**All but NFS**” in the File System Allowed menu.

Files associated with Knox Arkeia tailoring

Table 1 lists the files associated with the Knox Arkeia software. These files are located on the Sun Cobalt RaQ 550 server appliance.

Table 1. Files associated with Knox Arkeia tailoring

Path and file name	Description
/usr/local/sbin/cobalt_prebackup	Script that runs before a backup to create archives of the CCE database.
/usr/local/sbin/cobalt_postbackup	Script that runs after a backup to delete the archives created by cobalt_prebackup.
/etc/rc.d/init.d/cobalt_restore	Script that runs at startup and detects whether archives of the configuration databases exist. Extant archives are recovered and have their names changed.
/var/cobalt/backups/cce.tar	Archive of the CCE database. It is created by cobalt_prebackup, deleted by cobalt_postbackup and renamed to restored.cce.tar by cobalt_restore after disaster recovery.

Backing up a server appliance with Knox Arkeia

To back up your server appliance with Knox Arkeia, you must first configure and enable the Arkeia agent on the server appliance. For more information, see “Knox Arkeia Backup Settings” on page 91.

Backups are started by using the Knox Arkeia UI. Once a backup of a server appliance has begun, the `cobalt_prebackup` script creates the `cce.tar` file in the `/var/cobalt/backups` directory if the tree options for the server appliance were configured correctly.



Important: The server appliance will not restore properly if the tree options do not execute the `prebackup` and `postbackup` commands.

When the backup has successfully completed, the script `cobalt_postbackup` removes the `cce.tar` file.

Performing disaster recovery of a server appliance with Knox Arkeia

To perform a restore with the Knox Arkeia software, you must have backed up the server appliance to an Arkeia server.

Preparing for disaster recovery

Prepare your Sun Cobalt RaQ 550 server appliance for disaster recovery by performing the following steps:

1. Perform an OS restore to wipe the hard disk drive and return the server appliance to a factory-fresh state.
2. Configure the server appliance through the Setup Wizard and return it to the network. The server appliance must be able to communicate with the backup server; otherwise, the recovery will fail.
3. If possible, configure the server appliance to use a network time protocol (NTP) server to set the clock on the server appliance.

On the Server Desktop UI, select **System Settings > Time** to configure the time settings or to specify an NTP server.

4. Select **Maintenance > Knox Arkeia** and configure the Knox Arkeia client on the server appliance.
 - **Enable Client**—Click to enable the check box Enable Client
 - **Backup Server Name**—Enter the fully qualified domain name of the Knox Arkeia backup server
 - **Port Number**—Enter the port number to which your Knox Arkeia backup server is listening. The default port number is 617
5. Click **Save**.
6. Reattach and erase any additional storage that was connected to the server appliance before the OS restore.

Performing a disaster-recovery operation

After completing the preparation steps in the previous section, the Sun Cobalt RaQ 550 server appliance is now ready to be restored.

The restoration options on the Knox Arkeia backup server should include “Files modified since backup date” and “by user ID”.

Only certain directories can be recovered during disaster recovery. Select the following directories using the Arkeia tree navigator:

```
/home
/root
.nsr
/usr
/nsr
/var
/etc
opt
```



Important: DO NOT select `/lib`, `/boot`, or `/vmlinuz.gz` or your server appliance will crash during recovery and most likely will not reboot.

When the restore process is complete, reboot the server appliance.



Important: Disaster recovery is not complete until you reboot the server appliance.

The server appliance does not reboot automatically.

After the server appliance has rebooted, ensure that the CCE and Cobalt databases were recovered. Inspect the directory `/var/cobalt/backups/` for files. If `cce.tar` exists and does not have a 'restored' prefix, then you need to run the command:

```
/etc/rc.d/init.d/cobalt_restore start
```

as the root user and reboot the server appliance again.

The Arkeia log window indicates that the following files are “busy” and that it cannot overwrite the files. This is both normal and acceptable.

```
/usr/bin/perl5.00503  
/usr/sbin/httpd  
/usr/sausalito/cced.socket  
/usr/sausalito/sbin/cced  
/usr/knox/bin/nlservd
```

Files from other running processes may also be listed.

Legato NetWorker™

Tailoring the backup service

No server-side tailoring is required for Legato NetWorker other than adding the client to the backup server.



Important: When adding a Sun Cobalt RaQ 550 server appliance to a Legato NetWorker backup server, select “UNIX® Standard Directives” when creating the server appliance client resource.

Do not select “Compression directives”. If you select “Compression directives”, the tailoring for the server appliance will not work properly.

Files associated with Legato NetWorker tailoring

Table 2 lists the files associated with the Legato NetWorker software. These files are located on the Sun Cobalt RaQ 550 server appliance.

Table 2. Files associated with Legato NetWorker

Path and file name	Description
/usr	Directives for handling the server appliance file systems.
/usr/bin/cceasm	An external Application Specific Module (ASM) for the CCE database. <i>Note:</i> External ASMs are not compatible with “Compression directives”.
/usr/sausalito/sbin/disk_restorequotas.pl	A script to synchronize the configured quotas with the filesystem

Backing up a server appliance with Legato NetWorker

To back up your server appliance with Legato NetWorker, you must first configure and enable the NetWorker agent on the server appliance. For more information, see “Legato NetWorker™ Backup Settings” on page 92.

Sun Microsystems recommends specifying the “All” saveset when using Legato NetWorker. If you must specify individual savesets for a server appliance, you must backup up the following directories together to ensure consistency:

```
/etc  
/usr/sausalito
```

Performing disaster recovery on a server appliance with Legato NetWorker

To perform a restore with the Legato NetWorker software, you must have backed up the server appliance to a NetWorker server.

Preparing for disaster recovery

Prepare your Sun Cobalt RaQ 550 server appliance for disaster recovery by performing the following steps:

1. Perform an OS restore to wipe the hard disk drive and return the server appliance to a factory-fresh state.
2. Configure the server appliance through the Setup Wizard and return it to the network. The server appliance must be able to communicate with the backup server; otherwise, the recovery will fail.
3. If possible, configure the server appliance to use a network time protocol (NTP) server to set the clock on the server appliance.

On the Server Desktop UI, select **System Settings > Time** to configure the time settings or to specify an NTP server.

4. Select **Maintenance > Legato NetWorker** and configure the Legato NetWorker client on the server appliance.
 - **Enable Client**—Click to enable the check box to enable the backup client
 - **Legato Server Hostnames**—Enter the fully qualified domain names of Legato NetWorker backup servers. Legato servers must have valid host names
 - **Service port range**—Sets the range of the system's service ports to the one specified (default range is 7937–7938)
 - **Connection Port Range**—Sets the range of the system's connection ports to the one specified (default range is 10001–10200)
5. Click **Save**.
6. Reattach and erase any additional storage that was connected to the server appliance before the OS restore.

Performing a disaster-recovery operation

After completing the preparation steps in the previous section, the Sun Cobalt RaQ 550 server appliance is now ready to be restored.



Important: The `/var` recover operation must complete before the `"/` recover operation begins.

Restore the file systems for your server appliance in the following order:

```
/var
/
/home
/vol/<additional storage devices>
```

When the restore process is complete, execute the following command:

```
/usr/sausalito/sbin/diskrestorequotaspl
```

This script sets the configured quota values for the system. When this is complete, reboot the server appliance.



Important: Disaster recovery is not complete until you reboot the server appliance.

The server appliance does not reboot automatically.

Servicing the Sun Cobalt RaQ 550 server appliance

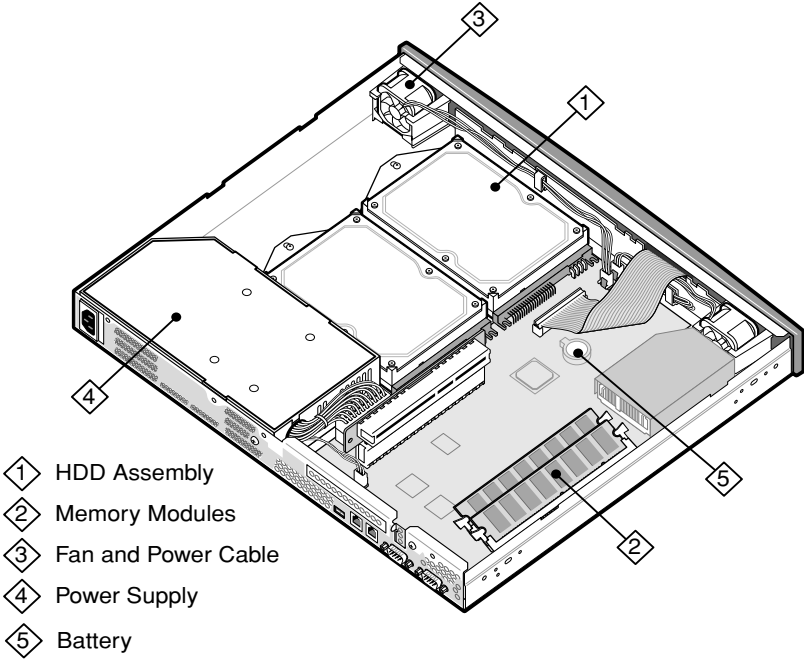
Your Sun Cobalt RaQ™ 550 server appliance can be serviced or upgraded in the field in the following areas:

- Replace the hard disk drives
- Add a memory module (DIMM)
- Replace the fan and power cable
- Replace the power supply
- Replace the CR2032 lithium CMOS backup battery

If the Sun Cobalt RaQ 550 server appliance is rack-mounted using slide rails, all components can be removed and replaced while the server appliance is in the rack. To gain access to the components, slide the server appliance out, unplug the AC power cord and remove the top cover.

The following sections provide step-by-step upgrade and replacement instructions.

Figure E-1. Components in the server appliance



Installing or removing a hard disk drive

The Sun Cobalt RaQ 550 server appliance can contain one or two hard-disk drives.

Before you replace or add a hard disk drive to the server appliance, read all of the following Notes and Warnings.



Note: If possible, replace a defective drive with another drive of the same model. If the original model of drive is not available, ensure that the replacement drive has a storage capacity that is equal to or greater than that of the drive being replaced.

Check the specifications of the replacement drive to verify that the usable memory (not the rated capacity) is equivalent to the capacity of the drive being replaced.

If you have to replace a hard disk drive, please notify Sun Cobalt Technical Support and arrange to return the drive. See “Customer Service and Technical Support” on page 5 for contact information.

If you add a drive (rather than replace an existing one), the new drive can be utilized by the Sun Cobalt RaQ 550 server appliance, but cannot be incorporated into the system’s RAID.



Warning: Do not swap disk drives from one Sun Cobalt RaQ 550 server appliance to another. Also, do not install a drive, that was previously partitioned for RAID, in a Sun Cobalt RaQ 550 server appliance as an additional (non-RAIDed) drive.

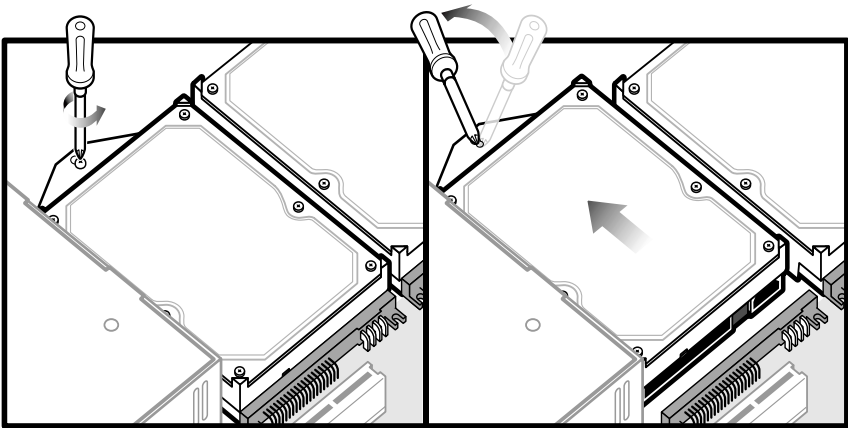
Follow these steps to remove a hard disk drive:



Caution: The chassis contains electrostatic-sensitive components. Observe proper ESD precautions when removing the top cover of the server appliance.

1. Power down and remove the Sun Cobalt RaQ 550 server appliance from the equipment rack. If it is on slide rails, slide it out of the rack.
2. Unplug the AC power cord, then remove the top cover.
3. Locate the drive.
4. Remove the drive mounting screw as shown in Figure E-2.

Figure E-2. Removing a drive



5. Insert the screwdriver in the pry point adjacent to the mounting screw boss.
6. Gently pry the drive loose from the board connectors.
7. Install a replacement drive using the reverse procedure.
8. Reinstall the top cover and return the server appliance to the equipment rack.

Installing additional memory

Before attempting to install additional memory, ensure that the DIMM to be installed is less than 0.158 inches (4.0 mm) thick. Contact Sun Cobalt Technical Support to receive a listing of approved memory vendors and the appropriate part numbers.



Caution: The chassis contains electrostatic-sensitive components. Observe ESD precautions when removing the top cover of the server appliance.

Follow these steps to install memory:

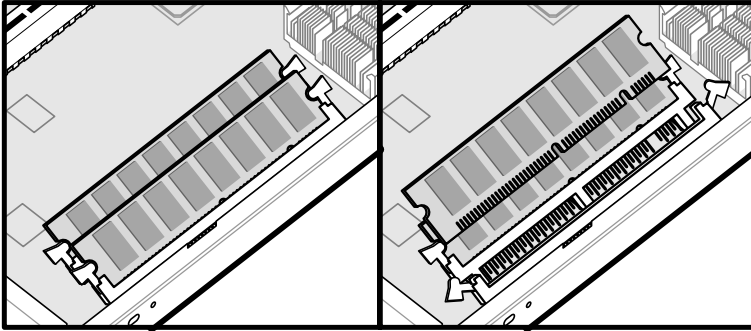
1. Power down and remove the server appliance from the equipment rack. If it is on slide rails, slide it out of the rack.
2. Unplug the AC power cord, then remove the top cover.
3. Locate the DIMM sockets as shown in Figure E-3.
4. To remove a DIMM, release the socket eject levers and withdraw the DIMM.



Caution: Observe proper ESD precautions and follow the manufacturer's instructions when handling the DIMM.

5. To install a replacement DIMM, release the socket eject levers, then press the DIMM into the socket until the levers close and engage the cutouts at each end of the DIMM. Note that the DIMM edge connector is keyed.
6. Reinstall the top cover, plug in the AC power cord and return the server appliance to the equipment rack.

Figure E-3. Removing a DIMM



Replacing the fans and power cables



Caution: The chassis contains electrostatic-sensitive components. Observe proper ESD precautions when removing the top cover of the server appliance.



Note: Before replacing the fans and power cables, contact Sun Cobalt Technical Support to receive a listing of approved vendors and the appropriate part numbers.

Replace a fan as follows:

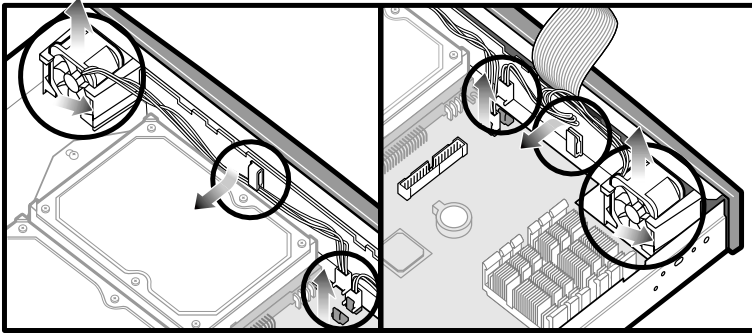
1. Login as the server administrator or site administrator and select the **Active Monitor** menu item.
2. When the “System Status - Overview” screen is displayed, go to the **Fans** entry and click on the magnifying glass icon. The “Fan Monitor” screen is displayed and indicates which fan is defective.
3. Power down and remove the server appliance from the equipment rack. If it is on slide rails, slide it out of the rack.
4. Unplug the AC power cord, then remove the top cover.

5. The fans (see Figure E-4) snap into their holders and are held by friction. Lift the fans straight up to remove them from their holders.

Note the routing of the fan wiring before removal.

6. Replace the fans using the reverse procedure.
7. Reinstall the top cover, plug in the AC power cord and return the server appliance to the equipment rack.

Figure E-4. Removing the fans and power cables



Replacing the power supply



Caution: The chassis contains electrostatic-sensitive components. Observe proper ESD precautions when removing the top cover of the server appliance.



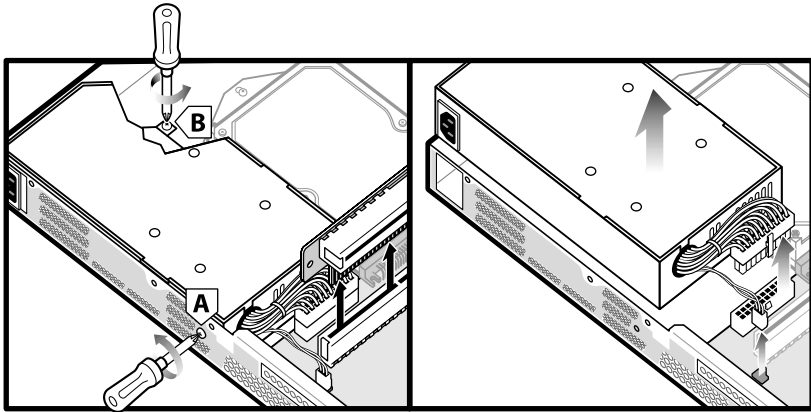
Note: Before replacing the power supply, contact Sun Cobalt Technical Support to receive a listing of approved vendors and the appropriate part numbers.

Replace the power supply as follows:

1. Power down and remove the server appliance from the equipment rack. If it is on slide rails, slide it out of the rack.
2. Unplug the AC power cord, then remove the top cover.
3. Locate the power supply (see Figure E-5).
4. Remove the PCI card riser.

5. Unfasten the two securing screws (A and B) and move the power supply toward the hard disk drive until the AC plug clears the chassis wall.
6. Release the two connectors on the motherboard and remove the power supply.
7. Replace the power supply using the reverse procedure.
8. Reinstall the top cover, plug in the AC power cord and return the server appliance to the equipment rack.

Figure E-5. Removing the power supply



Replacing the battery



Caution: The chassis contains electrostatic-sensitive components. Observe proper ESD precautions when removing the top cover of the server appliance.



Note: Before replacing the battery, contact Sun Cobalt Technical Support to receive a listing of approved vendors and the appropriate part numbers.

Replace the battery as follows:

1. Power down the server appliance and unplug the AC power cord.
2. Remove the top cover.
3. Using a small flathead screwdriver, gently pry the battery out of the battery holder (being careful not to bend the contacts).
4. Install the new battery with the + side up (you should see the + when the battery is installed).

The battery model number is CR2032 and is available in most stores that sell batteries. It is a 3V lithium battery that should last three years.

5. Dispose of the old battery correctly (do not burn or throw in the trash; see disposal instructions on battery packaging).
6. Replace the top cover of the server appliance and plug in the AC power cord.
7. Power up the server appliance, and reset the time and date settings through the browser interface.

Product Specifications

Hardware

The Sun Cobalt RaQ™ 550 server appliance has the following hardware components:

- Up to 1.2 GHz Intel Pentium III Tualatin processor
- 512 kB of L2 cache
- DIMMs (two slots). Supports total memory size from 256 MB to 2 GB. Slots accommodate 128 MB to 1 GB SDRAM DIMM modules (modules must be 168 pin, 3.3V, registered, ECC PC133). Qualified DIMM modules (256 MB, 512 MB, or 1 GB) can be purchased from Sun Cobalt.
- One or two internal Ultra ATA 100 hard drives (server is compatible with ATA 33, ATA 66, or ATA 100). Drives are direct connect (cableless).
- Two 10/100BASE-T Ethernet network interfaces (the connector labeled I on the back panel interface is the primary LAN interface and has Wake-on-LAN support)
- Dual DB9 serial port interfaces (one for console, one for UPS)
- USB 1.0 connector (solely for a printer connection)
- LCD console for easy setup and administration
- One PCI slot (64-bit, 33 MHz)
- Two system fans with RPM monitoring¹
- One power supply assembly fan with RPM monitoring¹
- CPU temperature and voltage monitoring¹
- System temperature monitoring¹
- Lithium battery voltage monitoring¹
- Support for uninterruptible power supply (UPS)

1. See “Active Monitor” on page 99

Software

The Sun Cobalt RaQ 550 server appliance has the following software features and system management capabilities:

Features

- Linux 2.4 multitasking operating system
- High-Performance Journaling Filesystem
- Apache 1.3.20 Web server, HTTP/1.1 compliant
- Virtual hosting services: name-based and IP-based
- Common Gateway Interface (CGI) support
- Support for Sun Chili!Soft Active Server Pages (ASP)
- PHP 4 support
- Support for Server Side Includes (SSI)
- Perl scripting
- JavaServer Pages™ (JSP™) and servlet support
- Email protocol support including: Simple Mail Transfer Protocol (SMTP), Internet Message Access Protocol (IMAP4), Post Office Protocol (POP3), Authenticated Post Office Protocol (APOP)
- File Transfer Protocol (FTP) and anonymous FTP access
- Shell access using Telnet or SSH
- Domain Name System (DNS) server
- 128-bit Secure Socket Layer (SSL) encryption
- FrontPage 2002 server extensions
- NTP client support
- Sun Cobalt™ Bandwidth Management software
- Support for Java™ runtime environment version 1.3 and JDK(TM) software from Sun Microsystems, Inc.

- Code development environment
- Legato NetWorker client and Knox Arkeia support
- Security enhancements:
 - PAM/shadow passwords
 - StackGuard buffer overflow protection of major services (for example, Web, email, FTP servers)
- Enhanced power up options:
 - Wake-on-LAN support
 - Support for powering on automatically after a power failure
- UPS support

System management

- SSL support for secure administration
- Port scan detection support
- Simple Network Management Protocol (SNMP) management support
- Browser-based Setup Wizard
- Browser-based server and site administration
- Browser-based software upgrade
- Browser-based performance and usage reporting
- Online Active Assist real-time help
- Active Monitor maintenance agents
- Advanced management using telnet or SSH
- Delegated server management

Physical data

The Sun Cobalt RaQ 550 server appliance has the following physical characteristics.

- Dimensions: 16.83 in. x 14.0 in. x 1.75 in. (42.75 cm x 35.56 cm x 4.45 cm)
- Weight with one hard drive: 11.8 lbs. (5.37 kg)
- Weight with two hard drives: 13 lbs. (5.90 kg)
- Power consumption: 90W (typical)
- DC voltages:
 - +5VSB $\pm 5\%$
 - +5V $\pm 5\%$
 - +12V $\pm 5\%$
 - -12V $\pm 10\%$
 - +3.3V $\pm 5\%$
- Power requirement for the PCI slot:
 - 5V @ 1A
 - +12V @ 0.5A
 - -12V @ 0.1A
- Input line voltage:
 - 90–135 VAC, 50–60 Hz
 - 180–260 VAC, 50–60 Hz
- Enclosure operating environment:
 - 1.00GHz CPU 39°F to 90°F (5° C to 32° C)
 - 1.26GHz CPU 39° F to 95°F (5° C to 35° C)
 - 10% to 80% humidity (non-condensing)
- Enclosure non-operating environment:
 - 14°F to 122°F (-10°C to 50°C)
 - 5% to 93% humidity (non-condensing)

- CPU maximum operating temperature:
156°F (69°C)
5% to 93% humidity (non-condensing)
- Lithium battery minimum voltage: 2.8V
- Light-emitting diodes (LEDs):
 - Primary Ethernet interface (I) network activity (green)
 - Secondary Ethernet interface (II) network activity (green)
 - Primary Ethernet interface (I) connection (green)
 - Secondary Ethernet interface (II) connection (green)
 - Disk 1 activity (green)
 - Disk 2 activity (green)
 - World-Wide Web activity (green)
 - System Fault (amber)

Regulatory approvals

- CISPR 22B
- VCCI-B
- UL
- C-UL
- TUV
- CE
- Austel
- BSMI
- GOST R

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 by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.engelschall.com/sw/mod_ssl/).”

4. The name “mod_ssl” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact rse@engelschall.com.
5. Products derived from this software may not be called “mod_ssl” nor may “mod_ssl” appear in their names without prior written permission of Ralf S. Engelschall.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

“This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.engelschall.com/sw/mod_ssl/).”

THIS SOFTWARE IS PROVIDED BY RALF S. ENGELSCHALL “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL RALF S. ENGELSCHALL OR HIS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Glossary

10/100BASE-TX

An Ethernet connection over twisted-pair cables with a throughput of 10 Mb/s or 100 Mb/s.

10BASE-T

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. 10BASE-T (part of the IEEE 802.3 specification) has a distance limit of approximately 328 feet (100 meters) per segment.

100BASE-TX

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. The Ethernet standard specifies cable lengths of from 1 to 100 meters. To guarantee proper signal timing, a 100BASE-TX segment cannot exceed 328 feet (100 meters) in length. 100BASE-TX is based on the IEEE 802.3 standard.

APOP

See *authenticated post office protocol (APOP)*.

Authenticated Post Office Protocol (APOP)

APOP prevents your popmail password from travelling over the network, instead using it to encrypt a session password which can be checked against one encrypted by the popmail server also using your password

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.sun.com` locates an Internet address for the domain name “sun.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 `sun.com` into a numeric IP address (`192.168.10.10`) 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)*.

ESMTP

See *Extended Simple Mail Transfer Protocol (ESMTP)*.

Ethernet

The most widely used technology for local area networks (LANs). Standard Ethernet runs at 10 Mb/s, 100 Mb/s or 1000 Mb/s. It balances speed, price, ease of installation and availability.

ETRN

ETRN (Extended Turn) is an extension to the Simple Mail Transfer Protocol (SMTP) that allows an SMTP server to send a request to another SMTP server to send any email messages it has. Typically, SMTP is used with two other protocols, Post Office Protocol 3 (POP3) or Internet Message Access Protocol (IMAP), to request messages from a server; SMTP by itself cannot request mail to be sent.

ETRN is designed for use by anyone who is traveling and wants to access their email. ETRN can only be used with Internet service providers (ISPs) that support ETRN.

Extended Simple Mail Transfer Protocol (ESMTP)

The Extended Simple Mail Transfer Protocol specifies extensions to the original SMTP protocol for sending email that supports graphics, audio and video files, and text in various national languages. ESMTP provides the capability for a client email program to inquire of a server email program about which capabilities it supports and then communicate accordingly.

File sharing

The public or private sharing of computer data or space in a network with various levels of access privileges.

File Transfer Protocol (FTP)

A standard Internet protocol and a way to exchange files between computers connected to the Internet. FTP is an application protocol that uses TCP/IP protocols. FTP is commonly used to transfer Web page files from the computer that was used to create the files to the computer that acts as the server for these files. It is also used to download programs and other files to your computer from other servers.

Using FTP, you can update—delete, rename, move and copy—files at a server. You need to log on to an FTP server. However, publicly available files are easily accessed using anonymous FTP.

FTP

See *File Transfer Protocol (FTP)*.

Gateway

A network device that acts as an entrance to another network. A gateway can also be any device that passes packets from one network to another network across the Internet.

HTML

See *HyperText Markup Language (HTML)*.

HTTP

See *HyperText Transfer Protocol (HTTP)*.

HyperText Markup Language (HTML)

A set of “markup” symbols or tags inserted in a text file intended for display on a World Wide Web browser. The markup tags tell the Web browser how to display a Web page’s content, words and images. HTML is a subset of Standardized Generalized Markup Language (SGML).

HyperText Transfer Protocol (HTTP)

A set of rules for exchanging files (text, graphic images, sound, video and other multimedia files) on the World Wide Web.

ICANN

See *Internet Corporation for Assigned Names and Numbers (ICANN)*.

IEEE 802.3

IEEE local area network (LAN) protocol that specifies an implementation of the physical layer and the media access control (MAC) sublayer of the data link layer. IEEE 802.3 uses CSMA/CD access at a variety of speeds over a variety of physical media. Extensions to the IEEE 802.3 standard specify implementations for Fast Ethernet. Physical variations of the original IEEE 802.3 specification include 10Base2, 10Base5, 10BaseF, 10BaseT and 10Broad36. Physical variations for Fast Ethernet include 100BaseT, 100BaseT4 and 100BaseX.

IMAP

See *Internet Message Access Protocol (IMAP)*.

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 252 and “Simple Mail Transfer Protocol (SMTP)” on page 255.

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.

Point-to-Point Protocol (PPP)

A protocol for communication between two computers using a serial interface, typically a personal computer connected by telephone line to a server. For example, your Internet server provider may provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet and forward your requested Internet responses back to you. PPP uses the Internet protocol (and is designed to handle others).

PPP is a full-duplex protocol that can be used on various physical media, including twisted pair, fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control for packet encapsulation. PPP can handle synchronous as well as asynchronous communication.

Point-to-Point Protocol over Ethernet (PPPoE)

A specification for connecting multiple computer users on an ethernet to a remote site through common customer-premises equipment such as a modem and similar devices. PPPoE can be used to allow an office or building full of users share a common digital subscriber line (DSL), cable modem or wireless connection to the Internet. PPPoE combines the Point-to-Point Protocol (PPP), commonly used in dial-up connections, with the ethernet protocol, which supports multiple users in a local area network (LAN). PPP information is encapsulated within an Ethernet frame.

POP3

See *Post Office Protocol (POP3)*.

Post Office Protocol 3 (POP3)

Post Office Protocol (POP) is a standard protocol for receiving email. POP is a client/server protocol in which email is received and held for you by your Internet server. When you read your mail, all of it is immediately downloaded to your computer and no longer maintained on the server. 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.

See also “Internet Message Access Protocol (IMAP)” on page 248 and “Simple Mail Transfer Protocol (SMTP)” on page 255.

PPP

See *Point-to-Point Protocol*.

PPPoE

See *Point-to-Point Protocol over Ethernet*.

RAID

See *Redundant Array of Independent Disks (RAID)*

Redundant Array of Independent Disks (RAID)

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

There are a variety of different types and implementations of RAID, each with its own advantages and disadvantages. RAID Level 1 (RAID-1), also known as disk mirroring, consists of at least two drives that duplicate the storage of data.

Although RAID can protect against disk failure, it does not protect against operator and administrator (human) error, or against loss due to programming bugs.

RAID can be implemented in hardware or in software. Hardware RAID is always a “disk controller”, that is, a device to which one can cable up the disk drives. Software RAID is a set of kernel modules, together with management utilities that implement RAID purely in software, and require no extraordinary hardware.

Root name server

On the Internet, the root name server system is the manner in which an authoritative master list of all top-level domain names (such as .com, .net, .org and individual country codes) is maintained and made available.

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 248 and “Post Office Protocol 3 (POP3)” on page 252.

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.

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.

USB

Universal Serial Bus. A personal computer external bus standard which can support up to 127 peripheral devices in a daisy chain configuration, can support plug-and-play (hot plugging), and has a total bandwidth of 1.5 megabytes per second. It uses inexpensive cable, which can be up to 5 meters long.

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.

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)*.