Managing Routers Using the HTTP Server

BayRS Version 13.10
Site Manager Software Version 7.10

Part No. 300019-B Rev. 00
November 1998

Bay Networks *Where Information Flows.*™

Bay Networks Where Information Flows™

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH BAY NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License Grant. Bay Networks, Inc. ("Bay Networks") grants the end user of the Software ("Licensee") a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Bay Networks Agent software or other Bay Networks software products. Bay Networks Agent software or other Bay Networks software products are licensed for use under the terms of the applicable Bay Networks, Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Bay Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Bay Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Bay Networks' and its licensors' confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Bay Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee's facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Bay Networks warrants each item of Software, as delivered by Bay Networks and properly installed and operated on Bay Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Bay Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Bay Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Bay Networks will replace defective media at no charge if it is returned to Bay Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Bay Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Bay Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Bay Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL BAY NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR

PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF BAY NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF BAY NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO BAY NETWORKS FOR THE SOFTWARE LICENSE.

5. Government Licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of Software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Bay Networks of any such intended examination of the Software and may procure support and assistance from Bay Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Bay Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Bay Networks copyright; those restrictions relating to use and disclosure of Bay Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Bay Networks the Software, user manuals, and all copies. Bay Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and Re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Bay Networks, Inc., 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN BAY NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST BAY NETWORKS UNLESS BAY NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Preface

This guide describes how to configure and use the Bay Networks® HTTP Server, an embedded Web-based router management tool included with the Bay Networks router operating system software and accessible from any standard Web browser. Using HTTP Server software, you can monitor network devices, viewing summary, fault, and statistical information on a device-by-device basis.

You can use the Bay Command Console (BCC™) or Site Manager to configure the HTTP Server software on a router. In this guide, you will find configuration instructions using both the BCC and Site Manager.

Before You Begin

Before using this guide, you must complete the following procedures. For a new router:

- Install the router (see the installation guide that came with your router).
- Connect the router to the network and create a pilot configuration file (see *Quick-Starting Routers*).
- Configure IP on the router (see *Configuring IP Services*).

Make sure that you are running the latest version of Bay Networks BayRS™ and Site Manager software. For information about upgrading BayRS and Site Manager, see the upgrading guide for your version of BayRS.

Text Conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is: **ping <***ip_address***>**, you enter: **ping 192.32.10.12**
bold text	Indicates command names and options and text that you need to enter. Example: Enter **show ip** {**alerts** | **routes**}. Example: Use the **dinfo** command.
braces ({})	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is: **show ip** {**alerts** | **routes**}, you must enter either: **show ip alerts** or **show ip routes**, but not both.
brackets ([ ])	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is: **show ip interfaces** [**-alerts**], you can enter either: **show ip interfaces** or **show ip interfaces -alerts**.
ellipsis points (. . .)	Indicate that you repeat the last element of the command as needed. Example: If the command syntax is: **ethernet/2/1** [**<***parameter***> <***value***>**] **. . .** , you enter **ethernet/2/1** and as many parameter-value pairs as needed.

italic text	Indicates file and directory names, new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is: **show at <***valid_route***>** *valid_route* is one variable and you substitute one value for it.
`screen text`	Indicates system output, for example, prompts and system messages. Example: `Set Bay Networks Trap Monitor Filters`
separator (>)	Shows menu paths. Example: Protocols > IP identifies the IP option on the Protocols menu.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is: **show ip** {**alerts** | **routes**}, you enter either: **show ip alerts** or **show ip routes**, but not both.

Acronyms

ARP	Address Resolution Protocol
BootP	Bootstrap Protocol
FDDI	Fiber Distributed Data Interface
FTP	File Transfer Protocol
HSSI	High-Speed Sserial Interface
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message protocol
IP	Internet Protocol
IPX	Internet Packet Exchange
MAC	media access control
RIP	Routing Information Protocol
SAP	Service Advertising Protocol
SMDS	Switched Multimegabit Data Service
SNMP	Simple Network Management Protocol
TCP	Transaction Control Protocol

Bay Networks Technical Publications

You can now print Bay Networks technical manuals and release notes free, directly from the Internet. Go to *support.baynetworks.com/library/tpubs/*. Find the Bay Networks product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Using Adobe Acrobat Reader, you can open the manuals and release notes, search for the sections you need, and print them on most standard printers. You can download Acrobat Reader free from the Adobe Systems Web site, *www.adobe.com*.

You can purchase Bay Networks documentation sets, CDs, and selected technical publications through the Bay Networks Collateral Catalog. The catalog is located on the World Wide Web at *support.baynetworks.com/catalog.html* and is divided into sections arranged alphabetically:

- The “CD ROMs” section lists available CDs.
- The “Guides/Books” section lists books on technical topics.
- The “Technical Manuals” section lists available printed documentation sets.

Make a note of the part numbers and prices of the items that you want to order. Use the “Marketing Collateral Catalog description” link to place an order and to print the order form.

How to Get Help

For product assistance, support contracts, or information about educational services, go to the following URL:

http://www.baynetworks.com/corporate/contacts/

Or telephone the Bay Networks Technical Solutions Center at:

800-2LANWAN

Chapter 1
Starting and Configuring the HTTP Server

The Bay Networks HTTP Server is an embedded Web-based router management tool included with the Bay Networks router operating system software and accessible from any standard Web browser. Using HTTP Server software, you can monitor network devices, viewing summary, fault, and statistical information on a device-by-device basis.

Before you can use the HTTP Server to monitor a router, you must configure and enable the HTTP Server software on the router using the Quick-Start installation script *install.bat*, the Bay Command Console (BCC™), or Site Manager.

Go to "Starting and Configuring the HTTP Server."

Browser Requirements

Your Web browser must support frames, Java applets, and cascading style sheets; for example, Netscape 4.0 or higher and Microsoft® Internet Explorer® 4.0 or higher. If you have changed the default settings for these browsers, you must ensure that Java is enabled. If you configure digest authentication, your browser must be enabled for this capability; otherwise, authentication reverts to basic.

Caution: Internet Explorer lets you store your browser password. For security reasons, it is wise *not* to store your password.

Go to "Starting and Configuring the HTTP Server."

Starting the HTTP Server Using *install.bat*

A new router comes with a flash memory card containing the software image for the router, two configuration files (*config* and *ti.cfg*), and the Quick-Start script *install.bat*.

The Quick-Start installation script creates an initial IP network interface on the router, so that your router can communicate with the configuration workstation from which you will manage the router. The *install.bat* script prompts you to enter the network information that dynamically configures the initial IP interface.

As the following example shows, the script asks whether you want to enable HTTP. Answer yes to this question. (The default is no.)

```
Step 7. Enable HTTP

Enable the HTTP (Web) Server
----------------------------

Do you want to enable the HTTP (Web) server? (y/n)[n]: y


HTTP server enabled.
```

Note: For complete instructions on running the *install.bat* script and verifying that the installation is successful, see *Quick-Starting Routers*.

When you enable the HTTP Server during the Quick-Start procedure, you can use the HTTP Server with its default configuration settings after completing the *install.bat* procedure. For information on modifying the default HTTP Server settings, see Customizing HTTP Parameters.

After you run the *install.bat* script, you can install Site Manager software, as described in *Quick-Starting Routers*.

Go to "Starting and Configuring the HTTP Server."

Starting the HTTP Server Using the BCC or Site Manager

If you did not use the Quick-Start procedure to start the HTTP Server, you can start it using the BCC or Site Manager. When you complete this procedure, the HTTP Server software is configured on the router. Before you start the HTTP Server, verify that you have configured IP on an interface.

You can start the HTTP Server using default values for all parameters. For information on modifying the default HTTP Server settings, see Customizing HTTP Parameters.

Using the BCC

Adding the HTTP Server to a router automatically loads TCP on all slots. To add the HTTP Server to a router, navigate to the box prompt and enter:

http

For example, the following command adds HTTP Server to a router:

```
box# http
http#
```

Go to "Starting and Configuring the HTTP Server."

Using Site Manager

You can configure HTTP Server software in any Configuration Manager mode. To start HTTP Server software, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Global Protocols**.	The Global Protocols menu opens.
3. Choose **TCP**.	The TCP menu opens.
4. Choose **Create TCP**.	You return to the Configuration Manager window.
5. Choose **Protocols**.	The Protocols menu opens.
6. Choose **Global Protocols**.	The Global Protocols menu opens.
7. Choose **HTTP**.	The HTTP menu opens.
8. Choose **Create HTTP**.	You return to the Configuration Manager window.

Go to "Starting and Configuring the HTTP Server."

Setting HTTP Server Security

The HTTP Server allows access to device information from anywhere in the network. To protect your network information, you can implement security controls. The HTTP Server offers access control through: user name/password security, basic access or digest authentication, and network address filtering.

User Name/Password Security Concepts

The HTTP Server controls access to network device information by grouping that information into collections, called *realms,* that share the same security attributes. The HTTP Server defines two security realms on the router: User and Manager. These are the same as the login names for the Technician Interface. Similarly, a user name/password authorization mechanism controls access to each realm.

- User access privileges let you view information.
- Manager access privileges grant complete access to the router, letting you, for example, enable and disable an interface.

Before allowing any Manager-level operations, however, the HTTP Server requires that the system administrator set a nonnull Manager password. If the system administrator does not set a User password, the HTTP Server accepts an empty (null) string as the password. Generally, the system administrator sets passwords using Technician Interface commands, just as for console access through the Technician Interface.

If you have User privileges and attempt to access information requiring Manager privileges (or, if you attempt to use the Manager login with a null password), the HTTP Server prompts you for the Manager password. If you do not provide the appropriate password, an error message appears, and you cannot perform that operation. You control the level of access authentication protection when you configure the Authentication parameter.

For specific information about how to set user names and passwords, see *Using Technician Interface Software*. For information about securing a router as part of the Quick-Start procedure, see *Quick-Starting Routers*.

Basic Access Authentication

In *basic access authentication*, the user name and password are passed over the network as clear text. While this serves to verify the identity of the user, the information is vulnerable to anyone with a sniffer or similar device.

Digest Authentication

Digest authentication, based on RFC 2069, uses an encrypted password to verify a user's identity. Like basic access authentication, digest uses a challenge-response model. To use digest authentication, you must configure the HTTP Server Authentication parameter as digest and your browser must be capable of supporting digest authentication. If your browser lacks this capability, the HTTP Server reverts to basic authentication.

Network Address Filtering

For additional security, you can implement IP access control filters when you configure IP on the router. These filters further restrict access to the router, limiting access to specific IP addresses or IP address ranges.

You must also ensure that IP is appropriately configured to support HTTP. To do this, you must ensure that:

- The configuration for the IP service also has HTTP configured.
- The appropriate access policy filters are configured for HTTP.

Specify these requirements as part of the IP configuration process, using the BCC. For additional information about IP access control filters and how to configure them, see *Configuring IP Utilities*. For general instructions about using the BCC, see *Using the Bay Command Console (BCC)*.

Using a Domain Name Instead of an IP Address

By specifying the Domain Name parameter, you let the server be accessible by a domain name, rather than by IP address. The Domain Name parameter must be set to the domain name that a DNS lookup would return for the router. The name can consist of any valid string of characters that constitute a domain name.

Accept the default value, no domain name, to indicate that the server is accessible only by the IP address; or specify a domain name to use instead of the IP address.

Go to "Starting and Configuring the HTTP Server."

Customizing HTTP Parameters

Adding the HTTP Server to a router automatically enables HTTP on the router using port 80, sets access authentication to basic, and uses the IP address to access the router. You can change these settings using either the BCC or Site Manager.

Using the BCC

To change these parameter settings, first navigate to the http prompt.

To disable http on the router, enter:
disable

For example:
`http#` **disable**

To change the port number, enter:
port <*port_number*>
For example:

`http#` **port 81**

To specify access authentication level, enter:
digest or **basic**

For example, the following command configures digest authentication:
`box#` **http**
`http#` **digest**
`http#`

To specify the use of a domain name for the router, enter:
domain-name <*domain_name*>

For example, the following command allows the use of the domain name, “myrouter”:
`http#` **domain-name myrouter**

Go to “Starting and Configuring the HTTP Server.”

Using Site Manager

To configure or change the HTTP Server parameters, first create HTTP on the router, then complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols > Global Protocols > HTTP > Global**.	The Edit HTTP Global Parameters window opens.
2. Set the **Enable/Disable** parameter to **Enabled** to enable the HTTP Server or to **Disabled** to disable the HTTP Server.	
3. Specify the **Port** number on which you enabled the HTTP Server.	
4. Set the **Authentication** parameter to **Basic** or **Digest**.	
5. Specify the **Domain Name** to use for the router. To use the IP address instead of a domain name, leave this parameter value blank.	
6. Click on **OK**.	You return to the Configuration Manager window.

Go to "Starting and Configuring the HTTP Server."

Chapter 2
HTTP Server Concepts

HTTP Server software lets you access device information from anywhere in the network using any standard Web browser that conforms to HTTP and HTML specifications. The HTTP Server is part of the router operating system for all Bay Networks non-VME-based GAME routers. This chapter provides an overview of the HTTP Server.

To obtain Web-accessible data, you must configure the HTTP Server software on the router. Chapter 1, "Starting and Configuring the HTTP Server," summarizes the configuration procedure.

What the HTTP Server Does

The HTTP Server is a graphical user interface (GUI) that lets you view real-time device summaries, events, alerts, and statistics. The HTTP Server graphically displays information similar to (and a superset of) the text-only information available through the BCC **show**, **enable**, and **disable** commands. Through this point-and-click interface, you also have direct access to online documentation and Bay Networks Technical Support.

The information that you gather through the HTTP Server interface can help you monitor your network's performance on a device-by-device basis. You can see, for example, where congestion is occurring or where transmission or reception problems exist. For detailed information about interpreting this information, refer to *Troubleshooting Routers* and *Event Messages for Routers*.

You see a multiframe window when you specify a device in your browser's location field or when you click on the Summary folder icon, then on the Info icon in the navigational frame.

- Banner -- The top frame shows the Bay Networks logo and the device type. The banner also identifies the device by name, specifies its physical location and IP address, and lists the name of the contact person responsible for that device. The IP address is a link that you can click on to establish a Telnet connection to the device.
- Navigational frame -- The frame on the left contains links to each monitored function. Initially, these links are all folders. The folders (and the documents they contain) in the navigational frame are active links to device information.
- Display frame -- The large frame on the lower right side displays the retrieved web data.

Navigating the HTTP Server Interface

The navigational frame contains the following expandable folders:

- Summary -- System information, hardware status, PROM information, software image information, system resource information, and system task information
- Fault -- Circuit alerts and the event log
- Statistics -- Services, ports, and protocols
- Support -- Help, release notes, technical manuals, and customer support links

Click on each folder in turn to display the information for the device you are monitoring.

- To show the types of data a folder contains, click on the folder icon. The folder opens, revealing document icons representing the types of data within that folder.
- To view a specific data type within a folder, click on its document icon.
- To close (that is, collapse) a folder's contents, click again on the folder icon.

Chapter 3
Monitoring Routers Using the HTTP Server

This chapter describes how to use the HTTP Server to monitor the operation of individual routers on your network. For specific descriptions of how to use the information from the HTTP (Web) Server to troubleshoot the devices in your network, refer to *Troubleshooting Routers*.

Getting Help

For this information	Click on Support, then on
HTTP Server interface help	Help icon
Release Notes	Release Notes icon
Bay Networks documentation	Documentation icon
Bay Networks technical support	Bay Networks Technical Solutions Center icon

After opening one of these links, choose File > Close to return to the HTTP Server page on the Web browser. Clicking on File > Exit shuts down the browser. The Back button may not be available on linked pages.

Go to "Monitoring Routers Using the HTTP Server."

Specifying a Router to Monitor

1. **Start your Web browser.**
2. **In the Location field, enter:**

   http://<*router_IP_address***>**

router_IP_address is an IP address on the device that you want to monitor, for example:
http://192.168.12.54

The browser displays a summary window for the specified device.

Go to "Monitoring Routers Using the HTTP Server."

Viewing Overall System Status

Use the summary information to get an overall picture of the operational state of the router. The summary provides hardware and software information including this router's configuration and its internal resource usage. To see the types of summary information available, click on the Summary folder icon in the navigational frame.

The following table lists the icons within the Summary folder and the information that each displays when you click on it.

Icon	Shows information for	Displayed summary information
Info	System	• Device name -- the mnemonic name that the system administrator assigns • Location -- the location, as defined by the system administrator • Contact person responsible for that device, as defined by the system administrator • Up time -- the time elapsed since the last device reset • MIB version -- the version number of the management information base (MIB) for the router software • Software version -- the version number and creation date and time of the router software image
Hardware	Specific device	• Model name and serial number • Type, revision, and serial number of the processor and link module in each slot.
PROMs	PROM modules in the device	For the Boot PROM and for the Diagnostic PROM in that slot: • Revision number • Date and time of installation
Software	Software image on the specified device	For each router slot: • Name of the software image file • Source of that image • Date and time the image was created • Name of the configuration file
Resources	System resources on the specified hardware device	For each router slot, usage data for: • CPU • Memory • Buffers
Tasks	System tasks on the specified hardware device	For each active task: • Name of each task • Usage data for the CPU, memory, and buffers • Slots on which the task is running

For detailed information about interpreting the information obtained through this interface, refer to *Troubleshooting Routers*.

Chapter 4
Monitoring Circuit Alerts and Events

With the HTTP Server, you can view the events and alerts generated by the entities on the router. When you click on the Fault icon, the folder opens and displays two document icons. Click on these document icons to view:

- All circuit alerts on the router
- All, or a selection of, event log messages

You must first have configured and enabled the HTTP Server on your router, as described in "Starting and Configuring the HTTP Server." For a detailed description of how to isolate and correct problems with a specific device, refer to *Troubleshooting Routers*.

Fault Icon

Clicking on Fault in the navigational frame reveals two additional choices. You can view:

- All circuit alerts on the router
- All, or a selection of, event log messages

Go to "Monitoring Circuit Alerts and Events."

Displaying Circuit Alerts

A *circuit alert* indicates a condition, such as a port/interface that has been brought down unexpectedly, that requires your immediate attention. To view any exceptional status conditions for any interface on the router, click on Fault > Circuit Alert in the navigational frame.

For each index item, the circuit alerts display shows:

- Index number
- Circuit name
- Administrative state
- Operational state
- Type
- MAC address
- Maximum transmission unit (MTU)
- Line speed

Go to "Monitoring Circuit Alerts and Events."

Viewing the Event Log

An *event* is something that happens to the operating status of a router. The router stores each event as a single entry in a memory-resident log file. The event log for a router is the composite of all the events that occur for all the processors in the router.

An event message provides a brief description of an event, along with the event code associated with that event. Use the event code to look up the meaning of the message and what you must do about it in the events database.

To view the events for a router, click on Fault > Events in the navigational frame.

Filtering What the Event Log Shows
Interpreting Event Messages

Go to Monitoring Circuit Alerts and Events.

Filtering What the Event Log Shows

By default, the event log display shows Fault, Warning, and Info event messages.

- To show other event messages, click on the check boxes to select the appropriate Event Message Severity Levels.
- To restrict the display to one or more specific slots or entities and to show only events that happen after a specific date and time, fill in the fields in this frame, separating individual entries with spaces.

Note: All entity names are case-sensitive. For a list of entity names, refer to the events database.

Go to "Monitoring Circuit Alerts and Events."

Interpreting Event Messages

Event Messages for Routers provides detailed information about interpreting event messages and taking appropriate action. Most messages document routine occurrences that do not require you to do anything. The following table lists and briefly describes the severity levels.

Event Message Severity Levels

Severity	Description
Fault	Major service disruption, usually caused by a configuration, network, or hardware problem. The entities involved keep restarting until the problem is resolved either by the router itself or by you.
Warning	Service acted in an unexpected manner.
Info	Routine event. Usually, no action is required.
Trace	Detailed history of everything that happens on the router. Because of the amount of information that the Trace function records, Bay Networks recommends viewing this type of message only when diagnosing specific network problems.
Debug	Information that Bay Networks Customer Support uses. With few exceptions, these messages do not appear in *Event Messages for Routers.*

Return to Monitoring Circuit Alerts and Events.

Chapter 5
Viewing Router Services Statistics

Examining the router's statistics along with the event log can give you a picture of how well your router is working. When you click on Statistics in the navigational frame, the folder opens to show the Services, Ports, and Protocols folders, each containing subordinate links. This chapter shows the Services statistics. For Port statistics, go to Chapter 6, "Viewing Router Port Statistics," and for Protocol statistics, go to Chapter 7, "Viewing Router Protocol Statistics."

Note: This guide presents the details of the HTTP statistics. Detailed descriptions of statistics for the other services are in the guides for each service.

Router Services Statistics

You can display router services statistics either through the Web interface, by clicking on Statistics > Services in the navigational frame, or by using the Site Manager Statistics Manager. For information on using the Statistics Manager, see Using the Statistics Manager to View HTTP Server Statistics.

Using the Web interface, clicking on Statistics > Services displays links to the statistics for each service.

To see these statistics	Use this path
TFTP	Statistics > Services > TFTP
TCP	Statistics > Services > TCP
FTP	Statistics > Services > FTP
Telnet	Statistics > Services > Telnet
BootP	Statistics > Services > Bootp This reveals several subordinate links: Traffic, Interfaces, Clients, Preferred Srv (Servers), and Relay Agents.
• Traffic	Statistics > Services > Bootp > Traffic
• Interfaces	Statistics > Services > Bootp > Interfaces
• Clients	Statistics > Services > Bootp > Clients
• Preferred servers	Statistics > Services > Bootp > Preferred Srv
• Relay agents	Statistics > Services > Bootp > Relay Agents
SNMP	Statistics > Services > SNMP This reveals the following subordinate links: Counters, Communities, Entity Traps, and Exceptions.
• Counters	Statistics > Services > SNMP > Counters
• Communities	Statistics > Services > SNMP > Communities*
• Entity traps	Statistics > Services > SNMP > Entity Traps
• Exceptions	Statistics > Services > SNMP > Exceptions
HTTP	Statistics > Services > HTTP This reveals the following subordinate links: Configuration, Counters, Requests, and Responses.
• Configuration	Statistics > Services > HTTP > Configuration
• Counters	Statistics > Services > HTTP > Counters
• Requests	Statistics > Services > HTTP > Requests
• Responses	Statistics > Services > HTTP > Responses

* You must have Manager-level access privileges to view the statistics for SNMP communities. If you logged in with user-level privileges, HTTP prompts you to enter the manager login name and password.

Go to “Viewing Router Services Statistics”.

Using the HTTP Server to View HTTP Statistics

You can display HTTP Server statistics either through the Web interface, by clicking on Statistics > Services > HTTP in the navigational frame, or by using the Site Manager Statistics Manager.

HTTP Configuration Statistics

HTTP configuration statistics provide the following information:

HTTP Statistic	Meaning
State	Whether the server is enabled or disabled
Status	Whether the server is currently up, down, initializing, or not present
Port	The port number on which this server listens to requests
Authentication	The level of access authentication security in use
Domain Name	The domain name, if any, that can be used to access this router

HTTP Counters

HTTP counters provide the following information:

HTTP Statistic	Meaning
Total Requests Received	The total number of requests that this entity received
Total Request Errors	The total number of request errors that this entity detected (as server)
Total Request Discards	The total number of requests that this entity discarded (as server)
Total Responses	The total number of responses that this entity generated or received
Total In Unknowns	The total number of unknown messages that this entity received

Total Rx Octets	The total number of bytes that this entity received
Total Tx Octets	The total number of bytes that this entity transmitted
Total Time Outs	The total number of timeouts for this entity
Start Time	The date and time that the HTTP services were enabled

HTTP Request Statistics

HTTP request statistics provide the following information:

HTTP Statistic	**Meaning**
Method	The HTTP standard request method to which these statistics apply
Total In	The number of requests of this type that this entity received
In Last Time	The date and time the last request was received

HTTP Response Statistics

HTTP response statistics include:

HTTP Statistic	**Meaning**
Status	An HTTP standard code and message description indicating the status of the response
Total Out	The number of times this response was generated
Out Last Time	The date and time the most recent response was sent

Go to “Viewing Router Services Statistics”.

Using the Statistics Manager to View HTTP Server Statistics

To use Site Manager Statistics Manager tool to view statistical information for the HTTP Server, click on Statistics on the toolbar or, from the Site Manager menu, choose Tools > Statistics Manager. Select the router that you want to monitor. The Statistics Manager window appears, showing the device IP address and, for each circuit on that device, showing the slot, connector, type, and protocols.

Selecting the Windows to Display

Use the Screen Manager tool to select the windows to display. In the Statistics Manager window, click on Tools > Screen Manager. Add the HTTP windows to the list of those to display, then exit the Screen Manager.

Starting the Statistics Launch Facility

In the Statistics Manager window, click on Tools > Launch Facility to display the Statistics Launch Facility window, which lets you choose the type of statistical information that you want to view for this device.

Click on the line that indicates the type of information you want to display, then click on Launch. To return to this window, click on File > Exit in the resulting window.

Viewing HTTP Statistics

Each statistical window shows the window name (*name.dat*), window description, SNMP agent IP address, and number of elements in the display.

To see these statistics	Choose this option	What the window shows for each element
HTTP requests	*httpreq.dat*	HTTP request statistics: • Methods • Total requests (Total In) for each method
HTTP responses	*httpresp.dat*	HTTP response statistics: • Status • Number of times the server responds for each status type (TotalOut)

To see these statistics	Choose this option	What the window shows for each element
HTTP server configuration	*httpsrv.dat*	HTTP server configuration statistics: • State (enabled or disabled) • Operational status • Port number • Access authorization level • Domain name
HTTP summary statistics	*httpsum.dat*	HTTP summary statistics (overview of the router's current state): • Total requests received • Total request errors • Total discarded requests • Total responses • Total unknown inputs • Total bytes received • Total bytes sent • Total timeouts • Start time

Chapter 6
Viewing Router Port Statistics

Clicking on Statistics > Ports displays the following folders in the navigational frame:

- Summary
- Ethernet
- Serial
- FDDI
- HSSI
- Token Ring

To get statistical information about any port type, click on the appropriate link. Each port-type folder contains links to summary statistics, *traffic* (number of packets transmitted and received) statistics, receive error statistics, and transmit error statistics. All but Ethernet also display system error statistics. The following sections summarize these displays.

Changing the Administrative Status of a Port

A user who has Manager-level access privileges can click on the first column of the table in the summary statistics window for any port type to enable or disable (that is, change the administrative setting of) the port.

Caution: If you disable the interface through which your Web browser is communicating with a router, you will no longer be able to monitor that router's operation with the HTTP Server.

The Enabled column displays the administrative setting, but it is not a clickable link. The State column shows the operational state of the port (up or down). If the Enabled column shows that the port is enabled, but the State column shows that the port is down, there is a problem with the port.

Viewing Traffic Statistics for All Ports

To view traffic statistics for all ports, click on Statistics > Ports > Summary.

Viewing Ethernet Port Statistics

Clicking on Statistics > Ports > Ethernet in the navigational frame reveals the following subordinate links: Summary, Traffic, Rx Errors, and Tx Errors.

To see these statistics	**Use this path**
Summary	Statistics > Ports > Ethernet > Summary
Traffic	Statistics > Ports > Ethernet > Traffic
Rx Errors	Statistics > Ports > Ethernet > Rx Errors
Tx Errors	Statistics > Ports > Ethernet > Tx Errors

Viewing Serial Port Statistics

Clicking on Statistics > Ports > Serial in the navigational frame reveals the following subordinate links: Summary, Traffic, Rx Errors, Tx Errors, and Sys Errors.

To see these statistics	Use this path
Summary	Statistics > Ports > Serial > Summary
Traffic	Statistics > Ports > Serial > Traffic
Rx Errors	Statistics > Ports > Serial > Rx Errors
Tx Errors	Statistics > Ports > Serial > Tx Errors
Sys Errors	Statistics > Ports > Serial > Sys Errors

Viewing FDDI Port Statistics

Clicking on Statistics > Ports > FDDI in the navigational frame reveals the following subordinate links: Summary, Traffic, Rx Errors, Tx Errors, and Sys Errors.

To see these statistics	Use this path
Summary	Statistics > Ports > FDDI > Summary
Traffic	Statistics > Ports > FDDI > Traffic
Rx Errors	Statistics > Ports > FDDI > Rx Errors
Tx Errors	Statistics > Ports > FDDI > Tx Errors
Sys Errors	Statistics > Ports > FDDI > Sys Errors

Viewing HSSI Port Statistics

Clicking on Statistics > Ports > HSSI in the navigational frame reveals the following subordinate links: Summary, Traffic, Rx Errors, Tx Errors, and Sys Errors.

To see these statistics	Use this path
Summary	Statistics > Ports > HSSI > Summary
Traffic	Statistics > Ports > HSSI > Traffic
Rx Errors	Statistics > Ports > HSSI > Rx Errors
Tx Errors	Statistics > Ports > HSSI > Tx Errors
Sys Errors	Statistics > Ports > HSSI > Sys Errors

Viewing Token Ring Port Statistics

Clicking on Statistics > Ports > Token Ring in the navigational frame reveals the following subordinate links: Summary, Traffic, Rx Errors, Tx Errors, and Sys Errors.

To see these statistics	Use this path
Summary	Statistics > Ports > Token Ring > Summary
Traffic	Statistics > Ports > Token Ring > Traffic
Rx Errors	Statistics > Ports > Token Ring > Rx Errors
Tx Errors	Statistics > Ports > Token Ring > Tx Errors
Sys Errors	Statistics > Ports > Token Ring > Sys Errors

Chapter 7
Viewing Router Protocol Statistics

Clicking on Statistics > Protocols displays the following folders in the navigational frame:

- IP
- IPX
- AppleTalk

To get statistical information about any protocol type, click on the appropriate link. Each protocol folder contains links to summary statistics, traffic statistics (number of packets transmitted and received), and interface statistics, as well as to other statistics specific to that protocol. The following sections show and briefly describe these displays.

Changing the Administrative Status of a Port

A user who has Manager-level access privileges can click on a radio button in the first column of the table in the interface statistics window for any protocol type to enable or disable (that is, change the administrative setting of) the port

Caution: If you disable the interface through which your Web browser is communicating with a router, you will no longer be able to monitor that router's operation with the HTTP Server.

The Enabled column displays the administrative setting, but it is not a clickable link. The State column shows the operational state of the interface (up or down). If the Enabled column shows that the interface is enabled, but the State column shows that the interface is down, there is a problem with the interface.

Viewing IP Statistics

Clicking on Statistics > Protocols > IP in the navigational frame reveals the following subordinate links: Global, Traffic, Interfaces, Routes, ARP Cache, RIP, and ICMP.

To see these statistics	Use this path
Global	Statistics > Protocols > IP > Global
Traffic	Statistics > Protocols > IP > Traffic
Interfaces	Statistics > Protocols > IP > Interfaces
Routes	Statistics > Protocols > IP > Routes
ARP Cache	Statistics > Protocols > IP > ARP Cache
RIP	Statistics > Protocols > IP > RIP
ICMP	Statistics > Protocols > IP > ICMP This reveals the following subordinate links: Counters, Received, and Transmitted.
• Counters	Statistics > Protocols > IP > ICMP > Counters
• Received	Statistics > Protocols > IP > ICMP > Received
• Transmitted	Statistics > Protocols > IP > ICMP > Transmitted

Viewing IPX Statistics

Clicking on Statistics > Protocols > IPX in the navigational frame reveals the following subordinate links: Global, Traffic, Interfaces, Forwarding, Hosts, Routes, Services, RIP, and SAP.

To see these statistics	Use this path
Global	Statistics > Protocols > IPX > Global
Traffic	Statistics > Protocols > IPX > Traffic
Interfaces	Statistics > Protocols > IPX > Interfaces
Forwarding	Statistics > Protocols > IPX > Forwarding
Hosts	Statistics > Protocols > IPX > Hosts
Routes	Statistics > Protocols > IPX > Routes
Services	Statistics > Protocols > IPX > Services
RIP	Statistics > Protocols > IPX > RIP
SAP	Statistics > Protocols > IPX > SAP

Viewing AppleTalk Statistics

Clicking on Statistics > Protocols > AppleTalk in the navigational frame reveals the following subordinate links: Global, Traffic, Interfaces, Routes, ARP Cache, and Zones.

To see these statistics	Use this path
Global	Statistics > Protocols > AppleTalk > Global
Traffic	Statistics > Protocols > AppleTalk > Traffic
Interfaces	Statistics > Protocols > AppleTalk > Interfaces
Routes	Statistics > Protocols > AppleTalk > Routes
ARP Cache	Statistics > Protocols > AppleTalk > ARP Cache
RIP	Statistics > Protocols > AppleTalk > RIP
Zones	Statistics > Protocols > AppleTalk > Zones

Appendix A
Site Manager Parameters

This appendix contains the Site Manager parameter descriptions for the HTTP Server. You can display the same information using Site Manager or the BCC online Help.

For each parameter, this appendix provides the following information:

- Parameter name
- Configuration Manager menu path
- Default setting
- Valid parameter options
- Parameter function
- Instructions for setting the parameter
- Management information base (MIB) object ID

The Technician Interface allows you to modify parameters by issuing **set** and **commit** commands with the MIB object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, see *Using Technician Interface Software*.

Caution: The Technician Interface does not verify the validity of your parameter values. Entering an invalid value can corrupt your configuration.

Site Manager Parameters

The Edit HTTP Global Parameters window contains the parameters that you can configure for the HTTP Server. To access the Edit HTTP Global Parameters window, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Global Protocols**.	The Global Protocols menu opens.
3. Choose **HTTP**.	The HTTP menu opens.
4. Choose **Global**.	The Edit HTTP Global Parameters window opens.

The parameter descriptions follow.

Parameter: Enable/Disable

Path: Configuration Manager > Protocols > Global Protocols > HTTP > Global

Default: When you enable the HTTP Server, this parameter is automatically set to Enabled.

Options: Enabled │ Disabled

Function: Enables or disables the HTTP Server on this interface.

Instructions: To prohibit the use of the HTTP Server on this interface, set this parameter to Disabled.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.22.1.1.2

Parameter: Port

Path: Configuration Manager > Protocols > Global Protocols > HTTP > Global

Default: 80

Options: 0 to 4096

Function: Specifies the port number on which you enable the HTTP Server.

Instructions: Accept the default value, 80, or specify a value from 0 to 4096.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.22.1.1.4

Parameter: Authentication

Path: Configuration Manager > Protocols > Global Protocols > HTTP > Global

Default: Basic

Options: Basic | Digest

Function: Specifies the type of authentication to use on this interface: basic or digest. Basic authentication verifies the user's identity using the user name and password passed over the network as clear text. Digest authentication uses an encrypted password. If you specify digest authentication, but your browser does not support this, authentication reverts to basic.

Instructions: Accept the default value Basic, or specify Digest.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.22.1.1.7

Parameter: Domain Name

Path: Configuration Manager > Protocols > Global Protocols > HTTP > Global

Default: None

Options: Any valid string of characters constituting a domain name

Function: Lets the server be accessible by a domain name, rather than by IP address. The Domain Name parameter must be set to the domain name that a DNS lookup would return for the router.

Accept the default value, no domain name, to indicate that the server is accessible only by the IP address; or specify a domain name to use instead of the IP address.

Instructions: Accept the default value, no domain name, to indicate that the server is accessible only by the IP address; or specify a domain name to use instead of the IP address.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.22.1.1.8

Appendix B
Show Commands for the HTTP Server

Use the Bay Command Console (BCC) **show** command to display statistical information about the HTTP Server on the router. The statistics available through the BCC are a subset of the information available through the HTTP Server interface itself. See *Using the Bay Command Console* for information about **show** scripts command syntax.

This chapter contains the following information about show commands:

Sample show Command Output

The **show** command displays summary information about the HTTP Server on the router. For example, if you enter the command:

bcc> **show http requests**

You see this type of output:

```
show http requests                                    Sep 21, 1998
11:48:04 [EDT]

Method  Total In  In Last Time
------  --------  ----------------------------
get          186  Sep 21 1998 14:20:57 [GMT-5]
head           0
trace          0
post           0
options        0
put            0
delete         0
```

Online Help for show Commands

You can display a list of available command options by entering **show** or **show** *<option>* without additional options or with a question mark as an option. For example, entering **show** or **show http ?** at the BCC prompt displays the list of all **show** or **show http** keyword (subcommand) options.

Show Commands for the HTTP Server

The **show http** or **show http ?** command lists the keywords (also called subcommands) available with this command. These keywords are:

- summary
- requests
- responses

The **show http** *<keyword>* command displays information about the HTTP Server activity on the router.

The HTTP Server **show http** commands have no command arguments, filter flags, or filter arguments. The router shows information for all applicable entries.

show http summary

The **show http summary** command displays summary statistics about HTTP services on the router.

The output contains the following information:

Total Requests Received	The total number of requests the router received.
Total Request Errors	The number of received requests that were in error.
Total Request Discards	The number of received requests that were discarded.
Total Responses	The number of router responses.
Total In Unknowns	The number of unrecognizable requests received.
Total Rx Octets	The number of received octets.
Total Tx Octets	The number of transmitted octets.
Total Time Outs	The number of time outs that occurred since the last reset.
Start Time	The time of the last router reset.

show http requests

The **show http requests** command displays HTTP request statistics for the router.

The output contains the following information:

Method	An HTTP keyword indicating a type of request.
Total In	The number of requests received.
In Last Time	The time the most recent request was received.

show http responses

The **show http requests** command displays HTTP response statistics for the router.

The output contains the following information:

Status	A numeric status code and a brief interpretation for a response category.
Total Out	The number of responses sent.
Out Last Time	The time the most recent response was sent.

Index

G

H

I

J

M

N

O

P

Q

R

S

T

U

W