BayRS Version 14.00

Part No. 308663-14.00 Rev 00
December 1999

4401 Great America Parkway
Santa Clara, CA 95054

Release Notes for BayRS Version 14.00

NORTEL NETWORKS™

THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH NORTEL 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. Nortel Networks NA Inc. ("Nortel 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 Nortel Networks Agent software or other Nortel Networks software products. Nortel Networks Agent software or other Nortel Networks software products are licensed for use under the terms of the applicable Nortel Networks NA 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. Nortel Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Nortel 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 Nortel 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 Nortel 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. Nortel Networks warrants each item of Software, as delivered by Nortel Networks and properly installed and operated on Nortel 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 Nortel Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Nortel 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. Nortel Networks will replace defective media at no charge if it is returned to Nortel 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. Nortel 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. Nortel 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 Nortel 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 NORTEL 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 NORTEL NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF NORTEL NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO NORTEL 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 Nortel Networks of any such intended examination of the Software and may procure support and assistance from Nortel Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Nortel Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Nortel Networks copyright; those restrictions relating to use and disclosure of Nortel 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 Nortel Networks the Software, user manuals, and all copies. Nortel 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 Nortel Networks, 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 NORTEL 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 NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN NORTEL 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 NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Tables

Preface

The Nortel Networks™ BayRS™ Version 14.00 is a software release that includes bug fixes and new features added since BayRS Version 13.20. These release notes contain guidelines for using BayRS Version 14.00.

Hard-Copy Technical Manuals

You can print selected technical manuals and release notes free, directly from the Internet. Go to *support.baynetworks.com/library/tpubs/*. Find the 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 selected documentation sets, CDs, and technical publications through the 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.

How to Get Help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	Telephone Number
Billerica, MA	800-2LANWAN (800-252-6926)
Santa Clara, CA	800-2LANWAN (800-252-6926)
Valbonne, France	33-4-92-96-69-68
Sydney, Australia	61-2-9927-8800
Tokyo, Japan	81-3-5402-7041

Release Notes for BayRS Version 14.00

This document contains the latest information about Nortel Networks BayRS Version 14.00, including information on the following topics:

Upgrading to Version 14.00

To upgrade BayRS to Version 14.00, see *Upgrading Routers to BayRS Version 14.xx,* in your upgrade package. In addition, read the following sections.

Upgrading FireWall-1 Configurations

To upgrade FireWall-1 from a BayRS version earlier than 13.20, complete the following steps.

Note: If you are currently running Firewall-1 from BayRS Version 13.20 and want to upgrade to BayRS Version 14.00, you do not have to follow these steps.

1. **Familiarize yourself with the Bay Command Console (BCC™).**

   Starting with BayRS Version 13.20, FireWall-1 no longer supports Site Manager as a configuration tool. You must use the BCC to manage and configure FireWall-1. For basic information about using the BCC, see *Using the Bay Command Console (BCC).*

2. **Make sure that you will not lose access to your router.**

   When you upgrade to BayRS Version 14.00, once you boot your router, the Version 14.00 software invokes the default FireWall-1 security policy. This default security policy drops all attempts at communication with the router.

   If you manage a router at a remote location, you will no longer be able to gain access to the router through the WAN connection. Before you upgrade, make sure that you can gain access to the router by dialing in through the console port, or that there is someone at the remote location who can configure the router.

3. **Reboot the router with BayRS Version 14.00, using an existing configuration file.**

4. **Use the BCC to reenable FireWall-1 on each IP interface.**

   To reenable FireWall-1 on each IP interface, use the BCC to navigate to the prompt for the slot/connector on which you have configured the IP interface (for example, **box; eth 2/2**). Then enter:

   ip address *<ip_address>* **mask** *<address_mask>*

ip_address is the IP address you have assigned to the interface.

address_mask is the mask associated with the IP address.

The prompt for the IP interface appears.

For example, the following command invokes the prompt for IP interface 2.2.2.2/255.0.0.0 (which has been configured on Ethernet slot 2, connector 2):

```
ethernet/2/2# ip address 2.2.2.2 mask 255.0.0.0
ip/2.2.2.2/255.0.0.0#
```

At the prompt for the IP interface, enter the following command to reenable FireWall-1:

firewall

The firewall prompt appears.

For example, the following command reenables FireWall-1 on the IP interface 2.2.2.2/255.0.0.0:

```
ip/2.2.2.2/255.0.0.0# firewall
firewall/2.2.2.2#
```

5. **To use FireWall-1 on more than 32 circuits, set the policy index number for each IP interface.**

   The policy index allows multiple circuits to share the same instance of FireWall-1. You can have up to 32 instances of FireWall-1, with many circuits making up each FireWall-1 instance. All circuits in a grouping must share the same security policy.

   By default, the policy index for a circuit is equal to the circuit number. If you are using FireWall-1 on fewer than 33 circuits, you do not have to use policy indexes.

   If you are using FireWall-1 on more than 32 circuits, group circuits that share the same security policy. Then, set the policy index on each circuit in a group to the same value.

For example, suppose you want to use FireWall-1 on 40 circuits. The first five circuits share one security policy; the next 35 share a different security policy. Using the BCC, assign policy index 1 to the first five circuits and policy index 2 to the next 35 circuits. You then have a total of 40 firewall circuits on the router, with two policy index values and two security policies.

Note: If you do not use policy index values and you configure more than 32 circuits on the router, all IP forwarding is disabled on circuits after the 32nd. If you use policy index values, but configure more than 32 policy index groupings, all circuits assigned policy indexes after the 32nd will have all IP forwarding disabled. The router logs warning messages that can help you determine whether you have any circuits on which all IP forwarding is disabled.

The Check Point log viewer treats circuits that share a policy index as one circuit.

If you are running FireWall-1 on more than 32 circuits and you therefore need to set the policy index value, use the BCC to navigate to the firewall prompt, as described in step 4. Then enter:

policy-index *<value>*

value is the index value, from 1 to 1023.

For example, the following command sets the policy index to 1:

```
firewall/2.2.2.2# policy-index 1
firewall/2.2.2.2#
```

6. **Save the configuration file and reboot the router.**

7. **Reinstall the security policy.**

   Since you previously defined a security policy (using the earlier version of BaySecure FireWall-1), you do not need to define it again. However, you must reinstall it in on the router. For complete instructions on how to install the security policy, see your Check Point FireWall-1 documentation.

   If you want to install different security policies for different policy indexes, use the Check Point FireWall-1 command line interface to enter the following command:

   fw load ../conf/*<config_file>* **pol***<policy_index_number>@<router_name>*

For example, the following command specifies that the system install the security policy in the configuration file *drop_ftp* on policy index number 1 on the router named *asn1*:

fw load ../conf/drop_ftp pol1@asn1

Upgrading ATM Configurations

If you are upgrading from a BayRS version earlier than 12.20 and you defined log event traps for asynchronous transfer mode (ATM), ATM signaling, or ATM LAN emulation, you must redefine these traps.

The ATM, ATM signaling, and ATM LAN emulation log event messages changed in BayRS Version 12.20. The ATM_SIG entity (entity #95) no longer exists as a separate entity. We have combined the ATM_SIG entity with the ATM entity (entity #78). Combining and reorganizing these entities resulted in changes to the ATM log event message numbers. We added new log events to the ATM_LE entity (entity #100), resulting in log event message number changes for LAN emulation as well.

You can view the new and modified ATM log event messages in the event database on the BayRS Online Library Version 14.00 CD, or on the World Wide Web at this URL:

http://support.baynetworks.com/library/tpubs/events/

Upgrading L2TP Configurations

If you have a BayRS Version 12.10 configuration file that includes L2TP operating on a router using BayRS Version 14.00, the router automatically upgrades the assigned user network addresses to L2TP IP interface addresses. L2TP IP interface addresses are internal to the router. When communicating with the remote user, the router associates the user's IP address with an L2TP IP interface address that you configure.

The user network addresses assigned to Version 12.10 apply to the entire router. In Version 14.00, each slot has a unique L2TP IP address. Consequently, if the number of configured L2TP slots is greater than the number of configured assigned user network addresses, the router will not be able to upgrade every slot from a Version 12.10 configuration to a Version 14.00 configuration. For slots that exceed the number of assigned user network addresses, you must manually configure L2TP IP interface addresses. To do this, delete L2TP from the slot, and then configure a new L2TP interface. Each slot must have L2TP IP interface addresses.

If the number of configured L2TP slots is less than or equal to the number of configured assigned user network addresses, the router automatically converts all assigned user network addresses to L2TP IP addresses.

Upgrading OSPF Configurations

When you upgrade BayRS from releases earlier than Version 12.20, there must not be an open shortest path first maximum transmission unit (OSPF MTU) interface mismatch. If a mismatch exists, adjacencies will not form between upgraded routers. All the OSPF routers forming adjacencies on a segment (broadcast, point-to-point [PPP], Point-to-Multipoint, or nonbroadcast multi-access [NBMA]) should have the same OSPF MTU size. You configure the OSPF MTU size through the MTU Size parameter in the OSPF Interfaces window in Site Manager.

BayRS Versions 12.20 and later comply with RFC 2178, which requires the OSPF MTU size feature.

Upgrading Static Forwarding Policy Filters

Internet Group Management Protocol (IGMP) static forwarding policy filters that you created in versions earlier than Site Manager Version 7.20 will not work correctly using Site Manager Version 7.20. To use these IGMP static forwarding policy filters, you must re-create them. For information about creating IGMP static forwarding policy filters, see *Configuring IP Multicasting and Multimedia Services*.

Upgrading IP Route Filters

If you have configured IP route filters and then disabled those filters (rather than deleted them), when you upgrade to Version 14.00, the filters will be re-enabled. You must disable the filters again after the upgrade is complete. If you do not want to use the filters, you might want to consider deleting them before you upgrade to Version 14.00.

New Features

The following sections provide brief descriptions of the new features in BayRS Version 14.00.

BCC Support for IP Inbound-Traffic Filters

In BayRS Version 14.00, you can configure IP inbound-traffic filters using the BCC. See *Configuring Traffic Filters and Protocol Prioritization* for information.

BayDVS Multilink PPP Accounting

In BayRS Version 14.00, the Bay dial virtual private network (BayDVS) feature reports multilink PPP protocol usage to the Remote Access Dial-In User Services (RADIUS) accounting server. This feature is enabled by default; there is no need for user intervention.

See *Configuring RADIUS* for more information.

DLSw Enhancements

BayRS 14.00 includes two enhancements to the data link switching (DLSw) protocol: MAC address translation and BAN2 termination. The following sections briefly describe these features. See *Configuring DLSw Services* for more information.

MAC Address Translation

MAC address translation allows you to redirect SNA and NetBIOS traffic to a host destination address that is different from the one configured in your PC. Redirection occurs on all LLC interfaces, including token ring, Ethernet, and frame relay Boundary Access Node (BAN) interfaces for outgoing connections. The router continues to support MAC addresses that are not translated.

BAN-2 Termination

From the router, you can use BAN-2 termination to locally terminate source route bridging (SRB) and LLC-2 frames destined for a token ring or frame relay network. The router forwards the traffic to the destination network using DLSw. (Before Version 14.00, you could forward traffic only between token ring and frame relay networks using SRB.)

While you typically use BAN-2 termination with frame relay networks, you can also use it to locally terminate any SRB-to-SRB connection. Therefore, you can locally terminate token ring-to-token ring, token ring-to-frame relay BAN, and frame relay BAN-to-frame relay BAN interfaces in a single switch DLSw router.

BootP Enhancement

Some boot PROMs, such as those manufactured by Bootware, might not support ARP (Address Resolution Protocol). Without ARP support, the client cannot use BootP to download a startup image over the network. With BayRS Version 14.00, you can overcome this obstacle by setting the MIB variable wfBootpRelayIntfArpCache to **enable** (**1**). When you enable this variable, the router creates an ARP cache entry based on the information received in the BootP reply from the server.

To set the wfBootpRelayIntfArpCache variable, you must use the Technician Interface. Set wfBootpRelayIntfArpCache to **1** to enable the ARP cache entry feature; set it to **2** to disable the feature. wfBootpReleayIntfArpCache is configurable on a per interface basis. By default, it is disabled.

For complete information on how to use the Technician Interface, see *Using Technician Interface Software*. The following example shows the commands you enter from the Technician Interface to first determine the setting of the ARP cache entry MIB variable on all interfaces and then set the ARP cache entry MIB variable to **enable** on the interface 10.10.10.1:

```
$ g wfBootpRelayIntfEntry.wfBootpRelayIntfArpCache.*
wfBootpRelayIntfEntry.wfBootpRelayIntfArpCache.10.10.10.1 = 2
wfBootpRelayIntfEntry.wfBootpRelayIntfArpCache.30.30.30.1 = 2

$ s wfBootpRelayIntfEntry.wfBootpRelayIntfArpCache.10.10.10.1 1;commit
```

Note: The setting of the wfBootpRelayIntfArpCache variable does not affect the operation of DHCP.

BootP Show Command Change

The show command **show bootp base** displays an additional column, labeled *ArpCache*, that indicates whether the ARP cache entry MIB variable is enabled or disabled, as shown in the following example:

```
Bootp Base Information
----------------------
    Interface                  Min     Max
     Address        State    Seconds   Hops  PassThruMode ArpCache
 ---------------- ---------- -------- ------ ------------ --------
 10.10.10.1       Up                0      4 BOOTP/DHCP   Enabled
 30.30.30.1       Up                0      4 BOOTP/DHCP   Disabled
```

See *Configuring SNMP, BootP, and DHCP Services* for more information about BootP.

Technician Interface osi lsp Command

The Technician Interface **osi lsp** command displays all, or a subset of, the link state packet (LSP) elements in the OSI link state database. You can use this information to help solve network problems.

IP MTU Enhancement

BayRS Version 14.00 allows you to set the maximum transmission unit (MTU) for an interface to a value less than the MTU of the underlying circuit. The default value (0) causes the IP interface to use the MTU value of the underlying circuit. If you configure a value greater than the MTU of the underlying circuit, the parameter is ignored.

Setting the MTU for an interface affects the transmission of IP frames only. Transmitted frames that are larger than the interface MTU value are fragmented into smaller frames. This parameter does not affect frames accepted by the driver.

See *Configuring IP, ARP, RARP, RIP, and OSPF Services* for more information.

Platform-Specific Names for BCC Help Files

Help files for the BCC now have platform-specific names. Previously, Help files for all platforms were named *bcc.help*. The new names are listed in Table 1.

Table 1. BCC Help File Names

Platform	File Name
AN	*bcc_an.hlp*
ARN	*bcc_arn.hlp*
ASN	*bcc_asn.hlp*
System 5000	*bcc_5000.hlp*
BN	*bcc_bn.hlp*

The first time you issue a **help** command from the BCC, the BCC automatically searches for its platform-specific Help file and initializes the Help system. To avoid confusion, when you upgrade to BayRS Version 14.00, remove any old versions of Help files (named *bcc.help*, by default).

To change the names of the Help file for any platform, configure a value for the help-file-name parameter at the box or stack level. For example:

```
box# help-file-name 3:arnhelp.hlp
```

This command instructs the BCC to use the file *arnhelp.hlp*, on slot 3, as the system Help file to load when the user enters the first Help command. See *Using the Bay Command Console* for more information.

IPsec Enhancements

The BayRS Version 14.00 implementation of Internet Protocol Security (IPsec) includes the following enhancements:

- You can configure BayRS IPsec to interoperate with Contivity IPsec Branch Office Connection.
- You can configure perfect forward secrecy (PFS) for Internet Key Exchange (IKE) exchanges through Site Manager.
- Preshared keys can be any length, and configured in either ASCII or hexadecimal.

See *Configuring IPsec Services* for more information.

X.25 Enhancements

The BayRS Version 14.00 implementation of X.25 includes the following enhancements:

- Permanent Virtual Circuits (PVCs) are now supported on the Public Data Network (PDN) service type. You must enable RFC1356 multiplexing to use more than one network protocol on a service record configured with PVCs.
- You can configure PTOP (Point-to-Point) Call Request service through Site Manager.
- You may now append up to 12 bytes of user data with a call request command by appending an uppercase D or an uppercase P after the number in a call request. The system ignores spaces in the user data. For example, to send the password “password” with a call request to number “1234567”, you can use any of the following commands:

  c1234567Ppassword

  c1234567Dpassword

  c1234567P pass word

See *Configuring X.25 Services* for more information.

Options to Enable TFTP

If you use the *install.bat* file to configure an IP address on the router, the system will ask you whether or not you want to enable TFTP upon startup. If you use Site Manager to configure an IP interface, for the first such interface the system will ask you whether or not you want to enable TFTP. The default for each of these queries is to enable TFTP.

After you create the configuration file, you must transfer this file to the router to enable TFTP. If the configuration file is already on the router, then you must enable TFTP using the BCC or the Technician Interface.

See *Configuring SNMP, BootP, and DHCP Services* for more information.

BCC Guidelines

The BCC is a command-line interface for configuring Nortel Networks devices.

Before using the BCC, see the following guidelines for using the software and the platforms, protocols, interfaces, and hardware modules that the BCC supports.

Deleting Interfaces with the BCC

Before using the BCC to delete an interface, make sure that you did not use Site Manager to configure the interface with a protocol that the BCC does not recognize. If you did, use Site Manager to delete the interface.

Sending BCC Feedback

After you use the BCC, we welcome your feedback. Please visit the BCC Web site at the following URL, where you can leave a message:

http://support.baynetworks.com/library/tpubs/bccfeedbk

Memory Requirements

To use the BCC, each slot on the router must have:

- 16 MB of dynamic RAM (DRAM)
- 2 MB of free memory available when you start the BCC

If you try to start the BCC with insufficient DRAM or free memory on a slot, the BCC returns the following message. In this case, you must use Site Manager instead of the BCC to configure the router.

```
**Error** Unable to load bcc command from file system.
Loadable Module: bcc.exe
```

Platforms Supported

The BCC runs on AN, ANH™, ARN, ASN®, System 5000™, and BN platforms including ARE, FRE, FRE-2, and FRE-4 processor modules.

Interfaces Supported

You can use BCC commands to configure the following interfaces:

- ATM
- Console
- DCM
- DSU/CSU
- Ethernet
- FDDI
- FE1
- FT1
- HSSI
- ISDN/BRI
- MCE1/MCT1
- Serial (synchronous)
- Token ring
- Virtual (referred to in Site Manager as Circuitless IP)

Tables 2 through 5 on pages 16 to 23 list the link and net modules that the BCC supports.

Protocols Supported

You can use BCC commands to configure the following protocols and services:

- Access (multiuser access accounts)
- ARP
- ATM
- BGP (including accept and announce policies)
- Data compression (WCP and Hi/fn)
- Dial backup
- Dial-on-demand
- DLSw
- DNS
- DVMRP (including accept and announce policies)
- FireWall-1
- Frame relay (multilink not supported)
- FTP
- GRE
- HTTP
- IGMP
- IP (including accept policies, adjacent hosts, static routes, and traffic filters)
- IPX (including static-netbios-route)
- IPXWAN
- LLC2
- MPOA
- NAT
- NHRP
- NTP
- OSPF (including accept and announce policies)
- PPP (certain line parameters only; no multiline or multilink supported)
- Proprietary Standard Point-to-Point
- RADIUS

- RIP (including accept and announce policies)
- Router discovery (RDISC)
- SDLC
- SNMP
- Source route bridge
- Spanning tree
- Syslog
- Telnet
- TFTP
- Transparent Bridge
- VRRP (Virtual Router Redundancy Protocol)

Identifying Board Types

Tables 2 through 5 identify the Board Type parameter values displayed by the BCC. Use the “BCC Board Type” column to find, in alphabetical order, a hardware module in an AN, ANH, ARN, ASN, BN, or System 5000 router configuration.

Note: You cannot use BCC commands to configure an X.25 PAD or V.34 console modem daughterboard for the ARN router. Use Site Manager to configure these daughterboards.

Note: Inserting a daughterboard into an AN base module redefines its module ID and board type.

Table 2 lists the AN and ANH board types.

Table 2. BCC Board Types: AN and ANH Modules

BCC Board Type	Technician Interface or MIB Module ID	Description
andeds	1033	AN-ENET (2 Ethernet ports, 2 serial ports)
andedsg	1050	ANH-8 (2 Ethernet ports, 2 serial ports) and an 8-port Ethernet hub active for the first Ethernet port
andedsh	1035	ANH-12 (2 Ethernet ports, 2 serial ports) and a 12-port Ethernet hub
andedst	1034	AN-ENET (2 Ethernet ports, 2 serial ports, 1 token ring port)
andst	1037	AN-TOKEN (2 serial ports, 1 token ring port)
andstc	1091	AN-TOKEN with CSU/DSU (2 serial ports, 1 token ring port)
andsti	1038	AN-TOKEN with ISDN (2 serial ports, 1 token ring port)
ansdsedst	1041	AN-ENET/TOKEN (1 Ethernet port, 2 serial ports, 1 token ring port)
anseds	1024	AN-ENET (1 Ethernet port, 2 serial ports) with 16 MB DRAM
ansedsc	1090	AN-ENET with CSU/DSU (2 Ethernet ports, 2 serial ports)
ansedsf	1100	AN-ENET with T1/FT1 (2 Ethernet ports, 2 serial ports)
ansedsg	1047	ANH-8 (1 Ethernet port, 2 serial ports) and an 8-port Ethernet hub
ansedsgc	1094	ANH-8 with CSU/DSU (1 Ethernet port, 2 serial ports) and an 8-port Ethernet hub
ansedsgf	1108	ANH-8 with T1/FT1 (1 Ethernet port, 2 serial ports) and an 8-port Ethernet hub
ansedsgi	1051	ANH-8 with ISDN (1 Ethernet port, 2 serial ports) and an 8-port Ethernet hub
ansedsgj	1127	AN-ENET (1 Ethernet port, 2 serial ports, 1 fractional E1 port) and an 8-port Ethernet hub
ansedsgjx	1137	AN-ENET (1 Ethernet port, 2 serial ports, 1 fractional E1 port) and an 8-port Ethernet hub and DCM
ansedsgx	1048	ANH-8 with DCM (1 Ethernet port, 2 serial ports) and an 8-port Ethernet hub
ansedsh	1026	ANH-12 (1 Ethernet port, 2 serial ports) and a 12-port Ethernet hub

(continued)

Table 2. BCC Board Types: AN and ANH Modules *(continued)*

BCC Board Type	Technician Interface or MIB Module ID	Description
ansedshc	1093	ANH-12 with CSU/DSU (1 Ethernet port, 2 serial ports) and a 12-port Ethernet hub
ansedshf	1106	ANH-12 with T1/FT1 (1 Ethernet port, 2 serial ports) and a 12-port Ethernet hub
ansedshi	1029	ANH-12 with ISDN (1 Ethernet port, 2 serial ports) and a 12-port Ethernet hub
ansedshj	1125	AN-ENET (1 Ethernet port, 2 serial ports, 1 fractional E1 port) and a 12-port Ethernet hub
ansedshjx	1136	AN-ENET (1 Ethernet port, 2 serial ports, 1 fractional E1 port) and a 12-port Ethernet hub and DCM
ansedsi	1027	AN-ENET with ISDN (2 Ethernet ports, 2 serial ports) with 16 MB DRAM
ansedsj	1119	AN-ENET (1 Ethernet port, 2 serial ports, 1 fractional E1 port) with 16 MB DRAM
ansedsjx	1133	AN-ENET (1 Ethernet port, 2 serial ports, 1 fractional E1 port) with 16 MB DRAM and DCM
ansedst	1025	AN-ENET/TOKEN (1 Ethernet port, 2 serial ports, 1 token ring port) with 16 MB DRAM
ansedstc	1092	AN-ENET/TOKEN with CSU/DSU (1 Ethernet port, 2 serial ports, 1 token ring port)
ansedsti	1028	AN-ENET/TOKEN with ISDN (1 Ethernet port, 2 serial ports, 1 token ring port)
ansedstj	1123	AN-ENET (1 Ethernet port, 2 serial ports, 3 fractional E1 ports) with 16 MB DRAM
ansedstjx	1135	AN-ENET (1 Ethernet port, 2 serial ports, 3 fractional E1 ports) with 16 MB DRAM and DCM
ansedstx	1058	AN-ENET/TOKEN with DCM (1 Ethernet port, 2 serial ports, 1 token ring port) with 16 MB DRAM
ansedsx	1055	AN-ENET with DCM (2 Ethernet ports, 2 serial ports)
ansets	1030	AN-ENET (1 Ethernet port, 3 serial ports) with 16 MB DRAM
ansetsg	1049	ANH-8 (1 Ethernet port, 3 serial ports) and an 8-port Ethernet hub

(continued)

Table 2. BCC Board Types: AN and ANH Modules *(continued)*

BCC Board Type	Technician Interface or MIB Module ID	Description
ansetsh	1032	ANH-12 (1 Ethernet port, 3 serial ports) and a 12-port Ethernet hub
ansetst	1031	AN-ETS (1 Ethernet port, 3 serial ports, 1 token ring port)
antst	1039	AN-TOKEN (3 serial ports, 1 token ring port)

Table 3 lists the BLN and BCN board types.

Table 3. BCC Board Types: BLN and BCN Modules

BCC Board Type	Technician Interface or MIB Module ID	Site Manager Model Number	Description
atmcds3	5120	AG13110115	ATM DS-3
atmce3	5121	AG13110114	ATM E3
atmcoc3mm	4608	AG13110112	ATM STS-3/STM-1 MMF
atmcoc3sm	4609	AG13110113	ATM STS-3/STM-1 SMF
comp	4353	AG2104037	Octal Sync with 32-context compression daughterboard
comp128	4354	AG2104038	Octal Sync with 128-context compression daughterboard
de100	4864	50038	100BASE-T Ethernet
dst416	40	5740	Dual Sync with token ring
dtok	176	5710	Dual token ring
enet3	132	5505	Dual Ethernet
esaf	236	5531	Dual Sync Dual Ethernet with 2-CAM filters
		5532	Dual Sync Dual Ethernet with 6-CAM filters
esafnf	232	5431	Dual Sync Dual Ethernet without hardware filters
gigenet	6400		Gigabit Ethernet-SX link module
gigenetlx	6401		Gigabit Ethernet-LX link module
mce1ii120	190	AG2111002	120-ohm Dual Port Multichannel E1 (MCE1-II) for ISDN PRI and Leased Line
mce1ii75	188	AG2111004	75-ohm Dual Port Multichannel E1 (MCE1-II) for 75-ohm Leased Line
mct1	168	5945	Dual Port MCT1
osync	4352	5008	Octal Sync
qef	164	5950	Quad Ethernet with hardware filters
qenf	162	5450	Quad Ethernet without hardware filters
qmct1db15	5377	AG2111007	Quad Port MCT1 DB15
qmct1ds0a	5378	AG2104052	Quad Port MCT1 DB15 with DS0A

(continued)

Table 3. BCC Board Types: BLN and BCN Modules *(continued)*

BCC Board Type	Technician Interface or MIB Module ID	Site Manager Model Number	Description
qtok	256	50021	Quad token ring
shssi	225	5295	HSSI
smce1ii120	191	AG2111001	120-ohm Single Port Multichannel E1 (MCE1-II) for ISDN PRI and Leased Line
smce1ii75	189	AG2111003	75-ohm Single Port Multichannel E1 (MCE1-II) for 75-ohm Leased Line
smct1	169	5944	Single Port MCT1
sqe100	6144		Quad 100BASE-TX link module
sqe100fx	6145		Quad 100BASE-FX link module
sse	118	5410	Single Sync with Ethernet
sync	80	5280	Quad Sync
wffddi1m	193	5943	Hybrid FDDI with single mode on connector B
wffddi1mf	197	5949	Hybrid FDDI with single mode on connector B and with hardware filters
wffddi1s	195	5942	Hybrid FDDI with single mode on connector A
wffddi1sf	199	5948	Hybrid FDDI with single mode on connector A and with hardware filters
wffddi2m	192	5930	Multimode FDDI
wffddi2mf	196	5946	Multimode FDDI with hardware filters
wffddi2s	194	5940	Single Mode FDDI
wffddi2sf	198	5947	Single Mode FDDI with hardware filters

Table 4 lists the ASN board types.

Table 4. BCC Board Types: ASN Modules

BCC Board Type	Technician Interface or MIB Module ID	Description
asnqbri	2560	Quad BRI Net Module
denm	1280	Dual Port Ethernet Net Module
dmct1nm	2944	Dual Port MCT1 Net Module
dsnm1n	1540	Dual Port Synchronous Net Module
dsnm1nisdn	1588	ISDN BRI/Dual Sync Net Module
dtnm	2048	Dual Port Token Ring Net Module
mce1nm	2816	MCE1 Net Module
mmasmbdas	1833	Hybrid PHY B FDDI Net Module
mmfsddas	1793	Multimode FDDI Net Module
qsyncm	1664	Quad Port Synchronous Net Module
se100nm	2304	100BASE-T Ethernet Net Module
shssinm	3584	HSSI Net Module
smammbdas	1825	Hybrid PHY A FDDI Net Module
smfsddas	1801	Single Mode FDDI Net Module
spex	512	SPEX Net Module
spexhsd	769	SPEX Hot Swap Net Module

Table 5 lists the ARN board types.

Table 5. BCC Board Types: ARN Modules

BCC Board Type	Technician Interface or MIB Module ID	Description
arn7sync	8873	ARN Seven-Port Serial Expansion Module
arndcsu	8768	ARN 56/64K DSU/CSU Adapter Module
arne7sync	8872	ARN Seven-Port Serial Expansion Module, with 1 Ethernet Port
arnentsync	8864	ARN Ethernet and Tri-Serial Expansion Module
arnfe1	8780	E1/FE1 DSU/CSU Adapter Module
arnft1	8776	T1/FT1 DSU/CSU Adapter Module
arnis	8784	ARN ISDN BRI S/T Adapter Module
arnisdnu	8800	ARN ISDN BRI U Adapter Module
arnisdnu	8880	ARN Token Ring and Tri-Serial Expansion Module
arnmbenx10	8896	ARN Ethernet Base Module xxMB DRAM with DCM
arnmbsen	8720	ARN Ethernet Base Module with 0, 4, 8, 16, or 32 DRAM
arbnbsfetx	8728	ARN 10/100BASE-TX Ethernet Module
arnmbsfefx	8729	ARN 100BASE-FX Ethernet Module
arnmbstr	8704	ARN Token Ring Base Module with 0, 8, 16, or 32 MB DRAM
arnpbenx10	8928	ARN Ethernet Expansion Module with DCM
arnpbtenx10	8960	ARN Ethernet and Tri-Serial Expansion Module with DCM
arnsenet	8832	ARN Ethernet Port Expansion Module
arnssync	8736	ARN Serial Adapter Module
arnstkrg	8816	ARN Token Ring Expansion Module
arntsync	8848	ARN Tri-Serial Port Expansion Module

Table 6 lists the System 5000 board types.

Table 6. BCC Board Types: System 5000 Modules

BCC Board Type	Technician Interface or MIB Module ID	Description
asnqbri	2560	Router Quad Port ISDN BRI Net Module
atm5000bh	524544	Centillion Multiprotocol Engine
denm	1280	Router Dual Ethernet Net Module
dmct1nm	2944	Router Dual Port MCT1 Net Module
dsnm1n	1540	Router Dual Synchronous Net Module
dtnm	2048	Router Dual Token Ring Net Module
iqe	1408	5380 Ethernet Router Module
iqtok	2176	5580 Token Ring Router Module
mce1nm	2816	Router MCE1 Net Module
mmasmbdas	1833	Router Hybrid PHY B FDDI Net Module
mmfsddas	1793	Router Multimode FDDI Net Module
qsyncnm	1664	Router Quad Port Synchronous Net Module
se100nm	2304	Router 100BASE-T Ethernet Net Module
shssinm	3584	Router HSSI Net Module
smammbdas	1825	Router Hybrid PHY A FDDI Net Module
smfsddas	1801	Router Single Mode FDDI Net Module

General Guidelines

The following guidelines supplement the instructions in the BayRS Version 14.00 documentation set.

Using Both Site Manager and the BCC

You can use either Site Manager or the BCC to manage Nortel Networks routers. If you want to use both tools, follow these guidelines:

- Do not try to use both Site Manager and the BCC to manage a single router at the same time. You are prohibited from doing so with a lock-out mechanism.
- Site Manager cannot understand traffic filters you configured using the BCC.

Traffic Filters Guidelines

Follow these guidelines when configuring traffic filters:

- If you apply a traffic filter to a *multinetted interface* (that is, an interface with more than one IP address), the traffic filter might not work correctly. To ensure that the filter works correctly, you must assign the same filter to all of the IP addresses on the interface.
- Site Manager cannot understand traffic filters you have configured using the BCC.
- When implementing outbound traffic filters for LAN protocols, in some configurations the filters might cause a decline in throughput performance. For LAN circuits where the forwarding rate of the router is critical, monitor the throughput performance after configuring outbound traffic filters. If you notice an unacceptable performance degradation, try using inbound traffic filters.
- If you use Site Manager or the BCC to configure IP traffic filters with precedence values that are higher than the number of traffic filters configured, you might reach the maximum precedence value before you create the maximum number of filters. When you reach the maximum precedence value of 31 traffic filters, the router generates an error if you try to configure a filter with a precedence of 32. The system does not place you in extended filtering mode.

For example, if you create the following five traffic filters, an error occurs when you create the fifth filter:

Filter 1 precedence = 28

Filter 2 precedence = 29

Filter 3 precedence = 30

Filter 4 precedence = 31

Filter 5 precedence = 32 (error occurs here)

As a workaround, you can take one of the following actions:

-- Reassign the precedence value of traffic filters 1 through 5 to lower values.

-- Use the Technician Interface to turn on extended filtering mode and let the system assign precedence values to additional traffic filters on the IP interface.

Downloading Internet Routes from an ISP

To minimize the time required to download routes from an Internet Service Provider (ISP), adjust two IP global parameters. Use the BCC to set the routing-table-indexes value to 10000 and the routing-table-deviation value to 50, as follows:

```
ip#routing-table-indexes 10000
ip#routing-table-deviation 50
```

See *Configuring IP, ARP, RIP, and OSPF Services* for more information about these commands.

Cisco Compatibility Issues Using PIM

This section describes Cisco compatibility issues that exist when running Protocol Independent Multicast (PIM) in a network that consists of both Cisco and Nortel Networks routers.

Fragment Tagging in Bootstrap Messages

In a PIM network in which Nortel Networks and Cisco routers interoperate, a Cisco router sends bootstrap packets that contain a fragment tag set to a zero value. When the Nortel Networks router receives these packets, it treats them as duplicate packets and immediately drops them.

To enable a Nortel Networks router to accept bootstrap packets from a Cisco router, set the Cisco Compatible parameter to Enable using Site Manager.

Cisco Drops RP Advertisement Messages with Zero Prefix Count

If you configure a Cisco router to serve as the bootstrap router (BSR) and you configure a Nortel Networks router to serve as an RP router for a PIM domain, the Cisco router drops any RP advertisement packet it receives from the RP router that contains a zero group prefix count. As a result, the Cisco router cannot advertise RP set information to all PIM routers in the domain.

To ensure that the Cisco router sends advertisement messages to all multicast group ranges using address 224.0.0.0/4, set the Cisco Compatible parameter to Enable.

Routers Ignore RP Priority and Hash Value During RP Selection

You configure multiple RPs responsible for the same or overlapping group ranges in a PIM domain. For RPs responsible for the same group ranges, a Cisco router selects the first RP on the RP list, regardless of the RP priority and hash value. For RPs responsible for overlapping group ranges, a Cisco router selects the router with the most specific group range, regardless of the RP priority and hash value.

As a workaround, configure only one RP router for each unique group range. This allows the Nortel Networks router and the Cisco router to select the same RP.

ATM Half Bridge Support

BayRS Version 14.00 includes support of the ATM Half Bridge (AHB) feature.

Please be aware that some users, operating under certain conditions, may encounter issues such as the following:

- When AHB caches an unsecure host that it learned via ARP, the associated idle time is 0. The idle time remains at 0 and does not age correctly.

- When you boot a router running AHB, the ARE slot logs a fault message.
- When you reset the AHB, it stops forwarding traffic out of the AHB port.
- If you configure AHB on an ATM null PVC, the router may crash.
- If you configure AHB and add a PVC to the router while another system is sending a ping message to your router, the ARE slot may crash and may begin executing the cold start hardware diagnostics.

Managing BayRS 14.00 and Carrier Network Services (CNS) 1.2.0.0

The MIBs for BayRS 14.00 and Carrier Network Services (CNS) 1.2.0.0 share common structures, but have not been synchronized. This could cause object conflicts in network management applications managing networks that include both BayRS and CNS elements. If you want to manage both BayRS 14.00 and CNS 1.2.0.0 elements in your network, we recommend loading the MIB for each system into a separate instance of the network management application.

Failover and Load Balancing for ATM VCs Not Supported

You can configure multiple ATM virtual circuits (VCs) to the same destination address. However, this kind of configuration does not provide load balancing or failover support.

MPOA and VRRP over LANE Support

BayRS Version 14.00 does not support running both Virtual Router Redundancy Protocol (VRRP) over LAN Emulation (LANE) and Multi-Protocol Over ATM (MPOA) on the same service record.

FRE-2 DRAM Requirements

The FRE-2 processor card requires a minimum of 16 MB DRAM.

OSPF Guidelines

If you are using Open Shortest Path First (OSPF) services, please keep the following guidelines in mind:

- As of BayRS Version 14.00, we do not support the OSPF backup soloist feature.
- According to RFC 2328, the cost of an OSPF route to an aggregated group of networks should be the distance to the furthest network in the group. A new MIB parameter, wfOspfAggrUseMaxCost, allows you to determine how to summarize the subnets using the area range. To use the furthest cost in the routing table, set this MIB to **1** (Enable). If you accept the default, **2** (Disable), the OSPF route cost is represented as the shortest path to a network within the aggregated group of networks.

IPsec Guidelines

This section describes guidelines you should follow if you are using Internet Protocol Security (IPsec) services.

IPsec 3DES Performance Considerations

IPsec performance can vary greatly, and IPsec can impact router performance in general. Factors that affect performance are cryptographic algorithms used by IPsec that consume substantial CPU resources, other protocols and features running on the slot that share the same CPU resources as IPsec, and the processing power of the BayRS router.

The following information will help you plan and manage CPU resources in BayRS routers configured with IPsec.

Greater security can adversely affect performance. Before deploying IPsec, identify the data traffic that must be protected. Effective traffic analysis might result in minimal performance impact on the router. Configure IPsec to bypass traffic that does not need to be protected, thereby reducing the CPU resources used. Also, the amount of CPU resources required varies significantly for different encryption and authentication algorithms.

These algorithms are listed in order of increasing CPU consumption and security:

- MD5
- SHA1
- DES
- DES with MD5
- DES with SHA1
- 3DES
- 3DES with MD5
- 3DES with SHA1

In addition, the key generation and periodic rekeying done by IKE Diffie Hellman imposes a CPU burden. Therefore, consider the keying intervals for IKE and for IPsec that you choose during configuration. Less frequent rekeying reduces the burden on the CPU. Consider rekeying the Phase 1 (IKE) SAs less frequently than the IPsec SAs.

Finally, the packet size influences the performance of the router. Smaller packet sizes at a given data rate impose a greater processing load than larger packet sizes.

You can optimize performance by using the information in this section to plan and manage CPU resources. For example, BayRS IPsec on a BN can fill a 2 Mb/s WAN pipe with bidirectional DES encrypted traffic. Conversely, 3DES + SHA1 traffic with aggressive Phase 1 (IKE) and IPsec rekeying (for example, every 10 minutes) might cause significant performance degradation under heavy traffic loads.

You might experience SNMP timeouts during periods when the router is carrying peak loads of protected traffic.

IPsec Executable

To use the IPsec option, you must purchase a separate IPsec CD that contains either the 56-bit (DES) or both triple DES (3DES) and DES cryptographic API executable (*capi.exe*) for the BayRS software. Purchase the CD for the router platform on which you plan to install the IPsec software. Follow the instructions included with the CD or in *Configuring IPsec Services* to install the IPsec option.

Adding the IPsec File to the BayRS 14.00 Base Kernel

To use IPsec, you must use Image Builder to add an IPsec file to the BayRS 14.00 base kernel. The IPsec file is located on a separate CD, which ships with the IPsec feature. To install IPsec, follow the instructions included on the IPsec CD. You do not have to modify or add anything to Site Manager.

Renaming the FireWall-1 Redundant Management Scripts

Nortel Networks provides redundant management script files to make it easy to synchronize firewall management stations using the **fwfilex** command. You can use these scripts to transfer security policies and configuration files from one Windows NT platform to another, or from one UNIX platform to another.

You can get the files necessary to synchronize backup stations from either the BayRS software CD or the World Wide Web.

If you are using UNIX systems for your backup management stations, copy the file (*fwfilex.*) in the *fwbkpscr/unix* directory on the CD into the FireWall-1 bin directory (typically */etc/fw/bin)* on your primary backup station**.**

Note: After you copy the file (*fwfilex.*) to the */etc/fw/bin* directory on the primary backup station, you must rename the file to *fwfilex* so that it no longer has a period (.) at the end.

For detailed information about the redundant management script files and how to synchronize firewall management stations, see *Configuring BaySecure FireWall-1*.

BayRS Bandwidth Broker for Differentiated Services

To implement a differentiated services network using a BayRS bandwidth broker, you must install the BayRS Bandwidth Broker software on a PC running Windows NT® 4.0. The Nortel Networks router that communicates with the bandwidth broker must be operating with BayRS Version 13.20 or later software.

To download the BayRS Bandwidth Broker software and learn how to configure it:

1. **Go to the Router Management Labs page at *http://www.nortelnetworks.com/rml*.**
2. **Click on Software Solutions.**
3. **If you are a registered user, enter your email address. If not, register.**

   You see a list of solutions for which you can download software.
4. **Scroll through the list to locate the BayRS Bandwidth Broker.**

   From here you can download the software and the user manual.

Event Database

You can view the event database on the World Wide Web and the BayRS Online Library Version 14.00 CD. To access the event database on the World Wide Web, go to: *http://support.baynetworks.com/library/tpubs/events*

To access the event database on the BayRS Online Library Version 14.00 CD, follow the instructions in the CD booklet.

The event database includes a search facility that allows you to sort events by entity number, event number, severity, and text of the event message. For example, you can list only the warning messages for the IPX entity.

Quick2Config

Quick2Config® Version 1.3.2, which shipped with BayRS Version 12.20, was the final release of Quick2Config. Quick2Config Version 1.3.2 is not compatible with BayRS Version 13.10 or later, and there will be no new versions of Quick2Config for these releases. Nortel Networks will maintain Quick2Config Version 1.3.2 until early 2001.

You can continue to configure routers with Site Manager and the BCC.

SunOS 4.1.4 Support for Site Manager

Customers using Site Manager with SunOS 4.1.4 must migrate to a supported Solaris OS platform. Site Manager Version 14.00 does not work with SunOS, but continues to work with Solaris and other supported operating systems.

Year 2000 Compliance

BayRS Version 14.00 is Year 2000 Compliance Certified by Nortel Networks. The software has successfully passed the Nortel Networks Test Procedure, which tests conformance to the Nortel Networks Year 2000 compliance definition. For more information, see the Nortel Networks Year 2000 Web Site at *http://www.nortelnetworks.com/corporate/year2000/bay/*.

Note: For Firewall-1, the embedded agent is fully Year 2000 compliant. For the separate management station that you use to download policies, you must use Version 4.0, Service Pack 4 for full compliance.

Protocol Statistics for MPLS

The HTTP Server interface contains a folder icon for displaying Multiprotocol Label Switching (MPLS) statistics. The following table summarizes these statistics and how to get them using the HTTP Server interface.

Clicking on Statistics > Protocols > MPLS in the navigational frame reveals the following subordinate links: MLM Interface, MLM Sessions, MLM Connections, LDP Sessions, and LDP Information.

To see these statistics	Use this path
MLM Interface	Statistics > Protocols > MPLS > MLM Interfaces
MLM Sessions	Statistics > Protocols > MPLS > MLM Sessions
MLM Connections	Statistics > Protocols > MPLS > MLM Connections
LDP Sessions	Statistics > Protocols > MPLS > LDP Sessions
LDP Information	Statistics > Protocols > MPLS > LDP Information

Using Embedded Web Server to Transfer Files

When you use the embedded web server to transfer files to or from the router, HTTP (Hypertext Transfer Protocol) encapsulates the data. You do not need to be concerned with selecting a file format (text or binary, for example) the way you would if you were using FTP (File Transfer Protocol) or TFTP (Trivial File Transfer Protocol) to transfer the files.

For example, to transfer an image file to the router, use your browser's default file format type to transfer the file to the router's FLASH memory. The file arrives at the router as an image file from which you can boot the router.

AN/ANH and ARN Guidelines

Follow these guidelines when using AN, ANH, or ARN routers.

Allocating Memory on ARN Routers

Although you can change the default memory allocation on other Bay Networks router platforms, the ARN platform does not support this "buffer carving" feature.

On the ARN, Site Manager does not support the Admin > Kernel Configuration option, and the Technician Interface does not support the **set** command for wfKernCfgParamEntry objects. Attempting to set wfKernCfgParamGlobMem on the ARN results in a warning message.

DSU/CSU Test LED Remains On After Reset

The ARN DSU/CSU Test LED properly goes on when the interface enters test or loopback mode. However, the LED remains on after resetting the DSU/CSU module, even though all looping terminates and the module hardware resets.

Restarting the router turns the LED off. However, this action is not necessary for proper operation of the DSU/CSU interface.

Network Booting on DSU/CSU Interfaces

AN and ANH DSU/CSU interfaces do not support network booting.

ARN Router Not a Supported DVS RADIUS Client

The ARN router is not a supported DVS RADIUS client.

Increasing Buffer Size on Non-Token-Ring AN Routers

By default, AN routers without token ring modules installed initialize with a buffer size of 1824 bytes, which makes these ANs unable to accept packets larger than 1590 bytes. To allow ANs without token ring modules to accept larger packets, you can increase the buffer size by setting the MIB variable wfKernCfgParamEntry.wfKernCfgParamBufSize to 4800.

For complete instructions on using the Technician Interface to set MIB variables, see *Using Technician Interface Software*. The following example shows Technician Interface commands you might use to reset the MIB variable wfKernCfgParamEntry.wfKernCfgParamBufSize to 4800:

```
set wfKernCfgParamEntry.wfKernCfgParamDelete.1 1
set wfKernCfgParamEntry.wfKernCfgParamBufSize.1 4800
set wfKernCfgParamEntry.wfKernCfgParamDelete.1 2
commit
save config 2:config
reset 1
```

To set the buffer size back to its default of 1824 bytes, issue the following command:

```
set wfKernCfgParamEntry.wfKernCfgParamBufSizeReset.1 1
commit
```

BayRS Version Flash Memory Requirements

BayRS software ships on the following flash memory cards:

Platform	Flash Memory Required	Associated Software Suites
AN/ANH	8 or 16 MB	corp_suite, ip_access, office_suite
ARN	8 or 16 MB	corp_suite, ip_access, office_suite
ASN	8 or 16 MB	corp_suite, lan_suite, system_suite, wan_suite
BN	16 or 32 MB	atm_suite, corp_suite, lan_suite, system_suite, vnr_suite, wan_suite
System 5000	8 or 16 MB	corp_suite, lan_suite, system_suite, vnr_suite, wan_suite

Configuring PU 4 and SDLC Link Stations

If you use PU 4 devices with Synchronous Data Link Control (SDLC) and modulo 128, set the SDLC parameters MAXOUT and MAXIN to 127. You see these parameters in the SDLC Link Station Configuration window. For instructions on setting these parameters, see *Configuring SDLC Services*.

Creating Multiple GRE Tunnels

When creating multiple GRE tunnels dynamically, you can configure a maximum of five point-to-point GRE tunnels. In multipoint configurations, you can configure 64 GRE tunnels per interface.

Configuring NAT Dynamically

When you configure a local or global interface for NAT in dynamic mode, the router returns an SNMP set error. However, this error does not affect the configuration of the router.

Protocol Prioritization No Call Filters and TCP Applications

Using a no call filter that applies to any TCP application can cause TCP to retransmit the filtered packet.

When two routers running a TCP application are connected using a demand line, and the demand line becomes inactive, the TCP application remains connected.

If a demand line configured with a no call filter goes down, the no call filter drops the TCP packet that matches the no call filter rule. Because TCP never receives an acknowledgment that the packet was dropped, the TCP application continues to retransmit that packet until the connection times out and the application stops operating.

Note: No call filters are specific to dial services. For additional information about traffic filters and protocol prioritization, see *Configuring Traffic Filters and Protocol Prioritization*.

Support for Strata-Flash Card

BayRS supports the Strata-Flash card on AN, ANH, ARN, ASN, and BN routers. For details about flash cards, see “Flash Memory Cards Supported” on page 50.

Adding SDLC Changes Serial Parameter Settings

When you configure SDLC on a serial interface, the router software automatically changes the values for the following serial parameters:

- cable type
- clock source
- internal clock speed
- signal mode

Defaults for serial parameters, without SDLC, are listed in Table 7.

Table 7. Default Settings for Serial Parameters without SDLC

Parameter	Default Setting
cable type	null
clock source	external
internal clock speed	clk64k
signal mode	balanced

After you add SDLC to an interface, the settings for the serial parameters change. The new settings are listed in Table 8.

Table 8. Default Settings for Serial Parameters with SDLC

Parameter	Default Setting
cable type	rs232
clock source	internal
internal clock speed	clk19200
signal mode	unbalanced

WEP Executable

To use the DES-40 WAN Encryption Option or DES-56 WAN Encryption Option to perform PPP or frame relay layer 2 encryption, you must purchase a separate CD containing the WEP executable (*wep.exe*) for BayRS 14.00 software.

To install WEP on a router, you must first add the WEP executable to your BayRS 14.00 base kernel using Image Builder in Site Manager.

You can purchase two WEP executables based on the key size: a 40-bit version and a 56-bit version, which are included on separate CDs.

You must purchase three CDs when ordering the WEP protocol for BayRS software:

- Base BayRS 14.00 CD, which contains no WEP functions
- 40-bit WEP CD, which contains the 40-bit executable file
- 56-bit WEP CD, which contains the 56-bit executable file

To configure WEP, you do not have to modify Site Manager.

IPv6 Supported on ATM PVCs

BayRS supports IPv6. You can configure IPv6 using Site Manager on an ATM PVC interface.

Configuring RADIUS Servers

To enable RADIUS authentication for multilevel access or to use vendor-specific attributes (VSAs), you must configure the BSAC RADIUS server with the following files:

- *bayrs.dct*
- *vendor.ini*
- *dictiona.dcm*

These files load at server startup and enable the server to recognize the vendor-specific RADIUS clients. You can locate these files in the *bsac* directory on the BayRS Router and Site Manager Software update CD.

- To configure a Bay Networks RADIUS server, copy the three files to the directory that you define at installation time (typically *C:\RADIUS\Service*).
- To configure a non-Bay Networks RADIUS server, use the *bayrs.dct* file as a reference to change the existing RADIUS dictionary. Because *bayrs.dct* is in the format of some popular RADIUS servers, you might be able to use it as a direct replacement for the existing RADIUS dictionary. For more information, see the vendor's documentation.

Note: To use RADIUS with IP utilities such as FTP, NTP, HTTP, and Telnet, your RADIUS server must support VSAs.

The RADIUS dictionary file (*bayrs.dct*) defines the Nortel Networks vendor-specific attributes. The Nortel Networks vendor ID is 1584, as allocated by the Internet Assigned Numbers Authority. Use this ID in the header when using VSAs.

For more information on	See this document
RADIUS	*Configuring RADIUS*
BaySecure Access Control	*BaySecure Access Control Administration Guide* (for your specific platform: UNIX, NetWare, or Windows NT)
Multilevel Access	*Using the Bay Command Console (BCC)*

Operating Limitations and Cautions

Be aware of the following limitations when using BayRS 14.00.

Deleting ATM from a Router if Signaling Is Enabled

Do not delete ATM from a router if you enabled signaling on an ATM circuit. Otherwise, Site Manager, the BCC, or the Technician Interface will restart after a few minutes.

Signal Ports Settings on a Switch and Router Conflict

If you are using a switch with signal ports set to V3.1, be sure to set the signaling setting on the router to V3.1. If you accept the default setting of V3.0 for the router, the router faults repeatedly until you change the setting to V3.1.

Creating FTP from the BCC

From the BCC, if you create FTP on the router, then delete it and recreate it, the BCC faults. In this case, you must restart the BCC and create FTP on the router again.

Using DVMRP with Interfaces with More than One IP Address

You cannot use the BayRS Version 14.00 implementation of Distance Vector Multicast Routing Protocol (DVMRP) with circuits with multinetted interfaces (that is, interfaces with more than one IP address).

Deleting a Hybrid Mode Permanent Virtual Circuit (PVC)

If you configure SRB on a router, do not delete hybrid mode PVCs. Otherwise, all slots will restart.

Using DLSw/APPN Boundary Port with AS400s and Other Adjacent Link Stations

Do not configure any explicit APPN adjacent link stations on the DLSw/APPN boundary (VCCT) port, unless you are certain that the adjacent link station (for example, an AS400) will not attempt to connect to the APPN node. Otherwise, the DLSw/APPN boundary (VCCT) function fails to operate correctly and the router might restart.

Virtual Channel Connections (VCCs) Becoming Inactive

On the ARE and 5782 MPE, BayRS 14.00 does not release virtual channel connections when they time out. To maintain the availability of VCCs for new activities, configure a LAN emulation client (LEC) other than the router to release the inactive VCCs.

Performing Flash Compaction or Extensive File Management on ARE Module

Do not perform a flash compaction or extensive file management on a busy or production ARE module. Doing so may cause a fault in the module.

Accessing the Embedded Web Server Using Microsoft Internet Explorer

When you access the embedded Web server using Microsoft® Internet Explorer Version 4.72.2106.8, the file page is blank. However, Internet Explorer Version 4.72.3110.8 works correctly. We suggest that you upgrade to Version 4.72.3110.8 or later.

Some Statistics Not Currently Supported

BayRS Version 14.00 does not currently support the following three MIB attributes: wfAtmizerVclRxOctets, wfAtmizerVclTxOctets, and wfAtmizerVclTxClipFrames. Ignore the values that these statistics return.

Maximum Burst Size Not Supported on ARE or 5782 Modules

The ARE and 5782 processor modules do not support the ATM traffic parameter maximum burst size (MBS). Please ignore references to MBS in *Configuring ATM Services*.

Loss of Signal Might Cause ARE Slot to Hang

If there is a loss of signal to a router during a period of heavy traffic, the ARE slot on the router might stop functioning. If the ARE slot stops functioning, you must reboot the router.

8 MB Flash Not Supported for BN Platform

Eight MB flash cards are not supported for BN routers. The minimum flash card size is 16 MB for the BN platform. See “Flash Memory Cards Supported” on page 50 for a list of supported flash vendors.

Router Loses IP Connection When Security Enabled

If you change the setting of the router's IP Security feature (MIB variablewfIpIntFCfgEnableSecurity) from Disabled to Enabled, the router loses its IP connection. You must reboot the router.

Protocols Supported

BayRS Version 14.00 supports the following bridging/routing protocols and router configuration features:

- Advanced Peer-to-Peer Networking (APPN)
- AppleTalk and AppleTalk Update Routing Protocol (AURP)
- Asynchronous transfer mode (ATM)
- ATM Data Exchange Interface (ATM DXI)
- ATM Half Bridge (AHB)
- ATM LAN Emulation (802.3 and 802.5)
- Bandwidth Allocation Protocol (BAP)

- Binary Synchronous Communication Type 3 (BSC3)
- Bisync over TCP (BOT)
- Bootstrap Protocol (BootP)
- Border Gateway Protocol (BGP-3 and BGP-4)
- Classless interdomain routing (CIDR)
- Data compression (WCP and Hi/fn)
- Data link switching (DLSw)
- DECnet Phase IV
- Differentiated services
- Distance Vector Multicast Routing Protocol (DVMRP)
- Dynamic Host Configuration Protocol (DHCP)
- Encryption (WEP; proprietary)
- Exterior Gateway Protocol-2 (EGP-2)
- File Transfer Protocol (FTP)
- Frame relay (PVC, SVC)
- HP Probe
- Hypertext Transfer Protocol (HTTP)
- Integrated Services Digital Network (ISDN)
- Interface redundancy (proprietary)
- Internet Control Message Protocol (ICMP)
- Internet Gateway Management Protocol (IGMP)
- Internet Key Exchange (IKE)
- Internet Packet Exchange (IPX)
- Internet Protocol (IP)
- Internet Protocol Version 6 (IPv6)
- Internet Stream Protocol (ST2)
- IP Security (IPsec)
- IPsec Encapsulating Security Payload (ESP)

- IPv6 PPP Control Protocol (IPv6CP)
- Layer 2 Tunneling Protocol (L2TP)
- Learning bridge
- Logical Link Control 2 (LLC2)
- Multicast OSPF (MOSPF)
- Multiprotocol Label Switching (MPLS)
- Multiprotocol Over ATM (MPOA)
- Native Mode LAN (NML)
- Network Time Protocol (NTP)
- Open Shortest Path First (OSPF)
- Open Systems Interconnection (OSI)
- Point-to-Point Protocol (PPP)
- Polled Asynch (PAS), also called Asynch Passthru over TCP
- Protocol prioritization
- Qualified Logical Link Control (QLLC)
- RaiseDTR dialup
- Remote Authentication Dial-In User Service (RADIUS)
- Resource Reservation Protocol (RSVP)
- Router discovery (RDISC)
- Router redundancy (proprietary)
- Routing Information Protocol (RIP)
- Service Advertisement Protocol (SAP)
- Simple Network Management Protocol (SNMP)
- Source route bridging (SRB)
- Source route bridging over ATM permanent virtual circuits (PVCs)
- Spanning tree
- Switched Multimegabit Data Service (SMDS)
- Synchronous Data Link Control (SDLC)

- Telnet (inbound and outbound)
- Transmission Control Protocol (TCP)
- Transparent bridge
- Transparent-to-source routing translation bridge
- Trivial File Transfer Protocol (TFTP)
- User Datagram Protocol (UDP)
- V.25bis dialup
- Virtual Network Systems (VINES)
- Virtual Router Redundancy Protocol (VRRP)
- X.25 with QLLC
- Xerox Network System (XNS)
- XMODEM and YMODEM

Standards Supported

Table 9 lists the Request For Comments (RFCs) and other standards documents with which Version 14.00 complies. BayRS Version 14.00 might support additional standards that are not listed in this table.

Table 9. Standards Supported by Version 14.00

Standard	Description
ANSI T1.107b-1991	Digital Hierarchy -- Supplement to formats specifications
ANSI T1.404	DS3 Metallic Interface Specification
ANSI X3t9.5	Fiber Distributed Data Interface (FDDI)
Bellcore FR-440	Transport Systems Generic Requirements (TSGR)
Bellcore TR-TSY-000009	Asynchronous Digital Multiplexes, Requirements, and Objectives
Bellcore TR-TSY-000010	Synchronous DS3 Add-Drop Multiplex (ADM 3/X) Requirements and Objectives
FIPS 46-2	Data Encryption Standard (DES)
FIPS 81	DES Modes of Operation (ECB, CBC)
IEEE 802.1	Logical Link Control (LLC)
IEEE 802.1Q	IEEE 802.1Q VLAN tagging
IEEE 802.3	Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
IEEE 802.5	Token Ring Access Method and Physical Layer Specifications
IEEE 802.1D	Spanning Tree Bridges
ITU Q.921	ISDN Layer 2 Specification
ITU Q.931	ISDN Layer 3 Specification
ITU X.25	Interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuits
RFC 768	User Datagram Protocol (UDP)
RFC 791	Internet Protocol (IP)
RFC 792	Internet Control Message Protocol (ICMP)
RFC 793	Transmission Control Protocol (TCP)
RFC 813	Window and Acknowledgment Strategy in TCP

(continued)

Table 9. Standards Supported by Version 14.00 *(continued)*

Standard	Description
RFC 826	Ethernet Address Resolution Protocol
RFC 827	Exterior Gateway Protocol (EGP)
RFC 854	Telnet Protocol Specification
RFC 855	Telnet Option Specification
RFC 856	Telnet Binary Transmission
RFC 857	Telnet Echo Option
RFC 858	Telnet Suppress Go Ahead Option
RFC 859	Telnet Status Option
RFC 860	Telnet Timing Mark Option
RFC 861	Telnet Extended Options: List Option
RFC 863	Discard Protocol
RFC 877	Transmission of IP Datagrams over Public Data Networks
RFC 879	TCP Maximum Segment Size and Related Topics
RFC 888	"STUB" Exterior Gateway Protocol
RFC 894	Transmission of IP Datagrams over Ethernet Networks
RFC 896	Congestion Control in IP/TCP Internetworks
RFC 903	Reverse Address Resolution Protocol
RFC 904	Exterior Gateway Protocol Formal Specification
RFC 919	Broadcasting Internet Datagrams
RFC 922	Broadcasting Internet Datagrams in Subnets
RFC 925	Multi-LAN Address Resolution
RFC 950	Internet Standard Subnetting Procedure
RFC 951	Bootstrap Protocol
RFC 959	File Transfer Protocol
RFC 994	Protocol for Providing the Connectionless-Mode Network Service
RFC 1009	Requirements for Internet Gateways
RFC 1027	Using ARP to Implement Transparent Subnet Gateways
RFC 1042	Transmission of IP over IEEE/802 Networks
RFC 1058	Routing Information Protocol

(continued)

Table 9. Standards Supported by Version 14.00 *(continued)*

Standard	Description
RFC 1075	Distance Vector Multicast Routing Protocol (DVMRP)
RFC 1076	Redefinition of Managed Objects for IEEE 802.3 Repeater Devices (AN hubs only)
RFC 1079	Telnet Terminal Speed Option
RFC 1084	BOOTP Vendor Information Extensions
RFC 1091	Telnet Terminal-Type Option
RFC 1108	Security Options for the Internet Protocol
RFC 1112	Host Extensions for IP Multicasting Appendix I, Internet Group Management Protocol
RFC 1116	Telnet Line-Mode Option
RFC 1139	Echo Function for ISO 8473
RFC 1155	Structure and Identification of Management Information for TCP/IP-based Internets
RFC 1157	Simple Network Management Protocol (SNMP)
RFC 1163	BGP-2 (obsoleted by RFC 1267)
RFC 1164	Application of BGP in the Internet
RFC 1166	Internet Numbers
RFC 1188	Proposed Standard for the Transmission of IP over FDDI
RFC 1191	Path MTU Discovery
RFC 1209	Transmission of IP Datagrams over SMDS
RFC 1212	Concise MIB Definitions
RFC 1213	MIB for Network Management of TCP/IP-Based Internets
RFC 1267	Border Gateway Protocol 3 (BGP-3; obsoletes RFC 1163)
RFC 1293	Inverse ARP for Frame Relay (obsoleted by RFC 2390)
RFC 1294	Multiprotocol Interconnect over Frame Relay (obsoleted by RFC 1490 and RFC 2427)
RFC 1304	Definition of Managed Objects for the SIP Interface Type
RFC 1305	Network Time Protocol
RFC 1315	Management Information Base for Frame Relay DTEs (obsoleted by RFC 2115)
RFC 1321	MDS Digest Algorithm
RFC 1323	TCP Extensions for High Performance

(continued)

Table 9. Standards Supported by Version 14.00 *(continued)*

Standard	Description
RFC 1331	Point-to-Point Protocol (PPP; obsoleted by RFC 1661)
RFC 1332	PPP Internet Protocol Control Protocol (IPCP)
RFC 1333	PPP Link Quality Monitoring (obsoleted by RFC 1989)
RFC 1334	PPP Authentication Protocols
RFC 1350	The TFTP Protocol (Revision 2)
RFC 1356	Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode
RFC 1376	PPP DECnet Phase IV Control Protocol (DNCP)
RFC 1377	OSI over PPP
RFC 1378	PPP AppleTalk Control Protocol (ATCP)
RFC 1390	Transmission of IP and ARP over FDDI Networks
RFC 1403	BGP OSPF Interaction
RFC 1434	Data Link Switching: Switch-to-Switch Protocol
RFC 1483	Multiprotocol Encapsulation over ATM AAL5
RFC 1490	Multiprotocol Interconnect over Frame Relay (obsoletes RFC 1294, obsoleted by RFC 2427)
RFC 1541	Dynamic Host Configuration Protocol
RFC 1552	The PPP Internetwork Packet Exchange Control Protocol (IPXCP)
RFC 1577	Classical IP and ARP over ATM
RFC 1585	MOSPF: Analysis and Experience
RFC 1634	Novell IPX over Various WAN Media (IPXWAN)
RFC 1638	PPP Bridging Control Protocol (BCP)
RFC 1654	Border Gateway Protocol 4 (BGP-4; obsoleted by RFC 1771)
RFC 1661	Point-to-Point Protocol (PPP; obsoletes RFC 1331)
RFC 1662	PPP in HDLC-like Framing
RFC 1717	PPP Multilink Protocol (MP; obsoleted by RFC 1990)
RFC 1755	Signaling Support for IP over ATM
RFC 1757	Remote Network Monitoring Management Information Base (RMON), for AN, ANH, and ARN equipped with data collection module only
RFC 1762	PPP Banyan VINES Control Protocol (BVCP)
RFC 1763	PPP DECnet Phase IV Control Protocol (DNCP)

(continued)

Table 9. Standards Supported by Version 14.00 *(continued)*

Standard	Description
RFC 1764	PPP XNS IDP Control Protocol (XNSCP)
RFC 1771	Border Gateway Protocol 4 (BGP-4; obsoletes RFC 1654)
RFC 1795	Data Link Switching: Switch-to-Switch Protocol, Version 1
RFC 1819	Internet Stream Protocol, Version 2
RFC 1974	PPP Stac LZS Compression Protocol
RFC 1989	PPP Link Quality Monitoring (obsoletes RFC 1333)
RFC 1990	PPP Multilink Protocol (MP; obsoletes RFC 1717)
RFC 2068	HTTP Version 1.1
RFC 2069	An extension to HTTP: Digest Access Authentication
RFC 2104	HMAC: Keyed-Hashing for Message Authentication
RFC 2115	Management Information Base for Frame Relay DTEs Using SMIv2 (obsoletes RFC 1315)
RFC 2138	Remote Authentication Dial-In User Service (RADIUS)
RFC 2139	RADIUS Accounting
RFC 2166	Data Link Switching, Version 2.0, Enhancements
RFC 2178	OSPF Version 2
RFC 2205	Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification
RFC 2338	Virtual Router Redundancy Protocol
RFC 2385	Protection of BGP Sessions via the TCP MD5 Signature Option
RFC 2390	Inverse Address Resolution Protocol (obsoletes RFC 1293)
RFC 2403	Use of HMAC-MD5-96 within ESP and AH
RFC 2404	Use of HMAC-SHA-1-96 within ESP and AH
RFC 2405	ESP DES-CBC Cipher Algorithm with Explicit IV
RFC 2406	IP Encapsulating Security Payload (ESP)
RFC 2407	Internet IP Security Domain of Interpretation for ISAKMP
RFC 2409	Internet Key Exchange (IKE)
RFC 2410	NULL Encryption Algorithm and Its Use with IPsec
RFC 2427	Multiprotocol Interconnect over Frame Relay (obsoletes RFC 1294 and RFC 1490)
RFC 2451	ESP CBC-Mode Cipher Algorithms
VINES 4.11	BayRS works with the Banyan VINES 4.11 standard. BayRS Version 8.10 (and later) also supports VINES 5.50 sequenced routing.

Flash Memory Cards Supported

You use Personal Computer Memory Card International Association (PCMCIA) flash memory cards to store the software image and the configuration files in Bay Networks routers. Software images for BayRS 14.00 require 8 or 16 MB flash cards; however, you can store configuration files on 4 MB flash cards.

Table 10 lists the flash memory cards approved for use.

Table 10. Approved Flash Memory Cards

Size	Vendor	Part Number
4 MB	Advanced Micro Devices (AMD)	AMC004CFLKA-150
	AMP	797262-3
		797263-2
	Centennial	FL04M-20-11119
		FL04M-20-11138
	Epson	HWB401BNX2
	IBM	IBM1700400D1DA-25
	Intel	IMC004FLSAQ1381
8 MB	AMD	AMC008CFLKA-150
		AMC008CFLKA-200
		AMC008CFLKA-250
		AMC008DFLKA-150
		AMC008DFLKA-200
		AMC008DFLKA-250
	Centennial	FL08M-25-11119-01
		FL08M-15-11119-01
		FL08M-20-11138
		FL08M-20-11119-01
	Epson	HWB801BNX0
	Intel	IMC008FLSP/Q1422
	Centennial (Strata-Flash)	FL08-20-11736-J5-61

(continued)

Table 10. Approved Flash Memory Cards *(continued)*

Size	Vendor	Part Number
16 MB	Epson	HWB161BNX2
	Centennial (Strata-Flash)	FL16-20-11736-J5-61
32 MB	Centennial	FL32M-20-11119-67