Release Notes for BayRS Version 13.20

BayRS Version 13.20
Site Manager Software Version 7.20

BCC Version 4.20

Part No. 301151-D Rev 00
May 1999

NORTEL NETWORKS™

Bay Networks, Inc.
4401 Great America Parkway
Santa Clara, CA 95054

Copyright © 1999 Bay Networks, Inc.

All rights reserved. Printed in the USA. May 1999.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Trademarks

ACE, AFN, AN, BCN, BLN, BN, BNX, CN, FRE, LN, Optivity, PPX, Quick2Config, and Bay Networks are registered trademarks and Advanced Remote Node, ANH, ARN, ASN, BayRS, BaySecure, BayStack, BayStream, BCC, BCNX, BLNX, EZ Install, EZ Internetwork, EZ LAN, FN, IP AutoLearn, PathMan, RouterMan, SN, SPEX, Switch Node, and System 5000 are trademarks of Bay Networks, Inc.

Microsoft, MS, MS-DOS, Win32, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks, Inc. Software License Agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as "Software" in this Agreement). 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

Release Notes for BayRS Version 13.20

Tables

Preface

BayRS Version 13.20 is a software release that includes new features added since BayRS Version 13.10. These release notes contain guidelines for using BayRS Version 13.20.

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

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

If you purchased a Bay Networks service program, contact one of the following Bay 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 13.20

This document contains the latest information about Bay Networks® BayRS™ Version 13.20, including information on the following topics:

Upgrading to Version 13.20

To upgrade BayRS to Version 13.20, or to upgrade Site Manager software to Version 7.20, see *Upgrading Routers to BayRS Version 13.xx*, in your upgrade package. Also, read the following sections for additional upgrading information.

Upgrading FireWall-1 Configurations

To upgrade FireWall-1 in BayRS Version 13.20, complete the following 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, refer to *Using the Bay Command Console (BCC)*.

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

   When you upgrade to BayRS Version 13.20, once you boot your router, the Version 13.20 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 13.20, 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#
```

Once you are 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 need 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 if 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 security policy in the configuration file *drop_ftp* be installed on policy index number 1 on the router named *asn1*:

fw load ../conf/drop_ftp pol1@asn1

Preventing Spoofing with FireWall-1

You can configure FireWall-1 to eliminate the possibility of *spoofing*, that is, someone violating the firewall by sending a packet with a source address from within the network. To configure FireWall-1 to eliminate spoofing, complete the following steps:

1. **Make sure that each firewalled interface has a unique policy index number. For best results, make sure that each circuit has a unique policy index number.**

   For example, suppose your router has three Ethernet interfaces to LANs protected by the firewall and one frame relay synchronous firewalled connection that includes multiple PVCs. Each Ethernet interface must have a unique policy index number. You may assign the same policy index number to each of the frame relay PVCs if necessary, although configuring the interfaces in this way allows each frame relay interface to spoof the other frame relay interfaces.

2. **Enter the BCC show command, show firewall interfaces, to note the policy index number for each router circuit.**
3. **In the Check Point user interface, click on Manage Network Objects.**
4. **Highlight the defined router object (you may need to create a router) and click Edit.**
5. **Click on the Interfaces tab.**
6. **Click on SNMP Get. (Ignore the outdated pop-up message.)**
7. **Highlight a circuit and click on Edit.**
8. **In the Name field, type pol.**
9. **In the Num field, type the policy index number of the circuit (which you noted from the BCC show command in step 2).**
10. **Repeat steps 7 through 9 for each firewalled circuit.**

For more information about preventing spoofing, refer to your Check Point documentation.

Upgrading ATM Configurations

If you are upgrading from a BayRS version earlier than 12.20 and you defined log event traps for 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, but has been combined with the ATM entity (entity #78). Combining and reorganizing these entities resulted in changes to the ATM log event message numbers. New log events were added 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 World Wide Web, or on the BayRS Online Library Version 13.20 CD.

Upgrading L2TP Configurations

If you have a BayRS Version 12.10 configuration file that includes L2TP operating on a router using BayRS Version 13.20, 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 13.20, 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 13.20 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, 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 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, PPP, Point-to-Multipoint, or 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 the BCC Help File

The following information updates instructions relating to the BCC Help file mentioned in *Upgrading Routers to BayRS Version 13.xx*.

If you received a flash card with the BayRS 13.20 (BCC 4.20) image, it should also contain the BCC Help file, *bcc.help*. The BCC looks for this file name as soon as you enter the first **help** *<option>* command after booting the router using the new Version 13.20 image.

If the *bcc.help* file is not already on the default volume in the router, you must transfer it from the BayRS Version 13.20 software CD to that volume. The BCC Help file on the BayRS software CD has the name *bcc_help*. In the process of transferring that file to the router, be sure to rename it as *bcc.help*. (The Version 13.20 router software is not configured by default to recognize the file name *bcc_help*.)

Upgrading Static Forwarding Policy Filters

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*.

New Features

The following sections provide brief descriptions of the new features in BayRS Version 13.20.

BCC Support for Additional Protocols and Services

With Version 13.20, you can now configure these additional protocols and services using the BCC:

- DLSw (data link switching) over token ring, FDDI, and Ethernet
- GRE (Generic Routing Encapsulation)
- MPOA/NHRP (Multiprotocol Over ATM/Next Hop Resolution Protocol)
- Dial services compression
- Transparent bridging
- Spanning tree
- Source route bridging
- NAT (Network Address Translation)
- FireWall-1
- SDLC (Synchronous Data Link Control)
- LLC2 (Logical link control) over token ring, FDDI, and Ethernet
- VRRP (Virtual Router Redundancy Protocol)
- RADIUS
- DVMRP accept, announce, and unicast accept policies

BCC Enhancements

The BCC now checks user input for configurable parameter values, ensuring that new values are within allowable ranges.

BCC Multilevel Access

Multilevel access adds a third login level, that of operator, to the existing manager and user login levels of the BCC. With multilevel access, multiple users (each with a distinct user name, password, and privileges), can access the router simultaneously.

See *Using the Bay Command Console (BCC)* for more information.

FireWall-1 Enhancements

Version 13.20 supports BaySecure™ FireWall-1 on ATM interfaces.

Also, you can configure FireWall-1 using the BCC only; Site Manager support is no longer available. See "Upgrading FireWall-1 Configurations" on page -2 for instructions if you are upgrading FireWall-1 from a previous version.

See *Configuring BaySecure FireWall-1* for more information.

SNMP View-Based Access Control

You can now filter the information from an SNMP agent, thereby controlling your view of the network. In other words, you can specify what can or cannot be seen in a router's MIB tree by including or excluding any MIB object, attribute, or instance. You can also include or exclude access to a MIB subtree for traps and for the SNMP operations get, get-next, and set. This feature allows you to manage overlapping private address spaces. It also enables a service provider to allow two different customers to view statistics on a router discretely.

You configure SNMP view-based access control using either the Technician Interface or the BCC.

For more information, see the *BayRS Version 13.20 Document Change Notice*.

OSPF NSSAs

Version 13.20 includes support for OSPF (Open Shortest Path First) NSSAs (not so stubby areas). An OSPF NSSA is similar to an OSPF stub area except that, to a limited degree, an NSSA can import AS (Autonomous Systems) external routes. Like a stub area, an NSSA consumes less memory and CPU resources by preventing the flooding of AS external link-state advertisements (LSAs) into the area and by using default routing to external destinations. Yet unlike a stub area, an NSSA is more flexible because it can import external routes into an OSPF routing domain. Also, with the configuration of type 7 address ranges, an OSPF NSSA area border router can summarize external routes from the NSSA.

For more information, see *Configuring IP, ARP, RIP, and OSPF Services*.

Backup Gateways and Load Balancing for Bay Dial VPN Services

For situations that require high availability or traffic load balancing, you can now configure additional Dial VPN gateways for frame relay connections. In addition to the primary gateway for a tunnel user, you can configure a pool of up to 10 secondary gateways. You can configure Dial VPN to use these as backup gateways if the primary gateway fails. Alternatively, to improve traffic flow, you can specify load distribution mode, in which Dial VPN randomly distributes tunnel traffic among the secondary gateways in the pool. You configure backup or load distribution mode by setting TMS parameters in BaySecure Access Control (BSAC).

For more information, see *Configuring and Troubleshooting Bay Dial VPN Services*.

IP Security (IPsec)

In BayRS Version 13.20, IPsec (IP Security Services) supports Internet Key Exchange (IKE) as the default method to securely and automatically establish keying material for IPsec security associations (SAs). This eliminates the need for frequent manual reconfiguration, and thus creates a more secure environment.

In addition, the triple DES (3DES) encryption algorithm is now available as an option for added security.

For more information, see *Configuring IPsec Services.*

Priority Queuing Over ATM and HSSI Lines

You can now set the priorities for the traffic sent across an ATM or HSSI line interface using a process called protocol prioritization. The ability to prioritize traffic is important for an application that is time-sensitive and that requires a fast response.

For more information about protocol prioritization, see *Configuring Traffic Filters and Protocol Prioritization*.

Differentiated Services

BayRS now supports differentiated services for IP. Differentiated services is a network architecture that lets service providers and enterprise network environments offer varied levels of service for different types of data traffic. Instead of using the “best-effort” service model to ensure data delivery, differentiated services lets you designate a specific level of performance on a packet-by-packet basis.

For more information, see *Configuring Differentiated Services*.

PIM Sparse Mode

Version 13.20 includes support for Protocol Independent Multicast (PIM) -- Sparse Mode, which is defined in RFC 2362. PIM Sparse Mode is a multicast routing protocol that efficiently routes multicast traffic between members of multicast groups that are sparsely distributed across various regions of the Internet.

The BayRS implementation of PIM supports only sparse mode. PIM has the following characteristics:

- Routes with downstream members to join a shared tree by sending explicit join messages.
- Uses rendezvous points (RPs) for receivers to meet new sources. Sources announce their existence to RPs; receivers query RPs to find out about multicast sessions.

- Establishes a shortest path tree to create a data path between sources and receivers.

Note: The Bay Networks implementation of PIM supports sparse mode only.

For more information, see *Configuring IP Multicasting and Multimedia Services.*

HTTP Server Enhancements

For Version 13.20, the HTTP server feature has several enhancements, as described in the following sections.

Getting Help

HTTP Server windows that offer interactive features also offer a Help button. When you click on Help, you see a secondary window containing detailed information about the elements in that window.

You can optionally load these help files onto another server and configure the HTTP Server to use the address of that server as its base address.

Troubleshooting Features

New icons in the Trouble Shooting folder in the navigational frame let you ping a device on an IP, IPX or AppleTalk network to determine whether the device is operational.

The event log display contains hot links for each event. Click on the hot link to view a secondary window with the description of the particular event from the events database.

Administration Features

The administration functions let any user view the system date, time, and time zone information, and information about the files on each volume.

A person with operator access privileges can also change the date and time, reset a slot, and reboot the router using an image that is already loaded on a volume.

In addition to having the same privileges as the person with operator access privileges, the person with manager access privileges can load, copy, or delete files on the router and format and compact volumes.

For more information, see *Managing Routers Using the Web Server.*

ATM WAN SVCs

ATM now supports WAN SVCs, which enable the router to dynamically establish virtual circuits (VCs) when there is a need to exchange data packets. Each WAN SVC has a static mapping of ATM addresses to IP and IPX protocol addresses on the same ATM service record. The router brings down the WAN SVC after a configured inactive period of time.

For additional information and instructions on how to configure an ATM WAN SVC, see *Configuring ATM Services*.

Multicast Migration Tools

You can now configure a router to receive and send multicast traffic over nonmulticast (IGMP static configured) interfaces as well as interfaces running multicast protocols, such as DVMRP and MOSPF.

For more information, see *Configuring IP Multicasting and Multimedia Services*.

DVMRP Policies

In Version 13.20, there have been some minor modifications to the Site Manager parameters for configuring DVMRP policies. These changes improve usability, but do not affect the functionality of DVMRP policies.

ATM UNI 4.0 Support

ATM now supports Version 4.0 of the UNI signaling protocol standard, which specifies how the interface defines Service Specific Connection Oriented Protocol (SSCOP) frames. The ATM Forum Versions 3.0, 3.1, and 4.0 methods of defining SSCOP frames are incompatible.

You must assign the same protocol standard for both the router interface and the switch interface to which this interface connects.

For information about how to configure the same version of the UNI signal protocol standard that the switch interface uses, see *Configuring ATM Services*.

BGP-4 TCP MD5 Message Authentication

BGP-4 lets you configure the authentication of BGP messages by TCP MD5 signatures, in compliance with RFC 2385, “Protection of BGP Sessions via the TCP MD5 Signature Option.” With BGP-4 authentication enabled, a BGP speaker can verify that the BGP messages it receives from its peers are actually from a legitimate peer and not from a third party masquerading as a peer.

For more information, see *Configuring IP Exterior Gateway Protocols (BGP and EGP)*.

BGP-4 Confederations

The BGP-4 confederations feature can reduce the size and complexity of an IBGP mesh by breaking large autonomous systems into a confederation of smaller subautonomous systems. This division reduces the size of IBGP meshes and the complexity of the associated configuration management. Other autonomous systems view the confederation as a single autonomous system with the confederation ID as its AS number. BGP confederations are available only with BGP-4. The BGP-4 confederation feature complies with RFC 1965 and provides the following functions:

- Lets you configure a confederation ID on the router
- Implements new AS_PATH segment types
- Lets you configure new AS_PATH variables, AS_CONFED_SET and AS_CONFED_SEQUENCE, for specifying confederation parameters
- Implements correct AS_PATH setting and manipulation to neighboring autonomous systems that are within and outside the confederation.

For more information, see *Configuring IP Exterior Gateway Protocols (BGP and EGP)*.

RADIUS Enhancements

With BayRS Version 13.20, RADIUS supports vendor-specific attributes (VSAs) and dial-up services for authentication (dial-on-demand, dial backup, and bandwidth-on-demand).

For more information, see *Configuring RADIUS*.

DLSw RSVP Support

DLSw now supports the Resource Reservation Protocol (RSVP), RFC 2205. RSVP allows you to reserve bandwidth specifically for use by DLSw. The RSVP function is available only for DLSw Version 2.0 (unicast) and RFC 2166 (multicast) connections; it does not support RFC 1434 or 1795 connections.

For more information, see *Configuring DLSw Services*.

OSA-2 ATM Adapter Support for SNA Connectivity

You can now connect to IBM's Open System Adapter 2 (OSA-2) to establish SNA sessions (over ATM, token ring, or Ethernet) between clients and IBM hosts. The current implementation of the ATM OSA-2 adapter for SNA subarea supports only the LAN emulation service (LANE). Both token ring and Ethernet LANE are supported.

L2TP Framed Route Support and Other Enhancements

The L2TP (Layer 2 Tunneling Protocol) now includes support for framed routes. With framed-route support, the LNS (L2TP Network Server) does not have to use RIP (Routing Information Protocol) to learn all routes on a remote network. Instead, when a user dials in, the RADIUS server sends the LNS a framed route, which includes all the information the LNS needs to communicate with the remote user.

Also, with Version 13.20, it is possible to have up to 150 L2TP sessions concurrently running on a router interface (except on the AN® router, which has a maximum of 75). You can also now configure an AN or ARN™ router as an LNS.

For more information, see *Configuring L2TP Services*.

BN Console Slot Election

The console slot election feature enables you to specify Backbone Node (BN®) slots eligible to run the console interface. Based on a list of router slots that you specify, the software chooses the slot with the greatest amount of available free memory.

For more information, see the *BayRS Version 13.20 Document Change Notice*.

VRRP Enhancements

VRRP now includes support for IPX (Internet Packet Exchange) and IGMP-Relay (Internet Group Management Protocol).

FRE-4-PPC Processor for BN

BayRS Version 13.20 supports a FRE®-4-PPC processor module for the BN router. The FRE-4-PPC processor module supports the following FRE-4-PPC link modules:

- 1000BASE-SX Ethernet
- 1000BASE-LX Ethernet
- 10/100BASE-TX Ethernet
- 100BASE-FX Ethernet

For more information, see *Installing FRE-4-PPC Processor Modules in BN Platforms* and *Installing FRE-4-PPC Ethernet Link Modules in BN Platforms*.

Documentation Reorganization for ATM and IP

The documentation for the ATM and IP protocols is reorganized to reflect the increasing number of features for these services included with BayRS. The following documents, available on the online documentation CD and the Nortel Networks home page, comprise the document set for ATM and IP:

- *Configuring ATM DXI Services*
- *Configuring ATM Half-Bridge Services*
- *Configuring ATM Services*

- *Configuring MPLS Services*
- *Configuring MPOA and NHRP Services*
- *Configuring IP Multicasting and Multimedia Services*
- *Configuring IP, ARP, RIP, and OSPF Services*
- *Configuring IP Exterior Gateway Protocols (BGP and EGP)*
- *Configuring GRE, NAT, RIPSO, and BFE Services*
- *BCC Show Commands for IP Services*
- *Configuring IP Utilities*
- *Configuring IPv6 Services*

BCC Guidelines

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

Before using the BCC, refer to the following sections that list 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 us a message:

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

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. Each slot 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 an error message. In that case, use Site Manager instead of the BCC.

Interfaces Supported

You can use BCC commands to configure the following physical/virtual 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 1 through 5 on pages -22 to -29 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 (multiline 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 1 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.

Notes:

- 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.)
- Inserting a daughterboard into an AN base module redefines its module ID and board type.

Table 1 lists the AN and ANH board types.

Table 1. 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 1. 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 1. 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 2 lists the BLN and BCN board types.

Table 2. 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 2. 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 3 lists the ASN board types.

Table 3. 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 4 lists the ARN board types.

Table 4. 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 5 lists the System 5000 board types.

Table 5. 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

Note the following guidelines when using BayRS Version 13.20. These guidelines supplement the instructions in the Version 13.20 documentation set.

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 Bay Networks routers.

Fragment Tagging in Bootstrap Messages

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

To enable a Bay 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 Bay 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 Bay Networks router and the Cisco router to select the same RP.

IPsec 3DES Performance Considerations

IP Security (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 may 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 encryption and authentication algorithms you choose vary significantly in the amount of CPU resources required.

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) may cause the router to experience significant performance degradation under heavy traffic loads.

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

Renaming the FireWall-1 Redundant Management Scripts

Bay 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 on 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, you 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 Chapter 2 in *Configuring BaySecure FireWall-1*.

NAT Synchronous Not Operational

The *Configuring GRE, NAT, RIPSO and BFE Services* book includes instructions for configuring NAT synchronization. BCC show commands (**show nat peers** and **show nat summary**), TI commands, and the Site Manager NAT base group record log mask may display information about NAT synchronization. Please disregard this information; NAT synchronization is not operational.

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 Bay Networks router that communicates with the bandwidth broker must be operating with BayRS Version 13.20 software.

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

1. **Go to the Router Management Labs Web 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 will then 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

Starting with BayRS Version 13.10, you can view the event database on the World Wide Web and the BayRS Online Library Version 13.20 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 13.20 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. Bay 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 plan to migrate to a supported Solaris OS platform. Site Manager Version 7.20 is the last release that will ship with SunOS support. Site Manager releases later than 7.20 will not work with SunOS, but will continue to work with Solaris and other supported operating systems.

Year 2000 Compliance

BayRS Version 13.20 and Site Manager Software Version 7.20 are Year 2000 Compliance Certified by Bay Networks. They have successfully passed the Bay Networks Test Procedure, which tests conformance to the Bay Networks Year 2000 compliance definition. For more information, see the Bay Networks Year 2000 Web Site at *http://www.baynetworks.com/year2000/*.

Frame Relay Multilink Not Supported

Configuring Frame Relay Services provides information about multilink service and how to configure it using Site Manager. Please disregard this information; frame relay multilink is not supported in Version 13.20.

8 MB Flash Not Supported for BN Platform

The size of the software image for the FRE-1, -2, and -4 processor cards in the BN routers has approximately doubled with Version 13.20. Consequently, 8 MB flash cards are no longer supported for BN routers. The minimum flash card size is 16 MB for the BN platform. See “Flash Memory Cards Supported” on page -51 for a list of supported flash vendors.

Protocol Statistics for MPLS

The HTTP Server interface for Version 13.20 contains a folder icon for displaying Multiprotocol Label Switching (MPLS) statistics. The following information 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

AN/ANH and ARN Guidelines

Note the following operational 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 in BayRS Version 13.20. The ARN DSU/CSU supports network booting only over interfaces configured for 64 Kb/s Clear Channel service.

ARN Router Not a Supported DVS RADIUS Client

The ARN router is not a supported DVS RADIUS client.

BayRS Version 13.20 Flash Memory Requirements

BayRS Version 13.20 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 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.

IPsec Executable

To use the IPsec option, you must purchase a separate IPsec CD that contains the 40-bit (exportable DES), 56-bit (DES), or triple DES (3DES) cryptographic API executable (*capi.exe*) for the BayRS 13.20 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 13.20 Base Kernel

To use IPsec, you must use Image Builder to add an IPsec file to the BayRS 13.20 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 need to modify or add anything to Site Manager 7.20.

NAT Guidelines

Please observe the guidelines described in the following sections when configuring NAT.

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.

Deleting NAT from a Router

If you delete NAT from a router, all previously configured instances of static entries will remain in the router MIB. You can delete the instances using the Technician Interface.

Entering a Global Range

When you enter a global range, if the range is on the same subnet as the global interface, you must also enable Address Resolution Protocol (ARP) proxy on the global interface. If you do not enable ARP proxy on the global interface, any ARP messages to hosts that are mapped to addresses within the global range will not receive a reply. When you enable the ARP proxy, ARP uses the global interface’s MAC address for any hosts with global range addresses.

Outbound LAN Traffic Filters

When implementing outbound traffic filters for LAN protocols, note that in some configurations the filters may cause a decline in throughput performance. For LAN circuits where the forwarding rate of the router is critical, you should monitor the throughput performance after configuring outbound traffic filters. If you notice an unacceptable performance degradation, try using inbound traffic filters.

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 eventually 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 Version 13.20 supports the Strata-Flash card on AN, ANH, ARN, ASN, and BN routers. For full details about flash cards that BayRS 13.20 supports, see "Flash Memory Cards Supported" on page -52.

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 13.20 software.

To install WEP on a router, you must first add the WEP executable to your BayRS 13.20 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 13.20 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 need to modify Site Manager.

X.25 PVCs

BayRS Version 13.20 software supports X.25 PVCs for X.25 IPEX Gateway services only.

IPv6 Supported on ATM PVCs

BayRS Version 13.20 includes support for 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 three 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 (usually *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 may be able to use it as a direct replacement for the existing RADIUS dictionary. For more information, refer to 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 Bay Networks vendor-specific attributes. The Bay 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	Refer to
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

Be aware of the following limitations when using BayRS 13.20.

Restriction When 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.

Restriction if 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.

Restriction When 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.

Restriction When 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.

Restriction When 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 may restart.

Restriction When Virtual Channel Connections (VCCs) Become Inactive

On the ARE and 5782 MPE, BayRS 13.20 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.

Restriction When Performing Flash Compaction or Extensive File Management on ARE Module

We do not recommend that you perform a flash compaction or extensive file management on a busy or production ARE module. Doing so may cause a fault in the module.

Restriction When 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.

Restriction for SNMP View-Based Access Control

The SNMP view-based access control feature, described in the *BayRS Version 13.20 Document Change Notice*, includes the restriction described in this section.

Because of the way that SNMP works, the SNMP get-next function does not allow you to exclude an attribute and include subsequent attributes. When you exclude an attribute, all subsequent attributes will also be excluded. For example, if you have 6 attributes, and you exclude attribute 2, you are really excluding attributes 2 through 6. You will not be able to view attributes 2 through 6 and you will not be able to view these attributes.

You can, however, edit any individual attribute. That is, you can perform sets on attributes 3 through 6 even though you will not be able to view them.

You need to meet these conditions before the set can take place:

- You must include the first attribute.
- You must enter valid values in every field, despite the fact that these will not be set.

Site Manager will display an `SNMP set error` message because it will attempt to set all attributes.

The only set that will happen is the one for the included attribute.

Protocols Supported

BayRS Version 13.20 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 Packet Exchange (IPX)
- Internet Protocol (IP)
- Internet Protocol Version 6 (IPv6)
- IPsec Encapsulating Security Payload (ESP)
- IPv6 PPP Control Protocol (IPv6CP)
- Internet Stream Protocol (ST2)
- Layer 2 Tunneling Protocol (L2TP)

- Learning bridge
- Logical Link Control 2 (LLC2)
- Multi-Protocol Over ATM (MPOA)
- Multicast OSPF (MOSPF)
- Multiprotocol Label Switching (MPLS)
- 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 6 lists the Request For Comments (RFCs) and other standards documents with which Version 13.20 complies. BayRS Version 13.20 may support additional standards that are not listed in this table.

Table 6. Standards Supported by Version 13.20

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 6. Standards Supported by Version 13.20 *(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 6. Standards Supported by Version 13.20 *(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
RFC 1294	Multiprotocol Interconnect over Frame Relay (obsoleted by RFC 1490)
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
RFC 1321	MDS Digest Algorithm
RFC 1323	TCP Extensions for High Performance

(continued)

Table 6. Standards Supported by Version 13.20 *(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)
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)
RFC 1764	PPP XNS IDP Control Protocol (XNSCP)

(continued)

Table 6. Standards Supported by Version 13.20 *(continued)*

Standard	Description
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 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
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 13.20 require 8 or 16 MB flash cards; however, you can store configuration files on 4 MB flash cards.

Table 7 lists the flash memory cards approved for use.

Table 7. 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
16 MB	Epson	HWB161BNX2
	Centennial (Strata-Flash)	FL16-20-11736-J5-61
32 MB	Centennial	FL32M-20-11119-67