BayRS Version 15.7.0.0

Part No. 308663-15.7 Rev 00
July 2006

600 Technology Park Drive
Billerica, MA 01821-4130

Release Notes for BayRS Version 15.7.0.0

NORTEL

Nortel Networks Inc. Software License Agreement

This Software License Agreement ("License Agreement") is between you, the end-user ("Customer") and Nortel Networks Corporation and its subsidiaries and affiliates ("Nortel Networks"). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

"Software" is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

1. Licensed Use of Software. Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment ("CFE"), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer's Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

2. Warranty. Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided "AS IS" without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER'S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. General

a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

b. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.

c. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.

d. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.

e. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.

f. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

Contents

Tables

Preface

Nortel Networks* BayRS Version 15.7.0.0 is a software release that includes new features and fixed anomalies since BayRS Version 15.6.0.0. These release notes contain guidelines for using BayRS Version 15.7.0.0.

Hard-Copy Technical Manuals

You can print selected technical manuals and release notes free, directly from the Internet. Go to the www.nortel.com/support URL. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe* Acrobat Reader* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader.

How to get help

This section explains how to get help for Nortel products and services.

Getting help from the Nortel web site

The best way to get technical support for Nortel products is from the Nortel Technical Support web site:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins

- search the Technical Support web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the phone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support web site, and you have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following web site to obtain the phone number for your region:

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

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

Release Notes for BayRS Version 15.7.0.0

This document contains the latest information about Nortel Networks BayRS Version 15.7.0.0, including information about the following topics:

New Revision of V.34 Modem Adapter and Console Modem Modules

Nortel Networks is now shipping Revision 3 of the V.34 Modem Adapter Module and the V.34 Console Modem Module. These V.34 modules, which function the same way as earlier revisions, are supported on the following routers:

- ARN
  - — V.34 Modem Adapter Module (order nos. CV0004005 and CV0011005)
  - — V.34 Console Modem Module (order nos. CV0004020 and CV0011020)
- Passport 5430 and Passport 2430: V.34 Modem Adapter Module (order no. CV0011048)

  For the Passport 5430, this module can also be used as a console modem if you install it in the WAN adapter slot labelled “Remote Console.”

The new V.34 Modem Adapter Module and V.34 Console Modem Module require the following versions of diagnostic code (Table 1).

Table 1. Minimum Required Version of Diagnostic Code for V.34 Modules, Rev. 3

Platform	Diagnostic Version
ARN	2.26
Passport 2430	2.08
Passport 5430	1.18

Note: If the V.34 module in the Passport 5430 is used as a console modem, the router must be running BayRS Version 15.6.0.0 or later. If the V.34 module in the Passport 5430 is used as a modem adapter, no BayRS software restrictions apply. (The Passport 2430 and the ARN require no BayRS version upgrade to use the new V.34 modules.)

Upgrading to Version 15.7.0.0

To upgrade BayRS to Version 15.7.0.0, see *Upgrading Routers to BayRS Version 15.x*, in your upgrade package. In addition, read the following sections.

Minimum Memory Requirements for Version 15.7.0.0

To run BayRS Version 15.7.0.0, your router must have the minimum amount of system memory specified in Table 2.

Table 2. Minimum System Memory Required for Version 15.7.0.0

Platform	Minimum System Memory (MB)
ARN	32
ASN	32
Passport 2430	32
Passport 5430	64
BLN/BCN[a]	64

a. Includes all processors: FRE2-060/060E, FRE4, and ARE

To accommodate the Version 15.7.0.0 image, flash cards must meet the requirements specified in Table 16 on page 41.

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 CD, or on the World Wide Web at this URL:

http://www25.nortelnetworks.com/library/tpubs/events/

Cell Scrambling Default Changes for DS1/E1 and DS3/E3

For pre-15.*x* versions of BayRS, the default for the cell scrambling parameter is set to On for DS1/E1 and DS3/E3 modules. However, the default for this parameter has been changed to Off for all BayRS 15.*x* versions. If you are upgrading from a pre-15.*x* version of BayRS (for example, Version 14.20), you will need to set this parameter to On to activate cell scrambling.

See *Configuring ATM Services* for additional information about setting this parameter using the BCC or Site Manager.

Upgrading DVMRP Configurations

In BayRS Version 15.1.0.0 and later, the default values for two DVMRP timer parameters have been changed to conform with the latest RFC for DVMRP (draft-ietf-admire-dvmrp-v3-10). Table 3 lists the parameters with their old and new default values.

Table 3. DVMRP Parameter Defaults Changed

Parameter Name		Default Value (in seconds)	
Site Manager	**BCC**	**Earlier Than 15.1.0.0**	**Version 15.1.0.0 and later**
Garbage Timeout	unconfirmed-route-timeout	340	260
Route Expiration Timeout	route-expiration-timeout	200	140

DVMRP timers must be the same throughout the network. Therefore, if your DVMRP network changes—for example, if you add a DVMRP router running Version 15.1.0.0 (or later) to the network, or if you create a Version 15.1.0.0 (or later) configuration file that contains DVMRP— make sure that the values for the timer parameters match the ones already configured for the network as a whole.

Upgrading FireWall-1 Configurations

Complete the following steps only if you are upgrading Check Point* FireWall-1* from a BayRS version earlier than 13.20. If you are running FireWall-1 from BayRS Version 13.20 or later, you **do not** need to complete these steps during your upgrade to BayRS Version 15.7.0.0.

Note: FireWall-1 is not supported on the Passport* 2430 and Passport 5430 platforms.

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 15.7.0.0, once you boot your router, the Version 15.7.0.0 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 15.7.0.0, 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 IP Route Filters

If you have configured IP route filters and then disabled those filters (rather than deleted them), when you upgrade to Version 15.7.0.0 from a version earlier than 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 may want to delete them before you upgrade BayRS to Version 15.7.0.0.

Upgrading L2TP Configurations

If you have a BayRS Version 12.10 configuration file that includes L2TP operating on a router using BayRS Version 15.7.0.0, 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 15.7.0.0, 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 15.7.0.0 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 OSPF maximum transmission unit (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 14.00 and later comply with RFC 2328, which requires the OSPF MTU size feature.

Upgrading IGMP 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 or later. 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 Quad Serial PMC Module Supplement for Passport 5430

The *Quad Serial PMC Module Supplement* for the Passport 5430 has been revised to correct an error and is now posted to the Nortel Networks Technical Support site. Consult the revised version of this book (Part No. 311905-B Rev 00), not the earlier version that is on the BayRS Online Library CD.

To obtain this revised document, go to the Nortel Networks Technical Support URL www.nortel.com/support and locate BayRS Routers in the product list. Select “Multiprotocol Router 5430” and then “Documentation.”

New Features

The following sections provide brief descriptions of the new features in BayRS Version 15.7.0.0. These features are as follows:

Secure Shell (SSH) and Secure FTP (SFTP)

BayRS now includes a Secure Shell (SSH) feature. The SSH supports a limited subset of the features of the SSH and Secure File Transfer Protocol (SFTP) servers. A Secure Shell (SSH) server provides a secure communication channel for the administrator to manage the router. An SFTP server transfers router software images to the box over an insecure network.

The SSH feature allows others using the SSH program to log into and maintain the Bay RS router over the networks. It provides strong authentication and a secure communication channel over the network. User authentication is based on password authentication and any other existing authentication mechanisms supported in the product. The traffic is encrypted, therefore intermediate hosts cannot intercept clear text username/password and other confidential data.

The SSH service interoperates with publicly available SSH clients using SSH protocol version 2. There can be up to 5 concurrent SSH sessions.

You can use either the Bay Command Console (BCC) or Site Manager to enable or disable SSH and SFTP on the router. BayRS disables SSH and SFTP by default.

For more information about the SSH feature, see Chapter 11, "Configuring IP, ARP, RARP, RIP, and OSPF Services," in the *BayRS Version 15.7.0.0 Document Change Notice*.

For a list of SSH event messages, see Chapter 26, "Event Messages for Routers," in the *BayRS Version 15.7.0.0 Document Change Notice*.

For a description of Site Manager parameters for SSH, see Appendix A, "Site Manager Parameters," in the *BayRS Version 15.7.0.0 Document Change Notice*.

OSPF MD5 Authentication

BayRS now provides Open Shortest Path First (OSPF) Message Digest 5 (MD5) authentication for secure message interchange between OSPF neighbors. Previously, with OSPF, you could use plain text or simple password authentication only. OSPF MD5 authentication provides tighter security because it uses cryptography.

OSPF supports both plain text and Message Digest 5 (MD5) authentication. With BayRS Version 15.7.0.0, and OSPF Version 2, you can configure authentication by area or by interface. This is implemented as per Request for Comment (RFC) 2328 for OSPF Version 2.

The OSPF MDF5 authentication feature allows you to:

- Define an MD5 signature for OSPF peers.
- Configure authentication and secret keys by area.
- Apply area-defined keys to individual interfaces.
- Enable/disable authentication on a per-interface basis, including virtual interfaces. At any one time, a configuration can have authentication enabled for some OSPF peers and disabled for others.

You can use Site Manager, Bay Command Console (BCC), or the Technician Interface (TI) Secure Shell to configure OSPF MD5 authentication.

For more information, see Chapter 11, "Configuring IP, ARP, RARP, RIP, and OSPF Services," in the *BayRS Version 15.7.0.0 Document Change Notice*.

For a list of event messages associated with the OSPF MD5 authentication feature, see Chapter 26, "Event Messages for Routers," in the *BayRS Version 15.7.0.0 Document Change Notice*.

Monitoring Circuitless IP Addresses using SNMP

BayRS now collects MIB statistics for circuitless IP addresses. This allows you to monitor these types of addresses on a router using an SNMP application. This enhancement makes it easier to monitor these statistics on the router.

A circuitless IP address can now be associated with an IfEntry in the Management Interface Base (MIB). Therefore, statistics about the circuitless IP address are now available in the MIB. These MIB statistics are automatically enabled when you configure and enable Circuitless IP.

To browse the MIB objects for circuitless IP addresses, use a network management application that uses the Simple Network Management Protocol (SNMP). Examples of these types of management applications are, the Nortel Site Manager, or Optivity Network Management System.

For more information, see Chapter 11, "Configuring IP, ARP, RARP, RIP, and OSPF Services" in the *BayRS Version 15.7.0.0 Document Change Notice*.

DSQMS Rate Limiting

BayRS now allows you to limit the traffic rate that exits an Ethernet interface running Differentiated Services Queue Management and Scheduling (DSQMS). This is useful for a wide area network (WAN) that uses external DSL or Cable modems connected to the BayRS router over an Ethernet interface. The link speed of these modems is typically less than 2Mbps, slower than the connected Ethernet interface. By limiting the maximum traffic rate on the Ethernet interface you can avoid exceeding the bandwidth capacity of the WAN.

You can use Site Manager, Bay Command Console (BCC), or the Technician Interface (TI) Secure Shell to configure DSQMS Rate Limiting.

This enhancement for rate limiting is supported on 10Mbps, 10/100Mbps and 100Mbps Ethernet interfaces on all supported BayRS router platforms.

BayRS 15.4.0.0 introduced the DSQMS Line Speed parameter to make DSQMS queue calculations configurable. The default for DSQMS Line Speed was 1.25 Mb/s (megabits per second) for all versions prior to version 15.7.0.0. BayRS 15.7.0.0 adds the additional role of DSQMS rate limiting for this parameter and changes the default value to 0 Mb/s which disables DSQMS rate limiting.

For BayRS versions 15.4.x, 15.5.x and 15.6.0.0, DSQMS Line Speed is a single-purpose parameter which only supports DSQMS queue calculations. If the DSQMS Line Speed parameter is set to the default of 1.25 Mb/s and you upgrade to 15.7 from any of these versions, the upgrade resets the prior default (1.25 Mb/s) to the new default of 0 Mb/s (disabled). If the DSQMS Line Speed parameter is set to any value other than the original default of 1.25 Mb/s, the upgrade retains the existing value prior to the upgrade.

The default value for DSQMS Line Speed for BayRS versions 15.6.1.0, 15.6.1.1, and 15.6.2.0 is 1.25 Mb/s. Since BayRS 15.6.1.0, DSQMS Line Speed has been a dual-purpose parameter supporting both DSQMS queue calculations and rate limiting. Upgrades to 15.7 from any of these BayRS versions will retain the DSQMS Line Speed value that existed prior to the upgrade. As a result, BayRS 15.7 will base DSQMS queue calculations on the existing value retained during the upgrade.

Rate limiting is independent of the settings of other MIB attributes.

For more information, see Chapter 8, “Configuring Ethernet, FDDI, and Token Ring Services” in the *BayRS Version 15.7.0.0 Document Change Notice*.

Site Manager support on Windows XP SP2

BayRS now delivers Site Manager support on Windows XP Service Pack 2. Windows XP now joins Windows NT* Version 4.0 and Windows* 2000 as supported Windows operating systems for Site Manager. Site Manager for Windows XP SP2 operates with all supported BayRS router platforms.

For more information, see “Site Manager System Requirements” in the *Release Notes for Site Manager Software Version 15.7.0.0*

Known Anomalies

The following anomalies exist for BayRS 15.7.0.0. Nortel Networks aims to resolve these anomalies in an upcoming release.

Circuitless IP

Anomaly: SNMP monitoring of Circuitless IP does not work properly if Circuitless IP Gate (soloist) reinitializes on another slot.

ID: Q01367118

Description: Monitoring Circuitless IP using SNMP does not work properly if Circuitless IP Gate (soloist) reinitializes on another slot. This is because the ifIndex changes whenever CIP reinitializes on another slot of a multi-slot router.

Anomaly: Disabling a Circuitless IP address causes the ifIndex associated with Circuitless IP to not appear when you monitor the MIB using SNMP.

ID: Q01367022

Description: If you disable a Circuitless IP address the ifIndex associated with Circuitless IP disappears instead of displaying a down status as it should. Therefore SNMP monitoring returns no value for ifAdminStatus when you monitor the MIB.

Hi/fn LZS Compression

The following known anomaly exists for Hi/fn* LZS* Compression operating on BayRS routers:

Anomaly: Establishing the full packet rate at a high line speed is not possible with Hi/fn LZS Compression configured on the Passport 2430, particularly with small packet sizes.

ID: Q00723924

NAT

Anomaly: Bidirectional NAT is not functional if you use a Passport 2430 as the NAT router.

ID: Q00064004-04

Description: The Passport 2430 router is not supported as a NAT router for bidirectional NAT.

Workaround: For BayRS Version 14.20 or later, do *not* use the Passport 2430 router as a NAT router with bidirectional NAT configured.

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.

BCC and BayRS Compatibility

Starting with BayRS Version 14.00, the BCC software version number matches that of BayRS. For example, the version for both the BCC and BayRS is 15.7.0.0. We have made this change to help you align versions of the BCC with versions of BayRS.

Using the source Command to Configure a Router

You must use the **source** command to configure a router from a command file. *Do not* cut and paste the output of the BCC **show config** command directly into the BCC. Such an attempt to configure the router will cause the router to fault.

To use the output of the **show config** command to configure a router, save the output in a text file and then use the BCC **source** command to import the file into device memory. For complete information about using the **source** command to configure the router, see *Using the Bay Command Console (BCC)*.

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.

Creating FTP from the BCC

If you create FTP on the router using the BCC, then delete it and re-create it, the BCC faults. You must restart the BCC and create FTP on the router again.

Setting the Impedance Value for the Passport 2430

The Passport 2430 can accommodate either BNC (requires 75 ohm impedance) or RJ45 (requires 120 ohm impedance) connectors. You can use the BCC to set the impedance-value attribute to either 75 ohms or 120 ohms.

To set the impedance value on the FE1 interface, go to the FE1 prompt (for example, **box; fe1**) and enter:

impedance-value *<value>*

value is one of the following:

rj45-120-ohms (default)
bnc-75-ohms

For example, the following command sets the impedance value to 75 ohms for this interface on the router:

```
fe1/1/1# impedance-value bnc-75-ohms
fe1/1/1#
```

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 ARN, ASN, Passport 2430, Passport 5430 and BN platforms including ARE, 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 ring15.7.0.0
- Virtual (referred to in Site Manager as Circuitless IP)

Table 4 through Table 8 on pages 19 through 24 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
- DSQMS
- DVMRP (including accept and announce policies)
- 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
- MD5
- NAT
- NHRP
- NTP
- OSPF (including accept and announce policies and MD5 authentication)
- 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

Table 4 through Table 8 identify the board type parameter values displayed by the BCC.

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.

ARN Board Types

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

Table 4. BCC Board Types: ARN Modules *(continued)*

BCC Board Type	Technician Interface or MIB Module ID	Description
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
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
arntrtsync	8880	ARN Token Ring and Tri-Serial Expansion Module
arntsync	8848	ARN Tri-Serial Port Expansion Module

ASN Board Types

Table 5 lists the ASN board types.

Table 5. 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

Table 5. BCC Board Types: ASN Modules *(continued)*

BCC Board Type	Technician Interface or MIB Module ID	Description
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

BLN and BCN Board Types

Table 6 lists the BLN* and BCN* board types.

Table 6. 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

Table 6. BCC Board Types: BLN and BCN Modules *(continued)*

BCC Board Type	Technician Interface or MIB Module ID	Site Manager Model Number	Description
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
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

Table 6. BCC Board Types: BLN and BCN Modules *(continued)*

BCC Board Type	Technician Interface or MIB Module ID	Site Manager Model Number	Description
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

Passport 5430 Board Types

Table 7 lists the Passport 5430 board types.

Table 7. BCC Board Types: Passport 5430 Modules

BCC Board Type	Technician Interface or MIB Module ID	Description
arndcsu	8768	56/64K DSU/CSU Module
arnfe1	8780	E1/FE1 DSU/CSU Adapter Module
arnft1	8776	T1/FT1 DSU/CSU Adapter Module
arnisdns	8784	ARN ISDN BRI S/T Adapter Module
arnisdnu	8800	ARN ISDN BRI U Adapter Module
arnssync	8736	ARN Serial Adapter Module
arnv34	8752	ARN V34 Modem Module
ds1e1atm	8160	DS1/E1 ATM
ds3e3atm	8161	DS3/E3 ATM
fbrmbdfen	8000	FBR Ethernet Module
pmcqsync	8321	Quad Serial PMC Module

Passport 2430 Board Types

Table 8 lists the Passport 2430 board types.

Table 8. BCC Board Types: Passport 2430 Modules

BCC Board Type	Technician Interface or MIB Module ID	Description
arndcsu	8768	56/64K DSU/CSU Module
arnfe1	8780	E1/FE1 DSU/CSU Adapter Module
arnft1	8776	T1/FT1 DSU/CSU Adapter Module
arnisdns	8784	ARN ISDN BRI S/T Adapter Module
arnisdnu	8800	ARN ISDN BRI U Adapter Module
arnmbsfetx	8728	10BASE-TX Second Ethernet Module
arnssync	8736	ARN Serial Adapter Module
arnv34	8752	ARN V34 Modem Module

Technician Interface Guidelines

The Technician Interface is an alternative command-line interface for configuring Nortel Networks devices. Before using the Technician Interface, see the following guidelines.

Disabling a Protocol Using the Technician Interface Command Only

Do not use the Technician Interface to disable a protocol via a MIB set to the wfProtocols MIB; this procedure can cause unexpected results. If you want to use the Technician Interface to disable a protocol, execute the **disable** command. You can also disable protocols using Site Manager or the BCC.

show ip routes Displays Partial Information in the Technician Interface

For a router configuration that includes IP equal-cost routes, the Technician Interface **show ip routes** command displays partial information only.

When using the Technician Interface, you must use the following command to retrieve all equal-cost routes and show the complete routing table information:

ip routes -A

General Guidelines

The following guidelines supplement the instructions in the BayRS 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.
- Site Manager configuration files that contain the / (forward slash) character in any of the ASCII text inputs (for example, Unnumbered CCT Name) cause an error when viewed in the BCC using the **show config -all** command. This error halts printing of the text parameter at the / character and displays the message `"Too many BCC ID values"` at the end of the display. To prevent this problem, do not use the / character when entering ASCII text for parameters in Site Manager.

ARN Guidelines

Follow these guidelines when using ARN routers.

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.

ARN Router Not a Supported DVS RADIUS Client

The ARN router is not a supported DVS RADIUS client.

ATM Guidelines

Follow these guidelines when configuring ATM:

ATM Half Bridge Support

BayRS supports ATM Half Bridge (AHB).

Note: ATM Half Bridge (AHB) is *not* supported on either the Passport 2430 or Passport 5430.

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.

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.

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.

Aggregate Limitations for Sustainable Cell Rate

The *aggregate* sustainable cell rate (SCR) for all PVCs configured should not exceed 353207 cells per second for ARE OC-3 SONET/SDH ILI pairs. It is advisable to set SCR to less than that to ensure there is sufficient bandwidth for any SVCs that may also be configured on this interface. The SCR is set at the Xmit Sustainable Cell Rate (cells/s) parameter using Site Manager and at the **scr** parameter using the BCC.

ATM Routing Engine Performance and Scaling for PVC Environments

The results in Table 9 and Table 10 reflect the performance of the ARE as the number of PVCs increased using the following PVC access methods, respectively:

- ATM Group Mode: multiple PVCs per service record
- ATM Direct Mode: single PVC per service record

These ARE performance figures are based on unidirectional 128-byte UDP traffic to ensure that each PVC shared an equal amount of load. All PVC configurations were tested using one ATM slot with an OC3-MM interface (155 Mb/s).

Note: Performance results may vary from router to router depending on how your network is configured.

ATM Group Mode Service Record

Table 9 lists the maximum number of PVCs that could be configured at the specified throughput rate using the ATM group mode access method.

Table 9. ATM Group Mode Service Record

Throughput Rate	Maximum Number of PVCs Tested
90 Mb/s	100

ATM Direct Mode Service Record

Table 10 lists the maximum number of PVCs that could be configured at the specified throughput rate using the ATM direct mode access method.

Table 10. ATM Direct Mode Service Record

Throughput Rate	Maximum Number of PVCs Tested
90 Mb/s	20
65 Mb/s	40
45 Mb/s	60
30 Mb/s	80 to 100

Setting Buffer Sizes and Global/Local Memory

BayRS Router Buffer Sizes and Options

Table 11 lists the default buffer sizes for BayRS routers and indicates whether or not buffers can be resized and to what sizes they can be set. The table also indicates whether global/local memory allocation (memory carving) is available by router, as configured.

For more information see, “Setting Buffer Sizes on Specified Routers” on page 29 and “Allocating Global/Local Memory on BayRS Routers” on page 30.

Table 11. BayRS Router Buffer Sizes and Options

Router	Default Buffer Size	Set Buffer Size?	Set Local/Global Memory?
BN/FRE2-040	5 KBs	No	Yes
BN/FRE2-060	5 KBs	No	No
BN/FRE2-060E	5 KBs	No	No
BN/FRE4	5 KBs	No	No
BN/ARE	10 KBs	Yes - 5, 6, 7, 8, or 9 KBs	No
ARN	1824 bytes	Yes - 4800 bytes	No
ARN with token ring	4800 bytes	No	No
ASN	5 KBs	No	Yes
Passport 2430	5 KBs	No	No
Passport 5430	5 KBs	No	No

Setting Buffer Sizes on Specified Routers

You can set buffer sizes on the following BayRS routers by setting a MIB variable using the Technician Interface:

- BN/ARE
- Non-Token-Ring ARN Routers

By default, ARN routers (*without* token ring modules installed) initialize with a buffer size of 1824 bytes, which prevents these routers from accepting packets larger than 1824 bytes. To allow the non-token-ring ARN router to accept larger packets, you can increase the buffer size by setting the MIB variable wfKernCfgParamEntry.wfKernCfgParamBufSize to 4800. You can also increase the buffer size for the BN/ARE using this procedure.

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 for a non-token ring router:

```
set wfKernCfgParamEntry.wfKernCfgParamDelete.1 1
set wfKernCfgParamEntry.wfKernCfgParamBufSize.1 4800
commit
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
```

Allocating Global/Local Memory on BayRS Routers

You can change the default memory allocation (between global and local) on the following routers:

- ASN (flash-based only)
- BN (FRE2-040 only)

You can use either Site Manager or Technician Interface to allocate global/local memory on these routers:

- Site Manager: Select Administration > Kernel Configuration option
- Technician Interface: Enter **set** command for wfKernCfgParamEntry object

Note: This "memory carving" feature is *not available* on the ARN, Passport 2430, Passport 5430, BN (with FRE2-060, FRE2-060E, or FRE4) with VNR (5782) configured.

Embedded Web Server Guidelines

Follow these guidelines when using the embedded web server:

Using the 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.

Accessing the Embedded Web Server Using 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.

BGP Guideline

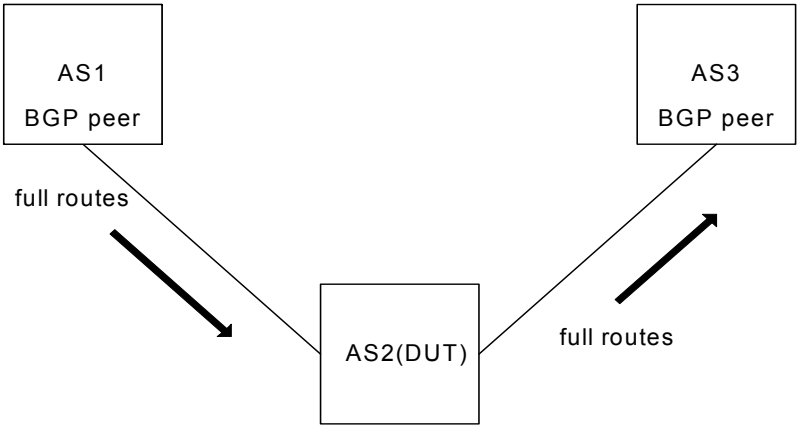
Currently, as many as 125,000 Internet routes can be accepted into the BGP and IP RTM route tables. As a result, the router may fault when the available memory is less than what is required to operate the router. The memory available to operate the router can also be affected by the following additional factors:

- How extensively the router is configured
- Amount of memory of the processor on which the BGP soloist is running

Figure 1 illustrates the tested configuration where:

- Router AS2 (DUT) BGP accept policy accepts all BGP routes from AS1.
- Router AS2 (DUT) BGP announce policy announces all BGP routes to AS3.

Figure 1. BGP Configuration Tested



Memory requirements are based on performance statistics gathered with BGP configured while using a FRE2-060, ARE, FRE4, and Passport 5430 system processor. You can use the statistics in Tables 12 through 15 as guidelines to determine how much memory is required on a particular BGP soloist slot. If you plan to accept all Internet routes into the BGP and IP RTM route tables, you should use processors with 128 MB of memory:

- BN platform: 128 MB FRE4 processor
- Passport 5430: 128 MB of memory in the system processor

Tables 12 through 15 provide the memory levels on the BGP soloist slot on AS2 with:

- Zero routes
- All Internet routes in the BGP table only
- All Internet routes in the BGP table and also in the IP RTM
- Impact on memory levels change when the BGP peer is disabled/enabled

Table 12. BGP Memory Levels - ARE

BGP soloist slot	Internet routes	Number of peers	Local memory BGP soloist slot	Global memory	Total memory
ARE	~125000	2	64MB	6MB	70 MB
		Total memory available	Memory used	Memory free	
	After boot (no routes)	61.00 MB	3.08 MB	57.92 MB	
	Full routes (BGP table only)		22.59 MB	38.41 MB	
	Full routes (also in IP RTM)		44.18 MB	16.82 MB	
	Disable remote peer =		44.81 MB	16.19 MB	
	Enable remote peer =		50.50 MB	10.50 MB***	
	***(Additional memory may be consumed when bouncing all routes)				

Table 13. BGP Memory Levels - FRE2-060

BGP soloist slot	Internet routes	Number of peers	Local memory BGP soloist slot	Gobal memory	Total memory
FRE2-060	~125000	2	48 MB	16 MB	64 MB
		Total memory available	Memory used	Memory free	
	After boot (no routes)	45.39 MB	3.32 MB	42.07 MB	
	Full routes (BGP table only)		22.30 MB	23.08 MB	
	Full routes (also in IP RTM)		42.99 MB	2.39 MB	
	Disable remote peer = local router faults with out of memory				

Table 14. BGP Memory Levels - FRE4

BGP soloist slot	Internet routes	Number of peers	Local memory BGP soloist slot	Global memory	Total memory
FRE4	~125000	2	128 MB	16 MB	144 MB
		Total memory available	Memory used	Memory free	
	After boot (no routes)	124.88 MB	3.04 MB	121.84 MB	
	Full routes (BGP table only)		22.58 MB	102.30 MB	
	Full routes (also in IP RTM)		55.65 MB	69.23 MB	
	Disable remote peer =		52.69 MB	72.19 MB	
	Enable remote peer =		57.77 MB	67.11 MB***	
	***(Additional memory may be consumed when bouncing all routes)				

Table 15. BGP Memory Levels - Passport 5430

BGP soloist slot	Internet routes	Number of peers	Local memory BGP soloist slot	Global memory	Total memory
5430	~125000	1	64 MB	64 MB	128 MB
		Total memory available	Memory used	Memory free	
	After boot (no routes)	60.42 MB	4.15 MB	56.27 MB	
	Full routes (BGP table only)		23.75 MB	36.67 MB	
	Full routes (also in IP RTM)		44.63 MB	15.79 MB	
	Disable remote peer =		45.94 MB	14.48 MB	
	Enable remote peer =		51.11 MB	9.31 MB***	

***(Additional memory may be consumed when bouncing all routes)

Dial Services Guideline

Dial backup services do not stay up on a Passport 2430 or ARN with an FT1 line configured for Bay Standard PPP protocol unless you first enable Remote Loopback Detection on the logical line. See Chapter 8, "Configuring FT1 Services," in the guide *Configuring WAN Line Services* for more information about enabling remote loopback detection.

DLSw Guideline

To establish connectivity for NetBIOS clients where DLSw is configured and attached to a switched environment, enter the following command string using the Technician Interface:

set wfLlcInterfaceEntry.24.<*circuit number*> **2;commit**

Within your set command you must specify the Ethernet <*circuit_number*> on the DLSw router where the clients are attached. You should also set the value for the MIB attribute to "2" to force the encapsulation of broadcast packets in the token ring format.

MPLS Guideline

BayRS does not support Multiprotocol Label Switching (MPLS). The former implementation of MPLS in BayRS (Versions 13.10 through 15.1.0.0) was based on an early draft of the specification developed by the IETF MPLS working group. This implementation has been removed from BayRS Because it was not compliant with RFC 3031 and did not interoperate with standard MPLS implementations.

NAT Guidelines

Follow these guidelines 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.

ISP Mode Not Supported by NAT

NAT does not support the ISP mode feature. ISP mode is a BayRS global IP parameter that allows you to enable the BGP soloist and disable IP forwarding caches. By default, ISP mode is disabled in BayRS.

Configuring Bidirectional NAT

For multidomain NAT to work, in addition to configuring bidirectional NAT on the router, you must:

1. Configure RIP2 on the NAT router interfaces and on each router with which the NAT router will be exchanging routing updates. Otherwise, you must configure static routes or a combination of RIP2 and static routes.
2. Install Domain Name System (DNS) server on a machine that is running UNIX or Windows NT and that has access to the NAT router. DNS server software is available from third-party suppliers and may be included with your operating system software.
3. Configure BayRS DNS proxy on each interface of a NAT router to be used for dynamic bidirectional translation. You do not need to configure DNS proxy for a static bidirectional network address translation.

4. Configure BayRS DNS client on each device that will be initiating traffic in the domains of your multidomain NAT configuration.

Protocols/Configurations Not Supported by Bidirectional NAT

- OSPF
- BGP
- IPsec on the same interfaces configured for bidirectional NAT
- BayRS ECMP

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, the OSPF backup soloist feature is no longer supported.
- 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.
- When OSPF is configured on a synchronous PPP interface using Site Manager, the interface type is set to Point-to-point rather than to the actual default, Broadcast.
- When an OSPF routing table contains two routes with the same network number (LSID), and one of the routes is unreachable and the other route has a 32-bit network mask, only the route with the 32-bit network mask will appear when you enter the **show ospf lsdb** command in 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 that you 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, RARP, RIP, and OSPF Services* for more information about these commands.

Interoperability with Non-Compliant Implementations of PIM

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

Note: The term "non-compliant router" is used in the following sections to indicate routers (such as Cisco* routers) that run implementations of PIM that do not comply with all elements of RFC 2362.

Nortel Networks routers can be configured for compatibility with non-standard implementations of PIM at the RFC2362 Non-Compatibility parameter using Site Manager. For additional information see "Enabling and Disabling Router Compatibility with RFC 2362" in *Configuring IP Multicasting and Multimedia Services*.

Fragment Tagging in Bootstrap Messages

In a PIM network in which Nortel Networks and non-compliant routers interoperate, a non-compliant 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 non-compliant router, select the PIM_BSR_ZERO_FRAGMENT_TAG option at the RFC2362 Non-Compatibility parameter using Site Manager.

Non-Compliant Router Drops RP Advertisement with Zero Prefix

If you configure a non-compliant 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 non-compliant router drops any RP advertisement packet it receives from the RP router that contains a zero group prefix count. As a result, the non-compliant router cannot advertise RP set information to all PIM routers in the domain.

To ensure that the non-compliant router sends advertisement messages to all multicast group ranges using address 224.0.0.0/4, select the PIM_RP_ZERO_PREFIX_COUNT option at the RFC2362 Non-Compatibility parameter using Site Manager. Selecting this option sends non-zero prefix count in RP advertisement messages.

Incorrect Computation of Checksum of PIM Register Messages

By default, Nortel Networks routers computes checksum on the PIM header only. Compatibility issues arise when Nortel Networks routers interoperate with non-compliant routers which compute checksum on the PIM header *and* data portion of the packet.

To enable checksum compatibility with a non-compliant router, select the PIM_REGISTER_CHECKSUM option at the RFC2362 Non-Compatibility parameter using Site Manager.

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 non-compliant 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 non-compliant 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 non-compliant router to select the same RP.

CES and TDM on Passport 5430 Only

The following features and parameters are supported for the Passport 5430 only:

- Circuit Emulation Services (CES)
- Time Division Multiplexing (TDM)
- Traffic Shaping parameters: Service Category, AAL Type, VBR Type, Congestion indication, Cell loss priority, Initial and Minimum Cell Rates, Cell rate increase and decrease factors

MPOA and VRRP over LANE Support

BayRS Version 15.7.0.0 does not support running both Virtual Router Redundancy Protocol (VRRP) and Multi-Protocol Over ATM (MPOA) over LAN Emulation (LANE).

FRE-2 DRAM Requirements

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

Event Database

You can view the event database on the World Wide Web and the BayRS Online Library CD. To access the event database on the World Wide Web, go to: http://www25.nortelnetworks.com/library/tpubs/events/

To access the event database on the BayRS Online Library 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.

BayRS Flash Memory Requirements

BayRS software ships the following software suites (Table 16) on flash memory cards (PCMCIA) for each platform listed:

Table 16. BayRS Flash Memory Requirements

Platform	Flash Memory Required	Associated Software Suites
ARN	16 MB	corp_suite, ip_access, office_suite
ASN	16 MB	corp_suite, lan_suite, system_suite, wan_suite
BN	32 MB	atm_suite, corp_suite, corpfre2_suite, lan_suite, system_suite, vnr_suite, wan_suite
Passport 2430	16 MB	corp_suite, ip_access, office_suite
Passport 5430	32 MB	corp_suite, ip_access, office_suite

Support for Strata-Flash Card

BayRS supports the Strata-Flash card on ARN, ASN, and BN routers. For details about flash cards, see "Flash Memory Cards Supported" on page 65.

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.

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*.

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 17.

Table 17. 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 18.

Table 18. Default Settings for Serial Parameters with SDLC

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

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 upgrade CD.

- To configure a Nortel Networks RADIUS server, copy the three files to the directory that you define at installation time (typically C:\RADIUS\Service).

- To configure a non-Nortel 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 (VSAs). The Nortel Networks vendor ID is 1584. Use this ID in the header when using VSAs.

For more information about	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)*

Configuring Frame Relay PVCs with Site Manager

When creating a new PVC or moving a PVC out of the frame relay default service record in Site Manager, the circuit name must be filled in or the BCC will not recognize the PVC.

VRRP Guidelines

Follow these guidelines when configuring VRRP:

- You must first configure an IP address before you can configure a VRRP interface to associate with that specific IP address.
- If you have VRRP configured on the router and you want to delete the associated IP address, you must *first* delete VRRP before deleting the associated IP address. Failure to do so results in an unforced panic on the router which causes other protocols to go down and come back up.
- Bridging and VRRP should not be configured on the same physical port.

For additional information on configuring VRRP, see *Configuring VRRP Services* and the *BayRS Version 15.7.0.0 Document Change Notice*.

Operating Limitations and Cautions

Be aware of the following limitations and cautions when using BayRS 15.7.0.0.

APPN

The following limitations exist for APPN services in BayRS:

- The value configured for the Advanced Peer-to-Peer Networking (APPN) TG Number parameter in Site Manager is not being used; the TG number on a link station is being auto-negotiated.
- A ping from an Advanced Peer-to-Peer Networking (APPN) network node (NN) or end node (EN) may fail to reach the remote end nodes if the ENs are located downstream from branch network nodes (BrNNs) and connect to the BrNNs over connection networks.
- When an APPN router with high performance routing (HPR) enabled experiences heavy traffic, it restarts.
- If Advanced Peer-to-Peer Networking (APPN) traffic ingress and egress points are configured on different slots on a BN router, then the number of APPN transactions processed per minute is significantly lower than when all APPN traffic is restricted to a single slot. However, you can reconfigure the BN to run APPN on only one slot as a workaround to this limitation.

ARN 10MB Ethernet Base Module – MTU for 802.1Q Tagging

When you configure VLAN tagging on the ARN 10 MB Ethernet Base Module, the MTU for the interface is set to 1518 bytes for packets on this line. Although the Ethernet Base Module supports tagged packets, it does not support 802.1Q tagged frames of greater than 1518 bytes (1514 *plus* 4-byte tag). However, there are other Ethernet interfaces (for example, Ethernet and Tri-Serial Expansion Module or the 10/100-TX UTP Base Module) with an MTU of 1522 which support the maximum size tagged packet (1518 plus 4-byte tag). You may have to correct for this by reducing the MTU set for the other tagged hosts on the LAN attached to the 10BT motherboard Ethernet port to 1518 bytes.

ATM

The following limitations exist for ATM services in BayRS:

- Failover and load balancing for ATM VCs is 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.
- The ATM traffic parameter maximum burst size (MBS) is not supported.
- Differentiated Services Queue Management and Scheduling (DSQMS) is not supported in ATM.
- Using the BCC to delete an ATM interface or a service record with more than 570 PVCs can cause a watchdog timeout on the router. To prevent this from occurring on configurations with more than 570 PVCs, use Site Manager to delete the interface, or use the BCC to delete the PVCs before you delete the ATM interface.
- If there is a loss of signal to a router during a period of heavy traffic, the ATM interface on the router might stop functioning. If the ATM interface stops functioning, you must reboot the router to recover.
- On the ARE, BayRS 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.
- ATM signal ports on a switch and router must have the same version number. If you are using a switch with ATM signal ports set to V3.1, be sure to set the signaling setting on the router to V3.1 to prevent a conflict between the two devices. If you accept the default setting of V3.0 for the router, the router faults repeatedly until you change the setting to V3.1.

BCC

If a context is deleted and re-created in the same BCC source file, unexpected results may occur. The create/delete MIB is set to deleted when issuing the deletion, but it is not reset to created when reconfiguring the context.

BGP

The following limitations exist for BGP services in BayRS:

- If you specify a router interface address as the BGP peer address and that address is included in the network list for an announce policy configured on that router, BGP will not announce that network to a BGP peer, even if the remote peer is configured to accept that network from the peer. To ensure that the router announces the network, set the local peer to a router address that does not fall in the network range of an announce policy. For example, if the local router interface 2.2.5.1 falls within the range specified by the network list of an announce policy, use a different interface as the local BGP peer.
- Attempts to source a BCC config file with BGP peers configured fail while using the command: **peer** *<local>*/*<remote>* **as** *<value>*. When this error occurs, the router displays the message "BGP PEER Config Error. LOCAL is not a local IP address." However, the following workaround is available. You can prevent this problem by rearranging the commands in the source input file to make sure that the IP addresses are configured before the BGP peers.

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.

Differentiated Services

You can configure differentiated services on no more than one IP address of a multinetted IP interface. Differentiated services are not supported on ATM or Gigabit Ethernet interfaces nor on dial lines.

DLSw — SDLC Fast and Slow Poll Timer Defaults

If you have a router performing SDLC to LLC conversion, and you use the default values for the SDLC parameters Fast Poll Timer and Slow Poll Timer, SDLC controller performance is degraded. To avoid this problem, change the Fast Poll Timer to 200 and the Slow Poll Timer to 400. Changing these settings improves performance for both single- and dual-switch DLSw configurations in which the router acts as an SDLC primary device. Depending on the number of SDLC controllers you are supporting, you may need to increase or decrease the numbers to improve controller response time and router performance.

DLSw/APPN Boundary Port Use with AS400s and Others

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.

DSQMS

The following limitations exist for DSQMS in BayRS:

- Queue starvation can occur despite priority-time-quantum settings. Queues with the same priority level and priority-time-quantum settings may nevertheless experience queue starvation if one of the queues is bandwidth-heavy.

  To address this condition you can configure traffic policing for the bandwidth-heavy traffic flow to an acceptable rate for its assigned DSQMS Priority Queue. Configure traffic policing before the DSQMS outbound interface to control UDP as well as TCP flows.

- DSQMS is not supported on ATM or Gigabit Ethernet interfaces nor on dial lines.

- If you configure DSQMS on an Ethernet interface that is connected to an interface on a device that uses MAC addresses with leading zeros (4 bytes or more), packets may be corrupted because DSQMS interprets the zeros as baggage and removes this baggage from the packet.

DVMRP – Use with Multinetted IP Interfaces

You cannot use the BayRS Version 15.7.0.0 implementation of Distance Vector Multicast Routing Protocol (DVMRP) with circuits with multinetted interfaces (that is, interfaces with more than one IP address).

FireWall-1

The following problems can occur while using FireWall-1 services in BayRS:

- Check Point Log Viewer displays the incorrect time which is approximately one hour behind. For example, if the correct time is 12:17, the Log Viewer displays the time as 11:17. Log events from the management station (or fw daemon) display the correct time.
- Check Point Log Viewer incorrectly reports that a router has stopped logging. You can ignore the "Stopped Logging" message whenever the logging continues uninterrupted.
- You cannot define an address range for source and destination addresses for a FireWall-1 Security policy.
- You cannot disable FireWall-1 dynamically using the BCC even though the legal values for the state object of firewall are listed as enabled and disabled.
- FireWall-1 is not supported for the Passport 2430 or Passport 5430.
- Running the GUI version of Packet Capture (UNIX or Windows*) connected to an interface with FireWall-1 services configured may result in tag violations on several slots.

Flash Compaction or Extensive File Management Use on ARE

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.

GRE

If a Generic Routing Encapsulation (GRE) tunnel is configured with an incorrect remote physical IP address, and the IP address is then corrected, the GRE tunnel does not come up as expected. This condition occurs when you configure a GRE tunnel using either the BCC or Site Manager.

However, the following workaround is available. To change the remote physical IP address to a valid IP address for a GRE tunnel, first delete and then re-create the adjacent host entry (IP) or the static host entry (IPX) for that connection.

Hot-Swapping Link Modules

Attempts to remove and reinsert (hot-swap) a link module without first powering down the router can cause a fault to occur. Following the fault, the slot does recover. When a link module is hot-swapped, the protocols must reset, so there is no additional downtime caused by the fault. However, you can prevent this router fault by disabling the interfaces on the slot before removing the link module. After reinserting the link module you can then reenable the interfaces on the slot.

IPsec

If you change the setting of the router's Internet Protocol Security (IPsec) feature (MIB variable wfIpIntFCfgEnableSecurity) from Disabled to Enabled, the router loses its IP connection. You must reboot the router to recover.

IP Services

If you disable the IP directed broadcast feature while configuring a router, a global reset of IP occurs, resulting in a temporary outage and the closing of all IP utility sessions such as TCP and Telnet.

ISDN-BRI – Configuring B Channels on the ARN

The ARN can use only three B channels. If you select 2B + D service for one BRI interface, you must use 1B + D service for the second interface.

MIBs

The following limitations apply to router MIBs:

- The MIB-II ifIndex is incorrect after you delete a circuit, causing problems with Omniview. The router creates MIB-II attributes when you create circuits on the router platform. The MIB-II attributes include the ifNumber, which is the number of network interfaces (regardless of their current state) present on the system, and the ifIndex, which is a unique value for each interface (the ifIndex value is in the range from 1 through the value of ifNumber).

If you dynamically delete a circuit on the router, the MIB-II attribute ifNumber decreases by 1. If you check the IfIndex, the result will be noncontiguous. When the router is polled for ifNumber, it shows the correct value but when the ifIndex is polled, there is a chance that there are indexes/circuits outside the correct range.

The result is that SNMP management stations such as Omniview will display an error.

- If a router receives a Breath of Life (BofL) packet, the router considers it an unknown protocol. The router increments the MIB entry that tracks unknown protocols each time an interface receives a BofL packet, wfIfEntry.wfIfInUnknownProtos. However, you can disable BofL packets for the interface as a workaround to this problem.

NAT Services

The following limitations and cautions exist for NAT services in BayRS:

- NAT does not operate in IP ISP Mode. To avoid this problem you should disable the global IP ISP mode parameter.
- NAT and IPsec cannot interoperate with overlapping source IP address ranges, because NAT takes precedence. IPsec cannot process a source address that is also in a NAT address range. However, the following workarounds are available:

  For UNIX systems, you can separate IP hosts on the networks into two groups: a NAT-only group and an IPsec-only group. You can then use the multinetted interfaces or two network interface cards on a host to establish these two logical groups on one physical host.

  You can also configure NAT and IPsec on different devices so that one BayRS router runs IPsec and another BayRS router runs NAT.
- If you are using BayRS Version 14.20 or later, you must use Version 14.20 or later of the nat.bat script file.
- NAT cannot handle more than 600 dynamic translations at an inter-packet rate of less than 10 milliseconds. For inter-packet rates of 10 milliseconds or greater, NAT successfully handles 1500 dynamic translations per slot. These performance thresholds pertain to the BN, BLN, and Passport 5430 routers with 64 MB processor cards installed.

- If you are using NAT and FireWall-1 on the same router, the FTP application does not work correctly using port 20.
- When disabled, the NAT Install Private Address feature does not block advertisement of private addresses within a unidirectional NAT environment. This feature is set using Site Manager (Install Private Address) or the BCC (visible-private-address). In order to prevent a NAT private address from being advertised into the NAT public domain, a RIP announce policy filter or an OSPF announce policy filter must be configured (depending on which routing protocol is used).

  The following two sections describe how to configure RIP and OSPF announce policy filters for unidirectional NAT.

Configuring a RIP Announce Policy Filter for Unidirectional NAT

Configure a RIP announce policy filter to ignore the networks in the private domain. Using Site Manager (or the BCC), create a RIP announce policy and set the Action parameter to Ignore. You should then specify matching criteria for the RIP announce policy by entering the NAT private networks in the Networks list and entering the IP address of the NAT public interface in the Outbound Interfaces list.

For additional information about configuring RIP announce policies, see *Configuring IP, ARP, RARP, RIP, and OSPF Services*.

Configuring an OSPF Announce Policy Filter for Unidirectional NAT

Do *not* configure OSPF on the NAT private interface(s). Otherwise, you will not be able to prevent the advertisement of private networks into the OSPF domain because these routes will be considered OSPF internal routes. OSPF announce policy filters apply only to OSPF external routes.

For NAT to work with OSPF, the NAT router must be configured as an OSPF ASBR (Autonomous System Border Router). As an OSPF ASBR, the NAT private networks are injected into the OSPF domain as OSPF external routes. To prevent this, an OSPF announce policy filter must be configured on the NAT router. Using Site Manager (or the BCC), create an OSPF announce policy and set the Action parameter to Ignore. You should then specify matching criteria for the OSPF announce policy by entering the NAT private networks in the Networks list.

For additional information about configuring OSPF announce policies, see *Configuring IP, ARP, RARP, RIP, and OSPF Services*.

OSI

You cannot filter OSI over X.25 with a user-defined filter.

Passport 2430 and Passport 5430

The following limitations exist on the Passport 2430 and Passport 5430 platforms:

- RMON and Mini-RMON are not supported in the Passport 2430. RMON is not supported on the Passport 5430.
- The Passport 5430 does not support any LAN emulation services (LANE or MPOA).
- The Passport 2430 does not support ATM, except for ATM DXI.
- If you want to run either of the following protocols/configurations on the Passport 2430, you must upgrade the router to 32 MB of dynamic RAM (DRAM):

  – Advanced Peer-to-Peer Networking (APPN)

  – IP with MTU size greater than 2048 bytes on the Passport 2430
- Passport 5430 Ethernet flow control on the 10/100 Ethernet module does not function correctly when the flow control pause time in the received MAC control frame is set to 65535 (the default value). When the router receives a control frame with a pause time value of 65535, it begins retransmitting data prematurely. However, the following workaround is available. Reset the Flow Control Pause Time parameter in Site Manager, or the fc-pause-time parameter in the BCC, to a value from 32 through 65534.
- The BCC CES admin-status parameter does not work on the Passport 5430. If you attempt to disable the CES PVC using the BCC admin-status down command, the CES circuit continues to pass traffic. However, the following workaround is available. To disable the CES PVC, go back one level in the BCC and enter state disabled. To reenable the CES PVC, go back one level and enter state enabled.
- The Passport 2430 second Ethernet adapter module supports 10 Mb/s line speeds only. The interface does *not* support 100 Mb/s line speed, auto-negotiation, full duplex mode, or PPP over Ethernet (Payee). The second Ethernet adapter module *must be* installed on **slot one** of the Passport 2430 only.

- The following limitations exist for the Passport 5430 with the Quad Serial PMC module installed:
  - — Unsupported protocols include AOT, BOT, SMDS, and ATM DXI, and X.25.
  - — Quad Serial PMC module is *not designed* to be configurable using the inst_pp5430.bat script file.
  - — In a configuration where an Ethernet interface forwards data to all four serial interfaces of the Quad Serial PMC module at rates of 2 MB/second per port, the Ethernet interface stops. This issue does not occur at lower traffic rates. However, the supportable performance level has not yet been determined. Nortel Networks is investigating this issue in search of a fix that will support full rate use.
  - — If you set up back-to-back configuration on a Passport 5430 with a Quad Serial PMC module installed, you must set the internal clock speed to rates *no greater than* 128 Kb per second.

RADIUS

The following limitations and cautions exist for RADIUS services in BayRS:

- Setting the debug message level for RADIUS enables you to specify the amount of information contained in the messages logged by a device. When an authorized user sets the debug message level to high, debug messages containing the server secret (password) are logged by the device. Because any user can view the message log, this could potentially compromise the security of your network. If you must set the debug message level to high for debug purposes, be sure to complete the following steps to reset the debug message level and remove the server secret from the log following your debug:
  1. Using either the BCC or the Technician Interface, set the debug message level to no-debug (default) for the device.
  2. Clear the log to remove instances of the server secret that could potentially be viewed by users with any and all access privileges.
- Cutting and pasting BCC commands to configure RADIUS entries on the router may cause a fault in RADIUS to occur. This fault is caused by the timing delays introduced when commands are copied across the network to the router interface. To prevent this fault, use the BCC **source** command to enter RADIUS entries on multiple slots.

RIP Export Filters

Setting the From Protocols parameter for a RIP export filter to any value other than the “Any” option causes the filter to fail. Consequently, the RIP export route filter does not work if you specify any of the following options: RIP, EGP, OSPF, Direct, Static, or BGP-3. To avoid this problem, be sure to use the “Any” option when configuring all RIP export filters.

SFTP

Running multiple SFTP sessions concurrently can cause unpredictable behaviors on the router.

Sync

If the cable is removed from any synchronous port except octal sync on a BN, the router gives no indication of the problem and the link remains active. The configured WAN protocol closes all connections when the synchronous line driver detects connection signal lost. To prevent this problem, enable the Sync Polling parameter (Configuration Manager -> Edit Line -> Edit Sync Parameters).

SYSLOG

The status of syslog changes to down when you set the slot-lower-bound and slot-upper-bound parameters to the same value (same slot) on a BN router platform. Both syslog and filter logging terminate operation. However, the following workaround is available. Do not set the slot-lower-bound and slot-upper-bound parameters to the same value.

TFTP

If you try to use the Router File Manager to TFTP a file to the router from a Windows directory that includes long names and spaces, the transfer fails. To prevent this problem, move the file you want to send to a directory with a simple name of no more than 15 bytes and no space characters.

Unnumbered IP Interfaces

You cannot use the disable and enable scripts on unnumbered IP interfaces. The scripts do not allow an interface IP address format specifying both the IP address 0.0.0.0 and the circuit number. However, you can use Site Manager or the Technician Interface to disable unnumbered IP interfaces.

WAN Encryption

DES-40 WAN Encryption Option (WEP) or DES-56 WEP are no longer supported on any BayRS platform. However, BayRS will support backward compatibility with earlier versions of BayRS that are currently running WEP. We recommend that you use Internet Protocol Security (IPsec) services for security.

WCP

WCP for PPP Multilink

If you configure an existing PPP/WCP non-multilink circuit for multilink (on BayRS Version 12.10 or later) and the CCP Type parameter is set to CCP, WCP must be deleted and re-added to the circuit to negotiate WCP above the bundle.

See *Configuring Data Compression Services* for additional information.

Adding Bandwidth on Demand Disables WCP Data Compression

Adding Bandwidth on Demand to a PRI circuit disables WCP data compression. The call comes up and traffic flows, but WCP never creates a VC and does not compress traffic.

Using Hardware Compression with Small Packets Causes Latency

When the traffic pattern on at least one line of a multilink bundle is primarily small packets (i.e., 64 bytes), using hardware compression will result in latency. To avoid this problem, use software compression or remove any lines with this traffic type from the multilink bundle.

Protocols Supported

BayRS Version 15.7.0.0 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)
- Circuit Emulation Services (CES) for Passport 5430 only
- Classless interdomain routing (CIDR)
- Data compression (WCP and Hi/fn)
- Data link switching (DLSw)
- DECnet Phase IV
- Differentiated services (except on ATM, Gigabit Ethernet, and dial lines)
- Distance Vector Multicast Routing Protocol (DVMRP)
- Dynamic Host Configuration Protocol (DHCP)
- 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 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)
- Time Division Multiplexing (TDM) for Passport 5430 only
- 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 19 lists the Requests For Comments (RFCs) and other standards documents with which Version 15.7.0.0 complies. BayRS Version 15.7.0.0 might support additional standards that are not listed in this table.

Table 19. Standards Supported by Version 15.7.0.0

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
RFC 826	Ethernet Address Resolution Protocol

Table 19. Standards Supported by Version 15.7.0.0 *(continued)*

Standard	Description
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
RFC 1075	Distance Vector Multicast Routing Protocol (DVMRP)
RFC 1076	Redefinition of Managed Objects for IEEE 802.3 Repeater Devices

Table 19. Standards Supported by Version 15.7.0.0 *(continued)*

Standard	Description
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 1321	The MD5 Message – Digest Algorithm
RFC 1323	TCP Extensions for High Performance
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)

Table 19. Standards Supported by Version 15.7.0.0 *(continued)*

Standard	Description
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 ARN equipped with data collection module only
RFC 1762	PPP DECnet Phase IV Control Protocol (DNCP)
RFC 1763	PPP Banyan VINES Control Protocol (BVCP)
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)

Table 19. Standards Supported by Version 15.7.0.0 *(continued)*

Standard	Description
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
RFC 2138	Remote Authentication Dial-In User Service (RADIUS)
RFC 2139	RADIUS Accounting
RFC 2166	Data Link Switching, Version 2.0, Enhancements
RFC 2205	Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification
RFC 2328	OSPF Version 2
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
RFC 3101	The OSPF Not-So-Stubby Area (NSSA) 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 Nortel Networks routers.

Note: The Passport 2430 and 5430 platforms support 5-volt flash memory cards only. All other BayRS router platforms support both the 5-volt and 12-volt flash memory cards. See "BayRS Flash Memory Requirements" on page 41 for the flash memory requirements by platform.

Table 20 lists the flash memory cards approved for use.

Table 20. Approved Flash Memory Cards

Size	Vendor	Part Number
16 MB	Smart Modular (Centennial) Strata-Flash	FL16M-20-11736-J5
	Smart Modular (Centennial)	FL16M-20-11119
32 MB	Smart Modular (Centennial)	FL32M-20-11119
	Smart Modular (Centennial) Strata-Flash	FL32M-20-11736-J5